GUÍA PRÁCTICA DE SEGURIDAD DE TI PARA EMPRESAS PEQUEÑAS

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

#protectmybiz

KASPERSKY lab

Existen pequeñas empresas de todas las formas y tamaños. Sin embargo, en la actualidad, no existe una organización que pueda ignorar la seguridad en línea, independientemente de si es un equipo que funciona en una oficina o si es un individuo que trabaja desde su hogar. Es un problema que nos afecta a todos.

Aunque los delitos cibernéticos frecuentemente acaparan los titulares, por lo general se conocen cuando una enorme multinacional o gobierno es la víctima. Pero, sin duda, los casos más pequeños son la historia más grande.

Solo en 2014 se detectaron 143 millones de nuevos casos de malware.[1] La mayoría de ellos estaban dirigidos a personas y organizaciones que no se consideran a sí mismos como posibles objetivos.

La verdad es que todo el mundo es un objetivo. La buena noticia es que aún existe una gran diferencia entre ser un objetivo y una víctima.

Mayoritariamente, simplemente se reduce a estar preparado. Por ello, hemos creado esta guía: para darle el conocimiento para mantener su empresa segura.

? ¿QUÉ ES MALWARE?

El término malware se refiere a los programas de computadora diseñados para un propósito malicioso. Estos atacan generalmente a los dispositivos sin que el usuario lo sepa. Kaspersky Lab es una empresa líder mundial en la detección de malware, galardonada con puntuaciones más altas que cualquier otro proveedor de seguridad.[2]

? ¿POR QUÉ NECESITO PROTECCIÓN?

Los cibercriminales no necesitan vaciar su cuenta bancaria para tener un costoso impacto en su empresa. Las alteraciones causadas por el malware pueden interrumpir su productividad y flujo de efectivo, provocando una cadena de efectos indeseables. Dado que usted puede protegerse contra estas eventualidades con medidas relativamente sencillas, no necesita mucho para estar tranquilo.

1. AV Tests
2. Estudio de resultados de ensayos independientes TOP3 2014

SU LISTA DE VERIFICACIÓN DE SEGURIDAD

EL PRIMER PASO PARA PROTEGER SU EMPRESA ES ECHAR UN VISTAZO A SU MANERA DE TRABAJAR Y VER DÓNDE PODRÍA REDUCIR EL RIESGO. REALICE UNA COMPROBACIÓN RÁPIDA DEL ESTADO DE LA SEGURIDAD DE TI:

PROTECCIÓN ANTIMALWARE ✔

Al igual que con las compañías de seguros, cuando se trata de productos que protegen a su empresa usted desea obtener lo mejor. Si aún no posee un software altamente capaz para proteger sus dispositivos contra infecciones, debe darle prioridad.

Por desgracia, el simple hecho de estar alerta en línea no es suficiente. Todos sabemos que no debemos abrir archivos adjuntos de remitentes desconocidos o realizar descargas desde sitios sospechosos, pero la verdad es que muchas infecciones provienen de fuentes de confianza que han sido comprometidas.

COMPORTAMIENTOS DE NAVEGACIÓN ✔

Educar a su personal sobre la importancia de sus acciones en línea puede ahorrarle muchos dolores de cabeza. Con suerte, sus empleados entenderán que hay ciertos tipos de sitios que no deben visitar en el trabajo. Pero si también están utilizando un dispositivo móvil (por ejemplo, un smartphone o tablet) para uso personal, una vez que salen del edificio pueden despreocuparse de la seguridad. Por lo tanto, es una buena idea bloquear sitios inadecuados para garantizar que son inaccesibles desde los equipos de trabajo. Aumentar la conciencia general sobre las amenazas a la seguridad de TI también ayudará a los empleados a mantenerse seguros en su uso personal.

? ¿CÓMO PODRÍA AFECTARME?

¿Alguna vez ha recibido un correo electrónico de un amigo o familiar que contenga un enlace interesante que, una vez abierto, parecía sospechoso? Una vez que el malware ha infectado una computadora, puede emprender acciones sin el conocimiento del usuario. Es por eso que las fuentes de confianza no siempre pueden ser de fiar.

CONTRASEÑAS ✔

Los empleados también necesitan asegurarse de que están utilizando contraseñas seguras y únicas que mezclan símbolos, números y letras mayúsculas y minúsculas. Las palabras de uso cotidiano pueden ser descifradas por programas que simplemente escanean diccionarios hasta encontrar la palabra correcta. Y aunque sea fuerte, si una contraseña comprometida se utiliza para múltiples propósitos, podría dar lugar a una vulneración aún mayor.

ACTUALIZACIONES ✔

Se detectan cuatro nuevos elementos de malware cada segundo.[3] Debe anticiparse. Eso significa utilizar actualizaciones automáticas para mejorar su software de seguridad cada día, actualizar sus otros software cuando sea posible y asegurarse de que todo el personal de la empresa haga lo mismo. Recuerde, los programas que no han sido actualizados son la ruta número uno que los criminales cibernéticos utilizan para hackear empresas.

ASEGÚRESE DE NO COMETER NINGUNO DE ESTOS CLÁSICOS ERRORES EN SUS CONTRASEÑAS:

1. Utilizar opciones fáciles de recordar, pero fáciles de adivinar como "contraseña" o " 123456"
2. Utilizar su dirección de correo electrónico, nombre o cualquier otro dato fácil de obtener como contraseña
3. Establecer preguntas de recordatorio de contraseña que un hacker podría responder con tan solo un poco de investigación, por ejemplo, el apellido de soltera de su madre
4. Hacer solo modificaciones obvias y leves a palabras regulares, como poner un "1" al final
5. Utilizar frases comunes. Incluso las frases pequeñas como "teamo" se descifran fácilmente

Para obtener más consejos sobre cómo crear contraseñas difíciles de descifrar, vea nuestra publicación en el blog sobre el tema.

3 AV Tests

EN 2014

295.500

NUEVAS AMENAZAS DE MALWARE MÓVILES[4]

BANCA ✔

Desde dirigirlo a versiones falsas de sitios de confianza hasta la utilización de software malicioso para espiar su actividad, los ciberdelincuentes tienen una serie de métodos para obtener su información financiera. Debe tomar medidas activas para detenerlos.

Esté alerta a los intentos de "phishing" en los que los estafadores suplantan a su banco: utilice siempre un navegador seguro y asegúrese de echar un vistazo a la URL antes de introducir sus datos en cualquier sitio. También es mejor evitar incluir dicha información en correos electrónicos, los que pueden ser vistos por ojos que no debieran.

DISPOSITIVOS MÓVILES ✔

Como el trabajo en movimiento es ahora parte de nuestra vida cotidiana, el crimen cibernético está cada vez más dirigido a los dispositivos móviles. En 2014, se detectaron 295.500 nuevas amenazas de malware móvil (creados específicamente para smartphones y tablets) cada mes.[5] Aunque es igual de importante proteger los teléfonos y las tablets que las computadoras Mac y PC, solo el 32 % de las pequeñas empresas reconocen actualmente el riesgo que presentan los dispositivos móviles.[6]

CIFRADO ✔

Si usted tiene datos confidenciales almacenados en sus computadoras estos deben estar cifrados, de modo que si se pierden o son robados no serán útiles. Es importante darse cuenta de que, en una empresa, la información que almacena es un activo muy valioso que necesita protección.

? ¿QUÉ ES EL PHISHING?

El "Phishing" es cuando los cibercriminales suplantan a una institución confiable, con la esperanza de obtener información, como contraseñas y detalles de tarjetas de crédito, que pueden utilizar para estafarlo.

4 y 5 Según Kaspersky Lab
6 Encuesta global sobre riesgos de la seguridad de TI corporativa de 2014

COMPRENDER LOS RIESGOS

ESTÁ MUY BIEN HABLAR DE SEGURIDAD CIBERNÉTICA, PERO PARA LA MAYORÍA DE NOSOTROS, A VECES PUEDE SER DIFÍCIL DE ENTENDER. NADIE ELEGIRÍA EL MÉTODO MÁS DIFÍCIL PARA LLEGAR A ENTENDER LA REALIDAD DE ESTOS PROBLEMAS. POR LO TANTO, HEMOS TRATADO DE HACERLO MÁS FÁCIL ILUSTRANDO UN PAR DE ESCENARIOS, SUS CONSECUENCIAS Y CÓMO PODRÍAN EVITARSE.

Una taza de café muy cara

Después de despedir al último cliente del día, Thomas deja que su compañero cierre. Hay una cafetería justo enfrente de la oficina, donde se reunirá con un amigo. Después de recordar que el pago de uno de sus proveedores vence mañana, decide encargarse de ello antes de que se le olvide.

Utiliza su computadora portátil para conectarse a la red Wi-Fi de la cafetería, inicia sesión en el sitio Web de su banco y hace la transferencia. Complacido de no haberse olvidado, se relaja y disfruta su café.

Cuando revisa la cuenta al día siguiente, está vacía. Mientras trata de averiguar por qué, su personal espera el pago.

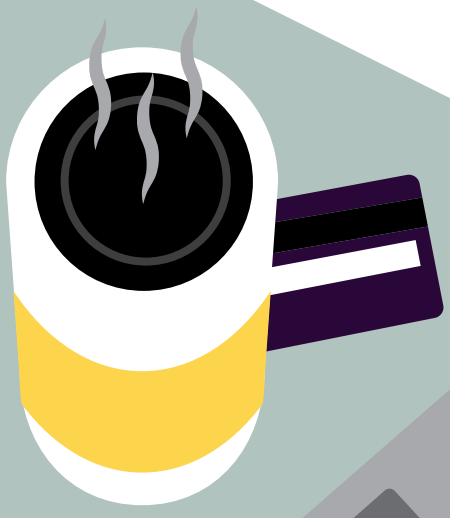
¿CÓMO SUCEDIÓ ESTO?

Desafortunadamente, no tenía ningún tipo de antimalware instalado y se había infectado con un programa de registro de pulsaciones malicioso. Quienes iniciaron el programa recibieron un registro de toda la información que Thomas había introducido usando su teclado. Y, como estaba utilizando una red Wi-Fi pública sin protección, existe el riesgo de que los datos de la transacción hayan sido interceptados.

¿QUÉ PODRÍA HABER HECHO?

Las operaciones bancarias deberían realizarse únicamente en dispositivos que tienen un antimalware instalado y siempre a través de un navegador seguro. Con la funcionalidad Safe Money de Kaspersky, Thomas hubiese tenido la certeza de que la transacción era segura.

Cabe señalar que, como estaba utilizando una red pública no segura, los datos que estaba transmitiendo fueron mucho más fáciles de interceptar que si hubiera utilizado una conexión privada. Pero con una funcionalidad como Safe Money instalada, podría disfrutar de la comodidad de las operaciones bancarias en línea sin tener que preocuparse.



Mayor cantidad de correos electrónicos no deseados

María es psicóloga y cada mañana abre su correo Web para verificar que su próxima cita esté confirmada. En la parte superior de su bandeja de entrada ve un mensaje de una red social que utiliza, pidiéndole que actualice su contraseña a una más segura. Hace clic en el enlace proporcionado, confirma su contraseña existente (que es la misma y luego reemplaza todas las otras letras con un asterisco).

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

...Hasta que recibe una carta de chantajistas amenazándola con publicar los detalles de cada uno de los clientes que acuden a ella para terapia.

¿CÓMO SUCEDIÓ ESTO?

María fue víctima de una estafa de phishing. Aunque el sitio se veía igual que aquel que había visitado miles de veces antes, era solo una copia falsa. Al tener acceso a su información del perfil, los hackers también se encontraron con los detalles de su profesión. Intentaron usar la misma contraseña, que obtuvieron con engaños, para hackear su correo electrónico laboral. Y como utilizaba la misma para ambas cuentas, pudieron leer todos sus mensajes y los archivos adjuntos en ellos; uno de los cuales era una lista completa de sus clientes y sus datos de contacto.

¿QUE PODRÍA HABER HECHO DE MANERA DIFERENTE?

En primer lugar, tenía que haber sido consciente de que las organizaciones y los sitios legítimos no le solicitarán información a través del correo electrónico. Con un buen software de seguridad instalado, una vez que hubiese hecho clic en el enlace hubiese sido alertada de que el sitio era una farsa.

Su otro error fue utilizar la misma contraseña en un contexto profesional y privado.

¿POR QUÉ ELEGIR KASPERSKY?

ES NUESTRA MISIÓN PROPORCIONAR LA PROTECCIÓN MÁS EFICAZ, SENSIBLE Y EFICIENTE DEL MUNDO CONTRA AMENAZAS CIBERNÉTICAS. EN KASPERSKY SMALL OFFICE SECURITY HEMOS CONVERTIDO DICHA EXPERIENCIA EN UNA SOLUCIÓN QUE ES TAN APROVECHABLE COMO ÚTIL. ASÍ QUE PUEDE CONTINUAR CON LO QUE SABE HACER MEJOR: MANEJAR SU NEGOCIO.

Entendemos que, cuando se trata de la seguridad cibernética, las pequeñas empresas están en una posición única. Se enfrentan a muchas de las mismas amenazas como empresa, a la vez que comparten muchas de las mismas vulnerabilidades con los usuarios domésticos. Creemos que esta posición única merece su propio enfoque sobre la seguridad.

No es adecuado simplemente volver a empaquetar un producto de consumo como una solución para una mediana empresa. Por ejemplo, no ofrecerá protección para servidores, pero muchas empresas pequeñas utilizarán una o pronto lo harán. Contrariamente a los usuarios domésticos, las empresas necesitan proteger múltiples dispositivos de manera fácil.

Sin embargo, simplemente eliminar funciones de una solución diseñada para una empresa grande tampoco funciona. Las pequeñas empresas no tienen equipos de TI dedicados o el tiempo para luchar con un software complicado diseñado para especialistas.

Kaspersky Small Office Security ha sido diseñado para ser completo sin ser complicado, por lo que puede estar tranquilo, sin que la seguridad se convierta en una pérdida de recursos. No lo retrasará y cubre una amplia gama de dispositivos, para que pueda mantenerse protegido sin importar donde lo lleve su negocio.

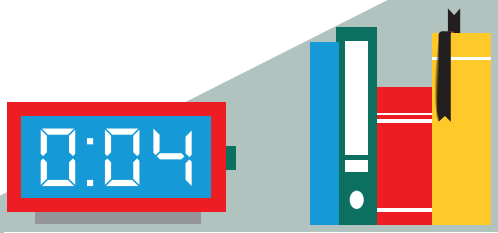
¿PERO PUEDO PROTEGERME DE FORMA GRATUITA?

Aunque hay las soluciones de seguridad gratuitas disponibles, simplemente no proporcionan una protección completa. De hecho, dejan un espacio deliberado para realizar mejoras. De esa forma, pueden animar a los usuarios a actualizar a una versión pagada.

Cuando su empresa está en juego, necesita la mejor protección posible, todo el tiempo.

HACERLO POSIBLE

AHORA QUE HEMOS IDENTIFICADO LAS ÁREAS QUE NECESITA CONSIDERAR COMO PARTE DE SU POLÍTICA DE SEGURIDAD, ES HORA DE CONSIDERAR CÓMO, CON LA AYUDA DE UNA SOLUCIÓN PERSONALIZADA, PUEDE IMPLEMENTAR SOLUCIONES.



ASEGÚRESE DE QUE LAS ACTUALIZACIONES SE REALIZAN PERIÓDICAMENTE

Cuando se trata de Kaspersky Small Office Security, ya no tiene de qué preocuparse. Actualizaremos su protección automáticamente en tiempo real, informándole de las nuevas amenazas que vayan surgiendo.

IMPLEMENTE CONTRASEÑAS SEGURAS

Hágalo más fácil para sus empleados utilizando Kaspersky Password Manager. Generará automáticamente contraseñas seguras y las almacenará en una base de datos cifrada. De esta forma, solo tiene que recordar una contraseña maestra y estará mucho más seguro.

CIFRAR Y REALIZAR COPIAS DE SEGURIDAD DE DATOS CONFIDENCIALES Y CRÍTICOS

Con Kaspersky Small Office Security es fácil almacenar su información crítica en "bóvedas" cifradas. Y la función de restauración permite que, incluso si sus computadoras o servidores colapsan, no existe una pérdida de datos vitales.

INCLUYA TODOS SUS DISPOSITIVOS

Kaspersky Small Office Security ofrece protección para tablets y smartphones compatibles. Además, si los dispositivos se pierden o son robados, le puede ayudar a localizarlos y eliminar de forma remota cualquier información confidencial.

BLOQUEE A LOS CHICOS MALOS

Nuestra galardonada funcionalidad Safe Money puede activarse en un par de clics y permite una navegación súper segura. Su uso para verificar que los sitios con los que está interactuando no son peligrosos, puede evitar al instante las posibilidades de una vulneración. Mientras tanto, nuestras funcionalidades de antimalware, antispam y firewall mantienen cerradas las puertas a los criminales durante sus otras actividades en línea.

PROTEJA SU EMPRESA AHORA.

Diseñado para atender las necesidades únicas de las empresas pequeñas, Kaspersky Small Office Security combina una protección avanzada con la facilidad de uso esencial para empresas como la suya.

Visite **kaspersky.com/protectmybusiness** y descubra cómo Kaspersky Small Office Security puede proteger a su empresa.

PROTEJA SU EMPRESA AHORA

ÚNASE A LA CONVERSACIÓN

#protectmybiz

Véanos en YouTube

Denos "Me gusta" en Facebook

Revise nuestro blog

Síganos en Twitter

Únase a nosotros en LinkedIn

Conozca más en kaspersky.com/protectmybusiness

ACERCA DE KASPERSKY LAB

Kaspersky Lab es el proveedor privado de soluciones de protección de terminales más grande del mundo. La empresa se encuentra entre los mejores cuatro proveedores del mundo de soluciones de seguridad para usuarios de terminales.* Durante sus más de 17 años de historia, Kaspersky Lab ha innovado en seguridad de TI y proporcionado las soluciones de seguridad digital más efectivas para las grandes empresas, las pequeñas y medianas empresas, y los consumidores finales. Kaspersky Lab, con su empresa controladora registrada en el Reino Unido, opera actualmente en casi 200 países y territorios del mundo y brinda protección a 400 millones de usuarios alrededor del globo. Conozca más en www.kaspersky.com.

* La empresa obtuvo el cuarto puesto en la clasificación de IDC de Ingresos en seguridad de terminales en todo el mundo por proveedor, 2013. La clasificación se publicó en el informe de IDC "Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares" (IDC #250210, agosto de 2014) (Pronóstico mundial de seguridad de terminales 2014-2018 y cuota por proveedor 2013, IDC #250210, agosto de 2014). El informe clasificó a los proveedores de software de acuerdo con los ingresos procedentes de la venta de soluciones de seguridad de terminales durante el año 2013.