



Riesgos y amenazas de la fuga de información en las empresas

EL 68% DE LAS EMPRESAS SE PONEN EN RIESGO AL SUBESTIMAR LA AMENAZA QUE SUPONE PARA LA SEGURIDAD DE SUS DATOS LOS DISPOSITIVOS MÓVILES DE ALMACENAMIENTO



Simon Reed

VICEPRESIDENTE DE INGENIERÍA
GFI Software

En el mundo digital actual el riesgo de brechas de seguridad, fugas o pérdidas de información nunca ha sido mayor. No sólo se ha multiplicado el volumen de información en circulación sino también el número de vías en las que la información puede ser almacenada y transferida sin el consentimiento del propietario.

A pesar de la mayor concienciación sobre los riesgos y amenazas a la seguridad que encaran las empresas y firmas profesionales de todo el mundo, las brechas de seguridad están aumentando y amenazando seriamente la solidez de los negocios y la privacidad de sus clientes.

Aún cuando los administradores de TI tienen a su disposición un extenso arsenal de soluciones de seguridad, los cibercriminales todavía atacan sistemas y roban valiosa información que pueden utilizar para fraude con tarjetas

de crédito, robo de identidad y otras actividades maliciosas. Las empresas de cada sector continúan informando de vulnerabilidades de seguridad y aun así, todavía permiten la exposición de su información más sensible y confidencial.

Los usuarios informáticos pueden considerarse como la menos predecible y controlada vulnerabilidad de seguridad

Algunos ejemplos de fuga de información

La creciente proliferación de dispositivos móviles de almacenamiento como *sticks* USB, unidades *flash* y PDAs entrañan un gran riesgo para las empresas, ya que según estudios realizados en la Unión Europea, el 49% de los empleados se lleva información cuando cambia de trabajo, poniendo así en riesgo la imagen y la integridad de la compañía.

Como ejemplo de esta situación cabe citar el caso de un ex-empleado de Boeing, acusado de robar 320.000 archivos y filtrarlos a un periódico, copiando la información sensible en una unidad extraíble, y violando así las directivas de seguridad de la compañía. La firma calculó que el daño potencial podría suponer entre 5 y 15.000 millones de dólares.

Sin embargo, la mayoría de las empresas no son conscientes de este peligro ya que según los últimos estudios realizados, el 68% de las empresas se ponen innecesariamente en riesgo al subestimar la amenaza que supone para la seguridad de sus redes los ya citados dispositivos móviles de almacenamiento.

El elemento humano en la seguridad de red

Los usuarios informáticos pueden considerarse como la menos predecible y controlada vulnerabilidad de seguridad. En la mayoría de casos, una falta de información y un desconocimiento de los principios y procedimientos básicos de seguridad son las principales causas de los agujeros de seguridad en lugar de la



actividad maliciosa (aunque esto último no se puede ignorar). Sin embargo, el resultado final es habitualmente el mismo: se pierde información inestimable, la empresa pierde credibilidad, etc.

Aunque no lo parezca, es realmente fácil que se produzca una vulneración de la seguridad de las redes de información de una compañía. Es habitual la pérdida de grandes cantidades de información porque los empleados ponen sus contraseñas en adhesivos sobre sus monitores, olvidan portátiles o dispositivos de mano en aeropuertos, gimnasios y restaurantes o en sus coches. También mantienen sus equipos desbloqueados o encendidos durante almuerzos, dejan sin atención sticks USB con información empresarial sensible o navegan por Internet desde sus casas mientras están conectados a sus redes empresariales.

Las repercusiones

Las empresas afectadas por vulnerabilidades de seguridad pueden esperar el pago de un alto precio y sufrir las consecuencias de la erosión de la confianza, de la marca, pérdida de negocio y, en algunos casos, sanciones civiles e incluso criminales. Un estudio de Forrester Research entre 28 empresas que tuvieron algún tipo de fuga de información destaca que la brecha media puede costar entre 60€ y 205€ por registro perdido. Aunque cada empresa valora diferentemente su información, la pérdida de información sensible puede tener un impacto devastador en el balance de una organización.

Abordar el problema

Las empresas necesitan tomar medidas preventivas de seguridad para evitar que ocurran estas fugas mediante la pertinente información a



sus empleados en materia de seguridad y barreras tecnológicas que impongan la directiva de la empresa. Es necesario hacer un mejor uso de las herramientas que están

Las vulnerabilidades en materia de seguridad y el robo de información pueden ocurrir en cualquier momento

disponibles para los equipos informáticos y comenzar a ver la seguridad como una inversión en lugar de como un gasto.

Alcanzar la óptima seguridad de red se alcanza con la gestión de riesgos y éste es un proceso continuo que incluye:

- Valoración minuciosa y continua de dónde residen los riesgos
- Establecimiento de barreras para mitigar los riesgos
- Tomar una aproximación proactiva a la seguridad en general

Los individuos maliciosos llegarán muy lejos para conseguir su acceso a las redes, utilizando todas las formas

de subversión y ataque posibles. Por ello, las empresas tienen que asegurar que todas las brechas están cubiertas, todos los sistemas están parcheados, todas las cuentas de sistema no utilizadas están deshabilitadas y por último, pero no menos importante, asegurar que los partícipes de la empresa son conscientes de las amenazas y están formados para contrarrestarlas.

Cada empresa debe poner en marcha una directiva eficaz de seguridad empresarial y darla a conocer a todos los partícipes de la empresa -y consecuentemente no fiarse de su buena voluntad para cumplir esta directiva. Más importante, esta directiva *debería* cubrir y forzar conceptos que ya *deberían* estar en vigor en todas las redes empresariales.

Las vulnerabilidades en materia de seguridad y el robo de información pueden ocurrir en cualquier momento. Sin embargo, hay formas eficaces de limitar el riesgo de que alguien desde algún lugar esté esperando pacientemente para infligir serios daños en la red de la compañía y robar información. Con la adecuada política de seguridad, las empresas pueden proteger satisfactoriamente sus negocios de daños financieros, legales y salvaguardar su reputación. ♦