

Se registra un significativo incremento en el crimen electrónico

Según el informe presentado por la revista CSO¹ realizado en cooperación con el Servicio Secreto de los Estados Unidos y el instituto CERT², un significativo número de organizaciones informan un incremento en el crimen electrónico y la instrusión a las redes y los sistemas de información durante el pasado año 2003, con perjuicios y daños que supera los 666 millones de dolares.

Incidentes

Un 70% de las organizaciones encuestadas⁴ informan al menos la ocurrencia de un ataque contra sus instalaciones, en tanto que un 43% reportan un incremento en el número de ataques e intrusiones. Según el Agente Larry Johnson de la División de Investigación del Crimen del Servicio Secreto, existe la tendencia a ocultar los ataques que sufren las organizaciones porque esto puede afectar su reputación, de modo que es muy probable que la cantidad de incidentes sea realmente muy superior.

Cuando a las organizaciones entrevistadas se les pregunta por el tipo de pérdidas experimentadas, un 56% informa perjuicios en su operativa, un 25% pérdidas financieras y económicas y un 12% dicen haber experimentado otros tipos de daño. En cuanto a las medidas de prevención, solo un 51% dicen tener un plan formal de informe y respuesta a los ataques.

Tipos de ataque

Un 77% informan haber tenido problemas con los virus, un 38% con el SPAM, un 44% ataques por denegación de servicio (DoS), un 36% accesos no autorizados desde el interior y un 27% accesos no autorizados desde el exterior.

Quienes son los criminales

Cerca del 30% no conocen el origen de los ataques, en tanto que el 70% que si lo conocen, informan que el 71% provienen del exterior de la organización en tanto que el 29% provienen del interior. Un 40% acusa a los hackers, en tanto que un 31% lo hace con los propios funcionarios o personal contratado.

Monitorización y respuesta

Un 95% dicen monitoriar sistemáticamente sus computadoras y redes⁵ en tanto que un 36% utilizan esta información para despedir a sus mpleados por actividades ilegales, en un 49% de los casos con ayuda de acciones legales.

Tecnología utilizada

El 98% utilizan firewalls, 94% sistemas de seguridad física, 85% encriptan los datos en tránsito, 81% usan sistemas de detección de intrusos (IDS), 71% encriptan la información almacenada, 56% usan autenticación de dos factores, 54% monitorean las conecciones wireless y un 39% monitorean lo que tipean (keystroke) los usuarios.

¹ www.cso.com

² El Centro de Coordinación del Instituto de Ingeniería del Software de la Universidad Carnegie Mellon (CERT/CC) localizado en Pittsburg, Pennsylvania, USA es una de las principales organizaciones encargadas de monitoriar e informar sobre la seguridad en Internet. Participa tambien en programas de Investigación y Desarrollo (R&D) para la solución de problemas de seguridad de la información.

⁴ Sobre un total de más de 500 organizaciones encuestadas, un 67% pertenecen al Sector Privado, en tanto que el 25% tiene menos de 500 empleados.

⁵ Informan destinar a esta tarea entre 1 y 19 personas el 57.4% de los encuestados y más de 100 el 12%.

Mejores prácticas

Los firewalls son considerados como la medida más efectiva por un 71%, la encriptación del flujo de información por un 63%, la encriptación de los datos almacenados por un 56%, la autenticación de dos factores por un 56% y los sistemas de seguridad física por un 48%.

Las cinco políticas y procedimientos más efectivas

El 51% considera que la realización regular de auditorías es la más efectiva de las políticas, el 49% privilegia la realización periódica de penetration tests, un 46% el monitoreo de las conexiones con internet y el 45% confía en los análisis periódicos de Risko.

Las cinco políticas y procedimientos menos efectivas

La monitorización y grabación de las conversaciones telefónicas de los empleados es considerada como la menos efectiva de todas las prácticas de seguridad por más del 50% de los entrevistados, el 20% considera el almacenamiento y revisión de archivos como el procedimiento menos efectivo en tanto que el 17% ve en la redacción de políticas de uso inapropiadas el menos efectivo de los procedimientos.

Traducción libre del artículo

www.csoonline.com/releases/052004129release.htm

por Juan F. Mancebo, Analista en Seguridad de Redes.

jmancebo@adinet.com.uy

Se autoriza la reproducción de este artículo citando la fuente.