SYNGRESS
SHINDERBOOKS

1 YEAR UPGRADE
BUYER PROTECTION PLAN

SCENE OF THE Cybercrime

Computer Forensics Handbook

TOMO II

Bring Cybercriminals to Justice

- Protect Your Business, Home, Employees, and Family from Becoming Targets
- Learn Techniques for Collecting and Preserving Digital Evidence
- Hundreds of CyberLaw Reviews, On the Scene Sidebars, and CyberStats

Debra Littlejohn Shinder
Ed Tittel Technical Reviewer

Indice:

CAPÍTULO 7

CÓMO PREVENIR EL DELITO INFORMÁTICO

Tema que se analizan en este capítulo:

- Los conceptos de seguridad
- Los aspectos técnicos de la seguridad de redes
- Potenciar la seguridad de hardware y software
- Qué son los cortafuegos
- Creación de un equipo de respuesta ante incidentes
- Diseño y aplicación de políticas de seguridad

- Resumen
- Preguntas frecuentes
- Recursos

Introducción

Comprender qué es el delito informático y cómo puede cometerse es solamente parte de lo que debe conocer un investigador. Al igual que todo oficial de policía debe dominar las tácticas de defensa personal, el investigador del delito informático debe conocer las tácticas que comúnmente se utilizan para defender una red frente a intrusiones o ataques delictivos. En el presente capítulo analizamos los conceptos básicos referidos a la seguridad de computadoras y redes. Se ha incluido la importancia de la seguridad multicapas y los componentes que conforman un plan de seguridad multicapas. Asimismo, se hace énfasis en la necesidad de que los investigadores "hablen la jerga" aprendiendo la terminología de la seguridad computacional.

Analizamos la seguridad física, la primera (y en ocasiones obviada) línea de defensa. Mostramos cómo los administradores de redes mantienen la seguridad de las estaciones de trabajo y los servidores, y cómo un buen plan de seguridad va más allá de proteger los enrutadores, conmutadores, concentradores y otros dispositivos de conectividad de la red, así como el cable por el que viaja la señal (y del cual puede ser interceptada). También analizamos problemas especiales referidos a la seguridad física de computadoras portátiles y algunos productos innovadores que pueden ser utilizados para proteger estos equipos y la información que contienen.

También, nos adentramos en el fascinante y complejo mundo de la *criptografía*, el estudio de "la escritura oculta". Pasamos revista a las tecnologías y los algoritmos de cifrado y las múltiples maneras en que se puede utilizar el cifrado para proteger los datos que están almacenados en las computadoras o que viajan por una red. Aprenderá sobre los objetivos del cifrado en el contexto de la seguridad de redes y cómo puede facilitar la autenticación y la confiabilidad e integridad de la información. Hacemos un breve recuento de la criptografía y analizamos los protocolos de cifrado comunes que se utilizan actualmente. Igualmente, explicamos la diferencia entre *cifrado* y *estenografía*, y cómo estas dos técnicas son utilizadas de conjunto para aumentar la seguridad –tanto por parte de "los buenos" como por los delincuentes informáticos. Finalmente, analizamos las técnicas de criptoanálisis y descifrado, y cómo el programa criptográfico está siendo utilizado en la actualidad como una herramienta terrorista.

Pasando de la teoría a la práctica, hablamos seguidamente de cómo las organizaciones pueden aprovechar al máximo los productos de seguridad basados en el hardware y el software para proteger sus redes. Primero analizamos los dispositivos de hardware, incluidos los aparatos cortafuegos y dispositivos de autenticación como lectores de tarjetas con microcircuitos (o tarjetas inteligentes), escáneres de huellas dactilares, escáneres de retina e iris, y dispositivos de análisis de voz. Analizamos además soluciones con programas de seguridad, incluidos los programas de criptografía, los certificados digitales y la infraestructura de clave pública.

En la sección siguiente vemos cómo los cortafuegos –tanto físicos como lógicos– funcionan "tras bambalinas". Aprenderán sobre el filtrado por capas y cómo los mejores cortafuegos ofrecen protección en los niveles de paquete, circuito y aplicación. Seguidamente explicamos sobre la detección integrada de intrusos y la forma en que muchos productos cortafuegos se pueden configurar para efectuar ataques predefinidos cuando ocurre un ataque.

Una vez abarcados los aspectos específicos de los productos de seguridad disponibles, pasamos a otro punto de ka creación de un plan global de seguridad: cómo

conformar un equipo de respuesta ante incidentes para hacer frente, de manera rápida y eficaz, a los ataques cuando estos ocurren. No obstante, haber organizado dicho equipo no brindará la protección que necesita una organización, a menos que el equipo –y los usuarios y los profesionales de la TI que son la parte humana de la red– se rija por políticas de seguridad específicas que tengan como centro el plan de seguridad de la organización y lo incorporen al uso diario de los sistemas y la red. Por consiguiente, la última sección de este capítulo se refiere a por qué y cómo se pueden desarrollar sólidas políticas de seguridad, y aplicarlas para crear una base sobre la cual aplicar todas las medidas de seguridad que hemos expuesto, a la vez que colocamos la piedra angular del plan de la organización para prevenir el delito informático.

Los conceptos de seguridad de redes

En el Capítulo 6 aprendimos sobre los ataques y las intrusiones "técnicas" contra redes y la forma en que los piratas (o los aprendices de piratas) pueden explotar los protocolos, sistemas operativos y aplicaciones para cometer los delitos de acceso no autorizado, interrupción de comunicaciones de redes, y destruir o dañar la información en las computadoras. Es importante que los investigadores tengan al menos una comprensión básica de la forma en que se realizan estos ataques. También es importante que los investigadores conozcan cómo se puede proteger a las redes frente a nuevos ataques, por diversas razones:

- Durante la investigación de una intrusión o ataque, saber cuáles medidas de seguridad estaban aplicadas en el momento en que ocurrió el incidente podrá ayudar a reducir el rango de investigación sobre la naturaleza exacta del ataque e incluso quién pudo haberlo realizado.
- La comprensión sobre la forma en que funcionan las diversas medidas de seguridad puede conducir a los investigadores hasta los ficheros de registro (log files) y otras fuentes de información útiles en la investigación.
- Conocer las medidas y los conceptos de seguridad permite a los investigadores sugerir a las víctimas las formas en que pueden impedir que ocurran nuevos incidentes.
- Algunas de las medidas que utilizan "los buenos" para proteger sus redes y datos (como el cifrado) pueden también ser utilizadas por "los malos" para encubrir sus actividades delictivas.

El conocimiento es poder. Este es un viejo slogan de los piratas (junto con otras joyas como "la información quiere ser libre" y el simplista y optimistamente ambicioso "¡A piratear el mundo!"). No obstante, es una perogrullada que se aplica no solo a las personas que tratan de acceder a información que no deberían tener que ver, sino también a los que tratan de protegerse de los intrusos. El primer paso para ganar cualquier batalla –y la seguridad de redes es sin dudas una batalla por la propiedad y el control de sus ficheros de computadora-- es el mismo de toda la vida: "Conoce a tu enemigo".

A fin de proteger los recursos de una red frente al robo, los daños o la exposición no deseada, los administradores deben conocer quiénes son los que realizan estos actos, por qué y cómo lo hacen. El conocimiento lo dará poder también a usted, el investigador, y le dará más capacidad para detectar y procesar judicialmente a los intrusos y atacantes.

APLICAR LOS ASPECTOS BASICOS DE PLANIFICACION DE LA SEGURIDAD

En el diseño de la seguridad de los bienes electrónicos de una compañía frente a los delincuentes informáticos deben participar no sólo los miembros del departamento de las TI; debe participar toda la organización, de la misma manera que para que el trabajo policial en una comunidad sea eficaz se necesitan los esfuerzos de todo el departamento de policía y no sólo de una "división de servicio comunitario" aislada. Para que los investigadores del delito informático comprendan el proceso de planificación y puesta en práctica de la seguridad deben comenzar desde el principio, con los fundamentos de la seguridad informática. En la siguiente sección se ilustra cómo se puede aplicar uno de los principios esenciales de la seguridad tradicional al contexto del trabajo en redes de computadoras.

Definición de la seguridad

Una definición genérica del término *seguridad* (tomada del *American Heritage Dictionary*) es "estar libre de riesgo o peligro". Esta definición pueden tender a confundir cuando se le aplica a la seguridad informática y de trabajo en redes de computación, porque implica un grado de protección que es inherentemente imposible en el ambiente informático moderno orientado a la conectividad.

Es por ello que ese mismo diccionario brinda otra definición, en este caso específica para la ciencia de la computación: "El *nivel al cual* un programa o dispositivo está libre de ser usado in autorización" (el énfasis es nuestro). Implícita en esta definición está la advertencia de que los objetivos de *seguridad* y *accesibilidad* –las dos prioridades supremas para los administradores de red—son, por su propia naturaleza, diametralmente opuestos. Mientras más accesible sea la información, menor será su seguridad. De igual manera, mientras más seguridad se aplique a su información más se impedirá la accesibilidad de esta. Todo plan de seguridad es un intento por alcanzar un equilibrio entre ambos objetivos.

El primer paso es determinar *qué* necesitamos proteger, y cuál debe ser el grado de protección. Y es que no todos los bienes tienen igual valor, algunos necesitan una seguridad más estricta que otros. Determinar esto nos lleva al concepto de la aplicación de las capas múltiples de seguridad.

LA IMPORTANCIA DE LA SEGURIDAD MULTICAPAS

Un plan de seguridad efectivo no descansa en una sola tecnología o solución, sino que asume un enfoque multicapas. Comparemos este enfoque con las medidas de seguridad física de una empresa; la mayoría de las empresas no dependen únicamente de las cerraduras de las puertas de sus instalaciones para impedir la entrada de los intrusos y los ladrones. Por el contrario, posiblemente tengan además una cerca perimetral, seguridad externa adicional como guardias o perros guardianes, sistemas de alarma externos e internos, y, para proteger sus posesiones de valor, tienen tomadas otras medidas internas

como la existencia de bóvedas o cajas fuertes. La seguridad de la TI también debe estar estructurada en capas. Por ejemplo:

- Cortafuegos en los puntos de entrada a la red (y quizás una subred DMZ o filtrada entre la LAN y la interfaz de la red conectada a la Internet) que funcione como protección perimetral
- Protección de contraseñas en las computadoras locales, que requiera la autenticación de los usuarios para entrar y deniegue el acceso a las personas no autorizadas
- Permisos de acceso establecidos a recursos de red individuales para restringir el acceso de los que están conectados a la red
- Cifrado de la información que se envía por la red o que se almacena en disco a fin de proteger lo que sea especialmente valioso, sensible o confidencial
- Los servidores, enrutadores y concentradores deben estar situados en locales cerrados y con llave para impedir que las personas con acceso físico puedan apoderarse de información sin autorización para ello

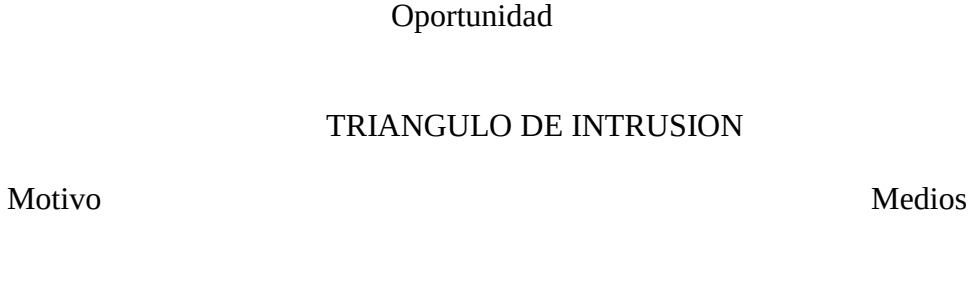
El triángulo de la intrusión

Los especialistas de la prevención del delito utilizan un modelo llamado Triángulo del Delito para explicar que antes de que pueda ocurrir un delito deben existir determinados criterios. Podemos adaptar a la seguridad de redes este concepto conocido en la esfera de la aplicación de la ley. Los mismos tres criterios del Triángulo del Delito deben existir para que se produzca una violación de la seguridad de una red. En la figura 7.1 se ilustran los tres vértices del triángulo.

Analicemos cada uno de ellos por separado:

- **Motivo.** Un intruso tiene que tener una razón para desear violentar la seguridad de una red (incluso si esa razón fuera solamente para pasar el rato.
- **Medios**. El intruso precisa tener la capacidad (ya sean los conocimientos de programación o, en el caso de script kiddies, el programa de intrusión creado por otros), de lo contrario no podrá violar nuestra seguridad.
- **Oportunidad**. El intruso precisa tener la oportunidad de entrar a la red gracias a fallas en el plan de seguridad, hoyos en un programa que abra una vía de acceso, o la proximidad física a los componentes de la red. De no existir la oportunidad para realizar la intrusión, el pirata potencial se marcharía a otra parte.

Figura 7.1 Los tres vértices del Triángulo del delito deben existir para que ocurra la intrusión



Si analizamos este criterio de intrusión veremos que en realidad hay un vértice del triángulo sobre el cual el administrador de red o el especialista de seguridad no tiene control. No es probable que alguien pueda hacer algo para eliminar el *motivo* del intruso. El motivo podría encontrarse en el tipo de información que hay en la red o incluso en la personalidad del intruso. Tampoco es muy posible con frecuencia poder impedir que el intruso obtenga los *medios* para violar la seguridad. Los conocimientos de programación están libremente disponibles y muchos piratas experimentados están más que dispuestos a ayudar a los que tienen menos experiencia. Lo único sobre lo cual pueden influir las personas dedicadas a impedir el delito informático es en la *oportunidad* que encuentren los piratas.

Para eliminar las oportunidades de intrusión

Los oficiales dedicados a la prevención del delito dicen a los miembros de la comunidad que probablemente no puedan evitar que un posible ladrón quiera robar, y sin dudas no pueden evitar que un posible ladrón adquiera las herramientas o los conocimientos que le permitan hacerlo. Lo que sí pueden hacer es eliminar, lo más posible, la oportunidad para que el ladrón actúe contra sus viviendas.

Ello significa poner cerrojos de seguridad en las puertas de sus viviendas (y usarlos); comprarse un perro grande y de fuerte ladrido al que no le gusten los extraños; e instalar un sistema de alarma. En otras palabras, el objetivo del dueño de casa no es impedir que el ladrón robe sino hacer de su casa un objetivo menos deseable. Para los "dueños" de redes, el objetivo es "reforzar" la red, de manera que todos los *hackers* que ya tengan el motivo y los medios vayan a buscarse una víctima más fácil.

Los mejores y más costosos cerrojos del mundo no impedirán la entrada de intrusos en su casa si usted no los utiliza. Y si esos cerrojos son difíciles de usar y le hace a usted difícil su salida y entrada a la casa, es muy probable que nos los use, o al menos no siempre. Un sistema de seguridad de redes insuficientemente implementado y que sea difícil de administrar o que cause indebidas molestias a los usuarios de la red puede acabar de la misma forma; con el tiempo, la persona encargada de su mantenimiento se halará de los pelos, se aburrirá de tratar y lo apagará todo. Con ello, la red quedará expuesta a los intrusos.

Hablar la jerga: terminología de seguridad

Toda industria tiene su propio vocabulario, la jerga que describe ideas, artículos, conceptos y procedimientos específicos de la esfera. Los abogados tienen su propia jerga, repleta de *por cuentos* y *por tantos*; los médicos y enfermeras utilizan términos que sólo ellos entienden, y los informes policiales están salpicados de abreviaturas para referirse a *perpetradores*, *víctimas*, entre otras categorías. La esfera de las redes informáticas son conocidas por su jerga técnica y la proliferación de siglas que a veces desconciertan a los no conocedores. Las esferas especializadas dentro de una misma industria en ocasiones también tienen sus vocablos específicos, y la subraya de la seguridad informática no es la excepción.

Quizás no sea absolutamente necesario que el investigador de delitos informáticos comprenda todos los aspectos técnicos de cómo funcionan las medidas de seguridad – pero conocer el lenguaje técnico que se utiliza para describir los conceptos y dispositivos de seguridad servirá, entre otras cosas, para:

- Le hará comprender qué puede y qué no puede lograr hacer un *hacker* en un determinado ambiente de red.
- Si usted es capaz de hablar la jerga –conversar inteligentemente sobre temas y medidas de seguridad– le será más fácil ganarse la confianza de los profesionales de las TI y comunicarse con ellos, que son los que brindan la mayor parte de la información que usted necesita para su investigación.

No es posible brindar aquí un glosario completo de términos relacionados con la seguridad, pero en esta sección presentamos la definición de algunas de las palabras y frases más comunes que se pueden encontrar al comenzar a explorar el fascinante mundo de la seguridad informática:

- **Algoritmo de encriptación:** Fórmula de cálculo que se aplica a los datos para cifrarlos.
- **Auditoria:** Seguir el rastro a sucesos relacionados con la seguridad, como la entrada al sistema o la red, el acceso a objetos, o ejercer derechos o privilegios de usuario/grupo.
- **Autenticación:** Verificación de la identidad de un usuario, computadora o proceso.
- **Autorización:** Las acciones que se permite hacer a un usuario, computadora o proceso una vez autentificado.
- **Cifrado:** Método utilizado para cifrar datos.
- **Clave:** Variable utilizada de conjunto con un algoritmo para cifrar o descifrar datos.
- **Confidencialidad de los datos:** Garantizar que el contenido de los mensajes se mantendrá en secreto. Véase además *integridad de la información*.
- **Criptografía (cripto):** Ciencia de ocultar información.
- **Encriptación:** El proceso de convertir datos (texto simple) en un formato (texto cifrado) que no puede ser leído ni comprendido por otras personas que no sean las autorizadas a recibirlos.
- **Fiabilidad:** La probabilidad de que un sistema o red de computadoras continúe funcionando satisfactoriamente durante un período de tiempo específico en condiciones normales de operación.
- **Gestión del riesgo:** El proceso de identificar, controlar y reducir al mínimo o eliminar totalmente los sucesos que constituyen una amenaza para la fiabilidad del sistema, la integridad de la información y la confidencialidad de esta.
- **Integridad de la información:** Garantizar que la información no ha sido modificada o alterada, que los datos recibidos son idénticos a los datos enviados.

- **Prueba de penetración:** Evaluar un sistema tratando de violar las medidas de seguridad de computadoras o una red.
- **Riesgo**: La probabilidad de que una amenaza de seguridad específica pueda explotar la vulnerabilidad de un sistema, provocando daños, pérdida de información u otro resultado no deseado.
- **TCSEC:** Siglas en inglés de Criterios fiables de evaluación de sistemas informáticos.
- **Texto cifrado:** Datos cifrados.
- **Violación:** Derrotar exitosamente las medidas de seguridad para tener acceso no autorizado a información o recursos, poner información o recursos
- **Vulnerabilidad técnica:** Falla o error en los componentes de hardware o software de un sistema que lo hacen vulnerable a la violación de la seguridad.
- **Vulnerabilidad:** Debilidad en el hardware, el software o el plan de seguridad que deja un sistema o una red abierta a la amenaza de un acceso no autorizado o el daño o destrucción de información.

NOTA

Para obtener definiciones de muchos otros términos referidos a la seguridad, véanse los siguientes sitios web:
www.securitypanel.org/glossary.html
www.mobrien.com/terminology.shtml
www.whatis.com

Importancia de la seguridad física

Uno de los aspectos más importantes, y a la vez más ignorados, de un plan integral de seguridad de redes es el control del acceso físico. A menudo, este asunto se deja en manos de los administradores de las instalaciones y los departamentos de seguridad de las plantas, o de compañías de guardias de seguridad contratados. Los administradores de redes se preocupan por las soluciones sofisticadas de hardware y software que impiden a los intrusos acceder a distancia a sus computadoras internas, a la vez que no hacen nada por proteger los servidores, enrutadores, cables y demás componentes físicos de la red respecto del acceso directo a ellos.

En demasiadas organizaciones supuestamente conscientes de la importancia de la seguridad, las computadoras permanecen todo el día encerradas fuera del alcance de los empleados y los visitantes, para después dejarlas por las noches accesibles al personal de limpieza, que usualmente tiene llaves de todas las oficinas. No es en absoluto inusual que los expertos del espionaje informático se hagan pasar por personal de limpieza a fin de poder tener acceso físico a las máquinas que contienen información sensible. Este es un método preferido por varias razones:

- Los servicios de limpieza a menudo son contratados a otras firmas; por ello, los directivos de una empresa tienen un control mínimo de la selección de las personas que son empleadas por el contratista, las cuales tienen acceso a las oficinas y otras partes de la instalación.
- Los trabajadores de limpieza a menudo son transitorios, por lo que los empleados de la empresa no podrán saber fácilmente quién es verdaderamente (o quién no es) empleado de limpieza.
- Las labores de limpieza por lo general se realizan durante horas avanzadas de la noche, cuando todos o la mayoría de los empleados se han marchado, lo que facilita aún más el robo subrepticio de información.
- Por lo general, el personal de limpieza es objeto de poca o ninguna atención por parte de los empleados de una empresa, quienes consideran su presencia algo normal y no se detienen a cuestionar la presencia de este personal en áreas donde se cuestionarían la presencia de otras personas.

Violentar la seguridad física del local donde se encuentra un servidor y robar el disco duro que contiene la información sensible sería un método burdo para cometer un delito informático; no obstante, sucede. En algunas organizaciones podría ser la forma más fácil de obtener el acceso autorizado, especialmente para un intruso que cuenta con ayuda "adentro". Una de las primeras cosas que haría un investigador ante un hecho de intrusión en una red es revisar las medidas de seguridad física, a fin de determinar si el acceso se logró por esta vía. Saber que el intruso se encontraba físicamente en el lugar reduce la lista de los posibles sospechosos, desde "todos los *hackers* de todo el mundo" hasta las personas que están o estuvieron en los alrededores.

No está dentro del ámbito de análisis de este capítulo entrar en detalles sobre cómo preparar la seguridad física de una red; no obstante, es importante comprender que el control sobre el acceso físico es el "perímetro externo" del plan de seguridad de cualquier organización. Garantizar el control sobre el acceso físico significa:

- Controlar el acceso físico a los servidores
- Controlar el acceso físico a las estaciones de trabajo en red
- Controlar el acceso físico a los dispositivos de la red

- Controlar el acceso físico al cable
- Estar al tanto de las consideraciones de seguridad con los medios inalámbricos
- Estar al tanto de las consideraciones de seguridad referidas a las computadoras portátiles
- Reconocer el riesgo de seguridad que entraña permitir que la información sea impresa
- Reconocer el riesgo de seguridad inherente a disquetes, discos compactos, cintas y otros medios removibles

Veamos cuál es la importancia de cada uno de ellos y cómo todos pueden ser abordados en el plan de seguridad física.

Protección del servidor

Los servidores de archivos en los que se almacena información sensible, así como los servidores de infraestructura que brindan servicios críticos, como autenticación de entrada y control de acceso, deben estar ubicados en locales altamente seguros. Como mínimo, los servidores deben estar en un local cerrado con llave, al cual tengan acceso solamente los empleados que precisan trabajar directamente con ellos. Las llaves deben ser distribuidas al mínimo, y se deben llevar registros de entrega y devolución de las llaves.

Si las necesidades de seguridad son elevadas debido a la naturaleza de la actividad o de la información, el acceso al local del servidor debe estar controlado por tarjeta magnética, cerrojos electrónicos que requieran la introducción de un código numérico, o incluso dispositivos biométricos de control de acceso, como escáneres de huellas dactilares o de retina. Otras medidas de seguridad son detectores u otros sistemas de alarma activados durante el horario no laborable, así como cámaras de seguridad. Estos dispositivos deben ser vigilados por un guardia de seguridad o una compañía dedicada a este trabajo.

Mantener la seguridad de las estaciones de trabajo

Muchos planes de seguridad de redes se concentran en los servidores pero ignoran el riesgo que representan las estaciones de trabajo que tienen acceso a ellos mediante la red. No es nada inusual que los empleados dejen sus computadoras sin protección cuando van a almorzar, o incluso cuando se marchan al concluir la jornada de trabajo. A menudo hay una estación de trabajo en el área de la recepción que está abierta al público de la calle que viene de visita. Si la persona que está atendiendo la recepción tiene que ausentarse brevemente, la computadora –y la red a la que está conectada—quedan vulnerables a menos que se hayan tomado medidas para garantizar su seguridad.

Un buen plan de seguridad incluye la protección de todas las estaciones no atendidas por una persona. Un sistema operativo de clientes seguro como Windows NT o Windows 2000 requiere un proceso de entrada interactivo con un nombre de cuenta y contraseña válidos a fin de lograr el acceso al sistema operativo (a diferencia del caso de Windows 9x). Estos sistemas permiten que el usuario "cierre con seguro" la estación de trabajo cuando se va a alejar de ella, de manera que otra persona no pueda llegar y comenzar a utilizar la computadora. Las organizaciones no deben depender solamente del permiso de acceso y otros métodos de seguridad de software para proteger la red. Si

un intruso potencial logra tener acceso físico a una computadora en red, estará más cerca de acceder a información valiosa o a introducir un virus en la red.
Algunas computadoras personales modernas vienen con una especie de mecanismo de cierre que ayuda a impedir que personas no autorizadas abran el chasis y roben el disco duro. También hay cierres que impiden el uso de las torres de disquetes, la copia de información a disquete, o el rearranque de la computadora a partir de un disquete.

Protección de los dispositivos de red

Los concentradores, enrutadores, conmutadores y otros dispositivos de red deben estar físicamente seguros frente al acceso no autorizado. Es fácil olvidar que simplemente porque un dispositivo no tiene un monitor por el cual *ver* la información, ello no significa que la información no pueda ser capturada o destruida en el punto de acceso.

Por ejemplo, un concentrador de ethernet tradicional exporta todos los datos desde todos sus puertos. El intruso que logre acceder al concentrador puede conectar un dispositivo "rastreador de paquetes" (o una computadora portátil con un software rastreador) que opere en un "modo promiscuo" en un puerto libre y capturar toda la información enviada a cualquier computadora de ese segmento, como se muestra en la figura 7.2.

Si bien los conmutadoras y enrutadores son de cierta manera más seguros que los concentradores, todos los dispositivos por donde pasa la información es un punto vulnerable. Sustituir los concentradores por conmutadores y enrutadores dificulta a los intrusos "husmear" en la red. Sin embargo, es posible utilizar técnicas como la de *redireccionamiento de enrutador* mediante suplantación de identidad en ARP, donde las máquinas cercanas son direccionadas para que envíen el tráfico a través de la máquinas del intruso, al enviar paquetes ARP que contienen la dirección IP del enrutador asignada a la dirección MAC de la máquina del intruso. El resultado de esto es que las otras máquinas creen que la máquina del intruso es el enrutador, y así le envían a ella su tráfico. Un método similar es el que usa mensajes de anuncio de enrutador ICMP.

Figura 7.2 Un intruso que tenga acceso a un concentrador puede interceptar la información fácilmente .
(Insertar aquí la figura que aparece en la página 360 del original)

Toda la información sale por todos los puertos
Concentrador
Conexión a un puerto libre
Laptop no autorizada

Con determinados conmutadores se puede desbordar las tablas de direcciones con múltiples direcciones MAC falsas o enviar un flujo continuo de basura aleatoria por el conmutador para hacerlo pasar de modo de enlace a modo de repetición. Ello significa que todos los cuadros serán transmitidos por todos los puertos, dándole al intruso la misma oportunidad de acceder a la información como si estuviera utilizando un concentrador normal. A esta actividad se le denomina *abarrotamiento de conmutador*. Si el conmutador tiene un puerto de monitor especial destinado a ser utilizado con un husmeador (sniffer) para fines legítimos (solución de problemas de red), el intruso que

tenga acceso físico a este conmutador puede simplemente conectarse a este puerto y capturar la información de la red. Por estas razones, todos los dispositivos de red deben estar ubicados en un local cerrado con llave; los administradores deben proteger sus dispositivos de la misma manera que protegen los servidores.

Asegurando el cable

El paso siguiente para proteger la red y su información es asegurar el cable por el que viajan los datos. Tanto el cable par-torcido (twisted-pair) como el coaxial son vulnerables a la captura de la información; el intruso que tenga acceso al cable puede interceptarlo y recuperar los mensajes que se envían por él. Hay varias empresas que confeccionan dispositivos de "intercepción". El cable de fibra óptica es más difícil de interceptar porque no produce pulsos eléctricos sino que usa pulsos de luz para representar los 0 y los 1 de los datos binarios. No obstante, un intruso con técnicas avanzadas puede utilizar un separador óptico e interceptar la señal en un medio de fibra óptica. Los dispositivos de intercepción de cable a veces pueden ser detectados utilizando un reflectómetro temporal de dominio (TDR) o un TDR óptico para medir la fuerza de la señal y determinar dónde está el dispositivo de intercepción.

El compromiso de la seguridad al nivel físico resulta una amenaza especial cuando los cables de red no están en una instalación sino que se extienden entre edificaciones. Este riesgo tiene incluso un nombre: *Manipulación subterránea* (manhole manipulation), que hace referencia al fácil acceso que en ocasiones tienen los intrusos a los cables que corren por conductoras subterráneas.

NOTA

Las conexiones inalámbricas son incluso más susceptibles de ser interceptadas que las conexiones por cable. Los cables al menos se pueden esconder dentro de la infraestructura, dificultando así su acceso. Las transmisiones inalámbricas viajan por las ondas aéreas y pueden ser "atrapadas " por cualquier persona que tenga el deseo y el equipo apropiado para hacerlo. En el Capítulo 8, "Puesta en práctica de la seguridad SW sistemas" analizamos cómo mantener la seguridad de las conexiones inalámbricas.

Con laptop se puede viajar

Las computadoras portátiles –laptops, notebooks y computadoras de mano plenamente funcionales como las Pocket PC (computadoras de bolsillo) y las Palm OS (computadoras de mano) —presentan sus propios problemas de seguridad por las mismas características que las hacen populares: su tamaño pequeño y su movilidad. La seguridad física de las computadoras portátiles es especialmente importante dada la facilidad con que puede robarse el equipo junto con la información.

Afortunadamente un gran número de empresas producen dispositivos de protección contra robos y programas de seguridad para laptops. Los dispositivos de cierre y las alarmas son fáciles de obtener, además de los programas de software que deshabilitarán las funcionalidad de la laptop en caso de robo, o incluso ayudan a rastrearla haciendo que la computadora "realice una llamada telefónica a casa" la primera vez que la computadora portátil es conectada a un módem. Además, los datos o la información que contienen las computadoras portátiles se pueden encriptar a fin de impedir el acceso a esta en caso de que el equipo sea robado.

Figura 7.3 Los programas de rastreo pueden ayudar a recuperar las computadoras portátiles robadas.
(Insertar aquí la figura que aparece en la página 362 del original. El texto del gráfico está traducido de izquierda a derecha, de arriba hacia abajo)

El usuario informa al Centro de Monitoreo sobre la laptop perdida
La laptop robada "telefonea a casa" cuando es conectada a un módem
Laptop
Módem
El Centro de Monitoreo registra la ubicación de la laptop (línea telefónica o dirección de IP) e inicia el proceso de recuperación
Módem
Centro de Monitoreo del proveedor de software de seguridad

Un ejemplo del software de recuperación y rastreo de laptops es Cyber Angel (www.sentryinc.com) de Computer Sentry Software. Otro producto, TrackIT (www.trackitcorp.com) es un dispositivo antirrobo de hardware para chasis de computadora y otros.

Algunas laptops vienen con discos duros removibles. Si el usuario tiene información altamente sensible a la que deba tener acceso con una laptop, resulta conveniente almacenarla en un disco removible (hay múltiples discos PC Card y los que se conectan a un puerto paralelo) y encriptarla. El usuario debe además no tener ese disco cerca de la computadora cuando no lo esté utilizando.

NOTA

La posibilidad de robo no es el único motivo por el cual las laptops son un riesgo para la seguridad. Otro riesgo para la red es que un ladrón de información que logre entrar a las instalaciones físicas puede conectar una laptop a la red, *crackear* las contraseñas u obtener una contraseña por medio de ingeniería social, y bajar la información al equipo portátil, el cual puede después llevarse fácilmente.

La caza del papel

Los especialistas de la seguridad de redes y los administradores tienden a concentrarse en proteger la información en formato electrónico, pero los intrusos también pueden robar información digital confidencial imprimiéndola o localizando una copia en papel impresa por otra persona. No vale de mucho aplicar estrictas políticas de contraseñas y controles de acceso a la red si los empleados pueden imprimir material sensible y dejarla sobre el buró, dentro de gavetas abiertas o dentro de cestos de basura asequibles. La práctica del "buceo en la basura" (en busca de secretos empresariales) es una forma común de espionaje corporativo que, sorprendentemente, a menudo da resultado.

Si es necesario imprimir información confidencial, la copia en papel debe ser mantenida bajo la misma seguridad física que la versión digital. Su eliminación debe incluir su destrucción en trituradora de papel, y en casos de información que requiera una

medida de seguridad especialmente elevada, el papel triturado se debe mezclar con agua para crear una pulpa que sea imposible de reamar posteriormente.

Riesgos con los dispositivos de almacenamiento extraíbles

Otro punto de posible falla del plan de seguridad de redes se refiere a la información en los medios removibles. Los disquetes, discos Zip y Jaz, cintas, tarjetas de PC, discos compactos y discos de DVD que contengan información sensible deben ser guardados en condiciones de seguridad física en todo momento. Como veremos en el capítulo 10, "Recopilación y preservación de evidencia digital", borrar los archivos de un disco, o incluso formatearlo, NO elimina totalmente la información; esta permanece allí y puede ser recuperada mediante un software especial hasta tanto sea sobrescrita.

Si bien los medios removibles pudieran representar una amenaza a la seguridad de la red, pueden también desempeñar un rol importante en el plan de seguridad integral, si se les usa adecuadamente. Los discos removibles (incluidos los discos duros de gran capacidad plenamente cargables [buteables] instalados) pueden ser retirados de la computadora y guardados en una caja fuerte o sacados del recinto para proteger los datos que contiene.

Los conceptos básicos de la criptografía

Criptografía es una palabra que se deriva del griego *kryptos* ("oculto"), y el uso de la criptografía es cientos de años anterior a la invención de las computadoras. La manera de mantener seguros los secretos ha sido desde hace mucho tiempo preocupación del ser humano, y el objetivo de la criptografía es esconder la información o cambiarla a fin de hacerla incomprensible a las personas a las cuales no está destinada. Las técnicas de criptografía incluyen:

- **Encriptación:** mediante esta se aplica un algoritmo al texto simple para convertirlo en algo incomprensible para alguien que no sepa descifrarlo.
- **Esteganografía:** es un medio para esconder la existencia de la información, no solamente su contenido. Usualmente esto se hace ocultando la información dentro de otro de carácter inocuo.

NOTA

Los términos criptografía y encriptación a menudo se utilizan indistintamente, pero la criptografía es un término mucho más amplio que el de encriptación. Esta última es una especie de criptografía. Es decir, toda encriptación es criptografía, pero no toda la criptografía es encriptación.

Objetivos de la seguridad criptográfica

Las técnicas criptográficas son una parte importante del plan de seguridad multicapas. Algunas medidas de seguridad, como la aplicación de un cortafuego y el uso de permisos de acceso, tienen en objetivo de intentar evitar la entrada de intrusos a la red o a las computadoras, muy parecido a la forma en que las cercas y los cerrojos de puertas intentan evitar el paso de ladrones. La criptografía brinda una línea interna de defensa. Como una caja fuerte en la pared cuya objetivo es brindar protección en caso de que el

ladrón llegue a penetrar en la casa –y proteger las posesiones de valor frente a personas que estén autorizadas a entrar en la casa—la criptografía protege la información frente a intrusos que logren burlar las defensas externas y frente a los autorizados a acceder a la red pero no a esta información en particular.

Las técnicas criptográficas abordan estos tres objetivos básicos:

- **Autenticación**: verificar la identidad de un usuario o una computadora
- **Confidencialidad**: mantener el carácter secreto de la información
- **Integridad**: garantizar que la información no varía desde el momento en que sale de la fuente hasta que el momento en que llega a su destino.

Uno o varios de estos objetivos será el prioritario en dependencia de la situación específica. Por ejemplo, si un investigador recibe una instrucción de su jefe de que debe viajar a la costa occidental para entrevistar a un testigo de un caso, la principal preocupación debe ser saber si en realidad fue el Jefe de Policía quien envió el mensaje y no un oficial que deseaba gastar una broma. En este caso, autentificar la identidad del remitente es de importancia suprema. Si el caso se refiere a una investigación de orden interno y resulta importante que nadie del departamento sepa hacia dónde se dirige el investigador, la confidencialidad de la información deberá ser también importante. Y si el mensaje dice que el investigador está autorizado a gastar $3000 en el viaje, deberá ser importante también garantizar que la información no se haya alterado (después de todo, los jefes no suelen ser ten generosos) en el camino, es decir, que la integridad del mensaje no se ha visto comprometida.

Los tres mecanismos se pueden utilizar de conjunto, o por separado cuando solamente una o dos de estas consideraciones son importantes. En la próxima sección analizamos cómo funcionada cada una relación con la seguridad de redes.

En la escena…

Perspectiva histórica de la criptografía

Es probable que la criptografía haya existido desde que existe el lenguaje escrito. Según dice Fred Cohen en su *A Short History of Criptograhy* (www.all.net/books/ip/Chap2-1.html), el estudio de la criptografía data de 4000 años o más atrás. Siempre que se hacen registros de comunicaciones surge el tema de cómo protegerlas.

Tanto en las comunicaciones corporativos como personales no siempre es conveniente que su contenido sea conocido por todos –de hecho, si así fuera los resultados sería a menudo desastrosos. Por ello, las primeras civilizaciones buscaron formas para ocultar de ojos indiscretos el contenido de los mensajes. En el antiguo Egipto se utilizaron con ese objetivo desviaciones del lenguaje de jeroglífico. Los griegos utilizaron un "código de transposición" en el cual cada letra del alfabeto era representada por otra que indicaba dónde estaba ubicada la letra en una serie de hileras. En la India, en tiempos remotos, los espías empleados por el gobierno utilizaban "códigos de sustitución"sobre una base fonética (el mismo sistema que utilizan los niños parar hablar en jerigonza). En los tiempos bíblicos, un método de cifrado por sustitución llamado *atbash* –que funcionaba sustituyendo la última letra del alfabeto hebreo por la primera y así sucesivamente– fue utilizado para encriptar los documentos. Los métodos de encriptación también fueron utilizados por personalidades históricas tan disímiles como Julio César (cuyo nombre lleva "la cifra César"), Thomas Jefferson (que inventó la rueda de cifrado), y Sir Francis Bacon. Desde hace muchos años los gobiernos utilizan la encriptación para proteger los mensajes militares secretos.

Autenticación de la identidad

Se pueden utilizar muchos métodos para autentificar la identidad de un usuario (o, en muchas oportunidades, de una computadora). En general, se solicita al usuario que brinde algo que esté relacionado con su cuenta y que no pudiera ser dado fácilmente por otra persona. La credencial solicitada por lo general cuenta de uno (o más) de los siguientes aspectos:

- **Algo que usted conoce**: Una de las formas de determinar si una persona es realmente quien afirma ser es preguntarle algo que solamente sabría esa persona. Si usted intercambia mensajes en línea con alguien que supuestamente es su hermano, antes de hablar de temas sensibles o personales podría preguntarle cómo se llama la hermana mayor de su madre, o pedirle que le diga el nombre que ustedes dos tocaban al piano a dúo de pequeños. En la seguridad de la información, aquello que solamente uno conoce es usualmente una contraseña o un número de identificación personal (PIN, por sus siglas en inglés).
- **Algo que usted tiene**: Las contraseñas pueden ser descubiertas, como vimos en el capítulo 6. Por ejemplo, se puede descubrir una contraseña mediante un ataque de fuerza bruta o mirando por encima del hombro del usuario cuando este escribe la contraseña. En muchos de estos casos, el usuario no sabe que

alguien más conoce la contraseña. Un mejor método de autenticación es requerir que el usuario presente un algo físico, como una "tarjeta inteligente" (dispositivo del tamaño de una tarjeta de crédito con un chip que contiene información de autenticación). Si la tarjeta se pierde o es robada, es probable que el usuario se percate de ello. Las tarjetas inteligentes se utilizan para entrar a redes de computadoras y para acceder a cuentas bancarias y efectuar compras.

- **Algo que usted es**: Si bien la tarjeta u otro objeto físico que deba estar en poder del usuario constituye un paso de avance respecto de la autenticación por contraseñas, las tarjetas se pueden perder o pueden ser robadas o incluso duplicadas. Un método aun mas seguro de comprobar la identidad es verificando quién es usted, es decir, información biológica como huellas dactilares, registro de voz, o una imagen de la retina o el iris. Los métodos biométricos son mucho más difíciles de burlar que otros métodos de identificación.

NOTA

En alguna literatura sobre seguridad se hace mención a un cuarto método para comprobar la identidad *algo que usted hace*. Un ejemplo sería una muestra de su escritura, y en esta categoría podría incluirse también los registros de voz.

En la escena…

Burlando mecanismos de autenticación "a prueba de fallas"
En el 2000, un ingeniero/*hacker* francés llamado Serge Humpich (también conocido como "el Conde de Monte Cripto") logró descifrar la clave de 640 bits utilizada por las tarjetas inteligentes emitidas por los bancos de Francia y que millones de consumidores franceses empleaban para hacer sus compras. El equipo que utilizó para descifrar la clave costaba solamente 250 dólares.

Hasta los métodos supuestamente libre de falla no lo son. Ello se debe a que la información biométrica debe ser analizada por un programa de computación y todo el que ha trabajado con computadoras sabe que no existe ningún programa que funcione a la perfección. Es por ello que los vendedores de soluciones biométricas establecen límites de tolerancia de fallas que están basadas en un determinado nivel de índices de rechazo falso y aceptación falsa (denominados respectivamente, FRR y FAR [por sus siglas en inglés]). El *rechazo falso* ocurre cuando un usuario autorizado es rechazado por el sistema, y *la aceptación falsa* ocurre cuando un usuario no autorizado es aceptado por el programa y obtiene así el acceso. De hecho, los escáneres de huellas dactilares han sido burlados por métodos tan simples como soplar sobre la superficie del censor para reactivar una huella dejada en él anteriormente o al aplicar polvo de grafito sobre una huella aún latente sobre el sensor para después aplicar cinta adhesiva sobre la superficie y ejercer una ligera presión sobre ésta. Estas técnicas son ejemplos de *reactivación de imagen latente* en un caso muy divulgado en mayo de 2002 un criptógrafo de Japón logró crear una huella dactilar falsa utilizando gelatina con la cual afirma haber burlado los equipos de detección de huellas en 80 de unas 100 ocasiones.

Para más información sobre la confiabilidad de los dispositivos biométricos, véanse los siguientes artículos: www.heise.de/ct/english/02/11/114/ y http://theregister.co.uk/content/55/25300.html.

Dado que ninguno de estos métodos de autenticación, ni ningún otro, está absolutamente exento de fallas, en un entorno de alta seguridad resulta sensato utilizar un sistema de autenticación multifactorial (en ocasiones denominado *autenticación bipartita* o *tripartita*, en dependencia de la cantidad de métodos de autenticación utilizados) combinando dos o más de ellos. Es decir, el usuario deberá presentar algo que tiene *y* algo que conoce (de hecho la mayoría de las tarjetas inteligentes para funcionar requieren que el usuario no solamente las inserte en el dispositivo lector sino que debe también introducir un PIN), o deberá someterse a un detector biométrico e introducir una contraseña para poder obtener el acceso.

Otro método es la *autenticación por capas* mediante la cual se acepta una forma de autenticación para conceder un nivel de acceso inferior, y se requiere una autenticación adicional para obtener un nivel de acceso más elevado. Para más información sobre este concepto véase el artículo de Jeff Parker titulado *Layered Authentication* en http://rr.sans.org./authentic/layered.php.

¿Cuándo es necesaria la autenticación?

Existen diferentes circunstancias en las que la autenticación es necesaria, a la vez que en circunstancias diferentes se utilizan métodos de autenticación diferentes. Por ejemplo:

- **Autenticación de entrada:** Cuando los usuarios acceden por primera vez a una computadora o a la red (lo cual se denomina entrar) un sistema operativo seguro le exige que el usuario confirme su identidad a una base de datos de cuentas de seguridad. Para entrar a una computadora local, el usuario debe ingresar el nombre y contraseña de cuenta que están almacenados en una base de datos de seguridad local en el disco duro de esa máquina. Cuando se entra a una red con base en un servidor (con un dominio de Windows NT/2000/.NET o a una red NetWare NDS) el usuario debe escribir un nombre y contraseña de cuenta que se encuentre en la base de datos de autenticación del servidor. Además, los dominios de Windows requieren que las computadoras con NT/2000/XP Pro/.Net tengan una cuenta de computadora para poder unirse al dominio. (Las credenciales de la computadora son enviadas automáticamente al controlador del dominio, sin intervención del usuario). No obstante, el usuario que tenga una cuenta en el dominio puede entrar desde una computadora no segura, como una máquina con Windows 9x/ME/XP Home. Windows NT usa autenticación NTLM, mientras que Windows 2000 –si bien soporta NTLM en aras de la compatibilidad con programas anteriores— tiene predeterminada la autenticación Kerberos. (En la siguiente sección, *Protocolos de autenticación*) se analizan el NTLM, Kerberos y otros protocolos).
- **Autenticación de acceso remoto**: Cuando el usuario accede a la red por una conexión remota (telefónica o VPN)**,** la seguridad adquiere una importancia especial porque la computadora con la cual se está accediendo no está físicamente conectada por cable a la red local. Para la autenticación de acceso remoto se utilizan protocolos diferentes. Cuando se realiza una entrada remota, el cliente remoto y el servidor de acceso remoto generalmente negocian un método y protocolos de autenticación para cuto soporte ambos han sido configurados. Existen diferentes métodos para autentificar usuarios remotos, algunos de los cuales se analizan en la próxima sección, *Protocolos de autenticación*.

NOTA

En una red que utilice un servidor de autenticación, los usuarios son autentificados cuando entran a la red, a partir de lo cual el acceso a los recursos individuales de la red es controlado sobre la base del permiso concedido a la cuenta con la cual el usuario ha entrado. En redes de grupos de trabajo (llamadas "peer-to-peer" o "igual a igual"), no hay servidor de autenticación, pero el acceso a los recursos se puede proteger utilizando la seguridad a nivel de archivos. Se asignan contraseñas a recursos individuales, y esas contraseñas son entregadas a los usuarios con autorización para acceder a ellos. Cada vez que un usuario desee abrir un archivo específico o utilizar una impresora determinada deberá ingresar la contraseña correcta. Este proceso no es realmente un proceso de autenticación, ya que no se verifica la identidad del usuario (la contraseña no está asociada a una cuenta de usuario), si bien al ingresar la contraseña el usuario está demostrando que está autorizado a acceder al recurso.

Protocolos de autenticación
Los protocolos que se utilizan para autentificar la identidad dependen del tipo de autenticación. Entre los protocolos que comúnmente se utilizan están:

- **Kerberos**: es un protocolo de autenticación de entrada basado en una criptografía de clave secreta (simétrica). Usualmente utiliza el algoritmo DES o Triple-DES (3DES), aunque en la versión más reciente, la Kerberos v5, se pueden utilizar otros algoritmos, además del DES. El Kerberos utiliza un sistema de vales para la verificación de la identidad en diferentes servidores en toda la red. El sistema trabaja de cierta manera como un sistema de pago en los parques de diversiones o ferias en las que, en lugar de pagar por cada vuelta en cada aparato, los clientes deben comprar vales en una casilla central y con ellos acceder a cada equipo. De igual manera, con Kerberos, el cliente que desee acceder a los recursos de los servidores de la red no es autentificado por cada servidor sino que todos los servidores dependen de "Vales" emitidos por al servidor central denominado Centro de Distribución de Claves (KDC, por sus siglas en inglés). El cliente envía una solicitud de vale (encriptada con la clave del usuario) al KDC. El KDC emite un vale llamado TGT (por las siglas en ingles de Ticket-Granting Ticket o vale que concede vales), el cual está encriptado y es enviado al Servicio de concesión de vales (TGS, por las siglas en inglés de Ticket-Granting Service, o servicio de concesión de vales). El TGS puede estar en el mismo equipo físico que tiene el KDC. El TGS emite un vale de sesión al cliente para que acceda al recurso de red específico solicitado (que usualmente está en otro servidor). El vale de sesión es presentado al servidor que hospeda el recurso y se concede el acceso. La clave de sesión es válida solamente para esa sesión en particular y está programada para expirar al concluir un período de tiempo determinado. El Kerberos permite la autenticación mutua; es decir, se puede verificar la identidad del usuario y del servidor. Para una explicación más detallada del funcionamiento de Kerberos, véase *Kerberos v5 Administratrors Guide (Guía para los administradores de Kerberos v5* en www.Ins.cornell.edu/public/COMP/krb5/admin/admin_2.html.
- **NT LanMan o NTLM** es otro método de autenticación de Microsoft, utilizado por los dominios de Windows NT y soportado por Windows 2000 en caso de que computadoras con "niveles inferiores" (las que operan con NT o Windows 9x) deseen entrar a la red. La actual versión, NTLMv2, brinda más seguridad que NTLMv1. La versión 2 es soportada por Windows 2000 y NT 4.0 con SP4 o superior. Si el software de cliente de Servicios de Directorio (disponible en el CD-ROM Servidor de Windows 2000) está instalado en una computadora con Windows 9x, se puede utilizar el NTLMv2; no obstante, para habilitarlo es preciso editar el registro. A diferencia de Kerberos, con el NTLM, cuando un cliente desea acceder a los recursos del servidor, ese servidor debe contactar al controlador del dominio para verificar la identidad del cliente. El cliente no posee credenciales preemitidas (que en Kerberos

serían los vales de sesión) en las que pueda confiar el servidor de archivos o de aplicaciones.

- **Protocolo de autenticación de contraseñas (PAP, por Password Authentication Protocol en inglés):** es un protocolo de autenticación de acceso remoto utilizado para conexiones PPP (telefónicas). Su característica distintiva (y la razón por la cual no debe utilizarse en redes seguras) es que envía contraseñas en texto simple. Ello significa que las contraseñas pueden ser interceptadas mientras son transmitidas y utilizadas por una persona no autorizada. La única buena razón para utilizar el PAP es cuando el servidor remoto no soporta otro método de autenticación segura. El Shiva PAP (S-PAP) resuelve este problema utilizando un método de autenticación bidireccional reversible que encripta las contraseñas de manera que no puedan ser interceptadas y utilizadas indebidamente.
- **Protocolo de Autenticación Challenge Handshake (CHAP) (Challenge Handshake Authentication Protocol) (CHAP):** utiliza un algoritmo de *hash* y un secreto compartido (sobre lo cual se hablará más en detalle posteriormente en este capítulo, en la sección sobre encriptación) para proteger la contraseña. El CHAP brinda más seguridad que el PAP. Microsoft desarrolló su propia versión de este protocolo, llamado MS-CHAP, el cual utiliza el algoritmo de encriptación DES y el LM/NTHASH.
- **Servicio de autenticación remota de usuario telefónico (Remote Authentication Dial-In User Service) (RADIUS):** es otro medio de autenticación de conexiones remotas el cual exime de la responsabilidad de autenticación a cada servidor individual de acceso remoto al brindar un servidor central para la autenticación segura de los clientes. Los intercambios son encriptados utilizando una clave encriptada, y múltiples servidores RADIUS pueden comunicarse entre sí e intercambiar información de autenticación.
- **Protocolo AppleTalk de acceso remoto (AppleTalk Remote Access Protocol) (ARAP):** es un protocolo de autenticación bidireccional que utiliza la encriptación DES para las conexiones de acceso remoto de las redes AppleTalk.
- **Shell segura (Secure Shell) (SSH):** permite a los usuarios entrar a distancia a los sistemas UNIX. Ambos extremos de la conexión (cliente y servidor) son verificados y es posible encriptar la información, además de las contraseñas. Los algoritmos 3DES, Blowfish y Twofish son algoritmos de encriptación soportados por SSHv2, que también permite utilizar las tarjetas inteligentes.

NOTA

También hay versiones de SSH para equipos con Windows y Mac. En el sitio www.openssh.org/windows.html se puede obtener gratuitamente in software de cliente SSH.

Un concepto estrechamente vinculado a la autenticación es el de *no-repudio (*nonrepudiation*).* Esta es una forma de garantizar que todo el que envíe un mensaje no pueda posteriormente afirmar que no lo envió. En ocasiones se considera que el no-

repudio es un objetivo independiente de la criptografía, pero lo estamos incluyendo en la explicación de la autenticación porque ambos conceptos van de la mano; el no-repudio va un paso más allá de la autenticación.

En la escena…

La identidad está confirmada; ¿y ahora qué?

Una vez que se ha verificado la identidad de un usuario, el próximo paso en el proceso de seguridad es la *autorización*, la cual se refiere a aquello que está autorizado a hacer el usuario. La autenticación y la autorización funcionan unidas para facilitar un sistema de seguridad que tenga en cuenta la necesidad de que diferentes usuarios tengan capacidades diferentes en la red.

Los administradores pueden controlar los archivos y otros objetos a los que puede tener acceso el usuario, así como el nivel de acceso (solo lectura, permisibilidad de cambios, etc.) estableciendo *permisos*. La mayoría de los sistemas operativos de red brindan un mecanismo para asociar permisos específicos sobre un objeto con determinadas cuentas de usuario o grupos de usuarios. Por ejemplo, Windows NT/2000/XP brindan dos niveles de persmiso: *permisos de compartición* que se aplica solamente a los usuarios que acceden a los recursos por la red, y el *permiso al nivel de archivo* (también llamado permiso NTFS) que se aplica tanto a lo que está en red como a los usuarios que accede al recurso desde un equipo local.

Los administradores también pueden controlar las acciones que un usuario (o un grupo de usuarios) determinado puede hacer en el sistema, estableciendo los *derechos de usuario*. Los derechos de usuario se diferencian de los permisos ya que estos últimos se aplican al acceso a archivos individuales, carpetas, impresoras y otros objetos.

Para garantizar la confidencialidad de la información

La *confidencialidad* se refiere a todo método que mantenga en secreto el contenido de la información. Usualmente ello entraña la encriptación para evitar que las personas no autorizadas comprendan lo que dice la información, incluso si la interceptan. En un entorno de elevada seguridad, en el que las comunicaciones por la red necesariamente involucran información que no debe ser compartida con todo el mundo, es importante utilizar una encriptación estricta para proteger la confidencialidad de la información. Más adelante, en la sección "Conceptos básicos de la criptografía" analizamos exactamente el funcionamiento de este proceso.

Para garantizar la integridad de los datos

La *integridad de los datos*, en el contexto de la criptografía, significa que existe la forma de verificar que los datos no han sido modificados después de haber salido del remitente, que los datos enviados son exactamente iguales a los datos recibidos en el destino final. En transacciones de red como el comercio electrónico, es esencial poder contar con garantía de la integridad de la información.

NOTA

El término *integridad de los datos* tiene un significado más amplio en la computación en general y el trabajo en red que en el mundo de la criptografía. En este sentido se refiere a la protección de los datos para que no sean dañados o destruidos; la integridad de los datos se puede ver afectada por un desnivel de electricidad, un campo magnético, incendio, inundación, o eventos similares, así como por la acción de personas que deliberadamente los alteren. Es posible instalar utilidades como Tripwire (www.tripwire.org) para monitorear los cambios que se producen en los datos del sistema en el disco duro.

Conceptos básicos de criptografía

Las técnicas criptográficas como la de encriptación son la base de los *certificados digitales*, *las firmas digitales* y la *infraestructura de clave pública* o *PKI*. Todas estas tecnologías son un componente importante de un plan de seguridad al nivel empresarial, y posteriormente en este capítulo analizamos el uso de cada uno de ellos. Ahora que ya comprendemos los objetivos de la criptografía, podemos analizar cómo se aplican estas tecnologías.

Deformación del texto con códigos y cifras

Existen muchas formar de "deformar" un texto u ocultar su significado de manera tal que solamente puedan leerlo las personas autorizadas (o al menos es así en teoría). Este texto deformado (encriptado) se denomina *texto cifrado*. El método para encriptar un texto es llamado *cifra* o *código*. Técnicamente, un código utiliza la sustitución al nivel de palabra o frase, mientras que la cifra trabaja a nivel de letras o dígitos individuales. Ambos términos a menudo se utilizan indistintamente, pero las técnicas criptográficas computacionales por lo general utilizan cifras que operan sobre la base de la forma binaria de los datos aplicando un *algoritmo* (un cálculo matemático). Algunos tipos comunes de cifra/código son:

- Sustitución
- Transposición
- Lenguajes oscuros

Cifras de sustitución

La *sustitución simple* es un método a menudo utilizado por los niños en sus experimentos iniciales con los códigos secretos. Una cifra de sustitución sencillamente sustituye diferentes letras, números u otros caracteres por cada carácter del texto original. El ejemplo más sencillo es la sustitución simplista en la que cada letra del alfabeto es representada por un dígito numérico, comenzado por el 1 para la A. Entonces, el mensaje *Goodbye* se representaría 7-15-15-4-2-25-5. Evidentemente, este código es extremadamente fácil de descifrar.

El Código César utilizaba un método de cambio simple, en el que cada letra del mensaje era representada por la segunda letra siguiente de la derecha (la A se convierte en C, la B en D, y así sucesivamente). Otros métodos de sustitución pueden resultar mucho más difíciles de descifrar. Por ejemplo, si dos personas intercambian mensajes sobre la base de un libro del cual ambas tienen una copia, podrían redactar sus mensajes

haciendo referencia a números de página, línea y palabra (por ejemplo, 73-12-6 querría decir que esa palabra es la sexta palabra de la línea 12 de la página 73 del libro). En este caso, el que no tenga una copia del libro (y para citar las páginas correctas tendría que ser una copia de la misma edición) no podrá descifrar el mensaje.

Algunos tipos de cifras de sustitución son:

- **Sustitución monoalfabética:** Cada letra está representada por otra letra o carácter en una relación uno a uno.
- **Sustitución polialfabética**: Caracteres de texto cifrado diferentes pueden representar la misma letra de texto simple, haciendo más difícil descifrar mensajes utilizando la técnica de análisis de frecuencia. Al arquitecto y teórico de arte del renacimiento Leon Battista Alberti se le acredita haber creado esta técnica, con lo cual se ganó el reconocimiento como el "padre de la criptografía occidental".
- **Cifra poligráfica (de bloque)**: Varias letras (o dígitos si se trata de datos binarios) se encriptan a la vez, utilizando un sistema que puede manejar todas las combinaciones posibles de un número determinado de caracteres.
- **Fraccionación**: **Múltiples símbolos son sustituidos por cada letra del texto simple, después se trasponen las letras o dígitos.**

Cifras de transposición

Las *cifras de transposición* utilizan tablas en las que el texto plano se escribe de una forma y entonces se lee de otra para crear el texto encriptado. Por ejemplo, cada carácter del texto se introduce en las celdas de la tabla de izquierda a derecha, entonces el texto cifrado se elabora leyendo los caracteres en columnas. Una variación utiliza una red cuadriculada con hoyos que se coloca sobre una hoja de papel, entonces se escribe el mensaje rotando la rejilla a intervalos.

Lenguajes desconocidos como código

Los *lenguajes desconocidos* han sido utilizados por los gobiernos como código en sus comunicaciones militares. Las lenguas antiguas ("muertas") han sido utilizadas con este fin. El ejército de Estados Unidos incluso utilizó a personas que hablan la lengua Navajo durante la Segunda Guerra Mundial para enviar comunicaciones secretas. Se escogió esta lengua porque era difícil de aprender y porque en el mundo había pocas personas que la conocían. La lengua Navajo no había sido escrita nunca, lo cual la hacía aún más desconocida. Se reclutaron miembros de la tribu Navajo para que desarrollaran una cifra basada en esa lengua. Para más información sobre ese proyecto, véase el artículo Navajo Code Talkers en http://raphael.math.uic.edu/~jeremy/crypt/contrib/mollo2.html.

Dispositivos de cifrado mecánicos y eléctricos

Los *dispositivos de cifrado*, como las ruedas y los cilindros de cifrado, se pueden utilizar para cifrar y descifrar textos. Un ejemplo temprano de esta técnica fue la *cifra del escitalo* o *cifra de bastón* que utilizaban los espartanos. Enrollaban una hoja de papiro alrededor de un bastón y escribían el mensaje a todo lo largo de este. Cuando se desenrollaba la hoja, el mensaje no podía leerse fácilmente a menos que se enrollara en un bastón cuyo diámetro fuera igual al del bastón original.

Para su sistema de cifrado polialfabético, Leon Battista Alberti utilizó dos discos que tenían grabado el alfabeto. Alineaba ambo discos para determinar cuál carácter del texto en cifra representaría cada letra del texto plano. Al rotar los discos a determinados intervalos, hacía que letras de texto en cifras representaran las mismas letras del texto plano en lugares diferentes del mensaje.

Gobiernos y entidades militares han creado diferentes equipos de cifrado. La mayoría utiliza múltiples discos rotatorios para lograr la sustitución de las letras, y pueden ser utilizados mecánicamente o utilizando la electricidad. Thomas Jefferson inventó una rueda de cifrado de este tipo. Durante la Segunda Guerra Mundial, los japoneses utilizaron máquinas de cifrado llamadas RED y PURPLE, y el quipo alemán Enigma (equipo con rotor enrollado con contactos eléctricos equidistantes a cada lado del disco, conectados entre sí de manera asimétrica) quizás sea el dispositivo de cifrado más conocido –o más tristemente conocido.

Computadorización del proceso de cifrado

La disponibilidad de la tecnología de la computación facilitó aún más la encriptación de los mensajes utilizando métodos muy complejos, los cuales serían difíciles o imposibles de utilizar a mano o con dispositivos mecánicos o eléctricos. Como se analizó en el Capítulo 4, "Comprendiendo los fundamentos de la computación", cuando se va al meollo del sistema, las computadoras hacen solamente una cosa: hacer cálculos numéricos. No obstante, son capaces de hacer una sorprendente cantidad de esos cálculos a una velocidad increíblemente rápida. Esto es precisamente lo que se necesita para los algoritmos complejos de encriptación. Como es natural, las computadoras facilitan mucho más el descifrado de la información. Las cifras cuya ruptura requeriría años de trabajo manual de criptoanalistas se pueden revelar en horas, días o semanas utilizando computadoras potentes.

Uno de los primeros sistemas conocidos de cifrado por computadoras fue LUCIFER, proyecto de IBM que fue la base de la popular cifra Estándar de Cifrado de Datos (DES, por Data Encryption Standard del inglés) que aún es ampliamente utilizada (conjuntamente con su versión más segura, el 3DES). LUCIFER era una cifra en bloque, como lo es también DES. Utilizaba una clave de 128 bits para encriptar bloques de datos binarios de 128 bits de largo. La cifra se aplicaba varias veces al mismo bloque. Aunque LUCIFER utiliza un bloque y una clave más grande que DES, es menos seguro. Ello se debe a que el programa de su clave es regular y, en consecuencia, más predecible. En la sección sobre "Algoritmos de encriptación" de este capítulo, analizamos la DES y otras cifras modernas utilizadas por los esquemas de encriptación por computadora.

NOTA

Para una información más detallada del funcionamiento de las cifras y los dispositivos de cifrado, véase http://pardus-larus.student.utwente.nl/librarilo/texts/computers/crypto.

Qué es la encriptación

La *encriptación* es una forma de criptografía que deforma el texto plano y los convierte en texto cifrado ininteligible. La encriptación es la base de medidas de seguridad como las firmas digitales, los certificados digitales y la infraestructura de la clave pública que utiliza esta tecnología para elevar la seguridad de las transacciones por computadora. Las técnicas de encriptación por computadora utilizan claves para encriptar y desencriptar los datos. Una *clave* es una variable (a veces representada por una contraseña) que es un número binario grande –mientras más grande, mejor. La longitud de la clave se mide en bits, y mientras más bits tenga la clave más difícil será violentarla.

La clave es solo un componente del proceso de encriptación. Debe utilizarse conjuntamente con un *algoritmo* de encriptación (proceso o cálculo) para lograr el texto cifrado. Los métodos de encriptación usualmente se categorizan como simétricos o asimétricos, en dependencia de la cantidad de claves que se utilicen. En las secciones siguientes analizamos estos dos tipos básicos de tecnología de encriptación.

Encriptación simétrica

La *encriptación simétrica* es llamada también *encriptación de la palabra clave*, y utiliza solamente una clave, denominada *secreto compartido*, para encriptar y desencriptar. Este es un método de encriptación sencillo y fácil de usar pero presenta un problema: la clave deben compartirla el remitente y el destinatario de la información, por lo que es preciso diseñar un método seguro para el *intercambio de claves*. De lo contrario, si una tercera persona intercepta la clave durante el intercambio podría fácilmente desencriptar la información.

Encriptación asimétrica

Para resolver el problema del intercambio de claves se creó otro tipo de encriptación. La *encriptación asimétrica* es denominada también *encriptación de clave pública*, pero en realidad descansa en un *par de claves*. Se generan dos claves matemáticas relacionadas entre sí, una llamada *clave pública* y la otra llamada *clave privada*. La clave privada no es compartida nunca; se mantiene en secreto y la utiliza solamente su dueño. La clave pública se pone a disposición de todo el que la desee. Debido al tiempo y la cantidad de potencia de procesamiento de computadora requeridos, se considera que "no es matemáticamente factible" que se pueda utilizar la clave pública para reproducir la clave privada, por lo que este tipo de encriptación es visto como un método muy seguro.

La ventaja principal de la encriptación asimétrica es que no es necesario transmitir de forma segura una clave secreta. Por el contrario, la clave pública se da a conocer abiertamente, y puesta a disposición de todo el mundo. No hay necesidad de mantenerla en secreto porque no puede utilizarse ella sola. El proceso de encriptación funciona así:

1. Para encriptar el mensaje el remitente utiliza la clave pública del destinatario, que está fácilmente asequible.
2. El destinatario desencripta el mensaje utilizando su clave privada. Solamente puede utilizarse la clave privada asociada con la clave pública que encriptó el mensaje para desencriptarlo.

El par de claves también puede utilizarse para autentificar la identidad del remitente de un mensaje, utilizando las claves de una manera algo diferente: el remitente utiliza su clave privada para encriptar el mensaje. El sistema no brinda confidencialidad alguna porque cualquier persona podría desencriptar el mensaje utilizando la clave pública del dueño. Sin embargo, si verifica la identidad del remitente, porque si la clave pública asociada desencripta el mensaje, este pudo haber sido encriptado solamente con la clave privada de esa persona.

Evidentemente, lo más importante en la criptografía de clave pública es la protección de las claves privadas. Este concepto es especialmente importante porque el compromiso de la clave privada no solo permite que una persona no autorizada lea los mensajes privados enviados al propietario de esta, sino que también permite que el que robó la clave "firme" transacciones simulando ser el propietario, robando así la identidad de este. Cuando el par de clave se utiliza para transacciones seguras con tarjeta de crédito o bancarias, el resultado puede ser desastroso.

Aseguramiento de los datos con algoritmos criptográficos

Se han creado literalmente miles de algoritmos criptográficos diferentes. Estos se pueden clasificar de la siguiente forma:

- **Algoritmos de encriptación** utilizados para encriptar la información y brindar confidencialidad
- **Algoritmos de firma** utilizados para "firmar" digitalmente la información con miras a permitir su autenticación
- **Algoritmos de *hash*** utilizados para brindar integridad a la información.

Los algoritmos (cifras) también están caracterizados por la forma en que trabajan al nivel técnico (cifras en flujo y cifras en bloque). Esta categorización se refiere a si el algoritmo se aplica a un flujo de datos, que operan en bits individuales, o a todo un bloque de datos. Las *cifras en flujo* son más rápidas porque trabajan en unidades de datos más pequeñas. La clave se genera como un *flujo de claves*, y esta se combina con el texto simple que será encriptado. La RC4 es la cifra de flujo más comúnmente utilizada. Otra de ellas es ISAAC.

Las *cifras en bloque* toman un bloque de texto simple y lo convierten en texto cifrado. (Por lo general, el bloque tiene 64 ó 128 bits). Entre las cifras en bloque más comunes están DES, CAST, Blowfish, IDEA, RC5/RC6 y SAFER. La mayoría de los candidatos a la Norma Avanzada de Encriptación (AES, por Advanced Encryption Standard) son cifras en bloque.

NOTA

El AES es una norma para la criptografía utilizada por el gobierno federal de Estados Unidos para proteger información sensible pero no clasificada. Varios algoritmos se consideraron candidatos para esta norma. El Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) seleccionó el algoritmo Rijndael para el AES. Para más información acerca de la AES, véase http://csrc.nist.gov/encryption/aes/aesfact.html.

Algoritmos de encriptación
Algunos algoritmos de encriptación populares (muchos de los cuales fueron candidatos a AES) son:

- **Rijndael (norma AES)** www.tcs.hut.fi/~helger/crypto/link/block/rijndael.html
- **DES y 3DES** www.rsasecurity.com/rsalabs/faq/3-2-1.html
- **SAFER** www.cylink.com/news/press/pressrels/92000.htm
- **IDEA** htpp://home.ecn.ab.ca/~jsavard/crypto/co0404.htm
- **DEAL** www.ii.uib.no/~larsr/newblock.html
- **CAST-256** www.entrust.com/resources/pdf/cast-256.pdf
- **MARS** www.research.ibm.com/security/mars.html
- **Blowfish y Twofish** www.counterpane.com/ blowfish.html y www.tcs.hut.fi/~helger/crypto/link/block/twofish.html

Otros algoritmos de encriptación son, por ejemplo, SERPENT, RC4/RC5/RC6, LOKI-97, FROG y Hasty Pudding.

Algoritmos de firma
Los *algoritmos de firma* se utilizan para crear firmas digitales. Una *firma digital* no es más que una forma de "firmar" datos (como se explicó anteriormente cuando hablamos de la encriptación asimétrica) con el objetivo de autentificar que el remitente del mensaje es realmente la persona que afirma ser. Las firmas digitales pueden además contribuir a la integridad de la información, conjuntamente con la autenticación y el no-repudio. Las firmas digitales han cobrado importancia en un mundo en que muchas transacciones comerciales, incluidos acuerdos contractuales, se realizan por la Internet. Por lo general, las firmas digitales utilizan tanto los algoritmos de firma como los algoritmos de *hash*.

Cuando un mensaje es encriptado con la clave privada del usuario, el valor de hash que esta crea se convierte en la firma de ese mensaje. Cuando se firme otro mensaje se creará una firma diferente. Cada firma es única y cualquier intento por mover una firma de un mensaje a otro creará un valor de hash que no se corresponderá con el original; de esa forma la firma será invalidada.

Algoritmos de hash
Hashing es la técnica mediante la cual un algoritmo (también llamado *función de hash*) se aplica a una parte de los datos para crear una "huella" digital única que es una variable de tamaña fijo. Si alguien varía los datos hasta en un dígito binario, la función de *hash* dará un producto diferente (llamado el *valor de hash*) y el destinatario se percatará de que los datos han sido modificados. La técnica de *hashing* puede garantizar la integridad y a la vez brindar autenticación.

No se puede utilizar el valor de *hash* para descubrir los datos originales a los que fue aplicada la técnica. Es por ellos que a los algoritmos de *hash* se les llama *hashes de una sola dirección*. Una buena función de *hash* no dará el mismo resultado a partir de dos entradas diferentes (lo que se denomina *colisión*); cada resultado debe ser único.

Hay varios tipos diferentes de *hashing*, incluido el resto de división, rearreglo de dígitos, y transformación de la base de numeración o "radix". Estas clasificaciones se

refieren al proceso matemático que se utiliza para obtener el valor de hash. Entre los algoritmos de hash comunes están:

- **MD2, MD4 y MD5:** Estos métodos utilizan un *compendio del mensaje* (el valor de hash) de 128 bits de longitud. Fueron creados por Ron Rivest y son ampliamente utilizados para las firmas digitales.
- **SHA (por Secure Hash Algorithm en inglés):** Existen varias variaciones de este algoritmo, entre ellas SHA-1, SHA-256. SHA-384 y SHA-512. Estas se diferencia por la longitud del valor de hash SHA fue creado como resultado del esfuerzo conjunto de dos organismos gubernamentales estadounidenses, el NIST y el NSA.

Cómo se utiliza la encriptación en la seguridad de la información

La encriptación se emplea con variados fines en las organizaciones que manejan información sensible de cualquier índole. Más adelante, en la sección "Diseño y aplicación de políticas de seguridad", analizamos los tipos de información que se debe proteger. En esta sección, abordamos las distintas maneras en que las tecnologías de encriptación se pueden utilizar para proteger la información.

Encriptación de la información almacenada en discos

El término *encriptación de disco* se refiere al proceso de encriptar el contenido de un disco duro, un disquete o un disco removible. *Encriptación de archivo* se refiere al proceso de encriptar la información almacenada en el disco archivo por archivo. En cualquiera de los dos casos, el objetivo es impedir que personas no autorizadas abran y lean los archivos que los discos contienen.

Los sistemas operativos o el sistema de archivo puede tener incorporado el soporte para la encriptación de disco/archivo. El NTFS v5, el sistema de archivos original de Windows 2000/XP/.NET incluye el EFS (Encrypting File System) que puede ser empleado para proteger los datos contenidos en un disco duro o en un disco removible de gran capacidad. (El EFS se puede utilizar para proteger la información contenida en disquetes flexibles porque no pueden ser formateados en el formato NTFS). El EFS permite la encriptación de archivos individuales y/o carpetas.

Programas de terceras partes –como ScarmDisk, PGPdisk y SafeDisk para sistemas operativos Windows y el Crypto File System y el Transparent Crypotographic File System (TCFS) para UNIX/Linux– se pueden instalar para la encriptación en sistemas de archivos que originalmente no soportan la encriptación o para facilitar la encriptación a nivel de partición o en torres virtuales.

Con la encriptación a nivel de partición o en torres virtuales el usuario no tiene que fijar explícitamente las propiedades de encriptación en archivos o carpetas individuales (como sucedería con la encriptación a nivel de archivo). Por el contrario, se marca como encriptada toda una partición o se crea una torre virtual encriptada, y toda la información en ella contenida se encripta automáticamente. Muchos usuarios optan por este método ya que el rendimiento es mejor que la encriptación a nivel de archivo. Algunos métodos de encriptación de archivo/disco utilizan contraseñas para proteger los datos encriptados; cuando una persona desea acceder a un archivo encriptado deberá escribir la contraseña. Otros métodos descansan en la cuenta de usuario que deben abrirse para determinar si se concede o no el acceso. El EFS, por ejemplo, utiliza los certificados digitales asociados a

las cuentas de usuario. Estos métodos más recientes requieren menos interacción del usuario, pero tienen sus inconvenientes. Quizás no se sea posible compartir con otras personas los archivos encriptados sin desencriptarlos en los casos en que tiene acceso a ellos una sola cuenta de usuario. Además, existe un riesgo de seguridad si el usuario abandona la computadora estando conectado a la red; entonces cualquier persona que se siente a la computadora puede acceder a la información encriptada.

Encriptar la información que viaja por la red

Al inicio del capítulo, en la sección acerca de la seguridad física, hablamos de cómo la información puede ser interceptada y capturada mientras viaja por la red, y cómo su contenido puede ser revelado con un "rastreador" o un analizador de protocolo. Cuando por la red se transmite información sensible, los usuarios se pueden proteger para que no sea decodificada velando por que esté encriptada, de manera que si una persona no autorizada la intercepta no pueda leerla. El método usual de la industria para hacerlo en una red TCP/IP es utilizar el mecanismo de encriptación Internet Security Protocol (IPSec, Protocolo de Seguridad de Internet).

Las especificaciones para el IPSec aparecen en RFC[*] 2401 (varios otros RFCs se refieren a protocolos diferentes utilizados por IPSec). IPSec puede ser utilizado con diferentes sistemas operativos y plataformas. Windows 2000/XP/.NET tiene incorporado un soporte para IPSec. IPSec puede brindar autenticación a nivel de máquina (verificación de la identidad de la computadora desde donde se originó una transmisión en red). Se le puede configurar para que trabaje en uno de dos modos:

- **Modo de transporte:** Este modo brinda seguridad punto a punto, desde la computadora-fuente hasta la computadora-destino. También se le llama *modo anfitrión a anfitrión (host- to- host).*
- **Modo túnel:** Este modo permite la encriptación entre dos puertas de enlace seguras (las computadoras que actúan como puertas de enlace entre una red interna e Internet, u otra interred).

Dada su capacidad para el tunelado, el IPSec se puede utilizar para crear redes privadas virtuales, y además se utiliza de conjunto con el L2TP (por Layer 2 Tunneling Protocol en inglés) para brindar encriptación en un túnel L2TPVPN.

Aunque a menudo se hace referencia a él clasificándolo de protocolo, el IPSec es realmente un proyecto de seguridad que incorpora varios protocolos diferentes. Entre ellos están los siguientes:

- **Protocolo de encabezado de auntenticación (AH por sus siglas en inglés):** Este protocolo se utiliza para la autenticación y para garantizar la integridad de la información al firmar cada paquete de datos. El AH firma todo el paquete (incluidos los encabezamientos IP) pero no brinda confidencialidad a la información.
- **Protocolo ESP (Encapsulating Security Payload);** Este protocolo se utiliza para encriptar la información en busca de su confidencialidad. También firma

[*] N. del T.: , Según glosarios de informática consultados, RFC (del inglés Request For Comments, o Petición de Comentarios en español) son una serie de documentos iniciada en 1967 que describe el conjunto de protocolos de Internet y experimentos similares. No todos los RFC's (en realidad muy pocos de ellos) describen estándares de Internet pero todos los estándares Internet están escritos en forma de RFC's

la porción de los datos del paquete en aras de su autenticación e integridad, pero no firma todo el paquete.

Estos dos protocolos se pueden utilizar independientemente o de conjunto (en este último caso, cuando se desee tanto la confidencialidad como la firma de los datos de todo el paquete). Otros protocolos que utilizan el IPSec son:

- **ISAKMP (Internet Security Association and Key Management Protocol [Protocolo de seguridad de Internet y gestión de clave].** Este protocolo crea asociaciones de seguridad entre dos computadoras que se comunican utilizando IPSec, para definir el proceso de intercambio de información.
- **El Protocolo de Generación de Clave Oakley**. Este protocolo crea la clave usada durante la transacción. Estas son claves temporales que se desechan una vez concluida la sesión de comunicación.

Dado que el IPSec utiliza claves compartidas (encriptación simétrica) es importante que exista la forma de intercambiar las claves por la red en condiciones de seguridad. El *algoritmo de Intercambio de clave Diffie-Hellman* permite que las computadoras en ambos extremos de la transacción generen claves idénticas sin enviar realmente la clave por la red y exponerla a la posibilidad de ser interceptada. El algoritmo de encriptación utilizado por el IPSec son cifras estándar como DES/3DES, IDEA, Blowfish, RC-5 y CAST-128.

Otra característica importante de IPSec es su capacidad de proporcionar un mecanismo de antirreproducción (*antireplay)* –protección contra *hackers* que pudieran intentar capturar las transmisiones y reproducirlas para crear una sesión de comunicación, aparentando ser una de las partes de la transacción original. El IPSec es un mecanismo importante para proteger la información durante el período vulnerable cuando se envía por la red. La versión actual del Protocolo de Internet, Ipv4, permite el uso de IPSec como una opción; la próxima generación, el IPv6, lo exigirá.

Encriptación de las comunicaciones por correo-e

Es cada vez mayor la cantidad de personas que utilizan el correo-e para todo tipo de comunicaciones, incluidos mensajes con información personal o comercial sensible. Existen varios programas de software que encriptan correo electrónico; el más popular es Pretty Good Privacy (PGP), creado por Phil Zimmermann a principios del decenio de 1990. Desde entonces, el PGP goza de una amplia distribución y existen versiones para la mayoría de los sistemas operativos comunes, incluso para los muy obsoletos y desconocidos como el OS/2 y Amiga.

El PGP primero comprime y después encripta el texto simple utilizando una clave secreta de un solo uso (o *clave de sesión*), que a su vez es encriptada con la clave pública del destinatario. La clave de sesión encriptada se envía al destinatario junto con la información encriptada, y este utiliza su clave privada para desencriptar la clave de sesión para poder usarla para desencriptar el mensaje. Como en este proceso se utiliza tanto la encriptación simétrica como la asimétrica, se dice que el PGP es un *criptosistema híbrido*. Versiones diferentes del PGO utilizan algoritmos de encriptación diferentes. La versión 2.6.x (a veces denominada "PGP clásico" y considerada por algunos como más segura que las versiones más recientes) utiliza una combinación de la cifra asimétrica

RSA y la cifra simétrica IDEA. El algoritmo de *hash* MD5 también se utiliza para crear una sustitución de longitud fija para cadenas de datos muy largos en firmas digitales.

Las claves públicas y privadas se almacenan en archivos diferentes llamados *keyrings*, en el disco duro de la computadora donde está instalado el PGP. Tanto el remitente como el destinatario deben tener instalado el PGP para poder utilizar el programa para comunicaciones seguras.

La mayor vulnerabilidad del PGP está relacionada con el hecho de que los usuarios deben utilizar una frase de paso para realizar operaciones como firmar documentos y desencriptar mensajes (todo para los cual se utiliza la clave privada). La protección de esta frase de paso es una cuestión de seguridad muy importante; las buenas prácticas de seguridad requieren que esta frase de paso no sea revelada a nadie ni almacenada en el sistema para la entrada automática. Toda persona que conozca la frase de paso puede leer los mensajes encriptado o enviar mensajes aparentando proceder de un usuario legal. Si se llega a comprometer la frase de paso, se puede generar un certificado de renovación de clave para anular la clave pública asociada. El PGP incluye además una opción de borrado (-w) que puede usarse para sobreescribir el contenido de un archivo encriptado al eliminarlo, de manera que no pueda ser fácilmente recuperado mediante utilidades de recuperación de datos.

NOTA

Para más información sobre el PGP, véase la página internacional del PGP en www.pgpi.org.

¿Qué es la esteganografía?

Esteganografía (del término griego que significa *escritura encubierta*) se refiere al método para ocultar datos –no solo esconder su contenido como lo hace la encriptación, sino ocultar su existencia misma. La esteganografía usualmente se emplea conjuntamente con la encriptación para una mayor protección de la información sensible. Este método reduce uno de los mayores problemas de la información encriptada –el hecho de estar encriptada llama la atención de las personas que están a la caza de información confidencial o sensible.

El concepto de la esteganografía ha existido desde hace mucho tiempo, se dice que los griegos de la antigüedad enviaban mensajes secretos afeitando la cabeza del mensajero y escribiendo el mensaje en su cuero cabelludo, para después esperar que le creciera el cabello antes de enviarlo a entregar el mensaje. Entre los métodos más tempranos de la esteganografía está el uso de tinta invisible y ocultar el mensaje dentro de otro mensaje mediante un código por el cual, por ejemplo, las palabras del mensaje oculto son una de cada cinco de las del mensaje visible. Uno de los primeros libros sobre el tema, *Steganographica*, por Gaspari Schotti, fue publicado en el decenio de 1600.

En el mundo de la computación, la esteganografía también oculta información dentro de otra información, pero la forma en que lo hace es algo más compleja. Dada la forma en que la información es almacenada en los archivos. A menudo existen bits no utilizados (vacíos) en un archivo como un documento o un gráfico. Se puede dividir un mensaje y almacenarlo en esos bits no utilizados, y cuando se envía el archivo parecerá que es solamente el archivo original (llamado *archivo contenedor*). La información escondida adentro usualmente está encriptada, y el destinatario necesitará un software

especial para recuperarla y después desencriptarla, si es necesario. Es posible esconder mensajes dentro de cualquier tipo de archivo, incluidos archivos ejecutables y archivos de audio. Otra forma de esteganografía es la marca de agua oculta que en ocasiones se utiliza para implantar una marca u otro símbolo en un documento o archivo.

Para tal fin se pueden utilizar diferentes programas, entre ellos el *JP Hide and Seek* – que oculta datos dentro de archivos con la extensión jpg– y MP3Stego, que lo hace en archivos con la extensión mp3. El Steganos Security Suite es un paquete de programas de computación que brinda posibilidades de esteganografía, encriptación y otras.

Otros programas, como StegDetect, están diseñados para buscar un contenido oculto en los archivos. El proceso de detectar los datos esteganográficos se denomina estaganálisis.

NOTA

Para más información y vínculos a una gran cantidad de buenos sitios web sobre esteganografía véase *Information Hiding* en www.jjtc.com/steganography.

Métodos modernos de desencriptación

El uso de la criptografía condujo de manera natural a la ciencia del criptoanálisis o el proceso de desencriptar mensajes encriptados. Uno de los primeros métodos para descifrar las cifras de sustitución polialfabéticas fue el *análisis de frecuencia*, el cual se trataba de examinar el texto cifrado en busca de cadenas de caracteres repetidas y utilizar la distancia entre las cadenas repetidas para calcular la longitud de la clave. (Los caracteres idénticos del texto simple cifrados de la misma manera se repetirán a intervalos que son múltiplos de la longitud de la clave). Posteriormente se podrán utilizar métodos estadísticos para determinar qué carácter del texto simple representa cada carácter del texto cifrado.

A lo largo de la historia los criptoanalistas han utilizado métodos diferentes para descifrar los algoritmos de encriptación, entre ellos los siguientes:

- **Análisis de un texto simple conocido** Si el analista tiene una muestra de un texto desencriptado que fue encriptado utilizando una cifra determinada, podrá deducir la clave estudiando el texto cifrado.
- **Criptoanálisis diferencial** Si el analista puede obtener el texto cifrado de un texto simple pero no puede analizar la clave, podrá deducirla comparando el texto cifrado y el texto simple.
- **Análisis del texto cifrado solamente** Se utiliza cuando solo se dispone del texto cifrado y el analista no tiene un texto simple como muestra.
- **Análisis de energía temporal/diferencial** Un medio de medir las diferencias en el consumo de electricidad por un período de tiempo durante el cual el procesador de una computadora encripta la información, con el objetivo de analizar las operaciones de computación claves.
- **Intercepción de clave** El analista engaña a dos partes que intercambian mensajes cifrados para que envíen sus claves, haciéndoles creer que están intercambiando claves entre sí.

El matemático Claude Shannon introdujo la teoría de la *carga de trabajo*. Este término se refiere al hecho de que aumentar la cantidad de trabajo (y el tiempo requerido para hacerlo) necesario para violentar un sistema de encriptación aumenta la fortaleza de

la encriptación y es una alternativa al aumento de la distancia de unicidad (la cantidad de texto cifrado necesario para descifrar lo encriptado).

Las cifras de encriptación por computadora son difíciles de violentar pero es posible hacerlo. Con suficiente tiempo y paciencia, un ataque de fuerza bruta que pruebe con todas las claves posibles lo logrará. El objetivo de los criptógrafos es crear cifras para las cuales este proceso se haga tan prolongado –incluso utilizando supercomputadoras o métodos de procesamiento distribuidos– que no valga la pena intentarlo. Los algoritmos de encriptación populares de la actualidad se basan en este efecto de disuasión.

Valladares contra el delito…

¿Una cifra perfecta?

Una cifra perfecta es aquella en que cualquier texto cifrado posible es igualmente probable para cada método, lo cual hace que la encriptación sea indescrifrable si no se tiene la clave.

En su escrito *A Communications Theory of Secrecy Systems*, publicado en 1948, Claude Shannon –matemático de Ball Labs llamado en ocasiones el "padre de la teoría de la información"– postuló que con suficiente tiempo y una amplia muestra del texto cifrado, es posible descifrar cualquier clave. Afirmaba que un número que denominó *distancia de unicidad*, que representaba la cantidad de texto cifrado necesario para descifrar el mensaje, se podía utilizar como medida de la fortaleza de la cifra. Si la distancia de unicidad es infinita (la secuencia de números en la clave es realmente aleatoria y es al menos tan larga como el mensaje, y la clave se utiliza solamente para ese mensaje) el mensaje es indescifrable.

Otro ejemplo de mensaje indescifrable es aquel en el que la longitud de todo el mensaje es menor a la cantidad de texto cifrado necesario para descifrar la clave. Si una cifra de sustitución alfabética tiene una longitud de clave superior a la longitud del mensaje, el mensaje no puede ser desencriptado analizando el texto cifrado.

Uso de la encriptación y la esteganografía por parte de los delincuentes informáticos

Hemos estado analizando el uso legal de las técnicas criptográficas como parte del plan de seguridad de una organización. Son muchas las razones para que tomemos medidas encaminadas a brindar mayor protección a la información relacionada con secretos comerciales, datos personales de los clientes, etc. No obstante, a menudo estas mismas técnicas son utilizadas por los delincuentes informáticos para encubrir la información que se envían entre sí y que pudiera incriminarlos. Se piensa que los terroristas utilizan la esteganografía y la encriptación (así como códigos menos técnicos insertados en correos electrónicos o páginas web aparentemente inocuos) para comunicarse entre sí y coordinar sus ataques y actividades financieras.

En los casos de delitos graves, los investigadores posiblemente tengan que contratar a un criptoanalista para que los ayude a descifrar los datos encriptados que pudieran contener información esencial para identificar a los criminales o impedir nuevas actividades delictivas.

En la escena…

La criptografía como herramienta terrorista

Según un artículo de *USA Today* reproducido posteriormente en www.wired.com/news/print/0,1294,41658,00.html, funcionarios gubernamentales piensan que los terroristas de Al Qaeda utilizan la esteganografía para encubrir sus comunicaciones secretas en mensajes y archivos publicados en sitios web e intercambiados en salas de chateo en Internet, así como las tecnologías de la encriptación para esconder el verdadero contenido de los correos electrónicos. Se han encontrado archivos encriptados contentivos de planes terroristas en las computadoras de varios sospechosos de terrorismo, como el terrorista paquistaní Khalil Deek, y el terrorista condenado por planear el primer ataque con bomba contra el Centro Mundial de Comercio (World Trade Center) en 1993, Ramzi Yousef. En ambos casos, matemáticos que trabajan para el FBI lograron descifrar los archivos con el uso de supercomputadoras, aunque en el caso de algunos archivos demoraron alrededor de un año.

Para más información, véase www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm.

Potenciar la seguridad de hardware y software

Un plan de seguridad multicapas incorporará múltiples soluciones de seguridad. En el tema de la seguridad no existen las "tallas únicas", de manera que la opción que resulte óptima para una organización no es necesariamente la mejor opción para otra. Las soluciones de seguridad pueden desglosarse generalmente en dos categorías: soluciones de hardware y soluciones de software.

Aplicación de la seguridad con base en el hardware

Las soluciones de seguridad con base en el hardware pueden ser dispositivos de red: cortafuegos, enrutadores, incluso interruptores, pueden servir para dar cierto nivel de seguridad. En general, estos dispositivos son ellos mismos computadoras con programas patentados.

Cortafuegos basados en el hardware

Muchos proveedores de cortafuegos brindan soluciones basadas en el hardware. Entre los cortafuegos de hardware más populares están PIX de Cisco, SonicWall, Webramp 1700, Firebox de WatchGuard Technologies, y los cortafuegos OfficeConnect de 3Com. Existen soluciones de hardware para todos los tamaños de redes. Por ejemplo, los productos de 3Com se concentran en usuarios de tipo oficina pequeña/oficina casera (SOHO por Small Office/Home Office), mientras que Cisco PIX viene en configuraciones que soportan hasta 250 000 conexiones.

Los cortafuegos con base en hardware son a menudo llamados *dispositivos cortafuegos*. Una desventaja de este tipo de cortafuegos es que el programa que utilizan es propietario o patentado. Otra desventaja de muchos de estos productos, como el muy respetado PIX de Cisco, es su alto costo. Los cortafuegos con base en hardware realizan básicamente las mismas funciones que los que están basados en software. Más adelante, en la sección "Para comprender los cortafuegos y los praxis" analizamos el funcionamiento de ambos.

Dispositivos de autenticación
Otros componentes con base en hardware dentro del plan de seguridad de una red podrían ser dispositivos que brindan una seguridad adicional para la autenticación, como:

- Lectores de tarjeta inteligente
- Escáneres de huellas dactilares
- Escáneres de retina e iris
- Dispositivos de análisis de voz

Estos dispositivos pueden ser utilizados en ambientes que requieren un alto nivel de seguridad para la autenticación segura y fiable en la red. Microsoft ha adquirido tecnología Biométrica API (BAPI) de I/O Software y tiene previsto incorporar el soporte para dispositivos de autenticación biométrica en versiones futuras de sus sistemas operativos. Windows 2000 ya soporta la autenticación de tarjetas inteligentes.

Autenticación de tarjetas inteligentes
El término tarjeta inteligente tiene varios significados. En un sentido amplio se refiere a cualquier tarjeta plástica del tamaño de una tarjeta de crédito que tiene integrado un chip de computadora (un chip de memoria y/o un diminuto microprocesador) que contiene información factible de ser modificada (a diferencia de las tarjetas "menos" inteligentes que utilizan una cinta magnética con información estática). Se necesita un *lector* de tarjeta –un dispositivo de hardware– para escribir y leer la información en la tarjeta. Las tarjetas inteligentes pueden ser utilizadas para fines diferentes, pero uno de los más populares es el de la autenticación. Los servicios de televisión por satélite utilizan las tarjetas inteligentes en el receptor SATV para identificar al suscriptor y el nivel de servicio de este. Los bancos utilizan las tarjetas inteligentes para realizar transacciones. Estas tarjetas son especialmente populares en Europa.

Las tarjetas inteligentes se pueden utilizar también para autentificar el ingreso en una red. Estas brindan un nivel de seguridad adicional. Por lo general, las tarjetas son a prueba de manipulación y es relativamente difícil alterarlas. Además, son poco costosas si se les compara con los dispositivos de autenticación biométrica.

Las tarjetas inteligentes utilizadas para la autenticación de entrada por lo general almacenan un *certificado digital* que contiene información de identificación del usuario, la clave pública del usuario, y la firma de la tercera parte fiable que emitió el certificado, así como la fecha de validez del certificado. Los certificados los almacena en las tarjetas un administrador autorizado. Para entrar con una tarjeta inteligente el usuario la inserta en el lector e ingresa un PIN asociado con la tarjeta. Si el PIN presenta problemas el administrador puede cambiarlo o emitir una nueva tarjeta. Para utilizar tarjetas inteligentes para el ingreso a una red la computadora debe tener un sistema operativo que soporte la autenticación por tarjeta inteligente, como Windows 2000 o XP, o utilizar un programa adicionado como Sphinx (www.securetech-crop.com/sphinx.html).

En la escena…

El futuro de las tarjetas inteligentes

En el futuro, si la autenticación por tarjeta inteligente gana en popularidad, las computadoras podrán venderse con lectores de tarjetas inteligentes ya incorporados. Varios dispositivos thin-client (como los fabricados por Sun Ray y Acer) ya tienen incorporados lectores de tarjetas inteligentes. En estos momentos se pueden adquirir lectores tanto internos como externos. El ChipDrive (www.towitoko.com/datintrn.html) es un ejemplo de lector interno.

Las normas para las tarjetas inteligentes han sido especificadas en la ISO 7816, emitida por la Organización Internacional del Normalización. Dichas normas definen las especificaciones solamente para protocolos de nivel más bajo. Existen dos normas principales para la programación de las tarjetas inteligentes: la norma PC/SC y la Norma OpenCard. Para más información sobre la tecnología de las tarjetas inteligentes, véase el sitio web de Smart Card Alliance en www.smartcardalliance.org/industry_infor/index.htm.

Son varias las empresas que producen tarjetas inteligentes y lectores de estas. Algunos productores producen teclados con lectores de tarjetas inteligentes incorporados, y existen combinaciones de escáner de huellas dactilares/ lector de tarjeta inteligente para brindar seguridad en ambas modalidades, con base en tarjeta y de tipo biométrico.

Aunque las tarjetas inteligentes brindan una seguridad adicional, no son (como cualquier otro método de autenticación) infalibles. Muchos criptógrafos han logrado burlar la encriptación de las tarjetas inteligentes. En general, existen dos métodos para violentar las tarjetas inteligentes: lógico y físico. Un ejemplo de ataque lógico es borrar parte de la información contenida en el microprocesador elevando o bajando el voltaje; en algunos casos, esto "abre" la seguridad sin borrar los datos. Un ataque físico podría ser cortar el microcircuito y sacarlo de la tarjeta y utilizar un microscopio con cortador de láser para examinarlo. Si bien con paciencia y determinación se puede violentar una tarjeta inteligente de esta manera, estos métodos no son fáciles de emplear y no siempre funcionan.

Autenticación biométrica

Los dispositivos de autenticación biométrica se basan en características físicas como huellas dactilares, patrones faciales, o patrones del iris o la retina, para verificar la identidad de un usuario. La autenticación biométrica está ganando popularidad en muchas aplicaciones, entre ellas la entrada a una red. Es preciso tener almacenado un modelo o identificador biométrico (una muestra que se conozca es del usuario autorizado) en una base de datos para que el dispositivo pueda efectuar la comparación con una nueva muestra que reciba durante el proceso de ingreso. La autenticación biométrica a menudo se utiliza de conjunto con las tarjetas inteligentes en los ambientes de alta seguridad. Los dispositivos biométricos más populares son los siguientes:

- **Escáneres de huellas dactilares** Distintos proveedores los comercializan para computadoras de mesa y portátiles, y se conectan por el puerto USB o por tarjetas PCMCIA.
- **Dispositivos de reconocimiento de patrones faciales** Estos dispositivos utilizan el análisis de la geometría facial para verificar la identidad de los usuarios.
- **Dispositivos de reconocimiento de la geometría de las manos** Estos dispositivos son similares a los de reconocimiento de patrones faciales pero sirven para analizar la geometría de las manos.
- **Dispositivos de identificación por escáner del iris** Los escáneres del iris analizan el tejido del iris, el cual se forma durante el octavo mes de gestación y permanece inalterado para siempre.
- **Dispositivos de identificación por escáner de la retina** Los escáneres de retina analizan el patrón de los vasos sanguíneos de la retina.

Es posible utilizar varias características fisiológicas como identificadores, y se han diseñado dispositivos que verifican la identidad sobre la base del estudio por escáner de la rodilla, la geometría de la oreja, el reconocimiento del patrón de las venas, e incluso el reconocimiento del olor corporal. Además, algunos dispositivos analizan y comparan características conductuales utilizando métodos como el reconocimiento del patrón vocal, la verificación de la firma, el reconocimiento de los golpes de tecla, reconocimiento del patrón de respiración, el reconocimiento del modo de andar, e incluso reconocimiento del patrón de las ondas cerebrales, si bien algunos de estos métodos están solamente en fase experimental.

Se considera que la biométrica es uno de los métodos de autenticación más fiables que puedan existir. No obstante, estos métodos están demostrando ser menos fiables de lo que se pensó en un momento. Por ejemplo, y según BBC (British Broadcasting Corporation) News. http://news.bbc.co.uk/hi/english/sci/tech/newsid_2016000/2016788.stm) en mayo de 2002 estudios realizados del sistema de reconocimiento facial utilizado en algunos aeropuertos arrojaron que sus resultados eran exactos en menos de un 50% del total de verificaciones. Algunos sensores de huellas dactilares pueden ser burlados si se respira encima de ellos o si se coloca sobre ellos una bolsa con agua para reconstruir la huella que fue registrada en ellos anteriormente. También es posible construir "dedos" falsos como una huella digital autorizada, el cual se utiliza entonces para burlar el sensor dactilar. Un criptógrafo japonés demostró esta técnica utilizando gelatina líquida para confeccionar una huella falsa (www.esecurityplanet.com/trends/article/0,,10751_1379041,00.html). Microcircuitos baratos y/o programas de computación defectuosos pueden provocar rechazos falsos y falsas aceptaciones con dispositivos biométricos.

NOTA

Para más información sobre las fallas de seguridad en los sistemas de reconocimiento biométrico, véase el artículo *Body Check* en www.heise.de/ct/english/02/11/114.

Puesta en práctica de la seguridad con base en software

Las soluciones de seguridad con base en software tienen una cobertura más amplia que las soluciones con base en hardware. Estas soluciones incluyen las características de seguridad incorporadas en el sistema operativo de la red, así como software de seguridad adicionales producidos por los proveedores del sistema operativo o por terceros. La seguridad con base en software tiene sus ventajas. A menudos es más barata que las soluciones con base en hardware y se integran con mayor facilidad en el sistema y la red. No obstante, la seguridad con base en software a menudo tiene problemas de rendimiento si se le compara con la seguridad con base en hardware, además de que las aplicaciones de seguridad que corren en sistemas operativos populares pueden ser burladas más fácilmente que los programas patentados utilizados en dispositivos de hardware dedicados. Sin embargo, la seguridad con base en software es popular y brinda una amplia gama de métodos para proteger los datos y facilitar la autenticación, confidencialidad e integridad.

Software criptográficos

Existen miles de productos criptográficos que cumplen diferentes fines: encriptación de disco/archivos, encriptación de correos electrónicos, esteganografía, entre otros. Hemos analizado algunos en las secciones que se refieren al funcionamiento de las tecnologías. Además de los productos comerciales, hay disponibles como productos gratuitos muchos programas de encriptación y autenticación. Para obtener una lista de estos productos y los vínculos a los sitios de descarga, véase www.alw.nih.gov/Security/prog-auth.html.

Certificados digitales

Como se ha dicho anteriormente, la encriptación de clave pública es más segura que la encriptación de clave privada porque no hay necesidad de transmitir una clave por canales no seguros, pero la criptografía de clave pública es también más compleja y más difícil de aplicar a gran escala. Debe existir un sistema que garantice que las claves públicas publicadas en Internet no sean falsificaciones hechas por alguien que se quiere hacer pasar por otro usuario. Si eso sucede, los datos encriptados con esa clave pública (y destinada a ser enviada al usuario cuyo nombre fue asociado a ella) podrían ser interceptados por el usuario no autorizado que publicó la clave. Dicha persona no autorizada podría entonces desencriptar los datos y leer el mensaje.

Necesitamos un mecanismo que permita que una tercera parte de confianza confirme que el usuario que publica la clave pública es en realidad la persona que afirma ser. Los certificados digitales brindan esa seguridad. Para comprender cómo funcionan los certificados digitales basta con pensar en la forma en que una licencia de conducción o una tarjeta de identidad estatal se utilizan para verificar la identidad de una persona. Si usted precisa demostrar su identidad en un comercio o un banco presentando su licencia o su tarjeta de identidad, la entidad estaría confiando en la palabra de una tercera parte de confianza (en este caso, el Departamento de Vehículos Automotores) de que usted es quien dice ser. El comercio o el banco presume que el DVA lo ha verificado a usted y no habría emitido el documento de identificación oficial a menos que haya confirmado su identidad.

De la misma manera que el comercio y el banco acepta su licencia de conducción como prueba de su identidad, otra computadora con la cual usted desea intercambiar datos o hacer transacciones aceptará el certificado digital emitido por una tercera parte de confianza. En el caso de certificados digitales, la tercera parte de confianza es una *autoridad de certificación (AC).* La AC verifica que una identidad determinada está vinculada a la clave pública que está incluida en el certificado.

Algunas AC públicas, como VeriSign, emiten certificados a personas en Internet. Autoridades de certificación privadas (internas) son creadas por organizaciones para emitir certificados a usuarios dentro de una red local. La AC es un servidor que corre un programa especial que le permite emitir, gestionar y revocar certificados digitales. El papel de la AC es garantizar a otros usuarios, computadoras y aplicaciones que una clave pública determinada pertenece en realidad a la entidad a cuyo nombre está asociada.

Infraestructura de clave pública

Una *infraestructura de clave pública*, o *ICP*, es una red de seguridad basada en certificados digitales. La ICP brinda un sistema para que los usuarios soliciten certificados y para que la AC emita, gestione y revoque certificados, y haga circular listas de revocaciones de certificados (LRC) de manera que otras entidades conozcan cuándo el certificado de una entidad determinada ha perdido su validez. La ICP está basada en las normas X.509 establecidas por la Organización Internacional de Normalización.

Un componente importante de la ICP es el conjunto de políticas de seguridad que la rigen. Estas políticas deben definir las reglas para la emisión y el uso de los certificados digitales y las claves asociadas a ellos. Las autoridades públicas de certificación, como VeriSign, deben brindar una declaración de práctica de certificado (DPC). Este documento detalla los procedimientos para aplicar la ICP.

Cuando hay múltiples CA en la misma IPC, como sucede en la mayoría de las grandes organizaciones, estas están dispuestas en un orden jerárquico. La *AC raíz* es la AC de más confianza en la IPC. Su certificado es autofirmado, y está a cargo de emitir certificados a las restantes AC en la IPC, las cuales se denominan *AC subordinadas*. Las AC subordinadas emiten certificados a usuarios y computadoras, mientras que la AC raíz por lo general emite certificados solamente a las AC subordinadas. Las AC públicas son publicadas en el Global Trust Register, que actúa como una AC raíz para las AC públicas (aunque en forma impresa).

Los certificados pueden ser emitidos por un AC con muchos fines diferentes, entre ellos la encriptación de archivos, la autenticación de tarjetas inteligentes, el correo electrónico, la seguridad de IP e ingreso a redes. Los usuarios pueden exportar o importar certificados, moviéndolos de una computadora a otra. La función de exportación también se utiliza para crear una copia de respaldo de un certificado, la cual podría ser restaurada en el *almacén de certificado* –la ubicación dentro del disco duro donde se guardan los certificados— en caso de que el certificado original quedara destruido. En algunos casos los certificados son emitidos de manera automática; en otros casos deben ser explícitamente solicitados por el usuario. Hay diferentes maneras de solicitar un certificado, en dependencia del software de la AC y de las políticas de la IPC. Si se solicita un certificado de una AC pública por lo general es preciso llenar un formulario de solicitud en el sitio web de la AC.

Es muy importante que la PC contenga un mecanismo para publicar las revocaciones de certificados para que otras entidades no confíen erróneamente en un certificado que haya perdido su validez. Los certificados son revocados cuando la clave pública queda comprometida o cuando los usuarios abandonan la empresa o por alguna razón ya no son fiables. Las LRC presentan una relación de los certificados que han sido revocados y son actualizadas de manera regular y distribuidas por toda la organización por la AC.

Cortafuegos con base en software

Además del software de IPC que facilita la verificación de la identidad, un tipo de seguridad con base en software de importancia vital es *el programa cortafuegos*. En realidad, todos los cortafuegos están basados en software. Los dispositivos de hardware que se venden como cortafuegos utilizan software patentados que realizan en esencia las mismas funciones que los programas que pueden instalarse en una computadora personal regular. Utilizamos el término *cortafuegos con base en software* para describir productos cortafuegos como el Servidor ISA de Microsoft o Secure Way de IBM, a diferencia de las combinaciones de hardware/software (o firmware) como los producidos por Cisco Systems. Algunos proveedores, como Check Point, comercializan ambos tipos de productos. En la siguiente sección analizamos detalladamente el funcionamiento de los cortafuegos.

En la escena...

La diferencia entre un cortafuegos y un proxy

Los servidores proxy se han estado utilizando desde hace ya algún tiempo. El significado original del término *proxy* era "aquel que está autorizado a actuar por otro". Quizás el uso más famoso –o notorio– de la palabra surgió en relación con la práctica del casamiento por poder (marriage by proxy, en inglés) en el que una persona sustituía a una de las partes, permitiéndose así que se realizara la ceremonia aunque el novio (o en las menos de las ocasiones, la novia) no estaba presente físicamente. Hubo un momento en que los casamientos por poder se hicieron populares para unir parejas mientras el novio estaba cumpliendo sus deberes militares.

Los servidores proxy también reciben ese nombre porque, al igual que el desafortunado que decía "Acepto" cuando en realidad era otro el que aceptaba, sirven de intermediarios que permiten que algo suceda (en este caso, las comunicaciones en red) entre sistemas que deben permanecer independientes. Los servidores proxy sirven de intermediarios entre las computadoras de una LAN y las de la red pública en el exterior. Otra analogía aplicable es la de un portero que está situado a la entrada de una propiedad para chequear a todos los visitantes que entran a fin de garantizar que estén en la lista de los invitados. El proxy puede de hecho ocultar del exterior las computadoras de la LAN. Solamente la dirección IP del servidor proxy queda visible a los demás en Internet; las computadoras internas utilizan direcciones de IP privadas (no enrutables por Internet) que no pueden ser vistas del otro lado del servidor proxy.

De hecho, un proxy puede ir más allá y actuar como el guardia de una cárcel, el cual no solamente garantiza que entre únicamente el personal autorizado sino que también vela por que salgan solamente los que tienen autorización para hacerlo. De la misma manera que el guardia verifica la lista para permitir la entrada o la salida de alguien, el proxy *filtra* los datos que salen y entran según criterios predeterminados. Es en este punto que el proxy actúa como un *cortafuego*.

Qué son los cortafuegos

El cortafuegos hace un poco más que ocupar el lugar de las computadoras locales y ocultarlas de la vista de la red global, como hace el proxy. Los cortafuegos están diseñados específicamente para controlar la entrada y la salida, impidiendo que los datos no autorizados entren en la red y restringiendo el tipo de datos que salen y la forma en que lo hacen.

El nombre cortafuegos procede de la industria de la construcción. En las estructuras comerciales, es común construir una pared que sirve de barrera y que está compuesta por material ignífugo, ubicada entre dos zonas del edificio. Esta pared tiene el objetivo de impedir que el fuego se expanda de una parte del edificio a otra. Otro ejemplo es la barrera térmica entre el motor de un automóvil y el compartimiento de pasajeros, a la cual se le llama cortafuegos. De la misma manera, el cortafuegos de una red actúa como una barrera que impide que "datos malos" –ya sean códigos de virus o mensajes dirigidos a sistemas no autorizados o procedentes de estos— se diseminan

desde la red externa (por lo general la Internet) hacia la red interna. También impide que determinados paquetes dirigidos a un usuario o computadora determinada, o procedente de ellos, se diseminen desde la LAN hacia la red externa.

Al seleccionar de entre diferentes soluciones cortafuegos, las organizaciones encuentran dos opciones de diseño básicas:

- Un cortafuegos puede estar diseñado para *permitir* el paso de todos los paquetes a menos que exista una prohibición expresa.
- Un cortafuegos puede estar diseñado para *denegar* el paso de todos los paquetes a menos que exista una autorización expresa.

Evidentemente, la segunda opción es más segura pero puede provocar que se niegue el acceso a algo que el administrador desee realmente autorizar. El primer método es más fácil de aplicar pero es también el más fácil de burlar.

Cómo usan los cortafuegos el filtrado por capas

Los productos cortafuegos soportan el filtrado de mensajes para permitir el paso de datos o para impedirlo, según criterios especificados. Los mejores cortafuegos soportan el *filtrado por capas*. Esto quiere decir que pueden realizar el filtrado en la capa de paquete, la capa de circuito o la capa de aplicación; algunos cortafuegos soportan solamente uno de estos tipos de filtrado, pero la mayoría de los productos cortafuegos avanzados, como el Servidor ISA de Microsoft o Firewall-1 de Check Point, soportan los tres tipos. Los cortafuegos que combinan el filtrado de capa de paquete, de circuito y de aplicación son los que brindan el nivel de seguridad más elevado. Estos tipos de cortafuegos también tienden a ser los más costosos. En las secciones siguientes analizamos brevemente la forma en que funciona cada método de filtrado.

Filtrado de paquete

El filtrado de paquete funciona principalmente en la capa de red del modelo OSI de trabajo en red (equivalente a la capa de interred del modelo DoD) que tiene que ver con los paquetes de IP. Los filtros de paquete examinan la información contenida en el encabezamiento de paquete de IP de un mensaje y entonces permite el paso de los datos a través del cortafuegos o rechazan el paquete sobre la base de esa información. Cuando está activado el filtrado de paquete IP, el cortafuegos interpreta y evalúa los paquetes antes de darles paso a un nivel superior en el cortafuegos o a un filtro de aplicación.

La información que utiliza el filtro de paquete para tomar su decisión incluye la dirección de IP de la(s) computadora(s) de origen y/o destino, así como el número de puerto TCP o UDP. (Efectivamente, los números de puerto están en el encabezamiento de capa de transporte, de manera que técnicamente, si bien el filtrado de paquete por lo general opera el nivel de capa de red, también procesa alguna información de más alto nivel). El filtrado de paquete permite que los datos continúen hasta la capa de transporte únicamente si las reglas de filtrado de paquete le permite hacerlo.

El filtrado de paquete permite al administrador bloquear paquetes que procedan de un determinado host de Internet o los que están destinados a un determinado servicio en la red (por ejemplo, el servidor web o el servidor SMTP). El *filtrado dinámico de paquete* ofrece un mayor nivel de seguridad porque abre el (los) puerto(s) necesario(s) únicamente cuando es necesario para que tenga lugar la comunicación, y lo(s) cierra inmediatamente una vez concluida esta. Los *filtros estáticos de paquete* están

configurados para permitir la entrada y salida desde y hacia una dirección IP (o grupo de direcciones IP) y número de puerto (o grupos de puertos) predefinidos.

Es importante señalar que los filtros de paquete no pueden realizar el filtrado sobre la base de cualquier contenido que tenga el campo de datos del paquete, ni pueden utilizar el estado del canal de comunicación como ayuda para tomar la decisión de aceptar o rechazar el paquete. Si es preciso tomar decisiones de filtrado sobre la base de alguno de estos criterios, el cortafuegos debe ser configurado para utilizar el filtrado que opere a un nivel diferente (filtrado de circuito o aplicación).

Filtrado de circuito

El *filtrado de circuito* opera en una capa superior del modelo OSI, la capa de transporte (la capa host-a-host en el modelo DoD). Los filtros de circuito restringen el acceso sobre la base de los equipos (no usuarios) host procesando la información contenida en los encabezamientos del paquete TCP o UDP. Ello permite a los administradores crear filtros que, por ejemplo, prohibiría que cualquier persona que utilice la Computadora A utilice el FTP para acceder a la Computadora B.

Cuando se utilizan filtros de circuito, el control del acceso está basado en flujos de datos TCP o datagramas UDP. Los filtros de circuito pueden funcionar sobre la base de banderas de estado de TCP y UDP e información de secuenciación, además de las direcciones de origen y destino y números de puerto. El filtrado a nivel de circuito permite a los administradores inspeccionar sesiones en vez de paquetes. En ocasiones se considera que una sesión es una conexión, pero realmente una sesión puede estar compuesta por más de una conexión. Las sesiones se establecen solamente como respuesta a la solicitud de un usuario, lo cual constituye una seguridad adicional.

Los filtros de circuito no restringen el acceso sobre la base de la información de usuario; tampoco pueden interpretar los significados de los paquetes. Es decir, no pueden distinguir entre un comando **GET** (coger) y un comando **PUT** (poner) enviado por un programa de aplicación. Para ello es necesario aplicar un filtro de aplicación.

Filtrado de aplicación

En algunas ocasiones, la mejor táctica es filtrar paquetes sobre la base de la información que contienen los propios datos. Los filtros de paquete y los filtros de circuito non utilizan el contenido del flujo de datos para tomar las decisiones de filtrado, pero esto puede hacerse con el *filtrado de aplicación*. El filtro de aplicación opera en la capa superior del modelo de trabajo en red, la muy bien llamada capa de aplicación. Los filtros de aplicación pueden utilizar la información del encabezamiento del paquete pero también pueden autorizar o rechazar paquetes sobre la base del contenido de los datos y de la información de usuario.

Los administradores pueden utilizar los filtros de aplicaciones para controlar el acceso sobre la base de la identidad de un usuario y/o sobre la base de una tarea determinada que trate de realizar el usuario. Con los filtros de aplicación, se pueden establecer criterios sobre la base de comandos emitidos por la aplicación. Ello significa que. Por ejemplo, el administrador puede restringir que un usuario determinado baje archivos a una computadora dada utilizando el FTP. Al propio tiempo, el administrador puede autorizar a ese mismo usuario a subir archivos por el FTP a esa misma

computadora. Esto es posible porque se emiten comandos diferentes en dependencia de si el usuario está recuperando archivos del servidor o si los está depositando en él.

Muchos expertos en cortafuegos consideran que las puertas de enlace de aplicaciones es la más segura de las tecnologías de filtrado. Ello se debe a que los criterios que utilizan para filtrar son más abarcadores que los de los demás métodos. En ocasiones los hackers crean programas malintencionados que utilizan la dirección de puerto de una aplicación autorizada, como el puerto 53, que es la dirección DNS. Un filtro de paquete o circuito no podría reconocer que el paquete no es una solicitud o respuesta DNS válida y le permitiría el paso. Sin embargo, el filtro de aplicación es capaz de examinar los contenidos del paquete y determinar que *no* debe autorizar su paso.

Este tipo de filtrado tiene inconvenientes. El mayor problema es que debe existir una puerta de aplicación independiente para cada servicio de Internet que el cortafuegos debe soportar. Ello exige un mayor trabajo de configuración: no obstante, esta debilidad constituye a su vez una fortaleza que eleva la seguridad del cortafuegos. Dado que es preciso habilitar una puerta para cada servicio, el administrador no autorizaría accidentalmente los servicios que constituyen una amenaza para la red. El filtrado de aplicación es el nivel de filtrado más sofisticado que realiza el servicio de cortafuegos, y resulta especialmente útil para proteger la red frente a tipos de ataques específicos, como comandos SMTP malintencionados o intentos de penetrar los servidores locales DNS.

Detección integrada de intrusión

Muchos cortafuegos también incorporan un *sistema de detección de intrusión* que de hecho pudiera reconocer que se está produciendo un ataque de un determinado tipo y puede realizar una acción predeterminada cuando se identifica dicha intrusión, por ejemplo:

- Enviar un mensaje de correo electrónico al administrador
- Enviar un mensaje de red al administrador
- Localizar al administrador
- Registrar el suceso en el registro de sucesos
- Ejecutar un programa o secuencia de comandos especificado previamente
- Detener el servicio de cortafuegos

Los sistemas de detección de intrusión pueden reconocer muchas y diferentes formas de intrusión en la red, como escáner de puerto, ataques LAND, Ping of Death, bombas UDO, ataques fuera de banda, entre otros. También pueden incorporarse filtros de detección especiales, como el filtro de detección de intrusión de POP (Post Office Protocol, o Protocolo de Correo) que analiza el tráfico de correo POP para impedir el desbordamiento del búfer POP, o el filtro de detección de intrusión DNS que puede configurarse para buscar ataques de desbordamiento de nombre de host DNS o de desbordamiento de longitud.

Creación de un equipo de respuesta ante incidentes

Una intrusión o un ataque puede ser atemorizante, frustrante y enloquecedor; al igual que sucede en el caso de un ataque físico contra una persona, las reacciones emocionales podrían dificultar llegar a un razonamiento adecuado y tomar decisiones correctas para responder a él. Esta situación se hace más fácil si estamos correctamente preparados para enfrentarla. Muchas compañías, que asumen un enfoque proactivo, crean equipos de

respuesta ante incidentes –llamados *equipos de respuesta ante incidentes de computación*, o ERIC—integrados por personas que se entrenan de conjunto (de manera muy similar a una unidad militar o un equipo especial de la policía) para trabajar en caso de incidentes ya previstos. El objetivo es poder entrar en acción cuando ocurra un incidente real, y en tal caso cada miembro del equipo cubre una zona de responsabilidad asignada previamente, lo cual disminuye el daño y aumenta la posibilidad de aprehender al autor del incidente.

En su libro *Incident Response: Investigating Computer Crime* (Respuesta a incidentes: investigación del crimen informático), Chris Prosise y Kevin Mandia definen el incidente como "un evento que interrumpe el procedimiento de operación normal y precipita el nivel de crisis". Las directrices CERT definen incidentes específicos, incluida la violación de la política de seguridad, intentos por obtener el acceso no autorizado, negación no deseada de servicios/recursos, uso no autorizado, y cambios realizados al sistema o los datos sin el conocimiento, instrucción o consentimiento del propietario. Un incidente puede ser desde un ataque que interrumpe el funcionamiento de todos los servidores y todas las comunicaciones de red, hasta una intrusión que no provoca daño real pero demuestra la vulnerabilidad de los sistemas de la organización. Los distintos tipos de ataques analizados en el Capítulo 6 (por ejemplo, las distintas variedades de ataques DoS/DdoS) son sin duda incidentes.

El equipo de respuesta debe tener su propio hardware y software para utilizarlos en la investigación. Es importante que los sistemas atacados sean preservados en el estado en que estaban cuando se descubrió la ocurrencia del incidente. Cualquier cambio que se haga al sistema pondría en peligro la integridad de la evidencia y afectaría su admisibilidad en un tribunal.

Los miembros del equipo de respuesta pueden ser citados a testificar en el tribunal si se abre un proceso judicial en relación con el incidente. Esta es una razón más para preparar una amplia documentación que pueda revisarse antes de testificar. A menudo, un caso no es llevado a los tribunales hasta varios meses, o incluso años, después de ocurrido el incidente, y la memoria humana en ocasiones no es fiable después de tanto tiempo si no se le ayuda un poco. El miembro del equipo que prepara la documentación debe ser el que testifique sobre su autenticidad si va a ser presentada como evidencia.

NOTA

Es importante que los miembros del equipo comprendan que sus informes sobre el incidente pueden llegar a ser presentados como evidencia en un juicio. Por esta razón, dicha documentación debe ser mantenida en un cuaderno especial con hojas enumeradas, y dicho cuaderno no debe contener ninguna información personal, ya que el mismo en su conjunto podría llegar a ser parte de la documentación oficial.

Los pasos que abarca la respuesta a incidentes:

- **Entrenamiento** Una vez versados en la teoría de la respuesta a incidentes, el equipo debe entrenarse de conjunto en ejercicios realistas hasta que las acciones de respuesta lleguen a ser algo automático. El entrenamiento abordar las leyes que están relacionadas consideraciones de privacidad y otros temas que pudieran afectar o restringir las actividades de los miembros del equipo durante las acciones de respuesta.

- **Reconocimiento del incidente** Se debe realizar una labor de monitoreo para garantizar que los miembros del equipo estén alertas ante la posibilidad de que ocurra un incidente incipiente.
- **Verificación de incidente** este paso incluye el examen de los registros, la observación del comportamiento del sistema/la red, entrevista a testigos, etcétera, para verificar que de hecho ha tenido lugar un incidente.
- **Clasificación de incidentes** Se debe realizar una evaluación para determinar la naturaleza del incidente y el nivel de amenaza.
- **Contención del incidente** Se deben tomar medidas inmediatas para detener el incidente e impedir un daño mayor.
- **Preservación de la evidencia** Se deben tomar medidas inmediatas para preservar toda la evidencia del incidente a fin de rastrear al responsable y para el posible procesamiento judicial de este, o un posible litigio civil.
- **Análisis del incidente** Se debe realizar una profunda investigación para determinar exactamente qué sucedió y cómo.
- **Restauración** Los sistemas deben ser puestos nuevamente en funcionamiento lo antes posible a fin de evitar una pérdida de productividad.
- **Actividades de seguimiento** Se deben establecer nuevas medidas de seguridad a fin de garantizar que no vuelva a ocurrir el mismo tipo de incidente.
- **Documentación** Cada paso del proceso de respuesta debe ser documentado y preservado para su revisión y uso posterior.

NOTA

La documentación podría incluir "fotografías de la escena del crimen"; en algunos casos sería conveniente tener fotos o instantáneas de la pantalla para preservar la información que aparece en el monitor. Los instrumentos a disposición del equipo de respuesta deben incluir una cámara digital.

No es necesario que cada miembro del equipo participe en todos los pasos del proceso de respuesta. Todos los miembros del equipo deben conocer cuál es su papel y permitir que el resto desempeñen sus funciones. Las funciones de cada miembro del equipo deben ser asignadas según la esfera de especialización de cada persona. Los equipos normalmente incluyen personas pertenecientes al departamento de TI (Tecnología de la Información), seguridad empresarial, administración, departamento jurídico, e incluso de los departamentos financiero, recursos humanos y relaciones públicas. Los miembros del equipo de respuesta deben estar localizables y listos para responder a incidentes a cualquier hora del día y cualquier día de la semana. En el Capítulo 10 sobre "Recopilación y conservación de la evidencia digital" se analizan en detalle los pasos de la investigación y los equipos necesarios.

La respuesta a incidentes es la culminación de todo lo que hemos analizado en este libro y el primer paso del proceso investigativo. En este capítulo, hemos pasado de la teoría y los conceptos de seguridad a los aspectos prácticos de un plan de seguridad: la puesta en práctica de medidas de seguridad y finalmente, en caso de que estas fallen, planificar una respuesta a un ataque. No obstante, el documento que compila todos estos temas es la *política de seguridad* de la organización, que rige todo, desde la forma en que deben ser utilizadas las tecnologías hasta los procedimientos prescritos para el equipo de

respuesta a incidentes. La siguiente sección presenta una reseña de las políticas de seguridad: lo que son (y lo que no son) y cómo se elaboran. Incluimos muestras de algunos temas de política específicos que deben ser abordados por todas las organizaciones.

Diseño y aplicación de políticas de seguridad

Los temas de seguridad encabezan las prioridades de seguridad en estos momentos. Las empresas pierden millones de dólares e innumerables horas de productividad de los trabajadores a causa de una insuficiente seguridad. Las empresas comprenden que la protección de sus bienes –digitales y físicos—ya no es un lujo; en el siglo XXI se ha convertido en una necesidad.

Una cantidad enorme de la información más crucial de una empresa, incluidos los datos financieros, registros personales, información de clientes y secretos comerciales están concentrados en un "lugar" virtual: la red de la organización. Esta centralización hace que la información sea vulnerable al acceso no autorizado y a la destrucción accidental o intencional, por parte de intrusos tanto internos y (suponiendo que la red local esté conectada a Internet, como lo están la mayoría actualmente) externos. Para que sea exitosa, la aplicación de medidas de seguridad debe estar basada en un plan empresarial que tenga en cuenta todos los aspectos de las necesidades de seguridad de la organización. Deben existir reglas y directrices que rijan la forma en que se pone en práctica el plan; las mismas son dadas a conocer a toda la organización en forma de *políticas*.

Para comprender la seguridad basada en políticas

Los que trabajamos en la esfera de la seguridad a menudo hacemos hincapié en la necesidad de contar con políticas detalladas adaptadas a las necesidades de cada organización específica –y a veces podemos sonar como un disco rayado. No obstante, hay razones para hacerlo: la política de seguridad es la base del plan de seguridad de una organización. Es el documento rector, en gran medida parecido a las órdenes generales de un departamento policial o la declaración de misión de una junta directiva. Las secciones siguientes analizan el funcionamiento y el objetivo de la *política de seguridad* de la TI y el proceso para evaluar y definir las necesidades de seguridad, elaborar la política y aplicarla en toda la organización.

¿Qué es la política de seguridad?

Según está utilizado el término en este escrito, una *política de seguridad* se refiere a un documento escrito que define el enfoque de una organización respecto de la seguridad o una esfera específica de la seguridad (en este caso, la seguridad de computadoras y redes) y establece un conjunto de reglas que deben observarse en la puesta en práctica de la filosofía de seguridad de la organización.

Las organizaciones pueden establecer reglas escritas y no escritas referidas a temas de seguridad, y pueden emitir diferentes tipos de documentos sobre estos tópicos. ¿En qué se diferencia una política de seguridad de memorandos y directivas, normas, especificaciones, directrices y documentos de procedimiento referidos a la seguridad?

NOTA

Las *Directrices* usualmente funcionan como procedimientos recomendados más que como reglas absolutas. Las directrices pueden servir de complemento a los políticas pero no las sustituyen.

Memorandos de seguridad

Por lo general, un *memorando de seguridad* o una *directiva de seguridad* se emiten en respuesta a un incidente específico y pueden ser utilizados como vía para establecer una regla que no esté comprendida en la política. Si la regla se refiere solamente a una situación única específica o si estará vigente solamente por un tiempo limitado, es posible que sólo se necesite un memorando. Si la regla ha de ser permanente o de largo plazo y es aplicable a un amplio espectro de situaciones, deberá ser incorporada a la política oficial de la organización lo antes posible. Un memorando puede también ser solamente informativo, con el objetivo de dar a conocer a los usuarios las consideraciones de seguridad sin establecer reglas o directrices específicas.

Normas y especificaciones de seguridad

Las *normas* y *especificaciones* generalmente son requisitos que se deben cumplir en la aplicación de procedimientos de seguridad específicos a un sistema y pueden servir para medir la fiabilidad general, compatibilidad u otras características del sistema. Por ejemplo, el gobierno de Estados Unidos ha elaborado criterios, definidos en el manual titulado *Department of Defense Trusted Computer System Evaluation Criteria* (Criterios de evaluación del sistema de computación fiable del Departamento de Defensa) (también llamado el "libro naranja") y el *Trusted Network Interpretation of the TCSEC* (el "libro rojo") para valorar las aplicaciones de seguridad. Otros países tienen sistemas de valoración similares. La ISO ha elaborado las ISO 17799 como un conjunto de "mejores prácticas" reconocidas internacionalmente sobre la seguridad de la IT. La política de seguridad podría especificar el cumplimiento de normas o especificaciones particulares.

Procedimientos de seguridad

Los *documentos de procedimiento* complementan la política y pueden integrarse a ella como parte de un manual de políticas y procedimientos. El documento de procedimiento brinda instrucciones detalladas sobre las tareas necesarias para poner en práctica las políticas. Por ejemplo, si la política estipula que los usuarios deben cambiar sus contraseñas cada 30 días, es posible que haya dos documentos de procedimiento asociados: uno dirigido a los administradores de red que detalle cómo establecer los requisitos de contraseña en el controlador de dominio de Windows para obligar a los usuarios a cambiar su contraseña a intervalos de 30 días, y otro destinado a los usuarios donde se detalle cómo cambiar las contraseñas. Cuando se encuentran en documentos separados, la sección de política y los documentos de procedimiento asociados deben guardar relación entre sí.

Por qué es importante esta información para los investigadores

Los investigadores que hace frente a delitos informáticos relacionados con una red empresarial necesitan poder comprender en detalle la forma en que se aplica la seguridad dentro de la organización, de la misma manera que un investigador que responda a una

invasión de morada necesita conocer la disposición de la casa, dónde y cómo están colocados los dispositivos de seguridad, cuál es la filosofía de seguridad de la familia, etc. A diferencia de la mayoría de las situaciones en la esfera residencial, las empresas a menudo cuentan con documentos escritos que establecen todas las directrices que se siguen para aplicar el plan de seguridad.

No obstante, estos documentos no siempre son fáciles de comprender –a menos que también comprendamos el proceso mediante el cual son elaborados, aprobados y llevados a la práctica. En las secciones siguientes presentamos una reseña de dicho proceso: cómo las organizaciones valoran sus necesidades en materia de seguridad sobre la base de factores de riesgo conocidos, niveles de amenaza y otros factores que determinan el grado y el tipo de seguridad que se aplicará, cómo se definen las zonas de seguridad; y cómo el documento en sí es elaborado (por lo general por un equipo encargado con la elaboración de la política).

Estos antecedentes les hará más fácil a los investigadores llegar a la organización y analizar su actuación como víctima o como origen de los delitos informáticos sobre la base de la información que contiene el documento de política. Por ejemplo, si el examen de las políticas demuestra que la organización tiene una estricta política de contraseñas, y otras técnicas investigativas como las entrevistas a los empleados revelan que las políticas son plenamente aplicadas, ello indicaría que para lograr el acceso los intrusos utilizan otras técnicas y no la de burlas contraseñas, o podría indicar que existe alguien dentro de la organización que está brindando información. En otras palabras, cuando se comprenden las políticas es posible reducir el campo de la investigación. A menudo, este es el paso más difícil y vital en el proceso investigativo.

Evaluación de las necesidades de seguridad

Si aceptamos la definición dada de política de seguridad es evidente que no puede existir una política de seguridad de TI única que funcione igual para todas las organizaciones. Las necesidades de seguridad varían en dependencia de:

- Factores de riesgo
- El nivel de amenaza percibido y real
- Vulnerabilidades de la organización
- La filosofía de la organización (sistema abierto frente a sistema cerrado)
- Factores jurídicos
- Fondos disponibles

Es importante analizar todos estos factores cuidadosamente a la hora de elaborar una política que brinde tanto una protección adecuada como un nivel de acceso conveniente.

Componentes del plan de seguridad de una organización

Las características de seguridad ya vienen integradas a los programas de sistemas operativos; Windows NT, 200, XP y –próximamente utilizado en un servidor cercano a usted– .NET incluyen numerosas características de seguridad. Recientemente Microsoft anunció que sus desarrolladores se concentrarán aún más en los temas de seguridad. Las distribuciones de UNIX y Linux vienen con características de seguridad incorporadas. Los productos de seguridad de las TI, tanto de hardware como de software, abundan. Es posible obtener entrenamiento en seguridad y numerosas certificaciones en esta esfera, y los profesionales de las TI están a la caza de estos.

Todos estos son componentes importantes del plan de seguridad global de una organización, pero no son suficientes. La coordinación e interacción efectiva de todos estos componentes requiere de algo más: una política de seguridad integral.

Definir las esferas de responsabilidad

A fin de valorar acertadamente las necesidades de seguridad es preciso estudiar la infraestructura de la empresa, sus procesos y procedimientos, e involucrar al personal en todos los niveles de la organización y de tantos departamentos como sea posible. Idealmente, las siguientes tareas serían realizadas por un equipo seleccionado cuidadosamente y que comprenda, como mínimo, a miembros de la gerencia, personal de las TI y un representante jurídico de la empresa. A cada miembro del equipo se le deben asignar esferas de responsabilidad específicas y se deben establecer plazos para el cumplimiento de sus tareas.

Responsabilidad para elaborar el plan y las políticas de seguridad

La elaboración de un buen plan de seguridad exige muchas horas de trabajo mental y esfuerzo. La política afectará a todos en todos los niveles de la organización y es conveniente que se soliciten ideas de tantos representantes como sea posible de distintos departamentos y esferas de trabajo. Un enfoque efectivo para ello es crear un comité integrado por personas procedentes de diferentes esferas dentro de la organización para que participen en la elaboración y examen del plan y las políticas de seguridad. Un comité de planificación de seguridad de este tipo podría incluir todos o algunos de las personas siguientes:

- El administrador de la red y uno o más administradores asistentes
- El administrador de seguridad del sitio
- Los jefes de departamento de varios departamentos o sus representantes
- Representantes de grupos de usuarios a quienes afectarán las políticas de seguridad (por ejemplo, el personal de secretaría, el centro de procesamiento de datos)
- Un miembro del departamento jurídico que se especialice en leyes referidas a la computación y la tecnología
- Un miembro del departamento de finanzas o presupuesto
- Un miembro de la gerencia principal

Responsabilidad para aplicar y hacer cumplir el plan y las políticas de seguridad

Por lo general, las políticas de seguridad son aplicadas por los administradores de red y el personal de TI, quienes velan por su cumplimiento. Las políticas y descripciones de los empleos deben designar con exactitud quién es el responsable de cada parte del plan. Debe existir una jerarquía de mando bien delimitada que especifique quién tiene la decisión final en caso de conflicto. En algunos casos –como la penetración física de la red– tendrá que involucrarse al personal de seguridad de la empresa. Deben existir políticas escritas y claramente formuladas que estipulen la responsabilidad concreta de cada departamento en tales circunstancias.

El plan de seguridad debe también abarcar los procedimientos para reportar las violaciones de seguridad, tanto internamente como en los casos en que sea necesario

involucrar a la policía o a otro organismo. Además, deberá especificarse quién es el encargado o el autorizado para solicitar la participación de agentes externos.

Uno de los aspectos más importantes en una buena política de seguridad es que debe ser factible de ser aplicada. Si es posible hacer cumplir la política mediante instrumentos de seguridad, es preferible utilizar este método. Si las políticas tienen que hacerse cumplir mediante reprimendas u otras acciones contra los empleados que las violen, deben existir documentos claramente redactados y distribuidos entre todo el personal sobre qué constituye una violación y cuáles sanciones se deberán aplicar, así como los encargados de hacerlo.

Analizando los factores de riesgo

Antes de establecer las políticas, el equipo que ha de elaborarlas necesita definir cuál es el tipo de seguridad que requiere la organización y los niveles de riesgo a tener en cuente. Tradicionalmente, el análisis de riesgo incluye:

- Determinar a qué tipos de violaciones de la seguridad es vulnerable la organización
- Para cada tipo de violaciones, determinar la probabilidad de que ocurra
- Para cada tipo de violaciones, determinar el grado de pérdida que tendría lugar en caso de ocurrir

Este análisis se conoce con el nombre de *análisis de riesgo cuantitativo*.
Otro tipo de análisis de riesgo, el *análisis de riesgo cualitativo*, no presta atención al elemento de probabilidad y en su lugar se concentra en las posibles amenazas y en las características del sistema o la red que provocan la vulnerabilidad a esas amenazas. Entonces, se diseñan métodos para prevenir o reducir la probabilidad de que ocurran violaciones, detectar cuando estas ocurran, y disminuir y reparar el daño provocado en caso de que ocurran.

Existen herramientas de evaluación de riesgo que ayudan a identificar las amenazas y vulnerabilidades, evaluar el nivel de amenaza, calcular el impacto en la organización y recomendar soluciones. Ejemplo de ellas es COBRA Risk Consultant (Consultor de Riesgo COBRA) de C&A Systems Security Ltd. La metodología COBRA es utilizada por las principales corporaciones y entidades gubernamentales.
¿Por qué es necesario el análisis de riesgo? Son varias las razones, entre ellas las siguientes:

- Desde el punto de vista del profesional de TI, el análisis de riesgo detallado es el paso primero, y quizás más importante, para justificar ante la gerencia los costos para aplicar las medidas de seguridad necesarias.
- Desde el punto de vista de la gerencia, el documento de análisis de riesgo brinda una base sólida y objetiva para tomar decisiones que afectan al presupuesto y el personal.
- Los datos recopilados durante el proceso de análisis de riesgo obliga tanto al personal de TI como a la gerencia a hacer frente y reconocer las amenazas y las vulnerabilidades sobre las cuales quizás no hayan tenido conciencia o que hayan podido obviar anteriormente.

- El análisis de riesgo permite a la organización concentrar recursos en las amenazas y vulnerabilidades existentes y evitar malgastar tiempo y recursos en medidas innecesarias.

Debido a que el proceso de análisis de riesgo involucra a personal de toda la organización, puede elevar la conciencia en torno a la seguridad y hacer que las prácticas de seguridad apropiadas sean responsabilidad de todos los que utilizan las computadoras y la red. Este es un principio básico de la prevención del delito.

Valoración de amenazas y del nivel de amenaza

El diccionario define el término amenaza como "alguien o algo factible de provocar daño". La porción de valoración de amenaza del análisis de riesgo deberá incluir:

- Fuentes de posibles amenazas
- La naturaleza de posibles amenazas
- La probabilidad de ocurrencia de cada tipo de posible amenaza

Las fuentes de posibles amenazas se pueden dividir en categorías internas y externas. A pesar de que muchas políticas de seguridad centran su atención en la amenaza de que ocurra una violación de la seguridad desde el exterior de la red o de la organización (por Internet), en la actualidad muchas organizaciones se percatan de que sus mayores pérdidas potenciales proceden del interior –acciones deliberadas o no intencionales de los empleados, contratistas u otras personas que tienen acceso legal a la red. Es importante abordar ambas categorías a la hora de realizar la valoración de las amenazas.

También, para definir las fuentes de las amenazas requiere que el equipo de valoración determine *quién* y *qué* podría representar una amenaza para la red. Entre las personas que podrían representar una amenaza están la mayoría de los tipos de delincuentes informáticos que se analizan en el Capítulo 3, por ejemplo:

- Hackers al azar, motivados por el deseo de divertirse, el desafío personal de invadir una red, o competir con otros hackers
- Ladrones de información que toman como blanco específico una organización o determinada información; en este tipo se incluye el espionaje empresarial
- Personas con motivaciones emocionales, como ex empleados con deseos de venganza, contrincantes empresariales que desean dañar la capacidad comercial de la empresa, o una persona con resquemores contra la empresa, su personal o la industria a la cual pertenece
- Personas que de manera accidental o sin percatarse provocan daño o pérdida de información (la más de las veces amenazas internas, como en el caso del empleado que está "experimentando" y borra sin querer archivos importantes del servidor)

La naturaleza de las posibles amenazas es el *qué* en esta ecuación. Cualquiera de estas personas podría provocar amenazas de uno o varios de los siguientes tipos:

- Acceso no autorizado a la información
- Revelación no autorizada de información
- Destrucción de datos
- Modificación o corrupción de datos
- Introducción de virus, gusanos y troyanos
- Negación o interrupción de servicio o congestión/desaceleración de la red

NOTA

Un programa de valoración exhaustiva de las amenazas no pasaría por alto las amenazas que representan eventos como incendios, inundaciones o fallos eléctricos, así como los causados por el ser humano.

El siguiente paso en el análisis de amenazas consiste en asignar un grado de probabilidad a cada tipo de amenaza. Una alta probabilidad indica que hay más posibilidades de que la amenaza ocurra, como en el caso de que haya un historial de su ocurrencia en el pasado. Una probabilidad media indica que la amenaza podría o no ocurrir. Una probabilidad baja indica que la amenaza probablemente no ocurra, aunque es posible que sí suceda. Finalmente, el equipo de evaluación debe evaluar el posible impacto de cada posible amenaza en la organización. Por ejemplo:

- Si quedara destruida la base de datos de clientes de la empresa ¿cómo afectaría esto actividades cómo las ventas, la facturación, etc.?
- Si la red de la empresa quedara inhabilitada durante un día ¿cuál es el posible costo para la compañía en cuanto a pérdidas de ventas, productividad, etc.?
- Si se hicieran públicos los registros de los clientes ¿cuál es el posible costo en cuanto a procesos legales, negocios que retiren los clientes, o acciones similares?
- Una vez que se hayan hecho y respondido todas estas preguntas, es relativamente sencillo elaborar una matriz de valoración de amenazas que pondrá esta información en perspectiva y ayudará a que el equipo de elaboración de política concentre las políticas de seguridad de la empresa en las esferas de amenaza de mayor probabilidad y de efectos más significativos.

Análisis de las vulnerabilidades organizativas y de red

En los Capítulos 5 y 6, hablamos sobre cómo analizar las *vulnerabilidades técnicas* de una red. Estas vulnerabilidades son aquellas características o configuraciones que pueden ser explotadas por un atacante a fin de obtener acceso no autorizado o utilizar indebidamente una red y sus recursos. Las vulnerabilidades de red a menudo son denominadas *hoyos de seguridad*. Los hoyos de seguridad deben identificarse como parte del proceso de elaboración de política. Estas vulnerabilidades pueden ser causadas por una característica de programación o (mala)configuración del sistema operativo, un protocolo o servicio, o una aplicación. Entre los posibles efectos están:

- Código de sistema operativo que permite a los hackers bloquear una computadora al acceder a un archivo cuya ruta contiene determinadas palabras reservadas
- Abrir innecesariamente los puertos TCP/UDP que los hackers pueden utilizar para entrar al sistema u obtener información sobre este
- Una manipulación del JavaScript por parte de un buscador de la web que permite que un código maligno ejecute comandos no deseados

Las conexiones de la red a la Internet y otras redes evidentemente afectan la vulnerabilidad. Los datos en una red que esté conectada permanentemente por una

conexión de alta velocidad son más vulnerable que en una red que esté conectada solo intermitentemente con el exterior. La red que permita múltiples conexiones externas (como módems y líneas telefónicas en varias computadoras diferentes) aumenta la vulnerabilidad a un ataque del exterior. Las conexiones por medio de un módem merecen una consideración especial. Aunque una conexión telefónica está menos expuesta a la intrusión que una conexión dedicada a tiempo completo –tanto porque está conectada con el exterior por un período menor, reduciendo la oportunidad de una intrusión, y dado que por lo general tiene una dirección IP dinámica, que dificulta que el intruso la localice en múltiples ocasiones—que permite que las estaciones de trabajo en la red tengan módems y líneas telefónicas puede crear un gran riesgo de seguridad.

Si está inadecuadamente configurada, una computadora con una conexión telefónica a la Internet que es también conectada por cable a la red interna puede actuar como un enrutador, y permitir que los intrusos externos accedan no solamente a la estación de trabajo conectada al módem sino además otras computadoras de la LAN. Una de las razones para autorizar los módems en estaciones de trabajo individuales es permitir que los usuarios se conecten telefónicamente a otras redes privadas. Una forma más segura de hacer esto es retirar los módems y hacer que los usuarios establezcan una conexión VPN con la otra red privada mediante la conexión LAN a Internet. La mejor política de seguridad es tener la menor cantidad posible de conexiones de la red interna al exterior y controlar el acceso en esos puntos de entrada (el *perímetro de red*).

NOTA

Las herramientas de software de terceros conocidas como *escáneres de vulnerabilidad* están destinadas para descubrir las vulnerabilidades de la red, utilizando una base de datos de debilidades conocidas y comúnmente explotadas, e investigar las debilidades en su red.

Las *vulnerabilidades organizativas* son aquellas esferas y datos abiertos al peligro o el daño si están expuestos a un ataque. A fin de determinar estas vulnerabilidades, el equipo de política debe primeramente identificar los valores que podrían quedar expuestos a los tipos de amenazas previamente identificadas. Por ejemplo:

- Los registros financieros de la empresa
- Secretos comerciales
- Información personal
- Información usuario/cliente
- Correspondencia privada
- Propiedad intelectual
- Documentos de estrategia de comercialización y de negocios
- Integridad de red
- Archivos de sistema y programa

Se deben tener en cuenta una serie de factores cuando el equipo esté valorando las vulnerabilidades, incluido el tipo de datos que pasan por la red de la organización. La vulnerabilidad de los datos altamente confidenciales (como secretos comerciales) o irreemplazables (como obras de arte o escritos originales) deben ser un tema de la más alta prioridad. La vulnerabilidad también se ve afectada por el tamaño de la organización

y la red. Mientras más personas tengan acceso a la red mayor será la posibilidad de exposición al daño intencional por parte de alguna persona.

Examen del ciberderecho o derecho informático
Desarrollo de política en el ambiente de alta seguridad

Determinados campos tienen requisitos de alta seguridad inherentes. Un ejemplo evidente son los organismos militares u otros gubernamentales que tienen que ver con temas de defensa o de seguridad nacional. Las empresas privadas con contratos de defensa gubernamentales también caen en esta categoría. Otros podrían ser menos evidentes:

Las firmas legales están obligadas por la ley y la ética a proteger la confidencialidad; las oficinas médicas deben proteger los expedientes de sus pacientes; las agencias encargadas de hacer cumplir la ley, los tribunales y otros organismos gubernamentales deben proteger la información sensible; las instituciones educacionales deben proteger la privacidad de los expedientes escolares. La compañía que recopila datos de individuos u organizaciones con la promesa de que dicha información se mantendrá confidencial, tiene la obligación de protegerla.

Asimismo, debe tener en cuenta el carácter competitivo de una actividad comercial. En una esfera como la investigación biogenética —que es un mercado codiciado— diariamente tienen lugar nuevos acontecimientos. Cualquiera de ellos podría representar elevadas ganancias para la empresa que patentara una idea, de manera que la protección de los secretos comerciales se convierte en algo de una importancia vital. La mayoría de las empresas tienen *alguna* información de carácter confidencial en los sistemas de computadora de su red, pero los requisitos de seguridad en algunas esferas son más elevados que en otras. Este nivel de exigencia debe tenerse en cuenta en la elaboración del plan de seguridad.

Por lo general es necesario proteger nóminas y registros de personal (expediente del personal, documentos de reclamación de seguros, por ejemplo), registros financieros de la empresa (documentos de contabilidad, estados financieros, documentos relacionados con los impuestos), así como diversos otros documentos relacionados con la actividad comercial. Incluso en los casos en que estos documentos se deban hacer públicos, es preciso tomar medidas para garantizar que no se les pueda modificar o destruir. Recordemos que la *integridad de los datos*, así como la *confidencialidad de los datos*, se protegen con un buen plan de seguridad.

En Estados Unidos las leyes que rigen la protección de la privacidad en determinadas industrias influyen en el plan y las políticas de seguridad de una organización. Por ejemplo, la Ley de portabilidad y responsabilidad del seguro de salud (HIPAA, de Health Insurance Portability and Accountability Act) rige el almacenamiento y transmisión por medios electrónicos de información sobre los pacientes y exige que los médicos y otras personas encargadas de brindar servicios de salud cumplan ciertas normas de seguridad, informen a los pacientes sobre las medidas de privacidad en vigor, y documenten cualquier caso en que la información sobre un paciente sea revelada a otras entidades (salvo algunas excepciones). Todas las actividades médicas están obligadas a cumplir la ley HIPAA desde abril de 2003. La violación de las regulaciones previstas en la ley HIPAA puede conllevar multas de entre $100 (por violación) y $250 000, y hasta

10 años de privación de libertad en casos de revelación deliberada de información de un paciente con la intención de vender, transferir o usarla en provecho propio o con fines comerciales o malintencionados.

La HIPAA es una ley federal; en algunos estados también existen leyes que imponen medidas de protección de la privacidad aún más rigurosas en la industria de la salud. Otras industrias se rigen por leyes similares. Por ejemplo, la ley Gramm-Leach-Bliley (GLB) impone restricciones de las instituciones financieras respecto de la divulgación de la información personal de los clientes, con penalidades similares en caso de infracción.

Análisis de los factores de la organización

El siguiente paso en la evaluación de las necesidades de seguridad es definir la filosofía de la gerencia de la organización en cuanto a la seguridad frente a la accesibilidad. Es importante recordar que ambas son características antagónicas: mientras más de una tenga un sistema, menos tendrá de la otra. La filosofía de la organización determina dónde cae una red específica en la ecuación seguridad-acceso (lo cual determinará sus políticas).

Algunas empresas instituyen un estilo de administración altamente estructurada y formal. Se espera que los empleados respeten una estricta línea de mando, y la información por lo general se difunde sobre la base de las necesidades informativas de cada cual. Los organismos gubernamentales, especialmente los relacionados con la actividad de hacer cumplir la ley, como departamentos policiales y organismos investigativos, a menudo siguen la filosofía que en ocasiones se conoce con el nombre de *modelo paramilitar*.

Otras empresas, especialmente las pertenecientes a las industrias "creativas" y otras esferas sujetas a poco grado de regulación estatal, se basan en la premisa opuesta: que todos los empleados deben tener la mayor cantidad de información posibles, que los gerentes deben actuar como "líderes de equipo" más que como supervisores autoritarios, y que las restricciones a las acciones de los empleados se deben imponer solamente cuando es necesario en aras de la eficiencia y la productividad de la organización. A veces a este modelo se le da el nombre de *modelo de "una gran familia feliz"*. Se le da más valor a la creatividad que a la aplicación de las reglas, y la satisfacción en el empleo se considera un aspecto importante de la elevación del rendimiento y la productividad de los empleados.

En los círculos de gerencia empresarial, estos dos modelos diametralmente opuestos son denominados *Teoría X* (estilo paramilitar tradicional) y *Teoría Y* (enfoque moderno con idea de equipo). Si bien en años recientes se han hecho populares numerosos otros modelos de gestión, como la gestión por objetivos (GPO) y gestión de calidad total (GCT), el estilo de gestión de cada empresa cae en alguna zona entre la Teoría X y la Teoría Y. El modelo de gestión está basado en las filosofías personales de los altos funcionarios encargados de tomar las decisiones en la empresa, respecto de la relación entre la gerencia y los empleados.

El modelo de gestión puede influir profundamente sobre lo que es y lo que no es aceptable en la planificación de la seguridad de la red. Una política de seguridad basada en la negación total del acceso que se considera apropiada en una organización de la Teoría X podría provocar tanto resentimiento e insatisfacción en el personal de una

empresa de Teoría Y que afectaría el desarrollo de las operaciones. Los formuladotes de política deben siempre analizar el "ambiente" de la empresa como parte de la planificación de la seguridad. Si existen buenas razones para aplicar una seguridad estricta en un ambiente de Teoría Y, es probable que sea necesario justificar las restricciones ante la gerencia y "venderlas" a los empleados, mientras que esas mismas restricciones podrían ser aceptadas sin cuestionamiento en una organización más tradicional.

Análisis de los factores jurídicos

Las medidas de seguridad dependen no solo de los deseos de los gerentes de la empresa, sino que también pueden ser dictadas, o al menos guiadas, por el derecho penal o civil en una jurisdicción particular. Si la industria de la empresa está sujeta a regulaciones gubernamentales, la información en su red se debe regir por las leyes de protección de la privacidad, o contratos empresariales prohíben la divulgación de la información en la red de la empresa, estos son factores jurídicos que deben tenerse en cuenta al establecer las políticas de seguridad.

Es importante proteger a la empresa de la responsabilidad en que podría incurrirse si los empleados u otras personas que utilizan la red violan las leyes. Por esta razón, es vital que en el equipo que elabore la política de seguridad participen uno o dos abogados conocedores de las leyes aplicables (por ejemplo, la Ley de protección de datos en el Reino Unido, o la Ley de derecho de autor del Milenio Digital en Estados Unidos) y que estén familiarizados con los términos de los contratos firmados por la empresa con socios, proveedores, clientes y otros.

Análisis de los factores de costo

Por último, algo que es también de gran interés; la evaluación de las necesidades debe tomar en consideración el costo monetario de la aplicación de un mayor nivel de seguridad. La determinación de los fondos disponibles para mejorar la seguridad afectará las políticas en esta esfera al obligar al equipo que las elabora a diferenciar entre las *necesidades* de seguridad y los *deseos* de seguridad de la organización.

Los factores de costo también pueden obligar al equipo a dar prioridad a las necesidades de seguridad, de manera que se puedan abordar las amenazas más probables o inminentes, proteger los valores más importantes y eliminar primero las vulnerabilidades más flagrantes.

Valoración de las soluciones de seguridad

Una vez que la empresa ha identificado y documentado sus necesidades de seguridad y establecido un presupuesto para abordarlas, es posible valorar las soluciones y determinar cual o cuales satisfacen las necesidades y se avienen al presupuesto. Las soluciones de seguridad de redes se pueden dividir por lo general en tres amplias categorías: soluciones de hardware, soluciones de software y soluciones de políticas solamente.

Soluciones de hardware

Las soluciones de seguridad basadas en hardware se refieren a la adición de algunos dispositivos físicos, como un cortafuegos dedicado para proteger la red o un lector de tarjeta inteligente para la autenticación de entrada. La eliminación de las unidades de

disquetes o de disco compacto de las computadoras para impedir la copia no autorizada de archivos o la introducción de virus, es también una solución basada en el hardware. Otros dispositivos de seguridad son:

- Dispositivos de captura de golpes de tecla para monitorear el uso de las computadoras
- Tokens De hardware para almacenar claves de seguridad.
- Dispositivos criptográficos para descargar el procesamiento de operaciones de criptografía.
- Dispositivos de autenticación biométrica, como escáneres de huellas dactilares o de retina.

Las soluciones de hardware pueden ser más costosas que las soluciones de software pero brindan varias ventajas. La seguridad basada en hardware generalmente es más segura porque la información de seguridad como las claves privadas, está menos expuesta y es más difícil violentar el hardware que el software. Además, las soluciones de hardware a menudo ofrecen un rendimiento más rápido.

Soluciones de Software

Las soluciones de software incluyen sistemas de detección de intrusión, software de filtrado de paquete/circuito/aplicación, y software de auditoria de seguridad, así como paquetes de software cortafuegos, como el servidor ISA (Internet Security and Acceleration, o Seguridad y Aceleración de Internet) de Microsoft que combina estas funciones. Otras soluciones de seguridad basadas en software son programas antivirus como los creados por Symantec y McAffe, "Spyware" utilizados para monitorear como se utiliza una computadora [incluidos los programas husmeadores de paquetes (packet sniffers)] que pueden capturar y analizar el tráfico en la red), y paquetes de gestión de redes que incorporan características de seguridad. Las revisiones (patches) para sistemas operativos y aplicaciones que solucionan fallas de seguridad también se pueden incluir en esta categoría.

Soluciones de política

La mayoría de las medidas de seguridad basadas en hardware llevan aparejadas políticas que prescriben cuando y como deben ser puestas en práctica y utilizadas, pero muchas medidas de seguridad consisten en políticas solamente:

- Políticas que prohíben que los usuarios divulguen sus contraseñas.
- Políticas que requieren que los usuarios cierren sus estaciones de trabajo cuando se ausentan de sus mesas.
- Políticas que requieren que los usuarios obtengan autorización antes de instalar cualquier programa en sus máquinas.
- Políticas que prohíben a los usuarios permitir que otras personas utilicen su computadora después que ellos hallan ingresado a la red.

Por supuesto, en muchos casos las políticas se aplican mediante el software o el hardware. Por ejemplo, una política que prohíba que los usuarios copien archivos de la red a sus discos duros locales se puede aplicar mediante permisos para un acceso de solo lectura. Una política que requiera que los usuarios cambien su contraseña cada 30 días puede aplicarse configurando el sistema de manera que las contraseñas expiren tras ese período.

Cumplimiento de las normas de seguridad

El documento de política de seguridad debe presentar las normas relacionadas con temas como confidencialidad e integridad de los datos, autorización y autenticación, acceso, uso apropiado de recursos de red, y temas de privacidad de empleados. Si se requiere que se cumplan normas federales (como clasificación C2) o normas de industrias específicas (como la ley HIPPA para las organizaciones de salud), entonces las especificaciones deben incluirse como obligatorias en el documento de política.

Se debe examinar si las políticas cumplen las normas internacionales como la ISO 17799. Quizás se desee hacer referencia a secciones de la ISO 17799 en políticas individuales, de la misma forma que se hace referencia a políticas conexas.

Niveles de seguridad gubernamental

Los niveles de seguridad podrían ser de interés en la elaboración de la política de seguridad de una empresa, aunque probablemente no sean importantes a menos que la organización trabaje con un contrato gubernamental que requiera un nivel de seguridad específico. El gobierno de Estados Unidos estipula especificaciones para la jerarquización de las medidas de seguridad de redes en una publicación que a la que muchos llaman el *libro naranja* y que oficialmente lleva el nombre de Department of Defense Trusted Computer System Evaluation Criteria (Criterios de evaluación del sistema de computación fiable del Departamento de Defensa) o TCSEC (por sus siglas en inglés). El *libro rojo* o Trusted Network Interpretation of the TCSEC (TNI) explica cómo se aplican los criterios de evaluación del TCSEC a las redes de computadoras.

Otros países tienen sistemas de jerarquización de seguridad que funcionan de forma similar. Por ejemplo:

- CTPEC (Canadá)
- AISEP (Australia)
- ITSEC (Europa oriental)

Para obtener un contrato gubernamental en Estados Unidos, a menudo las empresas necesitan obtener una clasificación C2. Esta clasificación tiene varios requisitos:

1- que el sistema operativo en uso sea capaz de rastrear el acceso a los datos, incluido quién accedió a ellos y cuándo lo hizo (como lo hace la función de auditoría de Windows NT/2000).

2- que el acceso de esos usuarios a objetos esté sujeto a control (permisos de acceso).

3- que los usuarios estén identificados claramente en el sistema (cuenta y contraseña de usuarios).

4- que los sucesos relacionados con la seguridad puedan ser rastreados y registrados de manera permanente para que sean auditados (registro de auditoría).

NOTA

Estas son directrices generales, y los requisitos deben ser aplicados de maneras específicas para obtener la clasificación. Si una organización necesita la clasificación C2 para sus sistemas, el equipo de elaboración de política debe consultar las publicaciones del Centro Nacional de Seguridad Informática (Nacional Computer Security Center, NCSC) para cerciorarse de que cumplen todos los requisitos).

Se puede acceder al documento (ver el TCSEC en español) o *libro naranja* en www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html.

Utilizando los modelos de políticas

Es posible utilizar modelos de políticas de seguridad que sirvan de guía al equipo de elaboración en su trabajo. Estos modelos pueden adquirirse de varias fuentes (por ejemplo, RUSecure Information Security Policies), y existen modelos que pueden descargarse del sitio de organizaciones como el SANS Institute.

Una ventaja asociada es que los modelos de política que se adquieran tendrán la garantía de cumplir la norma ISO 17799, la HIPAA o leyes y normas afines. No obstante, los encargados de redactar la política de seguridad deben tener cuidado de no copiar simplemente un modelo de política, sin antes realizar un estudio exhaustivo para cerciorarse de que se aviene a la filosofía, el presupuesto y el modelo comercial de la organización. Usualmente, los modelos de política se "sanean", es decir, los temas específicos de una organización son eliminados para brindar una política genérica diseñada para servir como punto de partida para crear políticas personalizadas.

Definición de las esferas de la política

Un elemento importante en la elaboración de política es la definición de las esferas que abarcarán las políticas de seguridad de la organización. Este proceso variará de una organización a otra, pero siempre existen esferas de interés comunes. Ejemplo de ello son las políticas relacionadas con las contraseñas. Seguidamente explicamos algunos de los factores más importantes en el establecimiento de políticas de contraseñas.

Políticas de contraseñas

En el mundo del trabajo en red, las contraseñas (conjuntamente con los nombres de cuenta de usuario) son normalmente las "llaves al reino" que dan acceso a los recursos y datos en la red. Podría parecer simplista decir que un plan integral de seguridad debe incluir una política de contraseñas efectiva; sin embargo, es un componente básico cuya aplicación es más compleja de lo que parece ser a primera vista. A fin de ser efectiva, una política de seguridad debe exigir que los usuarios escojan contraseñas difíciles de violentar pero fáciles de recordar, de manera que no cometan la usual violación de seguridad de anotar la contraseña en un papel con pegamento que después pegan al monitor o dejan en la gaveta superior del escritorio.

Una buena política de contraseñas es la primera línea de defensa para proteger la red de los intrusos. Las prácticas descuidadas de contraseñas (escoger contraseñas ordinarias como *dios* o *amor* o el nombre del cónyuge del usuario; escoger contraseñas cortas, sin cambios de minúsculas y mayúsculas o de letras y números; anotar las contraseñas o enviarlas por la red en texto simple) son como dejar la puerta del auto abierta con las llaves en el arranque. Si bien determinados intrusos atacan un sistema específico, muchos otros siempre están "buscando" una red fácil de violentar. Carecer de una buena política de contraseñas es para ellos una invitación en blanco.

Los que elaboran las políticas deben recordar que los cortafuegos costosos y sofisticados, así como otras medidas de seguridad estrictas (que no sean dispositivos de reconocimiento biométrico, como escáneres de huellas dactilares o de retina) no

protegerán la red si un intruso conoce un nombre de usuario y contraseña válidos. Es especialmente importante utilizar contraseñas fuertes para las cuentas de administrador.

Las mejores prácticas para la creación de contraseñas requieren tener en cuenta lo siguientes aspectos, los cuales analizamos en las secciones subsiguientes:

- Extensión y complejidad de la contraseña.
- ¿Quién crea la contraseña?
- Cambio obligatorio de contraseña.

Extensión y complejidad de la contraseña

Resulta fácil definir una "mala" contraseña: aquella que una persona que no sea el usuario autorizado puede adivinar fácilmente. Recordaremos que en el Capítulo 6 dijimos que una de las formas en que trabajan los *"cracker"* es mediante el uso de la fuerza bruta. En este tipo de ataque el *cracker*, manualmente o, por lo general utilizando una secuencia de comandos o programa de software escrito especialmente al efecto simplemente intenta todas las posibles combinaciones de caracteres hasta dar con la correcta. Por supuesto, si se usa este método será mas fácil adivinar una contraseña corta que una larga, ya que serán menos las combinaciones posibles. Por esta razón, la mayoría de los expertos de seguridad recomiendan que las contraseñas tengan una extención mínima (por ejemplo, ocho caracteres). Los sistemas operativos modernos de trabajo en red, como Windows 2000, permiten que los administradores de dominio impongan reglas como esa, de manera que si un usuario intenta establecer una contraseña que no cumpla con el requicito de extención mínima, la contraseña es rechazada.

¿Quién crea la contraseña?

Los administradores de red podrían sentir la tentación de instituir una directiva mediante la cual fueran ellos quienes crearan todas las contraseñas y las informaran a los usuarios. Esta política tiene la ventaja de garantizar que todas las contraseñas cumplan con los criterios del administrador en cuanto a extensión y complejidad. No obstante también tiene algunas desventajas significativas:

- Representa una pesada carga para los administradores quienes deben encargarse de cambiar todas las contraseñas e informar a los usuarios cuales les corresponden. Como es natural, el administrador no deseará notificar al usuario su contraseña por correo electrónico u otro canal no seguro de hecho, la mejor forma de hacerlo es entregar personalmente la información sobre la contraseña. En una organización grande, esta tarea se vuelve especialmente trabajosa si existe una política que requiera que las contraseñas se cambien regularmente.
- Para los usuarios será más difícil recordar contraseñas que no halla escogido ellos mismos. Ello significa que será más probable que anoten la contraseña, lo cual afecta la seguridad. De lo contrario tendrían que contactar frecuentemente al administrador para que les recuerde las contraseñas.
- Si el administrador crea todas las contraseñas ello significa que las conoce todas. Ello podría o no ser aceptable a tenor de la política de seguridad global. Para algunos usuarios (incluso los miembros de la gerencia) podrían sentirse incómodos sabiendo que el administrador conoce sus contraseñas. Aunque un administrador puede por lo general acceder a la cuenta y/o los

archivos de un usuario sin saber su contraseña, es menos evidente para los usuarios y por lo tanto menos preocupante.

Usualmente la mejor opción es permitir que los usuarios creen sus propias contraseñas según determinados parámetros (requisitos de extensión y complejidad). Es menos probable que el usuario olvide la contraseña porque puede crear una contraseña compleja que no tenga sentido para los demás pero para él sí. Por ejemplo, sería difícil para una persona adivinar la contraseña Mft2doSmis. Tiene diez caracteres combina letras y números y mayúsculas y minúsculas de una manera aparentemente aleatorio. Para un usuario podría ser fácil de recordar porque significa My favorite thing to do on Sunday morning is sleep (Lo que prefiero hacer el domingo en la mañana es dormir).

Política de cambios de contraseña

Las mejores prácticas establecen que los usuarios cambien sus contraseñas a intervalos regulares y cuando se sospeche que se ha producido una violación de la seguridad. Los sistemas operativos modernos de trabajo en red como Windows 2000 permite al administrador fijar un tiempo de validez máximo de la contraseña, que obligue a los usuarios a cambiarlas una vez transcurrido el período especificado (en días). Los períodos de expiración de las contraseñas pueden fijarse entre1 y 999 días. Las cuentas de usuarios individuales que precisan mantener la misma contraseña se pueden configurar de manera tal que la contraseña nunca expire. Así se deja sin efecto el período general de expiración de contraseña.

Dado que, por naturaleza, la mayoría de los usuarios tienden a crear contraseñas lo más fácil de recordar posible, las políticas deben estar dirigidas a evitar las prácticas siguientes, todas las cuales pueden representar riesgos para la seguridad:

- Cambiar la contraseña por una variación de la ya existente (por ejemplo, cambiar Tag2mB por Tag3mB)
- Cambiar la contraseña una y otra vez entre dos variantes preferidas siempre que tenga que hacerse el cambio (es decir, por ejemplo, cambiar Tag2mB por VERoh9 y después volver a poner la primera, y así sucesivamente)
- "Cambiar" la contraseña por la misma contraseña (poner la misma contraseña que existía como si fuera una nueva)

Los administradores pueden utilizar características de los sistemas operativos para impedir estas prácticas. Por ejemplo, en Windows 2000, es posible configurar el sistema operativo de manera que recuerde el historial de contraseñas del usuario y registre hasta un máximo de 24 contraseñas más recientes, y de esa forma el usuario no podrá cambiar la contraseña por una que ya haya sido utilizada en ese período.

Resumen de las mejores prácticas de contraseñas

Aquí presentamos una reseña de las mejores prácticas de contraseñas:

- Las contraseñas deben tener un mínimo de ocho caracteres
- Las contraseñas no deben ser palabras del vocabulario ordinario
- Las contraseñas deben tener una combinación de letras, números y símbolos
- Las contraseñas deben ser creadas por los propios usuarios
- Las contraseñas deben ser fáciles de recordar
- Las contraseñas jamás se deben anotar
- Las contraseñas deben ser cambiadas regularmente

- Las contraseñas se deben cambiar siempre que se sospeche que se han violentado
- Las políticas de cambio de contraseñas deben impedir que los usuarios realicen solamente cambios ligeros

Otras esferas de política comunes

Las políticas de contraseña son importantes para casi todas las organizaciones, pero entre las otras esferas de política que se deben abordar están:

- **Políticas de seguridad de servidores y estaciones de trabajo**: estas definen las reglas que rigen la seguridad física de las computadoras conectadas a una red, que exigen el cierre de la sesión de usuario o el uso de protectores de pantalla protegidos por contraseñas cuando se abandona la estación de trabajo, políticas de apagado, compartición de las estaciones de trabajo, etc.
- **Políticas de encriptación**: definen cuándo deben y no debe usarse la encriptación, así como las tecnologías y los algoritmos que son aceptables. Por ejemplo, una política podría estipular que se utilicen algoritmos probados como 3DES, RSA o IDEA y prohibir el uso de algoritmos patentados o no estándares.
- **Políticas de correo electrónico**: rigen cuestiones como la apertura de adjuntos, el uso de clientes de correo-e para mostrar mensajes HTML, el reenvío de correros-e internos a personas fuera de la organización, etc.
- **Políticas de acceso remoto**: definen reglas para conectarse a la red de la empresa desde el exterior mediante una conexión telefónica o una VPN; especifican cuáles métodos de autenticación se pueden utilizar, prohíben el "*dual homming*" (conectarse a otra red cuando a la vez se está conectado a la red de la empresa), etcétera.
- **Políticas de acceso inalámbrico**: establecer normas para conectarse a la red de la empresa utilizando un equipo inalámbrico, exigir el uso de WEP u otras tecnologías de encriptación, prohibir la conexión de puntos de acceso inalámbrico no autorizados a la red, etc.
- **Políticas de uso aceptable**: definen lo que está autorizado o prohibido hacer por parte de los usuarios en la red; rigen el uso personal (como navegar la web, el envío de mensajes de correo electrónico personales), la descarga de archivos, el ingreso y publicación en grupos de noticias, la prohibición de la instalación de software no autorizados, etc.

Muchas otras esferas de política podrían ser aplicables a organizaciones específicas; la definición de esferas de política que deben abordarse es una tarea importante para el equipo encargado de elaborar la política. Pueden encontrarse ejemplos de documentos de política que abarcan las esferas mencionadas (y otras) en la página del Proyecto de política de seguridad (Security Policy Project) del SANS Institute en www.sans.org/newlook/resources/policies/policies.htm#template.

Elaboración del documento de política

El equipo de elaboración de la política debería ser preferiblemente seleccionado con anterioridad al proceso de evaluación de las necesidades, en el cual debe participar. Debe estar integrado por personal administrativo y personal de la esfera de TI, conjuntamente

con algún miembro de cada departamento de la organización. También debe integrarlo un asesor jurídico. A medida que logran codificar y dar forma a las políticas, los miembros del equipo deben trabajar muy estrechamente a fin de:

- Establecer prioridades de seguridad sobre la base de la matriz de valoración de amenazas
- Tener en cuenta e incorporar, según sea necesario, normas de seguridad
- Determinar las prácticas y los procedimientos necesarios para lograr el nivel necesario de seguridad, tanto al nivel administrativo como de los usuarios
- Definir claramente tanto los comportamientos requeridos como los prohibidos
- Determinar y definir las consecuencias de las violaciones
- Determinar que las políticas sean factibles de hacer cumplir, así como los métodos para hacerlo.

Las políticas deben representar un consenso en cuanto a lo que es y no es apropiado en cuanto a comportamiento en relación con las computadoras.

Establecimiento del alcance y las prioridades

El equipo de elaboración de política debe determinar el alcance del documento de política. Por ejemplo, ¿se incluirán en la política de seguridad las políticas referidas al uso de teléfonos, teléfonos celulares y el fax o serán incluidas en un documento de política independiente? ¿Se abarcarán los procedimientos para la compra de hardware y software o será esto tema de un documento de política general sobre las compras de la organización? La forma más fácil de crear una pesadilla de política es tener dos documentos de política con directivas antagónicas.

Es posible que no existan los fondos necesarios para cubrir todas las necesidades de seguridad. Incluso si estuvieran disponibles fondos suficientes para ello, la mayoría de las organizaciones no podrían aplicar simultáneamente todas las medidas de seguridad. Es por ello que el equipo debe establecer prioridades para definir qué políticas se van a aplicar primero. Las prioridades se establecerán sobre la base de los siguientes factores:

- Inmediatez de la amenaza
- Posible pérdida
- Facilidad de la aplicación
- Disponibilidad de fondos

En la sección sobre evaluación de la amenaza analizamos la inmediatez de las amenazas y las posibles pérdidas. La facilidad de aplicación puede ser también un factor que ayude a establecer prioridades. Las políticas que pueden ser aplicadas fácil y rápidamente se pueden poner en primer orden, mientras comienza el trabajo en aquellas que requieren más tiempo y esfuerzo. Por lo general, las políticas exigen uno o varios de los siguientes elementos: salvaguardias físicas, mecanismos de seguridad técnica, o procedimientos administrativos. El cambio de los procedimientos administrativos a menudo es posible hacerlo con mayor celeridad y facilidad que la aplicación de salvaguardias físicas (la cual podría requerir la adquisición y el montaje de equipos o modificaciones a las instalaciones) o mecanismos técnicos (que podrían requerir la compra de software así como una curva de aprendizaje para el personal de TI y los usuarios).

Directrices para la elaboración de la política

Las políticas se pueden dividir en diferentes tipos: *políticas de reglamentación*, que deben aplicarse para cumplir la ley o requisitos de un organismo reglamentador; *políticas de asesoramiento*, que se recomiendan fuertemente pero no tienen carácter obligatorio; y *políticas informativas*, las cuales brindan información pero no prescriben ni proscriben acción alguna.

Las políticas de seguridad pueden cumplir diferentes objetivos secundarios, además del objetivo primario de impedir el uso no autorizado de la red. Por ejemplo, las políticas pueden ser la base para las acciones respecto del personal (disciplina o terminación), se pueden utilizar en defensa de la empresa (o en contra de ella) en un proceso legal civil, e incluso pueden ayudar en la preparación de un caso penal para llevar a los tribunales. De manera que es imperativo que las políticas que finalmente sean publicadas estén bien pensadas, sean razonables y estén claramente articuladas.

Los que redactan la política deben evitar, tanto como sea posible, el uso de palabras técnicas; las políticas de seguridad deben ser comprensibles y utilizables por parte de los administradores de la empresa, el personal de recursos humanos y los usuarios a los cuales se aplica, así como por el personal de TI. Es una buena idea incluir un glosario para definir la terminología técnica que sea imprescindible utilizar. También es importante establecer responsabilidades; en el documento de política se debe identificar la persona o las personas responsables para cada esfera de la seguridad de redes/computadoras, así como el ámbito de su responsabilidad.

Las políticas deben establecer cuáles acciones son exigidas, recomendadas o prohibidas. Además de definir la acción, deben exponer un ejemplo de comportamiento que constituiría tal acción, o una violación. Por ejemplo, si la política expresa, "Cada usuario deberá velar por el carácter secreto de su contraseña de entrada a la red", deberá poner ejemplos concretos como, "Los usuarios deberán memorizar sus contraseñas. Los usuarios tienen prohibido tener dentro de los predios de la empresa algún registro escrito de sus contraseñas y tienen prohibido divulgar sus contraseñas a otras personas. Si alguna persona pide a un usuario que divulgue su contraseña, el usuario deberá informarlo inmediatamente al administrador de la red".

Las políticas deben establecer claramente las consecuencias de las violaciones. Las consecuencias se deben basar en la severidad de la violación, el daño o la pérdida causada, la intención o falta de intención, y el historial de violaciones cometidas. Es importante garantizar que las políticas sean consecuentes, no solamente entre sí dentro del documento de política de seguridad informática, sino con otras políticas departamentales y a nivel de empresa. Por último, es imprescindible garantizar que las políticas no entren en conflicto con alguna ley local, estatal o federal.

Organización del documento de policía actuar el documento de política

El documento de política no debe ser una mezcolanza de directivas de seguridad. Debe estar organizado de manera lógica, con miras a que las políticas afines sean reunidas dentro de esferas de amplia definición. Por ejemplo, las secciones podrían ser:

- Seguridad física (por ejemplo, ubicación de los servidores, instalación de hardware, aseguramiento del cableado, aseguramiento de las impresoras, ubicación de las cintas de respaldo (backup), acceso a locales/edificios donde están ubicadas los equipos de computación.

- Seguridad del sistema local (por ejemplo, responsabilidades de los usuarios respecto de la seguridad de sus estaciones de trabajo, instalación de software, copia de archivos).
- Seguridad de contraseñas (por ejemplo, las políticas que rigen la extensión de las contraseñas, la complejidad, el cambio y la protección de estas).
- Seguridad de redes (por ejemplo, las políticas que rigen el uso de cortafuegos, la descarga y carga de archivos, el acceso a la web, el uso de programas de mensajería instantánea).
- Seguridad de servidores (por ejemplo, el acceso a servidores, protección a servidores web, servidores de archivos, servidores DNS, servidores de autenticación).
- Seguridad del acceso remoto (por ejemplo, políticas que rigen para quienes hacen trabajo a distancia, los ejecutivos en el exterior, el acceso desde el hogar fuera del horario laboral, software y configuraciones VPN designados).
- Políticas de administración de datos y manejo de documentos (por ejemplo, políticas que rigen la transferencia de datos, seguridad de las bases de datos, modificación de las estructuras de directorio, creación/borrado de archivos, políticas de nombres de archivos, clasificación de la sensibilidad de los datos).
- Seguridad de correo electrónico (por ejemplo, políticas que rigen el envío/recepción de adjuntos, el uso de correo HTML, configuración de cliente de correo electrónico).
- Políticas de desarrollo de software (por ejemplo, para la seguridad y control del código de software en otro de la empresa)
- Seguridad del comercio electrónico (por ejemplo, para las compras y ventas en línea)
- Seguridad de las comunicaciones inalámbricas (por ejemplo, políticas que rigen las normas para el uso de los dispositivos inalámbricos en la red)
- Políticas de intranet y extranet (por ejemplo, condiciones para el acceso, uso aceptable)
- Políticas de respaldo (por ejemplo, responsabilidad, retensión, almacenamiento)
- Prevención de desastres y políticas de recuperación (por ejemplo, continuidad de servicio, respaldo energético)
- Políticas que rigen las violaciones de la seguridad (por ejemplo, responsabilidad de información, manejo de respuesta)
- Políticas que rigen para los empleados que abandonan la empresa, tanto en condiciones amigables como en términos de enemistad (por ejemplo, la devolución de equipos y tarjetas de acceso, desactivación de cuentas de red)

El documento de política debería contener una detallada tabla de contenido. Cada política individual debe contener los componentes siguientes:

- Título que describa claramente a qué se refiere la política, con una nota sobre cualquier política que sustituya o sobre la cual tenga precedencia

- La fecha de entrada en vigor de la política (y su duración y fecha de expiración en caso de que sea transitoria)
- Referencia a políticas conexas
- Sección sobre el propósito y objetivo de la política
- Sección que identifique la amenaza o vulnerabilidad que se aborda
- Breve resumen de la política
- Sección que presente en detalle la política en sí, es decir, que defina qué está permitido y qué está prohibido; aquí deben identificarse las personas responsabilizadas con la aplicación de la política, a quién se aplica la política, así como cualquier excepción a ella
- Firma de la autoridad que emite la política

Educar a los usuarios de la red en los temas de seguridad

Las mejores políticas de seguridad del mundo serían ineficaces si los usuarios de la red no las conocen o si las políticas son tan restrictivas y representan tantos inconvenientes para los usuarios que éstos tratan de evadirlas. El plan de seguridad en sí mismo debería contener un programa para educar a los usuarios de la red –no solamente en cuanto a qué son las políticas sino también sobre por qué son importantes y cómo pueden beneficiarse de ellas los usuarios. Los usuarios deben además recibir instrucciones sobre cómo cumplir mejor las políticas y qué hacer en caso de no poder hacerlo o si se percatan de que otros usuarios las violan deliberadamente. Si los usuarios participan en las etapas de planificación y elaboración de la política, será más fácil educarlos y ganar su apoyo para las políticas en las etapas de aplicación y cumplimiento.

Hacer cumplir la política

Para que sean efectivas, las políticas deben ser factibles de cumplir y se deben hacer cumplir de manera coherente. Tener políticas que no sean factibles de hacerse cumplir (quizás porque no se cuenta con los medios para detectar las violaciones) o que no se desea hacer cumplir es peor que tener políticas inútiles; su existencia socava la credibilidad de las demás políticas. Las medidas de cumplimiento no deben ser selectivas; si es necesario hacer excepciones a las políticas en favor de determinadas personas o en determinadas circunstancias, tales excepciones deberán estar previstas en la propia política.

La facultad de aplicación debe estar dividida entre varias personas a fin de que exista un sistema de verificación y equilibrio. Los empleados deben ser informados sobre quién es el responsable de hacer cumplir la política, y el equipo encargado de hacer cumplirla debe estar facultado para hacerlo (por ejemplo, tener la facultad de monitorear el acceso al correo electrónico y la web). Los empleados deben ser informados, en el marco del documento de política, de que podrían ser objeto de ese monitoreo.

Divulgación de la política

Se deben distribuir copias de la política de seguridad informática a todo el personal a quienes se aplica. Todos los empleados deberán firmar un documento en el que reconozcan haber recibido, leído y aceptado los términos de la política. Las modificaciones a la política deben ser distribuidas y su distribución deberá ser igualmente

documentada. Esto es importante en caso de que se tome una medida disciplinaria contra un empleado que haya violado la política.

Copias de la política también deben ser puestas a disposición del personal en formato electrónico. Ello debe ser algo adicional, pero no sustitutivo del procedimiento recomendado anteriormente. Una de las formas más fáciles de hacerlo en la intranet es en formato HTML. Ello permite crear hipervínculos a los documentos de referencia y establecer referencias cruzadas entre políticas afines, además de facilitar que los usuarios consulten el documento en busca de palabras claves y frases. Se podrían incluir políticas de concientización y capacitación sobre seguridad, las cuales deben especificar las exigencias de capacitación para los diferentes niveles de personal (personal permanente, personal temporal, contratistas, gerencia, personal técnico, usuarios de nuevos sistemas, etc.).

Valoración permanente y actualización de política

La política de seguridad no es un documento estático. Las prácticas y prioridades comerciales empresariales varían y surgen nuevos tipos de amenaza, y los hackers aprenden nuevas formas de acceder y atacar las redes. El documento de política debería examinarse regularmente y revisarse cuando sea necesario para hacer frente a nuevos desafíos y adaptarse a las circunstancias cambiantes. El propio documento deberá incluir una política que prevea el programa de examen, quién es el responsable de realizar el examen, y el procedimiento para enmendar el documento, así como el procedimiento para divulgar los cambios a todo el personal afectado en la organización.

Resumen

Comprender los conceptos básicos de seguridad brinda al investigador del delito informático una clara ventaja para comunicarse con el personal de informática, así como una mejor idea de cómo exactamente se ha cometido el delito informático, sobre la base de las medidas de seguridad vigentes en ese momento. Además, los investigadores deben ser proactivos en cuanto a ayudar a las víctimas de los delitos informáticos a evitar un nuevo ataque. Si bien no es probable que al investigador se le pida que brinde asesoría detallada sobre la aplicación técnica de los sistemas de seguridad, deberá ser capaz de analizar opciones de manera general y guiar a las víctimas en la dirección correcta con algunas sugerencias generales

Un buen investigador, como buen especialista de seguridad de redes o un buen oficial para la prevención del delito, se percata de que todo plan de seguridad debe ser multicapas para que sea efectivo. Es importante abordar todas las esferas de seguridad principales. Estas incluye seguridad física, seguridad perimétrica (mediante la activación de cortafuegos en los puntos de entrada de la red), seguridad de los datos almacenados en discos (mediante la encriptación de archivos/discos), seguridad de los datos que viajan por la red (mediante la seguridad IP), y medios para verificar la identidad de los usuarios, computadoras, y otras entidades que tiene acceso a los recursos de la red (mediante la construcción de un PKI).

Muchas tecnologías de seguridad están basadas en técnicas criptográficas o las utilizan. Un investigador podría encontrar datos encriptados o incluso sospechar que la existencia de datos adicionales se está ocultando mediante la esteganografía. La comprensión de cómo se desarrolló la criptografía y cómo funciona en el mundo de la

informática es de gran valor para investigar muchos tipos de delitos informáticos. Conocer someramente al menos los diferentes tipos de encriptación y los algoritmos que usan permite al investigador valorar cuán seguro es un sistema específico, ya sea el sistema de la víctima de un delito informático o de un sospechoso de él.

Finalmente, es útil que el investigador comprenda el proceso de creación y aplicación de las políticas de seguridad y que vea muestras de ellas para que tenga una idea de dónde proceden (entenderá la filosofía general de la organización respecto de la seguridad) y cómo exactamente se despliega dentro de la organización para reducir el ámbito de la investigación. Un buen investigador de delitos informáticos debe tener un conocimiento al menos somero de todos los aspectos de seguridad de las tecnologías de la información. No tiene que ser necesariamente un profesional práctico de la TI, pero debe conocer la jerga y comprender lo que se dice cuando los verdaderos profesionales de la TI le brindan información sobre la red de la organización.

PREGUNTAS FRECUENTES

Las siguientes preguntas frecuentes, respondidas por los autores de este libro, están destinadas a medir su comprensión del concepto presentado en este capítulo y a ayudarlo en la aplicación práctica de estos conceptos. Para que el autor pueda responder sus preguntas sobre este capítulo, sírvase visitar el sitio www.syngress.com/solutions y hacer clic en "Ask the Author".

P: ¿Es conveniente que una organización adquiera software de encriptación que utilice algoritmos "secretos"?
R: No. La mayoría de los expertos de seguridad aconseja utilizar solamente algoritmos bien conocidos, viables y ya sometidos a prueba. Si bien un vendedor puede afirmar que su producto es más seguro porque los algoritmos que utiliza son patentados o secretos, en realidad los algoritmos patentados se consideran por lo general no seguros. La mayoría de los mejores algoritmos son públicos; conocer el algoritmo no le permite a un hacker descifrar la encriptación si la cifra es robusta. Si un vendedor no quiere hacer público su algoritmo, ello podría significar que no tiene confianza en que el algoritmo pueda soportar el escrutinio público. Para un excelente análisis de la encriptación normalizada abierta frente a las tecnologías patentadas, puede consultar *Secrets and Lies: Digital Security in a Networked World*, de Bruce Schneier.
P: ¿Las firmas digitales son jurídicamente vinculantes para firmar documentos como los contratos?
R: La respuesta breve es: depende. Muchos gobiernos nacionales y estaduales han aprobado leyes que rigen el flujo de las firmas digitales para diferentes tipos de transacciones. En 1998, el Congreso de los Estados Unidos aprobó la Ley de firma digital y autenticación electrónica (SEAL, por Digital Signature and Electronic Authentication Act) --la cual modificó la Ley de protección de la banca (Bank Protection Act), de 1968-- a fin de permitir el uso de firmas digitales para facilitar el uso de la autenticación electrónica por parte de las instituciones financieras (para más información sobre la ley, véase http://thomas.loc.gov/cgi-bin/query/z?c105:S.1594.IS:.).

En el 2000, el Presidente Bill Clinton firmó la Ley de firma electrónica en el comercio mundial y nacional (ESIGN por Electronic Signature in Global and National Commerce Act), con la cual se hizo legal el uso de las firmas digitales para la mayoría de los contratos concertados de manera electrónica (incluidas las hipotecas). Algunos acuerdos contractuales entre partes privadas en los Estados Unidos se rigen por leyes estaduales. La mayoría de los Estados han aprobado leyes que especifican las circunstancias en los cuales las firmas digitales se consideran jurídicamente vinculantes. Por ejemplo, el estado de Texas aprobó una ley sobre firma digital que entró en vigor en 1997, y que modificó el Código Comercial Uniforme, a fin de permitir que las comunicaciones electrónicas enviadas desde Texas y las recibidas en este estado en relación con la compra de mercancías estuvieran firmadas digitalmente. También especificaba que el uso de las firmas digitales estaría sujeto a las leyes penales incluidas en el código penal de Texas que se refieren al fraude y a los delitos en el ámbito de la computación. Fuera de los Estados Unidos, las leyes son muy diversas. En julio de 2001 entró en vigor una directiva de la Comisión Europea para los quince Estados

miembros de la Unión Europea, mediante la cual las firmas digitales son jurídicamente vinculantes para la firma de contratos, tanto como lo son las firmas escritas a mano.
P: ¿Los cortafuegos están a la prueba de fallas y son un método seguro y abarcador?
R: No existe ningún método de seguridad a prueba de fallas y abarcador; el único plan de seguridad efectivo es el que utiliza capas múltiples de seguridad. Un cortafuego es una parte importante de ese plan. Brinda protección al nivel del perímetro de la red, pero los cortafuegos no protegen frente a muchos tipos de violaciones de seguridad, como las violaciones internas, violaciones físicas, o intrusiones causadas por el comprometimiento de las contraseñas de usuario. En el sitio de preguntas sobre cortafuegos (www.faqs.org/faqs/firewalls.faq) se señala que muchas organizaciones activan un cortafuegos en la red y piensan que están protegidas, cuando en realidad existen numerosas otros vulnerabilidades (como módems de conexión telefónica en computadoras individuales) lo cual se asemeja a una persona que tiene una puerta de acero de seis pies de grosor instalada en una casa de madera con las ventanas sin cerrojo. Los cortafuegos tampoco protegen mucho frente a los virus y los troyanos. Por otra parte, los mejores cortafuegos sí permiten un filtrado muy granular de los datos de entrada y salida en diferentes niveles, sobre la base de las necesidades de la organización. Cada red comercial (y las computadoras caseras conectadas a Internet) deben tener algún tipo de cortafuegos. Los productos cortafuegos van desde dispositivos de hardware patentados que cuestan miles de dólares o cortafuegos de software que cuestan ciento de dólares, hasta productos simples freeware o shareware apropiados para el uso en el hogar. Windows XP incluso tiene un cortafuego incorporado, si bien es simple y no se debe depender de él para proteger sistemas vitales.

RECURSOS

- Cyber Angel (Computer Sentry Software)
  www.sentryinc.com
- Body Check: *Biometric Access Protection Devices and Their Programs Put to the Test*
  www.heise.de/ct/english/02/11/114
- The Register: *Gummi Bears Defeat Fingerprint Sensors*, por John Leyden
  http://theregister.co.uk/content/55/25300.html
- ISO 17799 Security Standard
  www.iso17799-web.com
- COBRA Risk Consultant (evaluation version)
  www.ca-systems.zetnet.co.uk/cobdown.htm
- Health Insurance Portability and Accountability Act (HIPAA) standards
  www.smed.com/hipaa/overview-fastfacts.php
- RUSecure Information Security Policies
  www.information-security-policies.com/index.htm
- SANS Institute Security Policy Project
  www.sans.org/newlook/resources/policies/policies.htm
- *Kerberos v5 System Administrator's Guide*
  www.Ins.cornell.edu/public/COMP/krb5/admin/admin_2.html
- SANS Institute: *Layered Suthentication*, por Jeff Parker
  http://rr.sans,org/authentic/layered.php
- *A Short History of Cryptography*, por Fred Cohen
  www.all.net/books/ip/Chap2-1.html
- *A Cryptographic Compendium*
  http://pardus-larus.student.utwente.nl/librarilo/texts/computers/crypto
- *Protection of Your Secret Key: How Secure Is PGP?*, por Ralf Senderek
  http://senderek.de/security/secret-key.protection.html#summary

CAPITULO 8

PUESTA EN PRÁCTICA DE LA SEGURIDAD DE SISTEMAS

Temas que se analizan en este capítulo:

- Aplicación de medidas de seguridad de banda ancha
- Aplicación de la seguridad de buscadores
- Aplicación de la seguridad de servidores web
- Para comprender la seguridad y los SOs de Microsoft
- Para comprender la seguridad y los SOs UNIX/Linux
- Para comprender la seguridad y los SOs Macintosh
- Para comprender la seguridad de las macrocomputadoras o “mainframe”
- Para comprender la seguridad inalámbrica

- Resumen
- Preguntas frecuentes
- Recursos

Introducción

En capítulos anteriores definimos el delito informático y analizamos quiénes son las personas que lo cometen; asimismo, hablamos de los conceptos básicos de las computadoras y el trabajo en red que son esenciales para comprender los delitos informáticos técnicamente sofisticados. Posteriormente, hablamos de los distintos tipos de intrusiones y ataques en la red, y de los conceptos básicos de seguridad de computadoras y redes. La seguridad es la clave para prevenir –o, en caso no poder hacerlo, detectar– la actividad criminal en las redes.

El delito informático es posible porque las computadores y redes no están debidamente aseguradas. Los oficiales encargados de hacer cumplir la ley saben que la mayoría de los delincuentes buscan las presas fáciles, es decir, los carteristas buscan personas que no guardan bien sus carteras o monederos, y los ladrones atacan las viviendas y los comercios donde no se han tomado las medidas de seguridad necesarias. No es de sorprender que los delincuentes informáticos hagan lo mismo. La mayoría de los ataques contra sistemas de computadoras y redes explotan vulnerabilidades bien conocidas –vulnerabilidad que, en muchos casos, pueden ser corregidas con una simple revisión (patch) o cambio de configuración. A menudo, no cuesta nada aplicar estas simples medidas de seguridad. No obstante, los usuarios de computadoras y los administradores de red son tan descuidados en la protección de sus datos de valor como la mayoría de los ciudadanos lo son para proteger su propiedad personal. El hecho de que estos conocidos ataque aún funcionen la mayoría de las veces es un ejemplo de que la mayoría de las personas y empresas no tienen la debida diligencia para proteger sus valores informáticos antes de conectarse a Internet.

Existen muchas razones para este comportamiento, entre ellas:

- El usuario promedio en el ámbito de la computación desconoce los temas de seguridad.
- Falta de tiempo de los profesionales de la red (el síndrome de "realmente tenía pensado trabajar en eso").
- Negación psicológica que lleva a las personas conscientes del riesgo a pensar que aunque tales cosas suceden, "no me puede pasar a mi".

Por supuesto, ninguna de estas razones es suficientemente buena para justificar la posible pérdida a manos de un delincuente informático, y esta realidad nos llega con una venganza después de que la red y sus datos se han visto comprometidos. Es importante comprender que no solamente son las personas ingenuas ni los pequeños negocios con escaso presupuesto los que descuidan sus necesidades de seguridad. Desafortunadamente, la mayoría de las empresas son como las agencias policiales que "no pueden darse el lujo" de adquirir chalecos antibalas para sus oficiales hasta que uno de ellos muere en un tiroteo. La naturaleza humana es tal que a veces es necesario que suceda una tragedia para que las personas responsables se sientan motivadas a tomar alguna medida.

¿Cómo pueden estar seguros los sistemas?

La seguridad de sistemas no es una cosa; es un proceso --el proceso de construir una barrera entre la red y aquellos que pudieran dañarla. La clave está en hacer que su barrera sea cada vez más difícil de cruzar que las demás. En otras palabras, la seguridad informática significa crear una disuasión para convencer a un posible intruso o atacante de que su sistema es más difícil de violar que el de alguna otra persona. No obstante, en caso de que un atacante desee específicamente violar su perímetro de seguridad, será capaz de hacerlo si tiene suficiente tiempo.

Los oficiales a cargo de la prevención del delito dicen a los vecinos en las reuniones que sostienen sobre vigilancia en los barrios, que no existen formas para lograr que las viviendas estén totalmente a salvo de los ladrones. Ningún cerrojo impedirá la entrada a quien esté decidido a entrar; sin embargo, si lograrán retrasar su entrada. Si usted dificulta de manera suficiente la entrada, un ladrón normal buscaría otra víctima, a la que fuera más fácil y más rápido atacar. De la misma manera, ninguna computadora y ninguna red puede estar 100% segura a menos que esté desconectada de toda interfaz de comunicación y totalmente apagada --y por supuesto, ese sistema plenamente seguro es también totalmente inútil para el usuario. Lo que sí pueden hacer los métodos de seguridad de sistemas es elevar el nivel de dificultad de entrada hasta el punto en el que la mayoría de los posibles intrusos se irían a atacar a otra parte, especialmente dado que no hay escasez de redes fáciles de violentar.

NOTA

Comprender que la seguridad informática no puede ser 100% efectiva debería hacerle concentrar sus esfuerzos en establecer el mejor plan de seguridad posible, más que desperdiciar tiempo y dinero en buscar la solución de seguridad "perfecta".

La mentalidad de seguridad

Stuart McClure y Joel Scambray, autores de la columna semanal *Security Watch* de *InforWorld Magazine*, han señalado que "La seguridad no es un objetivo, es un proceso; la seguridad no es un producto, es una mentalidad". Esta frase resume el estado mental necesario para practicar la seguridad.

Si ampliamos un poquito esta filosofía, podríamos decir mucho más: la seguridad no es algo que uno pueda instalar después de haberlo comprado, ni tampoco es algo que se puede alcanzar o concluir en algún momento. La seguridad es un proceder permanente que tiene que ver con una continua mejoría, perfeccionamiento y ajuste de los sistemas para protegerlos frente a nuevas vulnerabilidades y ataques. No se puede ver la seguridad como una característica limitada a las computadoras; la seguridad debe ser una solución integral. Para que su empresa esté segura, hay que abordarlo todo: computadoras, dispositivos de red, medios de conectividad, dispositivos de perímetro, dispositivo de comunicaciones, sistemas operativos, aplicaciones, servicios, protocolos, personas, acceso físico y las relaciones entre todos estos componentes.

Un buen especialista de seguridad de redes tiene al menos una característica en común con un buen oficial de un órgano de aplicación de la ley: ambos son, por naturaleza, desconfiados, a veces hasta llegar a ser casi paranoicos. Ambos apoyan la filosofía de que es mejor estar seguros que lamentarse. Un profesional de redes consciente de la necesidad de tener seguridad ve en cada vulnerabilidad un posible

ataque. Esto pudiera resultar molesto para otros usuarios de la red, tanto como la insistencia de un oficial policial de tener buena visibilidad de la puerta desde donde esté sentado podría ser molesto para sus amigos y familiares civiles. Sin embargo, tener en cuenta cualquier posible amenaza es parte del trabajo –de ambos trabajos. Después de todo, que usted esté paranoico no quiere decir que no haya quien desee atacarlo a usted –

En la escena...
Creando una mentalidad defensiva
Al inicio de su entrenamiento, la mayoría de los oficiales encargados de hacer cumplir la ley se familiarizan con los códigos de colores que identifican los diferentes estados mentales de la condición de alerta. Este sistema de colores por lo general se atribuye al Coronel Jeff Cooper, legendario experto en armas de fuego y defensa personal, y se utiliza para representar las "condiciones" mentales de la siguiente manera:

Estado Blanco: describe la mentalidad de la mayoría de las personas en su vida diaria, despreocupadas de los posibles peligros y concentradas en sus propios pensamientos y actividades.

Estado Amarillo: describe la mentalidad óptima para la autoprotección en condiciones normales --relajado pero alerta y en busca de síntomas de un posible peligro.

Estado Naranja: describe la mentalidad que debe tener una persona cuando existe algún peligro conocido (por ejemplo, cuando se camina por una calle en la noche en una zona de alta criminalidad), constantemente a la búsqueda de posibles peligros y listos para pasar a un estado superior si fuera necesario.

Estado Rojo: describe la mentalidad de una persona que se enfrenta a una amenaza; en esta condición, el cuerpo experimenta un alza súbita de adrenalina y la personas reacciona, por lo general, de una de estas dos formas: combate o huye.

Podemos tomar prestados estos códigos para describir el estado de nuestra seguridad de redes. Desafortunadamente, demasiadas redes funcionan en el Estado Blanco, y sus administradores y usuarios no prestan atención a las muchas amenazas que existen. Para nuestros propósitos, el Estado Amarillo quizá no sea suficiente para proteger adecuadamente los sistemas y redes de computación; toda la red que esté conectada a Internet se debe considerar ubicada en una zona de alta criminalidad. Por ello, los profesionales de seguridad de redes deben permanecer siempre en el Estado Naranja, un estado de alerta elevada, constantemente a la búsqueda de amenazas y listos para responder cuando ocurran intrusiones o ataques.

¡o a su información!

Elementos de seguridad de sistemas
La seguridad de sistemas es mucho más que sólo mantener a raya a los usuarios mal intencionados y evitar ataques. También se trata de mantener y brindar acceso a los recursos por parte de los usuarios autorizados, y de mantener la integridad de los datos y la infraestructura. Estos elementos relacionados pero independientes de la seguridad de sistemas se describen utilizando cuatro términos: autenticación, confidencialidad, integridad y disponibilidad. Si los administradores de redes no gestionan adecuadamente alguno de estos elementos, no lograrán brindar seguridad a la infraestructura informática.

Para diseñar, desplegar y mantener con éxito la seguridad se necesita un amplio conocimiento que siempre debe estar en expansión. Sería imposible en este libro brindar todos los detalles para cerrar siquiera un solo sistema operativo, mucho menos toda la infraestructura informática de una pequeña empresa. No obstante, podemos hacer hincapié en algunos de los grandes temas a que hacemos frente en nuestros esfuerzos de seguridad y mostrarles nuevos recursos que abordan cada uno de estos tópicos en mucho más detalle.

En este capítulo, analizamos los siguientes temas de seguridad.

- ¿Cómo aplicar la seguridad en las conexiones de banda ancha?
- ¿Cómo aplicar y mantener la seguridad de los buscadores web?
- Problemas especiales en la seguridad de un servidor web
- Reseña de cómo brindar seguridad a los sistemas operativos Microsoft
- Reseña de cómo brindar seguridad a los sistemas operativos UNIX/Linux
- Reseña de cómo brindar seguridad a los sistemas operativos Macintosh
- Reseña de cómo brindar seguridad a los sistemas de las macrocomputadoras
- Importancia y retos de la gestión de la seguridad de dispositivos inalámbricos

Aplicación de medidas de seguridad de banda ancha

Banda ancha es una de las palabras de moda en la conectividad a Internet actualmente. Las tecnologías de banda ancha han posibilitado que los usuarios residenciales y las redes de pequeñas oficinas obtengan tasas razonablemente altas de transferencia de datos a un costo relativamente bajo. Las conexiones de alta velocidad ya no están limitadas a las empresas con grandes recursos. La amplia disponibilidad y puesta en práctica de la conectividad de banda ancha ha llevado al menos al 10% de la comunidad en línea de Estados Unidos y al 22% de la canadiense a las vías rápidas de Internet, según la publicación *Cable Datacom News* (marzo de 2002). A medida que más usuarios obtienen acceso a un ancho de banda mayor, los sitios web les pueden ofrecer más recursos, más contenido multimedia y mayor volumen de lo que era posible con las conexiones más lentas a través de módems. No obstante, ha surgido una gran confusión, incluso entre los profesionales de la informática, sobre qué realmente es banda ancha. A veces se utiliza el término para hacer referencia a cualquier conexión de alta velocidad, pero su significado técnico es específico. *Banda ancha* se refiere a una tecnología de conexión que utiliza múltiples frecuencias en un medio común de trabajo en red (como el cable coaxial que se utiliza para la televisión por cable, o CATV) para explotar todo el ancho de banda disponible. Esto permite que los datos sean multiplexados para que puedan viajar a frecuencias (o canales) diferentes simultáneamente y se pueda transmitir mayor cantidad de datos en un período específico de tiempo que con una tecnología de banda de base (un canal) como Ethernet. El término *broadband* (banda ancha) se sustituye a veces por *wideband* (N. del T., que significa lo mismo en español).

NOTA

Además de banda ancha (*broadband*) y banda de base (*baseband*), escucharemos el término banda estrecha (*narrowband*). Este término se utiliza a menudo para hacer referencia a tecnologías que transportan solo comunicaciones de voz. En las radiocomunicaciones, la banda estrecha se refiere a un rango de frecuencia entre 50cps y

64kbps asignadas por la Comisión Federal de Comunicaciones (FCC) para los servicios de megafonía y de radio móviles.

Entre los factores que afectan la capacidad de transmisión de datos de un medio de comunicación están el rango de frecuencia y la *calidad* (o proporción señal-ruido) de la conexión. Un canal único tiene una capacidad fija dentro de esos parámetros, perola capacidad puede aumentarse incrementando el número de canales de comunicación. Así es como funciona la banda ancha.

Los módems de cable brindan la forma más común de conectividad de banda ancha a Internet. De hecho, el cable tiene muchas ventajas como tecnología Internet. Las compañías de cable tienen amplias infraestructuras de red para la transmisión de programas de televisión. Dado que es una tecnología de banda ancha, es posible enviar señales de datos computacionales por el cable en su propia frecuencia, de la misma forma que la señal de cada canal de televisión viaja por su propia frecuencia. La Internet por cable típicamente ofrece velocidades que van desde 500kbps hasta 1,5 Mbps (aproximadamente equivalente a T-1, a precios al menos 10 veces inferiores), y la tecnología es capaz de alcanzar velocidades muy superiores, de hasta 10Mbps o más.

A pesar de sus ventajas, el cable tiene algunas desventajas significativas, incluidas las siguientes:

- Las líneas de algunas compañías de cable pueden realizar transmisiones únicamente en una dirección (que, después de todo, es todo lo que se necesita para transmitir un programa de televisión). En este caso, los usuarios deben enviar los mensajes mediante una línea telefónica analógica regular; solamente los datos descendentes pueden viajar por el cable. Afortunadamente, la mayoría de las compañías de cable han mejorado sus infraestructuras para soportar transmisiones en doble dirección.
- Incluso con el cable bidireccional, muchas compañías de cable reducen a 128 kbps el ancho de banda para datos ascendentes. Ello tiene el objetivo de impedir que los usuarios operen servidores de Internet (lo cual está también prohibido en los acuerdo de condiciones de servicio de los suscriptores).
- Otra desventaja, en algunas zonas, es la fiabilidad. La red de cable puede "caerse" en muchas ocasiones, lo que deja a los usuarios sin conectividad a Internet. A diferencia de las soluciones comerciales costosas como las líneas rentadas, no existe garantía de tiempo de habilitación **(**ni tampoco garantía de ancho de banda) en un contrato de cable típico para el acceso a Internet.
- Quizás la desventaja más seria sea el hecho de que el cable es una tecnología de "ancho de banda compartido" . Esto quiere decir que todos los suscriptores en una zona inmediata comparten el mismo medio de conexión. En otras palabras, todas las personas de un vecindario están conectadas a la misma subred y por lo tanto tienen el potencial de convertirse en una amenaza a la seguridad para cualquier otro sistema en el vecindario. Esta es la principal debilidad de la tecnología de Internet por cable. Debemos recordar que para poder atacar una computadora debemos estar conectados a ella. Estar conectados al mismo medio de red facilita --incluso algunos dirían que permite-- el tráfico de comunicaciones maliciosas entre esas computadoras.

La tecnología DSL (por Digital Suscriber Line) brinda conectividad de Internet de banda ancha por las líneas telefónicas. La DSL asimétrica (ADSL), la forma de DSL de mayor accesibilidad, utiliza una técnica de codificación de señales llamada *multitono discreto* que divide en 256 canales un par de alambres de cobre de una línea telefónica ordinaria. Con esta técnica es posible transmitir datos a 8Mbps --pero solamente a una distancia relativamente corta, debido a la atenuación. Las frecuencias utilizadas están por encima de la banda de fonía; ello quiere decir que tanto las señales de voz como las de datos viajan por la misma línea telefónica a la misma vez.

NOTA

Para más información sobre el funcionamiento de la tecnología DSL, véase www.howstuffworks.com/dsl.htm

Otra tecnología de banda ancha que utiliza las líneas telefónicas es Broadband Integrated Services Digital Network (B-ISDN). No obstante, estas son líneas telefónicas de fibra óptica en lugar de cables de cobre. La B-ISDN permite velocidades de transmisión de datos de hasta 1,5 Mbps. La tecnología ISDN original estuvo destinada inicialmente a sustituir las líneas de fonía analógica por líneas digitales, que son más fiables y menos vulnerables al ruido (interferencia). Existen dos tipos de servicio ISDN: el BRI (Basic Rate Interface, o Interfaz de Tasa Básica) y el PRI (Primary Rate Interface, o Interfaz de Tasa Primaria). El BRI es mayormente utilizado por consumidores y pequeños negocios. Brinda dos canales (llamados *canales B* o *canales portadores*) por los cuales se puede transmitir voz o datos a 64 Kbps. Estos dos canales se pueden utilizar por separado de manera que sea posible conectarse a Internet a 64 Kbps y utilizar la otra línea al propio tiempo para llamadas de voz, o se pueden agregar ambos para elevar la tasa de transmisión de 128K. Otro canal, denominado *canal D* o *canal de datos*, tiene una velocidad de 16 Kbps y gestiona las señales. El PRI es mucho más costoso que el BRI pero brinda un ancho de banda mayor: 23 canales B de 64 Kbps más un canal D de 64 Kbps, para una capacidad total de 1,5 Mbps (esto se aplica a Estados Unidos; en Europa, el PRI brinda 1,98 Mbps).

Las conexiones DSL e ISDN no son conexiones compartidas, sino que el medio de conexión es utilizado solamente por los dos extremos de la conexión. Dado que en estas conexiones solamente hay dos partes, constituyen un medio de comunicación más seguro que los módems de cable. Aquellos para quienes la seguridad es importante –y deberían ser todas las personas que utilizan Internet– deberían optar por una opción de conectividad no compartida si la tienen disponible y asequible. Las tecnologías de Internet por satélite pueden brindar un acceso constante a velocidades de hasta 500Kbps en zonas donde no están disponibles ni el DSL ni el cable. El satélite está disponible en casi todas partes, siempre que se cuente con una vista del cielo sin obstrucción a la zona donde está ubicado el satélite. (Ello es necesario porque el satélite es una tecnología de "línea de visión"). Los satélites de primera generación son una tecnología unidireccional, como los primeros servicios de módem por cable, pero ya la situación ha cambiado. *Starband* se ha asociado con *Echostar* y Microsoft para brindar acceso satelital bidireccional y *DirectPC* de *Hughes Networks* brinda ahora servicios bidireccionales con sus sistemas *Direct Way*.

Temas de seguridad de la banda ancha

Los beneficios de la conectividad de banda ancha de alta velocidad se complican por problemas y vulnerabilidades propias de la banda ancha. Estos temas surgieron directamente de la aplicación de la banda ancha y no eran amenazas palpables para la comunidad que utilizaba módems de conexión telefónica. Una amenaza es el hecho de que la banda ancha siempre está conectada. Los usuarios ya no tienen que iniciar manualmente una conexión cuando desean navegar en la web o acceder al correo electrónico, ya que las conexiones de banda ancha siempre están activadas. En el pasado, los usuarios de módems se desconectaban de Internet una vez concluidas sus sesiones en línea. Con ello desvinculaba sus computadoras de Internet e impedían que los intrusos accedieran a sus sistemas o los atacaran. Como las conexiones de banda ancha están activas permanentemente y se reconectan automáticamente cuando se interrumpen, las computadoras están propensas a ser atacadas también permanentemente.

Otro aspecto de este tema de la conexión ininterrumpida es la dirección IP asignada al sistema. Con la conectividad por módems de conexión telefónica, las computadoras usualmente se configuran para utilizar el protocolo DHCP (Dynamic Host Configuration Protocol, o protocolo de configuración de host dinámico) para obtener su dirección y se les asigna una dirección IP diferente cada vez que establecen comunicación. Así, una PC conectada por módem tendrá hoy una dirección y normalmente tendrá otra distinta mañana, y la que utilizó ayer será asignada hoy a un sistema diferente. Esto dificulta el rastreo de sistemas individuales. No obstante, con la conectividad de banda ancha, a los sistemas por lo general se les asigna una dirección IP dedicada o son capaces de renovar continuamente sus direcciones IP asignadas por el DHCP, de manera que sus identificadores en línea permanecen iguales por un período prolongado (cuando no indefinidamente). Esto facilita en extremo el rastreo de un sistema específico.

Los oficiales encargados de hacer cumplir la ley pueden entender fácilmente el efecto que causan la detección y la captura; muchos delincuentes tradicionales (especialmente los artistas del *scam* o mensajes de correo electrónico no solicitados) siempre están en movimiento, viviendo en hoteles o con amigos y cambiando de dirección cada varias semanas o meses. Estos delincuentes son mucho más difíciles de rastrear que los que han establecido una residencia permanente y una dirección fija. Lo mismo sucede con los delincuentes informáticos. Los que utilizan direcciones IP invariables son más fáciles de encontrar que aquellos cuya dirección cambia constantemente. Si bien existen formas para que los delincuentes con conocimientos técnicos disfracen sus direcciones IP, el advenimiento de la banda ancha, con una mayor probabilidad de direcciones invariables, facilita el trabajo de los investigadores frente a los delincuentes informáticos menos conocedores de la tecnología.

Por otra parte, mientras más tiempo permanezca en línea un sistema, especialmente cuando mantiene su dirección IP, mayor será su vulnerabilidad a los ataques. Cuando se dispone de tiempo suficiente siempre es posible violar un sistema, incluso aunque los administradores conscientes de la necesidad de tener seguridad hayan tomado las precauciones normales, como la instalación de cortafuegos, la instalación de revisiones, y la asignación de contraseñas robustas. Recordemos que la seguridad es una disuasión, no una barrera impenetrable. Con suficiente tiempo y decisión, es posible violar cualquier medida de seguridad.

Apagar sencillamente la computadora cuando no se está utilizando no es suficiente para protegerse de los ataques. Mediante la potencia de la automatización, los atacantes pueden rastrear continuamente una dirección IP para determinar cuando la computadora está encendida o apagada. Es cierto que es posible impedir que el ataque continúe mientras la computadora esté apagada, pero ese ataque puede reiniciarse a partir del punto en que se interrumpió una vez que el sistema vuelva a encenderse. En lugar de depender de la "seguridad por medio de la oscuridad" (tratar de esconder la existencia de un sistema o de sus datos de los ojos de un atacante), usted puede tomar numerosas medidas proactivas para reducir su vulnerabilidad a los ataques específicos en la banda ancha. En la próxima sección analizamos esas medidas.

Podría parecer extraño, pero otra deficiencia en la seguridad de la banda ancha es la velocidad a la cual fluyen los datos. En primer lugar, esta velocidad permite que se realice un ataque más rápidamente contra sus sistemas. Un usuario malintencionado puede enviar una cantidad de datos significativamente mayor a su sistema mediante una conexión de banda ancha que por medio de una conexión telefónica por módem. En segundo lugar, una vez que su sistema esté comprometido, el atacante necesitará menos tiempo para bajar y subir archivos.

Evidentemente la conectividad de banda ancha tiene sus puntos en contra. Para muchos usuarios de la Internet constituye una promesa irresistible de conectividad a la velocidad de la luz y a un costo muy bajo. Es importante reconocer primero que existe un problema para después tomar medidas específicas para reducir el riesgo, de manera que en esta sección no solamente señalamos las deficiencias sino que brindamos una guía para reducir los riesgos asociados al uso de la conectividad de banda ancha.

Cuando se aplican estrategias para reducir el riesgo como es mejorar la seguridad, se debe tener en cuenta la configuración específica de hardware y software de cada computadora. Ello incluye el sistema operativo que utiliza, las aplicaciones instaladas y los servicios utilizados en la computadora conectada. Aplicar precauciones de seguridad en un aspecto de su sistema solamente, no le brinda una seguridad adecuada. Deberá usted poner en práctica una solución de seguridad multicapas a fin de que existan numerosas barreras para detener el acceso no autorizado.

NOTA

En el capítulo 7, “Cómo prevenir el delito informático" analizamos el concepto de seguridad multicapas.

Cuando una compañía de gran tamaño contrata con un ISP una conexión de ancho de banda de alta velocidad probablemente el tema de la seguridad sea el aspecto más importante del contrato de servicios. Sin embargo, los clientes individuales (y muchos negocios de pequeño tamaño) que contratan conexiones de banda ancha de bajo costo a menudo pasan por alto el tema de la seguridad. Esto se debe principalmente a que pocos individuos o empleados de pequeñas compañías son profesionales capacitados en temas de seguridad, y sencillamente no pueden hacer otra cosa. Incluso si tienen una idea vaga de lo que son los riesgos de seguridad que deben tratar de resolver, podrían estar abrumados por la complejidad del tema y el gran número de "soluciones" diferentes que existen, así como por el alto costo que entraña poner en práctica muchas de esas soluciones recomendadas. La promesa de tener acceso a descargas rápidas desde Internet

por un costo bajo hace que muchos usuarios no presten atención a otros temas importantes, como la seguridad y la privacidad, que deben ser tenidos muy en cuenta antes de desplegar la banda ancha.

En las secciones siguientes, analizamos estrategias específicas de reducción del riesgo que se pueden emplear a fin de elevar la seguridad de su computadora o red que utiliza conectividad de banda ancha. Las personas y compañías que utilizan la banda ancha deben también tener en cuenta los temas planteados más adelante en este capítulo cuando analizamos la forma de brindar seguridad a sistemas operativos específicos.

Despliegue de software antivirus

La seguridad tiene muchas facetas, entre ellas la necesidad de impedir el acceso *no autorizado* y la necesidad de soportar el acceso *autorizado*. Con demasiada frecuencia la prevención de ataques va en detrimento de la garantía del acceso a los datos por parte de los usuarios válidos. Es importante mantener una perspectiva equilibrada cuando se aplican medidas de seguridad. Pensemos en la seguridad en términos del famoso lema de la policía, "Proteger y servir". Si esas medidas de seguridad no respaldan adecuadamente alguno de estos elementos --proteger sus datos y servir a sus usuarios autorizados-- no habrá usted logrado aplicar un plan de seguridad verdaderamente efectivo.

En la escena...

Cómo una elevada seguridad se puede convertir en un alto riesgo

Paradójicamente, las políticas de seguridad excesivamente restrictivas pueden traer como consecuencia una reducción del nivel de seguridad (a la vez que crear un falso sentido de que se tiene una seguridad elevada) porque los empleados frustrados buscarán la forma de burlar las medidas de seguridad, de manera intencional o no. Los entusiastas de la seguridad que llegan y "cierran herméticamente" una red sin tener en cuenta las necesidades de los usuarios, a la larga pueden hacer más daño que provecho, a pesar de sus buenas intenciones.

El ejemplo más sencillo es la imposición de una política que requiera que los empleados utilicen contraseñas de 20 caracteres generadas al azar y que cambian todas las semanas. Como no pueden recordar esas contraseñas, es mucho más probable que los empleados decidan anotarlas (incluso cuando ello entrañe una violación de la política), lo cual no sería el caso si los propios empleados escogen sus contraseñas de manera que estas tengan un significado para ellos que los ayude a recordarlas. Anotar las contraseñas (especialmente debido a que las personas tienden a dejar esa pequeña nota cerca de la computadora para su propia conveniencia) representa un riesgo de seguridad mucho mayor que la posibilidad de que las contraseñas seleccionada por los usuarios puedan ser más fáciles de burlar. Una solución de avenencia en este caso es permitir que los usuarios seleccionen sus propias contraseñas, al tiempo que se establecen políticas (que pueden aplicarse mediante el uso de software apropiados) que requieran que las contraseñas de usuario cumplan requisitos de extensión y complejidad mínimas -- por ejemplo, estipular que se incluyan caracteres alfa y numéricos, y que las contraseñas tengan al menos ocho caracteres.

Esto constituye un reto porque la seguridad y la disponibilidad siempre estarán en los extremos opuestos de la ecuación. Mientras más se tenga de una, menos habrá de la otra. No obstante, se debe lograr un equilibrio, porque la política de seguridad que sea demasiado restrictiva podría tener el mismo resultado que una que fuera demasiado distendida -- es decir, un impacto negativo (quizás incluso catastrófico) en la compañía. Mantener la integridad de los datos de manera que pueda ser útil a los usuarios autorizados es tan importante como impedir que sea robados por alguien no deseado del exterior. Muchas son las cosas que pueden amenazar la integridad de sus datos, incluidos el error humano, empleados despechados e incluso fallos de hardware. Pero la amenaza más grave, prevalente e inminente es la corrupción, destrucción o alteración de los datos por una infección de virus. Una conexión de banda ancha tiene tantas probabilidades como una LAN o una conexión telefónica de ser una entrada para una infección de virus. No importa el tipo de conexión que tenga su computadora a Internet u otros sistemas, deberá usted protegerla de los virus.

Según un estudio realizado por Message Labs (www.messagelabs.com) el ritmo de propagación de los virus mediante el correo electrónico está elevándose exponencialmente. Los informes generados a partir de datos recopilados indican que en 1999 se detectaba un virus en correos electrónicos por hora. En el año 2000, la tasa de detección se elevó a uno cada tres minutos. En el 2001, se detectaban un virus cada 30 segundos. Para mediados de 2002, esta tasa se había acelerado a un virus cada diez segundos. Y ese ritmo continúa en aumento.

Cuando nos esforzamos para proteger la integridad de nuestros datos, la mejor inversión será instalar un software antivirus fiable. A la hora de seleccionar ese producto debemos tener en cuenta lo siguiente:

- El producto debe proceder de una compañía conocida y de reputación.
- El producto debe actualizar automáticamente sus definiciones de virus.
- El producto debe escanear lo archivos almacenados, la memoria (RAM), los medios extraíbles, el correo electrónico y los datos transmitidos por la web.
- El producto deberá limpiar o poner en cuarentena los archivos infectados que detecte.

Siempre que sea posible, instale en la red dos o más soluciones antivirus para que funcionen como sistemas por capas. No obstante, no instale dos herramientas antivirus en la misma computadora, porque hacerlo a menudo hace que el sistema colapse o se comporte de manera errática. Muchas organizaciones optan por poner un producto antivirus en cada sistema perimétrico (cortafuegos, gateway, proxy, etc.), en cada servidor y en cada cliente. Este enfoque multicapas brinda una protección mucho más amplia y elimina los problemas que pueda representar depender de la solución que brinda un único proveedor.

Valladares contra el delito…
Correo electrónico ciento por ciento libre de virus
El correo electrónico es el mecanismo número uno para la propagación de virus en la actualidad, por lo que es esencial mantener la mayor cantidad posible de mensajes maliciosos de correo electrónico fuera de su red. Con el aumento de la dependencia en el correo electrónico para las comunicaciones comerciales y privadas, el equilibrio entre la seguridad y la disponibilidad puede dificultarse especialmente en lo que se refiere al correo electrónico.
Algunas compañías brindan soluciones a este problema. Por ejemplo, Message Labs brinda un servicio que garantiza que sus servidores reciban mensajes de correo electrónico ciento por ciento libres de virus. Esta garantía se basa en la capacidad de Message Labs de revisar adecuadamente los mensajes electrónicos en busca de una posible infección por virus o agente portador. Esta tarea se logra enrutando los mensajes de correo electrónico de entrada a uno de los sistemas de torre de control de la compañía. Allí se inspeccionara cada mensaje con al menos tres soluciones antivirus procedentes de proveedores fiables, así como mediante una herramienta de búsqueda de inteligencia artificial que se sustenta en la heurística, la comparación de patrones, la comparación de firmas, y el análisis del flujo de tráfico para detectar amenazas de virus desconocidos. Después de una demora de alrededor de 1,5 segundos, su mensaje de correo electrónico es enviado a sus servidores internos de correo electrónico para que sea distribuido en su red. Message Labs tiene una excelente historial de promesas cumplidas. Para más información, visite el sitio de la empresa en www.messagelabs.com.

NOTA

En el capítulo 6, "Para comprender las intrusiones y ataques a la red", analizamos los virus, los troyanos y otros códigos malignos, y brindamos información más detallada sobre cómo proteger los sistemas de estas amenazas.

Definición de contraseñas de usuario robustas
Se necesita solamente dos elementos para tener acceso a los sistemas de la mayoría de las computadoras: la identidad de usuario (nombre de usuario) y la contraseña asociada a este. La mayoría de los nombres de usuario son evidentes o son fáciles de adivinar --el nombre de pila de una persona, la primera inicial y el apellido, o cosas por el estilo-- por lo tanto no son confidenciales. De manera que la autorización de acceso probablemente se base únicamente en la contraseña. Las contraseñas deben ser muy robustas y deben mantenerse seguras para tener el control del acceso. Esto es así cuando su sistema está conectado a una conexión de banda ancha, un cable de LAN o un vínculo de conexión telefónica. Sin embargo, debido a que las conexiones de banda ancha siempre están habilitadas, brindan a un posible intruso mucho más tiempo que una conexión telefónica para realizar su ataque (que es esencialmente un método de prueba constante donde se intentan varias combinaciones de caracteres hasta llegar a la que funciona).

En el capítulo 7 titulado “Cómo prevenir el delito informático", analizamos en detalle cómo crear contraseñas robustas difíciles de burlar y cómo establecer y hacer cumplir política de contraseñas para garantizar que ninguna de las que se utiliza en su organización constituya una vía de entrada fácil para los intrusos.

Establecer permisos de acceso

Controlar el acceso es un elemento importante para mantener la seguridad del sistema. Los ambientes más seguros siguen el principio de “menos privilegiado”. Este principio plantea que a los usuarios se le concede el menor grado de acceso posible que le permita realizar las tareas a ellos asignadas. Las ampliaciones de ese acceso son analizadas cuidadosamente antes de ser llevada a la práctica. Los oficiales encargados de hacer cumplir la ley están familiarizados con este principio en lo que se refiere a la información no computadorizada; este concepto usualmente se conoce como *saber cuando sea necesario*. Por lo general, seguir este principio hace que los administradores de redes reciban más quejas de los usuarios de que no pueden acceder a los recursos. Sin embargo, escuchar quejas de los usuarios autorizados es mejor que escuchar sobre violaciones de acceso que dañan la rentabilidad de una empresa o su capacidad comercial.

En la práctica, mantener el principio de “menos privilegiado” afecta directamente el nivel de gastos generales administrativos, gerenciales y de control, elevando los niveles necesarios para aplicar y mantener ese ambiente. Una alternativa --los grupos de usuarios-- logra ahorrar mucho tiempo pero también invita a que los administradores sean perezosos. En lugar de asignar controles de acceso individuales, los grupos de usuarios similares son asignados el mismo acceso. En los casos en que todos los usuarios del grupo tienen exactamente las mismas necesidades de acceso, el método funciona. Sin embargo, en muchos casos, algunos usuarios individuales necesitan más o menos acceso que el resto de los miembros del grupo. Desafortunadamente, en el pasado los proveedores de sistemas operativos como Microsoft y Novell han aconsejado que los administradores siempre asignen permisos a los grupos en lugar de a cuentas de usuario individuales. Sin embargo, cuando la seguridad es importante, el esfuerzo adicional para perfeccionar el acceso de usuarios individuales brinda un mayor control sobre aquello a que pueden o no acceder los usuarios.

Mantener el acceso de usuarios individuales lo más específico posible limita la amenaza de que una cuenta de usuario comprometida facilite el acceso no restringido a un intruso. No evita que se comprometan las cuentas con mayores privilegios, como la de administradores o de los operadores de servicios específicos. No obstante, sí obliga a los intrusos a concentrar sus esfuerzos en esas cuentas con mayores privilegios, en las que por lo general se tienen contraseñas más robustas y se realizan controles de cuenta más regulares.

En el capítulo 7 analizamos más detalladamente cómo se establecen y aplican las políticas de acceso.

Deshabilitar la función de archivos e impresoras compartidas

La capacidad de compartir archivos e impresoras con otros miembros de la red puede facilitar muchas tareas y, de hecho, este fue el objetivo original para enlazar en redes las computadoras. No obstante, esta capacidad también tiene su lado oscuro -- especialmente

cuando los usuarios no son conscientes de que están compartiendo recursos. Si un usuario de confianza puede obtener el acceso, existe la posibilidad de que un usuario malintencionado también lo pueda hacer. En los sistemas vinculados mediante conexiones de banda ancha, los atacantes tienen todo el tiempo necesario para conectarse a los recursos compartidos y explotarlos.

En los sistemas operativos Windows, existe un servicio llamado *Intercambio de archivos e impresoras* (o servicio de Servidor, en Windows NT). Cuando es habilitado, este servicio permite a otros acceder a su sistema por la red. Otros sistemas operativos tienen servicios similares (y por lo tanto debilidades similares). El servicio de Intercambio de archivos e impresoras de Microsoft utiliza el tráfico SMB (Server Message Block) del NetBIOS (Network Basic/Input/Output System) para dar aviso de los recursos compartidos pero no ofrece seguridad para restringir quién puede ver y acceder a ellos. La seguridad se controla estableciendo permisos a los recursos compartidos. El problema es que cuando se habilita un permiso compartido, por defecto los permisos se establecen para dar pleno control sobre el recurso al Grupo Todos –que incluye literalmente a todos los que acceden a ese sistema. Por defecto, el servicio de Intercambio de Archivos e Impresoras está vinculado a todas las interfaces (véase la sección sobre enlaces NIC más adelante en este capítulo). Ello quiere decir que cuando se habilita el intercambio con el objetivo de compartir por NIC recursos con la red interna confiable, el sistema está compartiendo los recursos con toda Internet por la conexión de banda ancha. Muchos usuarios no tienen la menos idea de la existencia de estas configuraciones por defecto y no se dan cuenta de que los recursos están disponibles para todo el mundo "por allá afuera" que conozca lo suficiente sobre Windows para encontrarlos.

Cuando menos, el servicios de Intercambio de Archivos e Impresoras debería estar desvinculado del adaptador de la conexión de banda ancha. Otra solución (o precaución adicional a esta) es utilizar un protocolo diferente en la red interna. Por ejemplo, las computadoras podrían comunicarse por la Interfaz de Usuario Extendida NetBIOS (NetBIOS Extended User Interface o NetBEUI) por una red local sin enrutar. Si el servicio de Intercambio de Archivos e Impresoras está vinculado al NetBEUI y desvinculado del TCP/IP (Transmisión Control Protocol/Internet Protocol) utilizado en Internet, los usuarios internos pueden seguir compartiendo los recursos pero estos no estarán disponibles a "extraños" en Internet.

Si el usuario no requiere compartir recursos con nadie en la red interna (local), se debe deshabilitar totalmente el servicio de Intercambio de Archivos e Impresoras. En la mayoría de las redes donde la seguridad es un elemento importante, este servicio está deshabilitado para todos los clientes. Con ello se obliga a que todos los recursos compartidos estén guardados en los servidores de red, los cuales generalmente tienen mejores controles de seguridad y acceso que los sistemas de cliente usuario-final.

Para utilizar la NAT

La facilidad NAT (Network Translation Address) es propia de muchos cortafuegos, proxies y sistemas factibles de enrutamiento. La NAT tiene varias ventajas, una de las cuales es su capacidad para ocultar la dirección IP y el diseño de la red interna. La capacidad para ocultar la red interna cuando se utiliza la Internet reduce el riesgo de que intrusos recopilen información sobre su red y la exploten para obtener acceso a ella. Si un

intruso no conoce la estructura de la red, su diseño, los nombres y la dirección IP de los sistemas, etc, le será muy difícil obtener acceso a ella.

La NAT permite a los clientes internos utilizar direcciones IP no enrutables, como las direcciones IP privadas definidas en el RFC 1918, y les mantiene el acceso a los recursos de Internet. La NAT restringe el tráfico de manera que solamente el tráfico solicitado u originado por el cliente interno pueda cruzar el sistema NAT desde redes externas.

Si hay solamente un sistema vinculado a Internet mediante una conexión de banda ancha, la NAT no es de gran utilidad. No obstante, para las redes locales que comparten una conexión de banda ancha, los beneficios de NAT se pueden utilizar con fines de seguridad. Cuando se utiliza la NAT, las direcciones internas son reasignadas a direcciones IP privadas y la red interna es identificada en el sistema NAT anfitrión. Una vez que esté configurada la NAT, los intrusos malintencionados solamente pueden acceder a la dirección IP del anfitrión NAT que está conectado directamente a Internet, pero no pueden "ver" ninguna de las computadoras internas que pasan por el anfitrión NAT para acceder a Internet.

En la escena...
Despliegue de una solución NAT
La NAT es relativamente fácil de aplicar y existen varias formas de hacerlo. Muchos dispositivos de hardware de banda ancha (cables y módems DSL) se denominan "enrutadores" de cable/DSL porque permiten que conectemos varias computadoras. Sin embargo, en realidad son dispositivos que combinan módem/NAT más que enrutadores, porque requieren solamente una dirección IP externa (pública). También es posible adquirir dispositivos NAT que conectan el cable básico o el módem DSL a la red interna. Por otro lado, la computadora que esté conectada directamente a un módem de banda ancha puede utilizar software NAT para hacer la función de dispositivo NAT. Esto puede ser un programa de software añadido como Sygate (www.sygate.com) o el software NAT incorporado en algunos sistemas operativos. Por ejemplo, el servidor Windows 2000 incluye un NAT plenamente configurable como parte de sus servicios de Enrutamiento y Acceso Remoto. Windows 98SE, 2000 Profesional, ME y XP incluyen una versión de NAT llamada Internet Connection Sharing (ICS).

Para una explicación ilustrada y rápida sobre el funcionamiento de la NAT con una conexión de banda ancha, véase el artículo de HomeNetHelp en www.homenethelp.com/web/explain/about-NAT.asp.

Cuando se utiliza la NAT para ocultar las direcciones IP internas, en ocasiones se le denomina cortafuegos NAT; no obstante, no debemos permitir que la palabra "cortafuegos" nos de un falso sentido de seguridad. Por sí sola la NAT resuelve solamente una parte del rompecabezas de la seguridad perimetral. Un verdadero cortafuegos hace mucho más que simplemente ocultar las direcciones IP internas.

Despliegue de un cortafuegos
Como analizamos en el capítulo 7, un cortafuego es un dispositivo o un producto de software cuyo principal objetivo es filtrar el tráfico que pasa por las fronteras de una red.

Esa frontera puede ser una conexión de banda ancha, un vínculo de conexión telefónica, o algún tipo de conexión LAN o WAN. La red puede ser una LAN de una empresa, o sistema independiente, o algo intermedio.

El uso más típico de los cortafuegos es restringir los tipos de tráficos que pueden atravesar las conexiones limítrofes de su red. Existen varios tipos de cortafuegos o de mecanismos de filtrado que pueden realizar este trabajo: filtros de paquete, sistemas de inspección con estado, sistemas proxy, y filtros a nivel de circuito.

Recordaremos que los filtros de paquete, también conocidos como enrutadores de filtrado, deciden qué tráfico es permitido o apropiado sobre la base de la información que encuentran en los encabezamientos TCP. La información que se utiliza de los encabezamientos TCP es normalmente la dirección IP de origen o destino y el puerto TCP o UDP (User Datagram Protocol) correspondiente. Los filtros de paquete son estáticos, están siempre abiertos y por lo tanto no tienen la capacidad para gestionar adecuadamente las aplicaciones de puerto dinámico. Además, los filtros de paquete no son capaces de controlar o transmitir el contenido.

Los sistemas de inspección con estado inspeccionan las actividades en curso dentro de sesiones de comunicación activas para cerciorarse de que el tipo de tráfico detectado es válido. La detección con estado fue diseñada para resolver las deficiencias de los filtros de paquete, especialmente para garantizar que el tráfico por los puertos dinámicos sea válido y autorizado.

Los sistemas proxy, también conocidos como puertas de enlace de aplicaciones o cortafuegos de aplicaciones, son capaces de filtrar el tráfico sobre la base de protocolos de alto nivel (como el Protocolo de Transferencia de Hipertexto o HTTP; el Protocolo de Transferencia de Archivos o FTP; Protocolo Simple de Transferencia de Correo o SMTP; y Telnet), aplicaciones, o incluso comando de control específico. Los sistemas proxy trabajan bien con las aplicaciones de puerto dinámico. El inconveniente de los sistemas proxy es que se necesita un servicio proxy específico para cada servicio o aplicación de Internet. Lamentablemente, algunos servicios y aplicaciones no se avienen muy bien con el uso del proxy. Además, los sistemas proxy hacen más lento el funcionamiento de la red debido a la cantidad de procesamiento que entraña la inspección completa de cada paquete.

El filtrado a nivel de circuito toma las decisiones de tráfico sobre la base del contenido de la sesión más que de los paquetes individuales. Los filtros a nivel de circuito abren los puertos solamente cuando los clientes internos realizan peticiones, con lo cual sustentan las aplicaciones de puerto dinámico como FTP. Este tipo de filtrado soporta una gama más amplia de protocolos que el sistema proxy, pero no brinda los controles detallados que proporciona este.

Al seleccionar un cortafuegos para proteger las conexiones de banda ancha, el usuario deberá buscar un producto que tenga todas estas capacidades de filtrado, así como características amplias de reporte y control, además de alarmas y alertas (las razones por las que estas últimas características son importantes se explican en el capítulo 9). Otra buena idea es buscar productos con capacidades de NAT y de detección de intrusión (que también se aborda en el capítulo 9).

Para los sistemas individuales, independientes y residenciales, existen varios productos cortafuegos de costo relativamente bajo que ofrecen una adecuada seguridad para computadoras no profesionales; entre ellos está el ZoneAlarm de Zone Labs. El

sistema operativo más reciente de Microsoft, Windows XP, también incluye un cortafuego personal incorporado. No obstante, para proteger una red comercial, los administradores no pueden depender de cortafuegos "personales". Las compañías deben invertir en un cortafuego que brinde un nivel de seguridad mayor y sea de una configurabilidad superior. Su despliegue se puede simplificar si se contrata una compañía de seguridad para que lo instale, configure, mantenga y administre.

Deshabilitar los servicios innecesarios

Uno las principales preceptos para mantener la seguridad física en una residencia o en un negocio es reducir la cantidad de vías que puede utilizar un intruso para lograr el acceso. Ello por lo general entraña la colocación de cerrojos en puertas y ventanas, el tapiado de túneles de acceso y el aseguramiento de los conductos de ventilación. Los administradores deberían aplicar la misma perspectiva con relación a las vías electrónicas de acceso a la red. Todas las vías por las cuales los datos válidos pueden llegar a la red o a la computadora son también vías posibles para el ataque o la visita de un intruso.

Los sistemas vinculados a Internet mediante conexiones de banda ancha deberían tener deshabilitados o totalmente eliminados o desinstalados cualquier protocolo, aplicación y servicio innecesario. Ante la proliferación de prácticas de programación deficientes que a menudo provocan vulnerabilidades de seguridad, resulta esencial limitar la exposición a los posibles ataques mediante la simple eliminación del software no necesario de los sistemas de computadora de la red. Por ejemplo, muchas versiones de Windows instalarán automáticamente un servidor Web durante la instalación por defecto del sistema operativo.Si un sistema no está destinado a funcionar específicamente como servidor Web, se debería deshabilitar ese componente del sistema operativo.

Configuración de la auditoria del sistema

Cuando un sistema queda comprometido sucede una de estas dos cosas:

- Suceden cosas malas y usted se da percata de ello (fallas del sistema, archivos borrados, o cosas parecidas).
- Suceden cosas malas y usted no se percata de ello (entra a su sistema una herramienta de un hacker, una cuenta de usuario queda comprometida, o una violación de seguridad similar).

Esperar que surjan indicios evidentes de violaciones del sistema es una mala práctica de seguridad, especialmente debido a que los comprometimientos no evidentes de la seguridad por lo general tienen consecuencias más graves. Los oficiales a cargo del cumplimiento de la ley pueden relacionar este concepto con la diferencia entre el trabajo *policial reactivo* (en el que un organismo de aplicación de la ley espera que se reporte un delito para entrar en acción) y el *trabajo policial proactivo* (el cual abarca actividades destinadas a evitar que los delitos ocurran). Todos sabemos que el método proactivo es más efectivo en la lucha contra el delito, pero tiene un inconveniente: entraña muchísimo más trabajo. Desafortunadamente, los administradores de sistema, oficiales de policía y otros seres humanos a veces sienten la tentación de escoger el camino menos trabajoso, y es por eso que proliferan los delitos prevenibles, incluidas las violaciones de la seguridad de redes.

La única forma de saber cuando un sistema ha sido violado o cuando ha ocurrido un intento fallido de penetrar su seguridad es monitorear en busca de actividad inusual o anormal, de la misma manera que los oficiales de la policía patrullan las calles en busca

de ocurrencias inusuales. La mayoría de los sistemas operativos incluyen capacidades de auditoría. Por ejemplo, los servidores de Windows y los sistemas operativos de cliente orientados a la esfera comercial, como NT Workstation y Windows 2000/XP Profesional, permiten el control de la seguridad mediante un registro de seguridad disponible para los administradores gracias a la herramienta de administración Visor de sucesos. Como mínimo, los administradores deberían auditar las entradas y las salidas del sistema, los cambios en las cuentas de usuarios y los privilegios, así como el uso de las funciones a nivel de administrador. Estas son actividades que a menudo están vinculadas a una violación de la seguridad y pueden servir como indicadores cuando se ha comprometido una computadora o una red.

Si la cantidad de datos que recopila el sistema de auditoria es demasiado para gestionarlo manualmente –como podría ser el caso en una red empresarial– quizás sea beneficioso invertir en un sistema de detección de intrusión (IDS). Un IDS automatiza la tediosa tarea de buscar actividad anormal o sospechosa en un sistema. El IDS utiliza el reconocimiento de patrones y el aprendizaje heurístico para detectar las actividades sospechosas por parte de cuentas de usuarios autorizados, así como por usuarios externos malintencionados.

Seguridad de buscadores y correo electrónico

Independientemente del tipo de conexión a Internet que utilice una empresa o una persona --ya sea una conexión de banda ancha, telefónica o LAN-- es importante abordar las vulnerabilidades de seguridad que representan los buscadores web para los sistemas y las redes. Muchos de los software de cliente de servicios de Internet más comúnmente utilizados, como los buscadores web o las utilidades de correo electrónico, son vulnerables a ataques malignos cuyo número es cada vez más elevado. La mayoría de estos ataques son posibles debido a las capacidades dinámicas y automatizadas que estas herramientas han adquirido con el paso de los años. La inclusión de los lenguajes de programación y de secuencia de comandos en estas utilidades (por ejemplo, JavaScript, Java y ActiveX) ha introducido nuevas y fácilmente explotables vulnerabilidades de seguridad a un entorno ya de por sí imperfecto. Como resultado de su esfuerzo por mantener su participación en el mercado de buscadores al ofertar una gama más amplia de capacidades y posibilidades, el buscador web de Microsoft, Internet Explorer, y sus clientes de correo electrónico Outlook y Outlook Express han adquirido una inmensa popularidad y, en consecuencia, son los clientes de servicio Internet más comúnmente atacados.

Es importante recordar que Microsoft no es el único proveedor cuyos productos de servicio Internet son susceptibles a los ataques; es sencillamente debido a que los productos de esta empresa son los más populares que se han convertido en el blanco favorito de los atacantes. Algunos usuarios --incluidos profesionales del trabajo en red que deberían hacer mejor las cosas-- operan bajo un falso sentido de seguridad (podríamos decir que están operando bajo una Condición Blanca) porque utilizan productos que no son de Microsoft. Cada vez que se anuncia una falla de seguridad de Internet Explorer, Outlook o un sistema operativo de Microsoft, se jactan orgullosamente de que no utilizarían nunca un producto no seguro. Sin embargo, si buscamos en la web vulnerabilidad de seguridad de UNIX y Linux encontraremos miles de páginas en las que

se detallan agujeros de seguridad en varias versiones de UNIX/Linux. Vale repetir una vez más que Ninguna computadora conectada a una red es totalmente segura.
En lo que se refiere a los buscadores web, la verdad es que cualquier utilidad que soporte la ejecución de scripts o códigos de programación descargado desde una página web o un mensaje de correo electrónico es vulnerable. En sus esfuerzos por mantenerse a la par con Microsoft en cuanto a las herramientas que brindan, Netscape soporta los mismos tipos de scripting y por ello sufre de las mismas vulnerabilidades. Opera, un pequeño buscador alternativo popular entre muchos usuarios, ahora soporta Java, aunque no era así en las versiones iniciales. La proliferación de estas vulnerabilidades es el resultado de la búsqueda de funcionalidad con la esperanza de obtener un porciento del mercado en lugar de investigar a fondo y abordar sus implicaciones de seguridad.

La mayoría de las vulnerabilidades de los clientes web y de correo electrónico están relacionadas con errores de desbordamiento del búfer o la ejecución arbitraria de códigos. Estas dos vulnerabilidades permiten que un sistema remoto, ya sea un sitio web o el remitente de un mensaje de correo electrónico, ejecute un código maligno en su computadora. En la mayoría de los casos, el código ejecutado obtiene privilegios a nivel de sistema, lo cual quiere decir que no existe literalmente restricción alguna respecto de las acciones que ese código puede realizar.

Las mismas tecnologías que crean las vulnerabilidades en los buscadores web pueden también utilizar el correo electrónico en HTML. Muchos clientes de correo electrónico populares, incluidos Outlook y Outlook Express, Eudora y Netscape Mail, pueden permitir que se ejecute un contenido activo, con lo cual el sistema queda abierto a los códigos malignos. Pegasus Mail es algo más seguro porque en su manejador de HTML no ejecuta secuencia de comandos, *applets* de Java ni controles ActiveX. (No obstante, Pegasus si permite que se abran documentos adjuntos que pudieran contener macros malignas).

En las secciones siguientes analizamos las tecnologías que crean los riesgos de seguridad en los buscadores web y el correo electrónico, y posteriormente analizamos cómo elevar la seguridad de cada uno de esos populares programas buscadores.

Tipos de códigos peligrosos

Se pueden utilizar diferentes tipos de código para mejorar las páginas web y el correo electrónico y para realizar acciones no deseadas e incluso peligrosas en una computadora. En las secciones siguientes brindamos una visión general de estos tipos de códigos más populares: JavaScript, ActiveX y Java.

JavaScript

JavaScript es un lenguaje de secuencia de comandos creado por Netscape para permitir que los códigos ejecutables se fijaran en las páginas web. Todos los principales buscadores web soportan el JavaScript. JavaScript es utilizado para manipular el tamaño de la ventana del buscador, abrir y cerrar ventanas, gestionar formularios, y alterar las configuraciones del buscador. El propio JavaScript es relativamente seguro. No obstante, aplicaciones no apropiadas (tales como errores de programación del proveedor) han permitido numerosos ataques. Cada proveedor ha creado revisiones para la mayoría de estas vulnerabilidades, pero aún es posible utilizar el JavaScript para realizar una actividad maligna si se logra hacer que los navegadores web hagan algo que no deberían hacer. Desafortunadamente, por lo general es fácil para un sitio web maligno engañará

los visitantes para que brinden acceso o permitan ejecución de códigos cuando no deberían hacerlo. Para información sobre ataques específicos que utilizan el JavaScript, véase el sitio web JavaScript for Beginners en http://polaris.umuc.edu/~mgaylor/Issues.html.

NOTA

El JavaScript es totalmente diferente del Java. La única similitud entre ellos está en las primeras cuatro letras del nombre.

ActiveX

ActiveX en una tecnología de fijación de códigos creada por Microsoft. Emplea un control de seguridad conocido como *firma de códigos*. Cada programa ActiveX es denominado un *control*. Cuando un control se descarga a un buscador web, es examinado en busca de una firma digital utilizando la tecnología *Authenticode*, o autenticación de código, para verificar la firma con una autoridad de certificación y garantizar que el control no ha sido alterado antes de su descarga. Se muestra un cuadro de diálogo, que indica que el ActiveX está firmado por una compañía o una persona específica, y pide al usuario que indique si acepta o no esté control, si acepta siempre los controles de esta entidad o si rechaza el control. Una vez que el control ActiveX está en un sistema, puede hacer todo para lo que esté programado, ya sea una acción benigna o maligna. Conocer la identidad de los autores de un control no es garantía de que el control sea seguro ni de que sus interacciones con otros controles no crearán nuevas vulnerabilidades en su sistema.

Una de las conocidas fallas de ActiveX era el control Exploder desarrollado por Fred McLain para ilustrar los peligros de ActiveX. Para más información respecto de esta falla, la cual puede apagar una computadora desde una página web, véase www.halcyon.com/mclain/ActiveX/Exploder/FAQ.htm.

Java

Java es un lenguaje de programación desarrollado por Sun Microsystems. Su diferencia principal con el JavaScript radica en que utiliza una técnica conocida como *sandboxing* para restringir sus capacidades. Los programas Java que se ejecutan localmente son denominados *applets*. Cada *applet* es verificada para garantizar que esté codificada adecuadamente y no esté corrupta antes de permitírsele ejecutarse. Posteriormente un monitor de seguridad controla la actividad del *applet* para impedirle que realice acciones las cuales no debería poder hacer, como leer datos, abrir conexiones de red o borrar archivos.

Desafortunadamente, algunas aplicaciones de Java se han visto comprometidas cuando se explotan diferentes fallas. Por ejemplo, en agosto de 2000, CERT emitió un aviso de seguridad en el sentido de que algunas versiones de Netscape Communicator contenían clases de Java que permitían que *applets* de Java no firmadas accedieran a los recursos locales y remotos violando las políticas de seguridad para las *applets*. Las *applets* hostiles pueden hacer colapsar buscadores y sistemas, matar otras *applets*, extraer nuestras direcciones de correo electrónico y enviarlas al distribuidor del *applet*, además de otras acciones impropias. Véase la página Hostile Applets en www.cigital.com/hostile-applets/index.html.

NOTA

Un excelente escrito sobre temas de seguridad de Java puede encontrarse en http://ei.cd.vt.edu/-wwwbtb/fall.96/book/chap14/index.html. La transcripción de una buena explicación que compara ActiveX y Java en términos de temas de seguridad está disponible del equipo de Secure Internet Programming de Princeton en www.cs.princeton.edu/sip/faq/java-vs-activex.html.

Elevando la seguridad de los buscadores y los clientes de correo electrónico

Son varias las medidas que pueden tomar los administradores y los usuarios de redes para elevar la seguridad de los buscadores web y de los clientes de correo electrónico, y protegerlos frente a códigos malignos o el uso no autorizado de la información. Entre estas medidas están restringir el uso de los lenguajes de programación, actualizar los revisiones de seguridad y conocer sobre el funcionamiento de los cookies.

Restricción de los lenguajes de programación

La mayoría de los buscadores web tienen configuraciones que permiten a los usuarios restringir o denegar el uso de lenguajes de programación con base en la web. Por ejemplo, Internet Explorer se puede configurar para que siempre permita, siempre deniegue los elementos JavaScript, Java o ActiveX o pregunte al usuario qué desea hacer cuando uno de ellos aparezca en una página web. Restringir todos los códigos ejecutables desde los sitios web, o al menos obligar a que el usuario tome la decisión cada vez que estos son descargados, reduce las violaciones de seguridad que provocan los componentes malignos descargados.

Un beneficio adicional de restringir estos lenguajes de programación en el caso de los buscadores web es que dichas restricciones a menudo se aplican también al cliente de correo electrónico. Ello es así en el caso del Internet Explorer como buscador y el Outlook o Outlook Express como cliente de correo electrónico, mientras que Netscape y Eudora también dependen del buscador Web para manejar los HTML. El mismo código maligno que puede ser descargado desde un sitio web puede ser también fácilmente enviado a la cuenta de correo electrónico de una persona. Si no están habilitadas esas restricciones, su cliente de correo podría ejecutar automáticamente el código descargado.

Mantener actualizados las revisiones (*patches*) de seguridad

Al parecer todos los días aparecen nuevas fallas de los buscadores web y los clientes de correo electrónico. Usualmente, los proveedores de productos abordan importantes amenazas de una manera rápida al emitir una revisión para sus productos. Para mantenerla seguridad de un sistema, es preciso mantenerlos informados sobre nuestro software y aplicar revisiones para las vulnerabilidades cuando éstas sean emitidas.

No obstante, es preciso tener en cuenta algunos elementos cuando se trabaja con revisiones de software:

- A menudo las revisiones son emitidas rápidamente, en respuesta a un problema inmediato, por lo que quizás no hayan sido probadas detalladamente. Ello puede traer como consecuencia fallos en la instalación, el colapso del sistema, la inoperabilidad de los programas, u otras vulnerabilidades de la seguridad.

- Es en extremo importante probar las nuevas revisiones en sistemas no relacionado con la producción antes de desplegarlas en toda la red.
- Si no se puede garantizar que una revisión es segura para su instalación, usted debe considerar las consecuencias de no instalarla y permanecer vulnerable a la amenaza, frente a la posibilidad de que la propia revisión pueda dañar su sistema. Si la amenaza es mínima, a menudo es más seguro esperar hasta experimentar el problema para el cual está destinada la revisión antes de instalarla.

Conocimiento sobre los cookies

Un *cookie* es una especie de mensaje que entrega un sitio web a un buscador web para ayudar a rastrear a un visitante entre un clic y otro. El buscador almacena el mensaje en el disco duro local del visitante en un archivo de texto. El archivo contiene información que identifica al usuario y su presencia o actividades anteriores en ese sitio web. Si el usuario visita nuevamente el mismo sitio web, el buscador del usuario envía la *cookie* nuevamente al servidor web. Los cookies son extremadamente útiles para permitir que un sitio web brinde comunicaciones aparentemente continuas a un visitante, como mantener un carrito de compras, recordar las palabras de una búsqueda, o personalizar los datos mostrados sobre la base de las preferencias del usuario. No obstante, debido a que los cookies contienen información de identificación, pueden ser utilizados para propósitos menos nobles.

En la prensa se ha analizado ampliamente el tema de los cookies. Estos artículos a veces adjudican a los cookies más poder del que realmente tiene y le prestan más atención de la que merecen. Los cookies crean preocupaciones acerca de la privacidad, sin embargo no son capaces de ejecutar códigos ni de acceder a archivos. Simplemente almacenan datos procedentes de una sesión de búsqueda en la web y los envían de vuelta al servidor web. Los cookies pueden ser enviados a una computadora por medio de las páginas web o de un correo electrónico habilitado por HTML. El uso malintencionado, o al menos no escrupuloso, de los cookies ocurre cuando son utilizadas para rastrear los hábitos de navegación de un usuario de un sistema a otro, apoderarse de la información de acceso de usuario en un sitio y enviarla a otro, o incluso para capturar la dirección de correo del usuario y enviarla a listas de correo sin el conocimiento del usuario. Afortunadamente, los cookies pueden ser deshabilitados de la misma manera que los lenguajes de programación.

Seguridad del programa buscador web

Si bien se aplican los mismos principios generales, cada uno de los programas de buscadores web populares tiene un método ligeramente diferente para configurar sus opciones de seguridad. Las secciones siguientes muestran cómo cambiar las configuraciones de los tres buscadores más populares --Internet Explorer de Microsoft, Netscape y Opera-- y deshabilitar características que permiten explotar fallas de seguridad.

Seguridad de Internet Explorer de Microsoft

Brindar seguridad al Internet Explorer (IE) de Microsoft incluye la instalación de las actualizaciones y revisiones, la modificación de algunas configuraciones, y la práctica de

una navegación inteligente. Al parecer Microsoft emite una revisión de seguridad para Internet Explorer todas las semanas. Este constante flujo de revisiones se debe tanto a que los programadores que escribieron el código pasaron por alto algunas cuestiones, como a los ataques que tienen como objetivo los productos de Microsoft y que realiza la comunidad de hackers malintencionados. A pesar de esta atención negativa, el IE puede aún emplearse como un buscador web relativamente seguro, cuando está correctamente configurado.

El primer paso para brindar seguridad al IE es instalar las revisiones y las actualizaciones más recientes. Los usuarios pueden hacerlo automáticamente mediante la ventana de Actualización, o hacerlo manualmente. Cualquiera sea la forma empleada, solamente mediante la aplicación de las revisiones se resolverá la mayoría de las vulnerabilidades conocidas en el programa IE. Para obtener información sobre las revisiones de seguridad disponibles para el programa de buscador más reciente de Microsoft, véase www.microsoft.com/windows/ie/security/default.asp.

El segundo paso es configurar el IE para la navegación segura. Los usuarios pueden hacer esto mediante el *applet* Opciones de Internet. En la versión 6 de IE (el buscador vigente en el momento de escribir este libro), se accede a esta *applet* mediante el Panel de Control de Windows o mediante el menú *Herramientas de IE*. Si se varían las configuraciones predeterminadas en las fichas *Seguridad*, *Privacidad*, *Contenido* y *Opciones Avanzadas*, como se muestra en la figura 8.1, la seguridad de IE se mejora significativamente.

En la ficha *Seguridad* se definen las zonas. Una zona no es más que una colección de sitios web (de Internet o una intranet local) a la que se puede asignar un nivel de seguridad específico. El IE utiliza las zonas para definir el nivel de amenaza para el sistema que representa un sitio web específico. El Internet Explorer ofrece cuatro opciones de zona de seguridad:

- **Internet** Contiene todos los sitios no asignados a otras zonas
- **Intranet local** Contiene todos los sitios dentro de una intranet local o en el sistema local. Esta zona es mantenida automáticamente por el sistema operativo
- **Sitios de confianza** Contiene solamente los sitios añadidos manualmente a esta zona. Los usuarios deben añadir a esta zona solamente los sitios que son plenamente fiables
- **Sitios restringidos** Contiene solamente los sitios añadidos manualmente a esta zona. Los usuarios deben añadir a esta zona cualquier sitio que sea específicamente no fiable o que se conozca como sitio maligno.

Figura 8.1 Las configuraciones en la ficha *Seguridad* de las *Opciones de Internet* del IE definen las zonas de seguridad

A cada zona se le asigna un nivel de seguridad predefinido o se puede crear un nivel personalizado. Los niveles de seguridad predefinidos aparecen en un control deslizante con cuatro pasos: Bajo, Medio-Bajo, Medio y Alto; se brinda una descripción del contenido que será descargado a tenor de las condiciones particulares (véase la descripción para el nivel Medio en la figura 8.1).

Es posible definir los niveles de seguridad para avenirse exactamente a las restricciones de seguridad del entorno en que usted trabaja. Existen más de 20 controles de seguridad individuales relacionados con la manera en que se manejan los ActiveX, las descargas, Java, la gestión de datos, el manejo de datos, scripting, y la entrada. La configuración más segura es fijar todas las zonas en el nivel de seguridad Alto. No obstante, debemos tener presente que a mayor seguridad menor funcionalidad y capacidad.

La ficha *Privacidad*, que se muestra en la figura 8.2, define cómo IE gestiona la información personal mediante *cookies*.

Figura 8.2 Las opciones de *cookies* se pueden fijar en el IE mediante la ficha *Privacidad* en *Opciones de Internet*.

Figura 8.3 Se pueden configurar las opciones de certificado en IE en la ficha *Contenido* en *Opciones de Internet*

Figura 8.4 La ficha *Opciones Avanzadas* en las *Opciones de Internet* de IE nos permite configurar la seguridad.

La ficha *Privacidad* incluye un control deslizante con seis niveles que van desde apertura total hasta aislamiento total. También es posible definir un conjunto de controles de *cookies* decidiendo si los cookies de origen y los de terceros estarán autorizados, denegados o requerirán que se despliegue un mensaje de pregunta, y si están permitidos los cookies de sesión. Es posible definir sitios web individuales cuyos *cookies* siempre estarán autorizados o siempre bloqueados. Impedir cualquier recurso de *cookies* es la configuración más segura, pero también es la menos funcional. Muchos sitios web no funcionarán adecuadamente bajo esta configuración, mientras que algunos ni siquiera le permitirán visitarlos cuando los cookies están deshabilitados.

La ficha de *Contenido*, que se muestra en la figura 8.3, nos da acceso a los certificados que son fiables y aceptados por IE. Si se ha aceptado un certificado el cual ha dejado de ser fiable, es posible eliminarlo.

Esta ficha también nos da acceso a la capacidad de Completamiento Automático de IE. Esta función es útil en muchas circunstancias, pero se convierte en un riesgo de seguridad cuando es utilizada para recordar nombres de usuarios y contraseñas a sitios de Internet. La configuración más segura requiere que esta función sea desactivada para los nombres de usuario y contraseñas, que se desactive la ventana de mensaje donde se pide salvar las contraseñas, y que se borre el caché de contraseña vigente.

En la fichas *Opciones Avanzadas*, que se muestra en la figura 8.4, se incluyen varios controles propios de la seguridad al final de una larga lista de controles funcionales. Estos controles de seguridad incluyen verificar la revocación de certificado, no salvar las páginas encriptadas al disco, borrar los archivos temporales de Internet cuando se cierre el buscador, utilizar Secure Shell/Transport Layer Security (SSL/TLS), y advertir cuando los formularios son presentados de manera no segura. La configuración más segura tiene todas estas características deshabilitadas.

Un paso final en el mantenimiento de un uso seguro de IE es practicar hábitos de navegación seguro. El sentido común debe determinar las acciones que realizan los

usuarios, tanto en línea como cuando se está desconectado. Desafortunadamente, como han observado muchos oficiales encargados del cumplimiento de la ley en el curso de sus funciones, el sentido común no es tan común. La mayoría de nosotros no caminaría por un callejón oscuro en el medio de la ciudad a las tres de la mañana, sin embargo hay quienes lo hacen y, desafortunadamente, aprenden la lección a las malas. Visitar sitios web de diseño cuestionable es el equivalente virtual de arriesgarnos al peligro en un callejón oscuro, sin embargo los usuarios de Internet lo hacen siempre. A continuación presentamos algunas ideas que se deben seguir para una navegación segura:

- Descargar software únicamente desde los sitios web del proveedor original.
- Siempre intentar verificar el origen o la propiedad de un sitio web antes de descargar materiales desde él.
- No suponer nunca que todo lo que aparece en línea es ciento por ciento exacto.
- Evitar visitar sitios web sospechosos --especialmente los que ofrecen herramientas de crackeo, programas pirateados o pornografía—desde un sistema cuya seguridad es preciso mantener.
- Rechazar siempre los certificados u otros cuadros de diálogo marcando No, Cancelar, o Cerrar cuando se pide una acción en sitios web o proveedores en línea con los cuales usted no está familiarizado.

Dando seguridad a Netscape Navigator

Dar seguridad a Netscape Navigator es una tarea similar a la de dar seguridad a Internet Explorer. Se debe mantener actualizado el software instalando las revisiones de seguridad Netscape, y se deben practicar hábitos de navegación seguros. Los ajustes de seguridad específicos de Netscape Navigator se definen en el cuadro de diálogo *Preferencias* en las secciones *Privacidad y seguridad*, y *Opciones Avanzadas*.

En la subsección *Cookies*, de *Privacidad y seguridad*, se define el manejo de los cookies. Se pueden habilitar o deshabilitar todos los cookies. Mediante el *Gestor de cookies* (Cookies Manager), al cual se accede accionando el botón View Stored Cookies [Ver cookies guardadas], es posible inspeccionar *cookies* individuales y decidir eliminarlas todas o algunas determinadas. La configuración más segura es deshabilitar todos los cookies. Una configuración menos segura pero más funcional es la que permite los cookies de origen pero desplegando una advertencia antes de guardarlas.

La subsección *Contraseñas web*, de *Privacidad y seguridad*, define si los nombres de usuario y contraseñas para sitios web se almacenarán en su sistema a fin de poderlos utilizar nuevamente de manera automática en visitas posteriores a esos sitios. Esta función puede ser activada o desactivada, además de que se puede borrar por separado cualquier credencial de entrada almacenada. La configuración más segura es deshabilitar el almacenamiento automático y borrar cualquier credencial almacenada. La versión de Netscape para Macintosh, que funcionan en el SO X, se muestra en la figura 8.5.

Figura 8.5 Las opciones de Privacidad y seguridad de Netscape nos permiten gestionar *cookies* y contraseñas.

Los usuarios pueden utilizar la subsección *Certificados*, de *Privacidad y seguridad* (en la versión de Netscape para Windows) para ver y gestionar certificados.

De manera parecida al administrador del IE, nos permite ver los certificados aceptados e incluso eliminarlos. Revisar regularmente los certificados aceptados constituye una buena práctica de seguridad.

La sección *Opciones Avanzadas* nos ofrece cuadros que se pueden marcar para habilitar o deshabilitar Java y JavaScript. El Netscape Navigator no soporta ActiveX. La configuración más segura es deshabilitar estos dos lenguajes de programación.

Dando seguridad a Opera

Dar seguridad al buscador web Opera es una operación similar al proceso con IE y Netscape Navigator. Primero, actualizar el software con las revisiones más recientes emitidas por el proveedor. Después, dar seguridad al buscador. Posteriormente, practicar hábitos de navegación seguros.

La operación de dar seguridad al buscador Opera se realiza mediante el cuadro de diálogo *Preferencias*, al cual se accede desde el menú *Archivos*. Opera soporta el JavaScript pero no ActiveX. Si se desea se puede añadir el soporte para Java. El JavaScript se puede desactivar mediante la sección *Multimedias* de la sección *Preferencias* de Opera. Si está instalado Java, aquí se puede igualmente habilitarlo o deshabilitarlo. La sección *Privacidad*, que se muestra en la figura 8.6, controla el uso de *cookies*. Los cookies se pueden habilitar, deshabilitar o aceptar solamente desde los sitios de origen.

La sección *Seguridad* de Preferencias, que se muestra en la figura 8.7, se utiliza para controlar certificados, el cacheo (caching) de contraseñas y la no seguridad de formularios. Los usuarios pueden escoger los protocolos de seguridad (SSL 2, SSL 3, y TLS 1) que serán habilitados, y pueden configurar las propiedades de cada uno de ellos.

Figura 8.6 La sección *Privacidad* en *Preferencias* de Opera nos permite controlar el comportamiento de los cookies.

Figura 8.7 La sección *Seguridad* en *Preferencias* de Opera nos permite controlar certificados, protocolos, contraseñas y envío de formularios.

Poniendo en práctica la seguridad de un servidor web

Actualmente la mayoría de las compañías y organizaciones tienen una presencia web en Internet. La presencia en Internet brinda numerosas ventajas comerciales, como la posibilidad de llegar a un auditorio amplio, publicar anuncios, interactuar con clientes y socios, y brindar información actualizada a las partes interesadas.

Las páginas web son almacenadas en servidores que ejecutan software de servicios web como Internet Information Server (IIS) de Microsoft, o Apache (en servidores Linux/UNIX). Los servidores web deben ser accesibles vía Internet para que el publico pueda acceder a sus páginas web. No obstante, esta accesibilidad facilita un punto de entrada a los "malos" de Internet que desean introducirse en la red, por lo que es de vital importancia que los servidores web sean seguros. Proteger un servidor web no es tarea fácil. Los sistemas vinculados a Internet, antes de ser plenamente fuertes, por lo general son detectados y comprometidos en cuestión de minutos. Los crackers maliciosos están siempre buscando activamente sistemas para infiltrarlos, por lo cual es esencial resguardar apropiadamente el servidor web antes de ponerlo en línea.

Primero que todo, los administradores deben cerrar el sistema operativo subyacente. Para este proceso se deben aplicar actualizaciones y revisiones, eliminar los protocolos y servicios no necesarios, y configurar adecuadamente todos los controles de seguridad nativos. Algunos de los temas importantes relacionados con los procedimientos de cierre de sistemas operativos específicos se analizan más adelante en este capítulo.

En segundo lugar, una medida inteligente es resguardar el servidor con una barrera protectora, como un cortafuego o un proxy reverso. Todo lo que limite, restrinja, filtre o controle el tráfico de entrada y salida del servidor web reduce los medios por los cuales los usuarios malintencionados pueden atacar el sistema.

En tercer lugar, los administradores deben cerrar el servidor web. Este proceso en realidad tiene numerosas facetas, cada una de las cuales es importante para mantener la seguridad de un servidor web. En las secciones siguientes analizamos estos temas.

ZDM o Fortaleza

Hay dos líneas generales de pensamiento en lo que se refiere a la seguridad de los servidores web. Una de ellas es presumir que el servidor web será comprometido y prepararse entonces para esa situación. La otra es tratar de impedir cualesquiera y todos los ataques a toda costa. La primera filosofía utiliza un despliegue denominado zona desmilitarizada (ZDM) o DMZ en inglés, por demilitarized zone); la segunda descansa en un diseño al cual se le llama *fortaleza* (stronghold).

Una ZDM es una zona de redes en el que su servidor web (y otros servidores que están asequibles por la Internet pública) está seguro frente a la mayoría de los ataques más comunes, pero tiene determinado grado de inseguridad en algún nivel. Como la ZDM es una red independiente, la red interna se mantiene más segura. La ZDM presupone que el tiempo y el dinero requerido para protegerse frente a todo ataque posible son un precio demasiado elevado, frente al valor de los datos hospedados en el servidor web.

NOTA

En algunos de sus documentos Microsoft utiliza el término *subred filtrada* (screened subnet) para hacer referencia a la ZDM. También el mismo concepto en ocasiones se denomina *red perimetral* (perimeter network).

Para compensar por la falta de seguridad de primera línea, las organizaciones que despliegan una ZDM, la configuración típicamente tiene un servidor web duplicado ubicado en su LAN interna, el cual mantiene una imagen réplica del servidor web accesible públicamente. En el caso de que el servidor web primario quede comprometido, la imagen de respaldo se puede reubicar para que haga las veces de servidor web público hasta tanto se repare el sistema primario. Otras empresas aplican una solución aún menos costosa al mantener solamente cintas de respaldo del servidor web primario. La empresa que actúe así debe presumir que el tiempo y el dinero que pierde mientras su servidor web está de baja no le afectará significativamente. Podría también suponer que el valor de su presencia en la web no justificar una solución que entrañe una gasto como el de crear y mantener un sistema de respaldo.

Una *fortaleza* es una zona de redes en la que el servidor web está protegido contra todo tipo de ataque y se realizan esfuerzos significativos por protegerlo frente a cualquier nueva posible amenaza. Una fortaleza presupone que los datos que hospeda en servidor

web son suficientemente valiosos para no escatimar gastos en su protección. Este tipo de configuración la utilizan a menudo las organizaciones para las cuales la integridad y disponibilidad de su servidor web son esenciales para los negocios, como por ejemplo, los sitios de comercio electrónico.

Cada organización debe escoger la política de protección que sea apropiada para sus condiciones y necesidades. La ZDM es más barata pero más propensa a los ataques que una fortaleza. Una fortaleza es más costosa que una ZDM será capaz de repeler una mayor cantidad de ataques.

Aislar el servidor web

Por razones de seguridad, el servidor web debe ser independiente de la LAN interna. De lo contrario, si el servidor web queda comprometido, el atacante podría obtener fácil acceso a toda la red. Separar el servidor web de la red interna de producción impide que un ataque desde la web destruya su organización.

Para separar el servidor web de la LAN se pueden aplicar muchas variantes:

- Habilitar un dominio independiente solamente para el servidor web y sus servicios de soporte
- Utilizar una solución de trabajo en web que no tenga otra capacidad más que la de ser un servicio de página web
- Colocar los servicios web en un ISP
- Contratar los servicios web a un ISP o a un tercero

Independientemente del método que seleccione una organización, también es conveniente analizar la idea de crear un canal de comunicación de banda lateral para todas las actividades de gerencia, administración y transferencia de archivos. Un canal de comunicación de banda lateral puede ser tan simple como utilizar un protocolo único entre su LAN y el servidor web e impedir que el TCP/IP cruce de ese vínculo. Dicho canal podría ser una conexión telefónica, una línea ISDN dedicada, o incluso un vínculo de puerto serie de conexión directa. Utilizar este tipo de canal restringe el tráfico que puede fluir entre el servidor web y la red interna. Este sistema podría atenuarla velocidad o las capacidades de la administración remota; no obstante, reduce grandemente la posibilidad de que usuarios maliciosos pasen de un servidor web comprometido a la LAN.

Cuando la seguridad es de importancia máxima, las organizaciones pueden desplegar un cortafuego en el canal de banda lateral o eliminar completamente la comunicación directa. Si es necesario que el administrador esté físicamente presente en el servidor web y transferir datos hacia y desde este utilizando medios extraíbles (unidades de CD-Rs, CD-RWs, Zip o Jaz, o similares), esto elimina totalmente la posibilidad de que un usuarios malicioso utilicen el servidor web como puente para entrar a la LAN.

Cierre del servidor web

El proceso de cerrar el servidor web comienza con algo con lo cual ya deben estar ustedes familiarizados: aplicar las revisiones y actualizaciones más recientes del proveedor. Una vez realizada esta tarea, el administrador de la red debe seguir las recomendaciones del proveedor para configurar los sitios web de manera segura. En las secciones siguientes

analizamos las recomendaciones que suelen hacer los proveedores de servidores web y profesionales de la seguridad.

Administración del control de acceso

Muchos servidores web, como IIS o Windows NT y Windows 2000, utilizan una cuenta de usuario nombrado para autentificar a los visitantes web anónimos. Cuando un visitante web accede a un sitio web utilizando esta metodología, el servidor web lo registrará automáticamente usuario como la cuenta de usuario IIS. El usuario visitante permanece anónimo, pero la plataforma del servidor huésped utiliza la cuenta de usuario IIS para controlar el acceso. Esta cuenta ofrece a los administradores de sistema un control de acceso granular a un servidor web.

Estas cuentas de usuario web especializadas deben tener un acceso restringido de manera que no puedan registrarse localmente ni acceder a lo que está fuera de la raíz web. Además, los administradores deben tener mucho cuidado en conceder a estas cuentas la capacidad para escribir a archivos o ejecutar programas; ello debe hacerse solo cuando es absolutamente necesario. Si se permite que otras cuentas de usuario nombrado se registren por la web, es esencial que estas cuentas no sean las mismas cuentas de usuario empleadas para la entrada a la red interna. En otras palabras, si los empleados se van a registrar por la web utilizando sus propias credenciales y no la cuenta de usuario web anónimo, los administradores deben crear cuentas especiales para que esos usuarios las utilicen para su entrada por la web. Las autorizaciones por Internet se deben considerar inseguras a menos que se hayan aplicado mecanismos de encriptación estrictos para protegerlas. El SSl se puede utilizar para proteger el tráfico web; sin embargo, la protección que brinda no es suficientemente significativa para justificar el uso de cuentas internas Internet.

Estas cuentas de usuario web especializadas deben tener un acceso restringido de manera que no puedan registrarse localmente ni acceder a lo que está fuera de la raíz web. Además, los administradores deben tener mucho cuidado en conceder a estas cuentas la capacidad para escribir a archivos o ejecutar programas; ello debe hacerse solo cuando es absolutamente necesario. Si se permite que otras cuentas de usuario nombrado se registren por la web, es esencial que estas cuentas no sean las mismas cuentas de usuario empleadas para la entrada a la red interna. En otras palabras, si los empleados se van a registrar por la web utilizando sus propias credenciales y no la cuenta de usuario web anónimo, los administradores deben crear cuentas especiales para que esos usuarios las utilicen para su entrada por la web. Las autorizaciones por Internet se deben considerar inseguras a menos que se hayan aplicado mecanismos de encriptación estrictos para protegerlas. El SSl se puede utilizar para proteger el tráfico web; sin embargo, la protección que brinda no es suficientemente significativa para justificar el uso de cuentas internas Internet.

Manejo de estructura de directorios y datos

Planificar la jerarquía o estructura de la raíz web es un elemento importante en la configuración de seguridad de un servidor web. La raíz es la web de más alto nivel en la jerarquía, que consiste en webs alojadas dentro de webs. Siempre que sea posible los administradores de servidores web deben ubicar todo el contenido web dentro de la raíz web. Toda la información web (páginas web escritas en HTML, archivos de gráficos,

archivos de sonido, etc.) normalmente están almacenados en carpetas y directorios en el servidor web. Los administradores pueden crear *directorios virtuales*, que son carpetas no incluidas dentro de la jerarquía del servidor web (pueden estar en una computadora totalmente diferente) pero que para el usuario aparecen como parte de esa jerarquía. Otra forma de brindar acceso a los datos que están en otra computadora es asignar unidades o carpetas. Estos métodos permiten a los administradores almacenar archivos donde se puedan actualizar más fácilmente o sea posible aprovechar el espacio en disco disponible en otras computadoras. No obstante, asignar unidades y carpetas o crear directorios virtuales podría facilitar el acceso a intrusos en caso de que la seguridad del servidor web se viera comprometida. Resulta especialmente importante no asignar las unidades de otros sistemas en la red interna.

Si los usuarios que tienen acceso a estas webs deben tener acceso a materiales ubicados en otro sistema, como bases de datos, es preferible tener una copia del servidor dentro de la ZDM o dominio del servidor web. Esta copia debe contener solamente una copia de seguridad del servidor, y no ser una copia de trabajo primaria de la base de datos. La copia del servidor debe además estar configurada de manera que ningún usuario o proceso pueda alterar o escribir en el almacén de datos. Las actualizaciones de la base de datos deben proceder únicamente del servidor protegido dentro de la red interna. Si es preciso guardar sesiones web en la base de datos, es mejor configurar una conexión colateral desde la zona web al sistema del servidor primario para las transferencias de datos. Los administradores también deben realizar grandes esfuerzos por verificar la validez de los datos de entrada antes de añadirlos al servidor de base de datos.

Vulnerabilidades del scripting

Mantener la seguridad de un servidor web exige garantizar que todos los scripts y aplicaciones web en él desplegadas estén libres de troyanos, puertas traseras u otros códigos malignos. En Internet están disponibles muchos scripts que pueden ser utilizados por los diseñadores web. No obstante, los scripts descargados de fuentes externas son más susceptibles a presentar problemas de codificación que los creados internamente. Si resultase necesario utilizar fuentes de códigos de programación externas, los diseñadores de administradores deben aplicar comprobaciones de garantía de calidad para buscar llamadas del exterior del sistema, extra códigos y funciones innecesarias. Estos segmentos ocultos de los códigos malignos son denominados *bombas lógicas.*

Una bomba lógica con la que hay que tener cuidado está relacionada con los scripts ISAPI (Internet Server Application Programming Interface). El comando **RevertToSelf()** le permite a la secuencia de comandos ejecutar cualquier comando de seguimiento en un contexto de seguridad a nivel de sistema. En una secuencia de comandos bien diseñada no se debe utilizar nunca este comando. Si está presente este comando, el código ha sido alterado o fue diseñado por un codificador malintencionado o inexpertos. La presencia de ese comando permite que los ataques en un servidor web mediante el envío de determinadas construcciones de sintaxis URL lancen una bomba lógica.

Registro de actividad

La importancia de registrar, auditar o monitorear la actividad del servidor web se incrementa en la medida en que se eleva el valor de los datos en él almacenados. El proceso de monitoreo debe concentrarse en los intentos por realizar acciones que no son normales en un usuario web. Entre estas acciones están:

- intentar ejecutar scripts
- tratar de escribir archivos
- intentar acceder a archivos que están fuera de la raíz web

Mientras mayor sea el tráfico que soporta su servidor web, más difícil será examinar las pistas de auditoria. Es preciso aplicar una solución automatizada cuando el tiempo necesario para examinar los archivos de registro excede el tiempo que tienen disponible para ello los administradores. Los sistemas de detección de intrusión (SDI, o IDS en inglés) son herramientas de monitoreo automatizado que buscan actividad anormal o maligna en los sistemas. Un SDI puede simplemente buscar problemas y notificar a los administradores o repeler activamente los ataques una vez que son detectados.

Copias de seguridad

Lamentablemente, todos los administradores deben presuponer que el servidor web se verá comprometido en algún momento y que los datos hospedados en él serán destruidos, copiados o quedarán corruptos. Esta suposición no siempre se hará realidad, pero estar preparado para lo peor es siempre la mejor práctica de seguridad. Debe estar instalado un mecanismo de copia de seguridad fiable para proteger al servidor de cualquier falla. Esta mecanismo puede ser un servidor réplica en tiempo real como respaldo del servidor web primario o simplemente solo una salva diaria en cinta. De cualquiera de las dos formas, una copia de seguridad es la única garantía de que disponemos para retornar a un estado de operación normal en un período de tiempo razonable. Si la seguridad tiene que ver tanto con el mantenimiento de la disponibilidad como de la confidencialidad, las copias de seguridad deben formar parte de la política de seguridad de cualquier organización.

Mantener la integridad

Bloquear el servidor web es solamente uno de los pasos en el proceso de seguridad. También es necesario hacerlo para mantener la seguridad con el paso del tiempo. Mantener un ambiente seguro exige monitorear el sistema en busca de anomalías, aplicar las nuevas revisiones cuando estén disponibles, y ajustar las configuraciones de seguridad para satisfacer las siempre cambiantes necesidades de la comunidad web interna y externa. Si ocurre una violación de la seguridad, la organización deberá revalorar las decisiones y las medidas de seguridad tomadas anteriormente. Las administraciones quizás hayan pasado por alto una vulnerabilidad de seguridad debido a la ignorancia, o quizá sencillamente no configuraron de manera apropiada algún control de seguridad.

Servidores web villanos

Para un administrador de redes hay algo peor que tener un servidor web sabiendo que no es ciento por ciento seguro, incluso después de haberlo bloqueado, y es tener un servidor web en la red sin saberlo. En ocasiones a estos se les llaman *servidores web villanos* y

pueden presentarse de dos maneras. Es posible que un usuario con conocimientos técnicos en la red haya configurado los servicios web en su computadora. Sin embargo, lo que se presenta más a menudo es que los servidores web villanos se desplieguen de manera no intencional. Muchos sistemas operativos incluyen software de servidores web y los instalan como parte de su instalación predeterminada. Si los administradores no ponen cuidado, cuando instalan Windows (especialmente un miembro de la familia Server) en una computadora en red, podrían crear un nuevo servidor web sin percatarse de haberlo hecho. Cuando un servidor web está presente en una red sin el conocimiento de los administradores de esta, nadie tomará las precauciones necesarias para dar seguridad al sistema. Esto hace que el sistema (y con él toda la red) sea vulnerable a todo tipo de ataque contra ese servidor web.

Valladares contra el delito
A la caza de servidores web villanos
Para verificar un sistema con miras a comprobar si está funcionando un servidor web local sin su conocimiento, puede utilizar un buscador web para acceder a http://localhost/. Si no está activo ningún servidor web, deberá ver entonces un error que le dice que no es posible acceder al servidor web. Si aparece cualquier otro mensaje o una página web (incluido un mensaje que advierta que la página está haciendo elaborada o que está pronta a aparecer), eso quiere decir que existe un servidor web habilitado localmente. Una vez que descubra la existencia de dicho servidor, puede darle seguridad, o eliminarlo, o deshabilitarlo. De lo contrario, el sistema continuará sin protección.

Para comprender la seguridad y los sistemas operativos de Microsoft
Microsoft es uno de los principales proveedores de sistemas operativos para servidores y computadoras de mesa. Casi todos hemos escuchado hablar de Windows o lo hemos utilizado en alguna de sus versiones. Sin embargo, incluso con el amplio empleo de los productos de Microsoft, el historial de seguridad de la compañía no es inmaculado. (Por supuesto, lo mismo se puede decir del resto de los sistemas operativos). Afortunadamente, Microsoft ha iniciado varios programas para mejorar su estructura de seguridad y para ayudar a los usuarios finales a utilizar sus productos de manera más segura.

A fines del 2001, Microsoft lanzó el Programa estratégico para la protección de la tecnología (STTP, por Strategic Technology Protection Program) el cual se concentra en el entrenamiento de los usuarios finales para instalar de manera segura los productos de Microsoft. El STPP ha mejorado los informes sobre temas de seguridad a la comunidad de usuarios y desarrollado sistema de herramientas de seguridad. Este sistema de herramientas incluye todos los paquetes de servicio y soluciones de seguridad, así como

utilidades y documentación de seguridad para Windows NT 4.0 y Windows 2000. Una vez que esté disponible Windows .NET, las herramientas incluirán materiales para él..

A principios de 2002, Microsoft inició su campaña interna llamada Trustworthy Computing (computación fiable). Dicha campaña concentra su atención en la disponibilidad, la seguridad y la privacidad. El objetivo inicial de la compañía es revisar el código de todos sus productos y crear procesos que garanticen una mejor seguridad en los productos y actualizaciones futuras.

Temas generales de seguridad en Microsoft

Antes de analizar temas específicos de la versiones de Windows, es preciso abordar diferentes problemas de seguridad que presenta casi toda, si no toda, la actual línea de productos de Microsoft: Windows 95, Windows 98/SE/Me, Windows NT 4.0, Windows 2000 y Windows XP.

NetBIOS

Sytek desarrolló NetBIOS para IBM a fin de permitir que las computadoras personales se comunicaran por una LAN. Microsoft adoptó el NetBIOS como su primer mecanismo de comunicación intranet (LAN). NetBIOS puede operar muy eficientemente, pero no puede ser enrutado y no ofrece seguridad. Las versiones iniciales de Windows dependían del NetBIOS para la resolución de nombre. Windows XP y Windows 2000 pueden operar sin NetBIOS en un dominio de modo nativo Windows 2000 (utilizando el Directorio Activo), pero NetBIOS sigue habilitado por defecto para garantizar la compatibilidad inversa con los sistemas Windows 9x y Windows NT.

Cuando el NetBIOS es eliminado de un sistema que no tiene soporte ni puede acceder a un dominio de Directorio Activo, dicho sistema pierde la mayor parte de sus capacidades para compartir los recursos. Por esta razón, quizás sea necesario habilitar el NetBIOS en las interfaces de red interna en la mayoría de los sistemas Windows. Cuando se da seguridad a un sistema Windows de Microsoft un paso importante es deshabilitar o desvincular el NetBIOS de toda interfaz Internet o externa. Cuando se tienen dudas, se deben verificar los cambios en un ambiente de laboratorio antes de realizar cambios totales a los sistemas y redes de producción.

Amplia funcionalidad automatizada

A menudo Microsoft es el líder en la innovación en lo que se refiere a características y capacidades presentes en Windows. Lamentablemente, muchas de esas capacidades y características aumentan la posibilidad de utilizar el producto y su conveniencia, pero no ofrecen seguridad o son inherentemente inseguras. Microsoft ha tomado medidas en algunas características para brindar alternativas seguras. Por ejemplo, el sistema de archivos factibles de asegurar NTFS (New Technology File System) está disponible en Windows NT, 2000 y XP. Solamente el sistema FAT (Tabla de Localización de Ficheros) , que es mucho menos seguro, está disponible en sistemas Windows 9x.

Algunas capacidades incluidas en Windows constituyen vulnerabilidades de seguridad considerables difíciles de salvar. Por ejemplo, Windows XP es vulnerable al menos a dos graves problemas de seguridad. Uno está relacionado con la capacidad de Plug and play universal (UPnP) y el otro a los sockets no utilizados. El UPnP fue diseñado para permitir la detección, instalación y configuración automática de dispositivos de hardware, tanto locales como de red. No obstante, el proceso para hacerlo abre puertos de conexión que podría explotar un usuario malintencionado en Internet. Para más información sobre esta vulnerabilidad y para descargar las revisiones, véase el sitio web de Microsoft www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-059.asp.

NOTA

Los sockets no utilizados no son exclusivos de Windows ni de XP. UNIX, VMS, Linux y Mac OS X también tienen esa capacidad. Windows 2000 también la incluye. Una de las razones por las que los sockets no utilizados han merecido tanta atención en el XP es que la versión XP Home Edition está destinada a consumidores individuales, mientras que los demás sistemas operativos son utilizados principalmente en ambientes corporativos. Otra razón es el hecho de que en XP esa capacidad está abierta a todos los usuarios (en Windows 2000 y en los sistemas operativos que no son Windows solamente los administradores tienen acceso a los sockets no utilizados). Esto se convirtió en una cuestión pública tal que en 2001 el estado de Nueva York aprobó una ley prohibiendo el uso de los sockets no utilizados al utilizar Internet (véase www.kumite.com/rsnbrgr/rob/grcspoof/cnn).

Los sockets no utilizados son una característica de la pila del TCP/IP que fue desarrollada inicialmente como una herramienta de búsqueda y no estuvo nunca destinada para sistemas de entorno productivo del mundo real. En esencia, los sockets no utilizados permiten obviar la pila del TCP/IP y conceder acceso a la capa de transporte de datos de la red. Esta capacidad posibilita la interferencia de la dirección IP y sobrecargas SYN (ambos ataques comunes en Internet). Microsoft incluyó los sockets no utilizados en su lista TCP/IP para Windows 2000 y XP, ya que esta característica la utiliza el nuevo cortafuegos de XP para la conexión a Internet. Esta opción originó una oleada de controversias. Para más información sobre los riesgos de seguridad inherentes a los sockets no utilizados, véase el artículo de Steve Gibson en http://grc.com/dos/xpsummary.htm. Para leer la respuesta de Microsoft a las críticas sobre los sockets no utilizados, véase su sitio web en www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/news/raw_sockets.asp.

Estos son dos ejemplos de problemas causados por la adición de características a Windows. Algunos de estos problemas de seguridad originados por las características añadidas han sido solucionados con las revisiones emitidos por Microsoft. Otras requieren soluciones de terceros o el despliegue de un cortafuego para restringir el acceso a los sistemas vulnerables.

Vulnerabilidad IRDP

El Router Discovery Protocol (IRDP) del Protocolo Internet para el control de mensajes (ICMP) se utiliza para detectar y configurar las direcciones de puerta de enlace predeterminadas en los clientes DHCP. Está habilitado por defecto en los clientes DHCP de Windows 9x y está presente pero deshabilitada por defecto en los clientes DHCP de Windows 2000. El IRDP no utiliza ningún tipo de autenticación, de manera que el protocolo es propenso a los ataques. El ataque más común utilizando el IRDP es enviar una entrada de ruta predeterminada a la víctima. Entonces este ataque sirve para facilitar el registro de tráfico (enrutar el tráfico por un sistema que registra cada paquete que pasa por él), ataques de intermediarios (actuando como impostor o un proxy para una conexión segura), y ataques de negación de servicio (enrutar todo el tráfico a direcciones equivocadas).

Este ataque por el IRDP predomina en las conexiones de banda ancha como los módems por cable. Entre las medidas de protección del IRDP están:

- Bloquear los paquetes 9 y 10 tipo ICMP
- Deshabilitar el IRDP mediante el registro (para Windows 95/98, véase el artículo Q216141 en http://support.microsoft.com/default.aspx?scid=kb;EN-US; q216141; para Windows 2000, véase el artículo Q269734 en http://support.microsoft.com/default.aspx?scid=kb;EN-US; q269734)

Asociación NIC

Los sistemas operativos Windows de Microsoft utilizan un mecanismo conocido como *asociación* para asociar servicios y protocolos específicos con interfaces de red particulares. Una interfaz de red puede ser cualquier puerto de entrada o salida de una computadora, incluido un NIC, un módem, o incluso un puerto serie. Por defecto, Windows habilita todas las asociaciones posibles cuando el SO se instala por primera vez y cuando se instala una nueva interfaz o un nuevo servicio o protocolo. Esto se hace para garantizar que todo funcione --es más fácil y conveniente para usuarios menos conocedores que tener que estar resolviendo problemas de comunicación y habilitando las asociaciones correctas. No obstante, también crea vulnerabilidades de seguridad, de manera que cada vez que se efectúe un cambio significativo en un sistema, es preciso reinspeccionar las asociaciones para cerciorarnos de que no se han habilitado asociaciones no deseadas.

Uno de los problemas más comunes que surgen de esta situación ocurre cuando un sistema es conectado a un dispositivo de comunicación de banda ancha por primera vez. Windows asocia automáticamente el TCP/IP a la nueva interfaz, así como el servicio de trabajo en red y los servicios de archivos e impresoras. Esto transforma de hecho un sistema independiente (standalone) en miembro de una red que abarca el resto de los sistemas del segmento de banda ancha local. Esta situación crea un riesgo de seguridad considerable. Para regresar el sistema a una configuración más segura, es preciso deshabilitar las asociaciones para cada servicio y protocolo que no sea el TCP/IP en la nueva interfaz de Internet.

NOTA

Es importante educar a los usuarios en relación con el hecho de que una computadora con conexión a Internet -- incluso con una conexión telefónica analógica estándar-- ha dejado

de ser un sistema verdaderamente independiente; es miembro de una red --la mayor red de todas.

Para dar seguridad a las computadoras con Windows 9x

Para mantener un entorno seguro es necesario utilizar clientes seguros así como servidores seguros. Para las redes que utilizan Windows 9x crear un entorno seguro puede ser difícil, cuando no imposible. Windows 9x estaba destinado a ser un sistema operativo para consumidores individuales (entorno de hogar) e incluye pocos controles y características de seguridad significativos. No obstante, dado que el costo es inferior comparado con los sistemas operativos de clientes de Microsoft orientados a la actividad comercial (NT Workstation y 2000, y XP Profesional), numerosas empresas utilizan equipos con Windows 9x como clientes de computadoras. Para mantener algo de seguridad con los sistemas Windows 9x, es preciso mantener un control absoluto del acceso físico. Si se controla el acceso físico, será posible tener un determinado grado de seguridad en las comunicaciones en línea. A continuación presentamos algunas medidas que deben tomar los administradores después de asegurar físicamente los sistemas:

1. Instalar las revisiones y actualizaciones más recientes de Microsoft.
2. Configurar los sistemas para que utilicen el Inicio de sesión de la familia de Windows. Con esto se restringe el registro solamente a las cuentas de usuario existentes.
3. Configurar el sistema para que no almacene localmente las contraseñas. Por defecto, las contraseñas son guardadas en un caché de contraseñas (un archivo .pwl).
4. Utilizar las Políticas de Sistema para restringir el acceso a las *applets* del Panel de Control, especialmente las utilizadas para instalar nuevos protocolos y servicios o para alterar la configuración del sistema.

Debido a que los sistemas Windows 9x son bastante inseguros, constituyen una opción no muy favorable para los ambientes que manejan información altamente confidencial. En caso de que resulte necesario utilizarlos en esos entornos, los administradores deberán restringir el acceso de los usuarios en estos clientes al mínimo necesario para realizar su trabajo. (En realidad, esta es la mejor política en un ambiente de alta seguridad, independientemente del sistema operativo del cliente). Debemos recordar que Windows 9x utiliza un algoritmo de encriptación no seguro para la autenticación (autenticación de Administrador de LAN) y utiliza solamente el sistema de archivos FAT no seguro. Si en un cliente con Windows 9x se guarda información confidencial, incluso en los archivos de paginación, puede ser extraída fácilmente.

Valladares contra el delito...
Encriptación de datos en computadoras con Windows 9x

Si bien Windows 9x y FAT no soportan EFS, el esquema de encriptación de archivos que utiliza Windows 2000/XP, existen productos de terceros que permiten encriptar los datos almacenados en una computadora con Windows 9x. Entre estos están:

- SecureAction Advanced Encryption Package 2002: www.secureaction.com/encryption_pro
- Cryptainer PE: www.sharewarejunkies.com/02zwd5/cryptainer.htm
- EasyCrypt: www.easycrypt.co.uk

Existen muchos programas *shareware* y *freeware* que permiten la encriptación de archivos en sistemas 9x. Para más información véase www.tucows.com/system/fileencryption95.html.

Si un cliente Windows 9x está desplegado en un dominio con directorio activo Windows 2000, podremos deshabilitar el NetBIOS en el cliente si se instala Active Directory Client Extensions para Windows 95/98. Esta actualización de seguridad puede encontrarse en el CD de Windows 2000 Server y el sitio web de Microsoft (www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp). Este complemento brinda a los sistemas Windows 9x conocimiento del sitio Active Directory, registro en dominio de Windows 2000, interfaces de servicio Active Directory, cliente de sistema de archivo distribuido (Dfs en inglés, por distributed file system), acceso a la Libreta de Direcciones de Windows, y NT Lan Manager (NTLM) v.2. No añade Kerberos, soporte para Política de Grupo, soporte para Intellimirror, IPSec, L2TP, nombre de proveedor de servicio, ni autenticación mutua.

Las medidas que se deben tomar para dar seguridad a un sistema Windows 9x son las siguientes:

- Aplicar el paquete de servicio más reciente y las últimas soluciones de seguridad.
- Deshabilitar el servidor de conexión telefónica para impedir la entrada de intentos de conexión a través de los módems de conexión telefónica o un vínculo Internet.
- Deshabilitar el intercambio de archivos y de impresoras
- desasociar o eliminar los protocolos superfluos
- Utilizar contraseñas robustas.
- Habilitar el inicio de sesión de Familia de Windows.
- No elegir salvar contraseñas, deshabilitar el caché de contraseñas y eliminar el archivo de contraseñas con la extensión .pwl.
- No descargar ni instalar controladores ni software que no estén firmados digitalmente.
- Realizar copias de seguridad regularmente y asegurar los medios para guardar copias de seguridad.
- Instalar y actualizar el software antivirus.
- Utilizar complementos o dispositivos de terceros para elevar la seguridad.

El proceso real de dar seguridad a clientes Windows 9x es aún más detallado. Afortunadamente, Microsoft mantiene una lista de verificación de seguridad útil para clientes Windows 95, 98, 98 SE y Me en www.microsoft.com/Education/?ID=Windows9xSecurity. Se recomienda de manera especial que todos los administradores examinen esta lista de verificación al 3 de instalar Windows 9x en una red productiva en la cual la seguridad sea vital.

Brindar seguridad a una red con Windows NT 4.0

La buena noticia es que Windows NT 4.0 es considerablemente más segura que los sistemas Windows 9x. Windows NT emplea NTLM para proteger la autenticación de registro entrada, que es razonablemente seguro, y soporta el sistema de archivos NTFS, políticas de sistema, política de contraseñas, políticas de derechos de usuario, auditoría, y otras características de seguridad. No obstante, la mala noticia es que Windows NT no está exento de problemas de seguridad. Por ejemplo, todos los sistemas Windows NT tienen dos cuentas usuario bien conocidas: administrador y huésped. Ninguna de estas cuentas puede ser eliminada (si bien la cuenta de huésped puede ser deshabilitada y de hecho lo está por defecto en las estaciones de trabajo NT, no así en el servidor NT). Ambas cuentas predeterminadas pueden ser renombradas; esto debe hacerse inmediatamente después de instalar el sistema operativo. De lo contrario, los hackers tendría ya la mitad de la información (nombre de cuenta de usuario y contraseña) que necesitan para acceder al sistema. Otro problema es que la cuenta de huésped predeterminada tiene asignada por defecto una contraseña en blanco. A estas dos cuentas incorporadas se deben asignar contraseñas robustas, y la cuenta de Huésped debe ser deshabilitada si no es necesaria.

Tal y como se comercializa, Windows NT es vulnerable a cientos de ataques, incluido la delegación de servicio, la elevación de privilegio, y la ejecución de código. Afortunadamente, muchas de estas vulnerabilidades se eliminan aplicando el Service Pack 6a y las soluciones posteriores a él.

Entre las medidas que se deben tomar para dar seguridad a un sistema Windows NT están:

- Formatear todas las particiones con NTFS para permitir que los administradores asignen permisos de acceso a nivel de archivos y aprovechen las ventajas de seguridad que brinda el NTFS.
- Asignar contraseñas robustas a las cuentas de Administrador y Huésped y deshabilitar la cuenta de Huésped cuando no sea necesaria.
- Deshabilitar protocolos y servicios innecesarios (véase el recuadro "En la escena" más adelante en esta sección para ver una lista de servicios que pueden ser deshabilitados).
- Deshabilitar cuentas no necesarias, incluida la cuenta de Huésped.
- Hacer más restrictivos los permisos en los directorios de sistema.
- Impedir el acceso anónimo al Registro.
- Establecer listas de control de acceso (ACL) en el registro.
- Restringir el acceso a la información sobre Autoridad de Seguridad Local (LSA).
- Habilitar SYSKEY para proteger la base de datos del Administrador de Cuenta de Seguridad (SAM), que incluye las contraseñas de cuentas.

- Deshabilitar la autenticación del administrador LAN.
- Programar el archivo de paginación para que vuelva a cero al apagar el sistema.
- Establecer estrictas políticas de contraseñas.
- Establecer una política de bloqueo de cuenta para evitar la entrada de usuarios tras una cantidad razonable de intentos de registro fallidos (tres a cinco) por entrada de contraseña incorrecta.
- Crear señuelos de cuenta de Administrador cambiando el nombre a la verdadera cuenta de Administrador predeterminada por otro inofensivo, y crear una cuenta que se llame Administrador que tenga acceso y privilegios muy restringidos.
- Eliminar el intercambio no necesario de recursos y cambiar los permisos predeterminados (quedan pleno controlar grupo Todos) en intercambios recién creados.
- Utilizar el axioma de "menos privilegiado" en todas las ACL.
- Restringir el acceso a los medios extraíbles solamente a los usuarios interactivos (aquellos que se registran localmente, y estar sentados físicamente frente a computadora).
- Restringir los derechos de usuario. Esto es algo diferente a los permisos; los permisos se asignan para controlar el acceso a recursos individuales como archivos o impresoras, mientras que los derechos de usuario controlan las acciones que pueden realizar los usuarios en todo el sistema, como el derecho a crear intercambios o el derecho a apagar el sistema.
- Configurar la auditoria de seguridad. Muchas actividades pueden ser auditadas, incluidos los intentos de registro, los cambios realizados a las cuentas de usuario/ grupo, apagados del sistema, e incluso el acceso a archivos y objetos individuales. Para auditarlo todo se necesitarían muchos recursos y se generaría un registro de auditoria enorme, difícil de examinar, por lo que es importante decidir cuidadosamente qué sucesos auditar.
- Ocultar el último nombre de usuario al iniciar la sesión. Esto se hace editando el Registro; las instrucciones para hacerlo pueden encontrarse en www.winguides.com/registry/display.php/1..
- Eliminar el acceso a red para todos los usuarios si la máquina es un cliente que no necesita compartir sus recursos. Esto se hace mediante la herramienta de Administrador de Usuarios, editando las políticas de derechos de usuario.
- Mantener un disco de reparación de emergencia (ERD) y mantenerlo en un lugar seguro.
- Realizar copias de seguridad regularmente y mantener seguros los medios de copias de seguridad (incluido el almacenamiento de copias de seguridad fuera de los predios).
- Instalar y mantener actualizado un software antivirus.
- Aplicar los últimos paquetes de servicio y las soluciones más recientes.

Para obtener detalles sobre estos temas de seguridad, véase las listas de verificación de seguridad para Windows NT que mantiene Microsoft. Estas lista de verificación están destinadas a simplificar la tediosa tarea de bloquear despliegues nuevo y existentes de

Windows NT 4.0 Workstation y Server (servidor miembro y controlador de dominio). Estas listas de verificación pueden encontrarse en el sitio web de Microsoft en www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp

En la escena
¿Qué servicios de red se deben deshabilitar?
Algunos servicios NT que pueden presentar vulnerabilidades de seguridad están incluidos en la lista siguiente. Los servicios que no son necesarios se pueden deshabilitar en Servicios, en el Panel de Control:

- servicio alerta
- servidor ClipBook
- buscador de computadora
- cliente DHCP (si el sistema tiene una dirección IP estática)
- replicador de directorio
- servicio de publicación FTP
- servicio administración IIS
- agente de política IPSec
- Messenger
- registro en la red
- DDE de red
- DDE de red: DSDM
- Plug and Play
- localizador de llamada de procedimiento remoto (RPC)
- servicio de registro remoto
- servicio RIP
- servicio RunAs
- servicio servidor
- servicios TCP/IP simples (si están instalados)
- servicio de trampa SNMP
- cola de impresión
- Ayudante de NetBios TCPIP
- servicio de telefonía
- rastreo de cliente
- estación de trabajo
- servicio de publicación de World Wide Web

Algunos de estos servicios son necesarios para conectarla computadora NT aún dominio de Windows 2000, y algunos son necesarios para ciertas aplicaciones, por lo tanto se deshabilitan solamente los que no se utilizan.

ubicado a mitad de página bajo el título Security Checklists).

Dando seguridad a una red de Windows 2000
Windows 2000 es un paso de avance significativo para Microsoft en cuanto a seguridad de sistema operativo. En Windows 2000 existen más características de seguridad que en

todas las versiones anteriores de Windows combinadas. Incluye soporte para Kerberos y tarjetas inteligentes para la autenticación segura, y soporta diferentes servicios de encriptación, como SSL, la PCT (Private Communication Technology), la DPA (Dsitributed Password Authentication), TLS, IPSec, L2TP, y otros, para las comunicaciones seguras. Sin embargo, como el caso de Windows NT, Windows 2000 tiene numerosas fallas de seguridad tal y como se comercializa. Muchas de estas fallas han sido resueltas en paquetes de servicio y soluciones emitidas. De manera que, en este caso también un elemento clave en la seguridad del sistema operativo está en la aplicación de los paquetes de servicio y soluciones más recientes.

Muchas de las características de seguridad de Windows NT que requería la edición de registro se definen ahora como controles de seguridad dentro de la Política de Grupo de Windows 2000. El uso de la Política de Grupo ha simplificado grandemente la gestión de seguridad para las grandes redes a descentralizar los controles de seguridad y los mecanismos de aplicación.

Muchos de los problemas de seguridad de Windows NT, como las ACL no seguras en las carpetas de sistema, están corregidos de Windows 2000. En muchos casos, para bloquear Windows 2000 se necesita menos esfuerzo en el caso de Windows NT.

Las medidas que se deben tomar para dar seguridad a un sistema de Windows 2000 incluyen:

- Formatear todas las particiones con NTFS.
- Asignan contraseñas robustas a las cuentas de Administrador y Huésped.
- Deshabilitar los servicios no necesarios.
- Deshabilitar las cuentas innecesarias, incluida la cuenta de Huésped.
- Establecer ACL en los archivos y carpetas.
- Establecer ACL en el Registro.
- Programar el archivo de paginación para que se ponga en cero al apagar la máquina.
- Establecer estrictas políticas de contraseña.
- Establecer la política de bloqueo de cuenta. Ahora la política de contraseña y de bloqueo se fijan mediante el objeto de Política de Grupo; si la computadora en un miembro de un dominio Windows 2000, la política de dominio sustituyen a la política de seguridad local.
- Crear señuelos de cuenta de Administrador.
- Eliminar el intercambio de recursos innecesarios.
- Utilizar el axioma de "menos privilegiado" en todas las ACL.
- Restringir el acceso a los medios extraíbles solamente a los usuarios interactivos.
- Restringir los derechos de usuario (se fijan mediante la Política de Grupo; como en el caso de las políticas de cuentas y contraseñas, las políticas de dominio sustituyen a las configuraciones locales.
- Configurar la auditoria de seguridad.
- Ocultar el último nombre de usuario al registrarse.
- Realizar copias de seguridad regularmente y mantener seguros los medios de copias de seguridad.
- Instalar y mantener actualizado un software antivirus.

- Aplicar los últimos paquetes de servicio y las soluciones más recientes

Para obtener detalles sobre estos temas de seguridad, véase las listas de verificación de seguridad para Windows 2000 que mantiene Microsoft. Estas listas de verificación están destinadas a simplificar la tediosa tarea de bloquear despliegues nuevos y existentes de Windows 2000 Professional y Server (servidor miembro y controlador de dominio). Estas listas de verificación pueden encontrarse en el sitio web de Microsoft en www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp ubicado a mitad de página bajo el título Security Checklists).

La Agencia de Seguridad Nacional (NSA) brinda un conjunto de directrices para dar seguridad a servidores de Windows NT y Windows 2000. Véase http://nsa2.www.conxion.com/index.html.

Windows .NET: el futuro de seguridad de Windows

Windows .NET promete ser un nuevo avance significativo para Microsoft en lo que se refiere a la seguridad del sistema. Aprovecha las bases de seguridad sentada por Windows 2000 y va más allá. Si bien Windows .NET estaba aún en su versión beta al momento de escribir estas líneas, Microsoft está afirmando que presenta varias mejorías en este nuevo sistema operativo, como por ejemplo:

- El CLR (Common Language Runtime), programa que verifica las firmas digitales, los orígenes de los códigos fuente, y las alteraciones de código para evitar que códigos malignos se ejecuten o impedir los problemas que puedan causar errores de programación o de corrupción.
- LANs inalámbricas y Ethernet seguras mediante la autenticación y la autorización de sistemas y usuarios conectados sobre la base de protocolos IEEE 802.1x.
- Políticas de restricción de software para controlar los software que pueden ser ejecutados en un sistema.
- Una configuración de bloqueo predeterminado para las instalaciones de IIS 6.0.
- Encriptación de la base de datos de Archivos Offline y archivos en la caché
- Un módulo Crypto de modo núcelo conforme a FIPS para facilitar el uso de servicios de encriptación modernos

Debido al hincapié puesto en la seguridad mediante las iniciativas STPP y Trusted Computing de Microsoft, Windows .NET Server va por buen camino de ofrecer un ambiente razonablemente seguro de la manera en que se comercializa. Para más información sobre las características de seguridad de Windows .NET Server véase el sitio web de Microsoft www.microsoft.com/windows.netserver/evaluation/overview/technologies/security.asp.

Para comprender la seguridad y los sistemas operativos UNIX/Linux

Al parecer los sistemas UNIX y Linux son conocidos como más seguros que los sistemas operativos de Windows. Hasta cierto punto, esta reputación podría ser justificada, pero UNIX y Linux tienen un número significativo de vulnerabilidades de seguridad propias de ellos, además de que comparten algunas vulnerabilidades comunes con los sistemas operativos Windows. Debemos recordar que ningún sistema operativo está exento de problemas de seguridad. Dado que UNIX existe desde hace más de 20 años, ya ha sido objeto de numerosos ataques y ciclos de reparación. Por esa razón, sus manifestaciones actuales son por lo general más seguras que muchos sistemas operativos Windows. Linux está basado en una arquitectura UNIX y es un sistema operativo relativamente nuevo (tiene un poco más de diez años; la versión 0.02 fue publicada en 1991). De manera general es más segura que Windows por dos razones: carece de varias de las fallas principales de Windows (como el soporte para NetBIOS) y es un blanco - preferido de los atacantes que prefieren concentrarse en crear ataques para los sistemas operativos

más ampliamente difundidos, lo cual quiere decir Windows. De todas formas, tanto UNIX como Linux siguen presentando problemas de seguridad.

Por ejemplo, el programa de contraseñas que utilizan algunas versiones de UNIX *al parecer* requieren contraseñas algo seguras: es decir, requieren contraseñas que contengan al menos cinco letras (o cuatro caracteres si se incluyen numerales o símbolos). Sin embargo, este requerimiento es una ilusión, porque el programa aceptará una contraseña más corta si el usuario la escribe tres veces, con lo que se obvia este requisito.

Muchos equipos UNIX utilizan cuentas con nombres como *lpq* o *date* que son utilizados para ejecutar comandos simples sin necesidad de que los usuarios se registren. A menudo dichas cuentas tienen contraseñas en blanco y una identificación de usuario de 0, lo que quiere decir que se ejecutan con permisos de súper usuario. Esto es una gran falla de seguridad porque cualquier persona puede utilizar estas cuentas, incluidos los hackers que pudieran reemplazar el comando que supuestamente debe ejecutar la cuenta por uno de sus propios comandos.

Cuando se de la seguridad a un equipo con UNIX o Linux, deben tomarse las medidas siguientes. Este listado no es exhaustivo y no se aplica a toda las versiones de UNIX o Linux:

- Aplicar las actualizaciones y revisiones de seguridad más recientes.
- Utilizar contraseñas robustas.
- Aplicar la expiración de contraseñas.
- Aplicar un archivo de contraseña sombra.
- Eliminar las cuentas no utilizadas y establecer fechas de expiración para las cuentas temporales.
- Deshabilitar las cuentas de huésped no utilizadas.
- Eliminar las cuentas compartidas. Este es un tipo de "cuenta de grupo" que es diferente a los grupos de seguridad que utilizan los sistemas Windows, NetWare y UNIX. Este último contiene cuentas de usuario; la cuenta de grupo compartida UNIX es una única cuenta utilizada por muchas personas diferentes -- a menudo miembro de un equipo de trabajo conjunto en un proyecto particular. En lugar de utilizar cuenta de grupo, la cuenta de usuario debe ser ubicadas en grupos evitando el archivo /etc/group.
- Se debe tener cuidado al aplicar los conceptos de "hosts de confianza". Esto permite a los usuarios designar computadoras host que debe ser consideradas de confianza, de manera que los usuarios no tendrán de escribir una contraseña cada vez que utilícela red. Este sistema puede ser explotado, por lo que la mejor práctica de seguridad es no permitir los hosts de confianza. Si se han de permitir los hosts de confianza, estos deben ser solamente hosts locales; los hosts remotos nunca deben ser de confianza. (Los hosts de confianza aparecen relacionados en el archivo/etc/hosts.equiv).
- Eliminar la designación "segura" de todas las terminales, de manera que la cuenta raíz no pueda registrarse este terminales no seguras, incluso utilizándola contraseña. Los usuarios autorizados podrán continuar utilizando el comando **su** para ser súper usuarios.
- Verificar que esté habilitada la seguridad del NFS. Algunas aplicaciones de UNIX no tienen características de seguridad del NFS habilitadas por defecto,

lo cual quiere decir que cualquier host Internet (incluidos host no confiados) puede acceder a los archivos mediante el NFS.

- No permitir el FTP anónimo a menos que sea necesario.
- No permitir que los shell scripts que tienen los bits de permiso *setuid* y *setgid*. (Para más información sobre estos bits del permiso, véase el recuadro "Los peligros de SetUID y SetGID").
- Establecer el bit fijo en los directorios para impedir que los usuarios corren o renombre los archivos de otros usuarios.
- Establecer permisos de archivos predeterminados de manera que no se conceda acceso de lectura/escritura grupo/todos.
- Proteger contra escritura los archivos de inicio de la cuenta raíz y el directorio de acceso.
- Utiliza solamente aplicaciones o daemons de servicios seguros. Asegurar el NFS, NIS, X Windows, etc. Deshabilitar los comandos **r** si no se utilizan.
- Eliminar los servicios y protocolos innecesarios. Se pueden eliminar los servicios innecesarios editando los archivos /etc/inetd.conf y /etc/rc.conf.
- Registrar todas las conexiones a los servicios de red.
- Impedir la suplantación (*spoofing*) del nombre de host DNS.
- Establecer permisos apropiados en todos los archivos.
- Utilizar el filtrado de paquete.
- Para los registros de entrada remota, utilizar una shell segura en vez de Telnet, FTP, RLOGIN, RSH, etc.
- Para la encriptación de archivos, utilizar programas complementarios que utilicen algoritmos robustos (como 3DES) en lugar del comando **crypt** estándar de UNIX, el cual es fácil de violar.
- Garantizar que los archivos de dispositivos como /dev/kmem, /dev/mem y /dev/drum no puedan ser leídos por todos. La mayoría de los archivos de dispositivos deben estar en la "raíz" usuario.
- Utilizar el comando **who** para determinar quién está registrado en el sistema en este momento. Este comando o muestra los contenidos del archivo /etc/utmp, el cual relaciona el nombre de registro, la terminal, la hora de registro, y el host remoto de cada usuario registrado. Utilizar el comando **last** para mostrar un registro de cada sesión de entrada (incluidas las sesiones FTP) así como el ahora de cada apagado y rearranque. Los scripts /etc/security que se ejecutan a diario se pueden utilizar para monitorear los sucesos relacionados con la seguridad.
- Ejecutar el daemon syslog (syslogd) en modo seguro para impedir la recepción de datagramas UDP falsificados desde otro sistemas..
- Si no está utilizando programa que requieran RPC, deshabilitar el daemon de puerto.
- Sendmail está habilitado por defecto en algunos sistemas UNIX. A paralelo sino necesita. Si está utilizando Sendmail, cerciorarse de que tiene las revisiones más recientes y garantice que los *spammers* no puedan utilizar su sistema para reenviar spam.

En la escena…

Los peligros de SetUID y SetGID

SetUNID y SetGID son programas UNIX que permiten a posprogramas ejecutarse con permisos adicionales que no tiene el usuario que ejecuta el programa. (Por lo general, una aplicación se ejecuta con los mismos permisos que tiene el usuario que la ejecuta). Cuando un programa recibe los permisos que dan SetUID y SetGID, se ejecuta como el usuario o el grupo que posee el archivo de programa. Usualmente esto significa que el programa se ejecuta con los permisos del usuario raíz. La raíz es la cuenta de usuario maestra en un sistema UNIX que tiene pleno control sobre el sistema (similar a la cuenta de Administrador en las computadoras con Windows). Los hackers pueden explotar SetUID y SetGID para acceder a recursos a los que no deberían tener acceso.

Para una explicación detallada de los pasos para bloquear un sistema UNIX o Linux, véase la excelente lista de verificación de UNIX en el sitio web de CERT en www.cert.org/tech_tips/unix_security_checklist2.0.html. Puede encontrarse una buena lista de verificación de Linux en el sitio web de la Universidad de Georgia en www.eits.uga.edu/wsg/security/linuxdetails.html.

Si la interfaz gráfica de X Window es utilizada en los sistemas UNIX, esta debería ser segura. Véase http://ciac.llnl.gov/ciac/documents/ciac2316.html para obtener información sobre cómo dar seguridad a X Window.

Para comprender la seguridad y los sistemas operativos Macintosh

Más del 85% de las computadoras en el mundo utilizan Windows. Del 15% restante, los sistemas Macintosh representan algunos puntos porcentuales. Ello significa que la mayor parte de la actividad maligna en Internet y fuera de ella están concentrados en sistemas que no son Macintosh, de manera que los sistemas Macintosh disfrutan una forma de seguridad no intencional gracias al anonimato. Además, las versiones Macintosh antes del sistema operativo X no tenían una interfaz de línea de comandos fácilmente accesible (o fácil de usar), ni tampoco utilizaban servicios de red estándar con los cuales los hackers estuvieran familiarizados. No obstante, eso no quiere decir que los usuarios de Macintosh puedan dormirse en los laureles de Apple. Los sistemas Macintosh siguen siendo vulnerables en términos de seguridad, en cuanto a ataques como negación de servicio, exploración de puertos, y virus.

Para protegerse de estos ataques es necesario seguir prácticas de seguridad comunes a todos los sistemas operativos, incluidas las siguientes medidas:

- Aplicar las actualizaciones y revisiones de seguridad más recientes.
- Utilizar contraseñas robustas.
- Eliminar las cuentas no utilizadas y establecer fechas de expiración para las cuentas temporales.
- Eliminar los servicios y protocolos no necesarios (editando el archivo inetd.conf o utilizando NetInfo GUI).
- Registrar todas las conexiones a los servicios de red

- Establecer permisos en archivos y carpetas
- Deshabilitar el intercambio de archivos
- Eliminar el intercambio no necesario de recursos
- Configurar la auditoria
- Realizar copias de seguridad regularmente y asegurar los medios para guardar copias de seguridad
- Instalar un software antivirus (Symantec y McAfee producen versiones para OS X) y mantenerlo actualizado
- Utilizar cuentas sin derecho de administración para las actividades no relacionadas con esa actividad
- Utilizar un cortafuego para filtrar el tráfico.

En 2001, Apple publicó el SO X, un nuevo sistema operativo Macintosh. Más que la versión más reciente del sistema operativo de Macintosh en una serie de actualizaciones, el SO X es un sistema operativo con desarrollo totalmente nuevo basado en el SO FreeBSD UNIX. A su implementación del BSD Apple la llama *Darwin* y lo ha hecho un proyecto de código abierto. El SO X es más parecido a UNIX que a SO 8 ó 9. Ello representa un cambio positivo en cuanto a estabilidad y seguridad, pero también significa que los usuarios de Mac se enfrentarán a nuevos problemas de seguridad. Además, muchas utilidades, programas y servicios que anteriormente estaban disponibles solamente en los sistemas UNIX están disponibles para el SO X, o lo estarán pronto. De manera que para garantizar la seguridad a largo plazo del sistema SO X es vital mantener la vigilancia.

El SO X tiene algunas ventajas de seguridad respecto de muchas otras aplicaciones de UNIX. Muchos de sus servicios de red (Telnet, HTTPD, Sendmail, etc.) están deshabilitados por defecto, y la cuenta raíz tiene que ser habilitada antes de poder utilizarse. No obstante, se deben tomar ciertas medidas de seguridad específicas para SO X, entre ellas:

- Deseleccionar la opción "Login automático" en Preferencias de Sistema del panel de Login (en la ficha de la ventana Login) y cerificar que la ventana Login esté configurada para mostrar "campos de entrada de nombre y contraseña", y no una lista de las cuentas de usuarios de la computadora.
- Configurar el refrescador de pantalla para que solicite información de autenticación (por el panel Refrescador de pantallas de Preferencias de Sistema).
- Eliminar los bits de permiso SetUID y SetGID de las utilidades RCP, RDUMP, RRESTORE, RLOGIN y RSH, o eliminar estas utilidades si no se utilizan.
- Revisar los archivos en los directorios heredados (los que ya estaban en una máquina con el Mac SO 9 antes de instalar el SO X) y cambiar los permisos; por defecto, los archivos y carpetas utilizados por el entorno Clásico tienen permisos de lectura y escritura asignadas a todos.
- Actualizar inetd, el "super servidor" que escucha los intentos de conexión a servicios Internet que están en la base de datos NetInfo, a un servicios más seguro como xinetd (freeware disponible en Xindetd.org).

- Configurar el cortafuegos IPFW incluido en el SO X; para una configuración más fácil, instalar Brickhouse, una interfaz gráfica para crear reglas de configuración.
- Utilizar un verificador de integridad de archivos que soporte SO X (como Osiris) para monitorear los cambios en el sistema.

Para comprender la seguridad de las macrocomputadoras (mainframes)
Las macrocomputadoras siguen estando presentes de manera significativa en muchos entornos educacionales y de investigación. Las macrocomputadoras ofrecen una capacidad computacional considerable, controles de acceso estrictos, así como la capacidad para emplear "thin clients" en la configuración de host-terminal. Tradicionalmente, las macrocomputadoras han sido menos vulnerables que las computadoras personales a las violaciones de seguridad, pero eso era cuando el acceso a ellas era solamente mediante las terminales internas. Ahora la conectividad a Internet y la adición de nuevas características (como las capacidades de servidor web y del comercio electrónico) han abierto los sistemas de las macrocomputadoras a muchos de los problemas que agobian a los administradores de las redes de computadoras personales. Para mantener la seguridad de un entorno de microcomputadora, se deben tomar las siguientes medidas:

- Aplicar las actualizaciones y revisiones de seguridad más recientes.
- Utilizar contraseñas robustas.
- Eliminar las cuentas no utilizadas y establecer fechas de expiración para las cuentas temporales.
- Eliminar los servicios y protocolos innecesarios
- Registrar todas las conexiones a los servicios de red
- Establecer permisos en archivos y carpetas
- Configurar la auditoria
- Realizar copias de seguridad regularmente y asegurar los medios para guardar copias de seguridad
- Instalar un software antivirus y mantenerlo actualizado
- Utilizar cuentas sin derecho de administración para las actividades no relacionadas con esa actividad
- Utilizar un cortafuegos para filtrar el tráfico
- Asegure los enlaces entre la macrocomputadora y los clientes remotos.

Para comprender la seguridad inalámbrica
La capacidad de mantener la conexión a la red mientras nos movemos por la oficina, sin estar atados a un cable, ha estado ganando popularidad muy rápidamente. Las tecnologías inalámbricas de trabajo en red existen desde hace casi 10 años, pero ha sido solo recientemente que sus capacidades y rendimiento han comenzado a acercarse a los de las soluciones tradicionales de trabajo en red por cable. Este aumento de la eficacia ha convencido a muchos administradores de red a desplegar esta tecnología simple y de precio razonable. El costo de una NIC inalámbrica ha bajado a menos de $100 y los puertos de acceso cuestan la mitad de ese precio. Ello significa que cualquier persona, incluso los usuarios individuales en sus casas, pueden conectar un puerto en un conector Ethernet en un concentrador, instalar una NIC inalámbrica y tener un servicio de red

inalámbrica totalmente funcional con una configuración mínima o sin cambiar la existente.

Los objetivos de la seguridad inalámbrica son las mismas que las de una red por cable: autenticación de usuarios y computadoras, brindar confidencialidad a los datos y mantener la integridad de estos. Sin embargo, la tecnología inalámbrica representa desafíos especiales porque la señal pasa por ondas aéreas y utiliza radiofrecuencias. Esto hace que la intercepción sea más fácil en una LAN (WLAN) inalámbrica que en una red por cable.

La mayoría de las tecnologías de red inalámbrica están basadas en la norma 802.11b. si bien esta norma en realidad define varios mecanismos de seguridad para proteger el tráfico inalámbrico, existen muchas maneras de pasar por alto esas restricciones. Lamentablemente, los puertos de acceso inalámbrico usualmente están conectados a una red interna detrás del cortafuego. Ello brinda a los usuarios externos que tengan el equipo adecuado casi el mismo tipo de acceso que tendrían si pudieran conectarse a un puerto abierto en el cuarto de conexiones maestras de la empresa.

Una forma de intercepción, llamada *war driving*, se trata de ir manejando sin un destino específico llevando una antena para localizar redes inalámbricas no seguras. Esta actividad se ha convertido en un pasatiempo popular entre los hackers. Lo que resulta alarmante de esta práctica es que cualquier persona puede construir una antena a un costo inferior a $5, y a menudo las antenas artesanales son más sensibles y direccionales que los dispositivos comerciales. Las organizaciones que utilizan soluciones de trabajo en red inalámbrica podrían suponer que las señales se mantienen dentro de su oficina, pero esta suposición no está sustentada en hechos. Las señales que son suficientemente fuertes para pueden ser detectadas a cientos de metros de distancia, incluso en calles laterales y del otro lado de las estructuras que deberían funcionar como bloqueo.

Una vez que un usuario malicioso ha detectado una conexión inalámbrica, es solo cuestión de tiempo para que logre acceder a toda la red o parte de ella. Los hackers pueden husmear los paquetes (packet sniffing), realizar ataques exhaustivos, y emplear otros ataques destinados a obtener información, con el objetivo de detectar debilidades y explotarlas. Afortunadamente, la meta de la mayoría de los que se dedican al *war driving* es interceptar y utilizar gratuitamente las conexiones Internet de alta velocidad de las grandes empresas, y no infiltrarse en la red interna. No obstante, el uso no autorizado de equipos y servicios de una empresa cuesta dinero, tiempo y productividad, de manera que estas acciones no deben considerarse como inocuas.

Hasta tanto existan soluciones para las tecnologías inalámbricas, estas deben ser utilizadas inteligentemente. Una manera común de mejorar la seguridad de las conexiones inalámbricas es utilizar un vínculo VPN en la red inalámbrica. Ello se hace conectando el portal inalámbrico directamente a un servidor VPN que sirva como puerta de enlace para los clientes autorizados y como cortafuegos para los no autorizados. Esta configuración obliga a los sistemas clientes a autenticarse adecuadamente antes de recibir acceso a la red y encripta todos los datos que pasan por el vínculo inalámbrico. Además, elimina el puerto inalámbrico de la red interna, de manera que su tráfico no puede ser interceptado por un husmeador y no es posible acceder directamente a los sistemas internos sin autentificarse en la VPN.

Entre otras opciones para mejorar la seguridad de las tecnologías inalámbricas están las siguientes medidas:

- Aislar de la red interna todos los puntos de acceso inalámbrico. Requerir mecanismos adicionales de autenticación o conexión antes de que se conceda el acceso a la red interna o la puerta de enlace Internet.
- Deshabilitar la transmisión por la red inalámbrica de SSID (Service Set Identifiers). Con ello se deshabilitan muchas de las características de configuración automática para los clientes, pero la configuración manual reduce considerablemente la posibilidad de que usuarios no autorizados logren conectarse.
- Exigir direcciones MAC específicas de tarjetas inalámbricas autorizadas para que puedan establecer la conexión.
- Estar atentos a la existencia de "WLAN villanas", que son puntos de acceso inalámbrico no autorizados creados por los empleados dentro de la compañía para su conveniencia personal. Por ejemplo, un miembro de la firma que desea llevar consigo su laptop a una reunión y mantener la conectividad podría comprar un punto de acceso barato y enchufarlo al conector Ethernet en la oficina, sin percatarse de los riesgos de seguridad que ello entraña.
- Habilitar WEP (Wired Equivalent Privacy, o Privacidad Equivalente a conexión por cable) en el sistema inalámbrico. Si bien tiene algunas fallas de seguridad, WEP brinda cierto grado de seguridad. Por defecto, la mayoría de los sistemas inalámbricos tienen deshabilitado WEP, lo cual deja totalmente vulnerable a la red.

Para más información sobre las vulnerabilidades del trabajo en redes inalámbricas y sobre cómo dar seguridad a este tipo de redes, véanse los sitios web siguientes:

- Security of the WEP algorithm
  www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Security Administrador: *802.11 Wireless Networks: Is Tours Really Safe?*
  www.secadministrator.com/articles/index.cfm?articleid=22147
- Gregory Rehm: *802.11b Homebrew Antenna Shootout, 2/14/2*
  www.turnpoint.net/wireless/has.html
- BBC: *Hacking with a Pringles Tube*
  http://news.bbc.co.uk/hi/english/sci/tech/newsid_1860000/1860241.stm
- Vnunet.com: *Wireless LANs Can Be Secure*
  www.vnunet.com/Features/1131228

Resumen

¿Por qué habría de interesarle todo esto al investigador de delitos informáticos? Solamente si se comprende cómo funciona la seguridad de las computadoras –y cómo a veces no funciona—es posible predecir dónde y cómo ocurrirán los ataques y las intrusiones contra una red, rastrear las acciones de los delincuentes informáticos que entran ilegalmente a los sistemas, recopilar evidencias sobre la base de esas entradas ilegales, y ayudar a las víctimas del delito informático a protegerse de ataques futuros.

La primera medida para impedir el delito informático es asegurar los sistemas y redes de computadora contra los ataques. Ningún sistema puede ser totalmente seguro, pero el objetivo de la seguridad es presentar una barrera suficientemente fuerte para repeler a la mayoría de los atacantes, cuando no a todos. Por lo general, los elementos o temas que se deben abordar para crear un entorno seguro son los mismos para todos los sistemas. No obstante, las especificidades sobre cómo aplicar la política de seguridad y cómo hacer que cambios de seguridad individuales varían entre los sistemas operativos, y tecnologías diferentes como la de banda ancha, sistemas de macrocomputadoras y redes inalámbricas representan retos de seguridad peculiares.

Dada uso extendido de las baratas conexiones de banda ancha de alta velocidad, ha aumentado el número de sistemas privados y profesionales vulnerables a los ataques sostenidos en Internet. Se deben tomar las precauciones de seguridad adecuadas para proteger estas conexiones permanentes contra los ataques desde Internet, incluidas la instalación de un programa antivirus, el uso de contraseñas robustas, deshabilitar el intercambio de archivos e impresoras, y utilizar un cortafuegos.

Al planificar la seguridad, debemos tener en cuenta no solamente el método que utilizamos para conectar nuestro sistema a Internet, sino también los programas de software que empleamos para interactuar con los recursos basados en Internet. Los buscadores web son notoriamente vulnerables a numerosos ataques. No obstante, con un poco de esfuerzo para mantener el software actualizado y configurarlo para obtener la mayor seguridad posible, es posible evitar la mayoría de los ataques comunes.

Al bloquear sistemas individuales, el sistema operativo del sistema determina los pasos que deben darse. Cada SO tiene sus propias vulnerabilidades y soluciones de seguridad. Comprender estas idiosincrasias y mantenerse informados sobre las nuevas revisiones y vulnerabilidades es esencial para prevenir muchos tipos de delitos informáticos.

PREGUNTAS FRECUENTES

Las siguientes preguntas frecuentes, respondidas por los autores de este libro, están destinadas a medir su comprensión de los conceptos presentados en este capítulo y a ayudarlo en la aplicación práctica de estos conceptos. Para que el autor pueda responder sus preguntas sobre este capítulo, sírvase visitar el sitio www.syngress.com/solutions y pinchar en "Ask the Author".

P: ¿Por qué son tan inseguras tantas tecnologías de computación?
R : Lamentablemente, muchas de las tecnologías de computación que se utilizan ampliamente hoy fueron diseñadas hace 20 años o más (por ejemplo, los protocolos TCP/IP y el sistema operativo UNIX). En aquellos momentos, ni siquiera se hablaba del fenómeno de los ataques a redes. Esto es un ejemplo de cómo los creadores o diseñadores de una tecnología o concepto no pudieron comprender el efecto que tendrían sus creaciones en el futuro. Alexander Graham Bell inventó el teléfono, pero él lo concibió como medio para avisar a los destinatarios de telegramas, no como *sustituto* del telégrafo. De la misma manera, muchas tecnologías TI fueron creadas para facilitar las comunicaciones, permitir capacidades o realizar nuevas funciones, pero la seguridad no fue un concepto esencial en su diseño. Actualmente, la mayoría de las tecnologías incluyen un exhaustivo examen y comprobación de la seguridad. No obstante, es probable que hoy se estén pasando por alto cuestiones que adquirirán importancia en el futuro.
P: ¿Cómo puedo mantenerme informado sobre las cuestiones de seguridad que son específicas a un producto, SO o dispositivo de hardware de mi red?
R: Para mantenerse informado, deberá buscar los recursos que contenga la información que desea tener. La mayoría de los proveedores de productos brindan esta información en un sitio web o en boletines. Dedicar tiempo a buscar en el sitio web de un proveedor o incluso buscar en sitios de proveedores utilizando palabras clave como *seguridad* a menudo revela abundante información valiosa. No obstante, no debemos depender solamente de lo que dice un proveedor si queremos una perspectiva imparcial y completa sobre los temas de seguridad relacionados con sus productos. Es preciso procurarnos también información de terceros. Numerosos sitios web, listas de correo y grupos de noticias son respaldados por profesionales de seguridad, grupos de vigilancia industrial, revistas y productos y servicios de seguridad. Al final de este capítulo hay una lista con los nombres de excelentes sitios. Podrá encontrar además otros sitios buscando en la web con palabras clave como *seguridad, vulnerabilidades*, o el nombre de un producto.
P: He escuchado decir que comprender la mentalidad de un hacker o cracker puede ayudar a frustrar sus intentos de infiltrar nuestra red. ¿Cómo puedo lograr esto sin ocasionar un riesgo adicional para mí o mi sistema?
R: De la misma manera que hay numerosas compañías de reputación en Internet que brindan herramientas y utilidades para verificar y mejorar nuestros sistemas, existen también grupos de hackers o crackers. Estos recursos de la comunidad "clandestina" son en ocasiones una colección invaluable de documentación y herramientas que no son posible encontrar en ninguna otra parte, especialmente de sitios comerciales. No obstante, debe tener la precaución de visitar esos sitios únicamente desde un sistema seguro que no esté conectado a su entorno de producción. Si descarga algún material de

esos sitios, tome la precaución adicional de verificar que no contengan virus ni troyanos, antes de trasladar el material a su sistema productivo.
P: ¿Cómo puedo verificar que las barreras de seguridad que he instalado y las revisiones que he aplicado han logrado eliminar las vulnerabilidades de seguridad?
R: La mejor forma de hacerlo es atacar nuestro propio sistema. Ed Tittel, autor de numerosos libros y artículos sobre las TI, y editor técnico de este libro, a menudo dice, "Agrédete a ti mismo, antes de que te agredan". Básicamente, debe emplear los métodos de ataque comunes utilizados por los crackers y hackers para determinar si los ataques logran vulnerar su sistema. Además de realizar ataques manuales contra su propio sistema, puede remitirse a varios sitios web, grupos de servicio y productos que pueden realizar una auditoría de seguridad automatizada y probar su red. Varios de estos sitios están incluidos en la lista de recursos siguiente.

Recursos

- BBC News: *Hacking with a Pringles Tube*
  http://news.bbc.co.uk/hi/english/sci/tech/newsid_1860000/1860241.stm
- CERT: Unix Security Checklist
  www.cert.org/tech_tips/unix_security_checklist2.0.html
- Ciac: *Securing X Window*
  http://ciac.llnl.gov/ciac/documents/ciac2316.html
- Gregory Rehm: *802.11b Homebrew Antenna Shootout, 2/14/2*
  www.turnpoint.net/wireless/has.html
- How Stuff Works: *How DSL Works*
  www.howstuffworks.com/dsl.htm
- Documento de configuración de seguridad de InterSect para Windows 2000
  www.intersectalliance.com/projects/Win2kConfig/index.html
- JavaScript for beginners
  http://polaris.umuc.edu/~mgaylor/Issues.html
- Lista de verificación de Linux, en sitio web de la Universidad de Georgia
  www.eits.uga.edu/wsg/security/linuxdetails.html
- *Security Operations guide for Windows 2000 Server* de Microsoft
  www.microsoft.com/downloads/release.asp?released=37123
- OpenSSH
  www.openssh.com
- SANS Institute
  www.sans.org
- Documentos sobre seguridad de Windows 2000 de SANS
  www. sans.org/infosecFAQ/win2000/standalone.htm
  www. sans.org/infosecFAQ/win2000/ win2000_sec.htm
- Security Administrador: *802.11 Wireless Networks: Is Tours Really Safe?*
  www.secadministrator.com/articles/index.cfm?articleid=22147
  www.secadministrator.com
- Gibson Research: *Shields UPI*
  www.grc.com
- lista de verificación de UNIX, por CERT

www.cert.org/tech_tips/unix_security_checklist2.0.html

- *Wireless LANs Can Be Secure*
  www.vnunet.com/Features/1131228
- *Hack Proofing Your Wireless Network*, por Christian Barnes y colaboradores
  Syngress Publishing, 2002, ISBN 1928994598
- *Configuring Windows 2000 Server Security*, por Thomas Shinder y colaboradores
  Syngress Publishing, 2002, ISBN 1928994024
- Computer Associates' Virus Information Center
  www3.ca.com/virus
- Computer Incident Advisory Capability (CIAC)
  www.ciac.org
- Sitio web de Peter Gutmann sobre debilidades de seguridad
  www.cd.auckland.ac.nz/~pgut001
- Evaluación de los filtros de seguridad
  http://img.cmpnet.com/nc/1201/graphics/f1-detect-results.pdf
- Federal Computer Incident Response Capability (FedCIRC)
  www.fedcirc.gov
- Herramientas gratuitas de Foundstone
  www.foundstone.com/knowledge/freetools.html
- Global Networking & Computing (GNAC)
  http://lists.gnac.net/firewalls
- *Home PC Firewall Guide*
  www.firewallguide.com
- TechWeb/Network Computing: *Hammering Out a Secure Framework*
  www.networkcomputing.com/1101/1101f3.html
- Sistemas de Seguridad de Internet BlackICE, ICEcap, advice
  www.iss.net
- Servicio de Asesoría y Notificación de Seguridad de Microsoft
  www.microsoft.com/security
- Microsoft TechNet
  www.microsoft.com/technet
- Network Associates' CyberCop and Anti-Virus
- HomeNetHelp: *NAT Basis*
  www.homenethelp.com/web/explain/about-NAT.asp
- Seguridad NFR
  www.nfr.net
- Guías de recomendaciones de seguridad de la NSA
  www.nsa.gov
- NTBugTraq
  www.ntbugtraq.com
- Security Toolbox de NTSecurity.nu
  www.ntsecurity.nu/toolbox
- Snort-win32: producto de código abierto (Open Source) para detectar intrusiones

www.snort.org

- Listas de correo sobre seguridad
  http://oliver.efri.hr/~crv/security/mlist/mlist.html
- Security Space: Auditorías de seguridad
  www.securityspace.com/smysecure/index/html
- Simovits Consulting: puertos que utilizan los troyanos
  www.simovits.com/nyheter9902.html
- Somarsoft
  www.somarsoft.com
- Sunbelt Software (lista nt-admin)
  www.sunbelt-software.com
- Norton Anti-Virus de Symantec
  www.symantec.com/avcenter

CAPÍTULO 9

APLICACIÓN DE LAS TÉCNICAS DE DETECCIÓN DEL DELITO INFORMÁTICO

Temas que se analizan en este capítulo:

- Auditoria de seguridad y archivos de registro
- Registros, reportes, alarmas y alertas del cortafuegos
- Sobre los encabezados de los mensajes de correo electrónico
- Rastrear un nombre de dominio o dirección IP
- Sistemas comerciales de detección de intrusión
- Direcciones IP ficticias y otras prácticas antidetección
- Tarros de miel (*honeypots*), panales (*honeynets*) y otros "señuelos" informáticos

- Resumen
- Preguntas frecuentes
- Recursos

Introducción

En el capítulo precedente pasamos nuestra atención del análisis y la explicación del delito informático, quien participa en los delitos, y los fundamentos de seguridad informática y de trabajo en redes para investigar quién participa en contrarrestar las posibles amenazas --es decir, abarcamos varios aspectos y esferas en las que es esencial aplicar la seguridad de sistemas, redes y comunicaciones. Lamentablemente, nuestras medidas de seguridad no siempre funcionarán. Otro elemento importante de los preparativos para repeler las posibles amenazas y riesgos asociados a las fechorías, intrusión o ataques delictivos es estar preparados para hacer frente a las consecuencias del delito informático y comenzar a recopilar la información que se necesitaría para conformar un caso judicial.

Una vez que ha ocurrido un ataque, o se ha comprometido un sistema o una red, es crucial poder filtrarla evidencia de lo que ha sucedido. Desde la perspectiva técnica de la tecnología de la información, ello significa cómo encontrar, reconocer y localizar la evidencia visible del delito informático. Desde la perspectiva de aplicación de la ley, esto significa cómo manejar esa evidencia para que sea admisible en un tribunal llegado, el caso. No obstante, estos papeles tienen cierto grado de solapamiento. Un buen investigador también necesita conocer las peculiaridades técnicas de dónde y cómo se puede obtener la evidencia, para poder conformar el informe sobre el delito y ayudar al fiscal a formular las preguntas a los testigos. Por otro lado, el profesional de las TI debe saber cómo tratar la evidencia para preservar su integridad a los ojos de la ley.

En este capítulo nos concentramos en la primera actividad. Presentamos diversas fuentes y tipos de evidencia posibles que los investigadores pueden recopilar sobre los intentos de delito informático. En algunos casos, la evidencia puede ser recopilada se haya consumado o no el ataque; en otros casos, la evidencia podría obtenerse como subproducto de un ataque exitoso.

Hasta cierto punto, las computadoras y otros dispositivos de red son capaces de registrar información sobre la actividad que ocurre en su interior o que pase por ellos. En los casos en que se necesita evidencia del delito informático cometido, este tipo de información puede ser esencial para conformar exitosamente un caso legal o tomar la decisión de enjuiciar a los responsables. Pero, como sucede con muchos otros aspectos de la seguridad de sistema y redes, es necesario comprender las tecnologías y los programas que deben aplicarse para obtener esa evidencia. También es preciso comprender cómo es esta evidencia, cómo puede interpretarse y que tipos de señales o datos de aviso deben procurarse que podrían ayudar no sólo a documentar que se ha cometido un delito informático, sino que ayudarán a identificar al responsable o los responsables y demostrar ante un jurado que lo cometieron.

Como ya hemos expuesto en otros capítulos anteriores, la falta de la debida diligencia en la protección de los bienes y datos informáticos muchas veces es uno de los factores que contribuyen a que las empresas y organizaciones queden expuestas a pérdidas o daños. Estas pérdidas o daños pueden ocurrir como resultado de un ataque interno (a manos de un empleado, un consultor u otra persona conocedora), o de un atacante externo. También hemos dicho que no exístela seguridad perfecta, de manera que es necesario aceptar que incluso una posibilidad remota de éxito en el ataque, penetración o compromiso significa que debemos ser capaces de vigilar, detectar y reaccionar ante incidentes de seguridad en el momento en que ocurran.

Así, una parte importante de la debida diligencia que se necesita para abordar los temas de seguridad es realizar análisis e investigaciones posteriores para determinar las causas y los responsables, cuando sea posible. Si una empresa decide o no llevar a la justicia un incidente de seguridad no viene al caso. Para la organización y los profesionales de las tecnologías de la información, el valor real de cómo recopilar e interpretar las evidencias del delito informático viene de la capacidad que brinda para mejorar la seguridad después del hecho, para evitar cualquier recurrencia de los ataques o de las circunstancias que permitieron que el ataque llegara a cometerse.

Incluso cuando la empresa u organización decide no llevar a tribunales el intento de ataque o el ataque consumado, la capacidad para recopilar, interpretar y responder a la información inherente a las huellas del ataque es un elemento esencial de un régimen de seguridad adecuado. Por último, es importante comprender que para mantener la seguridad de sistemas y redes es necesario verificar el cumplimiento de la política de seguridad y su funcionamiento para determinar si existen vulnerabilidades reales y posibles.

Esto se debe enfocar como una verificación de la situación y el trabajo de seguridad, que garantiza no sólo que los controles de seguridad aplicados se avengan a los requerimientos de la política de seguridad, sino también para valorar reiteradamente las vulnerabilidades a las nuevas técnicas de ataque. Esto no se diferencia del entrenamiento y la preparación que reciben regularmente los oficiales de policía para hacer frente a los actos de violencia. Incluso si no hubiesen razones para esperar que ocurran situaciones violentas, los oficiales siempre están preparados para si una situación toma un mal cariz, y durante y después de cualquier contacto relacionado con una llamada, los oficiales están constantemente monitoreando la situación. Asimismo, todo profesional de seguridad conocedor sabe que debe chequear regularmente el estado de la red, al menos para cerciorarse de que no ha ocurrido ni esté al ocurrir algo indeseado o inesperado. Esta forma empírica de evaluar la posición de seguridad es esencial para mantener una seguridad estricta en todo momento y es el primer paso de la respuesta ante cualquier incidente.

Auditoria de seguridad y archivos de registro

Un concepto importante en la seguridad de sistema y redes es lo que a menudo se denomina (en inglés) modelo de seguridad AAA, o “tripleA”. En este caso, esta sigla está sujeta a varias interpretaciones, entre ellas:

- Administración, autorización y autenticación (**A**dminitration, **A**uthorization y **A**uthentication)
- Autenticación, autorización y contabilidad (**A**uthentication, **A**uthorization y **A**ccounting)

En este capítulo utilizamos la segunda opción.

La idea que subyace en esta sigla AAA es que una seguridad fuerte descansa sobre un base con tres pilares:

- **Autenticación,** como se analizó exhaustivamente en el Capítulo 7, garantiza que los usuarios, procesos y servicios que pretenden hacer uso de los recursos

del sistema o acceder a sus contenidos den prueba fehaciente de su identidad para entrar a los sistemas y redes.

- **Autorización** (llamada en ocasiones también *control de acceso*) garantiza que las solicitudes de recursos no sean concedidas a menos que los solicitantes tengan no solamente los permisos necesarios para leer o inspeccionar los contenidos de los recursos a los que desean acceder, sino también los permisos explícitos para realizar las operaciones que pretenden realizar en el recurso. Algunas personas podrían recibir acceso de solo-lectura a la información respecto de la cual no tienen permiso de modificación (o de eliminación total), mientras que otros individuos podrían recibir el permiso para modificar o eliminar la información a su albedrío.
- **Contabilidad** se refiere a monitorear y rastrear la actividad del sistema. Algunas empresas u organizaciones asignan un valor monetario a los recursos, uso y acceso de las computadoras. En estos casos, la contabilidad rastrea ese tipo de actividad para evaluar los "cargos" por el uso de servicios de computadora o red sobre la base del consumo real. Sin embargo, desde el punto de vista de la seguridad, la otra forma de monitoreo o rastreo que se realiza dentro del encabezamiento general de contabilidad es la *auditoria*. Igual que el significado formal que tiene en la contabilidad financiera, la auditoria se trata de rastrear el acceso y el uso de los recursos –en este caso, vínculos de comunicación, sistemas, redes y recursos afines, de manera que pueda haber un registro de los recursos. Esta auditoria deposita datos tangibles en diferentes tipos de registros computadorizados para que puedan ser analizados con múltiples fines. Dichos registros son una vital fuente de evidencias para detectar y analizar los delitos informáticos, se hayan consumado o no.

Observemos que tanto la autenticación como la autorización colocan diversos tipos de barreras o controles entre los usuarios (o consumidores) y los recursos que pretenden utilizar. Solamente la contabilidad rastrea lo que realmente sucede en las redes y sistemas que monitorea. Así, la contabilidad –o más propiamente, la auditoria es la actividad esencial que cierra el resquicio entre lo que supuestamente debería suceder desde el punto de vista de la seguridad y lo que realmente ocurre en los sistemas y redes a los que se aplican los controles de autenticación y autorización.

La auditoria es una capacidad incorporada en la mayoría de los sistemas operativos de computadora y dispositivo de red. No obstante, como la creación de rastros de auditoria implica generar archivos en los que se almacenan registros de actividad, la auditoria por lo general se considera como una forma discrecional de rastreo y monitoreo, más que algo que debe ser aplicado a todas las actividades de los usuarios y el acceso a los recursos. Un buen principio general que se debe aplicar en el momento de decidir si se auditan o no determinados tipos de actividad o acceso a recursos específicos está basado en una valoración cuidadosa de los riesgos que ello entraña. En otras palabras, es de sabios auditar en busca de actividades potencialmente dañinas o peligrosas y del acceso a los archivos sensibles y otros recursos de similar índole. No obstante, también es importante reconocer que auditarlo todo es algo tan impráctico como no auditar nada. Estas exhortaciones generales tendrán más sentido si analizamos la forma en que determinados sistemas operativos manejan la auditoria y los tipos de actividad y acceso

que puede rastrear y monitorear. Después de dicho análisis, podemos presentar elementos más generales sobre la auditoria y las huellas que deja (generalmente denominados *archivos de registro* o *registros*) con un poco más de especificidad y precisión.

La auditoria en las plataformas Windows

Comenzando con las primeras versiones de Windows NT, todas las instalaciones de los sistemas operativos Windows con base comercial (NT, 2000, XP, etc., excluyendo no obstante a Windows 9x/ME) mantienen tres registros de auditoria para rastrear la actividad del sistema y los usuarios. Estos registros se pueden visualizar usando la utilidad Visor de Sucesos incorporado:

- **Registro de Aplicación:** muestra mensajes, información de estado, y sucesos reportados desde las aplicaciones y servicios no esenciales en la computadora con sistema Windows. (Obsérvese que algunos servicios de sistema escriben en este registro y no al registro del Sistema).
- **Registro de Sistema:** registra errores, avisos y sucesos de información generados por el sistema operativo Windows así como por servicios del sistema central conexos.
- **Registro de Seguridad:** muestra los registros de aciertos y errores de actividades auditadas. Cuando se habilita la auditoria y se establecen directivas o configuraciones de auditoria específicas en Windows, es en este registro donde aparecen.

Por supuesto, el último de estos registros es evidentemente el más importante a nuestros objetivos, si bien los investigadores no deberían ignorar los dos primeros. A partir de los registros de Aplicación y Sistema se puede obtener también información importante, como el inicio y la terminación del uso de un servicio o el comportamiento anormal de una aplicación.

NOTA

El Visor de Sucesos puede mostrar otros registros, además de los de Aplicación, Sistemas y Seguridad, si hay determinados servicios ejecutados (como Directorio Activo y servicios de servidor DNS).

La ejecución del Visor de Sucesos varía según la plataforma pero por lo general se puede encontrar en el menú de Herramientas de Administración (Windows NT, 2000, XP y .NET Server) o mediante la MMC (Consola de administración de Microsoft, en Windows 2000, XP, y .NET Server). El Visor de Sucesos es un buen punto de partida para investigar la actividad y sistema anormal o inusual y para monitorear la actividad del sistema en general.

En Windows 2000, los *objetos de directiva de grupo,* o GPO, controlan el nivel de la auditoria realizada por el sistema operativo; en Windows NT es necesario habilitar la auditoria en el menú Directiva de Auditoria en la herramienta de administración Administrador de Usuarios para Dominios. De cualquier forma, solamente quienes hayan entrado al sistema o a una cuenta con permisos de administración pueden habilitar la auditoria o establecer directivas de auditoria. Por defecto, Windows no habilita la

auditoria de seguridad; por lo tanto, por defecto, el registro de sucesos de Seguridad no contiene datos. Para habilitar la auditoria, simplemente se crea un objeto de directiva de grupo y se configura para que monitoree el acierto o el error de una o más clases de sucesos definidos (Windows 2000 o versión posterior) o se utiliza el Administrador de Usuarios para Dominios para habilitar la auditoria y establecer directivas de auditoria explícitas. Para Windows 2000, se pueden auditar las siguientes nueve clases de sucesos o actividades:

- **Sucesos de ingreso a cuentas:** se utiliza para monitorear la actividad de ingreso a las cuentas de usuario.
- **Administración de cuentas**: **se** utiliza para monitorear las actividades de administración de la cuenta administrativa (crear, eliminar, habilitar o modificar configuraciones de cuentas).
- **Acceso al servicio de directorio**: se utiliza para monitorear el uso de los servicios y objetos del Directorio Activo.
- **Sucesos de inicio de sesión**: se utiliza para monitorear todos los sucesos de inicio de sesión en las cuenta de sistema, cuentas de servicio y cuentas de usuario (en otras palabras, un súper conjunto de sucesos de ingreso a cuentas).
- **Acceso a objetos**: se utiliza para habilitar la auditoria de archivos, carpetas, impresoras u otros recursos individuales de la computadora (que también deben estar configurados para auditarse individualmente y por separado).
- **Cambio de directiva**: se utiliza para monitorear la creación, eliminación o modificación de objetos de directiva de grupo. Con ello se rastrean actividades administrativas importantes en los sistemas de Windows.
- **Uso de privilegios**: se utiliza para monitorear el uso de los privilegios de usuario y de administrador en un sistema Windows. También rastrea actividades de administración importantes en los sistemas Windows, así como el uso de privilegios de usuario y propietario/creador de objeto.
- **Rastreo de procesos**: se utiliza para monitorear la creación, los subprocesos y la eliminación de procesos. Muy pocas veces se utiliza con fines de seguridad (pero podría ser útil en ocasiones).
- **Sucesos de sistema: se** utiliza para monitorear las actividades del sistema operativo. También se utiliza en raras ocasiones a los fines de seguridad.

En la figura 9.1 se muestra un registro de seguridad del servidor Windows 2000 abierto en el Visor de Sucesos. Obsérvese que se han auditado aciertos y un error de inicio de sesión.

La profunda interrelación entre la auditoria y el rendimiento del sistema se manifiesta al menos de dos formas:

- Mientras más objetos y actividades se auditen, mayor será el impacto de la recopilación y el registro de esos datos en el rendimiento del sistema y en el consumo del espacio de disco (porque todas las actividades auditadas se escriben a archivos en disco).
- Mientras más objetos y actividades se auditen, mayor será la cantidad de datos que los administradores y los investigadores tendrán que analizar para encontrar algo de interés entre los sucesos o actividades de rutina o benignas que también se registrarán.

No obstante, si se recopila una gran cantidad de datos, no todo está perdido. El

Visor de Sucesos se puede configurar para filtrar todos los eventos registrados de manera que solamente determinados tipos de sucesos (por ejemplo, solamente los errores) o solamente los sucesos que tienen un origen, usuario o computadora específica se muestren en el registro. Otras opciones serían mostrar solamente los sucesos ocurridos en una fecha y/u hora específica o dentro de un período determinado, o sucesos en una categoría específica o los que están marcados con una identidad de suceso concreta. La Figura 9.2 muestra el cuadro de diálogo que se utiliza para configurar el filtrado de lo que aparecerá en pantalla.

Figura 9.1 El registro de Seguridad de Windows 2000 muestra los tipos de sucesos para los cuales se ha habilitado la auditoria.
(Aquí se inserta la primera imagen que aparece en la página 506)

Figura 9.2 Es posible filtrar los registros del Visor de Sucesos para que muestre solamente sucesos específicos.
(Aquí se inserta la segunda imagen que aparece en la página 506)

Para obtener una excelente información sobre la auditoria de los sistemas de Windows desde la perspectiva de Windows XP, sírvase consultar la siguiente referencia de TechNet: www.microsoft.com/TechNet/prodtechnot/winxppro/proddocs/ Audit_overview.asp (*Auditing Security Events Overview).* Para obtener información sobre la obtención y el análisis de los registros de otras aplicaciones de Windows, véase www.microsoft.com/TechNet/itsolutions/ecommerce/maintain/monitor/logcanda.asp (*Log capture and Analysis).*

En la escena…

Para definir una estrategia de auditoria efectiva

En última instancia, lo que el administrador informático decida auditar depende de los tipos de actividad que ocurran en el servidor o dispositivo de que se trate, los tipos de ataques o intrusiones que se prevén, y los tipos de información u otros bienes que la organización pretende monitorear (y proteger). Así, tendría quizás sentido auditar firmas de intrusión específicas en la periferia de la red (en cortafuegos, enrutadores de selección, puertas de enlace de aplicación, etc.). Pero en los servidores que guardan archivos sensibles, probablemente tenga sentido auditar el acceso a esos ficheros, incluidos los aciertos y los errores en los accesos. En general, también es conveniente monitorear actividades administrativas en todos esos dispositivos (y anunciar esa directiva) para que los profesionales de la informática sepan que se les pedirá cuentas de todas las actividades administrativas oficiales (y no autorizadas) que realicen.

En algunas situaciones –quizás cuando exista la posibilidad de que se comprometa una cuenta– podría ser conveniente deshabilitar esa cuenta (y crear una nueva para el usuario de dicha cuenta) y auditar entonces los intentos sucesivos de utilizar la vieja cuenta. Esta práctica permite a los administradores determinar si esa actividad se origina dentro o fuera del perímetro de la red local y puede ayudar a determinar la identidad del intruso.

El principio general es auditar en busca de actividades sospechosas, rastrear la actividad administrativa y monitorear la información o bienes de valor o interés conocido. Al combinar estas actividades en la estrategia de auditoria, es fácil lograr el equilibrio correcto entre el volumen de datos auditados y la cantidad de información útil que se puede discernir de esos datos.

Auditoria para plataformas UNIX y Linux

Cada distribución y versión diferente de UNIX y Linux registra información de auditoria crítica de una forma particular y almacena los archivos resultantes en ubicaciones específicas utilizando formatos según la plataforma. No obstante, la mayoría de los sistemas operativos UNIX y Linux soportan amplias capacidades de auditoria y tienen numerosas características comunes.

El daemon Syslog (syslogd) es un centro de intercambio de información para todos los tipos de información de registro en sistemas UNIX y Linux. El daemon es un proceso que desvía mensajes de sistema diferentes a archivos de registro diferentes, en dependencia del tipo de mensaje y de su urgencia y severidad. Por ejemplo, en un sistema FreeBSD, los aciertos y errores en el inicio de sesión FTP se muestran en el archivo ftp.log, la información sobre el acceso a los sitios de Apache Web se almacena en access_log y la información sobre los errores en el inicio de sesión se almacenan en secure.log.

La mayoría de las redes que incorporan los sistemas UNIX y Linux también establecen unidades de red especiales para salvar los datos de registro, de manera que todos residan en un sitio único centralizado. Además, el daemon Syslog recibe datos de sucesos de diversos sistemas operativos y aplicaciones de usuario (véase la Tabla 9.1); también almacena todos los datos de registro utilizando un formato único normalizado para su fácil interpretación y análisis. (Lamentablemente, la misma coherencia no existe

en todos los registros de los sistemas Windows, en los que el Visor de Sucesos utiliza un formato para sus registros, mientras que otras aplicaciones y servicios utilizan otros).

De hecho, Syslog hasta jerarquiza los mensajes de sucesos o error según un esquema predeterminado (véase la Tabla 9.2). Los mensajes de mayor prioridad aparecen al inicio de la tabla, mientras los que son menos prioritarios aparecen al final.

Como se ha dicho con anterioridad, archivos de registro específicos de UNIX o Linux almacenan tipos de sucesos o información específicos. Así, el *loginlog* registra errores en el inicio de sesión, mientras que *sulog* registra la actividad del comando **su** (súper usuario) en un sistema específico e identifica la cuenta de usuario en la que se originó la actividad. El registro *utmp* identifica a todos los usuarios que están activos en el sistema, mientras que el registro *wtmp* almacena instantáneas de la información de *utmp* a intervalos regulares. Estos son solo algunos de los muchos archivos de registro que existen en la mayoría de los sistemas Linux y UNIX; sírvase consultar la documentación de su sistema y las páginas *man* para una lista completa de las facilidades de registro, los formatos utilizados y las ubicaciones de almacenamiento (predeterminadas).

Tabla 9.1 Facilidades comunes de syslog

Facilidad	**Descripción**
Auth	Sistemas de autorización (por ej., *login* y *su*)
Cron	El daemon *cron* mueve las secuencias de comandos y los comandos programados y los ejecuta en consecuencia
Daemon	Distintos tipos de daemon no cubiertos por otras facilidades
Kern	Abreviatura de *system kernel* (núcleo de sistema) –el código de núcleo del sistema operativo residente en memoria
local0-local7	Reservado para uso local (numerado de 0 a 7)
Lpr	Sistema de cola de impresión (de impresora remota en línea)
Mark	Servicio de sello de tiempo que emite un sello de tiempo para el registro cada 20 minutos (1200 segundos)
Mail	Sistema de correo electrónico
Syslog	Datos internos de *syslog*

Tabla 9.2 Prioridades de syslog

Prioridad	Descripción
Emerg	Situaciones de pánico transmitidas a todos los usuarios
Alert	Situaciones que requieren intervención inmediata
Crit	Errores críticos, como fallos de un dispositivo
Err	Errores de prioridad normal
Warning	Mensajes de aviso
Notice	Notificaciones que podrían requerir acción o respuesta inmediata
Info	Mensajes informativos
Debug	Muestra los mensajes escritos a Syslog cuando los programas se ejecutan en modo de depuración

Para una excelente reseña básica de la facilidad Syslog de UNIX, véase www.la.utexas.edu/lab/software/lib/gnu/glibc/libc_377.html#SEC380. Además, la sala de lectura (Reading Room) del SANS Institute ofrece numerosos documentos sobre los registros de Syslog y UNIX , incluido el documento *Unix Security Logging* (18 de abril de 2001) de Ray McAlarnen. Utilice el buscador del sitio; para visitar este sitio de documentos y recursos de seguridad en línea se necesita tener una cuenta y su contraseña, pero es gratuita su obtención.

El OS X de Macintosh es un sistema operativo con base de UNIX y el daemon Syslog funciona como se explicó anteriormente. El OS X facilita el acceso de los administradores a los archivos de registro de UNIX mediante la aplicación Consola (que se encuentra en la subcarpeta Utilidades en la carpeta Aplicaciones del disco duro Mac). Los registros de seguridad y otros de importancia se encuentran en la carpeta /private/var/log, que está oculta por defecto pero a la que se puede acceder con la función **Ir a la carpeta** en el menú **Ir** (véase la Figura 9.3).

Figura 9.3 Los registros de seguridad y otros se almacenan en la carpeta /private/var/log en el sistema OS X de Macintosh
(Aquí se inserta la imagen que aparece en la página 510)

Registros, reportes, alarmas y alertas del cortafuego

En el capítulo 7 analizamos la función de los cortafuegos y el papel que desempeña en un plan de seguridad de redes. Como los cortafuegos están ubicados en la frontera entre las redes internas y externas, esta localización es ideal para observar el tráfico de entrada (y de salida). En consecuencia, no es de extrañar que los cortafuegos no solo representen una primera línea de defensa importante contra los ataques, sino que también puedan ser

configurados para monitorear y rastrear actividades que pudieran ser señales del inicio de un ataque. A menos que los atacantes tengan conocimientos suficientes para borrar los archivos (y, por desgracia, muchos son en realidad suficientemente inteligentes para hacerlo), los registros de los cortafuegos también pueden contribuir a documentar los ataques acertados o fallidos. La mayoría de los dispositivos periféricos, que incluyen no solo a los cortafuegos sino también a enrutadores, puertas de enlace, servidores proxy, etc., pueden -- y, de hecho, deberían-- registrarse siempre diferentes tipos de actividad. Dado que dichos registros pueden ser fuente de información muy importante cuando se necesita una evidencia contundente, ese tipo de dispositivos registran una gran diversidad de tráfico y distintos tipos de actividad.

Como son muchos los dispositivos de esta índole que están basados en entornos UNIX o similares, la buena noticia es que la misma información que presentamos en la sección anterior sobre la facilidad Syslog y las técnicas generales de registro en Linux y UNIX se aplica a menudo a los cortafuegos, enrutadores y otros dispositivos. Por ejemplo, si bien los dispositivos Cisco operan con un sistema operativo propiedad de Cisco, conocido como *Sistema Operativo de Internet o IOS* (por sus siglas en inglés) este entorno de programa utiliza una implementación de Syslog razonablemente estándar para respaldar sus capacidades de registro. Teniendo en cuenta que los detalles de bajo nivel varían entre sistemas de implementaciones, lo que presentamos de manera general sobre las facilidades y la operación de registro es aplicable a muchos (cuando no a todos) los dispositivos periféricos en amplio uso.

NOTA

Existen software complementario que pueden monitorear y analizar los registros de cortafuegos. Por ejemplo, *firelogd* es un daemon que monitorea los registros del cortafuego de Linux. *Fwanalog* es un manuscrito de instrucciones que decodifica y resume los archivos del registro del cortafuego en sistemas UNIX y Linux. El *XP Firewall Reporter* es un paquete de software comercial que analiza los archivos creados por el cortafuego "personal" incorporado en el sistema Windows XP. El Zoelog Analyzer importa los registros de los cortafuegos de ZoneAlarm en una base de datos fácil de revisar. Web Trends tiene un Firewall Suite que procesa los archivos de registro de los cortafuegos del Servidores ISA de Microsoft, de Check Point y Cisco, entre otros. (Para obtener información adicional sobre Firewall Suite, véase www.extralan.co.uk/products/diagnostic-tools/webtrends/webtrens.htm).

Para los cortafuegos y otros dispositivos periféricos, el registro es sólo una de las formas en que pueden brindar información sobre la actividad y el tráfico que manejan. Los cortafuegos (y otros dispositivos perimétricos) de hecho sí crean archivos de registro, en los que es posible escribir todo tipo de datos y almacenarlos por mucho tiempo. No obstante, estos dispositivos también soportan varios otros productos:

- **Alarmas** Se puede dar instrucciones a estos sistemas para que emitan mensajes de alta prioridad en caso de que ocurran actividades o sucesos especialmente sospechosos. Muchos de estos sistemas pueden enviar mensajes de correo electrónico a destinatarios específicos e incluso llamar a

números de teléfono designados, además de registrar información cuando ocurren sucesos determinados. Esta funcionalidad permite que estos sistemas provoquen respuestas inmediatas por parte de personas responsables. Dado que los enrutadores, cortafuegos y otros dispositivos perimétricos pueden estar sujetos a acciones de ping excesivas u otros ataques desde DoS, y debido a que pueden experimentar reiterados errores de inicio de sesión que también pueden ser una señal de que se ha iniciado un ataque, en ocasiones es esencial tomar medidas inmediatas ante tales sucesos.

- **Alertas** Algunos tipos de actividad de tráfico son un síntoma menos evidente de ataque pero se deben tener en cuenta. Ello explica por qué tantos sistemas perimétricos también pueden emitir alertas en caso de que ocurran condiciones particulares. Si bien estos alertas también pueden dar lugar a un mensaje de correo electrónico o avisos telefónicos, por lo general son menos urgentes que las alarmas.
- **Informes** Si bien los sucesos que deben informarse están dentro de una categoría más mundana de categorización de tráfico, actividad, errores e inicios de sesión fallidos u otros intentos de acceso, la mayoría de los dispositivos perimétricos también pueden informar otros comportamientos y estadísticas durante un período de tiempo específico (a diario, semanalmente, mensualmente, etc.). Estos informes son indicadores importantes de la salud y la seguridad general del sistema y se les debe consultar regularmente en el marco del proceso de monitoreo de seguridad y mantenimiento.

De hecho, la mayoría de los sistemas operativos tienen algún tipo de facilidad de alarma. Por ejemplo, las versiones de Windows NT/ 2000/XP/.NET de Microsoft soportan alertas de sistema (configurados por medio del Monitor de sistema en la herramienta administrativa Rendimiento) para alertar a los administradores sobre el rendimiento del sistema o sucesos de errores. Aunque el Visor de Sucesos no ofrece la posibilidad de configurar alertas cuando ocurre un suceso de seguridad, algún software de terceros como IPSentry (www.ipsentry.com) monitorea los registros de sucesos de Windows y envían alertas cuando ocurren sucesos detonadores.

En lo que respecta al trabajo con los registros de cortafuegos (o respuestas a alarmas o alertas conexas), algunos de los tipos más comunes de información que encontraremos se relacionan directamente, ataques y fallas que documentamos en otras partes de este libro. Así, no debería sorprendernos que los siguientes tipos de actividad o tráfico pudieran ser dignos de observarse desde el punto de vista de detección de un ataque o con posterioridad a este:

- **Tráfico ICMP** Exceso de solicitudes de ping, exploraciones ping, solicitudes de eco a la dirección de emisión, paquetes de tiempo de ICMP excedido, golpes de respuesta eco ICMP distribuidas.
- **Comportamiento de exploración regular, sistemática** Exploración del rango de dirección IP, exploración de los puertos TCP/UDP, exploraciones de los nombres de NetBIOS.
- **Intentos para acceder a direcciones de puerto específicas bien conocidas** entre estas están direcciones asociadas con software de acceso remoto (pcAnywhere, Back Orifice, etc.), mensajería instantánea, o aplicaciones de

troyanos específicos.

De hecho, cualquier tipo de tráfico o patrón de actividad -- conocido de otra forma como *firma de ataque*, o más simplemente como *firma*-- que puede ser asociado directamente con un tipo o método específico de ataque representa sucesos que deben ser registrados de ser posible. A veces reconocer una firma entraña obtener una cantidad mayor de información de lo que pudiera poseer un dispositivo típico de perímetro como un cortafuego. Por esa razón, regresaremos a este tema más adelante cuando analicemos una clase de sistemas conocido como *sistemas de detección de intrusión* o IDS (por sus siglas en inglés) que son producidos expresamente con este tipo de capacidad.

En cuanto al tipo de información que se puede encontrar en un registro de cortafuegos, usualmente consiste en registros de texto bastante simple que documentan los diferentes aspectos del tráfico de la red. Si bien en este caso también los detalles variarán en cierta medida, ningún registro estará completo si no incluye al menos la información siguiente (y usualmente más de lo que aparece en esta lista deliberadamente breve de campos de registro comunes):

- **Marca de fecha** Fecha y hora en que ocurrieron sucesos, actividades o comunicaciones.
- **Dirección de origen** Dirección IP reportada para el origen del tráfico.
- **Nombre de dominio de origen (si existiera)** Nombre de dominio reportado para el origen de tráfico.
- **Dirección de destino** Dirección de destino del tráfico.
- **Protocolo** Nombre de protocolo o servicio IP utilizado.
- **Tipo o clase de mensaje (cuando proceda)** Tipo de mensaje que se envía.
- **Dirección de puerto (cuando proceda)** Puerto TCP o UDP al que se dirige el mensaje.
- **Dirección de socket (cuando proceda)** Dirección de socket al que se dirige el mensaje.

En algunos casos, las entradas de registro también incluyen lo que se denomina *búsqueda inversa de DNS* o *seguimiento*. Algunos dispositivos perimétricos pueden configurarse para que verifiquen la dirección IP oficial asociada con nombres de dominio reportados para el tráfico de entrada frente a la dirección IP real incluida en el tráfico de ingreso. Cuando estos dos valores son diferentes, podemos asumirlo como un indicador claro de suplantación, lo que a su vez podría significar que se ha iniciado una actividad sospechosa, cuando no un ataque directo. Este tipo de detección por lo general lanza un alerta o una alarma.

Algunos productos cortafuegos, como el Servidor ISA de Microsoft, brindan una interfaz GUI amigable para configurar los registros y las alertas, como se muestra en la Figura 9.4.

El Servidor ISA facilita la configuración de las alertas de seguridad. El Asistente de Alerta Nueva se ejecuta accionando el botón derecho del ratón en **Alertas** en el nodo de **Configuración de Monitoreo** y seleccionando **Nueva** del menú. El Asistente nos guía por los pasos que se deben dar para establecer las alertas. Los administradores pueden seleccionar que se emiten alertas ante todas las detecciones de intrusión o escoger el tipo de detección específicos para los cuales desearían recibir alertas, como se muestra

en la Figura 9.5.

Figura 9.4 El cortafuegos del Servidor ISA utiliza la interfaz de la Consola de Administración de Microsoft (MMC, Microsoft Management Console) (Insertar aquí la figura que aparece en la página 514 del original).

Configurar los registros en el Servidor ISA también es muy fácil. Los registros se configuran mediante el nodo de Configuración de Monitoreo en la MMC (la carpeta de Registros). Se puede establecer una configuración para que se generen registros sobre una base diaria, semanal, mensual o anual, y estos pueden ser almacenados en un archivo o registrados directamente en una base de datos específicos. De manera predeterminada, los archivos de registro del ISA son almacenados en una carpeta llamada ISALogs ubicada en la carpeta de instalación de ISA (llamada por defecto Microsoft ISA Server y ubicada en el directorio de Archivos de programa en la partición donde se almacenan los archivos operativos de Windows 2000/.NET).

Los registros se pueden salvar en archivos de texto delimitados por comas, los cuales a su vez pueden ser importados en hojas de cálculo como las de Excel o a un programa de base de datos como Access. En la Figura 9.6 se muestra un ejemplo de archivo de registro del Servidor ISA.

Figura 9.5 Es fácil configurar las alertas del Servidor ISA para que emitan avisos de intrusión y otros sucesos. (Insertar aquí la primera figura que aparece en la página 515 del original).

Figura 9.6 **E**l Servidor ISA puede registrar sucesos en archivos de texto delimitados por comas. (Insertar aquí la segunda figura que aparece en la página 515 del original).

En el archivo que se muestra en la Figura 9.6 puede verse en las primeras tres columnas la fecha y la hora de los intentos de intrusión reiterados, así como la dirección IP del intruso. En la siguiente columna se muestra que el intruso intentó con diferentes direcciones IP de destino (64.90.59.35, después 64.90.59.36, después 64.90.59.37) en el puerto TCP 80, como se muestra en las columnas quinta y séptima. (En la sexta columna aparece el puerto utilizado en la computadora de origen). El intruso envió un paquete TCP SYN para tratar de establecer conexión, como se muestra en la columna 8; no obstante, el puerto 80 no estaba "escuchando" (abierto y en espera de una conexión) en ninguna de esas direcciones IP (indicado por la palabra BLOCKED en la columna 9). El último campo muestra la dirección IP primaria vinculada a la interfaz física que estaba siendo sondeada. (Estos sistemas tienen múltiples direcciones IP vinculadas a una misma tarjeta de red, desde la 64.90.59.34 hasta la 64.90.59.37).

Otro archivo de registro de ISA, que se muestra en la Figura 9.7, muestra el intento de un intruso por acceder a los archivos de una computadora mediante el servidor Web, utilizando su dirección IP (64.90.59.34). Podemos observar que todos estos intentos se originaron de la computadora del mismo intruso que estaba tratando de establecer conexión como se ve en el registro anterior. Los dos accesos Web registrados que utilizan el URL www.tacteam.net son legítimos. Los intentos desde la dirección IP 212.235.54.99 fueron negados por el Servidor ISA.

Figura 9.7 Otro registro del Servidor ISA muestra numerosos intentos por acceder a los archivos almacenados en la computadora. (Insertar aquí la figura que aparece en la pág. 516 del original).

Para obtener una explicación y análisis interesante de los datos de registro de un cortafuego, puede visitar los análisis de Lenny Zeltser en los archivos SANS en www.incidents.org/archives/y2k/123199-1220.htm. Haga la búsqueda del nombre de Zektser para ir directamente a la parte del archivo que contiene los análisis pertinentes. Matthew Tam también creó una presentación en PowerPoint para Professional Information Security Association (PISA) sobre la configuración de un cortafuego Linux que abarca los detalles referidos al filtrado del tráfico por ese dispositivo; véase www.pisa.org.uk/download/seminar20011117-fw/linux_firewall.ppt.

Sobre los encabezados de los mensajes de correo electrónico

Gestionar la seguridad de la información entraña más que preparar los dispositivos perimétricos y diferentes tipos de registros. El correo electrónico puede abrir las puertas a todo tipo de ataque e infección. Además de garantizar que se instale y utilice un software antivirus que inspeccione todos los mensajes (con la esperanza de que bloquee todas las fuentes potenciales de ataque) también es necesario que los usuarios y administradores tenga en cuenta el tema de los mensajes de correo electrónico no solicitados (también llamados *spam*) o los ataques de correo electrónico con base en DoS (los llamados *bombas de correo*). Para enfrentar adecuadamente los spam y los ataques de correo electrónico con base en DoS, es absolutamente esencial comprender cómo debemos leer los encabezados de correo electrónico. Conocer esto no solamente permitirá a los administradores e investigadores determinar al menos una fuente posible (cuando no real) del ataque o spam, sino que también ayuda a definir una estrategia para enfrentar ese tipo de situaciones.

La capacidad para rastrear los mensajes de correo electrónico es importante en muchos tipos diferentes de casos de delito informático. No es inusual que los delincuentes utilicen el correo electrónico de la siguiente manera:

- para hostigar a las víctimas (amenazas informáticas)
- para enviar exigencias o amenazas de extorsión
- para contactar posibles víctimas (pedófilos, violadores en serie)
- para solicitar "marcas" para estafas (scam nigeriano, proyectos de pirámide)
- para comunicarse con los cómplices

Por lo general, el correo electrónico pasa por diferentes computadoras desde que es enviado por el remitente hasta que llega al destinatario. En cada máquina se añade un encabezado al mensaje, hasta que llega a su destino. (Usualmente la estación de trabajo en la que el destinatario lee el mensaje no añade información de encabezado). Es importante que los investigadores conozcan cuál información se puede interpretar de los encabezados de los mensajes de correo electrónico, además de saber que los encabezados pueden ser falsificados.

Desentrañar y comprender los encabezados de correo electrónico requiere algún conocimiento sobre cómo reconocer y decodificar los campos que contienen. Este nivel

de estructura está bien documentado y se define principalmente en la recomendación RFC 822, que documenta el diseño y la estructura de los campos del encabezado de mensajes de SMTP (por Simple Mail Transfer Protocol, Protocolo simple de transferencia de correo). Si bien hay más campos que los que analizamos aquí, la Tabla 9.3 contiene los campos más importantes, así como aquellos que se deben verificar para tratar de rastrear los mensajes hasta su origen e identificar la ruta que siguieron desde su supuesto remitente original hasta el servidor de correo electrónico del destinatario.

Tabla 9.3 Los campos de encabezado de correo electrónico importantes contenidos en la RFC 822

Nombre de campo	**Explicación**
Campos de Origen/Remitente	
De	Identifica el remitente del mensaje, usualmente con nombre y dirección de correo-e
Remitente	Identifica el remitente real (podría ser diferente al campo De en algunos sistemas de correo-e)
Responder a	Dirección de correo-e a la que se deben dirigir las respuestas
Ruta de retorno	Ruta (dirección) de retorno al remitente
Recibido	Excepto cuando el usuario reside en el mismo servidor, conocido como *agentes de transferencia de mensajes* o *MTA*, todos los mensajes pasan al menos por un servidor intermediario en su viaje del remitente al destinatario. Cada no de los intermediarios aparece en su propia línea de Recibido.
Reenviado-xxx	Se aplica a los mensajes reenviados para los campos De, Remitente y Responder a
Campos de destino	
Para	Identifica el nombre y/o dirección de correo-e del destinatario
Cc	Destinatarios secundarios del mensaje
Bcc	Destinatarios ocultos del mensaje. (El mensaje se envía a todos los destinatarios designados como bcc pero en el encabezado no se incluye esta información).
Reenviado-xxx	Se aplica a los mensajes reenviados para los campos Para, cc y bcc
Encabezados de fecha	
Fecha	Fecha y hora en que fue enviado el mensaje original
Fecha de reenvío	Fecha y hora en que el mensaje reenviado fue enviado
Encabezados opcionales	
Asunto	Tema del mensaje

ID del mensaje	Identificador particular del mensaje (manejado por MTA desde el sistema de origen); también provisto para mensajes reenviados
En-respuesta-a	Identifica el mensaje al cual se responde
Referencias	Identifica otros mensajes a los cuales se aplica este mensaje
Palabras clave	Palabras clave que ayudan a seleccionar y organizar mensajes seleccionados (rara vez utilizado)
Comentarios	Comentarios en texto sobre el mensaje (rara vez utilizado)
Encriptado	Indica que el contenido del mensaje está encriptado
X-xxx	Identifica los campos definidos por el usuario

Los campos de mayor interés a la hora de abordar el tema de los mensajes de correo electrónico maliciosos o *spam* son los que identifican al supuesto remitente (de, responder a, remitente, ruta de retorno, etcétera) y todos los diferentes campos *recibidos* que indican los servidores de correo electrónico que participaron en el recorrido de los mensajes desde el remitente hasta el servidor de destino. Si bien las líneas de Recibido que no incluyen un campo De no identifican realmente el remitente, los usuarios pueden reportar que ese servidor está siendo utilizado para ratear spam a los ISP o a las organizaciones que los operan. En muchos casos, el proveedor podrá filtrar y eliminar el mensaje no deseado en lugar de reenviarlo al usuario que presentó la queja o a otra víctima. De hecho, es mejor concentrarse en la dirección IP reportada en estas líneas porque gran parte de la información puede ser falsificada por atacantes inteligentes. Para obtener más información sobre cómo hacer frente a los mensajes de correo electrónico no deseados, incluidas instrucciones detalladas sobre cómo crear y enviar quejas de spam a los operadores de los servidores que los reenvían, puede remitirse al excelente artículo titulado *Reporting SPAM* en www.freelabs.com/~whitis/spam_reporting.html. (Este sitio también contiene una sección de Vínculos útiles a otras informaciones sobre la investigación y las quejas sobre el spam).

Desafortunadamente, los mensajes de correo electrónico son demasiado fáciles de falsear, en el sentido de que los individuos conocedores pueden utilizar herramientas de software o construir a mano encabezados de correo electrónico según la RFC 822 totalmente falsas. Así, quizás no todos los informes de reenvíos no deseados produzcan el resultado deseado de eliminar o reducir el tráfico de mensajes no deseados. Algunos proveedores de servicios operan servicios especiales de correo electrónico conocidos como *remitentes anónimos* o *seudo-remitentes*. Estos servicios de anonimato están deliberadamente diseñados para ocultar a sus usuarios e impedir su identificación directa o personal; muchos operan fuera de los Estados Unidos.

Valladares contra el delito...
Haciendo frente a los proveedores de servicios de anonimato
En algunos casos, las compañías u organizaciones que operan servicios de anonimato responden favorablemente a las solicitudes de asistencia por parte de los profesionales encargados de hacer cumplir la ley que pretenden identificar a sus usuarios que están utilizando el servicio con fines delictivos. En otros casos, una compañía podría negarse a cooperar del todo; es mucho más probable que esa falta de cooperación se presente cuando los proveedores de servicio de anonimato operan en el exterior. No obstante, algunos de los servicios de anonimato más notorios (por ejemplo, anon.penet.fi, originalmente basificado en Finlandia) han dejado de operar, principalmente en respuesta a las reiteradas solicitudes de que identifiquen a sus clientes ante los profesionales del cumplimiento de la ley en todo el mundo. Hay un viejo refrán de Internet que se utiliza cuando se procura la cooperación de los remitentes anónimos: YMMV ("Your Mileage May Vary", en inglés). Esto es un eufemismo para la situación muy real en la que las cosas quizás no funcione exactamente como están descritas o anunciadas, o la asistencia por parte de un servicio quizás no se obtenga. Vale la pena tratar (o procurarse una orden judicial en los casos en que sea posible), pero intentar obtener la cooperación de estos servicios quizás no siempre produzca el resultado deseado!!

Para obtener más información sobre los campos de los encabezados de los mensajes de correo electrónico y la forma de interpretarlos, consulte el texto de la RFC 822 en www.faqs.org/rfcs/rfc822.html o el artículo titulado *Reading Email Headers* en el sitio web StopSpam, www.stopspam.org/email/headers/headers.html. También se puede encontrar valiosos recursos de correo electrónico en línea en http://everythingemail.net y por conducto del Internet Mail Consortium en www.imc.org.

A continuación presentamos un ejemplo de un encabezado de mensaje de correo electrónico parcialmente truncado, para ayudarlos a identificar los diferentes campos mencionados anteriormente. Este encabezado fue tomado directamente de un mensaje de correo electrónico reciente:

Return-Path (Ruta de retorno): <kate@syngress.com>
Received (Recibido): from mail20.jum.net by serv1.jump.net (mail20.jump.net
[206.196.91.20]) (8.9.3/jump.1.11)
id NAA25382; for <etittel@serv1.jump.net> Fri, 21 Jun 2002 13:56:18 -0500
(CDT)
Received: from osmtp1.electric.net (osmtp2.electric.net [216.129.90.29]) by
deliverator.io.com (8.9.3/8.9.3) with ESMTP id NAA28104 for <etittel@lanw.com> ;
Fri, 21 Jun 2002 12:56:15 -0500
Received: from [216.129.90.8] (hello=www1.electric.net)
by osmtp1.electric.net with smtp (Exim 3.22 #1)
id 17LTZu-0001IHm-04
for etittel@lanw.com Fri, 21 Jun 2002 11:56:14 -0700
Received: (qmail 16354 invoked by uid 99); 21 Jun 2002 18:56:12 -0000
Message-ID: <1024685772.3d1376cc8b1b0@www.electricwebmail.com>

Date: Fri, 21 Jun 2002 14:56:12 -0400
To: Ed Tittel <etittel@lanw.com>
From: "kate@syngress.com" <kate@syngress.com>
cc: Deb Shinder <deb@shinder.net>
Subject: Cybercrime ch 8
References: <NHEEJHCPPENDKBIKGHOEMECIGHAA.etittel@lanw.com>
In-Reply-To: <NHEEJHCPPENDKBIKGHOEMECIGHAA.etittel@lanw.com>

Algunos programas de correo electrónico no están predeterminados para mostrar todos los encabezados de los mensajes, pero es posible visualizarlos si se busca por la interfaz. Por ejemplo, en Microsoft Outlook 2002, hay que abrir el mensaje (no solamente visualizar la vista previa) y marcar **Ver | Opciones**. En la Figura 9. 8 se muestra "Encabezados de Internet" al final de la ventana de Propiedades de Mensaje. (Es preciso desplazarse línea a línea para verlos en su totalidad; también se puede copiar y pegar la información en un editor de textos o un programa de procesamiento de textos).

Figura 9. 8 Es posible que tengamos que buscar bien para encontrar todos los encabezados de correo electrónico en Outlook 2002 y otros clientes de correo. (Insertar aquí la figura que parece en la página 521).

Si este mensaje fuera parte de un ataque con bomba de correo o un spam, usted desearía contactar a los operadores de los diferentes servidores que están identificados en Ruta de retorno, De, y dentro de los diferentes campos de Recibido del encabezado. Sin embargo, sería más útil emplear primero el comando **whois** en la línea de comandos para verificar los nombres de dominio reportados a las direcciones IP utilizadas. El comando **whois** nos permite averiguar a nombre de quién está registrado el nombre de dominio, como explicamos en el Capítulo 8.

Normalmente Windows no tiene incorporadas capacidades del comando **whois**, pero sí existen numerosas fuentes para utilidades de **whois** que son compatibles con Windows, como las que existe en www.tatumweb.com/iptools.htm. O podemos utilizar los servicios de www.samspade.org para realizar la búsqueda necesaria en sus páginas web sin necesidad de utilizar la herramienta **whois** en un nuestra computadora con Windows. De igual manera, si tenemos acceso a una cuenta shell UNIX, debe ser posible utilizar el comando **whois** en la línea de comandos. El sistema OS X de Mac tiene una versión gráfica útil del **whois**, como se muestra en la Figura 9.9.

NOTA

Otros comandos útiles son **slookup** o **dig** para vincular nombres de dominio a direcciones IP.

Figura 9.9 El sistema OS X de Macintosh incluye una utilidad gráfica de **whois**, además de varias otras utilidades de red. (Insertar aquí la figura que parece en la página 522).

Rastrear un nombre de dominio o dirección IP

El Sistema de Nombres Dominio (DNS) es el encargado de mantener las asignaciones de nombre de dominio a direcciones IP en Internet. Numerosos dispositivos de perímetro, como los cortafuegos y enrutadores de selección, pueden realizar búsquedas inversas de DNS para cerciorarse de que los nombres de dominio reportados corresponden a las direcciones IP de destino reales en el tráfico de entrada. Cuando estas no se corresponden adecuadamente -- es decir, cuando la búsqueda del nombre de dominio produce como resultado una dirección IP diferente al de la dirección de destino-- es probable que el remitente esté tratando de falsear un nombre de dominio sin verificar que la dirección IP se corresponda. Esto apunta a un hacker nada avezado. Los hackers que saben lo que están haciendo generalmente se esfuerzan por lograr que las direcciones IP de donde supuestamente se origina el mensaje se correspondan con los nombres de dominio que utilizan.

No obstante, la técnica de "búsqueda inversa de DNS" permite a un dispositivo interrogar al servidor para que una dirección IP se corresponda con el nombre de dominio, así como para ejecutar las traducciones nombre-a-dirección más típicas que los DNS normalmente ofrecen siempre que una computadora intenta conectarse a otra utilizando un DNS "amistoso" en lugar de una dirección IP. La mayoría de los equipos perimétricos, y muchos servidores IP, pueden configurarse para que realicen una búsqueda inversa de DNS antes de conceder acceso incluso a usuarios anónimos y para que denieguen el acceso a usuarios cuyos nombres de dominio y direcciones IP reportados no concuerdan. Si bien ésta no es una técnica totalmente infalible para bloquear completamente el tráfico falseado, es altamente recomendada para las redes que permiten la entrada de tráfico desde el exterior de sus redes locales (especialmente de Internet).

En general, las interrogaciones DNS que utilizan la búsqueda inversa trabajan hacia atrás desde la dirección IP hasta el nombre de dominio, utilizando un archivo especial del servidor DNS llamado *in-addr-arpa*. Por ejemplo, si el servidor web tiene l dirección de Internet 206.224.64.194, la búsqueda procede en orden inverso hacia un archivo llamado 64.224.206-in-addr-arpa en algún servidor DNS en que las direcciones individuales en esa subred pueden resolverse (como el servidor web llamado www.lanw.xom en 206.224.65.194). La mayoría de los dispositivos perimétricos de red y servidores realizan esas búsquedas automáticamente y las escriben en los archivo de registro. No obstante, los investigadores deben además saber cómo llegar manualmente desde los nombres de dominio hasta las direcciones IP y desde las direcciones IP hasta los nombres de dominio, al menos para confirmar los resultados que encuentran en los archivos de registro del cortafuego, el enrutador o el servidor.

En la Tabla 9.4 se presenta un resumen de los comandos que pueden utilizarse para obtener información sobre el nombre de dominio y la dirección IP. En lugar de brindar información con una sintaxis completa, brindamos punteros a los comandos Windows y UNIX/Linux, como archivos de ayuda en lo que se pueden encontrar detalles y numerosos ejemplos. Sírvase observar además que se pueden encontrar variadas herramientas de búsqueda con base en la web que ofrecen la misma funcionalidad en www.tatumweb.com/iptools.htm. La ventana de este último enfoque es que se puede introducir simplemente un nombre de dominio o una dirección IP, así como otros argumentos, según sea necesario y observar los resultados sin necesidad de dominar las

sintaxis o los detalles del comando. De estas herramientas, la Toolbox de Elephant es particularmente útil dado que desglosa en teclas de opción las solicitudes **nslookup** más complejas.

Tabla 9.4 Utilidades de búsqueda de nombre de dominio/dirección IP

Comando	**Explicación**	**Ayuda de Windows**	**Ayuda de UNI/Linux**
Nslookup	Inspecciona los contenidos de los archivos del servidor DNS, incluidas las búsquedas progresivas y reversiva	Escriba **nslookup** y después, **help**	**man nslookup**
DiG	Brinda información desde los servidores DNS sobre los nombres de dominio y las direcciones IP	No está predeterminada en Windows	**man DiG**
Whois	Asigna nombres de host a direcciones IP y viceversa	No está predeterminada en Windows	**man Whois**

Un sitio web útil para obtener información sobre DNS es www.dnsreport.com. Los administradores pueden utilizarlo para conocer acerca de problemas y vulnerabilidades de sus servidores DNS, como se muestra en la Figura 9.10.

Figura 9.10 El sitio sobre informes de DNS es un recurso excelente para obtener información DNS para un dominio específico. (Insertar aquí la figura que aparece en la página 524).

Sistemas comerciales de detección de intrusión

En secciones anteriores dijimos que los cortafuegos y otros dispositivos perimétricos simples carecen de cierto grado de inteligencia en lo que se refiere a observar, reconocer e identificar las firmas de los ataques que pudieran estar presentes en el tráfico que monitorean y en los archivos de registro que recopilan. Sin la intención de criticar las capacidades de dichos sistemas, esta deficiencia explica por qué los sistemas de detección de intrusión (conocidos por la abreviatura IDS) son cada vez más importantes para contribuir a mantener una adecuada seguridad de red. Si bien otros dispositivos perimétricos pueden recopilar toda la información que es necesaria para detectar (y, a menudo frustrar) ataques que pudieran estarse iniciando o están ya en ejecución, no han sido programados para inspeccionar y detectar los tipos de tráfico o patrones del comportamiento de red que se corresponden con firmas de ataque conocidas o que sugieren posibles ataques no reconocidos que pudieran estar iniciándose o realizándose.

Muy brevemente, la forma más sencilla de definir un IDS sería describirlo como una herramienta especializada y capaz de leer e interpretar el contenido de los archivos de registro de enrutadores, cortafuegos, servidores y otros dispositivos de red. Además, a menudo los IDS almacenan una base de datos de firmas de ataque conocidas y pueden

comparar los patrones de actividad, tráfico o comportamiento que observan en los registros que monitorean con relación a esas firmas para reconocer cuando ocurre una correspondencia más o menos aproximada entre una firma y un comportamiento reciente o actual. En ese punto, el IDS puede emitir una alarma o alerta, tomar diferentes medidas automáticas que van desde cesar los vínculos a Internet o servidor específico hasta garantizar búsquedas inversas, y realizar otros intentos para identificar a los atacantes y recopilar evidencias de sus actividades nefastas.

Por analogía, en el trabajo en red el IDS realiza la misma función que un software antivirus ante un archivo que entra a un sistema: inspeccionar el contenido del tráfico en la red para detectar y frustrar posibles ataques, de la misma manera que un paquete antivirus inspecciona el contenido de los archivos adjuntos de mensajes de correo electrónico, contenido web activo, etc. de entrada, en busca de firmas de virus (patrones que se corresponden con programas malignos conocidos) o de posibles acciones maliciosas (patrones de comportamiento que son al menos sospechosos, cuando no del todo inaceptables).

Para ser más específicos, detectar una intrusión significa detectar el uso no autorizado de un sistema o una red o los ataques contra estos. Los IDS están diseñados y se utilizan para detectar y frustrar o detener (cuando sea posible) dichos ataques o uso no autorizado de sistemas, redes y recursos conexos. Al igual que los cortafuegos, los IDS pueden estar basados en software o ser una combinación de hardware y software (en forma de dispositivos IDS preinstalados y preconfigurados independientes). A menudo, el software IDS se ejecuta en los mismos dispositivos o servidores en los que operan los cortafuegos, proxies, u otros servicios perimétricos; un IDS que no se ejecute en el mismo dispositivo o servidor en los que están instalados el cortafuego u otros servicios monitorearán esos dispositivos cuidadosamente. Si bien dichos dispositivos tiende a operar como perimétricos de red, los sistemas IDS pueden detectar y hacer frente a los ataques tanto del interior como del exterior.

Caracterización de los sistemas de detección de intrusión

Los sistemas IDS varían según diferentes criterios. Al analizar esos criterios, podemos explicar los tipos de IDS que posiblemente encontremos y cómo funcionan. En primer lugar es posible distinguir los IDS sobre la base del tipo de actividad, tráfico, transacciones o sistemas que monitorean. En este caso, estos sistemas pueden dividirse en sistemas con base en red, con base en host y con base en aplicaciones. Los IDS que monitorean los ejes centrales de red y buscan firmas de ataque son llamados *IDS con base en red*, mientras que los que operan en hosts y defienden y monitorean los sistemas operativos y de archivo en busca de señales de intrusión son denominados *IDS con base en host*. Algunos IDS monitorean solamente aplicaciones específicas y son denominados *IDS con base en aplicaciones*. (Este tipo de tratamiento por lo general se reserva para aplicaciones importantes como sistemas de gestión de bases de datos, sistemas de administración de contenido, sistemas de contabilidad, etc.). A continuación se presentan detalles adicionales sobre los diferentes tipos de enfoques de monitoreo con IDS:

- **Características de los IDS con base en redes**
  Ventajas: Los IDS con base en redes pueden monitorear toda una red con apenas algunos nodos o dispositivos adecuadamente ubicados, y representa muy poco costo adicional a la red. Los IDS con base en redes son

principalmente dispositivos pasivos que monitorean la actividad en la red sin añadir un costo significativo ni interferir con el funcionamiento de la red. Son fáciles de proteger frente a los ataques y pueden incluso permanecer indetectables por los atacantes; también exigen poco esfuerzo para su instalación y uso en las redes ya existentes.
Desventajas: Los IDS con base en redes quizás no sean capaces de monitorear y analizar todo el tráfico en redes grandes y congestionadas, y por ello es posible que pasen por alto los ataques lanzados durante períodos de pico en el tráfico. Quizás los IDS con base en redes no puedan monitorear efectivamente las redes de alta velocidad. Normalmente, los IDS con base en redes no pueden analizar datos encriptados ni informar si los ataques tienen o no éxito. Por esta razón, los IDS con base en redes exigen una cantidad determinada de actividad, y de participación manual por parte de los administradores de red para valorar los efectos de los ataques reportados.

- **Características de los IDS con base en host**
  Ventajas: Un IDS con base en host puede analizar con un alto nivel de detalle las actividades que se realizan en el host que monitorea; a menudo puede determinar los procesos y/o usuarios que participan en las actividades maliciosas. Si bien es posible que cada uno de ellos se concentre en un solo host, muchos sistemas IDS con base en host utilizan un modelo de consola de agente en el que los agentes se ejecutan (y monitorean) en host individuales pero envían información a una consola única centralizada (de manera que una misma consola puede configurar, administrar y consolidar los datos procedentes de varios host). Los IDS con base en host pueden detectar ataques que no son detectables por los IDS con base en redes y pueden medir los efectos de los ataques con bastante precisión. Los IDS con base en host pueden utilizar servicios de encriptación con base en host para examinar el tráfico, los datos, las salvas y la actividad encriptada. Los IDS con base en host no tienen dificultades para funcionar en redes por conmutación.
  Desventajas: La recopilación de datos se realiza por cada host; la escritura en los registros o los reportes de actividad requiere enviar tráfico en la red y ello podría afectar el rendimiento de la red. Los atacantes avezados que comprometen un host pueden también atacar y deshabilitar los IDS con base en host. La acción de estos sistemas IDS puede ser burlada por ataques desde DoS (ya que podrían impedir que cualquier tipo de tráfico llegue al host donde están ejecutándose o impedir que se envíe un informe de ese ataque a una consola ubicada en otra parte de la red). Algo que es más significativo es que los IDS con base en host consumen tiempo de procesamiento, almacenamiento, memoria y otros recursos del host donde operan.
- **Características de los IDS con base en aplicaciones**
  Ventajas: Un IDS con base en aplicaciones se concentra en los sucesos que ocurren dentro de una determinada aplicación. Usualmente detectan los ataques mediante el análisis de los archivos de registro de aplicaciones y pueden por lo general identificar muchos tipos de ataques o de actividad sospechosa. En ocasiones un IDS con base en aplicaciones puede incluso

rastrear la actividad no autorizada de usuarios individuales. También pueden trabajar con datos encriptados, utilizando servicios de encriptación/ desencriptación con base en aplicaciones.
Desventajas: Los IDS con base en aplicaciones son a veces más vulnerables a los ataques que los IDS con base en host. También pueden consumir recursos de aplicaciones (y host) considerables.

En la práctica, la mayoría de los ambientes comerciales utilizan alguna combinación de estos tres sistemas de IDS para observar lo que sucede en la red cada vez que también monitorean más de cerca los hosts y las aplicaciones claves.

Los IDS también pueden distinguirse por los diferentes enfoques que aplican al análisis de los sucesos. Algunos IDS utilizan principalmente una técnica llamada *detección de firma*. Esta técnica se asemeja mucho a la forma en que los programas antivirus utilizan las firmas de virus para reconocer y bloquear archivos, programas o contenido web activo infectados, para evitar que penetren en un sistema de computadora, con la diferencia de que utiliza una base de datos de patrones de tráfico o actividad relacionados con ataques conocidos, los cuales se denominan *firmas de ataques*. De hecho, la detección de firmas es la aplicación más ampliamente utilizada en la tecnología IDS comercial actualmente. Otro enfoque es la denominada *detección de anomalías*. Este utiliza reglas o conceptos predefinidos sobre la actividad "normal" y "anormal" del sistema (método *heurístico*) para distinguir las anomalías del comportamiento normal del sistema y monitorear, informar o bloquear las anomalías a medida que ocurran. Algunos IDS soportan la detección de una cantidad limitada de tipos de anomalía; la mayoría de los expertos considera que este tipo de capacidad se incorporará en el futuro a la forma en que operan los IDS. A continuación presentamos informaciones adicionales sobre estos dos tipos de técnicas de análisis de sucesos:

- **Características de los IDS con base en firmas**
  Ventajas: Un IDS con base en firmas examina el tráfico, la actividad, las transacciones o el comportamiento para verificar que exista correspondencia con patrones de sucesos conocidos que son específicos de ataques sobre los cuales existe información. Al igual que sucede con el software antivirus, un sistema IDS con base en firmas requiere tener acceso a una base de datos actualizada de firmas de ataques y poder de alguna manera comparar el comportamiento que detecta con una amplia colección de firmas. Excepto cuando ocurre un ataque totalmente nuevo sobre cual no existe información, esta técnica funciona muy satisfactoriamente.
  Desventajas: Las bases de datos deben ser actualizadas constantemente y los IDS deben ser capaces de comparar las actividades que detecta frente a una amplia colección de firmas de ataques. Si las definiciones de firmas son demasiado específicas es posible que los sistemas IDS con base en firmas no detecten las variaciones de ataques conocidos. (Una técnica común para crear nuevos ataques es variar los ataques conocidos ya existentes en lugar de crear otros totalmente nuevos). Además, los IDS con base en firmas también pueden representar una desaceleración notable del rendimiento de los sistemas cuando el comportamiento que detecta se aviene con múltiples (o numerosas) firmas de ataque, total o parcialmente.

- **Características de los IDS con base en anomalías**
  Ventajas: Un IDS con base en anomalías examina el tráfico, la actividad, las transacciones o el comportamiento en busca de anomalías en los sistemas o redes que pudieran ser indicio de un ataque. El principio subyacente es la noción de que "el comportamiento de ataque" es suficientemente diferente del "comportamiento de usuario normal" como para poder detectarlo mediante catalogación e identificación de las diferencias entre ambos. Al crear puntos de referencia sobre el comportamiento normal, los sistemas IDS con base en anomalías pueden observar cuando el comportamiento se desvía estadísticamente de la norma. En teoría, esta capacidad brinda a los IDS con base en anomalías las posibilidades de detectar nuevos ataques que no son conocidos ni para los cuales se ha creado una firma.
  Desventajas: Debido a que el comportamiento normal puede variar rápida y fácilmente, los sistemas con base en IDS son propensos a arrojar falsos positivos cuando los ataques pudieran reportarse sobre la base de los cambios de la norma considerada "normal", en vez de representar ataques reales. Su comportamiento intensamente analítico también puede imponer en ocasiones grandes sobrecargas de procesamiento a los sistemas en los que se ejecutan. Además, los sistemas con base en anomalías demoran en crear puntos de referencia estadísticamente significativos (para separar el comportamiento normal de las anomalías); durante este período están relativamente expuestos al ataque.

Actualmente muchos paquetes antivirus incluyen características de detección con base en firmas y en anomalías, pero solamente unos pocos IDS incorporan ambos enfoques. La mayoría de los expertos piensan que la detección con base en las anomalías se convertirá en una característica más difundida entre los IDS, pero será necesario que se produzcan avances en las investigaciones y la programación para poder disponer del tipo de capacidad que la detección con base en anomalías debería brindar pero que en estos momentos carece.

Por último, algunos IDS son capaces de responder a los ataques cuando estos ocurren. Este comportamiento es conveniente desde dos puntos de vista. En primer lugar, un sistema de computadora puede rastrear el comportamiento y la actividad en tiempo casi real, y responder con mucha más rapidez y precisión durante las primeras etapas de un ataque. Como la automatización contribuye a que los hackers realicen los ataques, por lógica debería también ayudar a los profesionales de la seguridad a rechazarlos en el momento en que ocurren. En segundo lugar, los IDS están activos permanentemente, pero los administradores de red quizás no puedan responder con la misma rapidez durante las horas de descanso que durante las horas pico (incluso si los IDS pudieran emitir una alarma para avisarles que ha comenzado a producirse un ataque). Al automatizar una respuesta para bloquear el tráfico de entrada desde una o más direcciones desde la cual se origina un ataque, el IDS puede detener un ataque que se esté produciendo y propiciar ataques futuros desde la misma dirección.

Cuando se aplican las técnicas siguientes, los IDS pueden mantener a raya a los hackers expertos y a los novatos. Si bien es más difícil bloquear por completo la actividad de los expertos, estas técnicas pueden aminorar considerablemente sus efectos:

- Interrumpir las conexiones TCP introduciendo paquetes de restablecimiento en las conexiones del atacante frustra los ataques
- Desplegar filtros de paquetes automatizados para bloquear los enrutadores o cortafuegos a fin de que no reenvíen paquetes de ataque a servidores o hosts que son atacados logra frustrar totalmente la mayoría de los ataques, ya sean ataques DoS o DDoS. Estos funciona para las direcciones del atacante y para los protocolos o servicios que son atacados (al bloquear el tráfico en capas diferentes del modelo ARPA de trabajo, por decirlo de alguna manera).
- Desplegar desconexiones automatizadas para los enrutadores, cortafuegos o servidores puede detener todo tipo de actividad cuando otras medidas no surten efecto para detener a los atacantes (como en situaciones extremas de ataque DDoS, en los que el filtrado será efectivo únicamente en el extremo ISP de un vínculo Internet, cuando no a un nivel superior de la cadena ISP, lo más cercano posible a los ejes centrales de Internet).
- El empleo activo de las búsquedas inversas en DNS u otras formas de intentar determinar la identidad de un hacker es una técnica que utilizan algunos IDS, generando reportes de actividad maliciosa a todos los ISP en las rutas utilizadas entre el atacante y la víctima. Como esas respuestas podrían entrañar cuestiones legales, los expertos recomiendan obtener asesoría legal antes de pagar al hacker con la misma moneda.

Para tener acceso a un amplio conjunto de artículos y recursos sobre la tecnología IDS, sírvase visitar www.searchsecurity.techtarget.com y utilizar el motor de búsqueda del sitio para obtener resultados por *intrusion detection*. Consideramos que el artículo de Peter Mell en Tech Republic *Intrusion Detection: A Guide to the Options* es especialmente útil (véase www.techrepublic.com/article_guest.jhtml?id=r00620011106ern01.htm&fromtm=e036), pero hay también muchos otros artículos buenos.

IDS comerciales

Literalmente cientos de proveedores ofrecen diversas formas de aplicaciones comerciales de IDS. Las soluciones más efectivas combinan aplicaciones de IDS con base en red y con base en host. Asimismo, la mayoría de esas aplicaciones son primordialmente con base en firmas, con capacidades limitadas de detección de anomalías en algunos productos o soluciones específicos. Por último, la mayoría de los IDS modernos incluyen algunas capacidades limitadas de respuesta automática, pero por lo general estas se concentran en el filtrado y bloqueo automático del tráfico o la desconexión como último recurso. Si bien algunos sistemas afirman ser capaces de lanzar contraataques, las mejores prácticas indican que la identificación automática y las facilidades de rastreo inverso son los aspectos más útiles que ofrecen esas facilidades y son, por lo tanto, las que se utilizan con mayor probabilidad.

En la escena…
Para valorar entre las opciones de IDS

Además de los distintos proveedores de IDS que mencionamos en esta sección, el uso correcto de un motor de búsqueda de Internet apropiado puede ayudar a los administradores de red a identificar más posibles proveedores adicionales de IDS de lo que pudieran investigar en detalle. Es por ello que también instamos a los administradores a considerar una alternativa adicional: delegar en parte o totalmente las decisiones relacionadas con la tecnología de seguridad de redes de la organización a un tipo especial de compañía contratista. Estas organizaciones, conocidas como Proveedores de servicios de seguridad gestionados (MSSP en inglés, por *managed security services providers*), pueden ayudar a sus clientes a seleccionar, instalar y gestionar políticas e infraestructuras técnicas de seguridad de última generación. Por ejemplo, Guardent es un MSSP que incluye servicios integrales de cortafuegos y detección de intrusión entre sus diversos servicios al cliente; para una explicación de los diversos programas de oferta de servicio de la empresa puede visitar www.guardent.com. Los profesionales encargados de hacer cumplir la ley podrían encontrar en estas organizaciones fuentes especialmente útiles de información, ayuda y apoyo en lo que se refiere a las cuestiones de tecnología o la comprensión de las complejidades de la seguridad de las TI.

Un enorme número de posibles proveedores pueden ofertar productos de IDS a empresas y organizaciones. Sin favorecer a una en especial, a continuación brindamos un listado de algunas de las soluciones más conocidas y ampliamente utilizadas en este espacio de productos:

- **Cisco Systems** quizás sea el más conocido por sus conmutadores y enrutadores, pero Cisco también ofrece productos de cortafuegos y de detección de intrusión importantes (www.cisco.com).
- **GFI LANguard** es una familia de productos de monitoreo, exploración y verificación de integridad de archivos que ofrecen amplias capacidades de detección de intrusión y respuesta (www.gfi.com/languard).
- **Internet Security Systems (SSI)** ofrece una familia de productos de seguridad empresarial llamada RealSecure que incluye capacidades integrales de detección de intrusión y respuesta (www.iss.net).
- **Network-1 Security Solutions** ofrece diferentes familias de productos de detección de intrusión (con base en host) para computadoras y servidores, además de facilidades de gestión centralizada de la seguridad y cortafuegos (www.network-1.com).
- **TripWire** quizás sea el más conocido de todos los proveedores de utilidades de chequeo de firmas e integridad de archivos (también conocidas como TripWire). No obstante, TripWire ofrece además productos de verificación de integridad para enrutadores, conmutadores y servidores, además de una consola de administración centralizada para sus diversos productos (www.tripwire.com).

Un centro de intercambio de información para los proveedores de servicio de

Internet conocido como ISP-Planet ofrece todo tipo de información interesante en línea sobre los MSSP, además de servicios de cortafuegos, VPN, detección de intrusión, monitoreo de seguridad, antivirus y otros servicios de seguridad. Para más información, puede visitar los siguientes URL:

- ISP-Planet Survey: proveedores de servicio de seguridad gestionada, gráfico de proveedores participantes
  www.isp-planet.com/technology/mssp/participants_chart.html.
- Gráfico de servicios gestionados de cortafuegos
  www.isp-planet.com/technology/mssp/firewalls_chart.html
- Gráfico de servicios gestionados de trabajo en red privada virtual
  www.isp-planet.com/technology/mssp/services_chart.html
- Monitoreo gestionado de seguridad y detección de intrusión
  www.isp-planet.com/technology/mssp/monitoring_chart.html
- Antivirus gestionado y filtrado de contenido y bloqueo de URL gestionados
  www.isp-planet.com/technology/mssp/mssp_survey2.html
- Evaluación gestionada de la vulnerabilidad, respuesta ante emergencias e investigaciones
  www.isp-planet.com/technology/mssp/mssp_survey3.html

Direcciones IP ficticias y otras prácticas antidetección

A pesar de que realicemos los mayores esfuerzos por rastrear el tráfico de correo electrónico no deseado o los ataques, a veces no podremos determinar su verdadera fuente ni identificar a la persona o las personas que están detrás de esta actividad. La principal razón de este fenómeno es que por lo general los hackers generan tráfico de red o mensajes que contienen datos de dirección de origen inventados, al igual que número de puertos, ID de protocolo y otras informaciones que normalmente permiten que ese tipo de información se asocie de manera concluyente con una dirección IP de origen, además de con un identificador del proceso de origen (y por extensión, al usuario o el servicio responsable de haber creado el proceso). Esto es una técnica deliberada y calculada para impedir la identificación de los atacantes y desviar el interés de la fuente real de ese tráfico hacia terceros que nada tienen que ver con él.

La forma más común de suplantación ocurre cuando los atacantes tratan de insertar un tráfico o mensajes fabricados que aparentan originarse dentro de una red local por conducto de una interfaz externa. Ello explica por qué las reglas anti-suplantación más comunes que se aplican en la mayoría de los enrutadores de exploración y cortafuegos sea "tumbar" los paquetes que llegan desde una interfaz externa y que reportan una dirección de origen que solamente debe aparecer en una interfaz interna. Otras formas de suplantación se pueden detectar utilizando la búsqueda inversa en DNS para comparar los nombres de dominio y direcciones IP asociadas (cuando existen los datos) y drop todos los datos cuando estas dos informaciones no se corresponden (como cuando la dirección IP reportada se origina fuera de el rango de direcciones asignado a la organización desde dentro de la cual supuestamente procede).

El problema real con el tráfico de suplantación se presenta cuando el IDS o los administradores tratan de seguir el rastro del tráfico hasta su fuente y se tropiezan con varios callejones sin salida. Por ejemplo, recordemos que varios tipos de ataques DoS o DDoS dependen de que se hayan comprometido las computadoras intermedias, en

ocasiones llamadas zombies o agentes, y podremos comprender rápidamente por qué no siempre identificaremos a los atacantes rastreando los ataques hasta su fuente. Cuando se determina desde dónde se originaron determinados ataques, podremos únicamente identificar a otras víctimas en lugar de encontrar el arma del delito que apunte hacia un atacante. Mientras más experimentado sea el hacker que realiza el ataque menores serán las probabilidades de que brinde pistas directas que nos lleve indirectamente hasta su presencia primaria en Internet. Más bien veremos que nuestros esfuerzos de identificación nos llevarán a muchos intermediarios y servicios de anonimato, cada uno de los cuales deberemos investigar en busca de indicios sobre la identidad del autor intelectual del delito informático que nos ocupa.

Ello también explica por qué contactar a proveedores de servicio que pudieran estar reenviando los ataques --y trabajar con ellos no solamente para rastrear el origen del tráfico de ataques sino también para bloquearlo e impedir que nos llegue por intermediarios involuntarios-- es una parte importante del proceso de manejo de incidentes de seguridad y de rechazar ataques futuros. Además, numerosos servicios de Internet y sitios web mantienen listas de direcciones IP, nombres de dominio y direcciones de correo electrónico desde los cuales se han originado ataques anteriormente. Al suscribirse a esos servicios y utilizarlos para configurar filtros de paquete y de correo electrónico, los administradores pueden mantener a raya posibles fuentes de ataque –como hacen muchos ISP– y evitar interactuar con fuentes problemáticas.

Existen en línea numerosas fuentes de información sobre generadores de spam y atacantes; aquí mencionamos solo algunos ejemplos. Si desea conocer sobre otras, utilice los motores de búsqueda y palabras claves como *spam database (base datos spam), attacker database (base datos ataque), spam prevention (prevenir spam)*, entre otras:

- DNS-Based Spam Databases (Bases de datos spam con base en DNS): listado de todas las bases www.declude.com/junkmail/support/ip4r.htm
- Listado de generadores de spam, hostigadores, bombas de correo electrónico, y otros usos indebidos del correo electrónico www.sandes.dk/abusers/abusers.html
- *Instrusion Signatures and Analysis*. Stephen Northcutt, et.al. New Riders, 2001, ISBN: 0735710635. Este libro documenta cientos de firmas de ataque, además de soluciones que a menudo dependen de bloquear las direcciones IP, subredes o nombres de dominio de donde provienen los ataques. Contiene muchos de los detalles que se deben tener en cuenta para analizar todo tipo de ataque y responder a ellos.

Tarros de miel, panales y otros "señuelos" informáticos

Si bien la estrategia de incitar a los hackers a dedicar tiempo a investigar dispositivos o servicios de red atractivos puede entrañar problemas particulares, encontrar la forma de incitar a intrusos a entrar en nuestro sistema o red nos aumenta las posibilidades de que podamos identificarlos y perseguirlos más eficazmente. Un "tarro de miel", o *honeypot*, es un sistema de computadora que está deliberadamente expuesto al acceso público –usualmente en Internet– con el objetivo expreso de atraer y distraer a los atacantes. Asimismo, un "panal", o *honeynet*, es una red creada con el mismo objetivo, en la que los

atacantes no solamente encontrarán servicios o servidores vulnerables sino también vulnerabilidades en enrutadores, cortafuegos y otros dispositivos perimétricos de red, aplicaciones de seguridad, etc. En otras palabras, estos son el equivalente de las conocidas operaciones "señuelo", o encubiertas, de la policía.

Examen del derecho informático…
Entre la oportunidad y la provocación

La mayoría de los funcionarios y oficiales encargados de hacer cumplir la ley están conscientes de la delgadez de la línea por la que tienen que transitar cuando llevan a cabo una operación "señuelo" –aquella en la que los policías aparentan ser víctimas o participantes en delitos con el objetivo de lograr que los presuntos delincuentes cometan un acto ilegal en su presencia. La mayoría de los estados tienen leyes que prohíben la provocación; es decir, a los oficiales encargados de hacer cumplir la ley no les está permitido llevar a otras personas a cometer un delito y después arrestarlas por haberlo cometido. La provocación es un elemento para la defensa en un caso judicial; si el acusado puede demostrar que fue víctima de una provocación es posible que logra ser absuelta.

No obstante, los tribunales han sostenido tradicionalmente que brindar *una simple oportunidad* a un delincuente para que cometa un delito no constituye una provocación. La provocación entraña utilizar la persuasión, coacción u otra presión indebida para obligar a alguien a cometer un delito que no habría cometido de no ser así. Así, establecer un "tarro de miel" o un "panal" sería igual a la táctica (perfectamente legal) de la policía de poner un auto abandonado al borde de la carretera y esconderse para ver si alguien intenta robarlo o saquearlo. Debería señalarse además que el acto de provocación se aplica solamente a las acciones realizadas por el personal gubernamental o encargado de hacer cumplir la ley. Un civil no puede provocar, independientemente del grado de presión que ejerza sobre otra persona para que cometa el delito. (No obstante, un civil podría enfrentar otros cargos, como incitación al delito o conspiración para delinquir, por hacer que otra persona delinca).

Las siguientes son características típicas de los "tarros de miel" y "panales":

- Los sistemas o dispositivos utilizados para incitar se configuran solamente con instalaciones predeterminadas "listas para usar", de manera que están deliberadamente expuestas a todas las vulnerabilidades y ataques.
- Los sistemas o dispositivos utilizados como incitación no tienen ninguna información sensible verdadera --como contraseñas, datos, aplicaciones o servicios del que dependa realmente la organización o que se deba proteger absolutamente-- de manera que estos pueden ser comprometidos, o incluso destruidos, sin causar daños, pérdidas o perjuicios reales a la organización que los expone al ataque.
- Los sistemas o dispositivos utilizados como incitación también a menudo contener otros recursos atractivos, como archivos nombrados *password.db*, carpetas llamadas *Top Secret*, etc.--casi siempre consistentes sólo en datos

encriptados sin ningún valor o archivos de registro sin significado alguno--para atraer y mantener el interés del atacante el tiempo suficiente para poder rastrearlo hasta el punto de origen.

- Los sistemas o dispositivos utilizados como incitación también incluyen o están monitoreados por aplicaciones pasivas que pueden detectar e informar ataques o intrusiones tan pronto comiencen, de manera que pueda iniciarse lo antes posible el proceso de rastreo e identificación.

Aunque esta técnica puede sin dudas contribuir a identificar al atacante no sofisticado e incauto, también nos hace correr el riesgo de atraer la atención de los atacantes expertos. Una vez identificados, estos *tarros de miel* o *panales* a menudo son publicados en sitios de mensajes o listas de correos de hackers, por lo que quedan aún más expuestos a los ataques y la actividad de estos. De igual manera, si la organización que los ha establecido es identificada, sus sistemas y redes pueden quedar sujetos a una cantidad de ataques mayor.

La técnica del tarro de miel es mejor utilizada cuando la empresa u organización posee profesionales de seguridad informática empleados a tiempo completo que pueden monitorearlos y manejarlos permanentemente, o cuando las operaciones de aplicación de la ley están dirigidas a sospechosos específicos en una operación de "señuelo virtual". En estas situaciones es comprensible que se deban correr estos riesgos, y es mucho más probable que existan (y se apliquen) las precauciones y los procesos y procedimientos de seguridad apropiados**.** No obstante, para las organizaciones que pretenden identificar y perseguir a los atacantes de una manera más proactiva, estas soluciones pueden constituir una ayuda valiosa en esa actividad.

A pesar de que existen numerosos recursos de calidad relacionados con los *tarros de miel* y *panales* (puede probar buscando cualquiera de los dos términos en www.searchsecurity.techtarget.com), los recursos siguientes son especialmente valiosos para las personas que deseen obtener información adicional sobre el tema. El artículo de John McMullen *Enhance Intrusion Detection with a Honeypot* en www.techrepublic.com/article_guest.jhtml?id=r00220010412mul01.htm&fromtm=e036 ofrece nuevas ideas sobre el tópico. El Honeynet Project (Proyecto Panal) en www.honeynet.org quizás sea el mejor recurso que exista en línea; no solamente brinda amplia información sobre el trabajo del proyecto para definir y documentar tarros de miel y panales estándar, sino que además realiza un buen análisis de la mentalidad, las motivaciones, las herramientas y las técnicas de los hackers.

Resumen

¿Por qué la detección del delito informático es importante para los investigadores? Solamente si detectamos que se han producido (o se están produciendo) delitos informáticos pueden los investigadores tener una ventaja sobre los delincuentes y comenzar la investigación mientras la escena del delito está aún "caliente". Además, únicamente cuando se detecta o se observa actividad sospechosa podrán los investigadores saber que deben tomar las medidas necesarias para obtener, preservar y preparar la evidencia que será necesaria si deben tomarse medidas legales. Al seguir el rastro del tráfico de ataque desde sus víctimas hasta sus orígenes --incluso si esos orígenes apuntan a otras víctimas y no al atacante verdadero, como suele suceder-- los investigadores pueden trabajar con los proveedores de servicios intermediarios para informarles acerca de los ataques y ayudar a los administradores y al personal de seguridad a impedir que ocurran esos ataques. Incluso cuando no es posible emprender una acción legal, o cuando las víctimas deciden no hacerlo, la información obtenida y compartida durante el proceso de investigación puede repercutir positivamente en la conciencia y postura con relación a la seguridad de las diferentes partes que los investigadores contactan a lo largo del proceso.

Un elemento clave en la obtención de evidencia sobre los delitos informáticos puede encontrarse si habilitamos la auditoria de sucesos sospechosos en los dispositivos perimétricos y sistemas operativos susceptibles de ataque. Los profesionales de la TI deben comprender cómo establecer las instrucciones para que estos sistemas y dispositivos registren esos datos, y deben además ser conscientes de los tipos y clases de sucesos que son más convenientes registrar. Entre esos procesos están los intentos de inicio de sesión, el acceso a recursos sensibles, el uso de privilegios de administración, y el monitoreo de sistemas claves y archivos de datos. Igualmente, los profesionales encargados de aplicar la ley deben saber no solamente que esos registros existen, sino también que los mismos con frecuencia son la más importante fuente de evidencia de delitos informáticos fallidos o exitosos, y deben estar conscientes de que es preciso realizar todos los esfuerzos para protegerlos antes y durante la investigación. Los cortafuegos, enrutadores, servidores proxy, servidores de red y sistemas de detección de intrusión pueden contribuir a esos registros (además de brindar informes, alarmas y alertas conexas) para dar fundamento a las afirmaciones de que ocurrieron sucesos de acceso no autorizado, alteración, destrucción o negación de servicio en relación con la información o los servicios y, en algunos casos para contribuir a rastrear el origen del actividad.

En el modelo de seguridad conocido como triple A (autenticación, autorización y auditoria), la contabilidad es lo que posibilita la auditoria y el registro de actividad sospechosa o ilícita. Tanto los profesionales de las TI como los encargados de hacer cumplir la ley deben comprender este concepto. Los administradores deben aplicar técnicas apropiadas de auditoria y registro a fin de garantizar que se pueda detectar el delito informático (preferentemente antes de que logre comprometer o dañar a la organización y sus valores e infraestructura), obtener evidencias que puedan ayudar a documentar la actividad ilícita o no deseada, y ayudar a identificar a las partes involucradas. Obsérvese además que los dispositivos perimétricos, los sistemas Windows y UNIX/Linux tienen sus propios métodos para habilitar y registrar esos datos,

pero la evidencia es fácil de obtener por aquellos que saben qué se debe indagar y dónde encontrar la información deseada.

En el lado proactivo y preventivo de la seguridad de sistemas y redes, los sistemas y servidores perimétricos deben configurarse de manera que podamos impedir o frustrar los ataques comunes conocidos a la vez que auditamos y registramos cualquier evidencia de que pueda estar ocurriendo una actividad afín. Dentro de la información de registro suelen estar marcas de fecha y hora, direcciones y nombres de dominio de origen putativos, así como cualquier otra información que pueda servir para llevarnos hasta el sistema de origen del ataque. Los mensajes de correo electrónico incluyen información similar, de manera que los mensajes no deseados pueden ser rastreados a través de los sistemas que los reenviaron desde su remitente hasta su destinatario final. No obstante, en demasiadas ocasiones toda esa información nos lleva solamente a otras víctimas o a participantes involuntarios en el delito informático, y no a los verdaderos perpetradores.

Cuando rastrean el origen del delito informáticos y las rutas que sigue su actividad en redes desde el punto de origen hasta el punto de ataque, los investigadores encontrarán numerosas herramientas y utilidades que los pueden ayudar en la búsqueda de información. Los cortafuegos, enrutadores de selección y los IDS a menudo pueden obtener automáticamente esa información, además de que existen numerosas herramientas y comandos en Windows y Linux o UNIX para recuperar o confirmar manualmente esa información. Los profesionales de las TI y los encargados de hacer cumplir la ley deben saber cómo utilizar dichos comandos y utilidades, especialmente aquellas que nos permiten asignar direcciones IP a nombres de dominio, y viceversa, con el objetivo de contribuir a identificar los diferentes puntos a lo largo de la ruta de ataque, así como su origen definitivo.

Los sistemas de detección de intrusión (IDS) no solamente ayudan a detectar y frustrar activamente los delitos informáticos, sino que también muchas veces contribuyen a recopilar información sobre los patrones de ataque, detalles específicos sobre las actividades conexas, entre otros aspectos. Muchos de estos sistemas de detección de intrusión operan sobre la base de las llamadas firmas de ataque, que ofrecen información sobre patrones de actividad específicos, tráfico de redes o comportamiento, con lo cual comparar la actividad que tiene lugar en la red, con el objetivo de identificar (y en ocasiones hasta frustrar) los ataques mientras ocurren. De la misma manera que hacen los programas antivirus y sus bases de datos de firmas, los IDS deben ser también constantemente actualizados para mantener al día su registro de firmas de ataque. Algunos IDS también pueden identificar comportamientos anómalos en los sistemas y redes como forma de detectar posibles ataques sobre los cuales no exista una firma identificada. Además, los IDS pueden concentrarse en hosts individuales, aplicaciones o redes para buscar evidencia de ataques o actividad sospechosa.

A pesar de las capacidades reales de los investigadores para rastrear los ataques e identificar su punto de origen, las técnicas de suplantación pueden a menudo dar al traste con sus esfuerzos por identificar a los verdaderos responsables del delito informático. Muchas veces los sospechosos iniciales en caso de delito informático resultan ser ellos mismos víctimas que los delincuentes han utilizado como intermediarios, o pueden ser participantes involuntarios en actividades que se originaron en otra parte. Es por ellos que las técnicas contra la suplantación de identidad son un componente importante de la configuración de los cortafuegos, enrutadores de selección, etc. con el objetivo de evitar

posibles ataques, y los investigadores deben estar preparados para poder seguir el rastro del ataque, y no depender solamente de lo que revela la evidencia inicial disponible.

Algunas empresas y organizaciones pueden decidir crear señuelos para los atacantes --en ocasiones conocidos como tarros de miel (en el caso de sistemas individuales que actúan como señuelo) o panales (en el caso de redes enteras que funcionan como señuelo)-- como forma de atraer su atención, y distraerlos el tiempo suficiente para que sean mayores las probabilidades de identificar a los perpetradores. Si bien esta estrategia entraña riesgos adicionales (al igual que los asociados con lo que los profesionales del seguro denominan "molestias atractivas" o lo que los profesionales encargados de hacer cumplir la ley pudieran identificar como "operación encubierta"), cuando se aplican de manera adecuada pueden producir resultados definitivos y utilizables.

En un análisis final, la práctica apropiada de la seguridad entraña prever posibles casos de intrusión o compromiso, con herramientas y configuraciones adecuadas destinadas a recopilar evidencias de la existencia y la operación de actividades ilícitas o indeseadas. Dado que dicha evidencia es esencial para detectar el crimen informático, evitar su recurrencia y permitir su persecución legal, constituye un elemento clave de cualquier política de seguridad apropiada. Ello también explica por qué la actividad de rastreo y monitoreo representa una "verificación de la realidad" esencial para garantizar que la seguridad esté funcionando como debe ser y para ser capaces de hacer frente a los ataques o vulnerabilidades inesperados o no previstos cuando ocurran.

PREGUNTAS FRECUENTES

Las siguientes preguntas frecuentes, respondidas por los autores de este libro, están destinadas a medir su comprensión de los conceptos presentados en este capítulo y a ayudarlo en la aplicación práctica de estos conceptos. Para que el autor pueda responder sus preguntas sobre este capítulo, sírvase visitar el sitio www.syngress.com/solutions y pinchar en "Ask the Author".

P: ¿Qué medidas deben tomar los profesionales de las TI y de la aplicación de la ley en relación con los registros, trazas de auditoria y otras fuentes potenciales de evidencias o datos de respaldo durante el proceso de investigación de delitos informáticos?
R: La respuesta breve a esta pregunta es inventariar, inspeccionar, filtrar, documentar y preservar. Ampliemos un poco al respecto**:**

- **Inventariar**: Hacer un registro de todos los cortafuegos, enrutadores de selección, IDS, sistemas y servidores en uso por los cuales pudiera haber pasado el tráfico de ataque o sobre los cuales se pudo haber concentrado el tráfico o la actividad de ataque. Examinar cada elemento para identificar los archivos de registro o rastros de auditoria relacionados, y tomar nota de sus nombres y ubicaciones.
- **Inspeccionar:** Examinar los distintos archivos de registro o pistas de auditoria para determinar si contienen registros o entradas con trazas o evidencias relacionadas con el incidente que se investiga. De ser así, añadir el nombre y la ubicación de cada una de esas pistas de auditoria a su lista de archivos de evidencia.
- **Filtrar:** Los profesionales de las matemáticas llaman a este paso *reducción de datos* porque consiste en ignorar la entradas que no tienen relación alguna con el incidente que se investiga y recopilar solamente los que son pertinentes al asunto estamos tratando. La mayoría de los visores de sucesos o registros incluyen poderosas herramientas de filtrado de datos; aquellos que no las posean generalmente pueden ser importados a una hoja de cálculo o una base de datos en las que las herramientas de búsqueda incorporadas en esas aplicaciones nos ayudan a separar lo que es importante de lo que no nos debe interesar. Debemos cerciorarnos de que hemos anotado el nombre y la ubicación del archivo fuente original y de que nosotros (o un testigo experimentado) pueda dar fe de que a) el filtrado de datos es una práctica común en el análisis de registros y sucesos y b) podamos demostrar que existe una relación directa entre el archivo original y el archivo filtrado.
- **Documentar:** Explicar cómo las entradas de registro capturadas, las listas de sucesos, etc., brindan evidencias del delito informático. Además, documentar ampliamente las fuentes originales de esos datos, incluidas sus ubicaciones; nombre de archivo originales; ubicaciones actuales de archivos o unidades originales no alteradas; y cómo los datos fueron manejados desde que se detectó el incidente.
- **Preservar:** Tomar todas las medidas necesarias para preservar la fuente original de los archivo de registro o los datos de sucesos. Para ello quizás sea necesario retirar la unidad de disco duro del sistema o incluso sacar del

servicio un sistema con miras a preservar la evidencia en su estado más prístino posible. Véase el capítulo 10, "Recopilación y preservación de la evidencia digital", para obtener mayor información sobre el manejo la evidencia de delito informático.

P: Dada la necesidad de interpretar y explicar el contenido de algunos archivos de registro específicos o trazas de sucesos, ¿cómo puede un investigador obtener la información necesaria para realizar esta tarea?
R: Hemos señalado repetidamente que, si bien el tipo de información recopilada en los registros y trazas de sucesos es similar en los múltiples sistemas operativos y dispositivos perimétricos que existen, los detalles varían según cada sistema y aplicación. Para documentar la configuración e interpretar la importancia de los archivos de registro o las trazas de sucesos, será necesario contactar al proveedor del sistema operativo, aplicación o dispositivo de que se trate y solicitar a la empresa que nos brinde la documentación relacionada con esos archivos de registro o trazas de sucesos. En muchos casos, podemos encontrar esta información nosotros mismos si utilizamos el motor de búsqueda del proveedor en su sitio web o si consultamos su base de datos de apoyo técnico u otros recursos de información que tenga disponible en línea. Si no obtenemos los resultados deseados, quizás sea necesario recurrir al apoyo técnico del proveedor y solicitar ayuda para identificar y obtener la información correcta. En la mayoría de los casos, esto debería ser algo totalmente de rutina y relativamente fácil de realizar.
P: ¿Cómo puede un organización estar segura de que su IDS u otros dispositivos perimétricos están totalmente actualizados y poseen las firmas de ataque, actualizaciones, etc., más recientes?
R: En la mayoría de los casos, el proveedor del sistema o software que comercializa el IDS o los dispositivos perimétricos también ofrece un servicio de notificación, información de actualización en línea, e incluso quizás herramientas que podemos utilizar para evaluar el estado de la base de datos, las actualizaciones y mejoras para esos sistemas o servicios. Por lo general, si buscamos el producto en cuestión en el sitio web del proveedor lograremos encontrar indicaciones directas que nos lleven a esta información, ya que el proveedor comprende la importancia y la urgencia de esa información tanto como los propios clientes. Cuando tengamos dudas, debemos contactar al sistema de apoyo técnico del proveedor. En este caso también, obtener esta información debe ser un asunto totalmente de rutina y fácil de realizar.
P: Si una organización es objeto de un ataque aparentemente desconocido o para el cual no existe firmas, ¿cómo y a quién se deben informar esta situación?
R: Las probabilidades de ser presa de un primer ataque son bastante bajas, pero siempre ha de haber una organización que sea la primera víctima de nuevas vulnerabilidades o esté sujeta a ataques no documentados. Cuando esto suceda, es importante notificarlo a todas las partes que pudieran estar interesadas, incluidas las siguientes:

- Su ISP y otros ISP que pudieran estar entre sus redes e Internet.
- Cualquier proveedor cuyos productos manejen el tráfico relacionado con el ataque, incluidos cortafuegos, servidor proxy, enrutador de selección, IDS, aplicación, antivirus (cuando proceda) y sistema operativo. La mayoría de las empresas poseen mecanismos de reporte oficial que ponen al servicio de los clientes que deseen informar sobre incidente de seguridad. Sería de ayuda si

podemos identificar de antemano esas empresas de manera que nuestra respuesta durante un incidente no sea demorada porque estemos buscando esta información.

- Todos los grandes centros de intercambio de información de incidentes también deben ser notificados, incluidos www.cert.org, www.nipc.org y otras organizaciones más concentradas en temas de la seguridad que trabajen en temas relacionados con nuestra industria o nicho de mercado específico.
- En los Estados Unidos, si su estado tiene leyes penales que abarcan los ataques contra redes (como accesos no autorizados o negativa/interrupción de servicios de red), contacte a su oficina de policía local.
- En los Estados Unidos, el FBI y el Servicio Secreto han creado directrices encaminadas a estimular a las empresas a informar los ataques informáticos. Para una información detallada, véase *CIO Cyberthreat Response & Reporting Guidelines* (en formato PDF) en www.cio.com/research/security/incident_responde.pdf.
- Fuera de los Estados Unidos, contacte al organismo nacional o regional encargado de elaborar y hacer cumplir las leyes sobre el delito informático. Véase el Apéndice, "Fighting Cybercrime on a Global Scale" para obtener mayor información al respecto.

Recursos

- *Auditing Security Events Overview*
  www.microsoft.com/TechNet/prodtechnol/winxpro/proddocs/Audit_overview.asp
- *Log Capture and Analysis*
  www.microsoft.com/TechNet/itsolutions/ecommerce/maintain/monitor/logcanda.asp
- *Overview of Syslog* (La visión de GNU sobre la facilidad Syslog de UNIX)
  www.la.utexas.edu/lab/software/lib/gnu/glibc/libc_377.html#SEC380
- Utilice el motor de búsqueda de SANS para acceder a los artículos de la sala de lectura de SANS, entre ellos el escrito de Ray McAlarnen *Unix Security Logging*
  www.SANS.org
- Archivos de Lenny Zeltser sobre trazas y análisis de registros
  www.incidents.org/archives/y2k/123199-1220.htm
- *Configuring a Linux Firewall,* de Matthew Tam
  www.pisa.org.hk/download/seminar20011117-fw/linux_firewall.ppt
- *Reporting Spam,* por Mark Whitis
  www.freelabs.com/~whitis/spam_reporting/html
- RFC 822 (RFC sobre campos de encabezados SMTP de correo electrónico)
  www.faqs.org/rfcs/rfc822.html
- Everything E-mail
  http://everthingemail.net
- The Internet Mail Consortium
  www.imc.org
- Sam Spade
  www.samspade.org

- Ad Hoc IP Tools (Centro de intercambio de información para utilidades en línea de búsqueda y asignación de direcciones de correo electrónico, nombres de dominio, direcciones IP, etc.)
  www.tatumweb.com/iptools.htm
- *Intrusion Detection: A Guide to the Options*, por Peter Mell
  www.techrepublic.com/article_guest.jhtml?id=r00620011106ern01.htm&fromtm=e036
- Search Security (Buscar "IDS" o "intrusion detection system" para localizar excelentes artículos y recursos sobre este tema)
  www.searchsecurity.techtarget.com
- Cisco Systems
  www.cisco.com
- GFI LANGuard
  www.gfi.com/languard
- Internet Security Systems
  www.iss.net
- Network-1 Security Solutions
  www.network-1.com
- TripWire
  www.tripwire.com
- ISP Planet (Gráficos y estudios sobre proveedores MSSP)
  www.isp-planet.com/tehnology/mssp/participants_chart.html
  www.isp-planet.com/tehnology/mssp/firewalls_chart.html
  www.isp-planet.com/tehnology/mssp/services_chart.html
  www.isp-planet.com/tehnology/mssp/monitoring_chart.html
  www.isp-planet.com/tehnology/mssp/mssp_survey2.html
  www.isp-planet.com/tehnology/mssp/mssp_survey3.html
- Base de datos spam con base en DNS de Declude.com
  www.declude.com/junkmail/support/ip4r.htm
- Blocking Lists (listas de generadores de spam, hostigadores, bombas de correo electrónico y otros usos indebidos del correo electrónico)
  www.sandes.dk/abusers/abusers.html
- *Intrusion Signatures and Analysis*, por Stephen Northcutt y colaboradores, New Riders, 2001, ISBN: 0735710635.
- *Enhance Intrusion Detection with a Honeypot*, por John F.McMullen
  www.techrepublic.com/article_guest.jhtml?id=r00220010412mul01.htm&rfromtm=e036
- The Honeynet Project
  www.honeynet.org

CAPÍTULO 10

RECOPILAR Y PRESERVAR LA EVIDENCIA DIGITAL

Temas que se analizan en este capítulo:

- Para comprender el papel de la evidencia en un caso penal
- Recopilación de evidencia digital
- Preservación de la evidencia digital
- Recuperación de la evidencia digital
- Documentación de la evidencia
- Recursos de computación forense
- Para comprender los temas jurídicos

- Resumen
- Preguntas frecuentes
- Recursos

Introducción

En el capítulo 9 analizamos los métodos para detectar que se ha cometido un delito informático y rastrear a la persona o las personas que lo cometieron. El siguiente paso, quizás el más importante, para entablar proceso legal contra el culpable es la recopilación de la evidencia que se utilizará para conformar el caso que ha de presentarse a juicio.

La investigación forense se refiere al uso de las técnicas científicas o tecnológicas para realizar una investigación o establecer hechos (evidencias) en un caso penal. La investigación informática forense se define como la aplicación de las técnicas de investigación y análisis informático en interés de determinar posibles evidencias, según el investigador de delito informático Judd Robbins, según es citado por *Computer Forensic Legal Standards and Equipment* en el sitio web del Instituto SANS en http://rr.sans.org/incident/legal_standards.php. La computación forense incluye la identificación, obtención, documentación y preservación de la información que es almacenada o transmitida en formato electrónico o magnético (es decir, la evidencia digital). Como las huellas dactilares, la evidencia digital puede ser visible (como es el caso de los archivos almacenados en los discos y a los cuales se puede acceder por la estructura normal de directorio utilizando las herramientas normales de administración de archivos como el Explorador de Windows), o puede ser latente (no visible ni accesible fácilmente, por lo que se requiere algún tipo de procesamiento –con técnicas y software especiales– para localizarla e identificarla). Un aspecto importante de la computación forense se refiere a encontrar y evaluar el valor probatorio de estos "datos escondidos".

Se han desarrollado normas de computación forense que se aplican a la recopilación y preservación de la evidencia digital, y que se diferencian por su naturaleza de la mayoría de los demás tipos de evidencia y, en consecuencia, requieren métodos diferentes para su manejo. Seguir procedimientos adecuados, aceptados, y, en algunos casos, prescritos por la ley en el manejo de la evidencia es esencial para entablar un proceso judicial exitoso ante un caso de delito informático. El manejo adecuado de estos procedimientos es importante en dos fases diferentes de un juicio:

- Si la evidencia no es recopilada y manejada según normas adecuadas, el juez podría considerarla inadmisible (por lo general sobre la base de una *solicitud de exclusión de pruebas* presentada por el abogado contrincante) y los miembros del jurado no tendrán nunca la oportunidad de evaluarla ni de tenerla en cuenta para tomar su decisión.
- Si la evidencia es admitida, el abogado de la otra parte cuestionará su credibilidad durante el interrogatorio de los testigos que testificarán respecto de ella. Ello podría crear dudas a los miembros del jurado que quizás los lleven a desestimar la evidencia en el momento de tomar una decisión -- e incluso podría afectar la credibilidad del caso.

Toda la investigación tendrá poco valor si la evidencia que demuestra la culpabilidad del acusado no es aceptada en el juicio o si el jurado no le concede importancia. Es por ello que el manejo adecuado de la evidencia es uno de los temas más importantes que deben tener en cuenta los investigadores penales y los investigadores de delito informático en especial, dado el carácter intangible de la evidencia digital.

Habida cuenta de la importancia de este tema -- no sólo para los investigadores sino también para los fiscales, los jueces y los profesionales del sistema de justicia

involucrados en los casos de delito informático-- muchas organizaciones y publicaciones se dedican únicamente a temas relacionados con la evidencia digital. La Organización Internacional de Evidencia de Computación (IOCE) fue creada en 1995 con el objetivo de brindar un foro para que los organismos encargados de hacer cumplir la ley de todo el mundo pudieran intercambiar información sobre temas de computación forense; su componente en Estados Unidos es el Grupo de Trabajo Científico sobre Evidencia Digital (SWGDE). La Asociación Internacional de Especialistas de Investigación Informática (IACIS; www.cops.org) es una organización no lucrativa dedicada a educar a los profesionales encargados de hacer cumplir la ley en la esfera de la computación forense. El *International Journal of Digital Evidence* (www.ijde.org) es una publicación en línea dedicada a debatir sobre la teoría y la práctica del manejo de la evidencia digital. *Computer Forensics Magazine* (www.forensic-computing.com) es publicada por DIBS, productor de equipos de computación forense. *Computer Forensics Online* (www.shk-dplc.com/cfo) es una revista de la web dirigida por abogados y profesionales técnicos especializados en derecho informático. Existen muchos otros recursos similares que concentran su atención en la computación forense, y organizaciones de base más amplia como la Academia de Ciencias Forenses de Estados Unidos (www.aafs.org) abordan el delito informático y la evidencia digital, además de otros temas de la esfera forense.

Si analizamos cualquiera de estos recursos podremos ver que el manejo de la evidencia digital es un tema extenso que podría llenar fácilmente varios libros (y de hecho es así). El objetivo de este capítulo no es abarcar cada uno de los aspectos referidos a la recopilación y preservación de la evidencia digital. Por el contrario, en él se brinda una visión general del papel que desempeña la evidencia en un caso penal (especialmente en un caso de delito informático) y analizan los procedimientos típicos para el manejo de la evidencia digital, así como una técnicas específicas para ubicar y examinar la evidencia, como la recuperación de archivos supuestamente eliminados, la localización de información esteganográfica, la ubicación de datos "olvidados", y la desencriptación de datos encriptados. Asimismo, esbozamos los procedimientos para la documentación de la evidencia digital y analizamos algunos de los aspectos jurídicos referidos a la recopilación y manejo de la evidencia. Por último, brindamos muchos recursos excelentes disponibles en línea que ofrecen instrucciones detalladas para emprender las tareas que se describen en este capítulo, así como información sobre servicios comerciales y equipos que pueden ayudar en el proceso de recuperación de la evidencia.

Normas para el examen forense

Si bien las reglas de la evidencia sobre datos digitales no son muy definidas, siempre es preferible excederse en los requisitos mínimos para su admisibilidad. Cuando los investigadores toman precauciones adicionales para garantizar la integridad de la evidencia, más allá de lo que el tribunal pudiera considerar aceptable, no sólo se evita la posibilidad de que el juez excluya la evidencia sino que también será más favorable la impresión que esta causará sobre el jurado.

Organizaciones como IACIS brindan normas que rigen los procedimientos del examen forense por parte de sus miembros (véase www.cops.org/forensic_examination_procedures.htm). Demostrar ante el tribunal que durante la investigación hemos cumplido con esas normas elevadas reforzará nuestro caso.

La mayoría de las organizaciones y expertos en computación forense coinciden en algunas normas básicas en relación con el manejo de la evidencia digital, las cuales pueden resumirse como sigue:

- La evidencia original debe preservarse en un estado lo más cercano posible al estado en que fue encontrada.
- De ser posible se deberán hacer una copia exacta (imagen) del original para ser utilizada con fines de examen, de manera que no se dañe la integridad del original.
- Las copias de los datos destinadas al examen deben realizarse en medios que estén *estériles desde el punto de vista forense* -- es decir, es preciso que no haya existido dato alguno en el disco o el medio utilizado; debe estar completamente "limpio" y se debe haber verificado que no contenga virus ni defectos.
- Todas las evidencias deben ser etiquetadas y documentadas adecuadamente, además de preservarse la cadena de custodia; asimismo, se deberá documentar en detalle cada paso del examen forense.

Recopilación de la evidencia digital

Como analizamos en los capítulos 7 y 9, usualmente el administrador de red es la primera persona en detectar un delito informático en la empresa, mientras que el equipo de respuesta ante incidentes informáticos (en caso de existir uno en la empresa) tomará las medidas iniciales para detener el delito en curso y "congelar" la escena del delito antes de que asuma sus funciones el personal encargado de la aplicación de la ley. Incluso después de haberse llamado a la policía, en el proceso de recopilación de evidencia digital participan por lo general varias personas: los que toman las primeras medidas de respuesta (oficiales o personal oficial de seguridad que llegan primero al lugar del delito), el investigador o el equipo de investigación, y los técnicos y especialistas que son llamados para procesar la evidencia. Es importante designar a una persona a cargo de la escena del delito, la cual tenga la autoridad para tomar las decisiones finales en cuanto a cómo se preservará la escena del delito, como se realizará la búsqueda de la evidencia, y cómo se manejará esta. Por lo general este papel le corresponde al investigador de mayor rango. Es igualmente importante que cada miembro del equipo comprenda cuál es su papel y lo cumpla al detalle. La capacidad del equipo para trabajar de conjunto es un elemento vital para el éxito del proceso de recopilación de evidencias.

Papel de los primeros en tomar las medidas de respuesta

Este personal debe seguir el mismo principio al cual se comprometen los aspirantes a médicos que toman el juramento hipocrático: *Lo primero es no causar daño*. A menos que estén específicamente entrenados en la computación forense, las personas que llegan primero al lugar del delito no deben intentar hacer nada con las computadoras, sólo protegerlas para impedir que sean dañadas o alteradas. Es muy fácil que los delincuentes técnicamente astutos instalen troyanos en sus computadoras o las preparen para que automáticamente destruyan la evidencia cuando otra persona la apague o reinicie. El personal que se presente primero en el lugar del delito NO debe intentar apagar o

desenchufar la computadora ni acceder a ella en busca de evidencia. Por el contrario, su preocupación debe ser cumplir las tareas siguientes:

- **Identificar la escena del delito** Los oficiales que lleguen primero al lugar del delito deben determinar su dimensión y delimitarlo. Podría ser solamente una parte de una habitación o podría incluir varias habitaciones o incluso varios edificios si el sospechoso trabaja con una compleja red de computadoras. El personal debe comenzar a confeccionar una lista de los sistemas que pudieran estar involucrados en el incidente delictivo y de los cuales pudiera obtenerse evidencia.
- **Proteger la escena del delito** En un caso de delito informático en el que se procura encontrar evidencia digital, todos los sistemas de computación -- incluidos aquellos que parezcan estar apagados o que no funcionen-- deben ser considerados parte de la escena del delito, al igual que las computadoras portátiles como *laptops*, *notebooks*, etc. (incluidas las computadoras de mano y las PDA). Es posible que la orden de registro aplicable pongan límite a las piezas sujetas a incautación, pero el personal que llegue primero al lugar debe acordonar y proteger la mayor cantidad posible de computadoras y equipos electrónicos y esperar a que el investigador a cargo del caso determine qué equipos serán excluidos.
- **Preservar la evidencia temporal y frágil** En el caso de evidencia factible de desaparecer antes de la llegada de los investigadores (como la información que se visualiza en el monitor y que varía), este personal debe tomar todas las medidas posibles para preservarla o registrarla. Si se dispone de una cámara, se podrá preservar esta información tomando fotos de la pantalla. De no disponer de una cámara, los oficiales deben tomar notas detalladas y estar preparados para testificar ante un tribunal sobre lo que vieron.

NOTA

Para proteger el lugar del delito podría ser necesario también desconectar de la red las computadoras de manera de impedir que el sospechoso o un cómplice altere deliberadamente la evidencia, o que otra persona lo haga involuntariamente.

Papel de los investigadores

En algunos casos es posible que el equipo de TI de respuesta a incidentes informáticos ya haya comenzado a recopilar la evidencia. En tal caso, lo mejor es que un miembro del equipo de TI coordine la entrega (y explicación, si fuera necesario) de la evidencia con un miembro del equipo de investigación policial. El investigador (o el equipo de investigación) por lo general tiene la responsabilidad de coordinar las actividades de todas las demás personas en la escena del delito, y estará a cargo de lo siguiente:

- **Establecer la línea de mando** El investigador a cargo del lugar del delito debe garantizar que el resto del personal conozca cuál es la línea de mando y que las decisiones importantes se coordinen con él o ella. Las computadoras y los equipos conexos no se deben acceder, mover o retirar sin instrucciones explícitas del investigador principal. Los investigadores conforman y controlan la investigación. Si el investigador al mando debe ausentarse del lugar, deberá designar a una persona que le sustituya y con la cual estará en estrecho contacto

hasta tanto se recopile toda la evidencia y se traslade a un lugar seguro.

- **Realizar el proceso de búsqueda en el lugar del delito** Un investigador debe dirigir el proceso de búsqueda en el lugar del delito, el cual puede ser realizado por los investigadores o por otros oficiales. Si la orden judicial lo permite, los oficiales deberán buscar todo el hardware y software de computación, manuales, notas escritas y registros relacionado con la operación de las computadoras. Ello incluye impresoras, escáneres y todos los medios de almacenamiento como disquetes, discos ópticos (CD, DVD, etc.) cintas, Zip o Jaz y otros discos extraíbles, y cualquier disco duro "extra" que pudiera estar por lo alrededores.
- **Mantener la integridad de la evidencia** Los investigadores deben continuar protegiendo la evidencia mientras se realizan los preparativos para preservar la evidencia volátil, hacer duplicados de los discos, y apagar apropiadamente el sistema. El investigador deberá supervisar el trabajo de los técnicos en el lugar del delito y trasladarles cualquier consideración especial que se precise sobre la base del tipo de caso y el conocimiento sobre el/los sospechoso(s).

El papel de los técnicos en el lugar del delito

Los técnicos que respondan ante un caso de delito informático y se personan en el lugar del delito deberán, cuando sea posible, tener el entrenamiento específico en computación forense. (Véase más adelante en este capítulo la sección sobre "Entrenamiento y certificación en computación forense"). Los especialistas en computación forense deben tener un sólido conocimiento previo de la tecnología de computación y comprender cómo están estructurados los discos, cómo funcionan los sistemas de archivos y cómo y dónde se registran los datos. Por lo general, los técnicos de una escena del delito estarán a cargo de las siguientes tareas (aunque algunas de ellas pudieran coincidir con las de los investigadores):

- **Preservar la evidencia volátil y hacer copias de discos** Los datos volátiles son los que están en la memoria la computadora y consisten en procesos en ejecución. (Véase más adelante en este capítulo la sección "Preservar los datos volátiles" para conocer las instrucciones sobre cómo abordarlos). Las copias de los discos deben realizarse antes de apagar el sistema, en caso de que este esté preparado para borrar los discos al encenderse el equipo. (Véase la sección "Imagen de disco" para obtener información sobre cómo hacer duplicados de los discos).
- **Apagar los sistemas para su traslado** Es importante apagar adecuadamente los sistemas para mantener la integridad de la evidencia original. Una escuela de pensamiento plantea que la computadora debe apagarse mediante el procedimiento normal (cerrar todos los programas, etc.) a fin de evitar que se corrompan los archivos. Otra, por su parte, plantea que después de verificar que no se está ejecutando ningún programa de desfragmentación del disco, se debe apagar la computadora desconectándola de la entrada de electricidad, para evitar que se ejecute algún programa de autodestrucción que esté programado para el momento del apagado. Las computadoras con UNIX por lo general no deben ser apagadas abruptamente de esta manera mientras el usuario raíz tenga abierta una sesión porque hacerlo dañaría los datos. Algunos expertos en computación forense recomiendan que el técnico cambie las cuentas utilizando el comando **su** o, si dispone de la contraseña raíz, que se utilice el comando **sync;sync;halt** antes

de apagar el equipo.

NOTA

Si el equipo está apagado, el equipo de investigación usualmente deberá tomar la computadora y proceder a encenderla en un ambiente controlado. Cuando se accede al sistema, no se deberá realizar la carga desde el disco duro de la computadora sino de un disco de inicio controlado para impedir que el sistema operativo escriba en el disco, evitándose así que se sobreescriba alguna información crucial. Después se crea una imagen del flujo de bits del disco duro.

- **Etiqueteo y registro de la evidencia** Toda la evidencia debe ser etiqueteada y/o marcada con las iniciales del oficial o técnico, la hora y la información recopilada, el número del caso, y toda la información de identificación. La información de la etiqueta o la marca también se debe asentar en el registro de evidencia. (Véase más adelante éste capítulo la sección "Documentación de la evidencia").
- **Embalaje de la evidencia** La evidencia de computación, especialmente la que contenga tableros de circuitos expuestos (como discos duros) debe ser colocada en bolsas antiestática para su traslado. La documentación en papel, como manuales y libros, debe ser colocada en bolsas plásticas o protegida de cualquier otra manera.
- **Traslado de la evidencia** Toda la evidencia debe ser trasladada de la manera más directa posible hacia un lugar de almacenamiento seguro, que puede ser una habitación o un dispositivo de seguridad. Durante el traslado no se debe permitir que la evidencia entre en contacto con equipos que generen un campo magnético (incluidos los radios de la policía y otros equipos electrónicos en los autos policiales) ni se le debe dejar expuesta al sol o en un vehículo u otro lugar donde la temperatura sea superior a los 75 grados Fahrenheit. Durante el traslado se debe mantener meticulosamente la cadena de custodia.
- **Procesamiento de la evidencia** Cuando la copia del disco es llevada al laboratorio se puede reconstruir la imagen del disco y analizar los datos utilizando herramientas de software forense especiales. (Véase la sección "Equipos y software de computación forense" más adelante en este capítulo).

En la escena...

Lista de verificación de incautación de computadoras

Cada caso es diferente, pero debemos seguir determinadas directrices generales para la incautación de equipo de computación como evidencia en un caso penal. Si se siguen estos procedimientos, contribuiremos a proteger la integridad legal de la evidencia e impedir la pérdida de evidencias esenciales. Estos procedimientos presuponen que la computadora esté encendida al momento de nuestra llegada.

1- Fotografiar la pantalla del monitor para poder registrar todos los datos que se muestran en el momento de la incautación. Debemos tener en cuenta que quizás haya más de un monitor conectado a una misma computadora; los sistemas operativos modernos como Windows 2000/XP permiten mostrar la imagen hasta en 10 monitores. Los monitores acoplados a la computadora podrían mostrar partes del escritorio y las aplicaciones en ejecución aunque estén apagados.
2- Tomar medidas para preservar los datos volátiles. (Véase más adelante en este capítulo la sección "Preservar los datos volátiles").
3- Hacer una imagen del disco o de los discos para trabajar con ella, a fin de poder preservar la integridad del original. Este paso debe darse *antes* de apagar el sistema, previendo que el dueño haya instalado un programa de autodestrucción para que se active al momento de apagar o encender el equipo. (Véase más adelante en este capítulo la sección "Imagen de disco" para obtener información sobre los diferentes enfoques que se pueden utilizar para duplicar los discos).
4- Verificar la integridad de la imagen para confirmar que es una copia exacta, utilizando el verificador de redundancia cíclica u otros programas que utilice un algoritmo hashing o de suma de control para verificar que la imagen es exacta y fiable.
5- Apagar el sistema de manera segura según los procedimientos indicados para el sistema operativo que se utiliza.
6- Fotografiar la configuración del sistema antes de realizar cualquier movimiento, incluidas la parte posterior y frontal de la computadora mostrando todo el cableado y las conexiones.
7- Desenchufar el sistema y todos los periféricos, marcando/etiqueteando cada pieza que se recopila.
8- Utilizar una muñequera u otro método antiestático antes de trabajar con el equipo, especialmente con tarjetas de circuitos, discos y piezas similares.
9- Colocar las tarjetas de circuito, discos, etc., en bolsas aislantes para su traslado. Mantener todos los equipos lejos de fuentes de calor y campos magnéticos.

Preservar la evidencia digital

Por su naturaleza, la evidencia digital es frágil. Algunos datos son *volátiles*, es decir, son temporales y, a diferencia de los datos almacenados en disco, se perderán cuando la computadora se apague. Los datos que contiene el disco de una computadora pueden ser fácilmente dañados, destruidos o modificados ya sea deliberada o accidentalmente. El primer paso en el manejo de la evidencia digital es protegerla de cualquier tipo de

manipulación o accidente. La mejor forma de hacerlo es realizar de inmediato una imagen de copia completa del flujo de bits del medio en que está almacenada la evidencia.

NOTA

La *imagen del flujo de bits* es una copia que registra todos los bits de datos que fueron registrados en el dispositivo de almacenamiento original, incluidos los archivos ocultos, los archivos temporales, los archivos corruptos, fragmentos de archivos y archivos borrados que aún no han sido sobrescritos. En otras palabras, cada dígito binario es duplicado exactamente en el medio de copia. Las copias del flujo de bits (también llamadas en ocasiones *respaldos del flujo de bits*) utilizan los cálculos de código cíclico de redundancia (CRC) para validar que la copia es igual al original. Para más información véase *Bit Stream Backup--Defines* en www.forensics.intl.com/def2.html.

La "imagen especular" (mirror image) debe ser un duplicado exacto del original, mientras que este debe ser almacenado en un lugar seguro a fin de mantener su integridad. (Véase la sección "Factores ambientales" más adelante en este capítulo). La copia se realiza mediante un proceso llamado *imagen de disco*. En algunos casos, la evidencia podría estar limitada a unos pocos archivos de datos que se pueden copiar por separado en vez de crear una copia de todo el disco. En las secciones siguientes analizamos tanto las técnicas para realizar tanto una imagen de disco como una copia de archivos. También abordamos la importancia de garantizar la integridad de los discos que se utilizan para la obtención de una imagen especular o de una copia, así como los factores ambientales que pueden afectar la integridad de la evidencia, además de los problemas de preservación relacionados con tipos específicos de medios de almacenamiento.

Preservación de los datos volátiles

Los datos que se mantienen en almacenamiento temporal en la memoria del sistema (incluida la memoria de acceso aleatorio, la memoria caché, y la memoria de los periféricos del sistema como tarjeta de video o NIC) se denominan *datos volátiles* porque la memoria depende de la alimentación de electricidad para mantener su contenido. Cuando el sistema se apaga o si se interrumpe la alimentación de electricidad, los datos desaparecen.

Según el proyecto de Internet IEEE titulado *Guidelines for Evidence Collection and Archiving*, la evidencia que se debe recopilar primero es la más volátil. Esto es lógico porque la evidencia más volátil es la que mayores probabilidades tiene de desaparecer antes de ser documentada o recopilada. Este proyecto presenta la siguiente lista de "orden de volatilidad":

1- Registros y caché
2- Tablas de enrutamiento, caché ARP, tabla de proceso, y estadísticas del núcleo
3- Contenido de la memoria del sistema
4- Datos almacenados en el disco

La recopilación de los datos volátiles constituye un problema porque al hacerlo se modifica el estado del sistema (y el contenido de la propia memoria). Algunos expertos recomiendan que los investigadores o los técnicos de la escena del delito capturen datos como procesos en ejecución, el estado de la red y las conexiones de red, y una "descarga"

de los datos en la RAM, documentando cada tarea o comando que realice para hacerlo. Parte del trabajo puede realizarse utilizando comandos como **netsat** (tanto en sistemas Windows como en UNIX) y **nbtsat** (solamente en Windows) para visualizar las conexiones de red habilitadas. El comando **arp** nos mostrará cuáles direcciones están en la caché ARP (y por lo tanto se han conectado recientemente al sistema). El comando **dd** se puede utilizar para crear una foto del contenido de la memoria en las máquinas con UNIX, mientras que el comando **ps** se puede utilizar para visualizar los procesos en ejecución. En los equipos con NT/2000, la utilidad **pslist** puede utilizarse para obtener una lista de los procesos en ejecución, o estos pueden visualizarse en el Administrador de Tareas. Otros comandos como **ipconfig** (Windows) o **ifconfig** (UNIX) pueden utilizarse para obtener información acerca del estado de la red. Estos programas deben ejecutarse desde un CD forense especial que traigamos con nosotros (en lugar de ejecutarlos desde el disco duro de la computadora sospechosa) y no deberá ser necesario ejecutar ningún programa ni biblioteca desde el disco duro de la computadora.

Imagen de disco

La obtención de una *imagen de disco* se refiere al proceso mediante el cual se realiza una copia exacta de un disco. Esta operación a veces es también denominada *clonación de disco* (disk cloning) y también *ghosting*, pero estos últimos términos usualmente se refieren a imágenes creadas para fines distintos a los de preservar evidencias. La obtención de una imagen de disco se diferencia de una simple copia de todos los archivos en un disco en el hecho de que se preservan la estructura del disco y la ubicación relativa de los datos contenidos en este. Cuando copiamos todos los datos de un disco en otro, por lo general los datos se almacenarán en el nuevo disco en clústeres contiguos ya que existe espacio para almacenarlos. De esta manera, toda la información en ambos discos será idéntica, no así la forma en que está distribuida en ellos. Cuando creamos una imagen de disco (una copia del flujo de bits), se copia cada sector físico del disco de manera que los datos se distribuyen de la misma manera, y después la imagen es comprimida en un archivo llamado *archivo de imagen*. Esta imagen es exactamente igual al original, tanto desde el punto de vista físico como lógico.

Existen varias formas diferentes de crear un duplicado de un disco a nivel de bits, entre ellos las siguientes:

- retirar el disco duro de la computadora sospechosa y colocarlo en otra computadora (preferentemente una estación de trabajo para fines forenses) para hacer la copia
- colocar otro disco duro en la computadora sospechosa y realizar la copia
- utiliza un dispositivo de realización de imagen autónomo como el Dispositivo de toma de imágenes de acción rápida (RAID) de DIBS
- utilizar una conexión de red (conexión Ethernet, cable de conexión directa, USB, o similar) para transferir el contenido del disco a otra computadora o a una estación de trabajo con fines forenses.

La elección de uno de estos métodos por lo general depende del equipo de que se disponga. Una estación de trabajo portátil para fines forenses o un dispositivo de toma de imágenes autónomo probablemente sea la mejor solución, pero es también la más costosa.

Historia de la toma de imágenes

La toma de imágenes puede servir para muchos propósitos y se utilizó inicialmente con fines distintos a los de la computación forense y la recopilación de evidencia digital. Los investigadores de virus informáticos utilizaron la toma de imágenes de disco en los años ochenta cuando estudiaban los nuevos virus informáticos, con el objetivo de poder ejecutar el código del virus sin destruir o dañar los datos contenidos en el disco original. Copiar simplemente los archivos del virus no siempre resultaba porque algunos virus tenían que estar en partes específicas del disco para que realizaran la función para la cual habían sido creados. Por esta razón se desarrolló un programa para copiar exactamente los datos en la forma en que estaban ubicados en el disco, duplicando las direcciones de sector y creando un duplicado exacto o una "imagen" del disco.

Según el escrito *The History of Image Copying Technology* que aparece en el sitio web de DIBS Computer Forensics en www.forensic-computing.com/articles/imag.html, el primero en reconocer la utilidad de este programa para los investigadores de delitos fue el Inspector Detective John Austen de la Scotland Yard de Londres, y poco después nació el concepto de equipo de toma de imágenes con fines de computación forense.

Mientras tanto, la toma de imágenes se ha utilizado para crear salvas de seguridad que puedan ser utilizadas de manera rápida y fácil en caso de que el disco original sufra fallas, mediante una simple operación de recuperar el disco original a partir de su imagen. Otro uso popular de este procedimiento es la aceleración del proceso de instalación simultánea de sistemas operativos y software en un gran número de computadoras, con la misma configuración. A tal fin uno de los programas más populares es el Ghost de Norton. Existen varias versiones de Ghost; para más información, visite www.symantec.com y entre a Product.

Es importante que los investigadores comprendan las diferencias entre estos objetivos de la técnica de toma de imágenes y los productos que están destinados a esos fines diferentes. Los productos de clonación como Ghost no están destinados para preservar los datos del usuario en un disco; el objetivo es crear una configuración de instalación estándar que pueda distribuirse a múltiples computadoras. Si bien estos productos se pueden utilizar en un disco con datos de usuario, existe otro problema: la imagen que crean no es una copia bit-por-bit exacta del original. Según la Base de Conocimientos de Symantec, "Normalmente el programa Ghost no crea un duplicado exacto de un disco, sino más bien recrea la información de la partición según sea necesario y copia el contenido de los archivos". En consecuencia, la suma de verificación del disco de imagen casi siempre es diferente al valor de la suma de verificación del disco original. Ello podría ser motivo para que se excluya la evidencia en algunos tribunales, porque generalmente el Reglamento de evidencia exige que cuando se admita un duplicado como evidencia en lugar del original debe ser un duplicado *exacto* de este. Aunque algunos investigadores utilizan en ocasiones el software Ghost para crear imágenes de disco, y algunas versiones de este tienen switches y opciones que se pueden utilizar para obligarlo a crear una copia del flujo de bits, por lo general es mejor utilizar un software diseñado específicamente con fines forenses. Por otra parte, en el caso en que Ghost sea el único programa de duplicado de que dispongamos, la imagen que de él podemos obtener es mejor que no tener ninguna.

Software para la obtención de imágenes

Existen varios de estos programas que han ganado popularidad entre los especialistas de

computación forense encargados de hacer cumplir la ley. Estos programas fueron creados específicamente con el objetivo de obtener duplicados de discos para utilizarlos en el procesamiento de evidencia informática y el análisis de esta. A continuación presentamos algunos ejemplos de estos productos:

- **SafeBack** SafeBack ha sido comercializado a los organismos encargados de hacer cumplir la ley desde el año 1990 y ha sido utilizado por el FBI y la División de Investigaciones Criminales del IRS con el objetivo de crear imágenes de archivos con fines de examen forense y como evidencia. Es capaz de duplicar particiones individuales o discos completos de casi cualquier tamaño, y los archivos de imagen pueden transferirse a unidades de cinta SCSI o a casi todos los medios de almacenamiento magnético. El producto contiene funciones de CRC para verificar la integridad de las copias y las marcas de fecha y hora para mantener un rastro de auditoria de las operaciones del software. El proveedor brinda un curso de computación forense de tres días destinado a capacitar a los especialistas forenses en el uso del software. (De hecho, la compañía no brinda soporte técnico a personas individuales que no hayan pasado este entrenamiento). SafeBack está basado en DOS y se puede utilizar para copiar discos de DOS, Windows y UNIX (incluidos discos RAID con Windows NT/2000) en sistemas compatibles con Intel. Las imágenes se pueden salvar en archivos múltiples para almacenarlos en discos compactos o en medios de poca capacidad. Para evitar preocupaciones legales sobre una posible alteración, no se utiliza compresión ni traducción alguna en la creación de la imagen.
- **Encase** A diferencia de SafeBack, que es un programa basado en caracteres, Encase tiene una interfaz gráfica fácil de utilizar para muchos técnicos forenses. También brinda la posibilidad de vista previa de la evidencia, la copia de unidades (creando una imagen del flujo de bits) y de buscar y analizar los datos. Es posible buscar y analizar automáticamente documentos, archivos comprimidos y adjuntos de correo electrónico, además de que se incluyen los visores del Registro y gráficos. El software soporta múltiples plataformas y sistemas de archivo, incluido Windows NT con conjuntos de bandas y dispositivos Palm OS. El software denomina Archivo de Evidencia a la imagen del flujo de bits de la unidad y lo monta como una unidad virtual (un archivo de sólo lectura) que se puede explorar y examinar utilizando las herramientas GUI. Las marcas de fecha y hora y otros datos permanecen invariables durante el examen. El modo de vista previa permite al investigador utilizar un cable de conexión directa o conexión Ethernet para visualizar los datos en la máquina sin modificar nada; el proveedor afirma que es imposible alterar la evidencia durante este proceso.
- **ProDiscover** Esta aplicación con base en Windows, diseñada por el equipo de computación forense de Technology Pathways, crea copias del flujo de bits que se guardan como archivos de imagen comprimidos en la estación de trabajo forense. Sus características incluyen la capacidad para recuperar archivos borrados de espacios no utilizados, analizar los flujos de datos alternos de Windows NT/2000 en busca de datos ocultos, y analizar imágenes creadas con la utilidad *dd* de UNIX y generar informes. El proveedor tiene una lista de discusión por correo electrónico para intercambiar información y técnicas, y para el apoyo a los usuarios de productos de computación forense (www.techpathways.com).

NOTA

El Instituto Nacional de Normas y Tecnología (NIST, por National Institute of Standards and Technology) desarrolló una especificación de herramienta para la toma de imagen de disco como parte de su Proyecto de Ensayo de herramientas de computación forense, cuyo objetivo era facilitar la normalización de las herramientas automatizadas que se utilizan en las investigaciones de computación forense.

Herramientas autónomas de creación de imágenes

Las herramientas autónomas de creación de imágenes como la Unidad portátil de recuperación de evidencias (PERU, por las siglas en inglés de Portable Evidence Recovery Unit) y Dispositivo de toma de imágenes de acción rápida (RAID) de DIBS eliminan la necesidad de utilizar una segunda computadora, a la vez que mantiene la integridad de la computadora sospechosa. Estas unidades portátiles pueden hacer duplicados de los discos de la computadora sospechosa en otros disco duro limpio o en un medio óptico sin la necesidad de retirar el disco original de la computadora sospechosa.

El papel de la creación de imágenes en la computación forense

La creación de imágenes se acepta como una práctica típica en la computación forense para preservar la integridad de la evidencia original. La creación de imágenes difiere de la creación de una copia de seguridad normal de un disco (como previsión ante cualquier falla) en que los datos de entorno no se copian a la copia de seguridad; solamente se copian los archivos activos. Debido a que la copia de seguridad creada con programas de copias como la utilidad incorporada en Windows, Backup Exec, ARCserve, o similares no es un duplicado exacto (en otras palabras, una imagen del flujo de bits físico), estos programas no deben utilizarse para la creación de imágenes de disco. Los programas como Ghost de Norton incluyen *switches* que permiten crear una copia del flujo de bits, pero estos programas no fueron diseñados originalmente para un uso forense y no incluyen estas características y herramientas de análisis que presentan programas de creación de imágenes y sistemas de imágenes autónomos diseñado especialmente para el análisis forense.

Herramientas para toma de "fotos" y copia de archivos

En ocasiones no es posible ni recomendable hacer una imagen completa del flujo de bits de un disco. Ello puede deberse a que el sistema resulta vital en una misión y la administración no desea detener su funcionamiento durante una investigación o porque se ha decidido ya no emprender un proceso judicial. No obstante, existen maneras para recopilar los datos sobre la intrusión o cualquier otro delito con el objetivo de analizar qué sucedió e impedir que vuelva a suceder.

Un conjunto de herramientas de software diseñadas para que los administradores creen una "foto" del estado del equipo que ha sido comprometido es Coroner's Toolkit (Maletín de herramientas forenses), creado por los autores de la popular utilidad de UNIX llamada System Administrator Tools for Analyzing Networks (SATAN). Ejecutar estas herramientas en un sistema UNIX que ha sido objeto de una violación ayuda mucho en el análisis forense, porque nos brinda información sobre los procesos que se ejecutan, el estado de la red, los archivos borrados, información de usuarios, y muchas otros elementos. Para más información sobre este conjunto de herramientas, véase

http://rootprompt.org/article.php3?article=378.

En algunos casos, cuando la evidencia es de naturaleza documental, quizás sea posible presentar copias de archivos individuales en lugar de copiar el disco completo. Este método se debe utilizar únicamente cuando se necesitan documentos específicos identificables y no hay necesidad de buscar los datos de entorno o ningún otro dato oculto.

Consideraciones especiales

Debido a que determinados tipos de evidencia digital pueden ser increíblemente volátiles, y toda la evidencia digital puede ser dañada o comprometida por un proceso inadecuado de copia, almacenamiento o manejo, es esencial tener extremo cuidado y diligencia en el momento de recopilar y manejar la evidencia. Por lo tanto, se deben tener en cuenta numerosas consideraciones especiales, entre ellas factores ambientales, las marcas de fecha y hora, y la forma de preservar los tipos específicos de datos. Estas consideraciones se analizan en las secciones siguientes.

Factores ambientales

Los datos en soporte magnético se pueden destruir o dañar si se exponen a los efectos de un imán o al campo electromagnético que generan diversos tipos de equipos electrónicos. Las transmisiones de radiofrecuencia también pueden dañar los datos digitales, al igual que su exposición a la electricidad estática o a un calor extremo.

Es muy importante que los investigadores y los técnicos presentes en el lugar del delito estén conscientes de cuáles son los factores ambientales que pueden afectar la integridad de los datos. Deben garantizar que la evidencia digital sea empaquetada de manera que esté siempre protegida de cualquier posible daño, y que se almacene en un entorno libre de exposición electromagnética y con la adecuada ventilación.

Cuando se embalan medios magnéticos u ópticos (cintas, discos compactos, discos duros, disquetes, discos Zip/Jaz) estos se deben colocar primero dentro de una bolsa antiestática, y posteriormente en una caja con espacio suficiente para poder protegerlos con algún material que sirva de acolchonamiento. Se debe tratar de fijar el medio que se transporta al fondo o a los laterales de la caja para evitar que se mueva durante el trayecto. Debemos garantizar que se haga una relación del contenido y se pegue en el exterior de la caja, e identificarla como evidencia (como el número de la caja). También se deben colocar etiquetas para advertir a los encargados del traslado que deben manejar el paquete con cuidado. Si enviamos el paquete por correo o por algún otro medio, debemos utilizar un método que nos permita seguir su rastro (se recomienda el correo certificado siempre que se utilice el servicio postal).

Registrar las marcas de fecha y hora

La hora y fecha en que se crea o modifica un fichero puede ser un elemento importante en un caso penal. Debemos recordar que la marca de fecha y hora en los archivos concordará con la fecha y la hora que tenga el reloj del sistema. Algunos sistemas utilizan como predeterminada una zona horaria particular (por lo general la hora media de Greenwich, o GMT). Si el usuario configura el sistema sin configurar la zona horaria adecuada, o si el usuario cambia deliberadamente la configuración de hora y fecha, las marcas de hora y fecha podrían no corresponder con la realidad en cuanto al momento en que fueron creados los archivos.

Ello podría representar un problema si, por ejemplo, los registros del sistema muestran que un archivo fue creado en una fecha determinada y el sospechoso logra

probar que no se encontraba cerca de la computadora en ese momento. Por esa razón, debemos verificar la hora y la fecha de la configuración del sistema antes de apagar la computadora y documentarlo con una fotografía, si es posible; de lo contrario, se debe tomar nota escrita de esta información.

Cuando se abre un archivo se modifica el registro de fecha y hora. Es por ello que podría ser prudente fotografiar la pantalla donde se muestren la hora de acceso o modificación del archivo antes de abrirlo. Debemos estar preparados para testificar respecto de nuestras acciones y brindar testimonio especializado en el sentido de que las medidas que tomamos variaron las marcas de fecha y hora pero no modificaron el contenido del archivo. Cuando trabajamos totalmente sobre una imagen y no sobre una original, las fechas y horas originales están en el disco original. Podemos crear una segunda copia del original para ilustrar este hecho.

Para preservar los datos en PDAs y computadoras de mano

Si la evidencia está contenida en una PDA (personal digital assistant, o asistente digital personal) o en una computadora de mano (Palm OS o Pocket PC) debemos estar conscientes de que algunos de estos modelos pierden la información cuando se agotan sus baterías. La mayoría de ellos se comercializan con unidades recargables y resulta prudente mantener la unidad cargada hasta tanto los datos puedan ser extraídos.

Los investigadores de @Stake (www.atstake.com) crearon una herramienta forense denominada Palm Disk Duplicator (PDD, duplicador de disco palm) que hace un duplicado de los datos de los dispositivos que funcionan con Palm OS, incluido el Palm Pilots original y dispositivos comercializados por Sony (Clio), Handspring (Visor) y otros proveedores. El PDD crea una imagen completa de la memoria del dispositivo, la cual incluye todas las aplicaciones y los datos de usuario, así como los datos que han sido marcados para su eliminación. (Estos no son eliminados realmente hasta tanto ocurra la próxima sección de sincronización). La herramienta también recopila información acerca del dispositivo, como la versión del sistema operativo, información sobre el procesador y la RAM/ROM, y el ID Flash. Para más información sobre PDD**,** véase el documento oficial en http://63-251.138.38/atstake/acrobat/pdd_palm_forensics.pdf.

Si no contamos con esa herramienta, otra forma de preservar los datos contenidos en un dispositivo de mano es copiar los ficheros de interés en una memoria flash o similar. La mayoría de estos equipos de mano tienen una ranura para utilizar algún tipo de medio de memoria flash.

NOTA

LCTechnology International realiza un curso de 16 horas sobre el tema de técnica forense para dispositivos digitales personales que se concentra en la recuperación de evidencias en equipos Palm, Pocket PC y otros similares. Para más información, véase www.lc-tech.com/personal%20Digital%20Device%20Forensics.asp.

Recuperación de la evidencia digital

En algunos casos de delito informático la evidencia que necesitamos estará bien guardada en el disco duro (o en un medio extraíble de fácil acceso), y los archivos estarán convenientemente nombrados para indicar su contenido. En otros casos, el investigador no es tan dichoso. Los delincuentes informáticos pudieran presentir que están a punto de

ser descubiertos y borrarán los datos incriminatorios e incluso formatearán y/o reparticionarán el disco. Algunos delincuentes con experiencia técnica específica utilizan técnicas sofisticadas para esconder los datos en lugares no tradicionales. En otros casos, los datos que serían de utilidad al investigador no se almacenan nunca en el disco –al menos no con el conocimiento del usuario de la computadora. No obstante, una gran cantidad de *datos de entorno* son almacenados en lugares como archivos caché, archivos de intercambio o paginación, y archivos temporales (temp), así como datos remanentes que ocupan espacio no asignado en el disco, el espacio no utilizado en clústeres cuyo tamaño es mayor que el de los archivo que contienen, y las brechas entre particiones o sectores. En las secciones siguientes analizamos la forma en que los investigadores pueden recuperar los datos que no se muestran de inmediato cuando exploramos la estructura de archivos pero que pudieran resultar vitales para conformar un caso penal.

NOTA

La recuperación de datos digitales, especialmente los datos parcialmente destruidos o supuestamente borrados, en ocasiones se denomina *buceo en basureros electrónicos*.

Recuperación de datos "eliminados" y "borrados"

Muchos usuarios de computadoras –incluidos los delincuentes informáticos piensan que cuando eliminan un archivo este se borra del disco duro. Incluso se ha referido que supuestos expertos en computación han dicho por televisión y radio que una vez que se vacía la papelera de Windows, lo archivos desaparecen del disco duro. Esto sencillamente no es verdad. Cuando se elimina un archivo no se elimina su contenido; sencillamente se elimina su localizador de la tabla de asignación de archivos (FAT), la tabla maestra de archivos (MFT) u otro esquema que el sistema operativo utilice para ubicar un archivo particular en el disco. Los datos se almacenan en el disco en *clústeres*, que son unidades con un determinado número de bits. Como las partes de un archivo no siempre se almacenan en clústeres contiguos en el disco físico, sino que pueden estar diseminadas por el disco en ubicaciones separadas, cuando se elimina el localizador es difícil reconstruir el archivo –pero la palabra *difícil* no es igual a *imposible*.

Cuando se elimina el archivo, la ubicación en el disco en que está almacenado se marca como *espacio no asignado*, lo cual significa que está disponible para cuando sea necesario escribir nuevos datos. Sin embargo, en un disco de gran capacidad podría pasar bastante tiempo antes de que esa parte específica del disco vuelva a recibir nuevos datos. Mientras tanto, los datos antiguos permanecen ahí y pueden ser recuperados si el investigador tiene las herramientas apropiadas.

Se considera que un disco nuevo está "limpio", o totalmente vacío, pero en realidad está lleno de *caracteres de formato*, que son caracteres repetidos hechos por la máquina de verificación en la fábrica. Cuando los archivos y directorios son creados y salvados en el disco, sobrescriben lo caracteres de formato. Cuando los archivos o directorio son eliminados los clústeres en que son almacenados se reasignan hasta tanto se escriban en ellos nuevos datos. Cuando se formatea un disco no eliminan los datos. Incluso si el disco está reparticionado mediante FDISK, Partition Magic o una utilidad similar, los datos permanecen en su lugar hasta tanto se sobrescriban esos clústeres.

Existen varios programas de software que se pueden utilizar para recuperar los archivos en el espacio no asignado. Un ejemplo es la herramienta GetFree

comercializada por New Technologies Inc. (www.forensics-intl.com/getfree.html), los creadores de SafeBack. NTI produce varios paquetes de software forense, y GetFree está destinado específicamente para los especialistas de la aplicación de la ley y de la esfera forense con el objetivo de que se recopilen los datos de los espacios no asignados en la computadoras que funcionan con los sistemas operativos de Microsoft. Estos datos se pueden visualizar con la ayuda de otras utilidades como Filter I de NTI. WetStone Technologies (véase el sitio web de la empresa en www.wetstonetech.com) produce un programa llamado Extractor (o SMART Extractor) que recupera los archivos eliminados en Red Hat Linux.

En una computadora los datos supuestamente eliminados pueden estar ubicados en muchos lugares. Por ejemplo, cuando un disco es reparticionado es posible que los datos que estaban en las particiones configuradas anteriormente vayan a parar al espacio entre particiones, llamado la *brecha de partición*. Las herramientas de búsqueda en disco pueden localizar estos datos escondidos, los cuales pueden entonces convertirse en una posible fuente de evidencia para los investigadores.

Desencriptar los datos encriptados

Como aprendimos en el Capítulo 7 "Cómo prevenir el delito informático", la encriptación es un método de cifrar los datos para que no puedan ser leídos por quien no tenga la contraseña o la clave para desencriptarlos. Los delincuentes informáticos a menudo utilizan la encriptación para ocultar la naturaleza delictiva de sus datos. Podrían encriptar mensajes de correo electrónico que contengan frases incriminatorias, o podrían encriptar documentos factibles de utilizar como evidencia, o fotografías pornográficas de niños objeto de contrabando.

Los criptoanalistas se especializan en descifrar los algoritmos de encriptación. La encriptación altamente segura es difícil de descifrar, pero en muchos casos los delincuentes informáticos utilizan métodos relativamente débiles como la protección por contraseñas de documentos de Office que viene incorporada en las aplicaciones. Existen varios programas para recuperar contraseñas que pueden ser utilizados por usuarios legítimos que protegen sus documentos y que después olvidan las contraseñas. Estos programas también se pueden utilizar para descifrar las contraseñas de los documentos de Word o Excel. Estos son básicamente ataques de fuerza bruta y de diccionario. Un ejemplo es Advanced Office 2000 Password Recovery. Programas similares están diseñados para descifrar las contraseñas en el cliente de correo electrónico de Outlook Express, contraseñas de Internet Explorer para sitios web protegidos, archivos creados por programas de gestión financiera Quicken y QuickBooks, archivos PDF protegidos por contraseñas, documentos protegidos creados por Lotus 1-2-3 y otros programas de Lotus Office Suite, documentos protegidos creados por Corel WordPerfect, archivos con la extensión .zip protegidos por contraseñas y muchos otros archivos. Para obtener información sobre muchos de estos programas de descifrado de contraseñas, véase www.crackpassword.com.

Paraben (www.paraben-forensics.com) comercializa una serie de programas de desencriptación como parte de su línea de programas forenses. La serie está diseñada para descifrar contraseñas para una gran cantidad de programas de software populares y tipos de archivos, incluidos los sistemas operativos Windows XP/2000/NT, Exchange, módulos de Visual basic de VBA, y muchos otros.

Cómo encontrar los datos ocultos

En muchos casos los datos ocultos en un disco duro pueden ser muy útiles para los investigadores en la conformación de un caso contra un sospechoso de delito informático. Algunos de estos datos podrían ser datos de entorno que quedan después de que se eliminan archivos o cuando los discos son particionados. Además, existen varios lugares en los que los datos pueden ser ocultados por criminales experimentados con la ayuda de un editor de disco, software esteganográfico y otros métodos. Encontrar, recuperar y reconstruir estos datos ocultos puede resultar ser un proceso en extremo tedioso, pero bien vale la pena el esfuerzo si se obtiene una evidencia capaz de sustentar y ganar un caso.

Donde se esconden los datos

Un *sector de disco* es una unidad de espacio de tamaño fijo (como 512 bytes). En los discos duros más antiguos podrían existir espacios de almacenamiento desperdiciados en las pistas exteriores por la forma en que los discos están divididos en sectores que contienen un número igual de sectores por pistas. La discrepancia en la circunferencia entre las pistas internas y externas provoca este desperdicio de espacio. En algunos casos es posible esconder datos en el espacio entre sectores en la pista exteriores más grandes. Este espacio se denomina *brecha de sector*. Algunos servicios de recuperación de datos podrían ser capaces de ubicar y recuperar los datos que se encuentran ocultos en esta brecha.

Otro de los lugares donde pueden esconderse los datos es en la *zona no utilizada* ocasionada por los tamaños de archivos que no se corresponden exactamente con el tamaño de los clústeres donde son almacenados. El tamaño de los clústeres puede variar, pero cada vez que un archivo o parte de un archivo es más pequeño que el tamaño de un clúster, los bits remanentes en el clúster quedan sin usar. En los sistemas de archivo como FAT16, donde los tamaños de clúster aumentan sobre la base del tamaño de la partición, ello puede provocar que se creen muchos espacios vacíos, y dichos espacios pueden ser utilizados para ocultar otros bits de datos. Aquí se pueden ocultar datos sin que el usuario se percate de ello. Los clústeres están formados por sectores. Cuando el archivo demasiado pequeño para llenar el último sector en un archivo, DOS y Windows utilizan datos aleatorios de búferes de memoria del sistema para cubrir la diferencia. A esto se le llama *RAM vacía* y puede conllevar a que datos de la sesión de trabajo (la hora del último inicio de sesión de la computadora) se almacenen en el disco en este espacio no utilizado con el objetivo de "rellenar" el sector final En el espacio no utilizado puede existir cualquier tipo de datos procedentes de la memoria que pudieran servir a la investigación. Todos los tipos de disco (disquetes, discos duros y discos extraíbles) son susceptibles de tener espacio no utilizado. Las herramientas de análisis de computación forense como las que comercializa NTI pueden recuperar los datos escondidos en estas zonas no utilizadas.

Los *datos fantasmas* se crean porque la alineación vertical y horizontal de los cabezales mecánicos que escriben al disco no es exactamente la misma cada vez que se realiza una operación de escritura. Esto significa que incluso en el caso en que se sobrescriban los datos, podrían permanecer rastros de los datos anteriores. En ocasiones es posible reconstruir los datos a partir de estos remanentes, si bien esa es una tarea en extremo costosa y prolongada.

Para detectar los datos esteganográficos

Los software esteganográficos esconden los archivos dentro de otros archivos, utilizando

espacios libres o el bit menos importante para codificar los mensajes. Por ejemplo, los datos pueden ocultarse en un archivo de imagen alterando ligeramente un solo bit relacionado con un píxel particular. Si un píxel en una foto tiene un componente rojo, representado por el número binario 10001100, el bit menos importante (el último) puede cambiarse a 1, haciendo que el número binario sea entonces 10001101. Esto hará que ese píxel sea un bit más rojo, lo cual no será apreciable. Esto crea un bit "escondido", un 1. Para crear un 0, se dejaría como estaba el bit menos importante. Todo el archivo que queramos esconder se descompone en sus componentes binarios y estos son escondidos en diferentes partes de la imagen. Es posible determinar cuáles píxeles contienen los bits escondidos, y en qué orden, con la ayuda de un generador de números aleatorios que utiliza una clave, de manera que solamente la persona que conoce la clave podrá reconstruir el mensaje escondido al recuperar los bits ocultos en el orden correcto.

En el mercado existen varios programas "antiesteganográficos" que nos permiten detectar la presencia de datos ocultos dentro de otros archivos utilizando técnicas esteganográficas. Entre estos software está StegoWatch, comercializado por WetStone Technologies; para más información, véase www.wetstonetech.com/stegowatchdatasheet.pdf.

Detectar la presencia de datos enteganográficos es mucho más fácil que extraer el mensaje mismo. Ello por lo general se realiza mediante software que chequean el perfil estadístico de una imagen y buscan detalles estadísticos dejados por el software esteganográfico. El análisis esteganográfico es el proceso mediante el cual se detecta la esteganografía en los archivos y se inhabilitan los mensajes encubiertos.

Para más información sobre este tópico, véase *Steganalysis: The Investigation of Hidden Information* en www.jjtc.com/pub/it98a.htm.

Flujos de datos alternos

Los sistemas Windows NT/2000 que utilizan el sistema de archivos NTFS soportan una característica llamada *flujos de datos alternos* (ADS). Se pueden crear flujos de cualquier tamaño y vincularlos a archivos normales visibles (llamados *archivos primarios*), pero los flujos son invisibles y se necesita un software especial para detectarlos. Estos flujos brindan otra función legítima. Permiten que los sistemas operativos NT/2000 soporten los archivos Macintosh, que consisten en *dos bifurcaciones*: una bifurcación de datos y una bifurcación de recursos. La bifurcación de recursos se almacena en el flujo de datos alternos oculto. Además, algunos programas antivirus utilizan los flujos para almacenar sumas de verificación para archivos. Los flujos se pueden adjuntar a archivos o a directorios (carpetas).

No es posible eliminar directamente un flujo de datos alternos sin eliminar el archivo o directorio primario. De hecho, muchas herramientas destinadas a la eliminación de archivos eliminan solamente los archivos primarios y no los ADS. Los troyanos y virus se pueden esconder en flujos, o los delincuentes técnicamente expertos pueden esconder en ellos datos incriminatorios. Los flujos se pueden crear en el Block de Notas y otros programas preparados para ADS. El nombre de archivo tiene dos partes, está compuesto por el nombre del archivo primario y el nombre de flujo, separados por dos puntos de puntuación. Por ejemplo, si el archivo primario se llama *filename.txt*, el flujo podría llamarse *filename.txt:filestream*. El nombre de flujo no lleva una extensión de archivo como un archivo normal. Cuando se edita el archivo primario no se modifica el contenido del archivo de flujo, y viceversa. Para más información, véase ADS FAQ en

www.heysoft.net/Frames/f_faq_ads_en.htm.

Método para esconder archivos

Existen varias formas de esconder los archivos en un sistema. En los sistemas de archivos DOS/Windows, establecer el atributo oculto (**-h** en la línea de comando, o establecer el cuadro de diálogo File Properties en el GUI) evitará que el archivo se muestre como respuesta ante el comando **DIR** en la línea de comandos o en una lista de archivos en el Explorador *si* se ha predeterminado esa configuración en Opciones de carpetas ¦ Ver. No obstante, si la opción Mostrar Archivos y Carpetas Ocultos está habilitada, estos archivos ocultos se mostrarán. En los sistemas UNIX, los archivos y directorios cuyos nombres comienzan con un punto son ocultos y no se muestran como respuesta al comando **ls** a menos que se utilice el switch **-a**.

En la escena...

Esconder archivos a la vista de todos

Otro método para esconder archivos se conoce como *esconder a la vista de todos*. Con este método, un delincuente informático da a un archivo un nombre que lo hace aparecer como lo que no es y como algo que no resultaría de interés para un investigador. Por ejemplo, un archivo de imágenes que contenga pornografía infantil podría encontrarse como algo parecido a window.sys y almacenarse en el directorio de sistema de Windows. Para un observador casual aparecerá como cualquier otro archivo de sistema operativo. Cuando el delincuente desea acceder a él, sencillamente le cambia la extensión a .jpg o .gif y lo abre en cualquier programa de imágenes.

Las herramientas como Rootkit de NT nos permiten esconder archivos y directorios (así como procesos y entradas del Registro) cambiándoles el nombre con el prefijo *_root*. Esto funciona solamente en la máquina local; si se accede a distancia al archivo compartido asignándole una unidad, los archivos y directorios root serán visibles. El Rootkit de NT funciona en equipos con Windows NT/2000; el concepto proviene de los rootkits originales basados en UNIX.

Los sistemas Linux que utilizan el sistema de archivo ext2 brindan varias formas para esconder los datos. Una manera de esconder los archivos en la mayoría de los sistemas de archivo UNIX (incluido el ext2) es ejecutar un proceso que mantiene abierto el archivo, y entonces lo elimina utilizando el comando **/bin/rm**. Los datos permanecerán en el disco y en ese espacio hasta tanto sean sobrescritos por otros archivos. Es posible encontrar herramientas de "unerase" (deshacer la eliminación) que recuperan los archivos de ext2 eliminados. También es posible recuperar manualmente esos archivos utilizando la utilidad *debugfs*. Este proceso se describe en *Linux Ext2fs Undeletion mini-HOWTO* en www.tldp.org/HOWTO/mini/Ext2fs-Undeletion.html.

El sistema de archivo ext2 almacena los datos en *bloques* y crea espacios no utilizados cuando los archivos son de un tamaño menor a los bloques de 1-, 2- o 4KB utilizados por el sistema de archivos. Los datos se pueden esconder en ese espacio no utilizado, como sucede en los sistemas de archivos de DOS y Windows.

La papelera de reciclaje

Aunque podría parecer evidente para los expertos técnicos el hecho de que mover un archivo hacia la Papelera de reciclaje ni siquiera elimina el localizador del archivo como

lo hace la acción de borrarlo, muchos delincuentes informáticos NO son expertos técnicos y podrían pensar que han borrado la evidencia cuando, de hecho, esta permanece intacta en la Papelera de reciclaje. Naturalmente, esto será así más probablemente en el caso de los delitos informáticos "no técnicos", como la pornografía infantil, más que en los casos de intrusión en redes y otras actividades ilegales. No obstante, teniendo en cuenta el nivel de conocimientos técnicos requerido (o más bien, *no* requerido) para lanzar ataques utilizando los métodos script-kiddie y click-kiddie, nunca es ocioso verificar. La evidencia que necesitamos podría estar esperando por nosotros, fácilmente recuperable con un simple click del ratón.

Para ubicar la evidencia olvidada

Una gran cantidad de datos son almacenados automáticamente en las computadoras por lo programas de aplicación y/o el sistema operativo. Algunos usuarios desconocen que estos datos son almacenados; otros quizás lo sepan pero podrían olvidar deshacerse de ellos cuando destruyen evidencia en un sistema. En dependencia de la naturaleza del delito, algunos de estos datos podrían ser útiles al investigador del delito informático. Entre las fuentes de evidencia olvidada están las cachés de web, archivos temporales (temp), archivos de intercambio/paginación, y registros de aplicación. En las secciones siguientes analizamos cada uno de estos recursos y la forma en que pueden brindar información probatoria valiosa en algunos casos de delito informático.

Cachés de web e historiales de URL

Los buscadores web están diseñados para funcionar. Los usuarios desean que sus páginas web emerjan en el buscador lo más rápidamente posible. Una forma de acelerar el acceso es hacer que el buscador tome el archivo del disco duro de la computadora local, en lugar de descargarlo por una conexión Internet mucho más lenta. Por esta razón, los buscadores web están predeterminados para almacenar en la caché las páginas que un usuario visita, conjuntamente con archivos de gráfico, sonidos y otros conexos. En otras palabras, toda esta información se almacena en el disco duro de la computadora de manera que si visitamos nuevamente la misma página esta se pueda recuperar rápidamente del disco. Estos archivos generalmente se denominan *archivos temporales de Internet* y se almacenan en una carpeta especial, usualmente bajo el nombre de perfil del usuario, como se muestra en la figura 10.1. Estos archivos nos brindan un registro visual de los sitios que el usuario ha visitado recientemente. Esta información puede ser especialmente útil en los casos de pornografía infantil o en casos de terroristas que frecuentan determinados sitios web.

Figura 10.1 Los archivos temporales de Internet (la caché web) nos pueden brindar pistas sobre los sitios web que ha visitado recientemente el usuario de una computadora. (Insertar aquí la figura que aparece en la página 573 del original).

Otras fuentes de información sobre los sitios web visitados es la carpeta Historial. En ocasiones los delincuentes informáticos borran sus archivos temporales de Internet pero se olvidan de borrar los registros del historial. A diferencia de la caché web, la carpeta Historial no contiene copias reales de las páginas web; en realidad contiene una lista de vínculos (URL) a esos sitios. En los equipos con Windows que utilizan el buscador Internet Explorer, estos vínculos usualmente están ubicados en una carpeta llamada Historial bajo el nombre de perfil de usuario, como se muestra en la figura 10.2.

(Para cada usuario que tenga una cuenta local en la computadora se crean cachés web e historiales separados).
Figura 10.2 La carpeta Historial contiene los URL de los sitios web recientemente visitados. (Insertar aquí la figura que aparece en la página 574 del original).

El buscador Netscape almacena su historial de búsqueda en un archivo con el nombre netscape.hst y otro con el nombre fat.db, ubicado en el directorio Caché bajo el nombre del usuario en el subdirectorio Program Files\Netscape\Users. Estos son archivos binarios, por lo que se necesita una utilidad para visualizar los datos que contienen.

Archivos temporales

Las aplicaciones como Microsoft Word crean archivos temporales (temp) en el sistema. Estos archivos se utilizan para rastrear los cambios efectuados al original y recuperarlos si el programa falla. Cuando se trabaja en un documento de Word se crean decenas de archivos temporales, los cuales generalmente se almacenan en el mismo directorio que el archivo .doc original. En teoría, cuando cerramos el documento o la aplicación, estos archivos temporales se borran, pero esto no siempre es así. Incluso cuando el sistema los "borra" permanecen en el disco hasta tanto sean sobrescritos, al igual que sucede con los demás archivos "borrados", y pueden ser recuperados utilizando herramientas diseñadas a tal fin.

Otros archivos temporales son los que se descargan desde Internet o los adjuntos de correo electrónico que se han abierto y salvado en un directorio Temp, usualmente ubicado en el directorio raíz del sistema (el directorio donde están ubicados los archivos del sistema operativo, como WINDOWS o WINNT). Estos archivos temporales se pueden borrar cuando el sistema se apaga o se reinicia, lo cual es una razón adicional para obtener, cuando sea posible, una imagen del disco *antes* de apagar el sistema.

NOTA

Los archivos temporales casi siempre tienen la extensión .tmp. Si realizamos una búsqueda de todos los archivos con esta extensión podremos obtener una amplísima cantidad de datos olvidados, algunos de los cuales pueden ser útiles como evidencia.

Archivos de intercambio y de paginación

Los sistemas operativos más modernos utilizan una característica llamada *memoria virtual* que permite al sistema "burlar" a las aplicaciones y hacerlas creer que la computadora tiene más memoria RAM que la que está realmente instalada. Una parte del disco duro se utiliza como memoria adicional y los datos se intercambian desde la memoria física real hacia este espacio de espera en el disco según lo necesite el procesador. En Windows 9x, estos datos se mantienen en un archivo llamado *archivo de intercambio*. En los sistemas Windows NT/2000 se le llama *archivo de paginación* porque los datos se intercambian en unidades llamadas *páginas*. Los sistemas Linux crean una partición de intercambio en el disco para este mismo propósito. Estos archivos generalmente los crea el sistema operativo de manera automática.

Esto archivos contienen todo tipo de datos, incluidos mensajes de correo electrónico, páginas web, documentos de Word, y cualquier otro trabajo que se haya realizado en la computadora durante la sesión de trabajo. Muchos usuarios de computadoras desconocen de la existencia de estos archivos o no comprendes realmente

lo que son, lo que hacen, y el tipo de datos que contienen. Algunos archivos de intercambio son temporales mientras otros son permanentes, en dependencia del sistema operativo que se utilice y la configuración que tenga. Es posible que los archivos estén marcados con el atributo oculto, lo cual los hace invisibles en la estructura de directorio con la configuración predeterminada. El sistema operativo crea los archivos de intercambio en una ubicación predeterminada. En el Cuadro 10.1 se muestra el nombre de archivo de intercambio y su ubicación predeterminada para distintos sistemas operativos de Microsoft. Obsérvese que los usuarios con conocimientos técnicos pueden cambiar la ubicación del archivo de intercambio o crear archivos de intercambio/paginación adicionales, de manera que en un sistema pueden existir múltiples ubicaciones para la memoria virtual.

Cuadro 10.1 Nombres de archivos de intercambio y su ubicación

Sistema operativo	**Nombre de archivo**	**Ubicación predeterminada**
Windows 3.*x*	386SPART.PAR	Subdirectorio Windows/Sistema o directorio raíz de la unidad designada en el cuadro de diálogo de memoria virtual
Sistema operativo	**Nombre de archivo**	**Ubicación predeterminada**
Windows 9*x*	WIN386.SWP	Directorio raíz de la unidad designada en el cuadro de diálogo de memoria virtual
Windows NT/2000/XP	PAGEFILE.SYS	Directorio raíz en la unidad en la que está instalado el directorio raíz del sistema (WINNT por defecto)

Para encontrar la ubicación del archivo de intercambio o paginación debemos abrir el cuadro de diálogo de Memoria virtual. (Es aquí también donde el usuario puede cambiar la ubicación del archivo). Por ejemplo, en Windows XP Profesional, se abre la applet **Sistema** desde el Panel de control, se hace clic en la ficha **Avanzada**, clic en el botón **Configuración** en **Rendimiento**, clic nuevamente en la ficha **Avanzada** y luego en **Cambiar** al final de la página debajo de **Memoria Virtual.** Esta serie de pasos nos lleva hasta el cuadro de diálogo de Memoria virtual donde podemos ver la ubicación de uno o más archivos de paginación, como se muestra en la figura 10.3.

Figura 10.3 Para ver la ubicación, el tamaño y el estado de uno o varios archivo de

paginación en Windows XP, usamos el cuadro de diálogo de Memoria Virtual. (Insertar aquí la figura que aparece en la página 576 del original).

Podemos entonces navegar hasta la unidad en la cual el archivo está almacenado y localizarlo en ella, como se muestra en la figura 10.4. No obstante, obsérvese que el archivo de paginación no será visible a menos que hayamos desmarcado la casilla **Ocultar archivos del sistema operativo protegidos (recomendado)** en la configuración de **Herramientas ¦ Opciones de carpetas ¦ Ver** en el Explorador de Windows.

Figura 10.4 Cuando los archivos de sistema operativo protegidos no están ocultos, el archivo de paginación se puede visualizar en el Explorador de Windows**.** (Insertar aquí la figura que aparece en la página 577 del original).

Es posible visualizar el archivo de intercambio/paginación con una utilidad como DiskEdit, pero la mayor parte de la información que contiene es binaria (consistente en números 0 y 1) y no es muy útil. Existen programas especiales como Net Threat Analyzer y el "editor forense inteligente" Filter I, que están destinados a leer los datos de los archivos de intercambio y otros datos de entorno. El programa Filter I utiliza un tipo de inteligencia artificial (IA) para localizar fragmentos de diversos tipos de archivos, incluidos mensajes de correo electrónico, conversaciones de chateo, e incluso contraseñas de red y números de tarjetas de crédito y seguridad social. El proveedor del programa Net Threat Analyzer lo brinda gratuitamente a los organismos encargados de hacer cumplir la ley, y es utilizado para evaluar las búsquedas en Internet, la actividad de descarga y las comunicaciones por correo electrónico en datos de entorno en busca de evidencias en relación con actividades de terrorismo y otras de carácter ilícito. Estos dos paquetes de software son comercializados por NTI. La empresa también produce programas de búsqueda en texto y en disco capaces de explorar dispositivos de almacenamiento a nivel físico y ubicar los datos almacenados entre particiones asignadas o cadenas de texto localizados en espacios no asignados.

Recuperación de datos a partir de copias de seguridad

La copia de seguridad es una fuente para recuperar datos que a menudo es pasada por alto y puede ser especialmente útil en casos en los que el delincuente informático haya tenido la sagacidad de destruir totalmente los datos (por ejemplo, utilizando métodos analizados en la próxima sección "Para burlar las técnicas de recuperación de datos"). La copia de seguridad pudo haber sido hecha por el sospechoso o (si la computadora el sospechoso está en una red) por el administrador de sistemas como previsión ante cualquier falla. En muchos casos en los que los sospechosos han destruido los archivos incriminatorios, copias de estos archivos están en la copia de seguridad. Ello sucede especialmente en las empresas, en las que los administradores de sistema por lo general realizan diaria y automáticamente copias de seguridad de los datos de usuario a un servidor.

Incluso cuando el sospechoso utiliza una computadora personal en su hogar, vale la pena buscar en ella una copia de seguridad. Muchas personas acostumbradas a trabajar con computadoras, habiendo padecido una falla de sistema que les ha hecho perder datos valiosos, generalmente realizan copias de seguridad de sus archivos importantes. Los que se dedican a la pornografía infantil a menudo se sienten emocionalmente vinculados a sus colecciones y quizás realicen copias de seguridad de ellas para evitar perderlas en caso de

una falla del sistema. Si existe una unidad de cinta acoplada al sistema, es muy probable que se utilice para hacer copias de seguridad. Si la computadora tiene instalado un grabador de disco compacto o DVD, es posible que el sospechoso lo haya utilizado para copiar sus archivos. Debemos solicitar que la orden de registro especifique la requisa de cintas, discos, CD-ROMs u otros medios utilizados comúnmente para copiar archivos, además de la computadora propiamente dicha. Las copias de seguridad han salvado la situación en muchos casos en que no se ha podido encontrar evidencia alguna en los discos duros de las computadoras.

Para burlar las técnicas de recuperación de datos

Llegado este punto, quizás algunos oficiales encargados de hacer cumplir la ley estén preocupados por la seguridad de sus propios datos sensibles, y por saber si estas mismas técnicas de recuperación constituyen una amenaza de seguridad para ellos, y si es posible protegerse contra estas amenazas, además de cómo hacerlo. La mala noticia es que todos estos datos que se mantienen en lugares insospechados de hecho pueden representar un riesgo para el organismo oficial, en el caso de que la persona equivocada llegue a tener control sobre las computadoras oficiales. La buena noticia –en términos de la protección de los datos sensibles del organismo encargado de hacer cumplir la ley– es que existen formas para burlar los métodos de recuperación de datos. Por otra parte, los sospechosos pueden utilizar las mismas técnicas para encubrir sus huellas y destruir las evidencias de sus delitos. De manera que, por ambas razones, es preciso que los investigadores conozcan las formas en que se pueden eliminar los datos de un disco "de una vez y para siempre".

NOTA

Si es preciso utilizar nuevamente los discos que han sido utilizados como destino de copias del flujo de bits de discos sospechosos en exámenes forenses, es preciso borrarlos totalmente entre un uso y otro para impedir que restos de datos de casos anteriores queden en ellos y aparezcan como evidencias en el nuevo caso.

Algunas de estas técnicas de recuperación de datos requieren que accedamos físicamente al sistema, mientras que otras pueden iniciarse en la red. Además de los métodos de seguridad que analizamos en los capítulos 7 y 8, ¿qué podemos hacer para garantizar que los datos confidenciales no permanezcan en un disco después de haberlos utilizado? Por lo general, existen tres formas de hacerlo: sobrescribir, desmagnetizar y destruir físicamente el disco.

Sobrescribir el disco

El término *datos remanentes* se refiere a los residuos físicos de datos que supuestamente han sido eliminados o borrados. Muchas utilidades de "limpiar" discos que se comercializan actualmente y que están disponibles en Internet como software gratis y libre afirman ser capaces de eliminar estos remanentes, a partir de los cuales es posible reconstruir los datos. Estas utilidades funcionan escribiendo sobre el espacio no asignado en el disco. Windows XP Profesional incluye una utilidad en la línea de comandos llamada CIPHER.EXE que, además de encriptar, desencriptar y gestionar archivos encriptados utilizando EFS, tiene un switch que sobrescribe los datos en los clústeres no asignados. Estas utilidades intentan rellenar el espacio no asignado con valores binarios aleatorios y pueden realizar la función de sobrescritura varias veces (lo cual es necesario

para sobrescribir los datos fantasmas).

NOTA

Los mejores programas de limpieza de discos para los sistemas de archivo FAT y NTFS son los basados en DOS (programas de línea de comandos); los programas con base en Windows por lo general no pueden eliminar los datos de entorno en zonas oscuras del espacio de almacenamiento**.**

La prueba realizada a muchas de estas utilidades muestra que a menudo no afectan los datos en los flujos de datos alternos y pueden dejar remanentes de datos fantasmas. Para que sea efectiva, la sobrescritura debe realizarse varias veces, utilizando patrones diferentes, e incluso así podrían quedar algunos tipos de datos sin borrar. Si realmente deseamos eliminar los remanentes de datos mediante un método de sobrescritura, debemos utilizar un programa que cumpla o sobrecumpla las normas de seguridad del Departamento de Defensa de los Estados Unidos. Según estas normas, el proceso de sobrescritura debe realizarse al menos en tres pases: un pase sobrescribe los datos con un carácter, o segundo paso sobrescribe el anterior con el complemento de la primera sobrescritura de carácter, y un tercero utiliza un carácter aleatorio**.** Este proceso debe también verificarse.

Un ejemplo de programa para limpiar discos que cumple las normas del Departamento de Defensa es DiskScrub de NTI. Otro producto de NTI, M-Sweep Pro Data Eliminator, fue diseñado específicamente para utilizarse en sistemas notebook pero puede también ser usado en discos duros de computadora de mesa y en discos extraíbles; el mismo sobrescribe las zonas de almacenamiento de los datos de entorno. La venta de estos productos está limitada a los organismos de aplicación de la ley, instalaciones médicas y hospitales, instituciones financieras, firmas legales y de contabilidad, organismos gubernamentales de los Estados Unidos y empresas de Fortune 1000.

Desmagnetización

Otra forma de eliminar los datos remanentes de un disco es crear un campo magnético muy fuerte capaz de reducir a cero el estado magnético del medio. Este proceso es denominado *desmagnetización*, y el dispositivo que crea el campo magnético es el *desmagnetizador*. La desmagnetización se realiza ya sea aplicando un campo magnético alternativo mediante una fuente de corriente alterna o aplicando un campo unidireccional usando una fuente de corriente directa. También se pueden utilizar imanes permanentes de mano para desmagnetizar algunos tipos de medios magnéticos (disquetes y discos duros; usualmente no son utilizados para desmagnetizar cintas magnéticas). Existen diferentes tipos de cintas magnéticas, en dependencia de su grado de coercividad. Es importante tener el tipo de desmagnetizador adecuado para cada tipo de cinta, a fin de limpiarla totalmente de datos.

NOTA

Cuando los medios magnéticos están expuestos a temperaturas extremas o se almacenan durante largos períodos de tiempo, se vuelven más resistentes a la desmagnetización.

Destrucción física del disco

En los casos en que sea extremadamente importante eliminar toda posibilidad de que los

datos remanentes en un disco puedan ser reconstruidos en algún momento –por ejemplo, en el caso de una situación relacionada con la seguridad nacional en la que datos clasificados fueron almacenados en el disco– quizás sea preferible destruir físicamente el mismo. Ello puede hacerse de diferentes formas. Entre las maneras más eficaces están:

- pulverización (aplastar o triturar totalmente el disco hasta hacerlo polvo)
- incineración (quemar el disco hasta volverlo cenizas)
- abrasión (utilizar una rueda de esmeril para destruir totalmente la superficie del disco)
- ácido (aplicar una solución concentrada de ácido hidriódico a la superficie del disco)

Documentación de la evidencia

Según las *Normas y principios de la evidencia digital (Digital Evidence Standards and Principles)*, desarrollados por SWGDE e IOCE en 1999 y publicados en abril de 2000 en la edición de *Forensic Science and Communications* (publicación del FBI), "las notas y las observaciones de un caso deben estar escritas en tinta, no a lápiz, aunque el lápiz (incluido el lápiz de color) podría ser adecuado para hacer diagramas o trazos. Todas las correcciones a las notas deben estar inicialadas, y tachadas con una línea simple; ninguna información escrita a mano debe ser eliminada o borrada. Las notas y registros deben ser autentificados por firmas escritas a mano, iniciales, firmas digitales u otro sistema de marcación".

En las secciones siguientes analizamos el procedimiento para documentar la evidencia en una investigación de delito informático. Primero analizamos cómo se deben etiquetar o marcar las piezas que conforman la evidencia, así como la manera de mantener un registro de ésta. Posteriormente hablamos sobre cómo el análisis de la evidencia se debe documentar por la persona o las personas que realizas el examen forense. Finalmente, analizamos la cadena de custodia y la importancia de la documentación para preservar la integridad de dicha cadena.

Etiquetado y marcación de la evidencia

La evidencia es etiquetada y/marcada por la persona que la haya tenido primero bajo su custodia. Esa persona escribe sus iniciales o su nombre en la pieza, conjuntamente con la fecha y la hora y el número del caso. Es preferible marcar físicamente la evidencia siempre que sea posible, ya que las etiquetas pueden caerse, con lo cual se afecta la cadena de custodia. Las piezas que puedan ser marcadas físicamente se pueden colocar en una bolsa o contenedor, el cual se debe sellar y marcar. La marca se debe realizar con una tinta o marcador indeleble.

NOTA

En algunos casos, se puede utilizar una firma criptográfica (digital), si fuera posible hacerlo sin dañar la evidencia.

Registros de evidencia

El *registro de evidencia* es un documento que relaciona toda la evidencia recopilada en un caso criminal, con una descripción de cada pieza probatoria, quién la descubrió y la tomó, la fecha y hora en que lo hizo, y lo que se ha hecho con ella. La descripción debe ser suficientemente detallada para diferenciar una pieza de otras, y debe incluir números

de serie y otros números de identificación cuando sea posible. El registro muestra todos los traspasos de custodia de la evidencia de una persona a otra. Este proceso de registrar el traspaso de la evidencia es una prueba tangible de la conservación de la cadena de custodia.

Documentación del análisis de la evidencia

Otro tipo de registro debe ser realizado por la persona o las personas que realizan el examen del flujo de bits de los discos de la computadora del sospechoso. Este registro debe incluir todos los paso del proceso de análisis, entre ellos quién estuvo presente, qué se hizo (por ejemplo, ejecutar un software para eliminar los datos binarios de un archivo de intercambio), el resultado del procedimiento, y la fecha y hora.

Mientras se analiza el disco para determinar su valor probatorio, debemos documentar toda la evidencia posible que se encuentre. Por ejemplo, si abrimos un archivo con extensión .jpg que parezca ser una foto pornográfica de un niño, debemos anotar el número de archivo, el lugar en que está ubicado en el disco, las marcas de fecha y hora, así como todas las propiedades del archivo. Además de los datos volátiles y las zonas oscuras del disco donde se esconden datos y que ya hemos analizado anteriormente (espacio no utilizado, espacio no asignado, brecha de partición, etc.), algunos de los datos que deben examinarse en busca de evidencias, en dependencia del tipo de delito informático de que se trate, son los siguientes:

- listado de URL recientemente visitados (los cuales se obtienen de los archivos temporales de Internet o la caché web y el Historial)
- mensajes de correo electrónico y lista de direcciones de correo electrónico que aparecen en la libreta direcciones del sospechoso; el nombre de archivo depende del programa de correo electrónico que se utilice –por ejemplo, en el caso de Outlook es .pst (en algunos casos, esta información se almacena en un servidor de correo electrónico, como un servidor Exchange)
- documentos de procesamiento de texto; la extensión del archivo dependerá del programa que se utilice para crearlos; las extensiones más comunes son .doc, .wpd, .wps, .rtf, y .txt.
- Documentos de hojas de cálculo; la extensión del archivo dependerá del programa que se utilice para crearlos; las extensiones pueden ser, por ejemplo, .xls, .wgl, y .wk1.
- Gráficos, cuando se trate de caso de pornografía infantil; la extensión de los archivo puede ser .jpg, .gif, .bmp, .tif, entre otras.
- Registros de sesiones de chateo; el nombre de archivo depende del programa de chateo.
- El Registro de Windows (cuando sea el caso)
- Registros del Visor de sucesos
- Registros de aplicaciones
- Registros de colas de impresión

Documentación de la cadena de custodia

El término *cadena de custodia* se refiere a la continuidad de la evidencia. Es decir, debemos ser capaces de determinar la ruta que ha seguido la evidencia desde el momento en que es tomada hasta que es presentada en un tribunal, cada persona por cuyas manos

ha pasado, y cuándo y dónde fue transferida de una persona a otra. La documentación de la cadena de custodia es uno de los objetivos más importantes del registro de la evidencia.

Cualquier violación de la cadena de custodia da pie a la fiscalía para alegar que la evidencia ha sido violentada o que ha sido sustituida por otra. La prueba de la cadena de custodia se obtiene por el testimonio de las personas que recopilan la evidencia, estableciendo que lo que se presenta en el tribunal es de hecho la misma evidencia que fue recopilada (o es una representación exacta de esa evidencia), que la evidencia no fue violentada mientras estuvo bajo su custodia, y el momento y la forma en que su guarda fue transferida a la siguiente persona en la cadena de custodia. Este mismo proceso se puede seguir con cada persona que ha tenido a su cargo la guarda de la evidencia.

Evidentemente, mientras menos sean las personas que manejan la evidencia, más fácil será mantener la integridad de la cadena. Una práctica adecuada es designar a una persona como guarda de la evidencia. No obstante, en ocasiones es preciso entregar la evidencia hasta un laboratorio o un servicio forense/de recuperación de datos. Si el custodio designado no puede permanecer junto a la evidencia (y mantener contacto visual con ella) mientras es procesada, el laboratorio o el técnico deberán entregar un recibo como constancia de que la evidencia ha sido entregada, y ésta deberá ser examinada por el custodio una vez sea devuelta, a fin de garantizar que sea la misma evidencia. También será necesario que los técnicos de laboratorio testifiquen en relación con lo que sucedió con la evidencia mientras estuvo su cargo, así como sobre la forma en que fue almacenada y protegida en el laboratorio.

Recursos de computación forense

La computación forense es una esfera de actividad relativamente joven. Sin embargo, sus normas están evolucionando rápidamente y existen ya numerosos recursos para los que aspiran a convertirse en expertos en computación forense. Los investigadores de delito informático que desean ampliar sus conocimientos, el personal de empresas de TI interesado en especializarse en este esfera, y técnicos de criminalística que desean aprender a manejar la evidencia digital podrán encontrar numerosos programas de capacitación, equipos y software. Los investigadores que prefieren delegar los aspectos técnicos del examen de la evidencia digital podrán encontrar muchos servicios comerciales que realizan el trabajo de creación de imágenes, recuperación de datos y otras actividades afines. Muchos de estos servicios emplean personas calificadas para servir de testigos como expertos ante un tribunal. Varias asociaciones y organizaciones brindan documentos oficiales, artículos y otras fuentes de información que permiten mantener al personal de computación forense actualizado sobre los últimos acontecimientos en este esfera. En las siguientes secciones ofrecemos una breve información sobre algunos de estos recursos.

Capacitación y certificación en computación forense

Existen programas de capacitación que brindan compañías privadas productoras de software y equipos forenses, como NTI (www.forensics-intl.com/training.html) y DIBS (www.dibusa.com/training/training.html), en colegios y universidades, mediante algunas academias del personal encargado de hacer cumplir la ley, así como organizaciones y asociaciones relacionadas con el delito informático y la computación forense.

En esta esfera existen al menos dos programas de certificación reconocidos.

- IACIS ofrece una certificación como Examinador certificado en computación forense para personas individuales, pertenecientes o no a los

organismos encargados de hacer cumplir la ley, que presenten una solicitud donde demuestren poseer amplios conocimientos, entrenamiento y/o experiencia en la esfera de computación forense, así como una comprensión de los procedimientos, normas, ética y aspectos jurídicos y de privacidad referidos al tema. Los candidatos deben tener conocimientos y habilidades técnicas, además del equipo necesario para realizar el examen forense para poder obtener la certificación, los candidatos son sometidos a un proceso de prueba riguroso en el que deben realizar ejercicios de solución de problemas prácticos, preparar informes y presentar la evidencia obtenida, y aprobar posteriormente un examen escrito. Para más información sobre esta certificación, véase www.cops.org/External%20Certification.htm.

- La High Tech Crime Network (HTCN) ofrece certificaciones básica y avanzada como Técnico certificado en computación forense e Investigador certificado en computación forense. Para obtener estas certificaciones, los aspirantes deben demostrar que poseen un nivel mínimo de educación y experiencia combinadas (en la esfera de aplicación de la ley o en la esfera empresarial) y presentar la documentación referida a al menos 10 casos. Para más información véase www.htcn.org/certification.htm.

Un buen curso de capacitación en computación forense debe incluir teoría, proceso y metodología, además de prácticas en técnicas y herramientas.

Equipos y software de computación forense

Hay equipos especiales para el examen forense que son comercializados por varias compañías, como DIBS (www.dibusa.com). Los siguientes tipos de equipos pueden ser útiles para los investigadores y los técnicos forenses:

- **Equipo de creación de imagen** Estos dispositivos nos permiten realizar rápidamente copias del flujo de bits de los discos duros en otro disco duro, un cartucho óptico o una cinta. Existen unidades portátiles que pueden ser transportadas fácilmente hasta el lugar del delito para realizar la copia de disco en el lugar antes de apagar la computadora. Los medios de destino incluyen características de protección contra escritura a fin de garantizar que los datos no sean violentados después de realizar la copias.
- **Estaciones de trabajo forense** Estas son estaciones de trabajo de computación completas creadas para reconstruir y analizar fácilmente las unidades copiadas, usualmente con unidades extraíbles que permitan el arranque de las "copias de trabajo" de los discos sospechosos. Se ha instalado un software de análisis para ayudar en la búsqueda de tipos particulares de datos utilizando técnicas de Inteligencia Artificial o lógica borrosa para realizar búsquedas cuando el investigador no está seguro de cuál cadena de texto o tipos de archivo está buscando. Se ha instalado un software de recuperación de datos para localizar datos de archivos "eliminados" o "borrados". También existen estaciones de trabajo móviles en computadoras portátiles. Entre los ejemplos están las estaciones de trabajo forense de DIBS y F.R.E.D. (Forensic Recovery of Evidence Device, o Dispositivo Forense de Recuperación de Evidencia),

producido por Digital Intelligence (www.digitalintel.com/fred.htm).

- **Software forense** Los paquetes que ofrecen empresas como NTI y DIBS incluyen software de toma de imágenes, programas para deshacer la acción de eliminación ("un delete"), programas para la búsqueda global de cadenas de texto y archivos, programas que pueden verificar la exactitud de las copias del flujo de bits, programas que pueden eliminar caracteres binarios de los datos para facilitar el análisis de estos, programas que pueden documentar rápidamente listas de archivos y directorios, programas que pueden capturar los datos en los espacios no asignados, programas que pueden reconstruir la caché, herramientas de descompresión, utilidades de verificación del sistema, software de detección de esteganografía, programas para la recuperación de contraseñas, y muchos otros. Para obtener una lista de algunos de los mejores programas de software de computación forense, véase el sitio web de Timberline Technologies en www.timberlinetechnologies.com/products/forensics.html. NTI brinda varias herramientas forenses gratis en www.forensics-intl.com/donwload.html.

En la escena...
Para conformar una estación de trabajo forense
Podemos conformar nuestra propia estación de trabajo forense utilizando una computadora portátil o de mesa, en vez de comprar una combinación de hardware y software. El sistema debe ser suficientemente poderoso para ejecutar los software de aplicación forense; recomendamos un procesador de al menos 800 MHz y un mínimo de 512 MB de RAM. La estación de trabajo debe trabajar con un sistema operativo compatible con el software forense utilizado.

Quizás le resulte útil establecer una configuración de doble arranque para poder utilizar ya sea Windows o Linux, o puede ejecutar las máquinas virtuales (MV) VMWare (www.vmware.com) para visualizar un disco formateado con NTFS, por ejemplo, desde el sistema operativo Linux utilizando una MV Windows 2000.

Otra utilidad muy a propósito para la estación de trabajo es NTFSDOS, que nos permite visualizar los archivos en un disco formateado con NTFS desde MS-DOS o Windows 9*x*. Otra ventaja es que es de sólo lectura, por lo que no hay que preocuparse por sobrescribirlo accidentalmente y cambiar así los archivos originales. NTFSDOS se puede descargar desde www.sysinternals.com.

Servicios de computación forense
Un gran número de empresas ofrecen servicios de recuperación de datos y otros de computación forense. Muchos de estos servicios son sobre una base consultiva y nos permiten contar con expertos que actúen como testigos ante un tribunal. Los servicios se pueden cobrar por hora o por trabajo, y algunos ofrecen descuentos o incluso servicios gratuitos a organismos de aplicación de la ley. Algunas empresas que brindan servicios completos también pudieran alquilar equipos forenses a los investigadores que deseen realizar el trabajo forense personalmente, además de brindar entrenamiento en

computación forense.

En la mayoría de las ciudades de tamaño entre mediano y grande en Estados Unidos tienen una o más firmas locales especializadas en computación forense o que brindan estos servicios, además de otros. Si buscamos en la web el término *computación forense: servicios* (computer forensic: service) en el motor de búsqueda Google encontraremos numerosos resultados. Desde operaciones a cargo de una sola persona hasta las grandes empresas de renombre como Ernst & Young, se espera que esta esfera crezca aún más en los próximos años en la medida en que se incrementa la conciencia sobre el delito informático. Ello es particularmente así después de los ataques terroristas del 11 de septiembre de 2001 y las informaciones posteriores de que la red terrorista utiliza Internet y pudiera estar planeando ataques futuros en infraestructuras vitales de las TI.

Recomendamos que cuando tenga pensado contratar a un experto o un servicio de computación forense, indague acerca de su capacitación y certificación, pertenencia a una asociación profesional, así como su experiencia anterior, y pida referencias de clientes anteriores. Los organismos de aplicación de la ley también deben tener en cuenta que en muchos casos otros organismos de igual índole brindan servicios forenses, ya sea como una cortesía o mediando un pago, a organismos más pequeños que no tienen el equipo o el personal para hacer ellos mismos las labores de computación forense. Verifiquen con los organismos municipales y del condado de su zona, la policía estatal o el departamento de seguridad pública y, en casos importantes, el FBI y otros organismos federales para solicitar su asistencia.

Información de computación forense

La computación forense es un esfera que no solamente crece de manera acelerada sino que también evoluciona rápidamente. Todos los días se crean nuevas técnicas y tecnologías y es importante que los investigadores se mantengan el día en los últimos acontecimientos de este campo. Hay varias maneras para hacerlo, entre ellas:

- Leer publicaciones periódicas sobre computación forense y la especialidad forense en general, tanto impresas como las disponibles en revistas web, como *Computer Forensics Online* (www.shk-dplc.com/cfo) y *Computer Forensics Magazine* (www.forensic-computing.com).
- Asistir a seminarios y conferencias sobre delito informático y ciberdelito, como Incident Response and Computer Forensics, de Foundstone, la Conferencia Techno-Security patrocinada por Guidance Software (información sobre el evento del 2003 puede encontrarse en www.thetraining.com/html/Techno2003.html), Cybercrime 2003 (www.cybercrime2002.com/2003.html), y muchos otros.
- Afiliarse a asociaciones de computación forense y profesionales de investigación del delito informático, como IACIS (www.iacis.com), la High Technology Crime Investigators Association (http://htcia.org), el High Tech Crime Consortium (www.hightechcrimecops.org), y otros.

Para comprender los temas jurídicos

La computación forense tiene que ver tanto con el cumplimiento de la ley y la aplicación de los procedimientos prescritos para la recopilación de evidencia como con los aspectos técnicos de la recopilación de la evidencia digital. La evidencia que es inadmisible en un

tribunal es más que inútil; el registro e incautación ilícitos pueden no sólo dañar o destruir el caso de un fiscal y tener como resultado la liberación de un delincuente informático, sino que también pueden conducir a acciones administrativas e incluso penales contra los oficiales que violan las reglas.

Por lo tanto, es imprescindible que los oficiales encargados de hacer cumplir la ley y otros que participan en la recopilación y preservación de la evidencia comprendan las cuestiones jurídicas en el marco de las cuales operan. Las leyes varían entre una jurisdicción y otra y se modifican regularmente, de manera que todos los investigadores de delito informático deben tener como práctica mantenerse actualizados sobre la aprobación de estatutos y decisiones judiciales que rijan en su jurisdicción.

Este capítulo no pretende brindar asesoría jurídica. Las secciones siguientes tienen como único propósito brindar una visión general de algunas leyes y casos judiciales que se refieren a la búsqueda e incautación de computadoras y evidencia digital en los Estados Unidos al momento de escribir el presente. Estos temas son objeto de constante debate; regularmente se aprueban nuevas leyes y los tribunales emiten nuevos dictámenes. Por ejemplo, la Ley Patriótica de EE.UU., aprobada a raíz de los ataques terroristas del 11 de septiembre de 2001, dio mayor libertad al gobierno federal para monitorear las comunicaciones electrónicas y facilitó la obtención de una orden judicial para decomisar evidencia digital.

Búsqueda e incautación de evidencia digital

El término *búsqueda* (también *registro*) fue definido legalmente por los tribunales en el caso *El Estado contra Woodwall* como "el examen de la casa de un hombre u otra edificación o local, o de su persona, o de su vehículo, avión, etc., con miras a descubrir propiedad de contrabando, ilícita o robada, o alguna evidencia de culpabilidad para ser utilizada en el procesamiento de una acción penal por algún delito del cual se le acuse" (según el diccionario *Black's Law Dictionary*). El término *incautación* fue definido en el caso *Molina contra el Estado* como "el acto de tomar posesión de una propiedad, por ejemplo, por haberse violado la ley o en virtud de la ejecución" [de una orden judicial].

Las ideas tradicionales sobre registro e incautación no tomaban en cuenta las formas en que las computadoras se utilizan hoy día como depositarias de información (y de posibles evidencias). Los tribunales han tenido que hacer interpretaciones de la ley a fin de dar cabida a los aspectos singulares de estos "lugares" digitales y los tipos de evidencia que podemos encontrar en ellos. Por ejemplo, por lo general las leyes restringen la entrada al inmueble de una persona para realizar un registro sin orden judicial, excepto en determinadas circunstancias específicas. Por lo general los tribunales han sostenido que una persona puede esperar razonablemente el respeto a su privacidad cuando coloca información en una computadora, de la misma forma que si fuera un recipiente cerrado.

Por otra parte, cuando la evidencia está a la vista de todos en un lugar público, la ley permite que los oficiales la incauten. Tratar de aplicar estas mismas leyes a nuestra actualidad de interconexión suscita preguntas interesantes. ¿Los datos que contiene la computadora personal de un individuo que está conectada a la Internet pública y que es accesible al público se consideran alojados en un lugar privado o en un lugar público? Las respuestas están aún en el proceso de evolución a medida que los tribunales tienen que hacer frente a casos referidos a estos temas.

En los Estados Unidos las actividades de registro e incautación están regidas por

principios generales basados en las leyes federales y en la Constitución de la nación. No obstante, estamos conscientes de que los estados podrían imponer restricciones adicionales a las facultades de la policía en su jurisdicción, de manera que debemos comenzar también por conocer las directrices federales. En las secciones siguientes analizamos estos principios generales, teniendo en cuentas esas salvedades.

Cuestiones relacionadas con la Constitución de Estados Unidos

La Declaración de Derechos de la Constitución de Estados Unidos contiene 10 enmiendas destinadas a proteger a los ciudadanos de la opresión gubernamental y a garantizar determinados derechos humanos al pueblo. Una de las principales enmiendas en cuanto a sus implicaciones para la aplicación de la ley es la cuarta, cuya violación es en muchas ocasiones motivo para que se eliminen evidencias en procesos penales.

Para comprender la Cuarta Enmienda

La Cuarta Enmienda a la Constitución de los Estados Unidos prohíbe los registros e incautaciones arbitrarios. Señala textualmente: "El derecho de los habitantes a la seguridad en sus personas, domicilios, papeles y efectos, contra incautaciones y cateos arbitrarios, será inviolable, y no se expedirán al efecto las Órdenes correspondientes si no existe una causa probable, corroborada mediante Juramento o Declaración Solemne y que describan con particularidad el lugar que deba ser registrado y las personas o cosas que serán objeto de detención o embargo".

Quizás unas de las principales cuestiones que se deben entender de la Cuarta Enmienda es que sus restricciones se aplican solamente a agentes gubernamentales, como la policía y otros empleados o funcionarios públicos. Un privado no puede violar los derechos de un sospechoso a tenor de la Cuarta Enmienda a menos que actúe por instrucciones de la policía o de otro organismo gubernamental. En otras palabras, si un casero registra la casa de un inquilino o un empleador registra la oficina de un empleado no incurre en una violación de la Cuarta Enmienda. No obstante, el registro podría ser una violación de la privacidad y motivo de procesamiento civil en algunos casos; por ejemplo, los tribunales han afirmado que por lo general los empleados no deben esperar tener privacidad en una oficina propiedad del empleador.

¿Cómo se aplica esta interpretación al registro e incautación de computadoras? En este caso también la Cuarta Enmienda prohíbe solamente a los agentes del gobierno registrar el disco duro de una computadora. En el caso *Estados Unidos contra Hall,* caso que trataba de un técnico de reparación de computadoras que encontró pornografía infantil en la computadora de un cliente, el tribunal afirmó que "la Cuarta Enmienda no se aplica a los registros realizados por privados que no actúan como agentes gubernamentales", y en el caso *Estados Unidos contra Jacobsen*, el tribunal afirmó que "la Cuarta Enmienda es totalmente inaplicable al registro e incautación, incluso el de carácter arbitrario, realizado por un privado que no actúa como agente del gobierno o sin la participación o conocimiento de un funcionario gubernamental".

De manera que si un privado registra una computadora y encuentra evidencia de un delito, contacta posteriormente a las autoridades encargadas de la aplicación de la ley y estas obtienen una orden de registro sobre la base de la información que recibieron del privado, ello no constituye una violación de los derechos constitucionales del propietario de la computadora.

De hecho, la Corte Suprema ha afirmado (*Estados Unidos contra Jacobsen*) que los agentes encargados de la aplicación de la ley pueden volver a realizar el registro

privado original sin una orden judicial y ello no constituye una violación de la expectativa razonable de privacidad. No obstante, si los oficiales van más allá del alcance del registro original, la evidencia puede ser suprimida como lo fue en el caso *Los Estados Unidos contra Barth*, en el que un técnico de reparación de computadoras encontró pornografía infantil en la computadora del cliente y los agentes miraron otros archivos que el técnico no había revisado en su registro inicial. La evidencia observada inicialmente por el técnico debió haber sido utilizada para obtener una orden judicial de registro y poder visionar otros archivos.

NOTA

El hecho de si el registro o incautación es o no permisible en virtud de la Cuarta Enmienda es solamente un aspecto de su legalidad. Las leyes sobre privacidad y otros estatutos podrían aplicarse en casos particulares.

Jurisprudencia que rige el registro e incautación

Podemos revisar muchos casos judiciales en busca de guía en relación con el registro e incautación en general y el registro e incautación referido al equipo de computación y la evidencia electrónica en particular. En el caso *Katz contra los Estados Unidos* se afirmó que un registro se considera constitucional si no viola la expectativa razonable y legítima de una persona a la privacidad. Las circunstancias en las cuales una persona tiene o no expectativa razonable de privacidad están abiertas al debate y por lo general deben ser decididas por los tribunales en cada caso, si bien existe una jurisprudencia que establece las siguientes premisas:

- En *Payton contra Nueva York*, la Corte Suprema afirmó que existe expectativa razonable de privacidad cuando una persona está en su hogar.
- En el caso *Los Estados Unidos contra Ross*, la Corte Suprema afirmó que existe expectativa razonable de privacidad respecto de los contenidos de contenedores opacos cerrados.

Ha habido casos judiciales que establecen que una persona tiene derecho a expectativa razonable de privacidad respecto de los datos almacenados en el disco duro de una computadora (*Los Estados Unidos contra Barth* y *Los Estados Unidos contra Blas*). Por otra parte, los tribunales han dictaminado que cuando la persona pone a disposición pública la información de una computadora, se pierde la expectativa razonable de privacidad. En el caso *Katz contra los Estados Unidos* se afirmó que "lo que una persona expone a sabiendas al público, incluso en su propia casa y oficina, no está sujeto a la protección de la Cuarta Enmienda". Publicar información en un sitio web abierto al público evidentemente eliminaría la expectativa. En general, la información en tránsito (como un mensaje enviado por Internet) se ha considerado que no constituye exposición pública o sacrificio de la expectativa de privacidad. No obstante, la expectativa podría perderse cuando el mensaje llega a su destinatario. También se ha afirmado que una persona renuncia a la expectativa de privacidad si entrega información a otra y no pudiera esperarse razonablemente que pueda controlar el uso que esa persona haga de dicha información. En otros casos se ha decidido que la "simple información" revelada a terceros no califica dentro de la expectativa razonable de control o privacidad.

Cuando no existe expectativa razonable de privacidad, como cuando se abandona

una propiedad o cuando la evidencia de un delito es mostrada en un lugar público a la vista de todos, los oficiales por lo general pueden realizar el registro y la incautación sin que medie una orden judicial. Cuando las circunstancias crean una expectativa razonable de privacidad se requiere de dicha orden judicial.

Requisitos de orden judicial de registro o cateo

Una *orden judicial de registro* es un documento firmado por un magistrado donde se concede a los oficiales encargados del cumplimiento de la ley autoridad para registrar un lugar específico en busca de objetos específicos descritos en la orden. La orden debe estar basada en otro documento llamado *declaración jurada*, el cual es firmado bajo juramento por una persona (un oficial de la policía o cualquier otra persona) donde se expresa la creencia de que se encontrarán determinadas cosas en el lugar objeto de registro y donde se brindan hechos que sustentan esa creencia. Dichos hechos deben constituir *causa probable* de que los objetos del registro se encontrarán en el lugar descrito. Solamente podrán buscarse los objetos específicamente nombrados en la orden. Una orden judicial puede autorizar que se registre y decomise el hardware de una computadora, su información digital, o ambas. Si en la orden judicial se utiliza un lenguaje demasiado amplio (como autorización para incautar "todos los registros" o "todas las computadoras") ello podría invalidar la orden; en la misma se deben especificar los delitos o el delito con el cual guarda relación la evidencia.

En la escena....

Lista de verificación de la declaración jurada

La declaración jurada para obtener una orden judicial de registro debe exponer la causa probable de que:

1. Se ha cometido un delito (especificado por nombre y número que le corresponde en el código penal).
2. En el lugar mencionado existe evidencia digital.
3. La evidencia digital está asociada al delito (decir cómo).
4. La evidencia digital está asociada a una persona/un sospechoso en particular (mencionar nombre o describir).

La declaración jurada debe ser suficientemente específica para satisfacer los requisitos jurídicos y a la vez ser lo más general posible a fin de no excluir ninguna evidencia que pueda encontrarse.

Se puede obtener una orden de judicial para realizar registros en busca de tipos de propiedad específicos o una persona en particular. Las leyes estaduales por lo general deciden exactamente los objetivos por los cuales se puede emitir la orden de registro. Por ejemplo, según el Código de procedimientos penales de Texas, sección 18.02, se puede emitir una orden judicial de registro en busca de lo siguiente:

- Propiedad adquirida ilícitamente (mediante robo, fraude, etc.)
- Propiedad que fue producida, diseñada o adaptada para ser utilizada en la comisión de un delito e implementos o instrumentos que fueron utilizados en la comisión de un delito (las herramientas del delito, como una computadora utilizada para lanzar un ataque en la red)
- Contrabando (propiedad cuya posesión es ilícita; ello incluiría la

pornografía infantil destinada al uso personal del sospechoso)
- Drogas ilícitas, armas prohibidas y equipos de juego ilícito
- Material obsceno para su distribución comercial (ello incluiría la pornografía infantil destinada a la distribución comercial, así como cualquier otro material considerado "obsceno" que esté destinado a la distribución con fines comerciales)
- Evidencia de un delito
- Una persona

Las órdenes judiciales y las declaraciones juradas que las sustentas deben seguir directrices estrictas en cuanto a su forma y contenido; de igual manera, la confiabilidad del que ha prestado declaración jurada (la persona que ha firmado la declaración jurada) debe quedar demostrada suficientemente ante el magistrado que emite la orden judicial. Desde el punto de vista del oficial, siempre es preferible tener una orden judicial que realizar un registro sin en ella, porque la orden judicial releva al oficial de la responsabilidad de demostrar que existía causa probable y/o excepciones aplicables a los requisitos de una orden judicial de registro.

NOTA

Por lo general se debe entregar una copia de la orden judicial de registro a la persona que está a cargo del lugar que se registra, o se debe dejar o colocar en un lugar visible si no está presente ninguna persona para recibirla. En algunos casos, los tribunales han autorizado las llamadas órdenes judiciales "sneak and peek" (que permiten irrumpir y revisar de manera furtiva) que no requieren que los oficiales entreguen una notificación de que se ha realizado un registro. Algunos cambios realizados a la ley federal después de los ataques terroristas del 11 de septiembre de 2001 introdujeron excepciones aún más amplias al requisito de notificación en el caso de los registros en busca de evidencia de actividades terroristas.

Otro asunto que guarda relación con esto es la orden judicial "no-knock". De manera general, los oficiales deben anunciar su presencia cuando presentan una orden judicial de registro e identificarse como oficiales encargados del cumplimiento de la ley. Sin embargo, los tribunales han afirmado que el anuncio no es un requisito si ello representaría un peligro para la vida de alguna persona o la destrucción de la evidencia. Debido a que la evidencia informática es factible de ser destruida rápida y fácilmente, a menudo se considera que los oficiales que tienen una orden de registro en busca de evidencia digital están justificados de obviar el anuncio.

Podrían surgir problemas especiales en la elaboración de órdenes judiciales de registro en busca de evidencia electrónica debido a la naturaleza intangible de la evidencia. Por ejemplo, un sospechoso podría trasladar o destruir los datos de la computadora con rapidez y facilidad sin abandonar el local. Una persona con experiencia técnica debe asesorar a los oficiales y al magistrado en relación con los aspectos técnicos de la búsqueda y recopilación de evidencia digital sobre la base de las circunstancias de cada caso. Es igualmente importante, si no lo es más, recopilar toda la información posible acerca del objeto de la orden judicial en un caso relacionado con la informática como lo es en aquellos que entrañan el registro de un lugar físico. Ello incluiría las

plataformas de hardware, el ambiente del sistema operativo, y las aplicaciones de software en curso, así como las conexiones y la configuración de red. Al dejar consignadas todas esas especificidades se puede contribuir a determinar el tipo de archivos que se deben buscar en el registro y su posible ubicación.

Registros sin orden judicial

En algunas circunstancias no se aplican las protecciones de la Cuarta Enmienda porque se considera que lo que se ha realizado no es un registro. Si la policía incauta un vehículo (por ejemplo, porque han arrestado a la persona que lo conducía), estaba autorizada a inventariar el contenido del vehículo como un procedimiento normal. Esto no constituye un registro porque no se realiza con el objetivo de buscar evidencia de un delito sino con el propósito de proteger la propiedad del propietario (y de proteger al organismo frente a cualquier reclamación de robo). No obstante, esta excepción no autoriza a la policía a abrir objetos cerrados (como maletines) como parte del proceso de inventario. Para hacerlo por lo general necesitarían una orden judicial (a menos que se apliquen otras excepciones, como circunstancias apremiantes. Una laptop u otro tipo de computadora que se encuentre en el vehículo en el momento del decomiso, por lo general sería tratada como un objetos cerrado en el sentido de que en la mayoría de los casos los agentes encargados del cumplimiento de la ley deben obtener una orden judicial para abrirla y ver los datos que contiene.

Existen varias otras excepciones al requisito de orden judicial de registro, según establecen los estatutos y casos judiciales. Entre ellos:

- Registros con consentimiento
- Propiedad abandonada
- Circunstancias apremiantes
- Vista pública
- Registro a consecuencia de un arresto

Registro con consentimiento

Si la parte que tiene el control sobre el local o el objeto que debe ser registrado da su consentimiento voluntario al registro, lo oficiales no necesitan una orden judicial. A esto se le llama *registro con consentimiento*. Lo oficiales ni siquiera precisan demostrar la causa probable de que se ha cometido un delito; pueden realizar el registro lícitamente con consentimiento, incluso si no hubiera razones para creer que ha ocurrido un delito penal. En este caso el elemento clave es que el consentimiento debe ser voluntario. Si el consentimiento se ha obtenido mediante coacción, amenaza o intimidación, no es voluntario y por lo tanto no es válido.

Además, la persona que brinda el consentimiento debe estar facultada para ello. Por ejemplo, los tribunales han decidido que un casero no puede dar el consentimiento para que los oficiales registren la casa de un inquilino. Por otra parte, los tribunales también han afirmado que los empleadores pueden dar el consentimiento para que se registren las oficinas de sus empleados, mientras que los directores de escuelas pueden dar el consentimiento para que se registren las taquillas de los estudiantes. Para determinar la legalidad de un registro, los tribunales tienen en cuenta la autoridad de la

persona que da el consentimiento y el alcance del mismo. Es decir, si una persona da el consentimiento para que se registre su casa ¿incluye eso el registro del contenido del disco duro de su computadora?

En la escena....
El dilema de la propiedad compartida
Por lo general, si una o más personas comparten la propiedad de una computadora (por ejemplo, dos persona que comparten una habitación) será preciso obtener el consentimiento de solamente uno de esos propietarios para poder realizar un registro lícito. En ese caso se considera que la computadora es una "área común", como las áreas comunes de un hogar. No obstante, una de las partes no tiene autoridad para dar el consentimiento para que se registren las "áreas privadas" de la otra parte, como sería el caso del dormitorio que es utilizado de manera exclusiva por dicha persona. De la misma manera, un compañero de cuarto no puede dar consentimiento lícito para que se registre la computadora que es propiedad individual del otro compañero de cuarto. Incluso en relación con una computadora de propiedad compartida, la utilización de la protección por contraseñas o la encriptación de archivos por parte de uno de los compañeros de cuarto puede dejar establecido que dichos archivos son parte de una gran "área privada" en la computadora, y si el otro compañero de cuarto no ha sido informado de la contraseña o la clave no tiene autoridad para consentir que se registren esos archivos.

Por lo general, un cónyuge puede dar consentimiento válido para que se registre la propiedad del otro cónyuge, y los padres pueden dar consentimiento para que se registre la propiedad de sus hijos menores de 18 años. En el caso de hijos adultos que viven con sus padres y pagan renta, la situación es muy parecida a la de los compañeros de cuarto, en el sentido de que los padres pueden dar consentimiento para que se registren las áreas comunes pero no las privadas en la que sus hijos han demostrado tener expectativa de privacidad (por ejemplo, al colocar cerrojos en las puertas o encriptando sus archivos).

En la mayoría de los casos, se ha determinado que los administradores de sistemas tienen autoridad para dar el consentimiento para que se revisen los archivos almacenados en una red, si los usuarios de la red no tienen expectativas razonables de privacidad respecto de esos archivos (como en el caso en que los archivos son creados durante la actividad correspondiente al empleo de la persona y son almacenados en la red del empleador). En otros casos –como cuando una persona compra espacio en disco para almacenar datos en un servidor remoto– este tema no es tan definido.

NOTA

Si bien el consentimiento verbal para un registro puede ser lícito, siempre es mejor que los oficiales encargados del cumplimiento de la ley obtengan un consentimiento por escrito y firmado. A tal fin los oficiales siempre deben llevar consigo formularios preimpresos de Consentimiento de registro.

Propiedad abandonada

Por lo general los oficiales a cargo del cumplimiento de la ley están autorizados a registrar una propiedad que ha sido claramente abandonada, sin que medie una orden judicial. Por ejemplo, si un sospechoso porta un disquete y, habiendo observado la presencia de la policía en la zona, arroja el disquete en un latón de basura público, los oficiales pueden tomarlo y ello constituiría un acto lícito.

Circunstancias apremiantes

Otra situación en la que se pueden realizar registros sin una orden judicial es en los casos de *circunstancias apremiantes* –es decir, una emergencia ante la cual no hay tiempo para obtener una orden judicial y es preciso proceder de inmediato al registro para salvar una vida o impedir daño físico a una persona, impedir que se escape un sospechoso, o que se destruya una evidencia. Esta última situación es más aplicable a la evidencia digital debido a su carácter frágil. Es muy fácil destruir la evidencia que está en forma de datos informáticos. En los casos *Los Estados Unidos contra David* y *Los Estados Unidos contra Romero-García*, los tribunales decidieron que la incautación de evidencia electrónica sin una orden judicial fue un acto lícito porque la evidencia estaba a punto de ser destruida.

Un principio importante relacionado con la excepción sobre la base de circunstancias apremiantes es que los oficiales a cargo del cumplimiento de la ley no pueden crearlas. En el caso *Los Estados Unidos contra Reyes*, el tribunal dictaminó en contra del gobierno cuando se argumentó que los mensajes de entrada o el fallo de la batería podían destruir la evidencia en un localizador (*pager*) ya que los oficiales habían creado la situación apremiante al encender el localizador.

Registros a simple vista

El concepto de *simple vista* (en ocasiones también denominado *doctrina de campos abiertos*) descansa en la premisa de que el oficial a cargo del cumplimiento de la ley está lícitamente en un lugar particular en el cual puede ver a simple vista la evidencia de un delito. Esta doctrina no se aplica usualmente a la evidencia electrónica ya que por lo general no es posible apreciar a simple vista el contenido de los archivos almacenados en una computadora (a menos que el oficial haya entrado de manera lícita en la habitación en la que el sospechoso tiene abierto el archivo y lo tenga visualizado en la pantalla).

Este tema ha salido a colación en los casos en que los oficiales tenían una orden judicial para registrar en busca de evidencia de un delito (por ejemplo, pornografía infantil) y durante el registro lícito encontraron evidencias de otro delito (por ejemplo, una foto que indique que el sospechoso ha cometido un asesinato). Los tribunales por lo general han decidido que la doctrina de simple vista se aplica, pero al encontrar la evidencia del segundo delito, lo oficiales debieron haber contactado al magistrado con esa evidencia para establecer la causa probable con miras a que se emitiera una orden judicial de registro para buscar evidencias adicionales del segundo delito.

Registro a consecuencia de un arresto

Los oficiales pueden realizar un registro de una persona y sus inmediaciones al momento de realizar un arresto, sin tener una orden judicial. Ello se ha interpretado en los tribunales en el sentido de que los oficiales pueden registrar la billetera o el monedero de una persona, o su libro de direcciones, entre otras pertenencias. Los tribunales han afirmado que la información contenida en un localizador puede ser registrada cuando se

arresta a la persona que porta el localizador. Existen varios casos que sustentan este dictamen, entre ellos *Los Estados Unidos contra Reyes*, *Los Estados Unidos contra Thomas*, y *Los Estados Unidos contra Lynch*. No está claro si este dictamen también se aplicaría a las PDAs y las computadoras de mano o laptops.

NOTA

Otra excepción al requisito de orden judicial de registro es la inspección en la frontera. Los registros rutinarios de personas que entran o abandonan el territorio de los Estados Unidos están permitidos sin causa probable o indicio de actividad delictiva. Ello se afirmó como pertinente en un caso en que se incautó el disco duro de una computadora y se accedió a la información que contenía como parte de "un registro rutinario de exportación" a un hombre que se marchaba del país (*Los Estados Unidos contra Roberts*).

Incautación de evidencia digital

Son muchas y diferentes las formas en que puede incautarse la evidencia digital una vez que es localizada. En un inicio, los investigadores de los delitos informáticos solían imprimir los archivos incriminatorios o realizar copias digitales (en discos flexibles u otros medios extraíbles) de los archivos en cuestión. Otra opción es incautar la computadora completa y revisar en otro lugar los datos que contiene. Como dijimos anteriormente, la práctica más aceptada actualmente es realizar primero una copia exacta y total del flujo de bits del disco duro antes de apagar la computadora. Estas copias se pueden utilizar para reconstruir el disco sospechoso y analizarlo en otro lugar posteriormente. Después de realizadas las copias, los investigadores deben incautar el equipo y el disco original, marcarlos como evidencia y almacenarlos en un lugar seguro. El proceso de registro e incautación se debe planificar adecuadamente de antemano. Debe determinarse la hora y el día más apropiados para realizarlo, a la vez que calcular la cantidad de oficiales y técnicos –así como su nivel de experiencia– que serán necesarios al momento de efectuar esta operación.

Leyes de confiscación

Las computadoras que se utilizan como herramientas para la comisión de delitos (por ejemplo, el tráfico ilícito de drogas) pueden estar sujetas a las leyes estaduales y federales de confiscación de bienes. Ello significa que la propiedad del equipo se transfiere al estado o al organismo encargado del cumplimiento de la ley que realiza la incautación y puede pasar a ser propiedad de éstos o ser vendida por ellos.

Leyes de privacidad

La Ley de protección de privacidad de los Estados Unidos (PPA) abarca el registro y la incautación de objetos que abarca la Primera Enmienda (libertad de expresión, libertad de prensa). La Ley de privacidad está dirigida a proteger a periodistas, editores y todas las demás personas que pudieran poseer evidencias de actividad delictiva pero que no son sospechosos de haber cometido ningún delito. Esta ley se aplica a los materiales que son creados con fines de diseminación de información al público (por ejemplo, escritos para ser publicados en sitios web, dado que ésta es una forma de publicación en un foro público).

Si existen razones para sospechar que una persona que posee esos materiales está cometiendo un delito para el cual estos pudieran utilizarse, o si existiera el peligro de que

alguna persona pudiera sufrir daño físico o morir y ello pudiera evitarse al incautar la evidencia, la realización del registro y la incautación no constituye una violación de la Ley de privacidad. Las violaciones de la ley constituyen un delito civil y no penal. Quienes violan la ley están sujetos a proceso civil, aunque la violación de ésta no significa que la evidencia será desestimada por un tribunal, como sucedería en caso de que se violaron los derechos constitucionales.

NOTA

Algunos estados tienen sus propios estatutos de privacidad los cuales pueden ser aplicables en casos específicos, además de la Ley federal de protección de privacidad. Asimismo, existen reglamentos especiales a tenor de las leyes tanto federales como estaduales que rigen la información que se considera confidencial o privilegiada por el estatuto, como en el marco de una relación médico-paciente, abogado-cliente, o clérigo-feligrés. Estos se consideran *documentos legalmente privilegiados*.

La Ley de privacidad de las comunicaciones electrónicas (ECPA) fue aprobada para proteger los derechos de privacidad de los clientes de los ISP cuando se revelan sus informaciones personales. Entre las sanciones imponibles por la violación de dicha ley están el pago por daños civiles y, en algunos casos, la instrucción de cargos penales. Las disposiciones de la ECPA aparecen en el Título 18 del Código de los Estados Unidos. No obstante, con la aprobación de la Ley Patriótica de los Estados Unidos se modificaron las disposiciones de la ECPA, las cuales analizamos en la sección siguiente.

Repercusiones de la Ley Patriótica de los Estados Unidos

La Ley Patriótica de los Estados Unidos entró en vigor en octubre de 2001, en respuesta a la continuada amenaza de terrorismo en los Estados Unidos. Con su aprobación se efectuaron varias modificaciones a la ley federal en relación con las computadoras y la información digital como evidencia. Por ejemplo:

- Anteriormente, a tenor de la Ley de fraude y uso ilícito de computadoras, los investigadores gubernamentales no estaban autorizados a interceptar las comunicaciones inalámbricas de voz con el fin de utilizarlas como evidencia en casos penales. La Ley Patriótica añade el Título 18 del Código de los Estados Unidos, Sección 1030 (Ley de fraude y uso ilícito de computadoras) como uno de los delitos por lo cuales se puede obtener una orden de escucha electrónica.
- Anteriormente, los investigadores estaban obligados a obtener una orden de escucha electrónica para poder confiscar y escuchar mensajes de voz no abiertos almacenados por el proveedor. La Ley Patriótica modifica la definición de *comunicación por cables* de manera que los mensajes almacenados no sean incluidos y los investigadores puedan obtener evidencias a partir de mensajes de voz en virtud de una orden judicial de registro en lugar de tener que recurrir a un proceso más difícil de obtención de una orden de escucha electrónica.
- Anteriormente, los investigadores no podían emplazar determinados registros, como los números de tarjeta de crédito de los clientes de un proveedor de servicios Internet. La Ley Patriótica añadió nuevos tipos de registros que podían ser emplazados, como número de tarjeta de crédito y

otra información de pagos, direcciones de red (IP) asignadas temporalmente, y registros de fecha, hora y duración de sesiones.

- Anteriormente no era posible emplazar ni obtener mediante orden judicial de registro las informaciones registradas por las compañías de cable. Debía enviarse una notificación al cliente si el gobierno deseaba examinar los registros, y el cliente debía tener la posibilidad de comparecer ante un tribunal en el marco de una audiencia con miras a determinar si el gobierno tenía razones justificadas para examinar dichos registros. La Ley Patriótica modificó esto de manera que estos requisitos se apliquen solamente a los registros de la programación de televisión por cable y no a los servicios de Internet que brindan dicha compañías.
- Anteriormente los proveedor de servicios de Internet no estaban autorizados a revelar la información sobre sus clientes en situaciones de emergencia (por ejemplo, cuando se sospechaba que el cliente estaba planificando un ataque terrorista), ni tampoco existía la disposición que permitiera al proveedor de servicios de Internet revelar voluntariamente información que no fuera de contenido (por ejemplo, registros de inicio de sesión) cuando sus redes eran atacadas. La Ley Patriótica permite a los ISP revelar información de contenido u otro tipo en situaciones de emergencia cuando exista un riesgo inmediato de muerte o de daño físico grave o para proteger sus propiedades y sus derechos. (Los ISP no están obligados en virtud de la ley a examinar los registros en busca de peligros potenciales, ni se les exige que revelen dichos registros en tales situaciones). La Ley también prevé la defensa frente a los pleitos civiles para los ISP y otros que brinden información sobre la base de la buena fe a solicitud de un agente gubernamental para preservar la evidencia. La Ley Patriótica amplió el ámbito de los dispositivos de monitoreo electrónico (trap and trace) y registros de identidad de manera que se apliquen a la información utilizada en el procesamiento y enrutamiento de comunicaciones electrónicas, como la información de encabezamiento de mensajes electrónicos, direcciones IP y números de puerto. (Las órdenes de monitoreo electrónico no se pueden utilizar para interceptar el contenido de los mensajes –solamente se pueden utilizar la información de enrutamiento, direccionamiento y señalización). Las facultades de los tribunales federales se ampliaron a fin de permitirles emitir órdenes de pen/trap en cualquier lugar del territorio de los Estados Unidos (lo cual anteriormente estaba limitado al distrito o jurisdicción particular del tribunal).
- Anteriormente la capacidad jurídica de los oficiales a cargo del cumplimiento de la ley estaba limitada a la prestación de asistencia a los dueños de computadoras y redes en la fiscalización de la actividad, con miras a protegerlos frente a los ataques de intrusos. La Ley Patriótica específicamente autoriza a las víctimas de los ataques en redes a permitir que los oficiales a cargo del cumplimiento de la ley monitoreen esos sistemas en el marco de una investigación (civil o penal).

- La Ley Patriótica amplía el ámbito de las órdenes judiciales de registro de manera que abarquen las comunicaciones por correo electrónico sobre una base nacional, de tal forma que dichas órdenes pueden aplicarse a los registros que no se encuentran en el distrito del tribunal que emite la orden.
- La Ley Patriótica aumenta las sanciones y modifica las directrices para la imposición de sanciones por los delitos que entrañan daño intencional a las computadoras protegidas (en virtud de la Sección 1030 del Título 18) y amplía el ámbito de la ley a fin de que se aplique a las computadoras ubicadas en otros países, en caso de que se vea afectado el comercio interno entre estados o el comercio internacional de los Estados Unidos. Igualmente la ley esclarece el estado mental de culpabilidad (*mens rea*) que se requiere para inculpar a un hacker a tenor de la Sección 1030; solamente es necesario demostrar la intención de causar daño, en lugar de la intención de causar un daño por un monto monetario específico. Están previstas sanciones mayores cuando el daño es ocasionado a computadoras que se utilizan con fines de seguridad nacional o justicia penal.

NOTA

Para obtener una explicación detallada sobre los cambios efectuados en virtud de la Ley Patriótica de los Estados Unidos en relación con el delito informático y la evidencia electrónica, según se define en el memorando de orientación de la Sección de delito informático y propiedad intelectual del Departamento de Justicia (CCIPS), véase www.usdoj.gov/criminal/cybercrime/PatrioticAct.htm.

Resumen
La evidencia es la base de todo caso penal, incluidos los referidos al delito informático. La recopilación y preservación de la evidencia digital es un proceso que difiere en muchos sentidos de los métodos que utilizan los oficiales encargados de la aplicación de la ley para tratar los tipos de evidencias tradicionales. La evidencia digital es intangible; es una representación en formato magnético o electrónico de la información. Su forma física no revela su naturaleza con facilidad. Además, la evidencia digital es frágil. Es muy fácil para un delincuente borrar deliberadamente evidencia vital en pocos segundos, o para un oficial o técnico dañar o destruir la evidencia sin proponérselo.

Desafortunadamente, en muchos casos, la evidencia que aparentemente ha desaparecido continúa estando en el disco o en el medio electrónico y puede ser recuperada. En el mercado existen varios paquetes de software de recuperación de datos, varios de los cuales están destinados específicamente para las labores de la computación forense y se comercializan teniendo como objetivo principal los profesionales de la aplicación de la ley. Asimismo, existen muchos servicios comerciales de recuperación de datos que realizan la operación de recuperación a cambio de un honorario, y lo hacen con la ayuda de equipos sofisticados que quizás no están al alcance de nuestros presupuestos ni de los fondos disponibles para los organismos encargados de aplicar la ley.

La computación forense es una esfera de trabajo relativamente nueva cuyas normas están siendo establecidas muy aceleradamente. A fin de garantizar que la evidencia digital sea admisible en un tribunal, es preferible seguir las actuales normas y prácticas aceptadas y utilizar los programa de software que ya han sido utilizados con anterioridad. El objetivo principal es examinar los datos que contiene la computadora de un sospechoso y mantener el original en las mismas condiciones en que fue encontrado. Para ello, siempre que sea posible, se debe utilizar una tecnología de imagen de disco a fin de crear un duplicado exacto del disco duro sospechoso, y este duplicado es el que se debe utilizar en el examen. Con el objetivo de recuperar la información que pudiera estar oculta en zonas oscuras del disco o que pudieran quedar luego de una operación de borrado o eliminación de datos, la copia que se obtenga debe ser una imagen del flujo de bits, con lo cual se copia cada bits, sector por sector, del disco original. De manera ideal, este duplicado se debía hacer en el mismo lugar donde se incautó la computadora, antes de apagarla. Al propio tiempo, se deben tomar medidas para registrar o preservar los datos volátiles que pudieran perderse cuando se apaga la computadora.

Una vez que hayamos hecho uno o más duplicados, el original debe ser guardado en un lugar seguro, que puede ser una habitación o un local de evidencias. Durante todo el proceso se debe mantener la cadena de custodia. El duplicado del disco se puede examinar en busca de evidencias de actividad delictiva. Este examen debe incluir no solamente los archivos que son visibles en el sistema de archivos sino también la búsqueda de datos de ambiente que no son evidentes y cuya existencia no es conocida por el usuario la computadora. Será preciso utilizar un software especial de computación forense, el cual puede ser instalado en una estación de trabajo aparecen.

La recopilación de evidencia no solamente entraña conocimientos técnicos; también requiere conocimientos sobre las leyes relacionadas con la evidencia. Violar esas leyes podría provocar que la evidencia fuera desestimada por un tribunal, independientemente de su calidad técnica y de su pertenencia para demostrar definitivamente la culpabilidad del acusado. En los Estados Unidos, a menudo la

admisibilidad de la evidencia guarda relación con la Cuarta Enmienda de la Constitución, la cual protege a los ciudadanos frente al registro e incautación no razonables. Si el proceso de registro e incautación de computadoras y/o datos digitales viola los derechos constitucionales del sospechoso, la evidencia puede ser rechazada por el juez y nunca llegará a ser analizada por el jurado. Otras leyes federales y estaduales rigen la admisibilidad de la evidencia en procesos penales. Estas leyes por lo general están recogidas en codificaciones denominadas *Reglamentos de evidencia*, y todos los investigadores deben conocer las que son aplicables dentro de su jurisdicción.

En el próximo capítulo, "Preparación de un caso de delito informático" aprenderemos cómo utilizar la evidencia en el marco de un proceso de justicia penal básico –a fin de preparar un caso factible de llegar a tener éxito para la fiscalía– y qué sucede cuando el caso llega finalmente al tribunal.

PREGUNTAS FRECUENTES

Las siguientes preguntas frecuentes, respondidas por los autores de este libro, están destinadas a medir su comprensión de los concepto presentados en este capítulo y a ayudarlo en la aplicación práctica de estos conceptos. Para que el autor pueda responder sus preguntas sobre este capítulo, sírvase visitar el sitio www.syngress.com/solutions y pinchar en "Ask the Author".

P: ¿Cómo pueden los investigadores visualizar los atributos de hora y fecha en los archivos UNIX?

R: En los sistemas basados en Unix, los atributos de hora y fecha se muestran en la lista de archivos cuando se utiliza el comando **ls**. Los atributos de fecha y hora que se pueden visualizar son *atime* (la última fecha y hora en que se accedió al archivo), *ntime* (la fecha y hora de la última modificaciones al archivo), *ctime* (la fecha y hora del último cambio de estado) y en algunos sistemas Linux, *dtime* (la fecha y hora de la eliminación del archivo). Cada vez que alguien accede al archivo el atributo *atime* se actualiza, o, si el archivo es ejecutable, el atributo *atime* se actualiza cada vez que se ejecuta el programa. Cuando se realizan cambios a un archivo, el valor *mtime* se actualiza. El atributo *ctime* se actualiza cada vez que se efectúan cambios..., por ejemplo, si se modifican los permisos. Para más información sobre los atributos de fecha y hora en Unix, así como los atributos de fecha y hora de NTFS y de la forma en que pueden ser utilizados en una investigación, véase en w.../documents/s=880/ddj0010f/0010f.htm.

P: ¿Por qué es tan importante la documentación? ¿No es suficientemente explícita la evidencia?

R: En muchos casos penales relacionados con la informática, la evidencia utiliza un lenguaje que no es comprensible para la mayoría de los miembros del jurado (en ocasiones ni siquiera para el juez, el fiscal y los oficiales a cargo de cumplimiento de la ley). Anteriormente los jurados eran propensos a aceptar el testimonio de expertos sin cuestionarlo, pero a medida que el público ha aumentado sus conocimientos técnicos y el testimonio de expertos ha sido cuestionado en casos de alta publicidad como fue el de O.J.Simpson, los jurados se han vuelto más escépticos sobre la infalibilidad de los expertos y más propensos a aceptar el cuestionamiento de los abogados contrincantes respecto de la veracidad de los métodos utilizados para procesar la evidencia y las

técnicas forenses. Es por ello que resulta tan importante que se documenten las medidas tomadas por lo oficiales a cargo del cumplimiento de la ley y los técnicos. La documentación también sirve para refrescar la memoria de las personas que deben testificar en el caso. A menudo los juicios tardan meses e incluso años, y para el momento en que un oficial o un técnico es llamado a testificar ya ha participado en muchos otros casos.

P: ¿Por qué es importante que todos los programas de computación que utilicen los oficiales encargados del cumplimiento de la ley tengan licencia o estén registrados? A menudo el presupuesto de los organismos de aplicación de la ley es escaso; ¿por qué no utilizar cuando sea posible los software libres?

R: Algunas herramientas de software libre que están disponibles en Internet son de buena calidad y sin dudas el precio aceptable. Sin embargo, el uso de estos programas con fines forenses entraña algunos peligros. En primer lugar, nunca sabemos exactamente qué es lo que estamos recibiendo cuando descargamos un programa libre (y, por supuesto, no podemos pedir que se nos devuelva el dinero si este programa no funciona como esperamos). Las descargas pueden estar infectadas por virus o troyanos capaces de dañar el sistema en el cual se utilizan. El uso de software sin licencia (copias ilegales) es incluso peor. Para los abogados contrincantes será una victoria descubrir que la policía utilizó en la investigación programas pirateados o "prestados". Actuar de esta manera podría destruir la credibilidad de las personas que realizaron el examen forense e incluso conllevar a la pérdida del caso. Además, trabajar con software apropiadamente registrado y adquirido nos permite recibir el apoyo técnico del proveedor en caso de ser necesario. Los productores de software de computación forense a menudo ofrecen descuentos a los organismos encargados del cumplimiento de la ley, lo cual facilita la posibilidad de adquirir las herramientas adecuadas para esta labor. Después de todo, los oficiales y los organismos no sugerirían ahorrar fondos adquiriendo las armas de servicio en una tienda de empeños; ello se debe a que esas herramientas son esenciales para su trabajo y deben ser tan fiables como sea posible. Para el técnico o investigador de delito informático se aplica la misma idea respecto del software forense utilizado para recopilar y preservar la evidencia que puede servir para ganar o perder un caso penal.

RECURSOS

- IACIS Forensics Procedures Standards
  www.cops.org/forensic_examination_procedures.htm
- *International Journal of Digital Evidence*
  www.ijde.org
- *Digital Evidence Collection and Handling*
  http://faculty.ncwc.edu/toconnor/495/495lect06.htm
- Federal Rules of Evidence
  www.law.cornell.edu/rules/fre/overview.html#403
- *Computer Forensics Legal Standards and Equipment,* por Damian Tsoutsouris
  http://rr.sans.org/incident/legal_standards.php
- New Technologies, Inc.: SafeBack Mirror Image Backup Software
  www.forensics-int.com/safeback.html
- High Technology Crime Investigation Association (HTCIA)

http://htcia.org

- Computer Forensics Online
  www.shk-dplc.com/cfo
- High Tech Crime Network
  www.htcn.org
- SANS Institute: *Incident Handling/Forensics*
  http:// rr.sans.org/incident/incident_list.php
- *Computer Forensics Magazine*
  www. forensic-computing.com
- American Academy of Forensic Sciences
  www.aafs.org
- DIBS: *History of Image Copying Technology*
  www.forensic-computing.com/articles/welcome.html
- *Forensic Computing Analysis: An Introduction,* por Dan Farmer y Wietse Venema
  www.ddj.com/documents/s=881/ddj0009f/0009f.htm
- *An explanation of Computer Forensics,* por Judd Robbins
  www.computerforensics.net/forensics.htm
- New Technologies, Inc. (NTI)
  www.forensics-intl.com/intro.html
- Timberline Technologies Forensics Products
  www.timberlinetechnologies.com/products/forensics.html
- *Linux Data Hiding and Recovery*, por Anton Chuvakin, Ph.D.
  www.linuxsecurity.com/feature_stories/data-hiding-forensics.html
- SANS: *What You Don't See on Your Hard Drive*, por Brian Kupper
  http://rr.sans.org/incident/dont_see.php
- SANS Institute: *Incident Handling/Forensics*
  http://rr.sans.org/incident/incident_list.php
- *Windows Wipe Utilities Fail to Shift Stubborn Data Stains*, por John Leyden
  www.theregister.co.uk/content/55/23759.html
- *Secure Deletion of Data from Magnetic and Solid-State Memory,* por Peter Gutmann
  www.cd.auckland.ac.nz/~pgut001/pubs/secure_del.html
- *Memory Imaging and Forensic Analysis of Palm OS Devices*, por Joseph Grand
  http://63.251.138.38/atstake/acrobat/pdd_palm_forensics.pdf
- *Computer Evidence Processing: Good Documentation is Essential*, por Michael R. Anderson
  www.forensics_intl.com/art10.html
- DoJ Computer Crime and Intellectual Property Section: *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*
  www.cybercrime.gov/searchmanual.htm
- *Admissibility of Electronic Evidence*, por Michael R. Overly
  www.forensics.com/resources/admiss.htm

Capítulo 11

PREPARACIÓN DE UN CASO DE DELITO INFÓRMÁTICO

Tópicos analizados en este capítulo:

- Principales factores que complican el trabajo de la fiscalía
- Resolución de obstáculos a un trabajo fiscal efectivo
- El proceso investigativo
- Testimonios en un caso de delito informático

- Resumen
- Preguntas frecuentes
- Recursos

Introducción

Los investigadores experimentados saben que, a diferencia de la filosofía del misterio criminal moderno, descubrir "quién lo hizo" no es el fin de la investigación, sino solamente el comienzo. En el capítulo anterior analizamos cómo recopilar y preservar la evidencia. Si bien en un caso de delito informático este puede ser uno de los aspectos más difíciles de la investigación, no es el paso final. Para que una investigación penal concluya con el enjuiciamiento del delincuente, debe terminar en la preparación de un caso sólido que incluya la documentación de toda la evidencia que se utilizará para lograr la condena del tribunal.

El proceso de preparación de un caso penal es extenso y complicado. Mientras más técnicos sean los hechos del caso más difícil será prepararlo y presentar la evidencia de manera que pueda ser comprendida cabalmente por lo siguiente factores fundamentales:

- el fiscal o un gran jurado (uno de los cuales, en dependencia del nivel del delito y del código penal que rija, tomará la decisión de llevar o no el caso ante un tribunal)
- el jurado en el tribunal (el cual en última instancia decide sobre la culpabilidad o la inocencia en un caso de delito grave y en ocasiones establece la sentencia)
- el juez (que pudiera decidir sobre la culpabilidad o la inocencia en un caso de delito leve y quien está cargo de establecer la sentencia incluso en los casos en los que la inocencia o la culpabilidad es decidida por un jurado)

El investigador no es la única persona que participa en la preparación del caso aunque sí, por lo general, es quien desempeña el papel más importante y coordina las tareas que deben realizar otras personas. Entre estas otras personas están los oficiales que deben personarse primero en el lugar, los técnicos de la escena del delito, el personal del laboratorio de criminalística, y miembros de los organismos asistentes (por ejemplo, cuando los organismos locales de aplicación de la ley envían evidencia digital a la policía estadual o al FBI para su interpretación o ampliación). Dado el carácter técnico de algunos delitos informáticos, también es normal solicitar la colaboración de especialistas o expertos del sector privado durante la investigación. El investigador penal a cargo del caso precisará trabajar estrechamente con estos expertos de terceras partes para facilitar que comprendan el papel que les corresponde y obtener el tipo de documentación necesaria para preparar el caso. Las técnicas, herramientas y procesos investigativos son básicamente los mismos en un caso de delito informático que en cualquier otro caso penal, si bien se aplican consideraciones especiales y existen varios factores que complican el procesamiento de estos tipos de delitos. En el presente capítulo analizamos esos factores, como la dificultad para definir el delito, los temas referidos a la jurisdicción, y problemas especiales relacionados con el carácter de algunos tipos de evidencia. También analizamos brevemente cómo la actitud autoritaria de muchos oficiales encargados del cumplimiento de la ley, la actitud elitista y anárquica de muchas personas del mundo de la informática, así como las relaciones de animadversión natural que existe a menudo entre las personas de ambas profesiones puede llegar a complicar la investigación. También presentamos una visión general del proceso investigativo en lo

tocante a un delito informático típico, incluida la explicación de las herramientas de investigación, los pasos que se deben dar durante la investigación y la importancia de definir las esferas de responsabilidad y se mantenga la cadena de custodia. Por último, analizamos el proceso del juicio y brindamos algunas ideas sobre la presentación de testimonios en un caso de delito informático, ya sea como testigos que brindan evidencia directa o como expertos que ofrecen conclusiones y opiniones.

Principales factores que complican el proceso

Algunos procesos penales no son tan simples como pudiera parecer a primera vista. Incluso una multa por exceso de velocidad puede volverse algo complicado si llega a tribunales. Quizás a los oficiales se les exija demostrar que han recibido el entrenamiento adecuado en el uso del equipo de radar, y la veracidad de ese equipo puede ser cuestionada sobre la base de infinidad de posibilidades técnicas teóricas. El procesamiento de los delitos más graves exige incluso mayor preparación por parte de todas las personas que testificarán, así como de aquellas que no serán llamadas como testigos pero que participan en el manejo de la evidencia o en la recopilación de los documentos para el expediente. Los delitos informáticos son inherentemente complejos por su naturaleza. Las computadoras -- que son máquinas complejas, cuya operación en realidad es comprendida por muy pocas personas-- siempre desempeñan un papel clave en todo delito informático. A menudo los delitos informáticos no están bien definidos en los estatutos que los rigen. Ello se debe en parte a que los legisladores que elaboran las leyes no comprenden la tecnología y también a que las teorías en las que se basa el sistema de justicia penal se formularon mucho antes de que sugieran las computadoras y no previeron los cambios que ellas introducirían en la criminalidad. Las ambigüedades jurisdiccionales son motivo de pesadilla para los investigadores y los fiscales. Como si ello fuera poco, gran parte de la evidencia en un caso de delito informático pudiera ser intangible y circunstancial. En las sesiones siguientes analizamos cada uno de obstáculos que se presentan en un proceso y las formas de resolverlos.

Dificultad para definir el delito

El primer paso de la investigación de un delito es determinar que de hecho se ha cometido. Muchas personas que no trabajan en la esfera jurídica –incluidas las personas con preparación técnica– poseen solamente una comprensión vaga de la ley y de lo que constituye un delito. Muchos hemos escuchado (y la mayoría de nosotros hemos utilizado) la frase "Debe existir una ley", pero a menos que *exista* una ley –y que esta describa específicamente el acto cometido– no podemos procesar a nadie por muy "equivocado" que pueda parecer el acto.

No todo lo que es inmoral o falto de ética es contrario a la ley, y debemos dar gracias por ello. El sistema de justicia ya está sobrecargado y mientras más leyes existan en los libros mayores será el potencial de que surjan dos cuestiones conflictivas pero igualmente inconvenientes:

- Mayores posibilidades de que se haga uso indebido de las leyes, lo que conduce a que personas inocentes sean castigadas.
- Mayores posibilidades de que se ignoran las leyes, lo cual conduce a que las personas culpables queden impunes.

La sociedad que intente regularlo todo y proteger a sus ciudadanos de todo posible malestar (incluso el causado por ellos mismos) pronto se percatará de que ha limitado el espíritu de la creatividad de esas personas y creado un estado policial en el que la opresión no es el precio gusto de la ilusión de seguridad. Por otra parte, la sociedad que intente vivir sin reglas y acepte la primicia de que "todo es bueno" y que todas las personas deben ser libres de hacer lo que gusten pronto caerá en la anarquía y el caos. Encontrar un balance entre estos dos extremos es un reto para la rama legislativa del gobierno y es un desafío al que se enfrentan los legisladores en relación con las zonas del ciberespacio que con anterioridad estaban mayormente desreguladas. El delito en el contexto del ciberespacio se está definiendo constantemente a medida que los gobiernos y sus instituciones tratan de brindar una legislación adecuada –pero no en exceso opresiva– que equilibre nuestro deseo de tener control y orden y los derechos de libre expresión y los beneficios del flujo libre de ideas.

En las sesiones siguientes analizamos la forma en que la criminalidad se define en términos de los órganos de la ley y la teoría básica de la justicia penal, y analizamos además los conceptos de los elementos del delito y la carga y el nivel de la prueba en que descansa el sistema de justicia penal.

Cuerpos de ley

Las computadoras, redes y los datos que por ellos pasan, al igual que otros aspectos de nuestras vidas, están sujetos a un número confuso de leyes que han sido aprobadas por órganos legislativos a diferentes niveles del gobierno (local, estadual, nacional e internacional), han sido creada por tribunales en forma de jurisprudencia, o han sido establecidas mediante órdenes administrativas u órganos de reglamentación. Dado que la ley es un laberinto de reglas complicadas en constante cambio, muchas personas no conocedoras de la rama legal ni siquiera intentan comprender cómo funciona sistema jurídico, las diferencias que existen entre los diferentes tipos y órganos de leyes, y como interactúan todas estas leyes diferentes entre sí.

NOTA

En los Estados Unidos, las leyes son aprobadas por un órgano legislativo, mientras que grupos de leyes conexas se compilan en colecciones denominadas *codificaciones* o *códigos* . Por ejemplo, un código penal contiene leyes penales; un código para vehículos automotrices contiene leyes referidas al tránsito, los delitos de tránsito y la explotación y mantenimiento de vehículos; el código de familia contiene leyes relacionadas con la custodia infantil, la adopción, el matrimonio y el divorcio, así como otro asunto familiares.

Por lo general las leyes se pueden dividir en tres "cuerpos" diferentes. Cada uno de estos cuerpos legales tiene su propia reglas de procedimiento, sanciones diferentes para los casos en que son violados, y organismos diferentes encargado de su aplicación y tribunales que tiene jurisdicción en ellos. La carga y el nivel de prueba requeridos para ganar un caso son diferentes, en dependencia del cuerpo legal aplicable. Los tres cuerpos legales son:

- derecho penal
- derecho civil
- derecho administrativo/de reglamentación

En las secciones siguientes analizamos cada uno de estos cuerpos legales y la diferencia entre ellos.

NOTA

La información contenida en este capítulo se refiere directamente al sistema jurídico de Estados Unidos. Otros países poseen divisiones similares del derecho, aunque podrían variar. Para más información sobre los temas internacionales, véanse lo recursos que se relacionan en el Apéndice, "Lucha contra el delito informático a escala mundial".

Derecho penal

Cuando escuchamos o utilizamos el término *ilícito* por lo general pensamos en la violación del derecho penal. Consideramos como algo "contrario a la ley" todo acto por el cual una persona puede ir a la cárcel o puede ser multado por el estado. No obstante, muchos actos que violan la ley no son delitos, sino infracciones civiles o violaciones del contrato civil. Por ejemplo, en la industria técnica a menudo escuchamos decir "es ilícito" regalar una copia de software que hayamos comprado. Si bien la *piratería de software* (lo cual incluye realizar y distribuir copias de software protegido por derecho de autor sin la autorización del titular de ese derecho) es un delito penal en algunas circunstancias y jurisdicciones, regalar una copia de un software que hayamos comprado lícitamente no lo es. No obstante, hacerlo podría significar una violación contractual –el acuerdo de licencia de usuario final (EULA) que una persona "firma" cuando instala el software. Ello significa que el proveedor de software podría entablar pleito legal contra usted en un tribunal civil y solicitar el pago por daños monetarios, pero usted no será encarcelado por ese delito.

Un delito *penal* debe ser específicamente definido como tal por el estatuto escrito de la localidad, el estado o el país. (Más adelante en este capítulo analizamos algunos detalles del derecho estatutario). Las leyes penales están destinadas a proteger a la sociedad, así como a las personas individuales, frente a actos que pudieran ocasionarles daños. También tienen el objetivo de sancionar a los que cometen las faltas como una disuasión tanto para esta persona como para otras, y en algunos casos están destinadas a garantizar que los delincuentes no puedan representar un riesgo adicional a la sociedad encarcelándolos o, incluso en casos extremos, al costo de sus vidas.

Las quejas por delitos penales se pueden presentar por las personas que han sufrido el daño o por los oficiales encargados del cumplimiento de la ley, o los ciudadanos que han sido testigos del delito. Sin embargo, los cargos se imputan no en nombre de la víctima sino en nombre del gobierno o la entidad gubernamental con jurisdicción. Es decir, un delito definido en el código penal estadual es procesado por el estado, y un delito federal es procesado por el gobierno federal. Existe un lenguaje específico para identificar los casos en el encabezamiento de todos los documentos de un tribunal. Si un caso se procesa a tenor del derecho penal, el documento llevará palabras como las siguientes: *El Estado de Texas contra John Smith* o *Los Estados Unidos de América contra Jane Doe*. En un caso penal, la persona o entidad que presenta los cargos se denomina *demandante*, y la persona (o empresa) contra la cual se presentan los cargos se denomina *demandado*.

Las sanciones por violación del derecho penal pueden incluir el pago de dinero o

la pérdida de libertad y pueden ser ligeras o severas, entre ellas:

- citación de advertencia (por lo general en el caso de infracciones de las leyes de tránsito u otros delitos leves de nivel más bajo)
- una citación que impone una multa (pago monetario al estado)
- compensación o resarcimiento (pago monetario a la víctima)
- servicio a la comunidad (trabajo "voluntario " obligatorio destinado a alguna organización caritativa u órgano del gobierno)
- condena condicional (supervisión por parte del gobierno durante un período de tiempo especificado en sustitución de la reclusión, el cual debe incluir restricciones por orden judicial sobre determinado comportamiento como el no uso de computadoras o la exigencia de que se asista a sesiones con asesoría)
- encarcelamiento (usualmente durante un período limitado, desde unos pocos días hasta un año)
- confinamiento en una prisión (por lo general por un período de tiempo más amplio, desde algunos meses hasta cadena perpetua)
- pena de muerte (en algunas jurisdicciones; usualmente limitada para las personas condenadas por asesinato)

Examen del derecho...
Definición de derecho
Por lo general en los Estados Unidos cada estado adopta un código de procedimientos penales y un código penal que definen, respectivamente, la forma en que se aplicarán las leyes penales y cuales sólo delitos penales. El código penal usualmente establece la forma en que se clasifican los delitos (infracciones, delitos leves y delitos graves) los *grados de sentencias* dentro de cada clasificación (como leves clase A, B y C y delitos mayores de primer, segundo y tercer grado) así como el rango de sentencias para cada grado de delito.

Los delitos penales por lo general se clasifican de acuerdo a su gravedad y la severidad de la sentencia. Estas clasificaciones pueden incluir las siguientes, en dependencia de la jurisdicción: *infracciones*, los delitos menos graves, para las que se impone solamente una multa; *delitos leves*, más grave que la infracciones y que se sancionan con multa o un período de encarcelamiento: y *delitos graves*, los de mayor gravedad, que se sancionan con cárcel (y en algunas jurisdicciones con la pena capital para los casos más graves). Los delitos informáticos pueden estar incluidos en todas las clasificaciones y grados de sentencia. En algunas jurisdicciones, los delitos como robo, daño a la propiedad y otros que ocasionan pérdidas monetarias se clasifican según el monto monetario de la pérdida o daño. Es decir, la intrusión en una red que ocasione una pérdida pequeña constituye un delito leve, mientras que el ataque que ocasione pérdidas monetarias elevadas a la víctima constituye un delito grave.

En Estados Unidos, la Constitución concede a las personas acusadas de delitos graves el derecho a juicio con un jurado. El acusado puede renunciar a este derecho si lo desea y decidir que el caso sea sometido al fallo de un juez.

NOTA

Jurisdicciones diferentes manejan de manera distinta las infracciones de tránsito, como el exceso de velocidad y el no respeto a la luz roja. Por ejemplo, en algunos estados de la Unión, estas infracciones se consideran delitos penales leves mientras que en otros se consideran infracciones civiles.

Derecho civil

El objetivo del derecho civil es resolver controversias entre personas o entidades (las partes en un proceso o acción). Así, los documentos del caso por lo general tendrán consignado el nombre de las dos partes privadas (por ejemplo, *John Smith contra Joe Jones* o *Jane Doe contra X Corporation*), si bien las entidades gubernamentales pueden ser partes en los procesos civiles también. Las faltas civiles no son delitos. Se les considera *cuasidelitos* o delitos civiles y el litigio civil es el proceso legal mediante el cual se solicita a un tribunal compensación o enmienda para esas faltas. En un proceso civil, la parte que inicia el proceso es llamada el *demandante*, mientras que la persona contra la cual se entabla el proceso se denomina *demandado*. (Aunque podríamos escuchar que se denomina *acusado* al demandado, el término no es técnicamente correcto en estos casos).

En un proceso civil la parte que lo pierde no va a la cárcel ni a prisión, a menos que sea encontrada culpable de un delito penal como el de desacato al tribunal. Por el contrario, estará sujeta a una de estas dos órdenes judiciales:

- Una orden que le exija al demandado el pago monetario por daños. Estos daños podrían ser pagos compensatorios por pérdidas reales o anticipadas por parte del demandante –tanto tangibles como intangibles– y daños punitivos más allá de las pérdidas reales, destinadas a sancionar a la parte que cometió la falta.
- Orden judicial que exija que el demandado realice determinada acción o que *no* realice determinada acción. Por ejemplo, se podría ordenar que la parte cese de enviar mensajes de correo electrónico al demandante. Una orden judicial es una orden jurídicamente vinculante y no respetarla puede conllevar a la presentación de cargos penales.

NOTA

Una diferencia importante entre el derecho penal y el derecho civil es que las personas sometidas a un proceso en un tribunal civil no tienen los mismos derechos, protecciones y presunción de inocencia que los acusados de delitos penales.

Hay acciones que pueden ser tanto una falta penal como civil. De esta manera, los investigadores de delitos informáticos podrían encontrar que la evidencia en los casos que manejan constituye también evidencia en un proceso civil. Cuando la red de una empresa es invadida, además de presentar cargos penales contra el hacker la empresa también puede iniciar un proceso civil que pretenda obtener directamente compensación monetaria por daños y perjuicios como la pérdida de productividad de los trabajadores y pérdidas de venta debido a las acciones del hacker.

Otro concepto importante en el derecho civil es el de la responsabilidad indirecta. Esta es la responsabilidad jurídica que poseer una persona o una entidad por las acciones

de terceros. La responsabilidad indirecta usualmente surge por alguna relación de " supervisión". Es decir, una persona o entidad que tenga el deber de supervisar o controlar a otra persona puede tener responsabilidad civil respecto de las faltas de esa otra persona. Ello significa que un padre es responsable por los actos de su hijo, y a un empleador se le puede exigir por los actos de uno de sus empleados. De esta manera, si un hacker utiliza los equipos de la empresa y su tiempo para invadir ilícitamente otras redes, para enviar pornografía infantil o para cometer otro tipo de delito informático, la compañía empleadora podría ser demandada por haberlo permitido.

NOTA

Es importante comprender que la responsabilidad indirecta por lo general se aplica solamente al derecho civil. En el derecho penal existen circunstancias limitadas (como cooperación penal) en las que una persona puede ser acusada de un delito cometido realmente por otra, pero en general, la responsabilidad penal exige *culpabilidad* (participación abierta en la comisión del acto prohibido) antes de que se puedan presentar cargos.

Derecho administrativo /derecho reglamentario

Un tercer cuerpo legal, a menudo pasado por alto en los debates sobre derecho penal y civil, es el derecho administrativo, también denominado derecho reglamentario. Este cuerpo legal está formado por reglas y reglamentos aprobados por un organismo gubernamental a tenor de la facultad que se le ha otorgado por el órgano legislativo, y que se aplican a una esfera ocupacional particular o rigen una esfera específica de la vida. Entre los ejemplos de ello está el reglamento del Organismo de Protección Ambiental, así como lo reglamento que rige la práctica de la medicina, el derecho, la ingeniería y esferas similares.

Las leyes administrativas no son ni penales ni civiles pero tienen la facultad de ley dentro de sus esferas de su jurisdicción. Por ejemplo, es posible entablar un proceso administrativo contra un médico o un abogado que viole el reglamento del organismo reglamentario estatal. Si es hallado culpable, el acusado puede ser censurado, multado o se le puede revocar la licencia. (Si ocurre lo último y la persona continúa practicando se pueden presentar en su contra cargos penales por practicar sin licencia). Las acciones administrativas por lo general siguen procedimientos establecidos por la ley que son similares a los de un tribunal, pero los consejos u otros órganos que reciben los casos no son oficiales de tribunal. Por lo tanto los procedimientos se denominan *cuasijurídicos*.

NOTA

En algunos casos, un acto puede estar sujeto a más de un cuerpo legal. Por ejemplo, el asesinato de una persona podría conllevar tanto a un cargo de asesinato (a tenor del derecho penal) como a un proceso por homicidio culposo a tenor del derecho civil). Asimismo, un delincuente informático empleado en la industria de las finanzas que descubra y haga uso indebido de la información de una institución en la bolsa podría estar sujeto a cargos penales y a sanciones administrativas.

Tipos de leyes

Los tres tipos de leyes –penales, civiles y administrativas/reglamentarias– se establecen

por una de estas tres vías. Son aprobadas por un órgano legislativo, son creadas por las decisiones de los tribunales, o surgen como resultado de la tradición en la práctica. El origen de las leyes determinará si se les considera derecho escrito, jurisprudencia o derecho consuetudinario o **common law**.

Derecho escrito

El derecho escrito es de los tres el de mayor peso y es en el que generalmente pensamos cuando hablamos de "la ley". Las leyes escritas se crean mediante el proceso formal llamado legislación. Son presentadas como proyectos de ley, debatidas, en ocasiones enmendadas, sometidas a votación y aprobadas por uno o más cuerpos legislativos, y son firmadas como ley por un funcionario ejecutivo con jurisdicción. En la mayoría los casos, tanto los miembros del órgano legislativo y como el funcionario ejecutivo son elegidos por voto popular de los ciudadanos. Las leyes escritas son redactadas y publicadas como estatutos, posteriormente codificadas (recogidas en códigos) y aplicadas por la policía y otro organismo encargados de hacerlas cumplir.

Jurisprudencia

La jurisprudencia está basada en la interpretación judicial de las leyes que han sido aprobadas por los órganos legislativos (leyes escritas) y los documentos rectores (por ejemplo, la Constitución de los Estados Unidos o la Constitución estadual o la carta de la ciudad). La jurisprudencia no tiene el mismo peso que la ley escrita porque tribunales diferentes pueden emitir interpretaciones drásticamente distintas, y las decisiones de los tribunales están sujetas al proceso de apelación.

No obstante, si bien la jurisprudencia no es vinculante como sí es el caso de la ley escrita, las opiniones judiciales que conforman la base de la jurisprudencia sí establecen *precedente*, lo cual significa que a la jurisprudencia se le otorga un peso por parte de otros jueces que toman decisiones en casos posteriores. En los tribunales penales y civiles, un abogado cita decisiones de casos anteriores para respaldar el suyo, y esto constituye una parte importante de los fundamentos de la decisión de los jueces.

A menudo los principios que establecen los jueces en la jurisprudencia se trasladan posteriormente a la ley escrita. Por ejemplo, en el famoso caso *Miranda contra Arizona*, el Tribunal Supremo de los Estados Unidos dictaminó que los oficiales a cargo de la aplicación de la ley deben informar sus derechos constitucionales a los sospechosos en los casos penales antes de interrogarlos en relación con el delito. Esta decisión no estuvo basada en ningún estatuto sino en la interpretación de los jueces sobre las garantías del debido proceso contenidas en la Declaración de Derechos de los Estados Unidos. Sin embargo, después de este caso que constituyó un hito, los cuerpos legislativos de muchos estados aprobaron leyes escritas que exigen que los oficiales informen de sus derechos a los sospechosos de haber cometido un delito penal.

NOTA

La jurisprudencia es importante en la aplicación de la ley en los casos de delito informático porque muchos de estos delitos no han estado recogidos en los libros durante un largo período de tiempo, por lo que sus interpretaciones no han sido bien definidas en los tribunales. En esferas ambiguas como la referida a la jurisdicción, es importante que los investigadores y los fiscales se mantengan actualizados sobre la jurisprudencia

aplicable ya que puede determinar si un caso es procesable o no.

Derecho consuetudinario

El derecho consuetudinario ha perdido prominencia con el decursar de los años a medida que se han aprobado leyes más formales que rige en asuntos que otrora estuvieron regidos por la tradición y las costumbres. En los días iniciales de los Estados Unidos, el derecho consuetudinario (basado en el sistema de *common law* inglés) constituyó una forma importante de gobernar la sociedad en los años en que se aprobaban formalmente una cantidad de leyes mucho menor. El derecho consuetudinario se basa en la práctica, o "la forma en que siempre hemos hecho las cosas".

Un buen ejemplo del derecho consuetudinario que aún se aplica es el matrimonio consensual, el cual es lícito en muchos estados de la Unión. Dos personas pueden llegar a estar legalmente casadas sin obtener una licencia de matrimonio del estado siempre que cumplan los requisitos del derecho consuetudinario, que usualmente incluye una declaración pública de que están casados y viven juntos, tienen fondos comunes, y actúan como una pareja casada. Dado que el derecho consuetudinario es propenso a la ambigüedad (por ejemplo, en el caso del matrimonio consensual si una de las partes niega la existencia de la relación marital podría ser difícil para la otra parte poder demostrarlo), en los Estados Unidos y otros países se están legislando formalmente cada vez más asuntos que usualmente estaban comprendidos en el ámbito del derecho consuetudinario.

Podría decirse que en los primeros tiempos de la Internet regía una forma de derecho consuetudinario. Si bien no existían leyes impuesta por lo gobiernos que se refirieran directamente a la actividad en línea, los "ciudadanos de la red" establecían sus propias reglas sobre la base del consenso. Por ejemplo, los internautas incendiarios (*flamers*) (personas que lanzaban ataques verbales y personales contra otras) y los contaminadores (*spammers*) (la persona que inunda las listas de correo y abruma a los individuos con anuncios no solicitados) eran a menudo rechazados y excluidos de los canales IRC y las listas de correo. Existía incluso una especie de fichaje, ya que personas con determinadas direcciones de correo electrónico (por ejemplo, los que terminan en @aol.com) eran inmediatamente sospechosos. Como en sociedades anteriores, se establecieron rápidamente tradiciones que definían cuál comportamiento era aceptable o no. Estas tradiciones aún persisten en muchas esferas de la red e influyen sobre el comportamiento en ese medio. Como sucedió con el derecho consuetudinario en sociedades anteriores, esas reglas se están ahora integrando a la legislación formal a medida que los órganos rectores introducen leyes destinadas a penalizar los mensajes de correo no solicitados y otras actividades similares.

Niveles de leyes

Las leyes escritas se aprueban a diferentes niveles del gobierno. A menudo estas leyes se solapan, de manera que un acto podría ser tanto un delito estadual como federal, por ejemplo. Por lo general, el ámbito de la ley está comprendido en una de estas cuatro categorías:

- leyes locales
- leyes estaduales
- leyes federales
- leyes internacionales

Los procesos de aprobación de estas leyes son muy similares; la diferencia radica en el cuerpo legislativo que las aprueba, el funcionario ejecutivo que las firma, y la jurisdicción geográfica dentro de la cual se aplican.

Leyes locales

En los Estados Unidos, el derecho local se refiere generalmente a las leyes aprobadas por un consejo de ciudad o por una comisión de condado, y que son firmadas por el alcalde o el juez de condado. Algunas ciudades y condados brindan al funcionario ejecutivo la facultad de vetar leyes; en otras, la firma es una simple formalidad. Las leyes locales generalmente se denominan *ordenanzas*. Las ciudades y lo condados pueden aprobar ordenanzas convirtiendo determinados acto en delito penal, pero solamente por lo general a los niveles inferiores. Por ejemplo, en Texas un delito penal a tenor de la ley de la ciudad es un delito leve Clase C, el nivel más bajo de delito penal. Las leyes locales se pueden hacer cumplir dentro de la frontera de la ciudad o el condado que las aprueba.

Las personas acusadas de violar las ordenanzas son sometidas a juicio en tribunales municipales o de condado. Por lo general estos tribunales no son *tribunales de actas* (no se toman actas del proceso). A nivel de estos tribunales de primera instancia el veredicto de culpabilidad puede ser apelado en un tribunal superior. Las ciudades y los condados pueden aprobar leyes referidas al uso de computadoras y redes, pero por lo general esto no se hace a nivel local.

NOTA

Las leyes locales están sujetas a las leyes estaduales y federales. Una localidad no puede aprobar una ley que viole la Constitución de los Estados Unidos o la Constitución estaduales o leyes específicas que brinden al estado el control absoluto sobre determinado comportamiento. Por ejemplo, algunos estados tienen leyes que prohíben a las ciudades y a los condados aprobar leyes para el control de armamentos, preservando ese derecho para el estado. Por otra parte, en muchos estados vemos que algunas ciudades tienen leyes que imponen toques de queda para los jóvenes o exigen el uso de cascos a los ciclistas, mientras que otras ciudades del mismo estado no las tienen.

Leyes estaduales

La mayoría de las leyes penales (delitos penales) aplicadas por la policía –incluida la policía municipal y la oficina del alguacil de condado– son leyes estaduales aprobadas por una legislatura estatal y refrendada por el gobernador del estado. Muchos estados tienen una legislatura bicameral al estilo del Congreso de los Estados Unidos, de manera que las leyes deben ser aprobadas por ambas cámaras. En algunos estados el gobernador tiene poder de veto.

Los estados pueden aprobar leyes penales en todos los grados de delito (delitos menores y delitos graves), y las sanciones pueden ser desde multas hasta la pena capital (en los estados que la permitan). Los estados tienen un amplio margen de acción en cuanto a los tipos de comportamiento que pueden proscribir. En general, a menos que la Constitución de los Estados Unidos o la ley federal prohíban que un estado regule un comportamiento particular, el estado tiene libertad para hacerlo. Muchos estados de la Unión poseen ahora algunas leyes referidas al delito informático, si bien estas son diferentes entre un estado y otro.

Leyes federales

La Constitución de los Estados Unidos otorga facultades legislativas federales al Congreso, el cual consiste en dos cámaras: el Senado y la Cámara de Representantes. Las leyes federales se presentan como proyectos de ley, ya sea en la Cámara o en el Senado (designados por *HR* o *S* delante del número de proyecto de ley para designar su origen) y por lo general son debatidas y enmendadas por comités, donde se pueden efectuar audiencias públicas para obtener los criterios de los ciudadanos antes de que se presenten al pleno del órgano para su votación. Luego de la aprobación por parte de una de las ramas, el proyecto de ley pasará a la otra. Si se realicen cambios en esta instancia, deberá regresar al órgano originario para que sean aprobadas, y así sucesivamente hasta tanto se llegue a un acuerdo. De manera alternativa, se podría crear un comité de conferencia con miembros de la Cámara y el Senado para resolver las diferencias. Una vez que las leyes son aprobadas por ambos órganos, pasa al presidente, el cual puede refrendarla, vetarla o dejar que se apruebe como ley sin firmarla. El veto presidencial puede ser anulado por el voto de dos tercios de la Cámara y el Senado en su conjunto.

Las leyes federales son aplicadas por el FBI y demás organismos de aplicación de la ley que se especializan en esferas específicas, como la Dirección de Lucha contra la Droga (DEA); el Buró de Alcohol, Tabaco y Armas de fuego; y la División de investigaciones criminales del Servicio de Impuestos Internos. El FBI investiga los delitos informáticos a nivel federal, y la Sección de propiedad intelectual y delito informático (CCIPS) de la División Penal del Departamento de Justicia brinda asesoría jurídica a los fiscales federales. El Reglamento federal de procedimiento penal rige el procedimiento en estos casos. La mayoría de las leyes penales federales están contenidas en el Título 18 del Código de los Estados Unidos (el equivalente federal del código penal estadual).

El gobierno federal no tiene facultades policiales generales dentro de los estados. Es decir, el FBI no puede arrestar a las personas por violar las leyes estaduales. El gobierno federal sí tiene jurisdicción que penal general sobre los lugares que no están dentro de la frontera estadual, como los terrenos federales, los territorios de los Estados Unidos y el Distrito de Columbia.

Leyes internacionales

Las leyes también se pueden originar a partir de tratados, que son acuerdos que firman los países. Por ejemplo, el Congreso aprobó la Ley de derecho de autor del milenio digital (DMCA) en 1998 para poner en práctica el tratado sobre derecho de autor de la Organización Mundial de Propiedad Intelectual (OMPI) firmado en Ginebra, Suiza, en 1996. La OMPI es un organismo de las Naciones Unidas integrado por 179 Estados Miembros. Para más información sobre las leyes internacionales, véase el Apéndice, "Lucha contra el delito informático a nivel mundial).

Teoría de justicia penal básica

Para investigar y enjuiciar delitos de cualquier tipo es preciso tener una compresión básica de la teoría de justicia penal. Incluso teóricos experimentados en la justicia penal se ven ante el reto de tener que encontrar la forma de ajustar un tipo de criminalidad que no existía cuando estas teorías se establecieron en un sistema destinado a abordar delitos menos complejos que involucran propiedad y evidencia tangible. En esta sección

analizamos algunos de los conceptos en los que se basa el sistema de justicia penal de Estados Unidos y las formas en que el delito informático se ajusta a estos conceptos.

Mala prohibita* y *mala in se

Los delitos se pueden dividir en dos grupos sobre la base de si se les considera actos inherentemente malévolos o actos que son simplemente "erróneos" solamente porque un cuerpo legislativo los convirtió en algo ilícito:

- históricamente los actos que se consideran como *verdaderos delitos* a tenor de las leyes de la naturaleza o de Dios se describen como *mala in se*, lo que quiere decir "malos en sí mismos". Actos como asesinato, robo, violación, hurto, entre otros, son ejemplos de este tipo de delito.
- Los delitos que no son universalmente considerados como penales pero que se convierten en tales por acto de la legislatura se consideran delitos *mala prohibita*. Dentro de ellos están el exceso de velocidad, poseer un arma sin permiso en un estado en el cual se exija tener licencia, o beber alcohol cuando se es menor determinada edad.

La clasificación de algunos delitos informáticos es aún tema de debate. ¿Copiar datos de la red de otra persona sin su autorización es más parecido a coger flores de una propiedad estatal (*mala prohibita*) o a robar bienes tangibles que pertenecen a otra persona (*mala in se)*? La diferencia entre los delitos de *mala in se* y *mala prohibita* no es muy importante desde el punto de vista jurídico –ambos tipos de leyes son aplicados idénticamente– pero sí lo es desde el punto de vista filosófico.

Corpus delicti: el cuerpo del delito

El concepto de Corpus delicti, que literalmente significa el cuerpo del delito, es otro concepto importante del derecho penal. Este término describe la esencia del delito, o la evidencia material que demuestra que se ha cometido un delito. Se deriva de la regla histórica en un caso de asesinato de que es preciso tener el cadáver para demostrar que se ha cometido un asesinato. Esta regla ha evolucionado con el transcurso del tiempo para permitir que el corpus delito que se ha establecido mediante evidencia presuntiva -- es decir, evidencia concluyente que llevaría a una persona razonable a presumir que una persona ha sido asesinada, incluso si nunca se llegue encontrar su cadáver. Por ejemplo, grandes cantidades de sangre que pueda demostrarse por examen de ADN como perteneciente a una víctima presunta viva, conjuntamente con la desaparición de la víctima, constituiría evidencia presuntiva.

Un factor que dificulta el procesamiento de los delitos informáticos es la ausencia de un corpus *delictis* concreto. Es decir, podría existir en absoluto evidencia tangible de un delito.

Actus reus y *mens rea*

Antes de que se puedan presentar cargos penales, deben existir dos elementos esenciales.

- *Actus reus* (*acto culposo*, en latín) es el acto o la omisión que prohíbe el derecho penal. Por ejemplo, el acto de apropiarse de un artículo en una tienda y sacarlo de ellas sin pagar por él es el acto prohibido para el delito de robo. El acto de acceder sin autorización a un archivo en una red es un

acto prohibido a tenor del delito de acceso no autorizado. Además de los actos abiertos u omisiones, las leyes penales también pudieran prohibir la simple posesión, como en el caso de las leyes sobre drogas y algunos delitos relacionados con las armas.

- Mens rea (*mente culposa*, en latín). Este término se refiere al estado mental que debe ser probado por la fiscalía para condenar al acusado en un caso penal. En ocasiones también se denomina estado mental culposo. El estado mental particular requerido para que constituye un delito está definido en el estatuto de ese delito y difiere en dependencia del mismo.

El sistema de justicia penal de Estados Unidos está basado en el principio de *actus reus non facit reum nisi mens sit* reaI. En latín esto significa "un acto no hace culpable a una persona de un delito a menos que su mente sea también culpable". En otras palabras, para poder condenar, el fiscal debe demostrar no solamente que el acusado cometió el acto prohibido sino también que poseía el estado mental culposo en el momento en que cometió el delito.

La mayoría de los códigos penales describen los estados mentales culposos de la siguiente manera:

- **Intención**. Es el deseo deliberado de la persona de obtener el resultado del acto (como la muerte de una persona).
- **Conocimiento**. La persona está consciente de que el acto tendrá el resultado obtenido
- **Imprudencia.** La persona sabe que existe riesgo considerable de que si se involucra en ese acto obtendrá ese resultado
- **Negligencia**. La persona *debía haber sabido* que existía un riesgo considerable de que si participaba en ese acto obtendría ese resultado

Examen del ciberderecho...
Para comprender la culpabilidad penal

Por lo general, la culpabilidad penal incluye uno de cuatro estados mentales: intención, conciencia, imprudencia o negligencia. A menudo un solo acto puede ser interpretado como delitos diferentes en dependencia del estado mental de quien lo comete. Aquí presentamos un ejemplo extremo –el acto de dar muerte a una persona al atropellarla con un vehículo automotor.

1- Si la persona ve a un transeúnte cruzando la calle frente a sí, se percata de que se trata de su peor enemigo cuya muerte deseaba desde hacía tiempo, y deliberadamente dirige el auto hacia el transeúnte, acelera y le provoca la muerte, el estado mental es *intención* y el delito cometido es el de asesinato.
2- Incluso si no tiene intenciones de matar, si el conductor ve al transeúnte, simplemente no tiene deseos de aminorar la marcha y lo atropella, el estado mental es de *conciencia*. El delito sigue siendo el de asesinato en la mayoría de las jurisdicciones porque los estatutos de asesinato por lo general especifican "intencionalmente o a conciencia" como nivel requerido de culpabilidad para el delito.
3- La persona está conduciendo a una velocidad excesiva para las condiciones climatológicas, no se detiene ante señales de padre, no presta atención a la vía mientras escucha la música ensordecedora en el estéreo de su auto, y atropella a un transeúnte en una intersección causándole la muerte, el estado mental es *imprudencia* y el delito es el de homicidio.
4- Si una persona sabe que los frenos de su auto están defectuosos y los ha perdido en varias ocasiones pero continúa utilizando el auto sin arreglarlos; ve a un transeúnte que cruza la calle frente a él y trata infructuosamente de detener el auto y atropella y mata al transeúnte, el estado mental es el de *negligencia* y el delito es el de homicidio por negligencia.

Por otra parte, si una persona va conduciendo su auto por la calle, obedeciendo las señales de límites de velocidad y otras, y un transeúnte intempestivamente entre en la vía de entre los autos que están estacionados e interrumpe el paso del auto, es atropellado y fallece como consecuencia de ello, no existe el estado mental culposo ni existe delito. El incidente es un accidente.

¿Cómo se aplica esta definición al delito informático? Es importante que los investigadores de delitos informáticos comprendan que, al igual que otros delitos penales, deben existir evidencias que demuestren el *mens rea* y el *actus reus*. Es decir, una persona que llega a entrar a una red sin intención de hacerlo (por ejemplo, al ejecutar un determinado programa o *script* que un hacker ha dejado en su computadora, sin saber que el programa o el *script* hacen esa función) o que accidentalmente elimine archivos vitales en un sistema, no tiene la intención ni el conocimiento necesarios a tenor de determinados estatutos para merecer una condena penal.

Elementos del delito

El acto prohibido y el acto mental culposo son los dos *elementos del delito* más importantes. Los elementos son aquellas cosas que deben ser probadas por la fiscalía para obtener una condena. La mayoría de los códigos penales describen elementos adicionales, como:

- **Resultado requerido** Algunos delitos requieren un resultado específico del acto antes de que se puedan presentar cargos. Por ejemplo, no se pueden presentar cargos de asesinato a menos que ocurra la muerte como resultado de la acción realizada por el acusado. (La mayoría de las jurisdicciones también prevén un delito denominado *intento criminal*, del cual se puede acusar a una persona cuando intenta cometer el delito pero no logra consumarlo).
- **Negación de excepciones** Algunos delitos prevén en los estatutos las *excepciones* al procesamiento. Una excepción difiere de una defensa contra el procesamiento en el sentido de que si la excepción procede, no se pueden presentar cargos. Una persona puede ser acusada del delito aunque exista la defensa estatutaria aplicable. Depende del acusado demostrar la defensa (en el juicio), pero depende de la fiscalía demostrar la negación de excepciones.

En la escena...
Analizando los elementos del delito
La Sección 33.02 del Código Penal de Texas define el delito de Violación de la seguridad informática:

a) Una persona comete un delito si intencionalmente accede a una computadora, red de computadoras o sistema de computación sin el conocimiento efectivo del propietario;
b) [define los grados de sentencia]

La Sección 33.03 define las defensas:
constituye una defensa afirmativa al procesamiento a tenor de la Sección 33.02 el hecho que el autor sea un oficial, empleado o agente de un portador común de comunicaciones o empresa de electricidad y haya cometido el acto o los actos proscritos durante el ejercicio de sus funciones y la realización de actividades propias de sus deberes o de la protección del derecho o la propiedad del portador común de comunicaciones o la empresa de electricidad.

Si analizamos los estatutos, veremos que el acto prohibido es "acceder a una computadora, red de computadoras o sistema de computación sin el conocimiento efectivo del propietario". El estado mental culposo (*mens rea*) es "a conciencia". La defensa contra el procesamiento se puede argumentar en tribunales, si es aplicable. Si el acusado puede demostrar que la defensa procede, puede ser absuelto. Si ello fuera una excepción en lugar de una defensa, los oficiales a cargo del cumplimiento de la ley tendrían que garantizar que no procedía antes de que pudieran realizar el arresto lícito. Este delito particular no tiene un resultado requerido que no sea "el acceso". No es necesario que ocurra daño o pérdida para presentar cargos.

Todos los elementos de un delito que están establecidos en el estatuto deben estar presentes antes de que se pueda arrestar al sospechoso. Los investigadores de delitos informáticos deben estar familiarizados con los estatutos en virtud de los cuales pretenden presentar cargos, y deben asimismo garantizar que cada uno de los elementos esté presente antes de realizar el arresto.

Nivel y carga de la prueba
Dos diferencias importantes entre el derecho penal y el derecho civil son el *nivel de prueba* requerido para encontrar a una persona jurídicamente responsable por un acto, y la parte sobre la cual descansa *la carga de la prueba* –es decir, qué parte debe demostrar su caso para ganar el juicio.

En un caso penal, la carga de la prueba cae sobre la fiscalía, que deberá demostrar el caso; si no lo hace, el acusado será absuelto sin necesidad de presentar caso alguno.

Ello se basa en la presunción de inocencia hasta tanto se demuestre la culpabilidad, lo cual es la base del derecho penal de los Estados Unidos. El nivel de prueba requerido en casos penales es muy alto: se debe demostrar la culpabilidad *más allá de toda duda razonable* y en un juicio con jurado todos sus miembros deben estar de acuerdo con el veredicto.

El sistema penal de algunos países opera sobre la base de la presunción opuesta; a tenor del Código Napoleónico –que es la base del derecho penal de Francia y otros países europeos– una persona acusada de un delito se presume culpable y la carga de la prueba descansa en el acusado, quien debe probar su inocencia.

En un caso civil, la carga descansa generalmente en los hombros del demandado, el cual es acusado de una falta civil y debe demostrar que no tiene responsabilidad. El nivel de prueba requerido es mucho menor que en un juicio penal; la parte que demuestre su caso mediante una *preponderancia de la evidencia* (es decir, hay ligeramente más evidencias que respaldan a esa parte que a la otra) gana el caso. En muchos casos civiles es preciso convencer solamente a la mayoría del jurado; es decir, la decisión no tiene que ser unánime.

Los investigadores de delitos informáticos deben estar conscientes de que los casos penales se mueven en dos niveles diferentes de prueba en diferentes momentos de la investigación. *Causa probable* (hechos y circunstancias que llevarían a una persona razonable y prudente a creer que la persona acusada cometió el delito) es el primer nivel y es el requerido para realizar una arresto lícito. La condena exige muchas más evidencias –suficientes para constituir pruebas más allá de duda razonable en la mente de todos los miembros del jurado. Esta es la razón por la que los investigadores de seguimiento son tan importantes, incluso después de que se ha recopilado evidencia suficiente para arrestar al sospechoso.

Temas jurisdiccionales

Los casos de delitos informáticos, más que la mayoría de los demás delitos, a menudo involucran complejas cuestiones jurisdiccionales que pudieran presentar obstáculos tanto jurídicos como prácticos para el procesamiento. A fin de comprender por qué la jurisdicción representa un problema en la aplicación de las leyes referidas al delito informático, debemos analizar su definición, incluidos los diferentes tipos de facultades jurisdiccionales, niveles de jurisdicción, y derecho escrito y jurisprudencias referidas a la jurisdicción. En las secciones siguientes analizamos estos temas y exploramos las complicaciones que surgen cuando los casos multijurisdiccionales asumen un matiz internacional. Asimismo, examinamos las consideraciones prácticas que dificultan el procesamiento de casos que abarcan diferentes líneas jurisdiccionales.

Definición de la jurisdicción

La *jurisdicción legal* se refiere al ámbito de autoridad que se concede a un organismo de aplicación de la ley para que haga cumplir las leyes o a un tribunal para que emita fallos jurídicos. Todos los poderes gubernamentales son jurisdiccionales por naturaleza. Es decir, son aplicables solamente en relación al lugar específico o temas concretos. Una ley aprobada en Francia no se aplica a los estadounidenses a menos que viajen a Francia. Al menos, así solía ser. El ciberespacio complica las cosas porque una persona puede ahora –con el uso de una computadora– cometer un acto en Francia (o cualquier otro país accesible mediante Internet) sin estar físicamente allí. ¿Quiere esto decir que un

estadounidense que nunca haya pisado suelo francés puede ser acusado de un delito a tenor de la ley francesa? Más adelante en este capítulo analizamos un caso real que se refiere a esta precisa cuestión. No obstante, debemos primero analizar los diferentes tipos y niveles de facultades jurisdiccionales.

Tipos de facultades jurisdiccionales

La dirección de un organismo encargado de la aplicación de las leyes, o de un tribunal, se puede basar en diferentes elementos. Entre ellos:

- **El sistema jurídico que rige el derecho** Los organismos policiales tienen jurisdicción sobre los casos penales pero no sobre los civiles. A menudo los ciudadanos solicitan que los oficiales de la policía intervengan en controversias civiles, pero desde el punto de vista jurídico la policía está incapacitada de hacerlo. Ello corresponde a los organismos pertenecientes al sistema civil. Por ejemplo, en algunos condados los segundos jefes de la policía tienen la facultad de hacer cumplir órdenes civiles como desalojos y decomiso de propiedad en cumplimiento de fallos de tribunales civiles. Los organismos de reglamentación pudieran tener un órgano de aplicación que tenga jurisdicción en su ámbito específico de responsabilidad. De la misma forma, los tribunales tienen jurisdicción respecto de casos civiles o penales; mientras que otros tienen jurisdicción sobre ambos.
- **Tipo de caso**. La policía municipal y estadual tiene jurisdicción sobre todos lo delitos penales a nivel del estado, aunque algunos organismos encargados de la aplicación de la ley tienen jurisdicción solamente sobre determinados tipos de caso. Por ejemplo, la comisión estadual de bebidas alcohólicas tiene jurisdicción respecto de delitos referidos a la venta, el uso y la transportación de bebidas alcohólicas; la comisión estadual de carreras tiene jurisdicción respecto de actos delictivos referidos a las carreras hípicas, mientras que la junta estadual de farmacias debe encargarse de la aplicación de las leyes penales referidas a las sustancias controladas. En ocasiones los tribunales están limitados a la jurisdicción sobre tipos específicos de casos (por ejemplo, los tribunales de familia que se encargan solamente de casos referidos a la custodia de niños y casos juveniles).
- **Grado del delito**. Los tribunales a menudo procesan casos relacionados con grados de de delito específicos. Así, en Texas los tribunales municipales procesan casos relacionados con delitos leves de clase C, mientras los tribunales de condado procesan casos de delitos leves clase A y B; por su parte, los tribunales de distrito procesan los casos de delitos mayores.
- **Reclamación por daños y perjuicios**. Algunos tribunales civiles procesan casos sobre la base de los límites impuestos a la cantidad monetaria pagadera por daños y perjuicios. El ejemplo más común es el tribunal para reclamaciones de menor cuantía, en las que el pago por daños y perjuicios está limitado a no más de unos pocos miles de dólares. Por lo general este tribunal está presidido por un juez de paz, funcionario jurídico electo que, a diferencia de los jueces de tribunales de instancias superiores, normalmente no necesita ser un abogado con licencia.
- **Nivel gubernamental**. Tanto a los organismos encargados del cumplimiento de la ley como a los tribunales se les asigna jurisdicción sobre la base del

nivel de gobierno. De igual manera, los tribunales operan a nivel municipal, de condado, estadual y federal.

- **Zona geográfica**. La jurisdicción geográfica se refiere a la zona física respecto de la cual tiene jurisdicción un organismo o un tribunal. Los oficiales de la policía municipal tienen jurisdicción dentro de los límites de la ciudad, la policía del estado tiene jurisdicción en todo el territorio del estado, y así sucesivamente. En muchos estados, no obstante, los oficiales de la policía tienen jurisdicción legal en todo el estado aunque las políticas policiales en ocasiones los limitan a realizar arrestos solamente dentro de las fronteras de la ciudad o del condado en que trabajan. Igualmente, los tribunales tienen jurisdicción dentro de determinadas zonas geográficas. Por ejemplo, un tribunal municipal en la ciudad de Houston tiene jurisdicción respecto de delitos leves clases C, pero solamente aquellos que ocurren dentro de los límites de su ciudad.

Es en una jurisdicción geográfica en lo que principalmente pensamos cuando escuchamos el término jurisdicción. Sin embargo, es importante comprender que el ámbito de la autoridad jurisdiccional se puede basar en otras cuestiones además de la zona geográfica.

En la escena...
Fuerza de tarea multijurisdiccional
Una de las formas en que los organismos encargados del cumplimiento de la ley en los diferentes niveles jurisdiccionales pueden cooperar para resolver los problemas de delitos especiales, como el delito informático, es mediante la fuerza de tarea multijurisdiccional. El Servicio Secreto de los Estados Unidos ha ayudado a organismos creando este tipo de fuerza de tareas compuesto por miembros de los organismos de aplicación de la ley a nivel local, estadual y federal. El modelo para este tipo de fuerza de tarea fue la Fuerza de tareas para delitos electrónicos de Nueva York (NYECTF), ubicadas en el Centro Mundial de Comercio antes de los ataques terroristas del 11 de septiembre de 2001 que destruyeron ambas torres.

Nivel de jurisdicción
Los niveles de jurisdicción corresponden a los niveles de ley. La jurisdicción de los organismos encargados del cumplimiento de la ley y los tribunales puede ser local (ciudad o condado), estadual, federal o internacional. Los niveles jurisdiccionales se pueden solapar. La mayoría de los ciudadanos de Estados Unidos están familiarizados con el concepto de *prohibición contra doble enjuiciamiento.* Sobre la base de la Sexta Enmienda a la Constitución de Estados Unidos, este principio plantea que ninguna persona puede ser juzgada dos veces por el mismo delito. Lo que muchas personas no comprenden es que una persona puede de hecho ser acusada y juzgada dos veces por el mismo acto si dichos cargos son presentados en niveles jurisdiccionales diferentes. Esto fue lo que ocurrió cuando el sargento Stacy Koon y otros oficiales del departamento de policía de Los Angeles fueron juzgados y absueltos al nivel estadual por el acto de brutalidad policial en el caso de Rodney King en los años 90, y después fueron juzgados

y convictos al nivel federal.

Asimismo, un delincuente informático pudiera ser acusado de acceso no autorizado a una red a tenor de las leyes sobre delito informático de un estado y ser acusado a nivel federal por el mismo acto si dicho delito incluye cuestiones comprendidas dentro de la jurisdicción federal (por ejemplo, si la computadora pertenece a una institución financiera).

El problema del ciberespacio

La jurisdicción presenta un problema especial en casos de delito informático porque los delitos son por definición cometidos en el ciberespacio, el cual no es un "lugar" físico. El delincuente y la víctima en ocasiones están a millas de distancia entre sí, y el delincuente pudiera no haber pisado nunca el territorio del estado o país donde provoca el daño.

Otro factor que complica el asunto es la cultura del ciberespacio. Muchos consideran que Internet debería permanecer como una "zona libre" en la que no se aplique ningún reglamento gubernamental. Otros consideran que las leyes vigentes son suficientes y pueden ser aplicadas efectivamente al entorno del ciberespacio. No obstante, hay otros que piensan que deberíamos tener "ciberpolicías" cuya jurisdicción es la Internet. La última solución, si bien es intrigante, concita incluso nuevas interrogantes: ¿quién emplearía a los ciberpolicías? ¿Una entidad internacional como la ONU? De ser así ¿tendrían ellos jurisdicción solamente dentro de los Estados Miembros? ¿Tendría un órgano internacional autoridad para aprobar leyes que regulen el comportamiento en Internet? ¿Qué sucedería si dichas leyes entraran en conflicto con las leyes de los estados o naciones que pertenecen a ese órgano internacional?

Derecho escrito referido la jurisdicción

La mayoría de los estados de la Unión tienen leyes que abordan la jurisdicción de las leyes y los tribunales estaduales. Por ejemplo, el Código Penal de Texas, sección 1.04, titulada Jurisdicción Territorial, plantea:

" a) Este estado tiene jurisdicción respecto de un delito que cometa una persona por su propia conducta o por la conducta de otra respecto de la cual tiene responsabilidad penal si:

1) la conducta o un resultado que es un elemento del delito, ocurre dentro del estado;
2) la conducta fuera del estado constituye un intento de cometer un delito dentro del estado;
3) la conducta fuera del estado constituye una conspiración para cometer un delito dentro del estado, y un acto adicional relacionado con la conspiración ocurre dentro del estado; o
4) la conducta dentro del estado constituye un intento, solicitud, o conspiración para cometer, o establece responsabilidad penal en la comisión de un delito en otra jurisdicción que constituye también un delito a tenor de las leyes del estado".

Este código brinda al estado amplias facultades para presentar cargos en una amplia gama de casos y abarcar a la mayoría de delitos informáticos que se originan

dentro del estado o cuando se obtiene un "resultado" (como la pérdida de propiedad intangible) dentro del estado aunque en el perpetrador pudiera estar en otro estado o incluso fuera del país. Jurídicamente, entonces, Texas podría presentar cargos contra los ciudadanos de otros estados o países que nunca han estado en Texas. Prácticamente ello requeriría la extradición, que pudiera ser o no concedida por el estado o países donde esté físicamente el acusado. Más adelante en este capítulo analizamos que mayor detalle la forma en que las consideraciones prácticas pudieran complicar el procesamiento.

Jurisprudencia referida a la jurisdicción

Mencionamos ya el caso de Tennessee contra Robert y Carleen Thomas. En el caso de los Thomas, el brazo largo de la ley llegó a aproximadamente 2000 millas del tribunal de Tennessee hasta California, donde vivían y trabajaban los Thomas. El gran jurado en Tennessee presentó la acusación contra los Thomas por violar los estatutos de obscenidad de Tennessee, aunque su BBS para adultos había sido declarada legal por el condado de Santa Clara, California, donde estaban ubicados, y los Thomas fueron juzgados y condenados en Tennessee y enviados a prisión. Este caso fue un hito en el asunto de jurisdicción ya que se aplica a los actos cometidos en el ciberespacio.

Otro caso que promete ser importante en cuanto a la jurisdicción internacional se está desarrollando mientras escribimos este libro. En mayo de 2000, un tribunal francés ordenó a Yahoo, el servicio web con sede en Estados Unidos, retirar toda la parafernalia nazi que se ofertaba en venta en su sitio (hospedado en los Estados Unidos). Yahoo se negó y en noviembre de 2000 el tribunal francés amenazó con multar a Yahoo con 13,000 dólares diarios si la compañía no acataba el fallo. Al mes siguiente, Yahoo presentó ante los tribunales de los Estados Unidos una demanda para que se emitiera una declaración en el sentido de que la orden francesa no se podía aplicar por parte del gobierno los Estados Unidos. En noviembre de 2001 el tribunal de distrito de los Estados Unidos emitió una decisión en el sentido de que aplicar la orden francesa violaría el derecho constitucional de Yahoo a la libre expresión. Posteriormente, en febrero de 2002, el tribunal francés respondió que llevaría a juicio a Yahoo en Francia por aprobar crímenes de guerra! Este caso aún no ha concluido y será interesante ver cómo termina. En cuanto al caso de los Thomas, el acto cometido no es un delito grave en la jurisdicción en que está ubicado el acusado, pero se consideró un delito en otra localidad desde la cual se podía acceder por Internet a los objetos "de índole delictiva".

La posibilidad de disputas jurisdiccionales similares existe ahora que es tan fácil para un delincuente utilizar Internet para "salir y llegar hasta alguien" en un estado o país que no sea aquel en que está ubicado el delincuente.

Complicaciones internacionales

En el derecho internacional, el concepto de territorialidad se basa en el principio de que las naciones no deben ejercer su jurisdicción fuera de su territorio (*Dictionary of Law*, Oxford University Press). No obstante, a las naciones les está permitido ejercer jurisdicción dentro de su territorio respecto de los actos cometidos por sus ciudadanos cuando están fuera de sus fronteras. Además, por lo general se les permite ejercer jurisdicción respecto de actos delictivos en los cuales parte del acto ocurrió dentro de su territorio (es decir, el delito se originó en su territorio y fue concluido fuera de él, o se originó fuera de su territorio pero fue concluido dentro de él).

¿Cómo afecta este concepto a los casos de delito informático? ¿Puede una nación aplicar sus leyes a personas que residen fuera de su territorio y que, por ejemplo, operan sitios web que violan las leyes de esa nación? Todas estas preguntas deben responderse antes de abordar al nivel global el delito informático. Los tratados internacionales propuestos, como la Convención internacional para combatir el delito y el terrorismo informáticos, siempre terminan resaltando el hecho de que existe un gran desacuerdo dentro y entre las naciones respecto de qué constituye delito informático. No es probable que los problemas asociados con la aplicación de la ley a nivel internacional se resuelvan de manera fácil y rápida.

Consideraciones prácticas

Además del asunto de las legalidades, por varias razones prácticas los organismos encargados de la aplicación de la ley y los fiscales prefieren no emprender casos de delito informático que los hagan salir de su jurisdicción normal. Entre estas razones están:

- los costos de viajes para investigar las pistas en ciudades, estados o países distantes
- la dificultad de trasladar a testigos e informes desde lugares lejanos hasta la sede del tribunal
- la dificultad para extraditar a un sospechoso que está ubicado en otra jurisdicción
- la realidad política de que los ciudadanos por lo general desean que sean sus organismos policiales los que se encarguen primero del delito cometido en la localidad
- la falta de compresión y conocimientos técnicos dentro del organismo encargado de la ley y de la fiscalía
- el papeleo y la burocracia que a menudo son parte del proceso para obtener la cooperación de los organismos en otro jurisdicción, especialmente en otros países
- la barrera idiomática que en ocasiones dificulta la comunicación con otros organismos y los testigos en otros países

El hecho que un organismo que tenga autoridad jurídica para presentar cargos penales en un caso particular no significa que lo hará necesariamente, especialmente si se considera que es más rentable o más políticamente expedito no hacerlo. En este sentido, los delitos informáticos son iguales a los demás tipos de delitos. No obstante, pudieran existir más razones para no procesar un caso delito informático que en un caso penal típico.

Naturaleza de la evidencia

Además de la dificultad de definir el delito y los temas jurisdiccionales que complican el proceso, otro obstáculo en el camino para la preparación y la resolución satisfactoria de un caso contra un delincuente informático es la naturaleza de gran parte de la evidencia. Por lo general las leyes reconocen tres tipos de evidencias:

- **Evidencia física**. Artículos tangibles que brindan prueba de la comisión de un delito y/o la identidad del delincuente (por ejemplo, el arma utilizada para cometer un asesinato).

- **Evidencia directa**. El testimonio de testigos que presenciaron la comisión del delito y observaron al acusado cuando se preparaba para cometer el delito, o que de otra manera tienen conocimiento directo del delito.
- **Evidencia circunstancial**. Hechos y circunstancias que tienden a respaldar la teoría de que el acusado cometió el delito pero que no brindan una prueba definitiva.

Gran parte de la evidencia en los casos de delito informático es evidencia digital; ello significa que no es evidencia tangible sino que más bien está en forma de pulsaciones electrónicas o magnéticas almacenadas en forma de cargas electromagnéticas en un disco o una cinta. Esta evidencia no es solamente en gran medida intangible, sino que es también frágil, muy parecido a la evidencia que consiste en una huella de pisadas en la nieve. Se debe obtener un registro sobre la existencia de la evidencia antes de que esta se "derrita" y se pierda. Como sucede con la huella de una pisada, podría ser imposible preservar la evidencia original de un delito informático para presentarla en un tribunal, y la imposibilidad de presentar la evidencia original tiende a debilitar el caso de la fiscalía.

Los hackers con conocimientos técnicos pueden destruir la evidencia pasando por múltiples servidores hasta llegar a su objetivo y, entonces, una vez logrado su propósito, borrar los ficheros de registros en cada servidor para encubrir sus huellas. Según Dan Clements, investigador de fraudes y citado en http://news.com/2009-1017-912708.html, este es el equivalente digital de "limpiar la escena del crimen".

Como la evidencia digital es intangible, frágil y fácilmente destruible (ya sea de manera deliberada o accidental), el manejo apropiado de la evidencia es incluso más importante en los casos de delito informático que en los otros tipos de delito. Como analizamos en el capítulo 10, los investigadores deben hacer inmediatamente copias de los discos que pudieran contener material probatorio y trabajar solamente en esas copias, preservando la integridad de la evidencia original. Además, toda la evidencia debe ser documentada cuidadosamente.

Factores humanos

Los obstáculos para procesar por vías legales un caso de delito informático que hemos visto hasta el momento tienen que ver con cuestiones jurídicas o técnicas. No obstante, existen otros factores que dificultan la preparación de un caso de delito informático, los cuales podrían considerarse como *factores humanos*. Estos se refieren a la necesidad de que los oficiales del cumplimiento de la ley y los técnicos de las TI trabajen de conjunto para lograr mayor efectividad en la preparación de un caso procesable, y las dificultades que ambas partes enfrentan para lograrlo.

"Actitud" de los encargados de aplicar la ley

El personal encargado de la aplicación de la ley tiene un dicho: "Nadie entiende a un policía mejor que otro policía. Eso es verdad desde muchos puntos de vista. A los policías se les envía a las calles para que realicen un trabajo extremadamente difícil, con una inmensa responsabilidad y enfrentados a expectativas demasiado elevadas. A menudo con muy poco entrenamiento, se les ubica en puestos con mucha autoridad pero bajo el escrutinio público, limitados por la ley y políticas departamentales, con el deber de tomar decisiones rápidas en situaciones que afectan la vida de seres humanos. Posteriormente sus decisiones serán criticadas por gente que no tiene experiencia del

trabajo en la calle pero de quienes depende el futuro profesional de los oficiales.

Los organismos encargados de la aplicación de la ley son, en gran medida, organizaciones paramilitares –con énfasis en el prefijo *para*. El personal militar por lo general tiene una misión bien definida. Los oficiales de la policía a menudo operan según los caprichos de los políticos y los burócratas y se espera de ellos que satisfagan a todos: que sean "duros contra los delincuentes" pero siempre agradables con los ciudadanos, los héroes que nos salvan de los malos pero que son suficientemente sensibles para no ofender a nadie. Los oficiales a menudos tienen escaso entrenamiento, son mal pagados, están sobrecargados de trabajo y estresados. Los salarios son bajos, las horas de trabajo largas, y los índices de divorcio, alcoholismo y suicidio son elevados.

No es de extrañar que muchos oficiales de la policía tengan "una actitud". La mayoría de los jóvenes que se unen a la fuerza policial lo hacen porque en realidad desean ayudar a la gente y contribuir a hacer de este mundo un lugar mejor y más seguro para la vida. Como los policías ven a diario el lado más oscuro de la humanidad pueden poco a poco volverse cínicos y suspicaces, y desarrollar una mentalidad de "nosotros contra ellos" que excluye a todo el que no sea policía (incluso hasta su propia familia).

Esta es la cultura de la aplicación de la ley. Los que están del otro lado de esta "delgada línea azul" deben comprenderlo a fin de poder trabajar de manera eficaz con los oficiales de esta esfera. Por lo general los investigadores han de tener varios años de experiencia de trabajo en las calles antes de poder ser designados como investigadores, de manera que la "actitud" casi siempre está enraizada. Los profesionales de las TI que deseen integrar el equipo investigativo tienen que aprender a pensar como policías, de la misma manera que los investigadores policiales deben aprender a pensar como los hackers para penetrar en su cultura y comprender lo que hacen y cómo lo hacen. Llegar a entender a los oficiales de la aplicación de la ley no es difícil, si recordamos estos puntos básicos:

- **La mayoría de los oficiales de la policía no tienen tanta seguridad como parece** "Aparentar seguridad" es un requisito del oficio y los oficiales saben alardear; sin embargo, los que actúan de manera más autoritaria casi siempre son los menos seguros de sí mismos.
- **La mayoría de los oficiales de la policía no entienden la tecnología** Naturalmente, ha excepciones. No obstante, la mayoría de los oficiales no son versados en temas de tecnología. Generalmente saben mucho sobre radios, linternas y otros artículos utilizados tradicionalmente por la policía, pero piensan que las computadoras son cosa de "gansos". Esta actitud está cambiando a medida que las computadoras abundan más en las oficinas, pero los cambios son lentos.
- **A la mayoría de los oficiales de la policía les disgusta no entender** Son recelosos, e incluso hasta envidiosos, hacia las personas que sí saben sobre computadoras. Por lo general, los profesionales de las TI ganan más dinero que los policías, sin tener que arriesgar la vida. Por esa razón, es comprensible que los policías sientan cierto resentimiento.
- **Muchos oficiales de la policía se sienten bastante impotentes** A pesar del mito del "poder policial", muchos oficiales se sienten agobiados por el ambiente altamente estructurado del organismo, en el que el más mínimo desliz es motivo de medidas disciplinarias, y por el peso de las leyes, políticas,

factores políticos y requerimientos de las relaciones públicas.

Todo esto da lugar a cierta paranoia policial cuando trabajan con gente que no es del medio –que no son oficiales de policía juramentados. Es preciso vencer esta actitud para que la policía pueda trabajar con efectividad con los profesionales de las TI, la administración de las empresas y la ciudadanía en general para combatir el delito informático. Tanto para los oficiales como para los investigadores, el primer paso para vencer las actitudes negativas es reconocer que existe el problema. Para los profesionales de las TI, el primer paso es reconocer cómo la diferencia entre ellos aumenta con el marcado contraste entre el ambiente policial altamente estructurado y el estilo de vida más relajado de la alta tecnología.

El estilo de vida de la alta tecnología

Ahora que ha explotado la burbuja de los punto-com y muchas empresas de alta tecnología han desaparecido del mapa, el estilo de vida de la alta tecnología ha bajado un tanto, de lo ridículo a lo meramente sublime. Al menos, eso parece cuando el policía promedio compara sus ingresos salariales con los ingresos y los "plus" que se obtienen con muchos de los empleos en la industria de la tecnología. Sin embargo, la diferencia en los estilos de vida va más allá del simple tema monetario.

Los policías, que trabajan en un ambiente altamente estructurado, tienen la tendencia a llevar una vida estructurada también cuando no están de servicio. El policía típico es puntual y piensa que las cosas deben hacerse "según el manual", según las reglas. El típico miembro del mundo de la tecnología tiene un enfoque más relajado, y a menudo admira a los que son suficientemente inteligentes para violar las reglas. La mayoría de los policías son políticamente conservadores, mientras que los otros suelen ser liberales. Los policías suelen mantener un mismo empleo y a menudo se retiran del organismo al que ingresaron siendo muy jóvenes; tienden a echar raíces y permanecer en la misma comunidad la mayor parte de la vida o la vida entera. Por el contrario, los de la esfera de la alta tecnología suelen pasar de empleo a empleo y de un lugar a otro en busca de mayores salarios y mejores oportunidades. No es de extrañar que los policías y los profesionales de la alta tecnología no se entiendan entre sí.

¿Adversarios naturales?

A primera vista, los policías y los profesionales de la alta tecnología no compaginan de ninguna manera. Además de las diferencias entre ellos, no es raro encontrar en ambos bandos una mentalidad elitista. Los policías se sienten superiores en virtud de su autoridad gubernamental, mientras que los otros se sienten superiores sobre la base de su posición en el mundo de los negocios. También hay cierta mística en esto. Los policías portan armas, con las cuales la mayoría de los profesionales de la alta tecnología no tienen experiencia y que le son motivo de cierto temor. Por su parte, los expertos en tecnología pueden hacer lo que quieran con las computadoras, y muchos oficiales de la policía sienten temor ante esas máquinas misteriosas.

Muchos profesionales de las TI apoyan –o al menos comprenden– a los hackers, a quienes la policía considera delincuentes. Muchos profesionales de las TI no ven nada malo en el intercambio de software y en la descarga de música mediante servicios de intercambio de archivos al estilo de Napster, mientras que la policía considera que ello es una violación de la ley. Muchos policías no entienden o no aprecian la diferencia entre un hacker de "sombrero blanco" y otro de "sombrero negro", ni tampoco reconocen que

las habilidades que utilizan los delincuentes informáticos pueden ser también utilizadas con fines legítimos. Además, muchos profesionales de las TI culpan a la policía por la existencia de leyes con las cuales no están de acuerdo (como las que se oponen a la piratería de software) y no comprenden que la policía no es quien hace las leyes, sino simplemente se dedica a hacerlas cumplir.

Si bien ambas carreras parecen estar muy distantes, no es difícil encontrar puntos de convergencia. Los oficiales de la policía y los profesionales de las TI de hecho tienen muchas cosas en común.

- Ambos trabajan durante muchas horas sin horario fijo. ¿A quién encontramos a menudo trabajando a las tres de la madrugada de un domingo mientras todos los demás duermen? A oficiales de la policía y programadores.
- Por lo general ambos son profesionales dedicados a su trabajo que no desearían hacer otra cosa que lo que hacen.
- Ambos sufren de adicción a la cafeína, aunque pudieran tener sus preferencias en cuanto a su presentación.
- Ambos quieren que las cosas (la ley, los códigos) tengan sentido y se sienten frustrados cuando no resulta así.
- Ambos son por naturaleza solucionadores de problemas.

En esta última característica encontramos la clave para resolver todas las diferencias y trabajar de conjunto como partes de un equipo. En ambas profesiones se deben identificar los problemas o los posibles problemas y tomar medidas para resolverlos. Los policías y los profesionales de las TI que logran ver más allá de lo superficial podrán percatarse de que, después de todo, no son tan diferentes, al menos no de una forma trascendental cuando se trata de luchar de conjunto contra el delito informático.

Vencer los obstáculos a un procesamiento efectivo

A pesar de los muchos obstáculos que se enfrentan para procesar efectivamente los casos de delito informático –incluida la dificultad de definir el delito, las pesadillas jurisdiccionales que se presentan cuando el sospechoso y la víctima están en lugares geográficos diferentes, y las actitudes y los estilos de vida diferentes que dificultan el trabajo conjunto de la policía y los profesionales de las TI– es posible vencer todos estos desafíos y conformar un caso que logre tener éxito en los tribunales.

Los organismos a cargo del cumplimiento de la ley pueden trabajar con la fiscalía para esclarecer definiciones y garantizar que comprendan los elementos que deben probarse a fin de arrestar y condenar a un acusado de delito informático. El personal de las TI que tenga previsto trabajar con oficiales de la aplicación de la ley en casos de delito informático debe aprender los elementos básicos del funcionamiento del sistema de justicia penal, y ambos deben conocer las diferencias entre el derecho civil, el derecho penal y el derecho reglamentario, así como los actos específicos comprendidos en cada cuerpo de ley en su jurisdicción.

Hablando de jurisdicción, los investigadores deben estar preparados para cualquier complicación jurídica cuando los delitos informáticos traspasen las fronteras del estado o el país, como suele suceder. Asimismo, los investigadores deben ser realistas y comprender que incluso en los casos en que tengan jurisdicción legal, existen

numerosos factores prácticos que pueden impedir el procesamiento exitoso de casos de delito informático multijurisdiccionales.

Los oficiales a cargo de la aplicación de la ley y los profesionales de las TI pueden aprender a trabajar juntos en los casos de delito informático, lo cual repercutirá en una mayor eficiencia en las investigaciones. Un elemento importante para salvar las diferencias es aprender la jerga mutua. Los oficiales de la policía deben aprender la terminología técnica, mientras que el personal de las TI debe familiarizarse con el lenguaje legal y la jerga policíaca para lograr que exista una buena comunicación. El éxito en el procesamiento de un caso depende del trabajo de muchas personas y también de muchos factores. Un elemento importante en la preparación de un caso sólido gira en torno a la adecuada realización del proceso investigativo.

El proceso investigativo

Los investigadores de delito informático deben estar familiarizados con el proceso de recopilación de datos, materiales e información que pudieran estar relacionados con la comisión de un delito; esto, de hecho, es la definición de *investigación penal*. Los profesionales de las TI que trabajan con el personal encargado de la aplicación de la ley para facilitar el proceso pudieran sentirse intimidados por la palabra *investigación* y sus implicaciones oficiales, pero es más fácil de entender si nos percatamos de que en todo momento todos realizamos investigaciones. Siempre que conocemos a una persona por primera vez, hacemos una compra importante como en el caso de una vivienda o un auto, o tomamos una decisión trascendental como cambiar de empleo o casarnos, *investigamos* –lo cual se resume en una simple recopilación de información. Sin dudas el administrador de una red a menudo tiene razones para investigar; investigar cuando un servidor se cae, cuando un usuario no logra acceder a un recurso de red, cuando una aplicación no se ejecuta correctamente, etc.

Las únicas diferencias entre el tipo de investigación que son parte de nuestra vida diaria y una investigación policial radican en las formalidades y en los objetivos finales de la investigación. En ambos casos, el objetivo primordial es obtener información. En una investigación criminal, la información recopilada se utilizará para demostrar la culpabilidad de un acusado ante un tribunal. Por ello, el proceso debe ser formalizado a fin de tener una estructura estándar que garantice su avenencia con las leyes que rigen la recopilación de evidencia.

No obstante, es importante que los investigadores recuerden que incluso la evidencia que es inadmisible en un tribunal puede, no obstante, ser útil para la investigación ya que puede ayudar al investigador a reconstruir las circunstancias en que ocurrió el acto u omisión ilícita, y conducirnos a otra evidencia que sí sea admisible. Con miras a su presentación ante un tribunal, la evidencia debe ser evaluada a la luz de las siguientes preguntas:

- **¿Es pertinente?** En otras palabras ¿guarda relación con el caso? Si estamos investigando el caso de un hacker sospechoso de haber lanzado un ataque en DoS en una red de computadoras, descubrir que esta persona fue arrestada en una ocasión por utilizar medios para realizar llamadas de larga distancia y visitas no tiene ninguna influencia en el caso que nos ocupa y probablemente no sería admisible como evidencia (a pesar de que esa información *puede* ser presentada, en otras jurisdicciones, durante la

fase de dictamen de sentencia del juicio, una vez que el acusado haya sido declarado culpable).

- **¿Es material?** En otras palabras ¿prueba uno de los elementos esenciales del caso? ¿La evidencia demuestra que el sospechoso cometió el acto prohibido, demuestra el estado mental culpable del sospechoso, respalda el hecho de que ocurrió un resultado requerido, o niega la existencia de excepciones estatutarias?
- **¿Es competente?** ¿Es creíble la evidencia? Si la evidencia es un testimonio de testigo ¿es creíble ese testigo? Si la evidencia es digital ¿está probado su significado y cómo podemos probar que no ha sido violentada?

La investigación debe ser objetiva; después de todo, el objetivo de una investigación no es condenar a una persona en particular sino determinar la verdad. Los investigadores deben poner a un lado los sentimientos personales y abordar la investigación de la misma manera que un buen periodista aborda una historia. De hecho, es útil que el investigador utilice las reglas que los periodistas aprenden para recopilar información con miras a ser publicada: llegar a conocer *quién, qué, cuándo, dónde,* y *cómo*. Estas son las preguntas que se deben responder antes de que podamos afirmar que conocemos toda la historia. En el cuadro 11.1 se muestra un desglose de los objetivos de una investigación criminal y cómo se puede utilizar el enfoque periodístico para realizarla satisfactoriamente.

Cuadro 11.1 Objetivos investigativos y el enfoque de los cinco puntos

Objetivo	**Preguntas a responder**
Determinar si se ha cometido un delito	¿Qué sucedió? ¿Quién participó?
Proteger la escena del crimen	¿Dónde ocurrió el acto ilícito? ¿Cuándo sucedió?
Identificar al sospechoso	¿Quién tenía motivos, medios y oportunidad para hacerlo?
Determinar el modus operandi	¿Cómo se cometió el hecho?
Probar que el sospechoso lo hizo	¿Quién observó la comisión del delito o sus resultados? ¿Dónde estaba el sospechoso cuando se cometió el delito? ¿Qué registros/documentos identifican al sospechoso?

Cuando hayamos respondido estas preguntas, el siguiente paso en el proceso es efectuar un arresto lícito. Ello no significa que la investigación ha concluido. Cuando se realice el arresto debemos haber recopilado suficiente evidencia para que constituya causa probable, sin embargo, ello no es suficiente para lograr una condena –se necesitan pruebas más allá de duda razonable– de manera que la investigación continúa mientras preparamos un caso que resulte eficaz para el procesamiento.

NOTA

Se necesita *causa probable* en dos situaciones: para obtener una orden de cateo o arresto o para realizar un arresto sin orden judicial. No es necesario que la evidencia sea admisible en un tribunal a fin de utilizarla como elemento de causa probable.

En un caso de delito informático, al igual que en cualquier otro delito, el investigador quizás necesite volver a visitar a los testigos y es posible que se llegue a descubrir nuevas evidencias antes de que se realice el juicio. A tenor del sistema de justicia de los Estados Unidos, la existencia de evidencia debe ser puesta en conocimiento de los abogados de la defensa.

Herramientas investigativas

El investigador conforma su caso utilizando herramientas investigativas estándar. Estas son:

- Información
- Entrevista e interrogatorio
- Instrumentación

En las secciones siguientes analizamos en detalle cada una de estas herramientas y cómo se aplican a un caso típico de delito informático.

Información

La información, que es la base del caso, se puede obtener de diferentes formas. En esta sección nos referimos a la información que puede recopilar un investigador mediante observación, el examen de documentos o datos electrónicos, y el examen de la evidencia física. Un medio importante para obtener esta información es la investigación de la escena del delito. En el caso de un delito informático, probablemente gran parte de la evidencia se encuentre en la computadora, almacenada en el disco duro o incluso aún en la memoria. Sin embargo, es importante que los investigadores tengan el cuidado de no concentrarse únicamente en la computadora, porque la escena del delito puede incluir toda la zona alrededor del equipo.

Si existiera evidencia en el sistema de que una computadora en particular fue utilizada para acometer un delito informático, debemos de todas formas establecer un vínculo entre la computadora y el sospechoso. En tal caso es conveniente utilizar técnicas tradicionales referidas a la escena del delito, como la búsqueda de huellas dactilares y el registro minucioso del lugar que pudiera resultar en la obtención de evidencia como documentos impresos, notas hechas por el sospechoso en relación con el delito, disquetes o cintas con datos de copias de seguridad que contienen información probatoria, etc. También es importante recordar que es posible que se haya guardado evidencia en otro lugar desde el cual ha sido recuperada mediante Internet o a donde fue transportada físicamente en un medio electrónico.

Entrevista e interrogatorio

La herramienta de entrevista e interrogatorio se refiere al proceso de interrogar a las personas que de alguna manera estén involucradas en un delito informático. La diferencia estriba en el papel desempeñado por una persona en el delito y la forma de realizar el interrogatorio. La entrevista se refiere a las preguntas que se realizan a los testigos, víctimas y otras personas que pudieran tener información pertinente para la

solución del caso. Entre estas personas pudieran estar expertos técnicos que pueden explicar la forma en que se cometió el delito y que pudieran también testificar como peritos en el servicio, o que simplemente pudieran brindar información que contribuya a que el investigador comprenda los aspectos técnicos del delito. La entrevista es en esencia una conversación (grabada o documentada por el entrevistador) con el objetivo de obtener información fáctica que pueda contribuir a identificar a la persona que cometió el delito y preparar el caso para procesarla.

El interrogatorio es el proceso de interrogar a las personas sospechosas de haber cometido el delito o de haber contribuido a ello. Por lo general el interrogatorio se graba, y es importante documentar que el sospechoso ha sido impuesto de sus derechos antes de comenzarlo, ya sea grabando esa información al momento de brindársele o mediante la obtención de una renuncia de derechos escrita por parte del sospechoso, o ambas. El objetivo del interrogatorio es obtener declaraciones incriminatorias y/o una confesión.

NOTA

Aunque las entrevistas de los testigos se deben grabar o documentar, en la mayoría de los casos será necesario que el testigo de un caso penal testifique personalmente ante un tribunal. En la mayoría de los casos el sistema de justicia de los Estados Unidos brinda al acusado el derecho a enfrentarse a su acusador, y la evidencia referencial (evidencia de terceras partes) por lo general no es admisible. Existen excepciones, entre ellas los casos de abuso infantil (incluidos los casos de pornografía infantil y violaciones de menores que pudieran constituir delitos informáticos), declaraciones de moribundos, y otros casos en los que el testigo está emocional o físicamente incapacitado para testificar personalmente.

Un interrogatorio a menudo por naturaleza entraña un ambiente de antagonismo, aunque no tiene que ser así necesariamente. Una de las mejores formas de obtener información útil de un sospechoso es ganarse su confianza, hacerle creer que simpatizamos con él. En los delitos informáticos que involucran actos de piratería y ataques técnicos, sería útil que el interrogatorio lo realice un oficial con conocimientos técnicos, porque alguien que hable el mismo idioma que el delincuente puede lograr hacerlo alardear sobre el poder técnico necesario para realizar la acción. La vieja rutina de "el policía bueno contra el malo" podría también funcionar, especialmente si conformamos un equipo con un policía joven, bueno y con conocimientos técnicos, "enfrentado" a un policía malo, más viejo y aparentemente con fobias tecnológicas. Existen muchas técnicas de interrogatorio y el investigador debe utilizar aquellas que mejor le funcionen y que se adapten de manera más natural a su persona. Algunas técnicas probadas y satisfactorias son:

- **Enfoque lógico.** Utilizar el razonamiento para convencer al sospechoso de que le conviene confesar.
- **Indiferencia.** Hacer creer que no necesitamos una confesión porque ya tenemos suficiente evidencia. Esto puede funcionar bien en los casos en que existe más de un sospechoso, cuando podemos hacer creer a uno que el otro o los otros ya han confesado.

- **Enfoque justificativo.** Permitir que el sospechoso se excuse por su comportamiento y aparentar que comprendemos las razones por las que cometió el delito.

En la escena...
La confesión es buena para el alma –y para la fiscalía
Para qué sea admisible por un tribunal, la confesión debe ser voluntaria; es decir, se debe haber obtenido sin coerción, soborno o cualquier otra influencia indebida. En algunas jurisdicciones es preciso que la confesión sea corroborada por un ente independiente a fin de que pueda ser admitida. Por ejemplo, si una persona admite haber enviado mensajes de correo electrónico con amenazas a otra persona, ello podría corroborarse mediante el conocimiento de esta respecto del contenido específico de los mensajes, que no fueron hechos públicos y no pudieron ser del conocimiento de otra persona que no fuera el destinatario, los oficiales encargados de la aplicación de la ley y el propio emisor.

Los investigadores deben siempre estar atentos a la posibilidad de una confesión falsa. ¿Por qué desearía alguien aceptar haber cometido un delito cuando no ha sido así? En la mayoría de los casos esto sucede porque la persona desea llamar la atención. Ello pudiera resultar un problema cuando se trata de un delito "popular", en el caso de un sitio web que expresa una idea política popular o un ataque contra la red de una corporación que tenga una mala reputación con el público. Esta es una razón para que los investigadores no hagan públicos todos los detalles de un caso o, incluso, para que dejen "filtrarse" información falsa o tendenciosa sobre el caso a los medios de información. Las confesiones pueden compararse entonces con los hechos verdaderos del caso, los cuales serían del conocimiento de sólo unas pocas personas, una de las cuales es la persona que en realidad cometió el delito.

NOTA

En determinadas circunstancias, la declaraciones se pueden utilizar en contra de un sospechoso sin que se le haya advertido de antemano sobre sus derechos y este haya renunciado a ellos, incluidas las declaraciones *res gestae* (aquellas realizadas de improviso y no como respuesta en un interrogatorio).

En los casos de delito informático se aplican las mismas directrices básicas que en el resto de los delitos, tanto en el caso de las entrevistas como en los interrogatorios de los testigos y sospechosos:

- Separar a las personas que se están entrevistando o interrogando. Incluso en el caso de testigos que no son inocentes de delito, estos pueden ser influenciados por la declaraciones de otros. Los sospechosos pueden revelar su culpabilidad dando testimonios contradictorios.
- Utilizar técnicas kinésicas de entrevista; observar el lenguaje corporal, el tono de la voz, las expresiones faciales y otros detalles extralingüísticos en la conversación que pueden brindar indicios sobre si una persona está

diciendo o no la verdad. Imitar sutilmente las expresiones corporales de la otra persona para crear un sentido de identificación con ella es otra técnica que se puede utilizar.

- Tener un plan táctico para la entrevista o el interrogatorio; debemos conocer todos los hechos disponibles sobre el caso y saber exactamente qué información estamos buscando.
- Garantizar que se sigan los procedimientos normales para gravar y/u obtener declaraciones escritas**.**

Una vez que hayamos obtenido información mediante una entrevista o interrogatorio, debemos analizarla para determinar su valor y su admisibilidad. Este análisis se puede basar en las respuestas a las preguntas siguientes:

- ¿La información respalda uno o más elementos del delito (es material)?
- ¿Podría la información contrarrestar la defensa o la coartada del sospechoso?
- ¿La confesión del sospechoso corrobora la información?

A menudo los investigadores utilizan un método de prueba para evaluar la credibilidad de la información que brinda un testigo. Esta prueba consiste en evaluar por separado al testigo que brinda la información y la información propiamente dicha, como se muestra en el Cuadro 11.2.

Cuadro 11.2 Método de prueba para evaluar la credibilidad de la información brindada por los testigos

Evaluar la credibilidad el testigo	Evaluar la credibilidad del información
¿El testigo brindó anteriormente información que resultó ser verídica?	¿La información coincide con los hechos observados u obtenidos a partir de otras fuentes?
¿El testigo es un miembro respetable de la comunidad, se le considera honesto, etc.?	¿Tiene sentido la información?
¿Es objetivo el testigo (en otras palabras, tiene algún interés personal en la investigación o relación personal con la víctima o el sospechoso)?	¿Está el testigo en condiciones de conocer sobre la información?

Instrumentación

La instrumentación se refiere al uso de la tecnología para obtener evidencias. En los casos de delito informático, un tipo de instrumentación es el uso de técnicas de recuperación de datos para recuperar información "borrada" y "eliminada". Otros ejemplos más tradicionales incluyen las técnicas forenses para recopilar y analizar evidencias de micropartículas, análisis de ADN, etc.

En la escena...

¿Mala suerte, buena investigación, o ambas?

Colaboración del Dr. Bernard H. Levin, profesor de la universidad Blue Ridge (Virginia) y comandante del Departamento Policial de Waynesboro, y Robert S. Baldygo, vicepresidente de la mencionada universidad. Los nombres de la víctima y del delincuente informático, así como de la universidad involucrada, han sido cambiados.

En ocasiones los tipos malos tienen una racha de mala suerte, lo cual hace más fácil la vida de los investigadores. En el siguiente informe se resumen algunos elementos referidos a un arresto reciente, realizado tras el intento de extorsión por parte del sospechoso utilizando la Internet. El supuesto perpetrador, "James Palmer" ha sido arrestado y se ha declarado culpable de cargos federales. También está acusado de varios delitos estaduales.

El caso llamó la atención de las autoridades locales y federales cuando un individuo, "Timothy Vaughan" reportó a la policía de la Universidad Major Eastern que había recibido mensajes de correo electrónico con la amenaza de causar daño a su familia si no se pagaba al remitente de los mensajes una determinada suma de dinero. A las dos semanas, los mensajes aumentaban sus amenazas y los detalles sobre la vida personal del destinatario. Después resultó que un conocido de Palmer trabajaba con la esposa de Vaughan. Un elemento clave en este intento de extorsión fue la impresión que tenía Palmer de que podía mantener su anonimato. Esta suposición por parte de él resultó ser errónea.

Palmer envió a Vaughan una gran cantidad de mensajes, casi siempre durante las últimas horas de la tarde. Luego de que Vaughan presentó la denuncia, el departamento de policía de la universidad contactó al servicio público de correo electrónico de Palmer. El servicio permite que los usuarios creen anónimamente direcciones de correo electrónico, de manera que no podía brindar información directa sobre la identidad del remitente. No obstante, el servicio pudo brindar información sobre las direcciones IP utilizadas. Estas direcciones IP utilizadas por Palmer fueron rastreadas hasta diferentes computadoras en otra universidad cercana. A diferencia de las computadoras de muchas redes, las que utilizó Palmer tenían direcciones IP fijas. Este fue el primer elemento en contra de Palmer. En consecuencia, el personal informático de la universidad pudo brindar a los investigadores un listado completo y un diagrama con la ubicación de todas las computadoras con acceso a Internet en la universidad. Otro elemento de mala suerte para Palmer fue haber escogido una universidad con personal informático deseoso de participar en la investigación, quienes lograron identificarlo con bastante rapidez.

El día que Palmer había fijado como fecha límite para recibir el dinero que había exigido, los investigadores tuvieron un contacto telefónico en tiempo real con Vaughan y el proveedor de servicios de correo electrónico. Los investigadores estuvieron presentes además en la universidad desde donde procedían los mensajes. Lograron determinar rápidamente el lugar en que estaba ubicada la computadora (en un laboratorio de computación temporalmente deshabilitado). Palmer estaba sentado ante el equipo de espaldas a un cristal que lo separaba del pasillo. Los investigadores lo observaron por espacio de una hora aproximadamente mientras continuaba enviando numerosos mensajes de correo electrónico a Vaughan. Se logró confirmar que dichos mensajes salieron de la computadora que estaba bajo observación.

Palmer fue arrestado justo cuando estaba enviando uno de los mensajes y la computadora que estaba utilizando fue incautada como evidencia. Desafortunadamente para Palmer le quedaba aún mucha mala suerte por llegar. Otro elemento en su contra fue su meticulosidad en el uso del corrector ortográfico del servicio de correo electrónico. El servicio de correo electrónico que utilizó Palmer guarda fotos instantáneas de la visualización en pantalla de las correcciones ortográficas en archivos temporales de Internet. Para rematar su mala suerte, cuando fue arrestado Palmer llevaba consigo copias impresas de muchos de los mensajes de correo electrónico que había enviado.

Pasos de una investigación

Los investigadores deben seguir los mismos pasos en todas las investigaciones. Esto los ayudará a evitar la posibilidad de obviar pasos importantes. Estos pasos deben documentarse en un manual de procedimientos que puede ser parte de las políticas y procedimientos del organismo. Los siguientes son algunos pasos que sugerimos:

1. Analizar la queja
2. Recopilar evidencias físicas
3. Procurar la asesoría de expertos, si fuese necesario
4. Entrevistar a testigos e interrogar a sospechosos
5. Preparar el expediente del caso
6. Analizar el caso
7. Dar seguimiento a las investigaciones
8. Decidir si se debe emprender el procesamiento judicial

Analizar la queja

Una vez recibida la queja o la notificación de que ha tenido lugar un delito informático, el investigador debe analizarla primero a fin de determinar:

- si se ha cometido un delito
- de ser así, qué delito se ha cometido

El análisis incluye la evaluación de la plausibilidad de las acusaciones de que ha ocurrido una violación de la ley, teniendo en cuenta la naturaleza y gravedad del delito, así como otros factores que pudieran complicar el procesamiento del caso. En un mundo ideal, todas las quejas serían investigadas exhaustivamente y se procesarían todos los hechos delictivos. En nuestro mundo no ideal, las limitaciones de personal y otras consideraciones pudieran impedir que se aborden casos menos graves. Si el análisis de la queja llega a determinar que se ha cometido un delito y justifica una investigación preliminar, el próximo paso es comenzar a recopilar evidencias.

Recopilación de evidencias físicas

En este contexto, evidencia física es todo lo tangible que se pueda recopilar, marcar o etiquetear, y guardar en un lugar seguro hasta la fecha del juicio. Si bien la evidencia pudiera ser digital en un caso de delito informático, el disco que la contiene es algo tangible. Pudiera existir otro tipo de evidencia física además de la información digital, como huellas dactilares, documentos, etc. Todas se deben preservar según las prácticas normales referidas a la escena del delito.

Las técnicas tradicionales utilizadas en la investigación de la escena de un delito, como realizar bocetos del lugar, tomar fotos y películas de videos, pueden ser útiles. Ello es especialmente aplicable cuando los investigadores ocupan la computadora y en la pantalla de esta hay información que no ha sido grabada en el disco. Pudiera existir información en la memoria, además de información sobre el estado del sistema (conexiones de red abiertas, aplicaciones y procesos en ejecución, entre otras) que son de utilidad como evidencia pero que se perderían al apagar la computadora. Salvar los contenidos de la memoria u otra información o pasar el contenido de la memoria a un archivo modifica el sistema, de manera que estaríamos alterándolo y ya no podríamos testificar que está de la misma manera que como lo encontramos. Una manera de evitar este problema es recurrir a la fotografía para dejar constancia gráfica de la información

que se visualiza en la pantalla. Otro método es transferir los datos a otra computadora. Debemos recordar que siempre que realizamos una tarea en una computadora, incluso algo tan sencillo como salvar un archivo, la estamos cambiando de alguna manera. Véase el capítulo 10 sobre la recopilación y preservación de la evidencia digital para una mayor información sobre la forma de manejar la evidencia digital, a fin de no modificarla y para conocer qué debe hacerse cuando se han hecho ya cambios (por ejemplo, si el personal informático tomó medidas preliminares antes de que se involucraran en el caso los investigadores policiales).

NOTA

Los bocetos, fotografías y cintas de videos de la escena del delito cumplen funciones diferentes como material de documentación; ninguna sustituye a la otra. El boceto nos da una perspectiva, mientras que el video nos brinda una visión general del lugar. Las fotos fijas se utilizan para documentar los artículos específicos o una información concreta. Ninguno de ellos es admisible como evidencia a menos que esté acompañado del testimonio de un testigo (por lo general el artista que realizó el boceto, el fotógrafo que tomó las fotos, o el camarógrafo que tomó el video), que declare bajo juramento respecto de las circunstancias en que se realizaron y en el sentido de que son una representación del lugar de la manera en que recuerdan haberlo visto.

Procurar la asesoría de expertos

Cuando un delito involucra detalles técnicos que exceden el conocimiento del investigador y/o el fiscal, a menudo es necesario procurar la asesoría y ayuda de un experto en la materia, de la misma manera que se trataría de utilizar los servicios de un intérprete si los testigos de un delito hablaran un idioma que no conociéramos. Lo ideal sería tener policías con conocimientos técnicos. Como no siempre puede hacerse, los investigadores tendrán que procurarse la ayuda de terceros.

Cuando investigamos un delito informático que afecta la red de una empresa ¿por qué no utilizar como expertos al personal informático de dicha empresa? Aunque ello significaría un ahorro de tiempo y esfuerzo para el organismo, no es una idea feliz. Los expertos que consultemos deben ser objetivos, y a menudo es difícil obtener opiniones objetivas de personas cuya red ha sido atacada. Incluso en el caso en que los profesionales informáticos de la empresa puedan ser totalmente objetivos, cabría la posibilidad de que se pensara que no lo son, y ello podría ser explotado por los abogados de la defensa si llegan a descubrir que fueron ellos la fuente de la asesoría técnica. Es posible obtener la colaboración de expertos en informática de la comunidad con disposición para contribuir a una buena causa. Un lugar donde podría obtenerse esta ayuda es en el mundo académico; los instructores de computación y de seguridad informática en los institutos y centros educacionales locales a menudo están dispuestos a ayudar con cuestiones técnicas en los casos de delito informático. Las asociaciones de profesionales de computación también podrían ser una fuente de asesoría.

Entrevista e interrogatorio

Entrevistar a testigos e interrogar a sospechosos puede ser un proceso que se prolonga durante toda la investigación. A medida que se obtienen nuevas informaciones, es

posible que se hallen nuevos testigos y nuevos sospechosos. Quizás sea necesario realizar entrevistas adicionales a los testigos que ya han sido entrevistados con anterioridad.

Los investigadores deben cerciorarse de que poseen todos los datos que les permitan contactar a todos los testigos, incluso aquellos a quienes pudiera no ser necesario entrevistar por el momento. Esta información debe incluir la dirección y los números de teléfono del centro laboral, así como la dirección y el número telefónico de su residencia. No es inusual que los testigos cambien de trabajo o de residencia mientras dura la investigación, lo cual dificultaría su localización si contamos solamente con información de uno de esos dos lugares. También es buena idea, en el mundo actual de tanta movilidad e interconexión, tener las direcciones de correo electrónico de los testigos. Muchas personas mantienen la misma dirección de correo electrónico aunque cambien de residencia o de empleo, de manera que esta sería la única información de contacto que permanecería invariable.

Preparación del caso

Una vez recopilada y documentada la evidencia física, y de realizadas las entrevistas y los interrogatorios, el próximo paso es comenzar a preparar el expediente físico del caso. Según el diccionario legal *Black's Law Dictionary*, un *caso* es "una recopilación de hechos que prepara el camino para el ejercicio de la jurisdicción de un tribunal". *Preparación*, según el Diccionario Webster, es "la acción o el proceso de dejar algo a punto". De estas definiciones podemos extrapolar que una definición sencilla de *preparación del caso* es "una compilación de información puesta a punto para ser presentada ante un tribunal".

El expediente del caso contendrá toda la información sobre él, incluido (aunque no de manera exclusiva) lo siguiente:

- Informe inicial confeccionado por los oficiales o el investigador que respondió a la queja
- Informes de seguimiento
- Documentación de la recopilación de evidencia por parte de los técnicos en la escena del delito
- Informes de laboratorio preparados por el personal forense
- Declaraciones por escrito de testigos, sospechosos y expertos
- Bocetos, fotografías y cintas de videos de la escena del delito
- Copias impresas de evidencia digital, cuando proceda

El expediente del caso se utiliza para organizar la información y la evidencia en un mismo lugar y será empleado por la fiscalía para determinar si el caso se lleva o no a tribunales. De manera que el expediente del caso debe necesariamente contener documentación probatoria de los elementos del delito, la legalidad de la entrada/búsqueda/incautación/arresto, y la preservación de la cadena de custodia.

Análisis del caso

Cuando ya se tiene preparado el expediente del caso con toda la documentación necesaria, el próximo paso es analizar el significado jurídico de la información y la evidencia que contiene. Por lo general este paso debe involucrar a la fiscalía, que debería poder brindar al investigador una guía en cuanto a las debilidades que presenta el caso, y sobre cuál información o evidencia adicional se necesita para fortalecerlo. Esta podría

ser la primera de varias *conferencias previas al juicio* entre los miembros del equipo de la fiscalía y los investigadores.

Seguimiento

Después del análisis del caso, quizás sea necesario obtener evidencia adicional o esclarecer algunos hechos y datos. Una nueva entrevista con los testigos en este punto podría cumplir varios objetivos. Además de obtener información adicional específica, una segunda entrevista contribuiría a refrescar la memoria de los testigos respecto del caso, también la memoria del investigador, y preparar a los testigos para el proceso en el tribunal si es el caso llega a un juicio.

Decisión de emprender proceso

Luego de haberse recopilado toda la información adicional y una vez que se haya determinado que el expediente del caso está completo, el fiscal tomará la decisión de emprender proceso (o referir el caso a un gran jurado, en dependencia de la jurisdicción y sus procedimientos). En este momento, también se decide el cargo que se ha de imputar. En algunos casos es posible presentar cargos por varios delitos. El fiscal lo determinará sobre la base de la probabilidad de los elementos y la dificultad para obtener una condena, así como la severidad del castigo. Por ejemplo, las acciones de un sospechoso podrían contener los elementos de dos delitos diferentes -como el acceso no autorizado y el robo de secretos comerciales. Si el último cargo constituye un delito grave y el primero un delito leve, la fiscalía podría decidir presentar cargos solamente respecto del delito más grave. En otros casos, se presentarían ambos cargos. Por lo general, si un delito es una *infracción menor incluida* en otra, el jurado podría determinar si el acusado es culpable del delito menor aunque se hubieran presentado cargos solamente por el delito más grave.

Definición de las esferas de responsabilidad

En raras ocasiones una sola persona está encargada de una investigación compleja. El equipo investigativo deberá estar integrado por uno o más detectives, expertos en la escena del delito, fotógrafos y camarógrafos de videos, registradores y custodios de la evidencia, así como especialistas como miembros del equipo de computación forense.

Es importante que haya una persona designada como responsable de la investigación. Esta será el jefe del equipo y generalmente es un investigador de alto nivel. El jefe del equipo debe asignar a cada miembro de este una *esfera de responsabilidad* específica. Los miembros del equipo deberán responder por la esfera de responsabilidad a su cargo (por ejemplo, recopilar, etiquetear, documentar y asegurar la evidencia física) y no debe excederse en sus facultades ni realizar actividades que competan a otros miembros del equipo, a menos que cuenten con la aprobación del jefe del mismo.

Testimonio en un caso de delito informático

Todo el proceso de investigación y preparación del expediente del caso tiene como objetivo lograr la condena del delincuente informático en un tribunal de justicia. No importa cuán buena sea la evidencia que logramos obtener --archivos de registro que muestren el acceso no autorizado a la red, discos duros retirados de la computadora del sospechoso contentivo de indicios inequívocos de actividad delictiva, registros de red que vinculan al intruso siguiendo el rastro mediante la conexión a servidores Internet-- ninguna pueden mantenerse por sí sola.

En la mayoría de los sistemas judiciales, la evidencia física y la evidencia intangible deben estar respaldadas por testimonios. Es preciso que alguien atestigüe respecto del momento, el lugar y la forma en que se obtuvo la evidencia y de fe de que es la misma y está en el mismo estado en el momento en que es presentada ante el tribunal. Cuando la evidencia es de carácter técnico y resulta difícil su comprensión para las personas legas, podría ser necesario el testimonio de expertos que expliquen la naturaleza de la evidencia y su significado para que esta sea comprendida por el jurado y el jueves. Quizás los investigadores policiales y el personal de las TI tengan que testificar en un caso de delito informático. En las secciones siguientes analizamos el proceso de juicio penal, los dos tipos de testigos que pueden ser llamados a testificar en las acciones penales, así como algunas ideas sobre la forma de preparar y brindar testimonio como testigo de prueba o experto.

El juicio

El proceso del juicio realmente comienza cuando se arresta a un sospechoso o se emite una orden judicial para arrestar a un sospechoso. Una vez realizado el arresto, el acusado es llevado ante un magistrado (un juez o, en algunos casos, el alcalde de la ciudad) en un período de tiempo específico -- por lo general 48 horas-- para ser instruido de cargos. Esta instrucción de cargos es un proceso oficioso mediante el cual el magistrado informa al acusado los cargos que han sido presentados en su contra, le lee sus derechos y establece o deniega fianza.

Generalmente se celebra una audiencia preliminar en el curso de unos pocos días. En esta audiencia la fiscalía debe presentar evidencias suficientes para convencer al juez de que el acusado debe ser llevado a juicio. Este proceso es secreto y en él un gran jurado decide si finalmente se presentará una acusación. Posteriormente puede realizarse una instrucción de cargos oficial, en la que el acusado puede hacer su declaración respecto de los cargos en su contra.

Antes del juicio propiamente dicho, usualmente se celebra una conferencia o audiencia previa en la que se pueden presentar mociones (por ejemplo, solicitando un cambio de sede). Por último, el caso es llevado a juicio. Si el acusado se declara no culpable de los cargos, se selecciona un jurado mediante el proceso *voir dire*, durante el cual ambas partes realiza preguntas a los posibles miembros del jurado y los acepta o rechaza. El juez instruye al jurado sobre la ley aplicable y posteriormente los abogados realizan su declaración introductoria.

Debido a que la carga de la prueba descansa en la fiscalía, el fiscal es el primero en dirigirse a la sala. Después de la declaración introductoria de la defensa, la fiscalía procede a llamar a los testigos. La fiscalía interroga a cada uno de los testigos. Después la defensa tiene la posibilidad de interrogar a los testigos presentados por la fiscalía. Ambas partes tienen una segunda oportunidad para realiza preguntas a los testigos.

Una vez que la fiscalía ha concluido la presentación de sus testigos y su evidencia, los abogados de la defensa por lo general presentan una moción de desestimación del caso por falta de pruebas. Si la moción es aceptada, el juicio concluye y el acusado queda en libertad. De lo contrario, la defensa presenta sus testigos. El proceso de interrogatorio de estos testigos es similar a lo que sucede con los testigos de cargo, en el que ambas partes pueden interrogarlos en dos oportunidades. Después de que la defensa haya presentado su caso, la fiscalía puede llamar a comparecer a testigos de impugnación, los cuales pueden a su vez ser impugnados por la defensa.

Por último, cuando ha concluido todo este proceso, los abogados de ambas partes hacen sus declaraciones finales (el tribunal decide el orden en que lo harán) y el juez da nuevas instrucciones a los miembros del jurado, los cuales se marchan para llegar a un veredicto.

El investigador o el profesional de las TI que testifique como poseedor de conocimiento personal respecto de la evidencia en el caso (testigo de prueba) lo harán como testigo de cargo, por lo que es interrogado primero por la fiscalía y después por la defensa. Los testigos periciales pueden testificar a favor de cualquiera de las dos partes.

Testimonio como testigo de prueba

Un testigo de prueba es aquel que posee conocimiento directo del caso. Por ejemplo, un administrador de red podría ser llamado a testificar sobre lo que observó durante un ataque en la red, o un investigador puede ser llamado a testificar respecto de la evidencia que observó en una computadora que fue incautada sobre la base de una orden judicial de cateo. Un testigo de prueba también puede testificar respecto de los hechos (lo que vio o escuchó) pero no puede dar opiniones ni llegar a conclusiones.

Testimonio como testigo pericial

Un testigo pericial no tiene participación directa en el caso pero si posee conocimientos técnicos especiales que lo califican para dar opiniones profesionales sobre cuestiones técnicas. A veces los testigos periciales preparan informes en los que presentan sus opiniones y las fundamentan. En algunos países, los testigos periciales deben estar registrados como peritos en una esfera específica. En los Estados Unidos, los peritos deben probar sus conocimientos presentando sus credenciales ante el tribunal.

Requisitos para ser perito

Usualmente al testigo pericial se le hacen varias preguntas por parte del abogado que le ha pedido testificar. Estas preguntas están destinadas a demostrar su capacidad como perito. Entre ellas podrían estar:

- ¿Cuál es su calificación?
- ¿Qué cargos ha tenido en esta esfera?
- ¿Ha impartido cursos en esta esfera?
- ¿Qué libros o artículos ha escrito que guarden relación con esta esfera?
- ¿Cuál es su experiencia como testigo pericial en esta esfera?

El abogado de la otra parte podría cuestionar las credenciales del testigo pericial en un intento por que se desestime su declaración.

Uso de peritos

En muchos casos, a los testigos periciales se les paga por su testimonio. El pago por lo general se realiza como un *per diem* y pudiera incluir gastos de viaje y de alojamiento durante el juicio. Muchas personas suelen contratarse como testigos periciales, especializados en diferentes esferas técnicas y científicas, incluida la computación forense. Muchos de estos testigos periciales anuncian sus servicios en Internet. Por ejemplo, Expert Pages (http://expertpages.com/experts/computers.htm) es una base de datos con un listado de testigos periciales en muchas esferas y ubicados en todos los Estados Unidos.

Comparecencia como testigo

La primera regla para brindar testimonio directo (o cualquier testimonio bajo juramento) es decir siempre la verdad. Los testigos no deben sentir miedo por tener que decir "No

sé" o "No recuerdo" cuando eso es verdad. Más allá de ello, hay un número de mejores prácticas que se deben seguir para testificar ante un tribunal.

Si usted es un oficial encargado de la aplicación de la ley o un perito técnico que debe testificar ante un tribunal, recuerde que el jurado evaluará la credibilidad de todos los testigos y decidirá si cree o no el testimonio, sobre la base de esa evaluación. Los siguientes son algunos consejos para elevar nuestra credibilidad como testigos:

- Llegar al tribunal en tiempo o con ligera antelación. Esto le proporcionará tiempo para prepararse y familiarizarse con el lugar, el camino que deberá recorrer hasta el estrado, etc. Si llega tarde causará una mala impresión en el jurado y afectará su credibilidad.
- No aparente nerviosismo. El jurado espera que las personas se pongan nerviosos cuando mienten. Quizás no pueda usted controlar su estado anímico en ese momento, pero con práctica podrá controlar cualquier manifestación visible de nerviosismo, como gestos repetitivos.
- Mantenga la calma y no se enoje. El abogado de la otra parte quizás trate de hacerle perder la paciencia; si lo logra, su credibilidad quedará en entredicho ante el jurado. Los testigos nunca deben discutir ni ser sarcásticos al responder las preguntas de los abogados. Mantener la calma y la compostura profesional fortalecerá su posición.
- No brinde información adicional voluntariamente. Responda las preguntas que se le formulen pero no brinde información adicional ni se aparte del asunto. No presente evidencias de oídas (lo que escuchó decir a otras personas) porque generalmente son inadmisibles.
- Lleve ropas de apariencia profesional. La apariencia importa, y nuestra credibilidad se verá beneficiada si vestimos un atuendo conservador y de apariencia profesional.
- Analice cuidadosamente las preguntas antes de responder. Cerciórese de haber comprendido la pregunta, y si no es así pida al abogado que la repita. No comience a responder hasta tanto tenga la seguridad de que el abogado ha terminado la pregunta.
- Hable de manera clara y segura. Un testigo eficaz no grita sino que habla suficientemente alto para ser escuchado por el juez, el jurado y los abogados.

El testimonio de un testigo de prueba debe limitarse solamente a los hechos. No dé opiniones ni especule; de una manera imparcial y objetiva limítese a decir lo que hizo o lo que vio.

Tácticas de contrainterrogatorio

La función del abogado que realiza el contrainterrogatorio es desacreditar al testigo de la otra parte. Los abogados podrían utilizar técnicas psicológicas para intentar desacreditar a los testigos. Cuando testificamos en un caso de delito informático, debemos garantizar no caer en esas trampas. Tenemos que estar preparados para evadir tácticas como las siguientes:

- Preguntas excesivamente rápidas que no nos dan tiempo para responder entre una y otra
- Preguntas capciosas ("¿No es verdad que lo que usted vio fue...?")

- Repetir lo que usted ha dicho pero haciendo cambios que modifican el significado
- Aparentar ser amistoso para después, sorpresivamente, atacarnos
- Fingir desconcierto, ira o consternación ante lo que usted ha dicho
- Silencio prolongado con el objetivo de provocar una situación de malestar con la esperanza de que usted diga algo más

Lo más importante que debemos recordar cuando somos sometidos a tácticas como esas es que el abogado no usa estas tácticas contra nosotros por un problema personal, sino que simplemente está haciendo su trabajo. Nuestro consejo para el testigo es que él también debe hacer su trabajo: mantener la calma y referirse a los hechos.

Uso de notas y ayudas visuales

¿Y si tenemos que testificar ante un tribunal pero nuestra memoria es mala? ¿Y si tenemos temor de olvidar hechos importantes, especialmente información difícil de recordar, como es el caso de las cifras? ¿Es lícito que los testigos lleven consigo notas y las utilicen como referencia cuando brindan testimonio?

Los policías utilizan notas como ayuda para la memoria durante sus testimonios ante un tribunal. Ésta práctica tiene ventajas y desventajas. Algunos jurados podrían impresionarse por el hecho de que estemos leyendo notas, porque pudieran confiar más en la palabra escrita que en alguien que depende solamente de su memoria. Por otra parte, otros podrían pensar que usted está siendo dirigido o manipulado si recurre a notas; considerarían que si usted estuviera diciendo la verdad podría recordarla sin necesidad de tener que recurrir a la ayuda de anotaciones. Una consideración muy importante para definir si utilizamos o no anotaciones es el hecho de que si el testigo las utiliza, éstas serán presentadas como evidencia y quedarán bajo la custodia del tribunal mientras dure el juicio. Si finalmente usted decide utilizar anotaciones, debe entonces estar seguro de que el papel en que las escribió no tiene otras anotaciones sobre cuestiones no relacionadas con el caso, porque el abogado de la otra parte podría preguntarle acerca de todo lo que este escrito en ese papel.

Resumen
La preparación de un caso de delito informático es un proceso complicado, mucho más que los casos de cualquier otro tipo de delito. Ello se debe a que es preciso tener en cuenta factores especiales que representan obstáculos al procesamiento y que deben ser resueltos para que el investigador pueda preparar satisfactoriamente un caso con probabilidades de éxito en un tribunal. Debido a que muchos de los delitos que clasifican como delitos informáticos son relativamente nuevos, los elementos no siempre están claramente definidos, y a menudo no ha habido tiempo para esclarecer e interpretar los estatutos mediante el proceso de jurisprudencia. Es importante que los investigadores de delito informático se mantengan actualizados sobre los casos legales pertinentes que pudieran afectar la aplicabilidad de las leyes locales, estaduales y federales que se relacionan con el delito informático.

Comprender el sistema complejo de leyes que rigen nuestras vidas y la forma en que interactúan entre si es esencial para preparar un caso penal. Los investigadores y los que trabajan con ellos deben estar conscientes de la función de los diferentes cuerpos de ley, comprender las diferencias entre los diferentes tipos de derecho, estar conscientes de la existencia de diferentes niveles de ley, y aprender la terminología jurídica necesaria para comunicarse de manera inteligente dentro del sistema.

Las cuestiones jurisdiccionales son uno de los mayores retos para el investigador de delito informático y para los fiscales que tratan de hacer justicia en estos casos. Es importante que conozcamos el significado de la autoridad jurisdiccional y los temas prácticos que afectan los casos multijurisdiccionales. La naturaleza intangible de gran parte de la evidencia en un caso de delito informático constituye un obstáculo adicional.

La policía y el personal informático deben trabajar de conjunto como un equipo para procesar con eficacia los casos de delito informático, porque cada uno de ellos desempeña un papel esencial en la preparación del caso. Los profesionales de la informática comprenden la manera de pensar de los hackers, saben dónde buscar la evidencia digital y comprenden lo que puede y no hacerse con la tecnología. Los policías conocen la ley y los procedimientos investigativos que se deben aplicar para preservar la integridad de la evidencia. Juntos pueden combatir de manera eficaz el delito informático, pero deberán vencer la desconfianza natural y la relación de adversidad que a veces entorpece el proceso de cooperación entre ambos.

El proceso investigativo es básicamente el mismo en un caso de delito informático que en cualquier otro caso penal, pero los investigadores deben estar conscientes de la importancia de definir los papeles que cada miembro del equipo investigativo ha de tener, así como garantizar que cada miembro del equipo tenga una responsabilidad específica. Un buen expediente de caso es el resultado de un trabajo arduo por parte de muchas personas, pero su objetivo final es llevar el caso ante un tribunal y ganarlo. Con ese fin, tanto los investigadores policiales como el personal de la esfera informática con conocimiento directo del delito podrían ser llamados a comparecer como testigos de prueba en el juicio. Los profesionales de la informática también pudieran estar calificados para testificar como testigos periciales, a quienes les está permitido analizar la evidencia, dar opiniones y llegar a conclusiones, y/o explicar los aspectos técnicos del caso para beneficio del tribunal y del jurado.

PREGUNTAS FRECUENTES

Las siguientes preguntas frecuentes, respondidas por los autores de este libro, están destinadas a medir su comprensión de los conceptos presentados en este capítulo y a ayudarlo en la aplicación práctica de estos conceptos. Para que el autor pueda responder sus preguntas sobre este capítulo, sírvase visitar el sitio www.syngress.com/solutions y pinchar en "Ask the Author".

P: ¿Se debe ver el ciberespacio como un lugar distinto a los bienes de los temas jurisdiccionales?
R: Algunos expertos en temas jurídicos consideran que el enfoque más lógico es ese. David R. Johnson y David G. Post, en un artículo publicado en 1996 en *Stanford Law Review*, afirmaron que las fronteras geográficas no son pertinentes al analizar los temas jurídicos en el mundo interconectado y que tratar la Internet como un simple "medio de transmisión" confunde el asunto y tiene resultados a la larga insatisfactorios. Proponen que cuando emprendamos una actividad en línea, debemos considerar que estamos en un lugar o jurisdicción distinta con leyes propias, como cualquier jurisdicción geográfica. Afirman que el ciberespacio tiene fronteras definidas en el sentido de que estamos en línea o no lo estamos en un determinado momento, por lo que no hay ambigüedad sobre el momento en que nuestras acciones caerían en esa jurisdicción. Además, afirmaron que tratar el proceso de la entrada en línea como un cruce de fronteras simplificaría grandemente la capacidad para establecer y aplicar leyes que regulen el comportamiento en el "espacio" en línea. Para una explicación completa sobre sus ideas, véase el artículo *Law and Borders: The Rise of Laws in Cyberspace* en el sitio web del Instituto de Leyes del Ciberespacio en www.cli.org/X0025_LBFIN.html#II.%20%20A%20New%20Boundary%20for%20Cyberspace

P: Al parecer existen miles de testigos periciales de computación forense anunciados en Internet. ¿Cómo puede un investigador decidir cuál utilizar?
R: Muchas empresas e individuos brindan este servicio. Algunos son altamente calificados, mientras que otros tienen poca experiencia y conocimientos. En los Estados Unidos no existe regulación respecto de esferas como la computación forense. Los "peritos" no tienen necesariamente que cumplir determinados niveles educacionales o de experiencia, y no existen certificaciones típicas ni programas de entrenamiento. Básicamente, cualquiera puede poner un anuncio y autocalificarse de perito en computación forense. Para seleccionar a uno de entre los muchos que se autoproclaman peritos tendrá usted que utilizar sus propias técnicas investigativas. Trate de conocer los antecedentes del perito: si tiene un título en ciencias de computación y/o estudios forenses; cuál es su experiencia laboral real además de su experiencia académica; en cuántos juicios ha testificado como perito y cuál ha sido el resultado de esos juicios. En otras palabras, haga las mismas preguntas que haría el tribunal para determinar si esa persona está calificada para testificar como testigo de prueba. Pida referencias (de

clientes anteriores) y verifíquelas. Garantice seleccionar a alguien con experiencia en la presentación de testimonios en cuestiones penales, porque las reglas de procedimiento y otros aspectos del testimonio en juicios civiles son diferentes.

Recursos

- Criminal Justice Resource Center (Centro de recursos de justicia penal)
  www.wadsworth.com/criminaljustice_d
- Cornell Law School: *Criminal Law: An Overview*
  www.lawcornell.edu/topics/criminal.html
- *How Our Laws Are Made*, revisado y actualizado por Charles W. Johnson
  http://thomas.loc.gov/home/lawsmade.toc.html
- Reglamento federal de procedimiento penal (Federal Rules of Criminal Procedure)
  www.law.ukans.edu/research/frcrimI.htm
- Original Intent: *The Law*
  www.originalintent.org/thelaw.shtml
- ZDNet, junio 26 de 2002: *How the Secret Service Became Cybercops*
  http://zdnet.com.com/2100-1107-939425.html
- OAS: *Cybercrime and* Jurisdiction, por Jack Goldsmith
  www.oas.org/juridico/english/cybercrime_and_jusrisdiction.htm
- Nedbank ISS Criime Index: *Intangible Evidence? Policing in the Information Age*
  www.iss.co.za/PUBS/CRIMEINDEX/01VOL5NO4/Intangible.html
- Capsule Summary: *Criminal Procedure*
  http://lawschool.lexis.com/emanuel/web/crimpro/tocfull.htm
- The Expert Pages
  http://expertpages.com/experts/computers.htm

Apéndice

La lucha contra el delito informático a escala mundial

Temas que se analizan en este capítulo:

- Cómo están actualizando los países sus legislaciones sobre delito informático
- Comparación de leyes internacionales sobre delito informático
- Investigación de un delito informático internacional

- Resumen
- Recursos

Introducción

El delito informático es una plaga mundial contra la cual lucha la policía en todo el mundo. A consecuencia de él los países han sufrido daños estimados en miles de millones de dólares y se han visto obligados a actualizar su estructura jurídica para hacer frente a este nuevo tipo de delito. El delito informático ha provocado la creación de nuevos cargos dentro de los organismos encargados de la aplicación de la ley, nuevas unidades en los departamentos policiales y nuevas especialidades legales.

En las formas tradicionales de delito, por lo general una persona viola la ley dentro de una sola jurisdicción. El delito informático se diferencia de otros delitos porque un mismo delito puede abarcar múltiples jurisdicciones, incluso llegar a la jurisdicción internacional. Esta amplitud de ámbito ha creado problemas jurídicos y logísticos que deben abordarse, obligado a que los organismos de aplicación de la ley en todo el mundo cooperen entre sí, y evidenciado la necesidad de que los gobiernos trabajen de consuno. Lamentablemente, si bien la necesidad es real, muchos gobiernos no han cumplido con el objetivo de enfrentar eficazmente el delito informático.

En este apéndice analizamos los temas especiales que tienen que ver con las investigaciones internacionales y los problemas relacionados con esto. Veremos las diferencias entre las leyes de los diferentes países, los esfuerzos de cooperación entre los países que luchan contra el delito informático, y como los obstáculos jurisdiccionales y de otra índole pueden impedir el procesamiento de casos de delito informático.

Este apéndice también ofrece información de direcciones de sitios web donde pueden encontrarse materiales de referencia. Estos sitios ofrecen información sobre las leyes que rigen en otros países, sitios web de los organismos de aplicación de la ley y materiales de referencia útiles en la investigación de delitos relacionados con la computación a nivel internacional.

Cómo están las naciones actualizando su legislación sobre delito informático

Debido a que los delitos informáticos se cometen en todo el mundo, muchas personas en los Estados Unidos piensan que en todo el mundo hay leyes similares a las de su país. Nada más lejos de la verdad. Muchos países dependen de leyes ya existentes para hacer frente al delito informático y quizás las actualicen sólo después de que haya quedado evidenciado que no se podrán aplicar a los casos de delito informático (de la misma manera que las leyes de algunos estados de la Unión no fueron actualizadas –e incluso aún no lo están– hasta tanto fue evidente la necesidad de hacerlo). Tener leyes ineficaces es tan malo como no tener ley alguna, y cuando los elementos jurídicos de un delito no se avienen totalmente al delito real, la ley es ineficaz, por lo menos a los efectos de procesar ese delito.

Algunos países no cuentan con ninguna ley que se aplique a los delitos asociados normalmente con las computadoras e Internet, lo cual hace que sea "por defecto" lícito realizar acciones que merecerían el arresto de esa persona en los Estados Unidos. Sin embargo, la actitud internacional hacia el delito informático está cambiando, y en todo el mundo están apareciendo nuevas leyes. Mantenerse a la par de estos cambios representa un desafío para quienes deben trabajar con las leyes de jurisdicciones diferentes.

Al comparar las leyes de los países la conclusión más común es que muchos países no han logrado hacer frente al problema del delito informático porque carecen de

la legislación que lo aborde específicamente, mientras que otros han sido más agresivos que los Estados Unidos en este sentido. Como hemos apreciado a lo largo de este libro, muchos delitos relacionados con la informática son variaciones de viejos delitos. Por ejemplo, un país puede tener leyes escritas sobre pornografía infantil y no distinguir entre los materiales ilícitos que se distribuyen en papel o los de formato digital. El hecho de que el delito se está cometiendo ahora en Internet es simplemente una nueva forma de hacer algo que ya es ilícito. En estos casos, los estatutos existentes podrían aplicarse a alguien que comete el delito, independientemente de que haya utilizado o no una computadora.

Por otra parte, quizás no se apliquen. Si la legislación es demasiado vaga, podría interpretarse de una manera que descalifique cualquier variación en el ciberespacio. Un ejemplo de ello es el virus del Amor que atacó los sistemas en todo el mundo y provocó pérdidas monetarias ascendentes a varios miles de millones de dólares. La investigación determinó que el autor del virus estaba localizado en Filipinas, y un sospechoso de nombre Onel de Guzmán fue arrestado a tenor de la Ley de Dispositivos de acceso de Filipinas de 1994, conocida como Ley 8484 de la República. Esta ley, aplicada tradicionalmente a casos referidos al robo de tarjetas de crédito, abordaba el uso ilícito de números y contraseñas de cuentas. Desafortunadamente, después de determinar que la ley no era aplicable a este caso y que no se refería a la diseminación del virus o al caos que esto creaba, los cargos fueron retirados. Incluso en el caso en que la ley hubiera podido ser utilizada para procesar este delito, la misma impone una sentencia de seis meses a seis años de prisión solamente. El mismo delito, si es cometido en los Estados Unidos, podría ser procesado según las leyes que prevén una sentencia de hasta 20 años de cárcel.

Debido a que las leyes vigentes en aquel momento no eran adecuadas para procesar al autor del virus del Amor (y otros delincuentes informáticos), el gobierno de Filipinas se vio en la necesidad de crear nuevas leyes para enfrentar de manera efectiva el delito informático. La elaboración de leyes que aborden el delito informático y el delito en Internet es a menudo un enfoque de reacción similar a la legislación inadecuada. De hecho, pocos países han tomado medidas proactivas contra el delito informático. Incluso en los casos en que las leyes existentes se modifiquen para contrarrestar el delito informático, a menudo no llegan a abarcar todos los delitos posibles. Por ejemplo, si bien la República Checa ha actualizado sus leyes para hacer frente a temas como el acceso no autorizado y la modificación de datos, no hay leyes que se refiera a la diseminación de virus. En otras palabras, el mismo problema que experimentaron los filipinos se está repitiendo en otras partes del mundo.

Hasta tanto todos los países del mundo actualicen las leyes obsoletas y creen nuevas leyes que enfrenten directamente el delito informático, continuará el problema de nuestra incapacidad para procesar eficazmente a los culpables de estos delitos. Según una encuesta realizada por McConnell International en diciembre de 2000 (www.mcconnellinternational.com/services/CyberCrime.htm) mostró que asombrosamente existen pocas leyes en la actualidad que protejan a los ciudadanos del mundo contra el delito informático. De los 52 países encuestados, nueve tenían leyes referidas a cinco o menos tipos de delito informático, 10 tenían leyes referidas a

entre 6 y 10 tipos de delito informático, y 33 no habían actualizado sus leyes para enfrentar el delito informático. Si los delincuentes informáticos cometen sus fechorías en estos países, sus gobiernos tendrían una capacidad limitada para procesarlos legalmente.

Aprovechando los beneficios de la influencia internacional

A medida que los países cooperan entre sí en diferentes esfuerzos se ha ido creando una visión mundial sobre lo que se considera correcto e incorrecto en determinadas esferas. Debido a que numerosos países no cuentan con las leyes ni con la legislación adecuada para abordar la pornografía infantil, el terrorismo informático y otras actividades relacionadas con el delito informático, los consorcios internacionales consideraron necesario establecer un marco legal para la actualización de las leyes de esos países. Las organizaciones internacionales y las coaliciones políticas han influenciado los cambios jurídicos en muchos países, presionando a algunos de ellos a crear nuevas leyes o a revisar las ya existentes para hacer frente a los delitos que la mayoría del mundo considera aborrecible o potencialmente devastadores.

Con la intervención de las Naciones Unidas y la Organización Internacional del Trabajo (OIT), muchos países que anteriormente no tenían leyes sobre pornografía infantil han modificado su legislación o creadas nuevas leyes que penalizan este delito. Al hacerlo han penalizado la distribución o la obtención de pornografía mediante fuentes como Internet, y permitido que los órganos de aplicación de la ley cierren sitios web de pedofilia, arresten a los propietarios de estos sitios y a los usuarios de Internet que buscan este tipo de imágenes y películas. Por ejemplo, en el verano de 2002, EUROPOL (el organismo policial de la Unión Europea,) reportó que la policía europea llevó a cabo redadas contra la pornografía infantil en el marco de la Operación Twins en siete países, ocupando equipos y arrestando a sospechosos en Bélgica, Gran Bretaña, Alemania, Italia, Países Bajos, España y Suecia. En la operación participaron 12 países, incluidos los Estados Unidos y Canadá.

La Convención de las Naciones Unidas sobre los Derechos del Niño, que incluye un Protocolo Opcional sobre la prostitución y la pornografía infantiles, ha sido ratificada por unos 200 países, y más de 100 de ellos han firmado el Protocolo. (Para más información, véase www.unicef.org/crc/crc,htm.). La OIT ha estado combatiendo la pornografía infantil desde los años del decenio de 1930 y en la Conferencia Internacional del Trabajo celebrada en 1997 aumentó sus presiones sobre los países miembros para que aprobaran leyes severas contra la pornografía infantil "cualesquiera sean los métodos técnicos utilizados", garantizando así que las actividades que utilizan la Internet (o cualquier tecnología futura) pudiera estar incluida. En 1999, el Parlamento Europeo y el Consejo de la Unión Europea aprobaron un plan de acción multianual dedicado a promover un uso más seguro de Internet al combatir el contenido ilícito y dañino en las redes mundiales. El plan, dirigido por la Comisión Europea, se extiende hasta diciembre de 2002 y tiene un fondo ascendente a 25 millones de euros.

El impacto de este tipo de acuerdos entre países ha cambiado significativamente las leyes en todo el mundo. Por ejemplo, las leyes sobre pornografía infantil fueron añadidas recientemente al marco jurídico mexicano. En enero de 1999, el Congreso mexicano modificó el Código Penal del país a fin de categorizar la pornografía infantil y la prostitución infantil como "delitos de extrema gravedad". Antes de la fecha no existía ley alguna referida a estos delitos.

Como resultado de los sucesos del 11 de septiembre de 2001, el público norteamericano ha estado más preocupado por los posibles desastres que pudieran ocasionar el terrorismo informático. Este tipo de terrorismo incluye el uso de métodos comunes de hacking (como el acceso no autorizado a computadoras, la propagación de virus, las bombas de correo electrónico, entre otros) con el objetivo de provocar daños, especialmente en infraestructuras nacionales vitales (suministro de agua, redes eléctricas, compañías telefónicas) o sistemas nacionales de seguridad y defensa militar. Como al igual que otras formas de terrorismo, el terrorismo informático por lo general tiene motivaciones políticas y está dirigido contra objetivos civiles. Un acto de terrorismo informático puede dañar la economía y la infraestructura de un país, a la vez que provocar pérdidas de vida. Podríamos imaginarnos la devastación que podría causar un hacker que penetra el sistema de control del tráfico aéreo, el sistema de computadoras de un gobierno que controla los misiles nucleares, o un sistema de emergencia policial. La amenaza se exacerba por el hecho de que las prácticas tradicionales contra el terrorismo son inútiles frente a un enemigo que puede utilizar la tecnología para golpearnos mientras está a miles de millas de distancia.

Mientras más dependiente sea una sociedad de los sistemas de computación, más vulnerable se vuelve ante los terroristas informáticos. Las plantas de procesamiento de alimentos y de producción de productos farmacéuticos, las compañías de electricidad, los sistemas de control de tráfico, las instalaciones médicas, los sistemas de comunicaciones militares, públicas, de seguridad y civiles son todas esferas de alta vulnerabilidad. Por lo general el terrorista intenta crear destrucción a gran escala, y ello es sin duda posible para alguien que pueda asumir el control de uno o más de estos sistemas cruciales. Para una explicación sobre posibles escenarios referidos al terrorismo informático, véase http://afgen.com/terrorism.html.

El terrorismo informático es motivo de preocupación para los organismos encargados de la aplicación de la ley en muchos países desde hace varios años. La seguridad informática y de redes ha sido un objetivo importante para los departamentos de las técnicas de información y la policía en todo el mundo. Las regulaciones y las políticas internas referidas a la conectividad a Internet y la seguridad de la información son algo ya común. Los especialistas de la informática en las empresas y en las redes de pequeñas empresas se han mostrado cada vez más preocupados por poner en práctica cortafuegos y aplicar las actualizaciones de seguridad, los programas antivirus, y numerosas otras medidas.

La amenaza del terrorismo informático no es nueva. El primero de octubre de 1997, Arnaud de Borchgrave, director del Proyecto sobre el crimen organizado mundial del Centro de Estudios Estratégicos e Internacionales, testificó ante el Comité de Relaciones Internacionales de la Cámara de Representantes de los Estados Unidos. En su testimonio expresó que "ya hay ocho países hostiles o potencialmente hostiles que han desarrollado la tecnología y los conocimientos necesarios para emprender una guerra de la información por medio de sabotaje electrónico y destrucción letal, mientras que 120 países han desarrollado la capacidad para lanzar un ataque informático". La *guerra de la información* podría incluir no solamente actos de terrorismo informático sino también espionaje y recopilación de información de inteligencia. Se puede obtener más información sobre este testimonio en el sitio fue del Centro de Estudios Estratégicos e Internacionales (CSIS) en www.csis.org/hill/ts100197.html.

A pesar de que muchos países tienen leyes sobre terrorismo, varios han actualizado las leyes vigentes o creadas otras nuevas para abordar específicamente la amenaza del terrorismo informático. Por ejemplo, en diciembre de 2001, el gobierno canadiense aprobó la Ley Antiterrorismo que, entre otras cosas, aborda temas referidos a las diferentes formas de terrorismo, incluidas las actividades que afectan las computadoras y la información. Mediante legislaciones de este tipo, los países pueden abordar el tema del delito informático de manera que refleje los ideales nacionales de libertad y seguridad.

Las dificultades que entraña imponer una legislación referida al terrorismo informático y su repercusión en la ciudadanía guardan mucha similitud con los problemas de imponer medidas de seguridad en una organización. Durante años, las empresas han tenido que encontrar un equilibrio entre la seguridad con accesibilidad cuando se utilizaban nuevas políticas para limitar las actividades del personal. Con cada nueva política, los miembros de una organización pueden pensar que se ha reducido su capacidad para acceder a determinada información. Demasiada seguridad podría tener como resultado la incapacidad de las personas para realizar su trabajo, mientras que demasiada poca seguridad dejaría abiertas posibilidades que pondrían en riesgo la empresa. Los efectos de las leyes sobre terrorismo informático y otros tipos de delito informático pudieran tener riesgos similares y afectar la libertad de las personas para acceder a determinada información o realizar acciones que son normales para sus actividades en línea. La libertad y la seguridad son, por definición, polos opuestos de un todo. Mientras más haya por un lado menos habrá del otro. Encontrar el equilibrio necesario entre el control gubernamental para proteger a la ciudadanía y el deseo de esa ciudadanía de ser libre de una excesiva reglamentación opresiva es un dilema político al que se enfrentan los países democráticos basados en los principios de libertad y derechos humanos.

Otra categoría de delito informático relacionado con el terrorismo informático pero diferente de este es la actividad llamada "hackactivismo", que por lo general entraña daño a la propiedad sin riesgo de daño a personas. Durante el conflicto de Kosovo, muchos "hackactivistas" utilizaron Internet para diseminar propaganda, apoderándose del control de sitios web de organismos gubernamentales y modificándolos para reflejar sus opiniones políticas. Este "hackactivismo" no se debe confundir con el activismo político simple que utiliza Internet. Este último incluye actividades como la construcción de sitios web propios y la presentación de opiniones políticas. El "hackactivismo" es una actividad delictiva ya que incluye la intrusión en el sitio de otra persona sin el permiso de esta o la perturbación de las actividades de una organización en la red de los gobiernos cuyas políticas no son de su agrado. Los "hackactivistas" utilizan bombas de correo electrónico, ataques de sistema operativo, virus y gusanos, y otros métodos comunes de ataque informático con fines políticos. No obstante, cuando los ataques de estos activistas se exceden y perturban los servicios (como los de las instalaciones médicas o la compañía de servicios públicos) de una manera que amenace la vida humana o la vida diaria, se convierten en terroristas informáticos.

A fin de hacer frente a estos temas de delitos informáticos y delitos en Internet, numerosos países se han unido y firmado la Convención sobre delito informático del Consejo de Europa (COE) en virtud de la cual los miembros deben penalizar las actividades relacionadas con el terrorismo informático y otras formas de delito

informático. Estados no miembros como Estados Unidos, Canadá, Japón y Sudáfrica también lo han firmado. Mediante este esfuerzo de cooperación, las actividades como hacking, la injerencia en los sistemas de computación, el fraude, la falsificación y otros delitos afines son penalizados en los países signatarios de la Convención. La Convención también respalda la cooperación entre los países para investigar y procesar esos delitos y para recopilar evidencias mediante métodos electrónicos sobre delitos relacionados con el terrorismo, el crimen organizado y otros delitos realizados a escala mundial con el uso de computadoras y redes. El texto de la Convención puede encontrarse en el sitio web del COE en http://conventions.coe.int/Treaty/EN/projects/FinalCybercrime.htm. Para conocer sobre el estado actual de la Convención en cuanto a los países que la han firmado, favor acceder ahttp://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=&DF=.

Los grupos a cargo de la aplicación de la ley en diferentes países también están trabajando de conjunto contra la amenaza de la actividad delictiva en Internet. Debido a que estas actividades pueden llegar a ser de jurisdicción internacional, esta cooperación es vital para combatir el delito informático.

En diciembre 2000, un esfuerzo conjunto entre la policía de la ciudad de Moscú y el Centro de contrabando cibernético de la Aduana de los EE.UU. tuvo como resultado el cierre de el sitio web ruso Blue Orchid (Orquídea Azul), que publicaba imágenes y videos de abuso físico y sexual de niños. Como resultado de esta y otras operaciones se incautaron cientos de videocasetes y discos dvd y más de 1000 fotos pornográficas. Esta operación también llevó a la realización de arrestos en ambos países.

Hasta las empresas pueden ayudar a combatir los delitos informáticos internacionales, como fue el caso que concluyó con casi 1500 arrestos en el año 2000. La policía italiana procuró la asistencia de Microsoft para crear un sitio web de pedofilia falso llamado *amantidelbabini* ("Amantes de los niños"). El sitio advertía específicamente que su contenido era ilícito, pero a pesar de la advertencia se suscribieron a él 1032 personas. La policía italiana allanó 600 residencias, arrestó a 831 italianos e intentó extraditar a otros 660 de diferentes otros países.

Comparación de las leyes internacionales sobre delito informático

Cuando se investigan delitos que abarcan varios países, es importante reconocer que las leyes de un país pudieran no ser consecuentes con las de otros países. Cada país tiene sus propias opiniones sobre la justicia, las libertades y las libertades civiles. Cuando la investigación nos lleva hasta la jurisdicción de otro país, podríamos sorprendernos ante las diferencias entre las leyes de ese país y las nuestras. En algunos casos, podría sorprendernos que no existen leyes referidas a delitos particulares.

No es objetivo de este libro abarcar cada ley de cada país referida al delito informático y el delito en Internet, además de que las leyes en todas las jurisdicciones están en constante cambio. No obstante, es útil que el investigador tenga una lista de

recursos que relacionan las leyes sobre el delito informático en varios países y brindan información general sobre los aspectos globales de la investigación y el procesamiento del delito informático. Cuando analicemos estas leyes debemos recordar que el sistema de justicia de cualquier país es complejo y entraña mucho más que sólo sus estatutos penales. Los procedimientos y las reglas de los tribunales y de la evidencia son disímiles. Por ejemplo, según el Código Napoleónico de Francia los acusados se presumen culpables, mientras que la presunción de inocencia es la base del derecho penal de los Estados Unidos. Si usted precisa mas información acerca de las leyes de un determinado país, contacte a un miembro del gobierno o de la comunidad de la aplicación de la ley de ese país o a un abogado especializado en derecho penal en esa jurisdicción.

Un buen recurso para cualquier investigador es contactar primero a la INTERPOL y determinar si una actividad es ilícita en un determinado país. De ser posible, contacte con la embajada de ese país o con el organismo encargado de la aplicación de la ley dentro de ese país para determinar si existe alguna legislación específica (y si está vigente) dentro de dicho país. Al hacerlo podrá determinar si su investigación puede continuar más allá de sus fronteras jurisdiccionales.

Argentina

Argentina no tiene leyes especiales sobre delito informático. No obstante, el Código Penal de ese país sí contiene otras leyes que pueden ser aplicadas a determinados delitos, independientemente de si se han cometido o no utilizando computadoras e Internet. Por ejemplo, los artículos 128 y 129 referidos a la pornografía infantil penalizan la publicación, confección, reproducción o distribución de imágenes obscenas.

La capacidad para enfrentar los delitos informáticos que no sean el de pornografía infantil en Argentina ha sido muy limitada. Por ejemplo, veamos el ejemplo del fallo del tribunal argentino en abril de 2002 que afectó a un grupo de hackers llamado el Equipo X. Este grupo se infiltró en la página web de la Corte Suprema en 1998 y le modificó negativamente el diseño. Este fue el primer caso de ataque informático procesado en Argentina, pero en este caso el juez dictaminó que la ley argentina abarcaba delitos contra “personas, cosas y animales" pero no ataques digitales.

Australia

La legislación federal a tenor de las leyes de la Mancomunidad de Australia se refiere a temas relacionados con el delito informático. La Ley Penal de 1914, Parte VIA, secciones 76B y 76D (véase la Ley en http://courses.cd.vt.edu~cs3604/lib/Crime/Australia.law.html) se refiere al acceso ilícito a datos y penaliza el acceso no autorizado intencional a datos en una computadora de la mancomunidad o a datos almacenados en nombre de la mancomunidad en otra computadora. En otras palabras, de una manera muy similar al Título 18 de los EE.UU., esta ley se refiere solamente a los datos almacenados en sistemas gubernamentales, no a los de empresas o computadoras personales. La sanción a tenor de esta ley es de seis meses de cárcel; el castigo es más severo si la persona realiza estas acciones con la intención de estafar alguien o si sabe o tiene conocimiento razonable de que los datos están relacionados con determinada información sensible. Esto incluye datos referidos a la seguridad, la defensa, las relaciones internacionales, la aplicación de la ley, la protección de la seguridad pública, los asuntos personales de los individuos, registros financieros, secretos comerciales o información comercial de Australia. En tales casos, el delito merece una sanción de dos años de cárcel.

La legislación federal de la mancomunidad está limitada a las facultades especificadas en la constitución de Australia. Además, los seis estados y los dos territorios de Australia también tienen facultades irrestrictas, las cuales son anuladas por la ley de la mancomunidad en caso de conflicto. Los delitos no previstos en las leyes federales (como el acceso no autorizado a computadoras no gubernamentales) son procesados a tenor de las leyes de los estados y territorios individuales. Por ejemplo, en 1998, Victoria aprobó las primeras leyes estaduales sobre delito informático, y el resto de los estados y territorios también lo hicieron después (aunque las leyes no son uniformes en todos los estados y territorios).

En Australia, las leyes referidas a la pornografía infantil se manejan principalmente a nivel de los estados. La ley australiana define la pornografía infantil como algo que involucra a un sujeto aparentemente menor de 16 años de edad. Al calificar a la pornografía infantil de esta manera, los órganos de aplicación de la ley están relevados de la carga de demostrar la edad exacta que tenía un sujeto en el momento en que se produjo la pornografía. Si la persona aparenta ser menor de edad, el material se considera pornografía infantil.

Los estados de Victoria y Queensland han utilizando la Clasificación de la Ley de filmes y publicaciones como fuente de legislación para abordar los casos de pornografía infantil. A tenor de esta ley, pedir un niño que participe en un "filme objetable" (como el que entraña la penetración sexual) podría resultar en una sentencia de hasta cinco años de cárcel. La posesión de pornografía infantil podría llevar a una sentencia de un año de cárcel. Cada estado tiene leyes adicionales para abordar este delito.

Para más información sobre las leyes del delito informático en Australia, véase el sitio de Baker & McKenzie en www.bmck.com/Australia/australia_crime.htm.

Brasil

El año 2000 Brasil cambió varias leyes sobre delito informático. El artículo 313-A del Código Penal se refiere a la introducción de datos falsos o a la no introducción de datos correctos en un sistema de computación o banco de datos de la administración pública. Si una persona realiza esta acción con el objetivo de obtener ventajas inapropiadas para sí o para un tercero o provoca daños a terceros, puede ser encarcelada entre dos y 12 años y ser multada. Si una persona modifica o altera los datos sin autorización, puede ser acusada a tenor del artículo 313-B y ser encarcelada de tres meses a dos años además de recibir una multa. Las penas a tenor de cualquiera de los dos artículos pueden ser elevadas en entre un tercio y la mitad si los daños afectan a los sistemas de administración pública (en otras palabras, los sistemas de computación gubernamentales) o a los individuos cuya registros están almacenados en esos sistemas.

El Código Penal de Brasil contiene dos artículos que abordan específicamente la producción de pornografía infantil, pero no tiene leyes referidas a su posesión. El artículo 240 del Estatuto del niño y el adolescente de Brasil prevé que una persona puede ser condenada a entre uno y cuatro años de cárcel además de ser multada por producir o dirigir una obra de teatro, espectáculo de televisión o filme con escenas de sexo explícito o pornografía con la participación de un niño o un adolescente. El artículo 241 del Estatuto dispone además la misma sanción para las personas que tomen películas o realicen escenas pornográficas y de sexo explícito en público que involucren a un niño o un adolescente. En Brasil, un niño se define como alguien menor de 12 años de edad; el

adolescente se define como una persona de entre 12 y18 años de edad.

Canadá

En el Código Penal de Canadá hay varias secciones que abordan directamente el delito informático. La sección 342.1 se refiere al uso no autorizado de una computadora y (a diferencia de las leyes a nivel nacional de muchos países) se aplica a cualquier servicio de computadoras, incluidos los sistemas privados. Esta ley aborda temas referidos a los hackers que pueden llegar a penetrar un sistema de computación mediante diferentes programas o troyanos o utilizando las contraseñas de otra persona. También se refiere a la intersección de datos y la diseminación de virus: La violación de esta ley puede ser sancionada con hasta 10 años de cárcel.

La sección 342.1 se refiere al acto de uso no autorizado de computadora; la sección 342.2 va a un paso más allá y penaliza la posesión, la venta, la oferta de venta y la distribución de instrumentos y dispositivos factibles de ser utilizados para cometer los delitos mencionados en la sección 342.1. Además, incluso si el delincuente no logra infiltrar el sistema pero simplemente oferta la herramienta para hacerlo, podría ser sancionado a hasta dos años de cárcel.

El Código Penal también aborda el tema de la privacidad y la Sección 184 se refiere a la intercepción de comunicaciones. La intercepción de comunicaciones privadas es sancionada con hasta cinco años de cárcel.

La sección 380 se refiere a las transacciones fraudulentas en relación con contratos y el comercio y aborda el fraude informático. La persona que cometa este delito enfrentará sanción de hasta dos años de cárcel si el fraude asciende a una cantidad inferior a los 2000 dólares canadienses, mientras que la sanción puede ser de hasta 10 años de cárcel si el fraude excede la cantidad de 5000 dólares canadienses.

La Sección 430.1 se refiere a "daño provocado", mientras que la Sección 430 (1.1) aborda específicamente los daños provocados por el delito informático. Trata sobre la modificación de datos, la interferencia y el sabotaje de redes, y la diseminación de virus. La persona que cause daño a la propiedad de esta manera puede ser sancionada con hasta dos años de prisión, pero si el daño excede los 5000 dólares canadienses o si involucra datos (como cuando se modifican los datos o se destruyen), el delincuente puede ser sancionado a un máximo de 10 años de cárcel. Si la comisión del delito provoca peligro para la vida, la persona puede ser condenada a cadena perpetua.

La Sección 163.1 se refiere a la pornografía infantil. Esta ley no establece distinción entre los formatos en que pudiera presentarse existir la pornografía infantil. En otras palabras, no importa si la pornografía está en formato electrónico, en fotografía, filmes, vídeo o cualquier otra representación visual. La pornografía infantil es pornografía infantil, independientemente del medio en que sea representaba.

En Canadá hay pornografía infantil cuando el sujeto del material pornográfico tiene menos de 18 años de edad o está presentado como tal. Esto es una definición inteligente, porque podría ser difícil cuando –no imposible– seguir el rastro de cada modelo o actriz que participa en un film pornográfico para determinar su edad. Así, si la persona aparenta ser un niño, el material se considera pornografía infantil. Si alguien confecciona, distribuye o vende ese tipo de pornografía, puede ser sancionado con hasta 10 años de prisión. La persona que sencillamente posea este tipo de pornografía puede ser sancionada a cinco años de prisión como máximo.

En la escena...

¿Cuál es la diferencia entre la condena sumaria y la acusación?

A tenor de la ley canadiense, existen dos tipos básicos de delitos penales. Los delitos leves son conocidos como delitos de condena sumaria y llevan una sanción de multa de hasta 2000 dólares canadienses o seis meses de cárcel (a menos que se especifique una multa más elevada en el estatuto para el delito en particular). Además, a los condenados por delitos de condena sumaria no se les registran las huellas dactilares y tienen derecho a indulto después de tres años.

Los delitos considerados como más grave se clasifican como delitos mayores o merecedores de acusación. Dado que las sanciones son mayores (multas elevadas y/o cárcel), los acusados de delitos más graves tienen derecho a ser juzgados ante un jurado. El delincuente no tiene derecho a indulto hasta tanto haya concluido el quinto año de la condena.

Los delitos que pueden ser procesados como condena sumaria o como delitos más graves se denominan delitos híbridos, u "opción real" porque la Corona (equivalente al Estado en los Estados Unidos) tiene la opción de decidir en qué forma será procesado.

La Ley de derecho de autor es otra parte de la legislación que se refiere a la piratería informática. La persona que venda, alquile o distribuya software protegido por derecho de autor se enfrenta a multas y encarcelamiento. En la condena sumaria, los delincuentes pueden ser multados con hasta 25,000 dólares canadienses y/o seis meses de cárcel. En los casos de delitos más graves las condenas pueden ser multas de hasta un millón de dólares canadienses y/o cinco años de cárcel.

Países europeos

Como se dijo anteriormente, muchos de los miembros de la Unión Europea son signatarios de la Convención sobre delito informático del COE. Entre estos países están el Reino Unido, España, Portugal, Italia, Irlanda, Alemania, Polonia, Hungría, Francia, Grecia, Suiza y la mayoría de los países escandinavos. No obstante, el tratado no es de aplicación automática; en otras palabras, cuando un estado miembro lo adopta y ratifica, deberá aprobar leyes para aplicarlo en la práctica.

El tratado de la Unión Europea es similar a la Ley sobre fraude y uso ilícito de computadoras de los Estados Unidos (Título 18, sección 1030 del Código de los EE.UU.) en cuanto a las actividades que proscribe. Sin embargo, sí contiene disposiciones que exceden las previstas por las leyes estadounidenses, como la prohibición de las llamadas "herramientas de robo" (herramientas de hackers) que pueden ser utilizadas para acceder de manera no autorizada a computadoras y redes. Hubo intentos por incluir una disposición similar en la Ley de Derecho de autor del Milenio digital de los EE.UU. (DMCA), pero el Congreso las rechazó.

Algunos países europeos contaban ya con sus propias leyes sobre delito informático antes de la aprobación de la Convención. Por ejemplo, la Ley sobre el uso indebido de computadoras del Reino Unido, aprobada en 1990, abordaba actividades específicas como:

- acceso no autorizado a material de computación
- acceso no autorizado con intención de cometer o facilitar la comisión de delitos

- modificación no autorizada de material de computación

Para obtener el texto completo de la Ley, véase www.ja.net/CERT/JANET-CERT/law/cma.html.

El Código Penal de Francia cuenta con disposiciones sobre el delito informático desde 1993. Los artículos 323-1 hasta 323-4 se refieren al acceso fraudulento a sistemas de procesamiento automatizado de datos, la interrupción o perturbación de su funcionamiento o la introducción fraudulenta de datos en ellos. Las sanciones oscilan entre uno y tres años de cárcel y multas de hasta 300,000 francos franceses. El Código Penal de Alemania incluye secciones referidas al espionaje de datos, la alteración de datos y el sabotaje de computadoras (Código Penal, secciones 202a, 303a y 303b). El artículo 615 del Código Penal italiano prohíbe el acceso no autorizado a computadoras y sistemas de telecomunicaciones, la posesión ilícita y difusión de códigos de acceso a computadoras o sistemas de telecomunicaciones, y la difusión de programas destinados a dañar o interrumpir un sistema de computación. Por otra parte, países como España no tienen disposiciones específicas en su Código Penal referidas al delito informático, aunque las leyes que regulan la privacidad, el fraude y temas similares pueden ser aplicables a los delitos informáticos.

República Popular China

La República Popular China (RPCh) posee leyes que protegen la información de computadoras en el Decreto No. 147. El artículo 23 de este Decreto plantea que es ilícito introducir deliberadamente un virus informático u otro dato dañino que ponga en peligro el sistema de información de una computadora o vender sin autorización productos especiales de protección de seguridad para sistemas de computación. En tales casos, las organizaciones de seguridad pública pueden emitir advertencias o imponer una multa de 5000 yuanes a individuos o 15,000 yuanes a empresas. Los ingresos ilícitos procedentes de las acciones delictivas son confiscados, y se puede imponer una multa que puede ascender hasta tres veces la cantidad obtenida por la actividad ilícita.

La legislación de la RPCh se refiere a la producción, venta y distribución de cualquier tipo de pornografía, con distintas condenas. Si el delito se comete con fines de lucro, los delincuentes pueden ser condenados a hasta tres años de cárcel, trabajo forzado, o vigilancia, además del pago de una multa. Los que cometen delitos graves pueden recibir de 3 a 10 años de cárcel y una multa, mientras que los que cometen delitos "más graves" pueden ser sancionados con hasta 10 años de cárcel o cadena perpetua y con una multa o la confiscación de propiedades. En casos que incluyan la distribución de literatura, filmes, videos, o imágenes pornográficas, el delincuente puede ser sancionado a dos años de cárcel, detención o vigilancia.

Muchos actos son considerados delitos en la PRCh mientras que no lo son en otros países. Por ejemplo, el Reglamento del Ministerio de Seguridad Pública sobre la Protección, la seguridad y la gestión de redes de información de computadoras e Internet (Artículo 5) plantea que "ninguna unidad o individuo puede utilizar Internet para crear, replicar, recuperar o transmitir los siguientes tipos de información" y presenta una lista que incluye, entre otras cosas:

- incitar a la división del país, dañando así la unificación nacional
- lanzan calumnias o distorsionar la verdad, difundir rumores, destruyendo con ello el orden de la sociedad

- promover supersticiones feudales, material sexualmente sugestivos, el juego ilícito, la violencia, el asesinato
- participar en terrorismo o incitar a otros a cometer acciones delictivas; insultar abiertamente a otras personas o distorsionar la verdad para calumniar a terceros
- dañar la reputación de los órganos del estado

Esta es solamente una parte de la lista de actividades prohibidas. Existen muchas regulaciones sobre el uso de Internet en la esfera comercial, y todos los usuarios de Internet tienen que registrarse con el organismo policial local en un plazo máximo de 30 días posteriores a haber obtenido su cuenta con el ISP.

Otras leyes chinas pertinentes son:

- Reglamento de la PRCh para la protección y seguridad de los sistemas de información de computación
- Reglamento para la protección, la seguridad y la gestión de redes de información de computadoras e Internet
- Reglamento de telecomunicaciones de la TLC
- Reglamento de protección de secreto estatal para sistemas de información por computadoras en Internet

Las sanciones por violar algunas de las leyes pueden ser severas. Los usuarios pueden ser sancionados a la pena de muerte por publicar material con el cual el gobierno no está de acuerdo.

En la escena...
Crimen y castigo en la República Popular China
En abril de 2000, un escritor llamado Guo Qinghai fue sentenciado a cuatro años de cárcel en un juicio donde no tuvo la representación de un abogado. Su delito fue publicar artículos de una revista de Hong Kong que pedían reformas políticas. En septiembre de 2000, el autor Qi Yanchen fue sentenciado a cuatro años de cárcel por publicar en Internet fragmentos de su libro *El colapso de China*. En mayo de 2001, Jian Shihua, de profesión maestro, fue sentenciado a dos años de cárcel por publicar artículos en un boletín de Internet que criticaba al gobierno chino. Muchos otros ciudadanos chinos han sido detenidos, arrestados y condenados por delitos como descargar artículos con contenido político o religioso de sitios web extranjeros. Para más información véase www.hrw.oeg/backgrounder/asia/china-bck-0701.htm.

México
El Código Penal federal de México aborda el delito informático en varias secciones, mientras que otras leyes (como las referidas al fraude) son aplicables independientemente del medio (háyanse cometido por Internet o por otros medios). Los artículos 211 bis 1 y 211 bis 2 del Código son disposiciones referidas al acceso no autorizado a las computadoras privadas protegidas por dispositivo de seguridad; los artículos 211 bis 3, bis 4 y bis 5 se refieren al acceso no autorizado a computadoras del gobierno mexicano y del sistema financiero mexicano. Estos artículos de la ley y se refieren a la actividad de

hacking, propagación de virus, y otros actos delictivos relacionados con la computadoras y sus datos. Si una persona copia o visualiza información protegida por algunos dispositivos de seguridad, podrá ser encarcelada por un período que oscila de tres meses a un año y pagar una multa de entre 150 y 450 dólares estadounidenses. El uso no autorizado de una computadora mediante el cual se modifique, destruya o se pierda la información puede ser sancionado con entre seis meses y dos años de cárcel y una multa de entre 300 y 900 dólares de Estados Unidos.

Al momento de escribir estas líneas, se están realizando modificaciones en México a las leyes existentes a fin de abordar el problema de la pornografía infantil. La Comisión para la atención de grupos vulnerables, de la Cámara de Diputados del Congreso Federal mexicano, modificó el artículo 201 del Código Penal federal y la Ley sobre el Crimen Organizado. El artículo 201 penaliza la creación, reproducción o transmisión de pornografía infantil en Internet. La persona que cometa este delito puede ser sancionada a entre 10 y 14 años de cárcel y a una multa equivalente a entre 500 y 3000 días del salario mínimo legal. Si en el delito de pornografía infantil o en el robo y el tráfico de niños participan tres o más personas, pueden ser sancionadas en virtud del Artículo 2 de la Ley sobre el Crimen Organizado.

Federación de Rusia

La Federación de Rusia tiene tres artículos en el Código Penal que se refieren específicamente a distintos tipos de delito informático. La violación de esto artículos es motivo de multas, encarcelamiento o ambos. La Federación de Rusia también cuenta con otros artículos en su Código Penal que pueden ser aplicados a los delitos referidos a la computación e Internet, si bien no abordan directamente el tema de las tecnologías utilizadas para cometer los delitos.

El artículo 272 del Código Penal se refiere al acceso no autorizado y la modificación o bloqueo de información. La violación de esta ley puede provocar sanción de multa y/o cárcel de hasta dos años. Si el delito involucra conspiración, en la que un grupo planea y comete el delito, la sentencia puede ser de hasta cinco años de cárcel.

El artículo 273 del Código Penal se refiere a los programas malignos. Si una persona es declarada culpable de producir y distribuir un programa de computación peligroso, puede ser sancionada a un máximo de siete años de cárcel.

El artículo 274 es el último que se refiere directamente al delito informático y a la explotación de redes de computación. Violar esta ley puede provocar una sanción de hasta cuatro años de cárcel.

La Federación de Rusia no tiene una legislación específica referida a la pornografía infantil, aunque sí tiene leyes que abordan el tema de la pornografía en general. El artículo 242 de su Código Penal señala que es ilícito distribuir o promocionar materiales pornográficos u objetos pornográficos (no relacionados específicamente con niños). La sentencia es una multa de entre 500 y 800 veces el salario mínimo –u otro ingreso de la persona condenada– por un período de entre cinco y ocho meses o encarcelamiento por un período de dos años. Si bien se están analizando la aprobación de nuevas leyes y la modificación de las existentes, la Federación de Rusia no tiene definida la pornografía infantil, la edad legal que debe tener un sujeto de este material, ni ninguna legislación definitiva referida a ese delito. En estos momentos, no existe una edad legal para el consentimiento sexual en Rusia, aunque la legislación considera ilícitos los actos sexuales que involucran a niños menores de 14 años de edad.

NOTA

Para obtener una excelente explicación de las leyes de delito informático en 43 países, regularmente actualizada, véase www.mossbytrett.of.no/infor/legal.html.

Investigación de un delito informático internacional

La capacidad para realizar investigaciones más allá de las fronteras jurisdiccionales casi siempre depende de la cooperación con las entidades encargadas de la aplicación de la ley en esas zonas. La policía de un país por lo general no tiene jurisdicción oficial en otros países. No obstante, el trabajo conjunto de la policía de diferentes países puede repercutir de manera significativa en la incidencia de la criminalidad. Esta repercusión se ha hecho evidente en varios casos de colaboración entre la policía y otros organismos de aplicación de la ley en diferentes países.

Un gran logro del esfuerzo policial internacional fue el caso llamado Operación Catedral dirigida por las fuerzas británicas, y que se concentró en una red de pedofilia llamada País de las Maravillas (Wonderland) que ofertaba material de pornografía infantil a sus miembros por Internet. Para ingresar como miembro de esta red y participar en el intercambio de pornografía infantil, las personas tenían que demostrar que poseían al menos 10,000 imágenes de pornografía infantil. En septiembre de 1998 se realizaron 100 allanamientos en Gran Bretaña, Australia, Austria, Bélgica, Finlandia, Francia, Alemania, Italia, Noruega, Portugal, Suecia y Estados Unidos. La cooperación de la policía en todos estos países logro el cierre de esta operación masiva de delito informático.

En algunos casos no será necesario contactar a los organismos de aplicación de la ley de otros países hasta tanto tengamos preparado un caso sólido. Si estamos investigando a un sospechoso dentro de nuestro país y vemos que esta persona utiliza Internet mediante servidores y servicios de otros países, pudiéramos sentirnos inclinados a contactar a la policía de esa jurisdicción para obtener mayor cantidad de evidencias. Como veremos en las secciones siguientes, no siempre será necesario recurrir a otro organismo de aplicación de la ley durante las primeras etapas de investigación. Si bien será necesaria una cooperación para procesar el caso, la recopilación de evidencias a menudo puede hacerse sin involucrar a otros organismos.

Recopilación de evidencias

Los servicios de correo electrónico gratuitos son un medio comúnmente utilizado para cometer delitos. Por ejemplo, un sospechoso podría utilizar un servicio gratuito de correo electrónico para incitar a las víctimas a participar en un proyecto de fraude, enviar amenazas de muerte o cometer cualquier otro delito. Una vez descubierto este delito y de haber localizado el origen de los mensajes de correo electrónico (utilizando las técnicas que analizamos en el capítulo 9), podríamos determinar que el servicio de correo electrónico gratuito está ubicado en otro país.

Dado que muy probablemente necesitaremos la información de cuenta del ISP para verificar la identidad de la persona, debemos primero contactar a la compañía que ofrece este servicio. Visite el sitio web de la compañía y busque la dirección de correo electrónico que haya hecho uso ilícito de su cuenta. Si no posee ninguna otra información de contacto, podría utilizar como punto de partida la dirección de correo electrónico que es utilizada para reportar al servicio los mensajes no deseados y otros

usos ilícitos. Esta dirección de correo electrónico usualmente sería abuse@*nombrededominio*. Por ejemplo, la dirección de correo electrónico de Hotmail para el uso indebido de cuentas es abuse@hotmail.com. Puede contactar a la compañía mediante esta dirección para solicitar información de contacto más específica e informarle que se está realizando una investigación que involucra ese servicio. En muchos casos, estas compañías tienen una política referida a la revelación de información de clientes. La página web del proveedor a menudo brinda información sobre números telefónicos para contactar a la compañía, lo cual es útil para descubrir el tipo de documentación que requieren para hacer pública la información de cuenta. En algunos casos, la compañía requiere algún tipo de orden judicial. Esto es así especialmente en los Estados Unidos y otros países con estrictas leyes de privacidad. En otros casos, la compañía simplemente pedirá una carta con el membrete policial donde se pida oficialmente la información.

Una vez contactado el proveedor, se puede redactar una carta oficial o contactar a la oficina del fiscal de distrito o la oficina de la fiscalía que corresponda a su jurisdicción particular. Cuando tengamos la documentación que exige el proveedor la puede enviar por fax o por correo y recibir la evidencia que necesita.

Se puede utilizar el mismo método si el sospechoso vive en su país pero realiza la operación ilícita desde un servidor ubicado en otro país. En muchos casos, un sitio web está hospedado en un proveedor de servidor por una ISP o a una empresa que vende espacio de servidor (llamada empresa de hospedaje web). El nombre de dominio pertenece a su sospechoso y puede estar diseñado y mantenido por esa persona, pero los archivos están en un servidor que pertenece a otra empresa. Esta empresa brinda servicios técnicos y/o de administración, con lo cual los clientes son eximidos de la carga técnica del mantenimiento del servidor web. En algunos casos el sospechoso nos facilita el trabajo al colocar en su propia página web un hipervínculo al sitio web de la empresa que lo hospeda, o alguna otra información de contacto. En muchos casos, tendremos únicamente que visitar el sitio web de la empresa de hospedaje y buscar una dirección de correo electrónico o número de teléfono para contactar al proveedor del espacio en servidor. En otros casos, quizás sea necesario utilizar NSLookup o Whois para obtener este información.

Uso de herramientas de búsqueda

NSLookup es una herramienta que se puede ejecutar en computadoras con Windows NT y 2000, aunque en Internet hay disponibles versiones con base en web. NSLookup puede brindarnos una dirección IP para un nombre de dominio especificado o un nombre de dominio para una dirección IP especificado. Whois es una herramienta con base en la web que puede brindarnos un poquito más de información, incluida la información de contacto (dirección de correo y número telefónico) de la persona que tiene registrado el sitio. Cuando se utilizan, estas herramientas interrogan a los servidores DNS que tiene almacenada la información sobre un sitio web particular. Un buen sitio web que pudiéramos utilizar para determinar la información sobre un sitio web es *name.space*. Este sitio se puede visitar en http://swhois.net y nos permite buscar información utilizando cualquier de estas herramientas. Al escribir la dirección del sitio web en el campo **Whois** y hacer clic en el botón **Search**, podemos realizar una búsqueda del titular de esta dirección. La pantalla que se muestra en la figura A.1 nos brinda una gran

cantidad de información sobre un sitio.

Figura A.1 Resultados de una búsqueda con Whois en el sitio web name.space
(insertar aquí la imagen que aparecen en la página 682 del original)

En la figura A.1 realizamos una búsqueda con Whois sobre tacteam.net (uno de los muchos sitio web registrados por el autor de este libro). En la pantalla podemos ver que la sección de "Registrant" (Registrante) muestra diferentes informaciones de la sección "Technical Contact" (contacto técnico). El nombre de la persona que registra el sitio aparece en la sección "Registrant"; este campo probablemente contenga el nombre de la persona que pagó por el registro del sitio o el nombre de la persona que lo diseñó. En el caso de algunos sitios veremos aquí un nombre y una dirección. En otros casos en que los registradores son más cuidadosos (como el autor) y conscientes de que cualquiera puede obtener esta información con facilidad, se brinda solamente un nombre de compañía y una dirección postal. Esta información podría o no ser exacta, dado que no se verifica y no se requiere que sea actualizada en caso de que quien hace el registro se mude o cambie su número telefónico. La sección "Technical Contact" contiene la misma información que la sección "Registrant", pero en este caso se utiliza otra empresa para que esté a cargo de los asuntos técnicos del sitio. A menudo se obtienen datos sobre números de teléfono, número de fax y direcciones de correo electrónico. Utilizando estos datos podemos obtener información valiosa sobre los medios de contacto así como datos sobre dónde buscar información adicional sobre el dueño del sitio.

Al menos esa es la forma en que funciona en un mundo ideal. En realidad, podríamos ver que la información que obtenemos mediante la búsqueda Whois no es tan útil como desearíamos. Los delincuentes informáticos que saben que están involucrados en una actividad ilícita mediante sus sitios web, así como ciudadanos ordinarios a quienes les preocupa la privacidad, por lo general no serían tan dadivosos para ofrecer sus direcciones particulares y números de teléfono verdaderos. Cuando los sospechosos tienen su propio servidor web en sus propios locales y utilizan sus propios servidores DNS se hace aún más difícil rastrear esta información.

Para interpretar los nombres de dominio

Cuando leemos un nombre de dominio encontraremos que terminan en un nombre de dominio principal, que se utiliza para mostrar el propósito o el país de origen del dominio. Los dominios principales más comunes y sus usos generales son los siguientes:

- **.com** Sitios para usos comerciales
- **.edu** Sitios pertenecientes a una institución educacional
- **.gov** Sitios pertenecientes a los organismos gubernamentales de Estados Unidos
- **.int** Organizaciones y bases de datos establecidas mediante tratados internacionales
- **.mil** Sitios militares de Estados Unidos
- **.net** Proveedores de redes
- **.org** Organizaciones (no lucrativas)

Cuando ha navegado por Internet podrá haber apreciado que muchos de estos dominios no están ya destinados exclusivamente para su objetivo original. Algunos sitios

que terminan en .com quizás no sean sitios relacionados con la actividad comercial; pueden ser sitios personales o sitios web con objetivos no lucrativos. Esto también sucede con los sitios .net; los utilizan empresas y personas que no son proveedores de servicios de redes. Por lo tanto, no debemos aceptar estas terminaciones como evidencia definitiva del objetivo de un sitio.

Recientemente la cantidad de dominios principales se ha ampliado para incluir los siguientes:

- **.aero** Compañías relacionadas con la aviación
- **.bis** Sitios relacionados con actividad comercial (sustituye el uso previsto para los .com)
- **.coop** Negocios cooperativos
- **.info** Empresas relacionadas con la información
- **.museum** Museos
- **.name** Sitios personales
- **.pro** Profesionales (por ejemplo, médicos, abogados).

Otros dos dominios principales populares son .cc y .tv, que fueron inicialmente códigos de país. Los códigos de país son nombres de dominio que especifican el país en el cual está registrado el sitio y terminan en designaciones como .cc, .tv, entre otros que se muestran en el Cuadro A.1. Si bien muchos dominios de código de país están limitados a empresas e individuos dentro del país asociado, .cc y .tv son excepciones de la regla. Tuvalu (una pequeña isla del Pacífico) tiene la extensión .tv pero llegó a un acuerdo con una empresa de televisión de California y el dominio .tv es ahora utilizada comúnmente por la televisión y sitios web de TV por Internet. De igual manera, la terminación .cc pertenece a las Islas de Cocos (Keeling), un pequeño territorio de Australia, pero el que desee pagar por esa tensión para tenerlo como su nombre de dominio puede comprarlo.

La información que contiene el Cuadro A.1 es particularmente útil cuando estamos investigando las direcciones de correo electrónico o los sitios web con dominios no familiares. Si estuviéramos viendo un sitio o un correo electrónico como un dominio que concluye en .zw ¿sabría realmente que está registrado en Zimbabwe? Saber dónde está registrado un sitio buscando ese nombre en una tabla como la que presentamos es un punto de partida para determinar dónde se originó el mensaje de correo electrónico, dónde está ubicado un sitio, y qué motor de búsqueda Whois debemos utilizar para obtener información adicional. No obstante, al utilizar esta tabla debemos recordar que algunos datos pueden cambiar. Además, debemos recordar también que debido a que un sitio esté registrado en un país determinado no significa que la persona que lo trabaja viva en él. Los delincuentes pueden utilizar identificación falsa para registrar un sitio en otro país, y si el que lo registró vivía en ese país en el momento en que fue registrado sitio no existe generalmente ningún requisito que deba renunciar a él después de haber abandonado el país.

Para obtener información adicional mediante los motores de búsqueda Whois, es preciso utilizar un motor de búsqueda que indague por los códigos de país que usted está buscando. Entre los motores de búsqueda Whois comunes que se pueden utilizar para obtener información sobre esos sitios están:

- ARIN para registro en Estados Unidos: www.arin.net
- CIRA para registro en Canadá: www.registry.ca
- RIPE NCC para registro en la Unión Europea: www.ripe.net
- APNIC para registro en Asia Pacífico: www.apnic.net
- Registro.br para registro en Brasil: http://registro.br
- NIC-México para registro en México: www.nic.mx

Cuadro A.1 Códigos de país de sitios web y direcciones de correo electrónico

Código de país-Internet	Nombre de país
ad	Andorra
ae	Emiratos Árabes Unidos
af	Afganistán
ag	Antigua y Barbuda
ai	Anguila
al	Albania
am	Armenia
an	Antillas Neerlandesas
ao	Angola
ar	Argentina
as	Samoa Americana
aq	Antártica
at	Austria
au	Australia
aw	Aruba
az	Azerbaiján
ba	Bosnia-Herzegovina
bb	Barbados
bd	Bangladesh
be	Bélgica
bf	Burkina Faso
bg	Bulgaria
bh	Bahrein
bi	Burundi
bj	Benin
bm	Bermuda
bn	Brunei Daresalam
bo	Bolivia
br	Brasil
bs	Bahamas
bt	Bhutan
bv	Islas Bouvet

bw	Botswana
by	Belarrus
bz	Belice
ca	Canada
cc	Islas de Cocos
cd	República Democrática del Congo (antiguo Zaire)
cf	República Centroafricana
cg	República del Congo
ch	Suiza
ci	Cote d'Ivoire (Costa de Marfil)
ck	Islas Cook
cl	Chile
cm	Camerún
cn	China
co	Colombia
cr	Costa Rica
cs	Checoslovaquia (antigua)
cu	Cuba
cv	Cabo Verde
cx	Isla Christmas
cy	Chipre
cz	República Checa
de	Alemania
dj	Djibouti
dk	Dinamarca
dm	Dominica
do	República Dominicana
dz	Argelia
ec	Ecuador
ee	Estonia
eg	Egipto
eh	Sahara
er	Eritrea
es	España
et	Etiopía
fi	Finlandia
fj	Fiji
fk	Islas Malvinas
fm	Micronesia
fo	Islas Faroe
fr	Francia
fx	Francia (zona metropolitana)
ga	Gabón
gb	Gran Bretaña (Reino Unido)
gd	Granada
ge	Georgia

gf	Guayana Francesa
gh	Ghana
gi	Gibraltar
gl	Groenlandia
gm	Gambia
gn	Guinea
gp	Guadalupe
gq	Guinea Ecuatorial
gr	Grecia
gs	Georgia del Sur e Islas Sandwich del Sur
gt	Guatemala
gu	Guam
gw	Guinea Bissau
gy	Guyana
kh	Camboya
hk	Hong Kong
hm	Islas Heard y McDonald
hn	Honduras
hr	Croacia (Hrvatsaka)
ht	Haití
hu	Hungría
id	Indonesia
ie	Irlanda
il	Israel
in	India
io	Territorio británico del Océano Índico
iq	Iraq
ir	Irán
is	Islandia
it	Italia
jm	Jamaica
jp	Japón
jo	Jordania
ke	Kenya
ki	Kiribati
km	Comoras
kn	Saint Kits y Nevis
kp	Corea del Norte
kg	Kirguistán
kr	Corea del Sur
kw	Kuwait
ky	Islas Caimán
kz	Kazajstán
la	Lao
lb	Líbano
lc	Santa Lucía

li	Liechtenstein
ls	Lesotho
lr	Liberia
lt	Lituania
lu	Luxemburgo
lv	Letonia
ly	Jamahiriya Arabe Libia
ma	Marruecos
mc	Mónaco
md	Moldavia
mg	Madagascar
mh	Islas Marshall
mk	Macedonia
ml	Mali
mm	Myanmar
mn	Mongolia
mo	Macao
mp	Islas Marianas Septentrionales
mq	Martinica
mr	Mauritania
ms	Monserrate
mt	Malta
mu	Mauricio
mv	Maldivas
mw	Malawi
mx	México
my	Malasia
mz	Mozambique
na	Namibia
nc	Nueva Caledonia
ne	Níger
nf	Islas Norfolk
ng	Nigeria
ni	Nicaragua
nl	Países Bajos
no	Noruega
np	Nepal
nr	Nauru
nu	Niue
nz	Nueva Zelanda (Aotearoa)
om	Omán
pa	Panamá
pf	Polinesia Francesa
pe	Perú
pg	Papua Nueva Guinea
ph	Filipinas

pk	Paquistán
pl	Polonia
pm	Saint-Pierre y Miquelón
pn	Islas Pitcairn
pr	Puerto Rico
ps	Territorio palestino
pt	Portugal
pw	Palau
py	Paraguay
qa	Qatar
re	Reunión
ro	Rumania
ru	Federación de Rusia
rw	Rwanda
sa	Arabia Saudita
sb	Islas Salomón
sc	Seychelles
sd	Sudán
se	Suecia
sg	Singapur
sh	Santa Elena
si	Eslovenia
sj	Svalbard e Islas Jan Mayan
sk	Sri Lanka
sk	Eslovaquia
sl	Sierra Leona
sm	San Marino
sn	Senegal
so	Somalia
sr	Suriname
st	Sao Tomé y Príncipe
su	Rusia
sv	El Salvador
sy	República Árabe de Siria
sz	Swazilandia
tc	Islas Turcas y Caicos
td	Chad
tf	Territorios australes y antárticos franceses
tg	Togo
th	Tailandia
tj	Tayikistán
tk	Tokelau
tm	Turkmenistán
tn	Túnez
to	Tonga
tp	Timor Oriental

tr	Turquía
tt	Trinidad y Tabago
tv	Tuvalu
tw	Taiwán
tz	Tanzanía
ua	Ucrania
ug	Uganda
um	Islas menores distantes estadounidenses
us	Estados Unidos
uy	Uruguay
uz	Uzbekistán
va	Ciudad del Vaticano
vc	San Vicente y las Granadinas
ve	Venezuela
vi	Islas Vírgenes (británicas)
vn	Vietnam
vq	Islas Vírgenes (EE.UU.)
vu	Balboa
wf	Islas Wallis y Futuna
ws	Samoa
ye	Yemen
yt	Mayotte
yu	Yugoslavia
za	Sudáfrica
zr	Zaire (antiguo)
zm	Zambia
zw	Zimbabwe

Extradición y enjuiciamiento

La capacidad para investigar y enjuiciar los delitos informáticos se puede complicar cuando un mismo delito trasciende una o más fronteras internacionales. Aunque un sospechoso podría estar físicamente sentado ante una computadora en un país, la información a la que accede podría estar en otro país o en otra jurisdicción. En algunos casos, el delincuente informático podría utilizar direcciones de correo electrónico anónimas o tecnologías que lo harían aparecer como que está trabajando en un país diferente al que está en realmente. Al atacar un sistema de esta manera, el delito es más difícil de detectar y de procesar. Otras dificultades inherentes al procesamiento de delitos informáticos internacionales son:

- **La barrera idiomática** La dificultad para comunicarse con el personal de la aplicación de la ley y otros en países cuyo idioma no hablamos.
- **Factores de tiempo** Cualquier investigación de delito informático puede tardar meses e incluso años. Mantener viva la investigación es ya una tarea difícil cuando todas las partes involucradas están en una misma zona geográfica, pero se dificulta aún más cuando es preciso traspasar las fronteras nacionales.
- **Costos** Para investigar un caso quizás sea necesario viajar a otro país o

varios otros países. Pocos organismos policiales tienen incluido en sus presupuestos ese tipo de gastos, excepto para los casos de delitos más graves.

- **Factores políticos** Incluso en el caso en que los organismos encargados de la aplicación de la ley en jurisdicciones diferentes deseen cooperar, podrían estar limitados por factores políticos que se van de sus manos.

En muchos casos, la fuente de un delito podría estar en un país cuya legislación difiere del nuestro, o donde el acto no es considerado delito. Por ejemplo, aunque la pornografía infantil pudiera estar definida como imágenes pornográficas de personas menores de 18 años de edad en América del Norte, la edad legal para posar para tales imágenes en otros países podría ser considerablemente menor. Esta diferencia podría causar un dilema para los oficiales encargados de la aplicación de la ley, dado que es lícito para un sitio web de un país distribuir las imágenes mientras que descargarlas es ilícito para las personas de otro país. Los investigadores pueden arrestar a las personas que tengan en su poder archivos pornográficos, pero quizás no tenga facultades para cerrar el sitio web que esté distribuyendo el material pornográfico.

Si un delito se comete en un país y el delincuente está ubicado en otro, en ocasiones es necesario extraditarlo. No obstante, ello no siempre es posible. La extradición requiere la cooperación del país en el que reside el delincuente. En el caso de la persona que supuestamente creó el Virus del Amor, los oficiales del cumplimiento de la ley de los Estados Unidos trataron de que fuera extraditado desde Filipinas. Como ha sucedido en el caso de numerosos delitos cometidos en un país en los que el delincuente estaba en otro, la solicitud de extradición fue denegada por el gobierno de Filipinas. Muchos países tienen leyes y sentencias distintas a los de los Estados Unidos, para ir pudiera negarse a la extradición si consideran que el castigo que recibirán el delincuente en los Estados Unidos por un delito particular es que otro a tenor de sus leyes. En otros casos, podrían pensar que se sentaría un precedente negativo al entregar sus ciudadanos a una nación extranjera cada vez que se le solicite. Aunque la persona que supuestamente creó el Virus del Amor fue instruida de cargos en Filipinas, como ya apuntamos, algo resultó que no pudo ser procesada porque no existían leyes que se relacionarán explícitamente con la diseminación de virus.

NOTA

A tenor del derecho internacional, los países no están obligados a extraditar a menos que exista un tratado vinculante entre ellos a tal efecto. Esta situación concede un amplio margen de maniobra para conceder o rechazar la extradición. Los tratados de extradición que Estados Unidos ha firmado por lo general requieren que se presenten evidencias que demuestren que la persona acusada ha violado tanto las leyes de Estados Unidos como la ley del país que solicita la extradición. A menudo, los tratados de extradición especifican los delitos particulares por los cuales se puede extraditar a una persona. A diferencia de los Estados Unidos, algunos países europeos procesan a sus propios ciudadanos por delitos cometidos en otros países.

Una vez que el sospechoso es extraditado a nuestra jurisdicción, por lo general se necesita de la cooperación internacional. Quizás los testigos deban ser trasladados desde

otros países. Si ellos deciden no presentarse voluntariamente, se puede emitir una citación oficial. Ignorar esta citación puede conllevar a que la persona sea declarada en desacato al tribunal por un juez, quien puede entonces obtener una orden judicial para arrestar al testigo. Sin embargo, dado que el testigo está en otro país y quizás nunca llegue a estar en el nuestro, la orden judicial no puede ser entregada y de hecho es inútil. El sospechoso de haber cometido el delito podría haber sido extraditado, pero no es seguro que la solicitud de extradición sea concedida en el caso de los testigos que no se han presentado a juicio. Si el testigo no se presenta, será necesario transportarlo hasta el lugar del tribunal y se deberán coordinar alojamiento y alimentación durante el juicio. También quizás sea necesario contratar intérpretes si el testigo no habla nuestro idioma. Todos estos factores incrementan el costo del procesamiento del delincuente, lo cual pudiera hacer que la fiscalía retire los cargos o que nunca llegue a presentarlos.

Resumen

En este apéndice hemos analizado los problemas que surgen cuando los delitos informáticos traspasan las fronteras nacionales. Cuando investigamos un delito informático podríamos encontrar que la persona que lo cometió ha navegado por el ciberespacio traspasando numerosos jurisdicciones y ha cometido delitos utilizando computadoras ubicadas en otros países, a veces con la deliberada intención de evadir la justicia. Cuando los delitos se cometen de esta manera, quizás sea necesario tener en cuenta las leyes de otros países en nuestro intento por arrestar y procesar al sospechoso.

Si bien muchos países carecen de leyes que aborden específicamente el delito informático, esta situación está mejorando a medida que los países modifican las leyes ya existentes y aprueban otras que hacen frente a esta creciente amenaza. En algunos casos, sin embargo, podríamos encontrar que el culpable de un delito no puede ser arrestado o extraditado a causa de las leyes o de las costumbres del país en que reside. En otras situaciones, la cooperación podría ser posible e incluso algo recibido con beneplácito por la policía y los gobiernos de otros países. Es importante contactar a los funcionarios de esos países para determinar el nivel de cooperación que podremos obtener antes de seguir con el caso.

Internet puede ser una herramienta poderosa para adquirir información sobre la legislación y los organismos de aplicación de la ley de otros países. Muchos organismos policiales y de aplicación de la ley en todo el mundo poseen sitios web y direcciones de correo electrónico, que nos permiten contactar a un representante y establecer relaciones de cooperación cuyo valor es inestimable para proceder contra un delincuente informático internacional.

Recursos

- Sección de Delito Informático y Propiedad Intelectual del Departamento de Justicia de los Estados Unidos: Información sobre delitos informáticos cometidos en todo el mundo (Information on cybercrimes committed around the world)
  www.cybercrime.org
- Departamento de Justicia de Canadá: motor de búsqueda para determinar cuáles leyes canadienses se aplican a un delito particular
  http://laws.justice.gc.ca/en/index.html
- Canadian Security Intelligence Service (CSIS)
  www.csis-scrs.gc.ca
- Communications Security Establishment (CSE) of Canada: brinda seguridad informática al gobierno
  www.cse.dnd.ca
- Policía Real Montada del Canadá (RCMP, Royal Canadian Mounted Police): Información sobre la investigación del delito informático y la ayuda a los servicios policiales locales en los casos de delitos relacionados con computadoras, redes y la Internet
  www.rcmp-grc.gc.ca/scams/cpu-cri.htm
- La Policía Metropolitana de Londres (London Metropolitan Police) en Inglaterra: Información sobre delito informático; ofrece ideas para prevenir los delitos e información conexa
  www.met.police.uk/computercrime

- The Police Services of the UK (Servicios policiales del Reino Unido): Vínculos a organizaciones de aplicación de la ley en todo el Reino Unido
  www.police.uk
- Organización Internacional de la Policía Criminal (INTERPOL): Guía de referencia sobre delitos de abuso sexual en los países miembros. Brinda una lista de las leyes por cada país miembro. Es importante observar que las leyes pueden haber cambiado desde la última actualización del sitio y quizás sea necesario contactar con representantes del país sobre el cual estemos realizando la búsqueda
  www.interpol.int/Public/Children/SexualAbuse/nationalLaws
- Europol: Oficina Europea de Policía
  www.europol.eu.int
- Asociación Internacional de Jefes de Policía Criminal: Organización policial con miembros de 100 países
  www.theiacp.com
- Officer.com: ofrece recursos para los oficiales de la aplicación de la ley
  www.officer.com
- Sitio sobre la guerra de la información (The Information Warfare Site)
  www.iwar.org.uk/law/index.htm
- Center for Democracy and Technology (Centro para la democracia y la tecnología)
  www.cdt.org/international/cybercrime
- Investigative Resources International: Vínculos a información factibles de utilizar en las investigaciones
  www.factfind.com/database.htm
- Internet Watch Foundation (IWF): Los usuarios reportan los materiales de pornografía infantil ubicados en cualquier servidor del mundo y el material de contenido racista localizado en cualquier servidor del Reino Unido. Una vez realizado un informe de pornografía infantil, IWF lo revisa para determinar su es ilícito y posteriormente contacta con el ISP que hospeda el sitio y con la policía
  www.internetwatch.org.uk
- Cyber Criminals Most Wanted (Los delincuentes informáticos más buscados)
  www.ccmostwanted.com
- FindLaw: Búsqueda de leyes en un gran número de países
  http://findlaw.com/12international/countries
- Centro de Estudios Estratégicos e Internacionales: Artículos sobre diversos tipos relacionados con el delito y la seguridad informáticos, incluido el terrorismo informático
  www.csis.org
- Moss tingrett (Tribunal de distrito de Moss): sitio noruego que brinda información sobre las leyes relacionados con el delito informático en 43 países
  www.mossbyrett.og.no/info/legal.html
- Sección sobre delito informático de Privacy International
  www.privacyinternational.org/issues/cybercrime

Epílogo

En este libro hemos analizado los antecedentes históricos del delito informático, así como la forma en que los delincuentes que se mueven en el entorno de Internet pueden ser contrarrestados y llevados ante la justicia. ¿Qué nos depara el futuro en términos de la delincuencia en línea? Sin dudas cabría esperar que los delincuentes informáticos y los métodos utilizados para combatirlos sean más sofisticados. También cabría esperar un mayor número de leyes que regulen el comportamiento en Internet. Actualmente los delitos informáticos oscilan entre los que son aparentemente triviales y los que son mortalmente graves, y es probable que en los años futuros ambos tipos se incrementen.

Al momento de imprimir este libro, los funcionarios estadounidenses están actuando cada vez con mayor fuerza contra la práctica crecientemente popular de los estadounidenses de adquirir habanos cubanos en Internet. Desde el decenio de 1960, el embargo comercial de Estados Unidos contra Cuba ha prohibido a los ciudadanos estadounidenses adquirir productos hechos en Cuba, incluso cuando viajan a otros países. Durante años, los aficionados al habano han viajado a Canadá y a otros países para adquirir los altamente cotizados habanos cubanos, pero en años recientes Internet ha facilitado y abaratado la violación de esta ley por parte de los estadounidenses.

Al propio tiempo, el terrorismo informático (tema que hemos esbozado solamente en este libro) está cada vez más presente en las noticias, especialmente durante las últimas semanas. El 27 de junio de 2002, se reportó en el Washington Post que las autoridades están investigando patrones sospechosos de vigilancia –que se originaban en el Oriente Medio y el Sudeste Asiático– contra los sistemas de computación de las empresas de servicios públicos e instalaciones gubernamentales en la zona de San Francisco. Existe un creciente temor de que Al Qaeda y otras organizaciones terroristas estén planificando un intento de asumir el control de componentes de infraestructura vitales mediante las computadoras que los dirigen. Las represas, las estaciones eléctricas, las compañías telefónicas, el control de tráfico aéreo, y las instalaciones nucleares y de gas son solamente algunos de los sistemas vulnerables. El daño que puede hacer un hacker común palidece en comparación con estas posibilidades.

La recientemente creada Oficina de Seguridad Nacional se está apresurando para hacer frente a estas amenazas, conjuntamente con otros organismos. El presidente George W. Bush nombró al primer asesor especial de la presidencia para la seguridad en el ciberespacio, y los funcionarios gubernamentales al parecer están conscientes del grado de dependencia Estados Unidos y de las economías del mundo de los sistemas de redes de computación y las comunicaciones electrónicas.

Mientras tanto, los legisladores a nivel estatal y federal, en los Estados Unidos y otros países, se debaten en otros temas relacionados con el delito informático más mundano. Los mensajes de correo electrónico no solicitados son un asunto que preocupa a los legisladores en todo el mundo. En mayo de 2002, el Parlamento Europeo aprobó una directiva que penaliza el envió no solicitado de anuncios por correo electrónico a personas con quienes la empresa en cuestión aún no tiene una relaciones de negocios. En los Estados Unidos, los primeros intentos por parte de las legislaturas estaduales de California y Washington de aprobar leyes contra los mensajes de correo electrónico no solicitados fueron frustradas por los jueces que dictaminaron que las leyes eran anticonstitucionales –que violaban la inactiva cláusula de comercio de la Constitución que prohíbe a los estados imponer cargas indebidas al comercio interestatal. El gobierno

federal ha asumido esta causa. Comenzando con la Ley de Privacidad de la carpeta de entrada, de 1999, se presentaron varios proyectos de ley ante el Congreso de Estados Unidos, pero por lo general no llegaron a ser aprobados. Mientras escribimos este libro, se presentó otra medida en contra de los correos electrónicos no solicitados presentada por los senadores Conrad Burns, Ron Wyden y Ted Stevens, la cual fue aprobada por el Comité de Comercio del Senado.

Los debates continúan sobre el tema de la pornografía (y el software de filtrado destinado a mantenerlo a raya) en relación con su acceso en las bibliotecas públicas. Se han presentado pleitos judiciales y/o amenazados con presentarlos contra bibliotecas en varias partes del país, tanto por permitir el acceso a la pornografía como por violar los preceptos de la libre expresión al bloquear ese acceso. Los legisladores de muchos estados se han enfrascado en la lucha por determinar si las bibliotecas tienen la obligación legal de proteger a los niños de materiales obscenos u ofensivos disponibles en Internet, y cómo esa obligación se puede reconciliar con la Primera Enmienda. Algunos estados (incluidos Virginia y Arizona) han aprobado leyes que requieren la aplicación de software de filtrado en las computadoras de bibliotecas y escuelas; el Congreso aprobó una ley federal llamaba la Ley de Protección de los niños en Internet (CIPA) que exige el filtrado de la web en las bibliotecas públicas. Se han presentado pleitos judiciales en contra de esas leyes alegando razones constitucionales. Antes de que este libro llegara a la imprenta, un panel de tres jueces en el Tercer circuito de Apelaciones de los Estados Unidos dictaminó que la CIPA era inconstitucional; la próxima apelación será ante la Corte Suprema. Está por ver cuál será la decisión definitiva.

Internet también está siendo cada vez más utilizada para publicar y diseminar información sobre delincuentes acusados y convictos. Muchas localidades están utilizando Internet para avisar al público acerca de la ubicación de la residencia de delincuentes sexuales que tienen registrados. La mayoría de los estados exigen que los convictos por delitos sexuales se registren con el estado después de haber salido de prisión, y mantienen actualizada la información sobre su lugar de residencia. Esta información es hecha pública a la comunidad. Las bases de datos de delincuentes sexuales son populares en los sitios web de estados y municipios. Existen también otros sitios que permite a los usuarios indagar en base de datos de historial delictivo para obtener información pública acerca de todo tipo de delitos (usualmente a cambio de un pago). Un sitio en el condado de Maricopa, Arizona, incluso brindó temporalmente la posibilidad de ver imágenes en vivo mediante una cámara web de los prisioneros en determinadas zonas de la cárcel del condado. En diciembre 2001, el sitio reportó haber recibido 3 millones de visitantes por semana. La "cámara de la cárcel" fue motivo de controversias, y posteriormente de un pleito legal. Un juez retirado presentó el pleito acusando al alguacil del condado de violar los derechos de privacidad de los prisioneros. El sitio que presentó las imágenes en vivo de la vida tras los barrotes de la cárcel ha sido eliminado, aunque el aviso dice solamente que la cámara de la prisión no está disponible "temporalmente".

Los hackers continúan siendo noticia y los sentimientos sobre los delincuentes de alta tecnología son ambiguos. Kevin Mitnick, condenado por numerosos ataques informáticos ampliamente conocidos a finales del decenio de 1980 y los años noventa, ha salido de prisión y está realizando una gira con conversatorios sobre tecnología en

programas como Screen Savers de Tech TV. Su libro titulado *The Art of Deception* debe salir a la luz en el otoño de 2002, y ya estaba entre los más vendidos en una lista de ventas de Amazon.com tres meses antes de su fecha de publicación anunciada. El gobierno está arrestando a hackers, y a los cadetes se les expulsa deshonrosamente del ejército si son sorprendidos en esa actividad. Al propio tiempo, el personal gubernamental y militar frecuentan populares convenciones de hackers como Def Con, que patrocina eventos como "Meet the Feds" (Conozcamos a los federales) e intenta reclutar a hackers talentosos para que utilicen sus conocimientos de manera lícita. Las grandes corporaciones también están contratando a hackers como personal de seguridad.

Estas y muchas otras cuestiones complican el ya complejo mundo del derecho en el ciberespacio en los albores del siglo XXI. Mirando hacia el futuro parece probable que las cosas se harán aún más confusas. Como resultado de la hibridación de las tecnologías de telefonía móvil y de Internet inalámbrica, muy pronto podremos literalmente llevarnos con nosotros Internet a cualquier parte. Es cada vez más evidente que en el mundo de mañana, quien controle la Red controlará nuestras vidas. La demografía en línea está en constante cambio y la brecha digital se está estrechando. La idea de que el acceso de alta velocidad a Internet estaba disponible solamente para una élite o para los adinerados se está desvaneciendo con rapidez. Muy pronto las computadoras conectadas a la red serán algo común como los televisores a color, incluso en zonas de bajos ingresos en los Estados Unidos y otros países del primer mundo. ¿Llegará el día en que nuestras direcciones IP sustituyan a nuestros números de seguridad social y de licencia de conducción como nuestra identificación principal?

Los científicos trabajan ahora en el desarrollo de máquinas basadas en la mecánica cuántica llamadas computadoras cuánticas, las cuales, en teoría, serían capaces de hacer cálculos de números muy diferentes simultáneamente utilizando bits cuánticos, o *qubits*, como la base del procesamiento en lugar de los bits. Un qubit puede existir en más de un estado a la misma vez, a diferencia de los bits regulares que pueden representar solamente a 1 ó 0 a la vez. La mayoría de los expertos concuerdan en que si el trabajo con la computación cuántica llega a ser una realidad, pondrá de cabeza las medidas actuales de seguridad informática. Las máquinas cuánticas podrán descifrar rigurosos algoritmos de encriptación con rapidez y facilidad. Peter Shor, de AT&T Laboratorios, ya ha desarrollado un algoritmo cuántico para la facturación eficiente de grandes números; una computadora que pueda utilizar ese tipo de algoritmos será capaz de realizar en un periodo corto tareas que requerirían ciento de años si usamos una computadora normal. Los tiempos cambian y con cada cambio existe la posibilidad de expandir el universo virtual en un grado jamás imaginado. De algo estamos seguros, sobre la base de la historia: mientras más creció una comunidad más crece la criminalidad que sufre. Y con cada avance tecnológico, la comunidad en línea crece a pasos agigantados.

Todos tenemos interés en ayudar a disminuir el índice de criminalidad informática. El mundo en línea se está convirtiendo rápidamente en nuestra casa lejos de casa. Yo no deseo que Internet se convierta en una zona con tanta criminalidad que todos sintamos temor de permitir que nuestros hijos accedan a ella a jugar, a estudiar y a aprender. En los últimos años, la policía de muchas zonas de los Estados Unidos y otros países han logrado reducir la incidencia general de los delitos en sus comunidades logrando que sus ciudadanos participen en la lucha contra la delincuencia. Considero que

esa misma técnica se puede aplicar al mundo en línea.

Con este libro he deseado reunir a las personas que tienen los conocimientos y la autoridad para hacer lo necesario con miras a lograr que el ciberespacio sea un lugar más seguro y más placentero para todos. Ello incluye al personal técnico que muchas ocasiones será el primero en percatarse de los resultados del trabajo de los delincuentes informáticos, y quienes tienen los conocimientos especializados para ayudar a encontrarlos. Incluye a los oficiales encargados de la aplicación de la ley que tendrán la tarea de recopilar la evidencia para preparar el caso contra un delincuente informático, y quienes deben trabajar estrechamente con los expertos técnicos para garantizar que se agoten todos los medios para encontrar la evidencia y presentarla adecuadamente. Pero también incluye a los legisladores que hacen las leyes que los oficiales de la policía tendrán que hacer cumplir, así como los jueces que supervisarán los juicios, y a los jurados que en última instancia tomarán la decisión sobre la culpabilidad o la inocencia de los acusados de delito informático. Finalmente, nos incluye nosotros, los ciudadanos de bien de la comunidad en línea y todos cuyas vidas están afectadas por el delito informático, de una otra forma.

El delito informático no es simplemente un subtema interesante del derecho penal. Es un problema muy real, que seguirá creciendo hasta tanto los involucrados trabajen de conjunto para recuperar las redes de manos de los delincuentes, de la misma manera que muchas personas que viven en vecindarios que solían ser de alta criminalidad han logrado recuperar su calles.

El delito informático trata de mucho más de lo que pudiera abarcar este libro. Incluso mientras lo escribíamos han ocurrido nuevos acontecimientos en la esfera del delito informático. En cierto sentido, siempre será un proyecto inacabado. Invito a que me envíen preguntas, comentarios y sugerencias sobre cómo puedo mejorar este libro. Sírvanse enviar sus mensajes de correo electrónico a debshinder@sceneofthecybercrime.com. Si desea obtener actualizaciones sobre los temas abordados en el libro y otras noticias sobre delito informático, puede visitar mi sitio web en www.sceneofthecybercrime.com y el sitio web del editor www.syngress.com/solutions.