ENJOY SAFER TECHNOLOGY™

GUÍA DE CIBERSEGURIDAD PARA PEQUEÑAS EMPRESAS

Por Stephen Cobb, Investigador de Seguridad Senior de ESET

Si bien las computadoras e Internet les brindan muchos beneficios a las pequeñas empresas, estas tecnologías no están exentas de riesgos. Algunos de ellos, como el robo físico de equipos y los desastres naturales, se pueden reducir o controlar si uno se maneja con cautela y precaución, como dicta el sentido común. Así y todo, los riesgos resultantes del crimen cibernético, como el robo de información que luego se vende en el mercado negro, son más difíciles de controlar.

Más del 70% de las violaciones de seguridad están dirigidas a las pequeñas y medianas empresas; a pesar de ello, muchos empresarios creen que no son vulnerables a los ataques cibernéticos debido a su tamaño pequeño y sus activos limitados.[1] Lamentablemente, no es así.

Esta guía de seguridad cibernética lo ayudará a defender su empresa contra las amenazas del crimen cibernético.

La información personal que puede ser utilizada para robar su identidad, es uno de los objetivos principales de los delincuentes, e incluso las pequeñas empresas muchas veces almacenan datos de clientes o proveedores que son valiosos para robar. Otro objetivo de los ciberdelincuentes es la **información de cuentas**, que incluye datos de **tarjetas de crédito**, **números de cuentas bancarias**, **claves de banca online**, **cuentas de e-mails** y **credenciales de usuario** para servicios como *eBay*, *PayPal* y *TurboTax*. Todos estos datos están en riesgo.

1 Predicción de pequeñas y medianas empresas estadounidenses de 2014 a 2018; por IDC

Una vez que obtienen los datos, los ciberdelincuentes los venden a otros que se especializan en usarla para cometer una amplia gama de fraudes y estafas.

Consecuencias del robo de datos

Como casi todas las pequeñas empresas, la suya seguramente también maneje información de cuentas y datos personales de interés para los delincuentes. Por eso, recuerde que sufrirá las consecuencias del robo de datos, por ejemplo, si los ciberdelincuentes roban la información sobre sus clientes y la utilizan para cometer fraudes.

Algunos datos están protegidos por leyes y regulaciones, como el **Reglamento General de Protección de Datos Personales o GDPR** en la Unión Europea, o la **Ley de portabilidad y responsabilidad de seguros médicos** o **HIPAA** (para datos médicos) y el **Estándar de seguridad de datos para las tarjetas de pago** o **PCI** (para datos de tarjetas de crédito) en los Estados Unidos. También hay regulaciones que obligan a las empresas a informar si sufren una violación de seguridad que pueda llegar a exponer datos personales, aunque solo se trate de la pérdida de una computadora portátil con información de clientes o de una memoria con registros médicos.

Esto demuestra que, más allá de lo pequeña que sea su empresa, deberá adoptar un enfoque sistemático para proteger los datos que se le confían. Además, a medida que vaya protegiendo los activos digitales corporativos, deberá documentar el enfoque implementado. Esto lo

ayudará a capacitar a los empleados sobre sus responsabilidades en materia de seguridad.

También es muy común que las empresas más grandes les exijan a los partners y proveedores pruebas de que han capacitado a sus empleados e implementado las medidas de seguridad necesarias. De esta forma, si se llegara a producir una brecha de seguridad, esta documentación de las políticas aplicadas lo ayudará a demostrar que actuó con diligencia para proteger la información.

Pasos a seguir

Los siguientes pasos lo ayudarán a proteger su empresa ante las amenazas de seguridad cibernética.

- **Analice** sus activos, riesgos y recursos
- **Cree** sus propias políticas
- **Elija** sus controles
- **Implemente** los controles
- **Capacite** a sus colaboradores, ejecutivos y proveedores
- **Evalue, audite y pruebe**

Analice sus activos, riesgos y recursos

Haga una lista de todos los sistemas y servicios informáticos que utiliza. Asegúrese de incluir los dispositivos móviles (como los *smartphones* y las *tablets*) que tanto usted como sus colaboradores pueden llegar a usar para acceder a información corporativa o de los clientes.

Esto es importante porque se estima que el **60%** de los empleados evitan las funciones de seguridad en sus dispositivos móviles, y el **48%** deshabilita la configuración requerida por el empleador.[2]

No olvide los servicios online (como *SalesForce* y los sitios web de banca online) y los servicios en la nube (como *iCloud* o *Google Docs*).

Una vez finalizado, lea la lista y piense en los riesgos asociados a cada elemento. ¿Quién o qué es la amenaza? o ¿qué podría salir mal? Algunos riesgos son más probables que otros: clasifíquelos y enumérelos según el daño que podrían causar y su probabilidad de ocurrencia.

Es posible que necesite ayuda externa para este proceso, por lo cual deberá hacer otra lista con los recursos que tenga disponibles para resolver los problemas de seguridad cibernética. Puede incluir algún colaborador, partner o proveedor con conocimientos sobre seguridad.

Finalmente, capacite a sus empleados y asegúrese de que todos estén al tanto de las mejores prácticas de seguridad.

¿POR QUÉ ES IMPORTANTE LA AUTENTICACIÓN EN DOS FASES?

Para las pequeñas empresas en particular, la autenticación en dos fases (2FA) constituye un elemento esencial para proteger los datos y evitar violaciones de seguridad.

La implementación de la 2FA añade una capa adicional de seguridad, ya que requiere que el usuario ingrese una contraseña de un solo uso generada al azar además de su nombre de usuario y contraseña habituales.

Muchas de las brechas de seguridad de conocimiento público que tuvieron lugar en los últimos meses podrían haberse evitado si las empresas hubieran tenido implementada la 2FA. De esta forma, aunque los atacantes hubieran logrado infectar una computadora y robar una contraseña, no habrían podido acceder a la cuenta asociada ya que no sabrían el código de acceso de un solo uso.

Al agregar la 2FA a su solución de seguridad actual, no solo protegerá los datos, sino que también lo ayudará a cumplir con las reglamentaciones que exigen el uso de autenticación de múltiples factores y además impedirá que personas externas accedan a computadoras portátiles y otros dispositivos perdidos o robados.

2 El costo de los dispositivos móviles sin protección en el lugar de trabajo, según el Instituto Ponemon, 2014

Cree sus propias políticas

Un programa de seguridad comienza con la aplicación de políticas, y para ello se necesita que los directivos de la empresa las aprueben. Transmita que le preocupa la seguridad y que su empresa se compromete a proteger la privacidad de todos los datos que maneja. Detalle las políticas que desea aplicar, por ejemplo, que no se permita el acceso no autorizado a los sistemas y datos corporativos, y que los empleados no puedan desactivar la configuración de seguridad en sus dispositivos móviles.

Elija sus controles

Use controles para hacer cumplir las políticas. Por ejemplo, si desea aplicar una política para impedir el acceso no autorizado a los sistemas y datos corporativos, puede optar por controlar todo el acceso a los sistemas de la empresa mediante la solicitud de un nombre de usuario, una contraseña y alguna forma de autenticación en dos fases (ver apartado).

Para controlar qué programas tienen permiso de ejecutarse en los equipos de la empresa, puede decidir no darles derechos de administrador a los colaboradores. Para evitar las filtraciones causadas por dispositivos móviles perdidos o robados, podría exigirles a los colaboradores que reporten el incidente en el mismo día, y comuníqueles que el dispositivo se bloqueará y el contenido se borrará de inmediato y en forma remota.

Como mínimo, debería utilizar tres tecnologías de seguridad básicas:

- Software *antimalware* para evitar la descarga de códigos maliciosos en los dispositivos
- Software de cifrado para evitar accesos a los datos de los dispositivos robados
- Un sistema de autenticación en dos fases para requerir algo más que un nombre de usuario y una contraseña cuando alguien desee obtener acceso a sus sistemas y datos.

Implemente los controles

Cuando implemente los controles, asegúrese de que funcionen correctamente. Por ejemplo, si tiene una política que prohíbe el uso de software no autorizado en los sistemas de la empresa, uno de sus controles será el software *antimalware* que busca códigos maliciosos. No solo debe instalarlo y probar que no interfiera con las operaciones normales, sino que también tiene que documentar los procedimientos que los empleados deberán seguir en caso de que el *software* detecte *malware*.

Capacite a sus colaboradores, ejecutivos y proveedores

Su personal necesita saber algo más que las políticas y los procedimientos de seguridad de la empresa. Invierta en capacitación y concientización sobre seguridad: la medida más importante y efectiva que una empresa puede implementar.

Por ejemplo, cree conciencia sobre temas como los correos electrónicos de *phishing*. Un estudio reciente demostró que el **21%** de los correos electrónicos de *phishing* enviados a empleados fueron abiertos y que el **16%** de los destinatarios abrieron el archivo adjunto[3]. Ambas cosas aumentan considerablemente las posibilidades de que se produzca una filtración de datos y se robe información.

Asegúrese de capacitar a todos los que usen sus sistemas, incluyendo directivos, proveedores y partners, y recuerde que el incumplimiento de las políticas de seguridad tiene consecuencias estrictas.

Evalúe, audite y pruebe

Para cualquier empresa, ya sea grande o pequeña, la seguridad es un proceso continuo, no un proyecto que se hace una sola vez. Mantengase actualizado sobre las amenazas emergentes, subscríbase a portales como *WeLiveSecurity.com/latam*, *KrebsOnSecurity.com* y *DarkReading.com*.

3 El costo de los dispositivos móviles sin protección en el lugar de trabajo, según el Instituto Ponemon, 2014

Es posible que necesite actualizar sus políticas de seguridad y sus controles más de una vez al año, dependiendo de los cambios en la empresa, como las relaciones con nuevos proveedores, nuevos proyectos, contratación de empleados o empleados que dejan la empresa (por ejemplo, revocar todos sus accesos al sistema cuando se van). Considere contratar a un consultor externo para realizar una auditoría de seguridad para detectar los puntos débiles y poder abordarlos.

Por lo que podemos ver, la ola de delitos informáticos no va a terminar en un futuro cercano, de modo que debe hacer un esfuerzo continuo de buena fe para proteger los datos y los sistemas, que son el alma de las pequeñas empresas de hoy.

Stephen Cobb ha estado investigando la seguridad de la información y la privacidad de los datos por más de 25 años, y ha asesorado a las agencias gubernamentales de los Estados Unidos y a algunas de las empresas más grandes del mundo sobre las estrategias de seguridad de la información. Cobb también cofundó dos exitosas empresas de seguridad de TI que fueron adquiridas por compañías que cotizan en bolsa, y es el autor de varios libros y cientos de artículos sobre seguridad de la información. Es profesional certificado en seguridad de sistemas informáticos desde 1996 y reside en San Diego como parte del equipo de investigación global de ESET.

Por más de 30 años, ESET® ha estado desarrollando soluciones de seguridad para las empresas y los usuarios de todo el mundo, que van desde la protección de endpoints y dispositivos móviles, hasta el cifrado y la autenticación en dos fases. Los productos de alto rendimiento y fáciles de usar de ESET les ofrecen a los usuarios y a las empresas la tranquilidad que necesitan para disfrutar de su tecnología sin riesgos. ESET brinda protección y supervisión las 24 horas, los 7 días de la semana, y actualiza las defensas en tiempo real para mantener a los usuarios seguros y a las empresas funcionando sin interrupciones. Para obtener más información, visite www.eset.com/latam.

LOS PRÓXIMOS PASOS

Conozca las soluciones de seguridad informática que ofrece ESET para las pequeñas empresas

MÁS INFORMACIÓN

Descubra la autenticación en dos fases de ESET para la protección adicional de datos

MÁS INFORMACIÓN

Lea sobre el Reglamento general de protección de datos de la UE y conozca su impacto

MÁS INFORMACIÓN