

Proteja a su empresa del robo de datos

Los archivos electrónicos son altamente deseados por los ladrones de datos por la gran riqueza de información personal que contienen. Hay archivos de Recursos Humanos, información financiera, clientes, lista de suplidores, etc.

Todos estos tipos de registros tienen mucha información sensible que puede ser empleada para beneficio personal de los ladrones de datos.

Como un dueño de un negocio, usted está consciente de cómo proteger su compañía de un robo físico, pero los ataques electrónicos no son tan bien entendidos o la mayoría de las compañías no se protegen de ellos. Los elementos más atractivos para un ladrón de datos son:

No se necesita estar cerca de la víctima; se puede inclusive estar en otro continente.

Muchas de las informaciones que se necesitan para cometer un robo de identidad, están en la web.

La mayoría de las compañías mantienen una gran cantidad de información sensible en archivos los cuales están pobremente protegidos.

Las computadoras pueden ser un punto de entrada fácil hacia tus datos, los ladrones solo necesitan encontrar un punto débil para entrar en tu sistema.

Técnicas más comunes usadas por los ladrones de datos:

Correos electrónicos de phishing – Estos falsos correos pretenden ser de compañías legítimas pidiendo a la víctima que verifique su información personal.

Spear phishing – Estos son correos enviados a empleados de una compañía pretendiendo ser de la administración, pidiendo contraseñas o información sobre proyectos.

Computadoras zombies o redes zombies – Estas son computadoras comprometidas y redes que contienen programas que permiten a los delincuentes acceder al sistema. Estas computadoras pueden estar relacionadas entre ellas y así formar lo que se llama botnet.

Botnet – Una vez comunicadas entre sí, estos botnets son usados como plataforma para lanzar ataques de denegación de servicio (DOS), pagar por clics o correo spam. En muchos casos el dueño de la computadora comprometida no sabe que su sistema está siendo usado para estos fines.

Sitios web falsos. Sitios que pretenden ser legítimos y engañan a los usuarios para obtener información personal. Estas informaciones, una vez obtenidas son usadas por los delincuentes en el sitio real.

Crackers – Son programadores y expertos en computadoras que usan sus habilidades para penetrar en redes y encontrar sus puntos débiles a explotar.

Rastreo de redes inalámbricas – Cuando se usan routers inalámbricos desprotegidos, tal como encontramos en cibercafés, aeropuertos y en algunas casas, los hackers pueden espiar en tu computadora.

Rastreo de galletitas (cookie sniffing) – Los hackers usarán rastreadores de galletitas para examinar todas las galletitas que has usado y enviarán esta información (útil ya que generalmente las personas usan la misma clave para diferentes sitios) a sus sistemas para usar esta información.

Programas maliciosos – Estos son varios tipos de programas: hijackers, adware, troyanos, etc. los cuales actúan en contra de las funciones del sistema operativo, envían información personal a alguien fuera de tu sistema, te dirigen a sitios falsos o cualquier otro tipo de acción maliciosa.

Secuestradores de páginas web – Es un programa pequeño que redirecciona tu navegador a un sitio diferente al que querías visitar. Este puede ser un sitio web falso que atenta a capturar tu información personal o que te direcciona a un sitio pornográfico.

Acceso piggybacking – Esta es una práctica de penetrar en un computador poco seguro para acceder a una red externa y usando este último computador como una conexión legítima entre las dos redes.

Sitios de investigación de personas – Por un precio de entre USD\$ 40 y \$80 usted puede obtener información personal sobre casi cualquier persona.

Ataque de diccionario – Es una de las formas más fáciles de adivinar una contraseña/ Un archivo de diccionario es cargado y como ningún lenguaje tiene un número ilimitado de palabras, este frecuentemente puede generar la clave con relativa facilidad.

Ataque híbrido – Es una variante más sofisticada del ataque de diccionario, este toma las palabras del diccionario y las combina con números y símbolos en un intento de romper o penetrar un sistema protegido por una contraseña.

Ataque de fuerza bruta – Este es un ataque en el cual un programa sistemáticamente trabaja con cada combinación posible de números, letras y símbolos. La cantidad de tiempo que se necesita para encontrar la clave depende del número de caracteres usados en la misma.

Keyloggers o recolectores de teclazos – Este es un tipo de spyware el cual graba cada pulso del teclado hecho en una computadora y envía esta información a un usuario remoto. Estos programas son muy difíciles de detectar por la mayoría de los antivirus y rastreadores de spyware.

Rastreadores de redes (sniffers) – Son aplicaciones usadas para capturar el tráfico de la red sin el conocimiento

de los usuarios. Estos sniffers son muy útiles para los hackers para encontrar debilidades de las redes, lo cual les ayuda a planear otros ataques en una red.

Consejos para evitar robos de datos:

Puede contratar un consultor externo de seguridad para analizar y mejorar la seguridad en su compañía.

Mantener actualizado todos los programas en sus computadores.

Usar programas de seguridad tales como: antivirus, firewalls, etc.

Encriptar toda información sensible.

Usar tokens o tarjetas de acceso a su red y estaciones de trabajo.

Entrenar apropiadamente a cada uno de sus empleados para que sepan que cuidar y así poder prevenir robo de informaciones.

Fuente: <http://www.tecnoseguridad.net/>