

ETHICAL HACKING

Buscando esa debilidad

Las simulaciones de ataque a los sistemas por parte expertos informáticos son cada vez más utilizadas para conocer la vulnerabilidad real de las empresas.

Le tomó tres días de trabajo, pero consiguió el trofeo: una foto del desktop, el número de tarjeta de crédito corporativa y el acceso a la casilla de correo del director de la compañía. La falla hubiese tenido consecuencias millonarias, pero sólo costó los honorarios del profesional que llevó a cabo el *ethical hacking*.

Esta modalidad de "hacking ético", que algunas compañías llaman "intrusión testing" es una de las prácticas más utilizadas hoy para medir la real vulnerabilidad de los sistemas informáticos. Consiste en "simular el comportamiento y las acciones de un hacker, buscando todas las maneras de vulnerar, explotar o ingresar a un sistema", define el ingeniero informático Pablo Masoero, presidente de Baicom, una consultora de seguridad en sistemas.

Para Federico Seinfeldin, titular de la firma Openware y director de la Escuela de Hackers de Rosario, "el *ethical hacking* es un concepto amplio, que se refiere a la búsqueda de problemas con el propósito de ayudar. Esto tiene que ver con la esencia de lo que es el hacker: un programador inquieto y empedernido, que quiere descubrir cosas, pero no agredir como el *cracker*", define.

Este tipo de evaluación permite, en períodos acotados de tiempo, hacer un diagnóstico global de los sistemas de información de una empresa, y "es una de



las formas más eficaces para identificar y corregir las vulnerabilidades críticas", señala Nicolás Ramos, del laboratorio de Seguridad informática de la consultora Ernst & Young.

"La ventaja es que se pueden mostrar y cuantificar los riesgos, presentando evidencias reales del acceso obtenido, como capturas de pantalla (*screen shots*), claves de acceso y números de la compañía", dice Luciano Fain, de la misma consultora.

PASO A PASO. El *ethical hacking* incluye diferentes métodos y herramientas, pero el primer paso suele ser recabar información sobre la empresa, identificar los dispositivos y el software utilizado. Luego se evalúan las posibles vulnerabilidades, con técnicas de uso público y otras desarrolladas *ad hoc*.

A partir de allí se puede simular un ataque (según lo convenido con la empresa y siempre evitando dejarla sin sistema). Finalmente se presenta un informe detallado, con las "pruebas" obtenidas, una descripción de las fallas detectadas y recomendaciones para su solución.

Para Seinfeldin, "en la mayoría de los casos no es necesario simular un ataque, porque con un buen diagnóstico se detectan el 80% de las fallas. Lo importante es realizarlo con frecuencia, ya que todas los meses surgen nuevas vulnerabilidades".

PÉRDIDAS MILLONARIAS

- Todos los días se producen unos 200 ataques graves a la seguridad informática de las empresas.
- El 90% de las compañías del mundo son víctimas de algún tipo de ataque informático.
- El 70% de los ataques provienen de Internet.
- Se estima que este año se detectarán 500 nuevas vulnerabilidades.
- En 2004 los ataques provocaron pérdidas que van de los 40 mil a 50 mil u\$s millones.



» "El *ethical hacking* consiste en emular a un hacker, buscando todas las formas de vulnerar un sistema".

PABLO MASOERO



EXPUESTAS. La mayoría de las empresas no saben cuán fácil es ingresar a sus sistemas y hacer pública la información privada.

Por una cuestión de ética, la empresa que implementa las soluciones o parches en el sistema debe ser distinta a la que detectó los problemas.

CAJA DE SORPRESAS. Quienes se dedican al "hacking ético" muchas veces descubren fallas increíbles en empresas que hacen transacciones millonarias y dejan información sensible al alcance de cualquiera. "Sistemas mal configurados, accesos ocultos que instalan los administradores de sistemas para entrar a la com-

OPINIÓN

GUERRILLA INFORMÁTICA

POR CLAUDIO AVIN *



En la actualidad, los ataques informáticos están motivados por un fin más fuerte y suculento que los antiguos graffiti cibernéticos, virus inofensivos que sólo querían transmitir algún mensaje. Hoy el objetivo es el dinero. Obviamente si se trata de obtener grandes sumas, la tecnología y el capital humano utilizado es más grande.

Se espera por lo tanto un crecimiento importante en los fraudes electrónicos, pero ya no a grandes empresas, sino apuntando al usuario final, ya que

este no suele estar al día con todas las medidas de seguridad necesarias, ni al tanto de la correspondiente educación sobre los problemas de la red. Los ataques tienden a dejar de ser realizados a través de mecanismos, sino que ahora se efectúan ataques más pequeños y modulares.

Finalmente, es importante advertir que se están incrementando los ataques a dispositivos móviles tales como los teléfonos celulares, y aunque cueste creer, a las consolas de juegos.

En suma, hoy las amenazas en la red apuntan a nuestros bolsillos, por eso la prevención es el arma más eficaz para los ataques en los tiempos que corren.

* SYSTEMS ENGINEER SYMANTEC
ARGENTINA

putadora de trabajo desde sus casas, *passwords* debajo del teclado, o tan triviales que al tercer intento se adivinan", enumeran los especialistas. "Una multinacional quería saber por qué la competencia siempre le ganaba de mano en el lanzamiento de nuevas ofertas. Llevaban

gastados millones en *firewalls* y sistemas de seguridad", cuenta uno de los especialistas de Baicom. El misterio se develó en la computadora del director de marketing, cuyo password era "rivercapo". **F**

GABRIELA ENSENCK

Fuente: Revista Fortuna
Fecha: 31/10/2005
Pagina: 86