Alerta de delitos informáticos:

6 debilidades que los hackers aman

¿Crees que los hackers no te molestarán porque tu pequeña empresa es insignificante? Piénsalo bien. Los delitos informáticos dirigidos a pequeñas empresas están aumentando. Una encuesta realizada en 2016 por Ponemon Institute LLC y patrocinada por Keeper Security reveló que 50% de las pequeñas y medianas empresas reportó robo de datos durante los últimos 12 meses, y 55% de los que respondieron a la encuesta también dijo haber experimentado ataques informáticos durante los últimos 12 meses.[1]

Mientras tanto, las consecuencias financieras de los delitos informáticos podrían ser perjudiciales:

- Los ataques cibernéticos les cuestan a las pequeñas empresas alrededor de $7,000 USD en promedio.[2]
- Cuando también atacan las cuentas bancarias de estas pequeñas empresas, las pérdidas ascienden a $32,000 USD en promedio.[2]
- Las empresas que han experimentado un delito informático o robo de datos que acabó en daño o robo de activos de TI gastó en promedio más de $879,000 USD en arreglar los daños causados.[1]

En algunos casos, estas cifras pueden ser devastadoras, ya que un estudio descubrió que 60% de las pequeñas empresas que experimentan robo de datos quiebran en seis meses.[3]

¿Qué hace que tu negocio sea un blanco tan tentador para los criminales informáticos? Pero lo más importante es saber qué podemos hacer para evitarlo. A continuación mencionaremos seis debilidades que te pueden hacer vulnerable a los hackers, y también te daremos tips para defenderte de estos ataques.

1. No invertir lo suficiente en medidas de seguridad

Las pequeñas empresas redujeron su presupuesto en seguridad durante los últimos años, mientras que las grandes empresas han aumentado sus inversiones. Como las grandes empresas se han convertido en blancos difíciles de atacar, los criminales informáticos están atacando a las empresas más vulnerables.

– **La mejor defensa:** Destina un presupuesto adecuado a la seguridad informática.

2. Sin protección TI

Es menos probable que las pequeñas empresas cuenten con especialistas en TI internos que se encarguen de los riesgos y las tendencias de seguridad.

– **La mejor defensa:** Contrata seguridad externa con socios de TI confiables. Usa actualizaciones automáticas y software de seguridad para proteger tus datos de manera continua.

3. Aumenta tu uso en la nube

Las pequeñas empresas están usando soluciones de almacenamiento en la nube con más frecuencia. El uso de almacenamiento en la nube y las aplicaciones de datos compartidos tiene sus beneficios, solo asegúrate de que las soluciones que elijas están diseñadas para uso empresarial, ya que de lo contrario podrían poner tus datos en riesgo.

– **La mejor defensa:** Usa almacenamiento en la nube empresarial y soluciones y aplicaciones de datos compartidos.

4. Conexiones de red extendidas

Los datos de los dueños de pequeñas empresas se han vuelto más conectados. Por ejemplo, los sistemas actuales de los puntos de venta (POS) y las impresoras incluyen software que las vuelve vulnerables porque están conectadas a una red, son compartidas y están conectadas a muchas otras aplicaciones dentro de la empresa.

– **La mejor defensa:** Elige impresoras que tengan seguridad integrada y empresarial como detección de intrusiones durante la ejecución y funciones de seguridad de reparación automática. Compra hardware POS que incluya estándares de cumplimiento para la industria de tarjeta de pago (PCI) y que soporte dispositivos que admitan PCI. Limita las conexiones entre tus datos del sistema de pago POS y otros sistemas que haya en tu empresa.

5. Uso de tecnología personal

Los dueños de pequeñas empresas tienden a usar tecnología del consumidor para sus negocios sin tomar en cuenta los riesgos de seguridad porque es más económico.

– **La mejor defensa:** No prestes tu laptop a tus hijos, mejor compra computadoras creadas para las empresas que estén diseñadas para proteger tus datos, tu identidad y tus dispositivos. Compra tecnología con seguridad local (integrada) y funciones de seguridad tales como software de seguridad precargado y sistemas básicos de protección (BIOS) de entrada y salida que te permita bloquear tu disco duro, limpiar datos cuando sea necesario y habilitar una amplia variedad de opciones de autenticación.

6. Permite el acceso de datos

Las pequeñas empresas tienden a ser más descuidadas con la seguridad física. Todos se conocen en tu empresa, ¿no es así?

– **La mejor defensa:** Evita los delitos informáticos internos al limitar el acceso físico a tus datos. Mantén el cuarto de los servidores cerrado y solo permite el acceso a los empleados que lo necesitan. Si mantienes los respaldos físicos ahí mismo, bloquéalos. Protege los dispositivos y los datos portátiles usando una protección física sencilla como cubiertas de seguridad para tablets o candados para laptops.

No importa qué tan pequeña sea tu empresa, lo importante es que te tomes la seguridad informática en serio porque así protegerás lo que tanto te costó construir.

Fuentes

[1]Keeper Security LLC y Ponemon Institute, "The 2016 State of SMB Cybersecurity," https://signup.keepersecurity.com/state-of-smb-cybersecurity-report/.

[2]National Small Business Association, "2015 Year-end Economic Report," http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.

[3]StaySafeOnline.org, "America's Small Businesses Must Take Online Security More Seriously," https://staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic.

¿Quieres más tips de los expertos en tecnología?
Suscríbete a nuestro boletín gratuito de Tecnología HP en el trabajo.

4AA7-0519SPL, Julio 2017