¿Qué tan seguras son sus redes sociales?

Cómo protegerse de los delincuentes cibernéticos.

Según un informe realizado por Blue Coat Systems, la mayoría de las pequeñas y medianas empresas no cuentan con políticas formales para proteger su actividad en las redes sociales de los ataques de hackers y otras amenazas. Aquí, un resumen de lo relevado por la compañía.

El uso de redes sociales es una herramienta indispensable para una comunicación más eficiente. Sin embargo, estos sitios tienen altos índices de vulnerabilidad, y facilitan a los ciberdelincuentes el acceso a las cuentas de los usuarios. Una vez que el hacker obtiene entrada a una cuenta, puede extraer más información e infiltrarse en otras cuentas.

Las empresas deberían revisar sus políticas de seguridad sobre la utilización de Internet por parte de sus empleados: según un relevamiento realizado por Blue Coat Systems, el 87% de las pequeñas y medianas empresas no cuentan con políticas formales para el uso de Internet y 70% de éstas carecen de políticas para empleados sobre el uso de las redes sociales.

Aunado a esto, los empleados utilizan cada vez más sus propios dispositivos móviles para uso de la compañía, lo cual incrementa la información disponible en las redes sociales y expone aún más a las empresas.

El uso cada vez más habitual de dispositivos móviles para difundir información de la empresa potencian la intromisión de ciberdelincuentes

Las 10 peores amenazas detectadas actualmente en redes sociales son las siguientes:

1- Virus de redes sociales: a través de *Botnets* o robots informáticos, los hackers pueden tomar el control de las computadoras y enviar correos que inciten a hacer clic en un enlace determinado.

2- *Phishing bait*: es el mail que lleva al usuario entrar a su cuenta de Facebook, esperando que éste no logre identificar correctamente la página en su buscador y así obtener su contraseña.

3- *Trojans*: la zona URL es similar a un banco *Trojan*, pero más astuto. Puede calcular el valor en la cuenta de su víctima y ayudar a decidir la prioridad para el ladrón.

4- Filtración de información: los usuarios comparten demasiada información acerca de la organización. En las redes, pueden llegar a filtrarse proyectos, producto, finanzas y otra información sensible.

5- Abreviación de enlaces: los servicios que ayudan a abreviar enlaces para que quepan en lugares más pequeños (Bit.ly, Tinyurl), también funcionan escondiendo los enlaces *malware*, lo cual puede hacer que las víctimas no se den cuenta de que están haciendo clic para instalarlo.

6- *Botnets* en Twitter: las cuentas de twitter han sido usadas para dirigir y controlar los canales de algunos botnets.

7- Amenazas avanzadas persistentes (ATP): es la inteligencia que recopila datos de personas de alto nivel (ejecutivos, oficiales o individuos de alto poder adquisitivo), quienes pueden llegar a ubicar información importante en sus cuentas de redes sociales.

8- Cruce de páginas web para falsificación de solicitudes (CSRF): este tipo de ataques aprovechan la confianza que brindan las aplicaciones de las redes sociales al ingresar en el buscador de los usuarios. Cuando la aplicación de las redes sociales no refleja el encabezado del sitio referido, es más fácil iniciar un ataque. En el momento en que un usuario comparte una imagen en una secuencia de eventos, otros usuarios podrán hacer clic para difundirlo.

9- Impostores: muchos han recolectado cientos y miles de seguidores en twitter haciéndose pasar por terceros. Los personificados pueden verse afectados de distintas maneras por la falsificación de su identidad.

10- Confianza: cuando un correo electrónico se vuelve popular, las personas confían en los enlaces, las fotos, los videos y ejecutables; consideran que viene de parte de "amigos". ■

PROHIBIR NO ES UNA OPCIÓN

Ignacio Conti, *Regional Manager SoLA en Blue Coat Systems*

Actualmente, es impensable una comunicación sin redes sociales. Dado que las compañías conviven con esta realidad, el viejo estereotipo de la política de seguridad basada en el no resulta obsoleta.

Las redes sociales son una puerta de entrada al hackeo, lo que obliga a las empresas a tomar ciertos recaudos en materia de seguridad informática. El fenómeno del BYOD (*Bring Your Own Device* o Traiga Su Propio Dispositivo), que consiste en el uso de los dispositivos móviles personales de los empleados para asuntos de trabajo, cambió en forma radical el manejo de las redes internas de las organizaciones. En estos casos, la vulnerabilidad de las redes sociales afecta no solamente a sus usuarios directos, sino que pone en riesgo la información de la compañía.

En tal sentido, es preciso que las empresas cuenten con soluciones de seguridad para resguardarse de riesgos como la introducción de aplicaciones maliciosas, las cuales pueden generar pérdidas de información, afectar su imagen o producir perjuicios económicos. No continuar las cadenas de mensajes de origen dudoso, elegir claves de acceso difíciles de descifrar o cerrar las sesiones cuando no se usa la red son algunos consejos útiles para el uso responsable de las redes sociales. También se recomienda tener los instrumentos correspondientes de protección en los dispositivos móviles (como antivirus y filtrado de contenidos).

Sin dudas, hoy es fundamental contar con herramientas que estén a la vanguardia y que contemplen el contexto actual de una Internet móvil, colaborativa, de uso laboral y social, bajo un entorno de las nuevas políticas de seguridad. Blue Coat Systems ha marcado tendencia al servicio del sector TI, gracias a soluciones innovadoras, capaces de afrontar un fenómeno que llegó para quedarse.