SECURITY SPOTLIGHT

Pequeños Negocios
Guía Practica de Seguridad Informática

¿Cómo asegurarse de que su negocio tiene una protección de seguridad integral?

KASPERSKY lab

$86,500

Promedio del impacto total de una violación de datos a PYMEs.[1]

Probablemente la ciberseguridad suena como algo por lo que las grandes empresas tienen que preocuparse. ¿Qué pueden querer los cibercriminales de una pequeña -o mediana- empresa (PYME)? La respuesta: Muchísimo.

Si es un pequeño negocio que actúa como vendedor de una gran organización, las vulnerabilidades en seguridad de su compañía son oportunidades para los cibercriminales. ¿Envía facturas a las grandes organizaciones? ¿Sus empleados envían correos electrónicos a ellas? ¿Tiene información confidencial en su base de datos? Las oportunidades son, tiene todas las anteriores, lo que significa que la ciberseguridad debe de ser una de sus máximas preocupaciones para proteger la información de su compañía, la privacidad de sus empleados y su relación con sus clientes.

Muchas de las pequeñas empresas no entienden los enormes costos en los que podrían incurrir debido a una violación de datos. Como se ha señalado anteriormente, tan solo una violación de datos cuesta en promedio a las PYMEs $86,000. ¿Se encuentra dentro de su presupuesto? ¿Se encuentra en su presupuesto en caso de que ocurra en múltiples ocasiones? Y si es un ataque dirigido, el promedio aumenta a $143,000.[2]

Nuestra reciente encuesta muestra que el **86% de los pequeños negocios están preocupados por la pérdida de datos**, especialmente como resultado de la perdida física de dispositivos por parte de los empleados. Tienen razón en estar preocupados. Si una violación de datos no se detecta durante más de una semana en una PYME, alrededor de 70,000 archivos de empleados y clientes se verán comprometidos.[3] Y cuando se trata de Bring Your Own Device (BYOD, en español Traiga su propio dispositivo), 54% de los negocios han tenido datos expuestos porque los empleados han perdido dispositivos. De hecho, **el descuido de los empleados contribuye directamente al 48% de los incidentes en ciberseguridad, incluso más que el robo de dispositivos.**

Claramente, la ciberseguridad debe ser una de sus principales preocupaciones si es una PYME que tiene como clientes a grandes empresas, mantiene información sensitiva en su base de datos, o tiene empleados que tienen acceso a información sensitiva. En otras palabras, es algo que afecta a todos los negocios y ningún tamaño de negocio es inmune.

Ahora que sabe que tan importante es, ¿qué puede hacer al respecto?

1, 2, 3. *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International

Su lista de verificación de seguridad

Hay pasos específicos que puede hacer para proteger su compañía, y no necesita un título en Tecnología de la Información o conocimientos anteriores en ciberseguridad para implementarlos.

☑ Solución de seguridad multicapa

Ningún departamento de IT es una isla. Tener la tecnología adecuada para respaldarse le asegurará que su compañía esté protegida contra todas las amenazas, incluídas aquellas que resulten de los errores humanos.

Tener una solución de seguridad multicapa robusta que prediga, detecte, prevenga y responda a las amenazas es esencial para cualquier pequeño negocio.

☑ Educación de empleados

Con el 48% de los incidentes de ciberseguridad atribuidos directamente al descuido de los empleados, no puede permitirse ignorar la educación de empleados acerca de ciberseguridad. De hecho, sus empleados son su primera línea de defensa, pero frecuentemente ellos no se dan cuenta del rol que juegan. Cuando ellos se abstienen de abrir un archivo sospechoso o cuando saben cómo alertar al departamento de IT cuando algo ocurre, la compañía es mucho más segura.

En muchas compañías, las políticas de IT están escritas de tal manera que no pueden ser absorbidas efectivamente por los empleados. Muchas empresas dan a sus empleados documentos llenos de páginas que todos firman, pero pocos leen o los entienden. Diseñar programas educativos para los empleados, que sean, divertidos e informativos al mismo tiempo. Comidas y aprendizajes, juegos y premios son un buen camino para atraer a las personas en este tema tan importante.

¿Qué es pishing?

El pishing es el último ataque de ingeniería social que implica el envió de correos electrónicos o textos disfrazados de fuentes legítimas. Estos pueden parecer que provienen de un vendedor confiable o alguna autoridad policial, pero en secreto, contienen un malware. Estos mensajes están específicamente diseñados para engañar a la víctima para abrir el correo electrónico por medio de las tácticas de miedo e intimidación. Una vez que la persona lo abre, el software malicioso se descarga en su computadora, y el cibercriminal está en su sistema.

Consulte nuestro eBook *El peligro del pishing* para más información acerca de esta táctica peligrosa.

Contraseñas

Además, los empleados necesitan asegurarse de que están utilizando una única y fuerte contraseña, que combina símbolos, números y letras en ambos casos. Todos los días las palabras pueden ser quebrantadas por programas que sencillamente escanean mediante diccionarios hasta que encuentran la correcta. Inclusive, aunque sea fuerte, si una contraseña comprometida es usada para múltiples propósitos, podría conducir a una brecha aún mayor.

Parches y actualizaciones

Los cibercriminales tienden a aprovechar las vulnerabilidades en el software para comprometer los sistemas. Por esta razón, es necesario reservar un tiempo para ejecutar parches y actualizaciones que son emitidos regularmente por las compañías de software.

Con las herramientas de evaluación automatizada de vulnerabilidades y la administración de parches de Kaspersky Lab, puede descansar estando seguro de que su sistema será escaneado y que los parches se distribuirán regularmente para mantener su sistema actualizado.

Asegúrese de no cometer ninguno de estos clásicos errores en tus contraseñas:

1. Utilizar opciones fáciles de recordar y fáciles de adivinar como "contraseña" o "123456".
2. Utilizar su correo electrónico, nombre u otra información fácil de obtener, como contraseña.
3. Establecer preguntas de recuperación de contraseña que un hacker pueda responder con un poco de investigación -nombre de soltera de su madre, por ejemplo.
4. Hacerla ligera, modificaciones obvias a palabras comunes, como colocar un 1 al final.
5. Utilizar frases comunes. Incluso pequeñas frases como "teamo" son fáciles de quebrantar.

54% de los negocios han tenido datos expuestos debido a que sus empleados han perdido sus dispositivos.[4]

Bring Your Own device (BYOD)

Más y más pequeñas y medianas empresas están adaptando las políticas BYOD como medida de conveniencia para los empleados y ahorro de gastos. Pero muchos problemas pueden surgir si no se gestiona correctamente. Por último, el éxito de la implementación BYOD depende de que los empleados sigan las reglas, especialmente cuando se trate de la perdida de dispositivos que puedan comprometer información sensitiva.

Con el 40% de los negocios alrededor del mundo reportando que los empleados ocultan los incidentes de seguridad cuando estos ocurren, [4] asegúrese de que su gente se sienta cómoda de reportar cualquier accidente que ocurra con sus dispositivos, especialmente pérdida o robo.[4]

Cifrado

Cada vez más y más pequeñas y medianas empresas están adaptando las políticas BYOD como medida de conveniencia para los empleados y ahorro de gastos. Pero muchos problemas pueden surgir si no se gestiona correctamente. Por último, el éxito de la implementación BYOD depende de que los empleados sigan las reglas, especialmente cuando se trate de la perdida de dispositivos que puedan comprometer información confidencial.

4. *The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from Within*

Entender el riesgo

Algunas historias de ciberseguridad son legendarias.
Tome nota de estos cuentos cautelosos, y asegúrese
que su compañía no entre en este notorio salón de la fama.

Una taza de café realmente costosa

Hacer la ola para despedirse del último cliente del día, Thomas cerró y se fue del trabajo. Justo enfrente de su oficina está un café, donde se encontrará con un amigo. Recuerda que mañana vencerá el plazo para pagarle a uno de sus proveedores, decide ocuparse del asunto antes de olvidarse de ello.

Utiliza su laptop para conectarse al WiFi del café, inicia sesión en el sitio web de su banco y realiza la transferencia. Satisfecho de no haberse olvidado, se sienta de vuelta y disfruta su café.

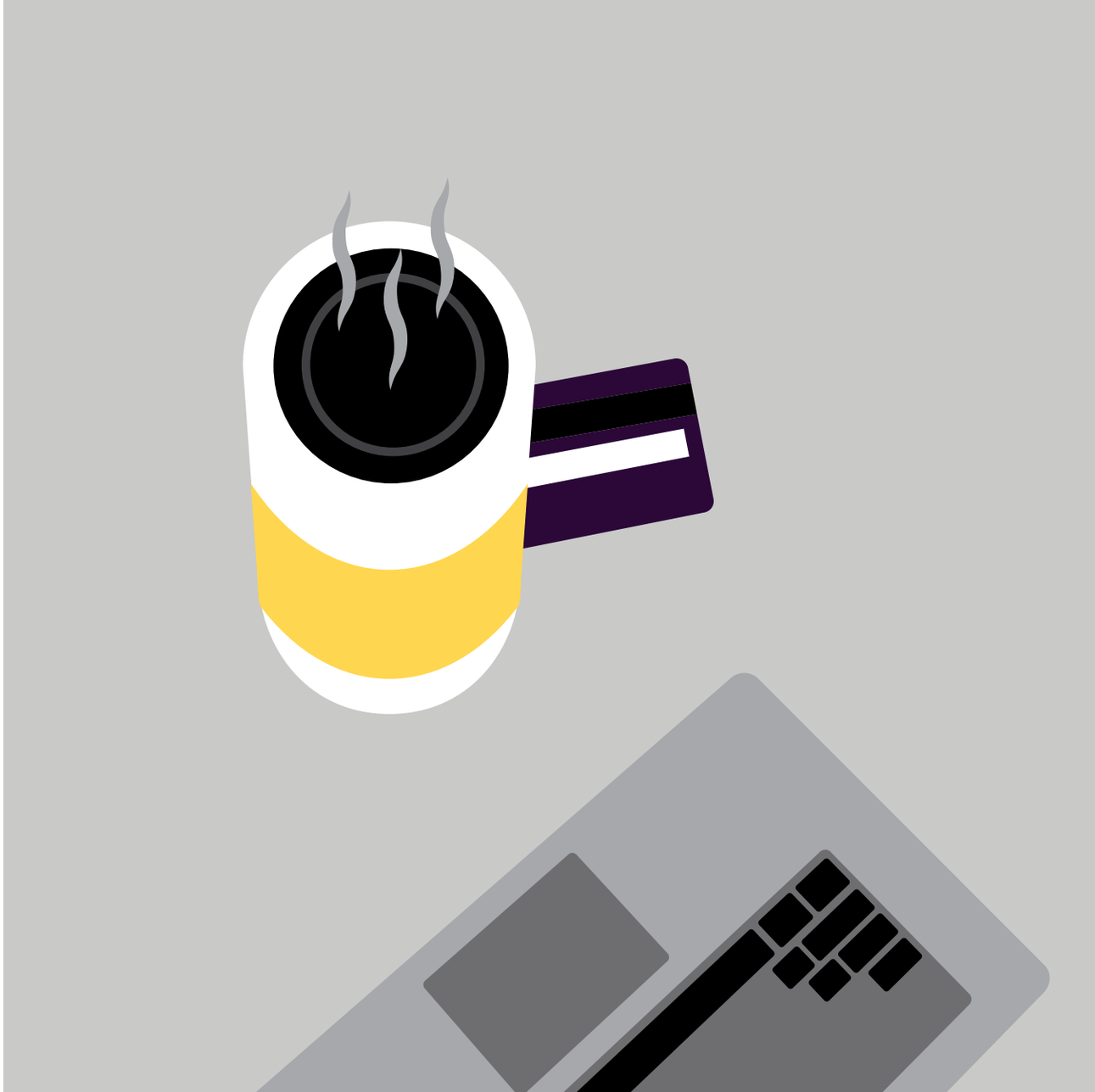
Cuando vuelve a revisar su cuenta, esta vacía. Mientras él se queda tratando de averiguar por qué, sus empleados están esperando su nómina.

¿Cómo sucedió?

Desafortunadamente, él no tenía ningún antimalware instalado y contrajo un programa de keylogging malicioso. Aquellos que crearon el programa recibieron un registro de toda la información que él había introducido. Y, como estaba utilizando una red Wifi pública desprotegida, existía el riesgo de que se interceptaran los datos de la transacción.

¿Qué podría haber hecho diferente?

Las transacciones bancarias solo deben hacerse en dispositivos que tengan instalado un antimalware, y siempre desde un navegador seguro.



Incremento del correo no deseado

María es psicóloga. Cada mañana, abre su correo para revisar la confirmación de su siguiente cita. En la parte superior de su correo, ve un correo de una red social que utiliza pidiéndole que actualice su contraseña, para hacerla más fuerte. Hace clic en el enlace proporcionado, confirma su contraseña actual, la cual es la misma, y luego reemplaza todas las demás letras con asteriscos.

Feliz de que su cuenta será más difícil de hackear, vuelve a su bandeja de entrada, y pronto se olvida del asunto.

Después, recibe una carta de los extorsionadores amenazándola con publicar los detalles de todos los clientes que van a su terapia.

¿Cómo sucedió?

María fue víctima de una estafa phising. A través de un sitio que se veía exactamente igual que otro que ella ya había visitado miles de veces, era una copia falsa. Después de tener acceso a los detalles de su perfil, también obtuvieron los detalles de su consulta. Lo lograron utilizando la misma contraseña, la engañaron para hackear su correo electrónico de trabajo. Debido a que usa la misma contraseña para ambas cuentas, fueron capaces de leer todos sus mensajes y los archivos adjuntos – uno de ellos era la lista completa de todos sus pacientes con sus datos de contacto.

¿Qué podría haber hecho diferente?

Primero, debería haber sido consciente de que los sitios legítimos y las organizaciones no pedirán sus datos por correo electrónico. Con un buen software de seguridad instalado, habría sido alertada del hecho de que el sitio era falso.

En segundo lugar, utilizó la misma contraseña para uso personal y profesional. Variar sus contraseñas es un paso crucial para asegurar una fuerte seguridad cibernética.

True Cybersecurity for Business

El enfoque de True Cybersecurity de Kaspersky Lab combina la seguridad multicapa con el aprendizaje automático y la inteligencia sobre amenazas asistida por la nube para proteger contra amenazas que pueda enfrentar su negocio. True Cybersecurity no solo previene ataques, sino que también predice, detecta y actúa rápidamente, asegurando al mismo tiempo, la continuidad de tu organización.

Síganos en YouTube

Síganos en Facebook

Revise nuestro blog

Síganos en Twitter

Síganos en LinkedIn

Descargue ya su prueba gratis >

Conozca más en:
latam.kaspersky.com

Acerca de Kaspersky Lab

Kaspersky Lab es una de las compañías de ciberseguridad de más rápido crecimiento en el mundo y la más grande como propiedad privada. La compañía se encuentra entre los cuatro principales proveedores mundiales de soluciones de seguridad para usuarios finales (IDC, 2014). Desde 1997, Kaspersky Lab ha sido un innovador en ciberseguridad y ofrece soluciones efectivas de seguridad digital e inteligencia contra amenazas para grandes empresas, PyMES y consumidores. Kaspersky Lab es una compañía internacional que opera en 200 países y territorios alrededor del mundo, proporcionando protección a más de 400 millones de usuarios a nivel global.

Para aprender más acerca de Kaspersky Endpoint Security for Business, ingrese a:
latam.kaspersky.com/small-to-medium-business-security

Contáctenos:
latam.kaspersky.com/small-to-medium-business-security/contact-us

KASPERSKY lab