GUÍA PRÁCTICA DE SEGURIDAD DE IT PARA PEQUEÑAS EMPRESAS

Cómo asegurarse de que su empresa cuenta con protección completa para la seguridad de IT

#protectmybiz

KASPERSKY lab

Hay pequeñas empresas de todas las formas y tamaños. Sin embargo, en la realidad actual, no hay ninguna organización que pueda permitirse ignorar la seguridad online, ya se trate de un equipo que trabaja fuera de la oficina o de una única persona que trabaja desde casa. Es un problema que afecta a todo el mundo.

El cibercrimen ocupa a menudo los titulares, sobre todo cuando la víctima es el gobierno o una gran empresa multinacional. No obstante, los casos que afectan a entidades más pequeñas son, probablemente, los más frecuentes.

Solo en el año 2014, se detectaron 143 millones de nuevos casos de malware.[1] La mayoría de estas amenazas estaban dirigidas a individuos y organizaciones que no se consideraban a sí mismos objetivos probables.

La realidad es que cualquiera puede ser el objetivo de un ataque. La buena noticia es que existe una gran diferencia entre ser el objetivo y ser la víctima.

La mayor parte de las veces, se trata únicamente de estar preparado. Esta es la razón por la que hemos creado esta guía: para proporcionarle los conocimientos necesarios que le permitan proteger su empresa.

¿QUÉ ES EL MALWARE?

El término malware hace referencia a programas de ordenador diseñados con un fin malicioso. Generalmente, atacan a los dispositivos sin que el usuario sea consciente de ello. Kaspersky Lab es un líder mundial en la detección de malware y ha recibido las mejores puntuaciones más veces que ningún otro proveedor de seguridad.[2]

¿POR QUÉ NECESITO PROTECCIÓN?

Los cibercriminales no necesitan vaciar su cuenta bancaria para provocar un impacto costoso en su empresa. El malware causa molestias que pueden interrumpir su productividad y el flujo de caja, algo que puede provocar una cadena de efectos no deseados. Dado que puede protegerse contra estas eventualidades con pasos relativamente sencillos, su tranquilidad no requiere un gran esfuerzo.

1. Pruebas de AV-Test
2. Estudio de los resultados de las pruebas independientes que analizan los 3 primeros puestos de 2014

LISTA DE COMPROBACIÓN DE LA SEGURIDAD

EL PRIMER PASO PARA PROTEGER SU EMPRESA ES OBSERVAR LA FORMA EN QUE TRABAJA PARA DETECTAR LOS PUNTOS EN LOS QUE PUEDE REDUCIR EL RIESGO. CREE UNA LISTA RÁPIDA DE COMPROBACIÓN DEL ESTADO DE LA SEGURIDAD DE IT:

PROTECCIÓN ANTIMALWARE ✔

Al igual que sucede con el seguro de su empresa, busca obtener la mejor opción posible cuando se trata de productos para proteger su negocio. Si todavía no dispone de un software de alta capacidad que proteja sus dispositivos contra las infecciones, esto debería convertirse en su prioridad.

Por desgracia, estar atento en la Red no es suficiente. Todos sabemos que no debemos abrir archivos adjuntos enviados por desconocidos ni descargar contenidos de sitios sospechosos, pero lo cierto es que muchas infecciones se producen en fuentes fiables que han sido vulneradas.

COMPORTAMIENTOS DE NAVEGACIÓN ✔

Informar al personal sobre la importancia que tienen sus acciones online puede ahorrarle muchos quebraderos de cabeza. Con suerte, los trabajadores comprenderán que hay ciertos tipos de sitios que no deben visitar en el trabajo. Sin embargo, si también utilizan un dispositivo móvil (como un smartphone o tablet) para su uso personal, es posible que sean menos conscientes de la importancia de la seguridad al dejar su lugar de trabajo. Por ello, bloquear los sitios inapropiados puede ser una buena opción a la hora de garantizar que no sean accesibles desde los equipos de trabajo. Si sus empleados son cada vez más conscientes de las amenazas de seguridad de IT, esto les ayudará a proteger también su uso personal de los dispositivos.

? ¿CÓMO PODRÍA AFECTARME?

¿Alguna vez ha recibido un correo electrónico de un amigo o familiar que contenga un enlace interesante que, una vez abierto, parece sospechoso? Una vez que el malware ha infectado el equipo, puede realizar acciones sin que el usuario sea consciente de ello. Esta es la razón por la que las fuentes fiables no siempre son dignas de confianza.

CONTRASEÑAS ✔

Los empleados deben asegurarse de que están utilizando contraseñas seguras y exclusivas que combinen símbolos, números y letras en mayúscula y minúscula. Las palabras comunes se pueden descifrar con programas que se limitan a analizar el contenido de determinados diccionarios hasta encontrar la palabra correcta. Incluso si es segura, puede vulnerarse y utilizarse para diversos fines, lo que podría provocar una brecha aún mayor.

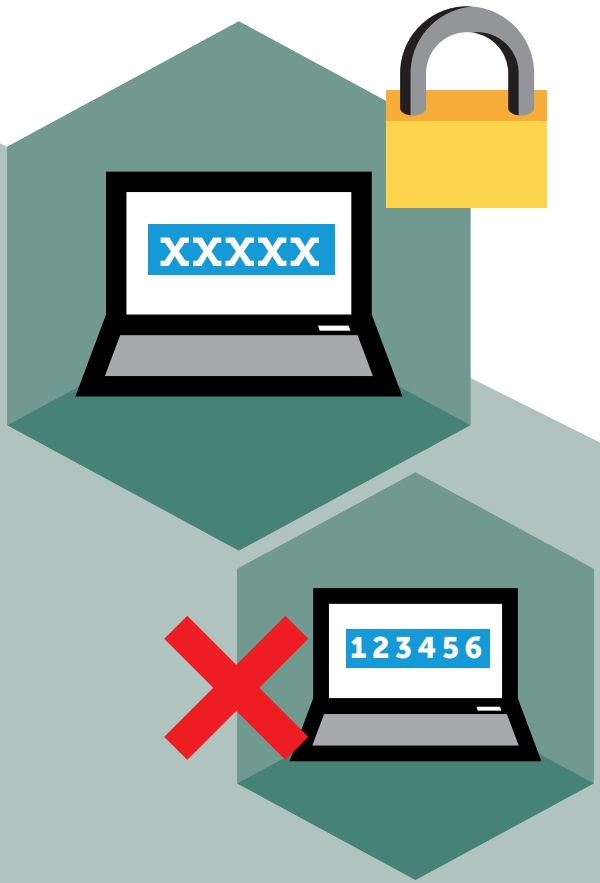
ACTUALIZACIONES ✔

Cada segundo se detectan cuatro casos nuevos de malware.[3] Por lo tanto, debe anticiparse. Esto implica utilizar actualizaciones automáticas para mantener su software de seguridad en perfecto estado y actualizar el resto de software siempre que sea posible, así como asegurarse de que todo el mundo haga lo mismo en la empresa. Recuerde que los programas que no se han actualizado son el principal objetivo de los cibercriminales a la hora de acceder ilegalmente a las empresas.

ASEGÚRESE DE NO COMETER NINGUNO DE ESTOS ERRORES CLÁSICOS DE CONTRASEÑA:

1. Utilizar opciones fáciles de recordar, pero también 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 para recordar la contraseña que un hacker podría responder con solo investigar un poco: por ejemplo, el segundo apellido de su madre
4. Realizar pequeñas modificaciones o cambios evidentes en palabras comunes, como colocar un "1" al final
5. Utilizar frases comunes. Incluso las frases cortas como "tequiero" se pueden descifrar fácilmente

Para obtener más sugerencias sobre cómo crear contraseñas difíciles de descifrar, consulte la publicación en nuestro blog relacionada con este asunto.



3 Pruebas de AV-Test

EN 2014

295,500

NUEVAS AMENAZAS DE MALWARE PARA DISPOSITIVOS MÓVILES[4]

BANCA ✔

Desde el direccionamiento a versiones falsas de sitios de confianza, hasta el uso de malware para espiar su actividad, los cibercriminales cuentan con varios métodos que les permiten obtener su información financiera. Debe tomar medidas activas para detenerles.

Permanezca alerta para detectar los intentos de "phishing" en las que los estafadores se hacen pasar por miembros de su banco: utilice siempre un navegador seguro y asegúrese de examinar con atención la URL antes de introducir sus datos en ningún sitio. Asimismo, es mejor no incluir esta información en correos electrónicos, ya que podría caer en manos de personas a las que no está destinada.

DISPOSITIVOS MÓVILES ✔

Dado que trabajar mientras nos desplazamos es ahora parte de nuestra vida cotidiana, el cibercrimen está cada vez más dirigido a los dispositivos móviles. En 2014, se detectaron 295 500 amenazas móviles nuevas de malware (específicamente creadas para smartphones y tablets) al mes.[5] A pesar de que la protección de teléfonos y tablets es tan importante como la de los equipos Mac y PC, solo el 32 % de las empresas pequeñas reconoce el riesgo que representan los dispositivos móviles.[6]

CIFRADO ✔

La información confidencial almacenada en sus equipos debe estar cifrada para evitar que pueda utilizarse en caso de pérdida o robo. Es importante que sea consciente de que la información empresarial que posee es un activo de gran valor que necesita protección.

? ¿QUÉ ES EL PHISHING?

El "phishing" es una práctica mediante la que los cibercriminales se hacen pasar por una institución de confianza con la intención de obtener información, como contraseñas y datos de tarjetas de crédito, que se pueden utilizar para estafarle.

4 y 5 Según los datos de Kaspersky Lab
6 Encuesta de riesgos de seguridad de IT globales en la empresa 2014

COMPRENDER LOS RIESGOS

HAY QUE TRATAR EL TEMA DE LA CIBERSEGURIDAD PERO, PARA LA MAYORÍA DE NOSOTROS, PUEDE SER UN ASUNTO DIFÍCIL DE ENTENDER A VECES. HACER FRENTE A ESTA REALIDAD POR LAS MALAS NO ES PRECISAMENTE LO QUE QUEREMOS. POR ELLO, HEMOS INTENTADO HACERLO MÁS SENCILLO AL ILUSTRAR UN PAR DE CASOS, SUS CONSECUENCIAS Y LA MEJOR FORMA DE EVITARLAS.

Una taza de café muy cara

Después de despedirse del último cliente del día, Thomas deja que su socio cierre la empresa. Hay una cafetería justo al otro lado de la oficina, donde ha quedado con un amigo. Se acuerda de que tiene hasta mañana para realizar el pago a uno de sus proveedores y decide ponerse manos a la obra antes de que se le olvide.

Utiliza su equipo portátil para conectarse a la red Wi-Fi de la cafetería, inicia sesión en el sitio web de su banco y realiza la transferencia. Contento por no haberse olvidado de hacerlo, se relaja en su asiento y disfruta de su café.

Cuando comprueba su cuenta al día siguiente, se da cuenta de que está vacía. Mientras él trata de averiguar qué ha ocurrido, sus empleados están a la espera de recibir su pago.

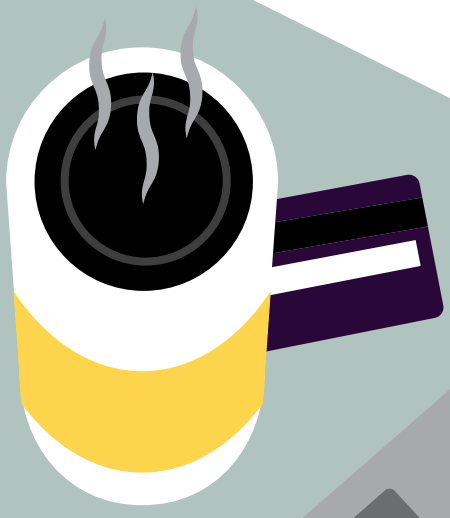
¿CÓMO HA OCURRIDO ESTO?

Desafortunadamente, Thomas no tenía ninguna herramienta antimalware instalada y se topó con un programa malicioso de registro de pulsación de teclas. Los que iniciaron el programa recibieron un registro de toda la información que la víctima había introducido. Además, dado que estaba utilizando una red Wi-Fi pública no protegida, el riesgo de que la información de la transacción fuera interceptada era aún mayor.

¿QUÉ PODRÍA HABER HECHO LA VÍCTIMA?

La banca electrónica solo debe utilizarse en dispositivos que dispongan de herramientas antimalware y, en todo caso, a través de un navegador seguro. Con la función Pago Seguro de Kaspersky, Thomas habría podido comprobar, sin ninguna duda, que la transacción era segura.

Es importante señalar que, dado que estaba utilizando una red pública no segura, la información transmitida era más fácil de interceptar que con una conexión privada. Pero con una función como Pago Seguro, Thomas podría disfrutar de la comodidad de la banca online sin tener que preocuparse.



Correo electrónico no deseado

María es psicóloga y cada mañana abre su correo web para comprobar que hayan confirmado su próxima cita. En la parte superior de la bandeja de entrada, ve un mensaje de una red social que utiliza, en el que se le pide que modifique su contraseña para que sea más segura. Hace clic en el enlace proporcionado, confirma su contraseña actual y crea una nueva (que es idéntica a la anterior, salvo por el hecho de que sustituye cada dos letras con un asterisco).

Satisfecha de saber que su cuenta es más difícil de hackear ahora, vuelve a su bandeja de entrada y pronto se olvida de todo el asunto.

Hasta que recibe una carta de los chantajistas en la que la amenazan con publicar los datos de cada uno de los pacientes que acuden a terapia.

¿CÓMO HA OCURRIDO ESTO?

María fue víctima de una estafa de phishing. A pesar de que el sitio tenía el mismo aspecto que el que ella había visitado miles de veces antes, se trataba de una copia falsa. Al tener acceso a los datos de su perfil, los estafadores también accedieron a la información de su consulta. Intentaron utilizar la misma contraseña con la que la habían engañado en primer lugar para acceder de forma ilegal a su correo electrónico de trabajo. Dado que María la había utilizado en ambas cuentas, los estafadores tuvieron acceso a todos sus mensajes y archivos adjuntos. Uno de ellos era una lista completa de sus pacientes y sus datos de contacto.

¿QUÉ PODRÍA HABER HECHO LA VÍCTIMA?

En primer lugar, debería haber sabido que las organizaciones y sitios legítimos no solicitan información a través de correos electrónicos. Con un buen software de seguridad instalado, al hacer clic en el enlace, María habría recibido una alerta indicando que el sitio era falso.

El otro error que cometió fue utilizar la misma contraseña en el ámbito profesional y privado.

RAZONES POR LAS QUE ELEGIR KASPERSKY

NUESTRA MISIÓN ES PROPORCIONAR LA PROTECCIÓN MÁS EFICAZ Y EFICIENTE DEL MUNDO CONTRA LAS CIBERAMENAZAS. EN KASPERSKY SMALL OFFICE SECURITY, HEMOS DADO FORMA A NUESTRA EXPERIENCIA PARA CREAR UNA SOLUCIÓN TAN FÁCIL DE USAR COMO ÚTIL. PARA QUE PUEDA CONTINUAR CON LO QUE MEJOR SABE HACER: ADMINISTRAR SU EMPRESA.

Entendemos que, cuando se trata de ciberseguridad, las empresas pequeñas se encuentran en una posición única. Se enfrentan a un gran número de amenazas que acechan típicamente a las empresas, a la vez que comparten muchas de las vulnerabilidades de los usuarios domésticos. En nuestra opinión, esta posición única se merece un planteamiento propio de la seguridad.

La simple adaptación de un producto al consumidor en la elaboración de una solución para la pequeña empresa no parece adecuada. Por ejemplo, no ofrecerá protección para los servidores, pero muchas pequeñas empresas utilizan uno o pronto lo harán. A diferencia de los usuarios domésticos, las empresas necesitan proteger varios dispositivos de forma sencilla.

Por lo tanto, limitarse a eliminar funciones de una solución ideada para las grandes empresas tampoco parece una solución válida. Las empresas pequeñas no disponen de equipos de IT dedicados ni del tiempo suficiente para batallar con el complejo software que elaboran los especialistas.

Kaspersky Small Office Security se ha diseñado para ofrecer una protección completa sin complicaciones, de forma que pueda estar totalmente tranquilo sin necesidad de que seguridad se convierta en un costoso gasto. No ralentiza su rendimiento y da cobertura a una amplia gama de dispositivos, para que pueda protegerse, independientemente de adónde le lleve su negocio.

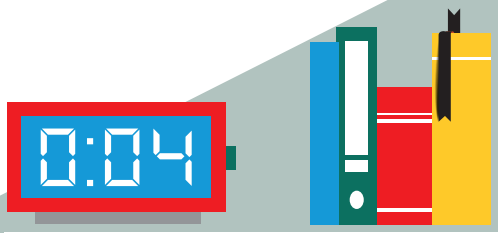
¿PUEDO PROTEGERME DE FORMA GRATUITA?

Hay soluciones gratuitas disponibles, pero no proporcionan una protección completa. De hecho, incluyen deliberadamente muchas posibilidades de mejora. Así se anima a los usuarios a obtener una versión de pago.

Cuando es su empresa lo que está en juego, necesita la mejor protección posible en todo momento.

HÁGALO REALIDAD

AHORA QUE HEMOS IDENTIFICADO LAS ÁREAS QUE DEBE TENER EN CUENTA COMO PARTE DE SU POLÍTICA DE SEGURIDAD, ES HORA DE PENSAR EN UNA FORMA DE IMPLEMENTARLAS, CON LA AYUDA DE UNA SOLUCIÓN PERSONALIZADA.



ASEGÚRESE DE QUE REALIZA ACTUALIZACIONES PERIÓDICAMENTE

En lo que respecta a Kaspersky Small Office Security, no tiene que preocuparse. Actualizaremos su protección de forma automática en tiempo real, lo que le dará ventaja con respecto a las nuevas amenazas que aparecen.

UTILICE CONTRASEÑAS SEGURAS

Haga que esta tarea resulte más sencilla para sus empleados con Kaspersky Password Manager. Genera automáticamente contraseñas seguras y las almacena en una base de datos cifrada. De esta forma, solo deberá recordar una contraseña maestra y estará mucho más protegido.

REALICE COPIAS DE SEGURIDAD Y CIFRE SU INFORMACIÓN CONFIDENCIAL/IMPORTANTE

Con Kaspersky Small Office Security, es fácil almacenar su información más importante en "repositorios" cifrados. La función de restauración permite que la información importante no se pierda, incluso en el caso de que sus equipos o servidores dejen de funcionar.

INCLUYA TODOS SUS DISPOSITIVOS

Kaspersky Small Office Security ofrece protección para los tablets y smartphones compatibles. En caso de robo o pérdida de los dispositivos, puede ayudarle a encontrarlos y borrar cualquier información confidencial de forma remota.

BLOQUEE A LOS DELINCUENTES

Nuestra función galardonada Pago Seguro se puede activar con un par de clics y le permite obtener una navegación extremadamente segura. Al utilizarla para comprobar si los sitios con los que interactúa son vulnerables, puede evitar de forma inmediata la aparición de brechas. Mientras tanto, nuestras funciones antimalware, antispam y firewall bloquean el acceso de los criminales durante su actividad online.

COMIENCE A PROTEGER SU EMPRESA HOY MISMO.

Diseñado para satisfacer las necesidades exclusivas de las empresas pequeñas, Kaspersky Small Office Security combina una protección avanzada con la facilidad de uso que necesitan las empresas como la suya.

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

COMIENCE A PROTEGER SU EMPRESA HOY MISMO

ÚNASE A LA CONVERSACIÓN

#protectmybiz

Véanos en YouTube

Síganos en Facebook

Revise nuestro blog

Síganos en Twitter

Únase a nosotros en LinkedIn

Más información en kaspersky.com/protectmybusiness

ACERCA DE KASPERSKY LAB

Kaspersky Lab es el mayor proveedor privado de soluciones de protección de endpoints del mundo. La empresa figura entre los cuatro proveedores principales de soluciones de seguridad para usuarios de endpoints.* A lo largo de sus más de 17 años de historia, Kaspersky Lab se ha mantenido como una empresa innovadora en seguridad de IT y suministra eficaces soluciones de seguridad digitales para grandes empresas, pymes y particulares. Kaspersky Lab, cuya sociedad de cartera está registrada en el Reino Unido, opera actualmente en casi 200 países y territorios de todo el mundo, y brinda protección a más de 400 millones de usuarios en todo el mundo. Más información en www.kaspersky.es.

* La empresa logró el cuarto puesto en el índice de IDC de ingresos de seguridad para endpoints en todo el mundo por proveedor de 2013. Este índice se publicó en el informe de IDC "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (Previsión de seguridad mundial de endpoints 2014-2018 y acciones de los proveedores en 2013) (IDC núm. 250210, agosto de 2014). En el informe se clasifican los proveedores de software según los ingresos de ventas de soluciones de seguridad para endpoints en 2013.