El 48% de las empresas ha sufrido màs de 25 ataques de ingeniería social en los dos últimos años

El coste empresarial de estos ataques oscila entre 18.000 y 73.000 euros, teniendo en cuenta la disrupción de negocio, retrasos con clientes, pérdida de ingresos y daños de marca. El phishing y las redes sociales son las principales fuentes de este ti.

Madrid, 22 de septiembre de 2011 – Check Point® Software Technologies Ltd. (NASDAQ: CHKP), líder mundial en seguridad de Internet, anuncia hoy las conclusiones de un nuevo informe que revela que un 48% de las empresas encuestadas ha sido víctima de ataques de ingeniería social y ha sufrido 25 o más ataques a lo largo de los dos últimos años. El coste empresarial de estos incidentes de seguridad está entre 18.000 y 73.000 euros. Al hablamos de este tipo de ataques nos referimos a cuando un estafador, en lugar de utilizar técnicas de hacking, manipula o engaña a los usuarios para que realicen ciertas acciones o divulguen información personal.

El informe “Riesgo de la Ingeniería Social en la Seguridad Informática” señala el phishing y las redes sociales como las principales fuentes de amenazas y anima a las empresas a combinar estrategias tecnológicas y de concienciación para minimizar la frecuencia y el coste de los ataques.

Tradicionalmente, estos ataques tenían como objetivo a personas con información delicada o que tienen acceso a la misma. En la actualidad, los hackers recurren a una amplia gama de técnicas y aplicaciones para obtener información personal y profesional y detectar el eslabón más débil en una organización.

“Los resultados de la encuesta muestran que casi la mitad de las empresas encuestadas son conscientes de que han sufrido ataques de ingeniería social. Sabiendo que muchos de estos ataques pasan desapercibidos, debemos tener en cuenta que este es un vector de ataque muy amplio y peligroso que no debe ser ignorado”, señala Oded Gonda, vicepresidente de productos de seguridad de red de Check Point Software Technologies.

Si bien las técnicas de ingeniería social confían en aprovecharse de las vulnerabilidades de una persona, la omnipresencia de la Web 2.0 y las tecnologías móviles también han incrementado las alternativas de cara a acceder a información personal, creando nuevas vías de penetración para la ejecución de estos ataques concretos. Los nuevos empleados (60%) y contratistas (44%), menos familiarizados con las políticas de seguridad corporativas, fueron señalados como los colectivos más susceptibles de

convertirse en víctimas de estas amenazas, seguidos por personal de contratas, administrativos, recursos humanos y el departamento de informática.

“A fin de cuentas, las personas son un componte crítico del proceso de seguridad, en tanto y en cuanto son susceptibles ser víctimas de los engaños de los criminales y cometer errores que pueden llevar a infecciones por malware o pérdidas de datos no intencionadas. Muchas organizaciones no ponen suficiente empeño en involucrar a sus usuarios, cuando, de hecho, los empleados deberían ser la primera línea de defensa", añade Gonda. “Una buena manera de hacer que los usuarios sean más conscientes de su importancia es involucrarlos en el proceso de seguridad, otorgándoles capacidades para evitar y remediar incidentes de seguridad en tiempo real.”

Principales Conclusiones de Informe:
• Las amenazas son reales – El 86% de los profesionales informáticos y de seguridad son conscientes o muy conscientes de los riesgos que comportan los ataques de ingeniería social. Aproximadamente el 48% de las empresas encuestadas admite haber sufrido más de 25 ataques en los dos últimos años.

• Estos ataques salen caros – Los encuestados cifran entre 18.000 y 73.000 euros el coste de los incidentes de seguridad, teniendo en cuenta costes de disrupción de negocio, retrasos con clientes, pérdida de ingresos y daños de marca.

• Las fuentes más comunes de ataques de ingeniería social – Los correos electrónicos de phishing ocupan el primer puesto en el ranking (47%), seguidos de las redes sociales, donde se expone información personal y profesional (39%) y dispositivos móviles inseguros (12%).

• El ánimo de lucro es la principal motivación de estos ataques (51%) – seguido por el acceso a información propietaria (46%), la obtención de ventajas competitivas (40%) y la venganza (14%).

• Los nuevos empleados son más susceptibles a las técnicas de ingeniería social – Según los encuestados, los nuevos empleados son los más expuestos a estos riesgos, seguidos por los contratistas (44%), secretarios/as de dirección (38%), recursos humanos (33%), altos ejecutivos (32%) y personal informático (23%). Independientemente de su función en la organización, tanto la implementación de programas de formación adecuados, como la concienciación, son componentes críticos en cualquier política de seguridad.

• Falta de formación proactiva para evitar los ataques – El 34% de las empresas carece de políticas de seguridad o programas de formación para prevenir que sus usuarios sean víctimas de las técnicas de ingeniería social, si bien el 19% tiene previsto implementarlos.

Para alcanzar el grado de protección que los entornos informáticos modernos demandan, el concepto de seguridad tiene que ampliarse, otorgándole la misma consideración que a cualquier otro proceso efectivo de negocio, en lugar de

verla como una mera colección de tecnologías dispares. 3D Security de Check Point ayuda a las empresas a implantar un esquema de seguridad que trasciende la tecnología, educando a los empleados involucrándoles en el proceso. “Así como los empleados cometen errores y son responsables de la aparición de amenazas o vulnerabilidades en la organización, también pueden desempeñar un papel crucial en la mitigación de los riesgos”, añade Gonda. Gracias a la tecnología UserCheck™ de Check Point, las empresas pueden informar y educar a sus empleados acerca de las políticas corporativas a la hora de acceder a la red, los datos y las aplicaciones corporativas—ayudando a las empresas a minimizar la frecuencia, los riesgos y los costes asociados a las técnicas de ingeniería social.

Puede acceder al informe y completar el sondeo online aquí: http://www.checkpoint.com/surveys/socialeng1509/socialeng.htm.

“La seguridad no es sólo un problema para los administradores informáticos; sino que tiene que ser parte de las funciones de cada perfil profesional. A medida que las amenazas a las que se enfrenta la industria se hacen más sofisticadas y especializadas, la colaboración de los usuarios incrementa el grado de inteligencia y de efectividad de las tecnologías de seguridad,” concluye Gonda.

Acerca de Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. (www.checkpoint.com), líder mundial en seguridad en Internet, es el único fabricante que se caracteriza por ofrecer una protección completa frente a todo tipo de ataques, que reduce la complejidad de la seguridad y, por tanto, el coste total de la propiedad. Check Point fue pionero en la industria con FireWall-1 con su tecnología patentada, Stateful Inspection. En la actualidad, Check Point continúa innovando con el desarrollo de la arquitectura de Software Blade. La arquitectura dinámica Software Blade está compuesta por soluciones de seguridad sencillas y flexibles, completamente adaptables a las necesidades concretas de cada cliente o entorno.

Check Point es el único proveedor que va más allá de la tecnología definiendo la seguridad como un proceso de negocio. La Seguridad 3D de Check Point combina la política, las personas y el cumplimiento para una mayor protección de los activos de información, ayudando a las organizaciones a implementar un plan de seguridad alineado con las necesidades del negocio. Entre los clientes de Check Point se cuentan miles de organizaciones de todos los tamaños, incluidas todas las empresas del Fortune 100. Las soluciones ZoneAlarm defienden millones de PCs de hackers, spyware y posibles robos de identidad