La seguridad cibernética y su empresa

Cuánto cuestan los delitos cibernéticos y cómo proteger sus datos

Brought to you by

Contenido

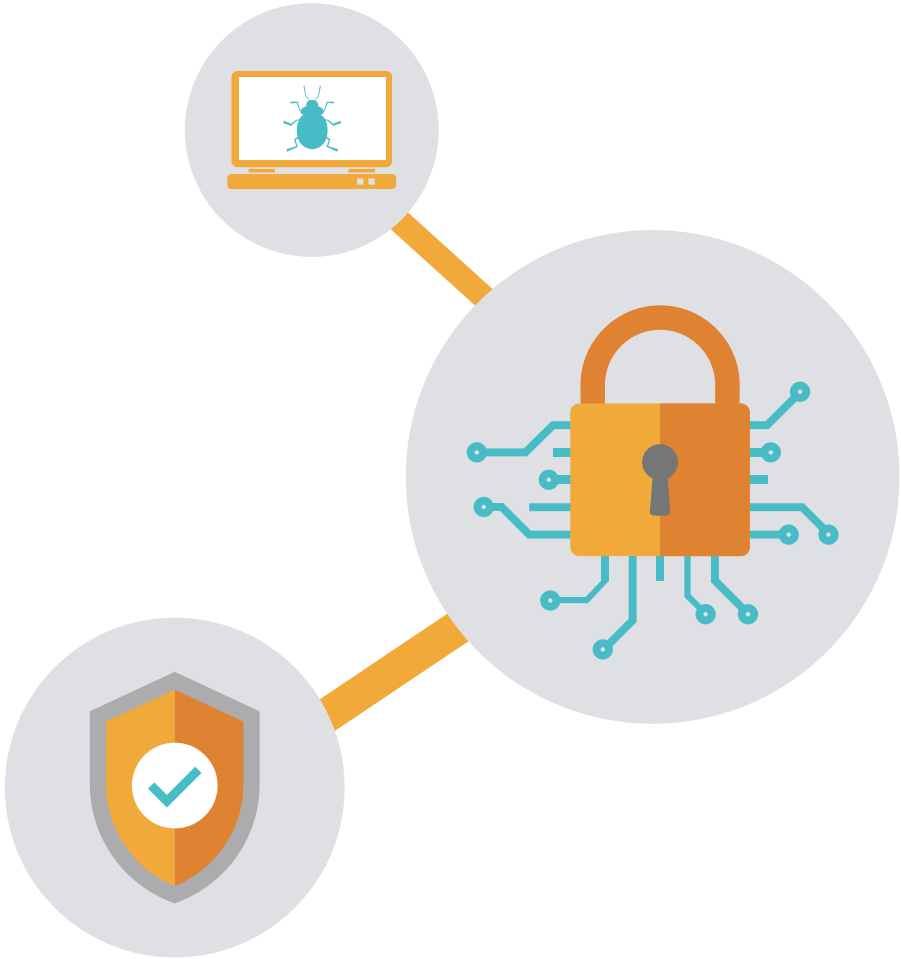
Introducción

«Muchos ejecutivos afirman que los delitos cibernéticos definirán nuestra generación», Dennis Chesley, líder global en servicios de consultoría de gestión de riesgos, PwC[1]

La seguridad cibernética no es una amenaza reciente, pero está creciendo. Los hackers son cada vez mejores. Y disponen de más puntos por los que filtrarse en una red. El Internet de las cosas está multiplicando el número de dispositivos de puntos de conexión que, a menudo, son la forma más sencilla de acceder a una red. Los objetivos son cada vez mayores y los problemas aumentan en escala.

El 21 de octubre de 2016, el proveedor estadounidense de DNS Dyn sufrió el mayor ataque de denegación de servicio (DDoS) de la historia. La actividad de algunos de los sitios web más importantes del mundo, incluidos Netflix,[2] Amazon y Twitter, fue nula durante horas.

En enero de 2017, Lloyds Bank sufrió importantes interrupciones del servicio de red. Sus clientes no pudieron acceder a sus cuentas ni realizar pagos. El acceso mediante aplicación móvil tampoco funcionaba. Si bien Lloyds no ha confirmado nada, se rumoreaba que el causante había sido un ataque DDoS.[3]



Fuente: [1] PwC: The Global State of Information Security Survey 2016 (PwC: Encuesta sobre el estado global de la seguridad de la información de 2016) [2] http://thehackernews.com/2016/10/dyn-dns-ddos.html
[3] https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Introducción

Estas brechas de seguridad suponen algo más que una publicidad negativa. Cuestan dinero.

Según el informe sobre encuestas de seguridad de la impresión de 2016 de Spiceworks, el 34 % de las organizaciones ha declarado que una brecha de seguridad implica el aumento de las llamadas al servicio de asistencia técnica y del tiempo de asistencia, el 29 % ha declarado que las brechas de seguridad reducen la productividad/efectividad, y el 26 % ha declarado que el aumento del tiempo de inactividad en el sistema supone un problema.[4]

Casi el 60 % de los responsables de seguridad entrevistados para un informe de evaluación de responsables de seguridad (CSO) de IBM, ha declarado que la sofisticación de los atacantes supera la sofisticación de las defensas de sus organizaciones.[5]

Los responsables de seguridad (CIO), preocupados por el problema, han declarado durante más de una década que la seguridad cibernética se halla entre sus diez mayores problemas y ahora se sitúa en el número dos, según el estudio de SIM Trends.[6]

Muchos de estos daños se pueden evitar. En las páginas siguientes, hablaremos sobre algunas de las creencias falsas más habituales en torno a la ciberseguridad, estudiaremos detalladamente el impacto que tienen los delitos cibernéticos en las empresas y hablaremos sobre qué puede hacer para defenderse de estos ataques. Por último, veremos qué nos depara el futuro y hablaremos sobre qué nos espera y cómo prepararnos.

Fuente: [4] HP Printer Security Research 2016 (Investigación sobre la seguridad de las impresoras de HP de 2016), Spiceworks [5] IBM CSO Assessment 2014 (Evaluación de responsables de seguridad de IBM de 2014)
[6] SIM IT Trends Survey 2015 (Encuesta sobre tendencias de TI de SIM de 2015)

Desmitificación de los mitos sobre ciberseguridad

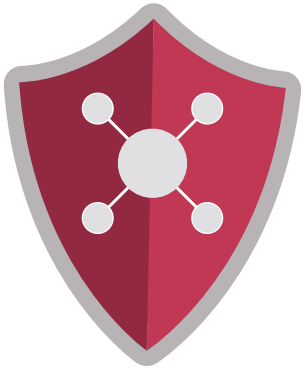
Cinco creencias falsas habituales
que pueden poner en riesgo su empresa frente a la amenaza de los delitos cibernéticos

Cuando se produce una filtración de datos, las firmas más conocidas son las que acaparan los titulares. Sin embargo, ninguna organización está libre de esta amenaza. A continuación, incluimos cinco mitos sobre ciberseguridad que pueden dejar a las empresas a merced de los hackers.

Brecha de seguridad

Fuga de información

Prácticas de seguridad



Software antivirus

Ciberataques

1 Las empresas pueden recuperarse rápidamente de cualquier brecha

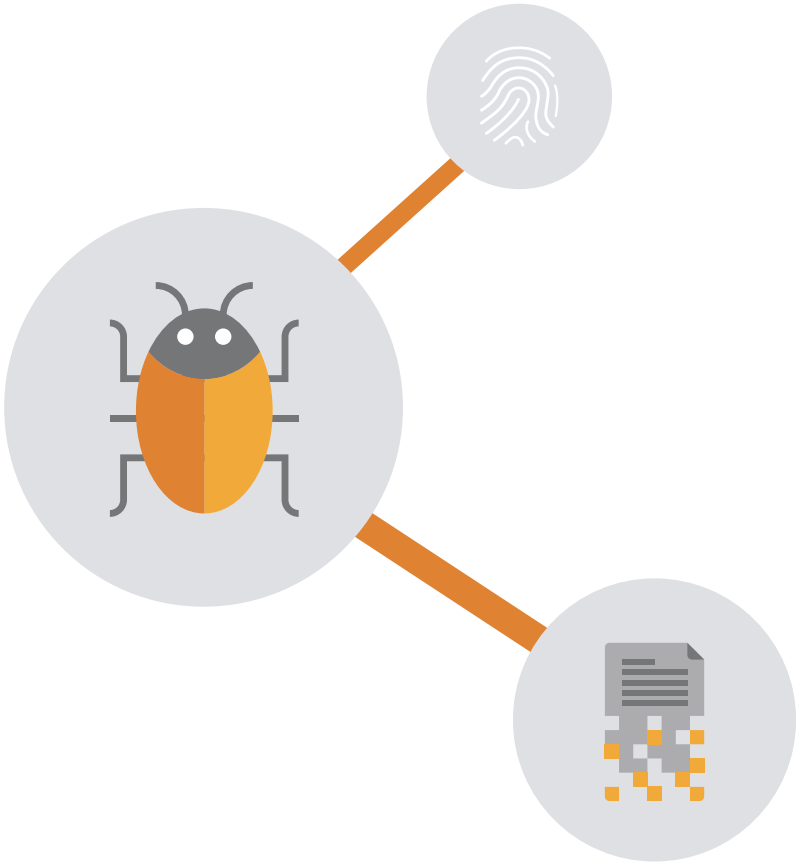
Las empresas siguen teniendo problemas para evaluar el coste de las brechas de seguridad. Antiguamente, existía la creencia de que el impacto de los delitos informáticos se veía reflejado en un descenso en el precio de las acciones.

Pero el precio de las acciones no es más que una parte del conjunto. De hecho, no es más que la primera parte. Si bien el precio de las acciones puede restablecerse pasadas unas semanas, los costes a largo plazo se acumulan. Nuevos programas de seguridad, personal de sustitución e incluso gastos legales.

Tras sufrir un ataque informático, todos estos factores pueden poner en jaque a las empresas durante largos periodos de tiempo.
Y los costes van en aumento. Un reciente estudio de Ponemon reveló que los costes anuales medios de una brecha de seguridad pasaron de **7,7 millones de dólares** en 2015 a **9,5 millones de dólares** en 2016.[7]

Fuente: [8] Ponemon Institute Cost of Cyber Crime Study 2016 (Ponemon Institute: Estudio sobre el coste de los delitos informáticos de 2016)

2 Las brechas de seguridad son poco frecuentes, por lo que no es necesaria una gran protección



IDC reveló[8] que la proporción de empresas que sufren una brecha de seguridad alcanzó el 99 % en 2016, mientras que el número de empresas que afirmó haber sufrido entre 6 y 10 ataques informáticos al año, pasó del 9 % en 2014 al 18,9 % en 2016.[9]

Es muy probable que estas cifras tiendan a la baja. Las empresas no suelen informar de los ataques informáticos que sufren para evitar la mala prensa.

El otro punto que no tiene en cuenta este mito es el impacto debilitador que puede tener una brecha de seguridad. Es posible que su empresa solo experimente una fuga de información. Pero esto es más que suficiente para generar importantes retos.

Fuente: [8] IDC [9] Ponemon Institute Cost of Cyber Crime Study 2016 (Ponemon Institute: Estudio sobre el coste de los delitos informáticos de 2016)

3 Hemos contratado a un especialista en TI encargado de la seguridad y, por lo tanto, no debemos preocuparnos

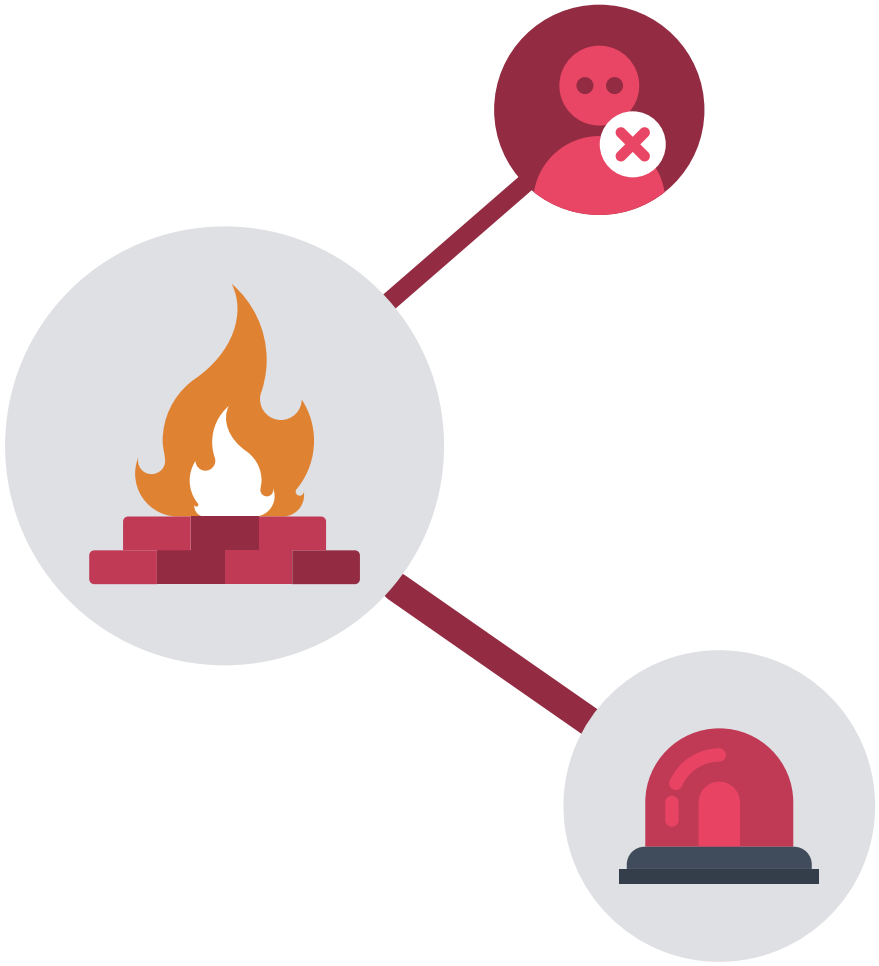
Si bien la contratación de un experto es una buena idea, se debería formar a todos los empleados de una empresa en cómo adoptar unas buenas prácticas en seguridad cibernética.

Consideremos por un momento a un empleado que, ignorando lo que conlleva, descarga los archivos adjuntos maliciosos de un mensaje de correo electrónico o visita un sitio web peligroso, infectando la red de una empresa con malware que ralentiza los ordenadores o envía información confidencial a un delincuente cibernético.

Según el informe de amenazas cibernéticas de 2016 de CyberEdge, las organizaciones han declarado que una «falta de concienciación sobre la seguridad» supone el principal problema que les impide defenderse de las amenazas de seguridad. Para las empresas, este hecho es más preocupante que la «falta de presupuesto» o la «falta de personal cualificado».[10]

Fuente: [10] Ponemon Institute Cost of Cyber Crime Study 2016 (Ponemon Institute: Estudio sobre el coste de los delitos informáticos de 2016)

4 Nuestros sistemas disponen de un potente antivirus y, por lo tanto, estamos protegidos



Los antivirus escanean los sistemas en busca de malware descargado de sitios web o mensajes de correo electrónico. Pero los delincuentes cibernéticos cuentan con otros medios para eludir esta protección.

Un software antivirus es incapaz de bloquear ciberataques como: ataques de denegación de servicios (DDoS), que inundan de tráfico basura un sitio web hasta que este se ralentiza o deja de funcionar; ataques basados en la web, donde los hackers inyectan código malicioso en un sitio web con el objetivo de robar datos o realizar espionajes remotos; y hackers que obtienen el acceso mediante dispositivos robados.

5 Si un intruso entra en el sistema, nos daremos cuenta enseguida

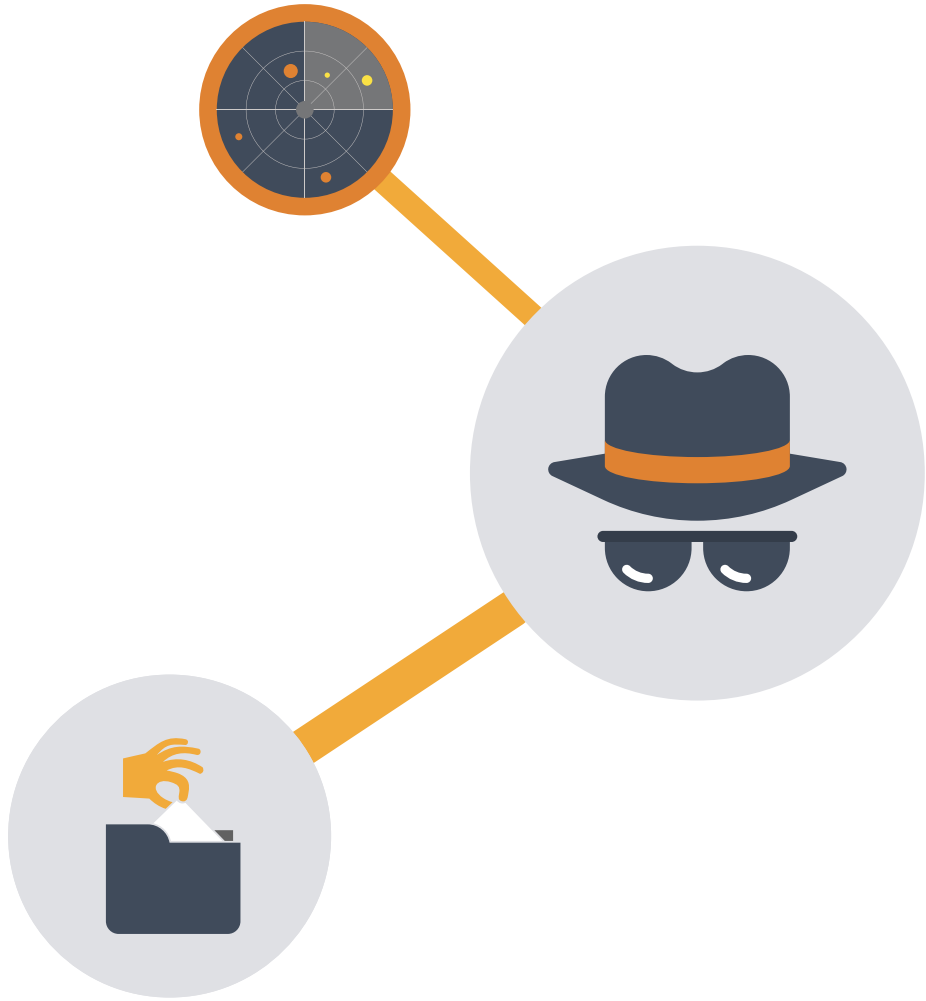
Detectar un ciberataque no es sencillo. El malware que se filtra en un sistema no altera las operaciones inmediatamente; en su lugar, puede espiar el sistema y darle información al hacker para que orqueste ataques más definidos, a menudo para conseguir acceso a toda la red.

Estos ataques realizados en sistemas específicos reciben el nombre de amenazas persistentes avanzadas (APT). Los ataques APT se caracterizan por un seguimiento y obtención continuada de datos de una infraestructura informática concreta durante un periodo de tiempo, a menudo sin ser detectados.

La consultora informática Daisy Group calculó que se podrían hackear la mitad de las empresas británicas en menos de una hora.

CONSEJO:
El control de los datos de salida en casos de tráfico superior a lo habitual, puede ayudar a identificar el robo de datos (un posible ataque APT).

ACTÚE:
Elija software de seguridad con protección de datos, como HP SureStart, que restaura la BIOS de un ordenador automáticamente cuando detecta un ataque de malware, deteniendo las brechas de seguridad antes de que los datos se vean afectados.

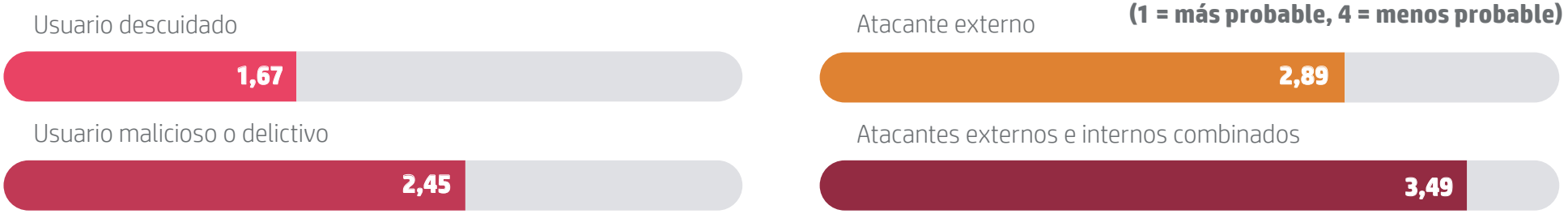


¿De dónde provienen las amenazas?

La protección de una red comienza por conocer sus puntos más débiles.

La causa más probable de una brecha de datos:[11]

(1 = más probable, 4 = menos probable)



Tipos de amenazas externas más comunes:

- **30 %** Suplantación de identidad
- **32 %** Virus
- **38 %** Malware

Modo en que se producen las brechas de seguridad internas:[12]

- **21 %** Empleados que utilizan una red doméstica/ pública
- **29 %** Empleados que utilizan dispositivos personales
- **42 %** Error humano/del usuario

Fuente: [11] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [12] Ponemon Institute Cost of Cyber Crime Study 2015 (Ponemon Institute: Estudio sobre el coste de los delitos informáticos de 2015)

¿Cuánto cuesta recuperarse de un delito cibernético?

Los tipos de ciberataque más costosos son:[13]

25 %

Un millón de libras esterlinas

Código malicioso y malware

Software que daña un sistema creando agujeros de seguridad, dañando archivos o robando datos (como secuencias, virus y gusanos)

24 %

960 000 libras esterlinas

Ataques de denegación de servicios

Los ataques «DDoS» provocan inundaciones de tráfico web ocasionando que el sitio web y los servidores de una empresa dejen de funcionar

16 %

640 000 libras esterlinas

Ataques web

Ataques enfocados a los visitantes de su sitio web, como puede ser un código inyectado que redirige a los navegadores a sitios web con malware

13 %

520 000 libras esterlinas

Dispositivos robados

Los dispositivos perdidos de los empleados con acceso a datos de inicio de sesión de la empresa pueden derivar en robos de datos y de identidad

9 %

360 000 libras esterlinas

Suplantación de identidad e ingeniería social

Mensajes de correo electrónico o mensajes emergentes que se hacen pasar como solicitudes de acceso legítimas

9 %

360 000 libras esterlinas

Abuso de información privilegiada

Empleados que ceden información confidencial

4 %

160 000 libras esterlinas

Botnets

Redes de ordenadores infectados que se controlan para actividades maliciosas como el envío de correo no deseado

Fuente: [13] http://www.nttcomsecurity.com/as/uploads/documentdatabase/Global_Infographic_Risk_Value_UEA_v1.pdf

El impacto de los delitos cibernéticos en las empresas

El verdadero coste de los delitos cibernéticos no se limita a reparar el daño de una brecha

Las brechas de seguridad conllevan un precio muy alto. A grandes rasgos, existen tres formas en las que una brecha de seguridad puede perjudicar las finanzas de su empresa.

Recursos empresariales

Obviamente, las cosas tendrán que volver a la normalidad. Esto conlleva una dedicación de tiempo considerable por parte de los empleados, así como otros costes. Lo que significa que es muy probable que tenga que dejar de lado el trabajo que realmente genera ingresos.

Multas/sanciones

Cabe la posibilidad de que sea sancionado con una multa por incumplimiento (p. ej., HIPAA). Una vez se instaure el reglamento general de protección de datos de la Unión Europea el próximo año, las empresas que no cumplan la normativa, podrían verse obligadas a pagar una multa total del 4 % de su facturación global. Podría incluso acabar en los tribunales en el caso de que una fuga de información derivase en un incumplimiento de la confidencialidad de los clientes.

Reputación dañada

Este puede ser uno de los impactos más perjudiciales de una brecha de seguridad. Las brechas de seguridad permanecen durante mucho tiempo en la memoria colectiva. La recuperación de la confianza puede conllevar mucho tiempo.

Anatomía de un hackeo informático inesperado

Cuando Sony Pictures fue atacado en 2014, los hackers entraron literalmente por la puerta principal.[14]

Según «Lena», del grupo de hackers Guardianes de la paz (GOP, por sus siglas en inglés), que se autoproclaman autores del ataque, Sony «ya no se ocupa de la seguridad física». Los hackers accedieron a la red de Sony entrando físicamente en el edificio y robando las credenciales de un ordenador a un administrador del sistema.

Una vez dentro, introdujeron malware que se apropió de archivos privados, códigos fuentes y contraseñas de las bases de datos de Oracle y SQL. A partir de ahí, robaron los calendarios de producción de varias películas, mensajes de correo electrónico y documentos financieros, entre otros, y buena parte de ello fue publicado en Internet.

Los hackers amenazaron con publicar más datos confidenciales si la empresa no retiraba de los cines la película «La entrevista».

Sony acabó capitulando, perdió unos ingresos en taquilla incalculables y su reputación se vio seriamente dañada.

Sony cometió dos errores. No contar con que unos intrusos consiguieran acceder físicamente a los datos de la empresa, y no invertir en más capas de seguridad que podrían haber evitado el acceso a información confidencial después de la brecha de seguridad inicial.

Como escribió el experto en seguridad Bruce Schneier tras el ataque: «Todas las redes son vulnerables frente a un atacante habilidoso, firme y motivado». El truco consiste en saber dónde es vulnerable su red. Podría ser en la puerta delantera.

ACTÚE:
Cree un plan de respuesta frente a las brechas de seguridad para cada departamento, desde el de TI hasta el de atención al cliente, con el fin de minimizar el tiempo de recuperación.

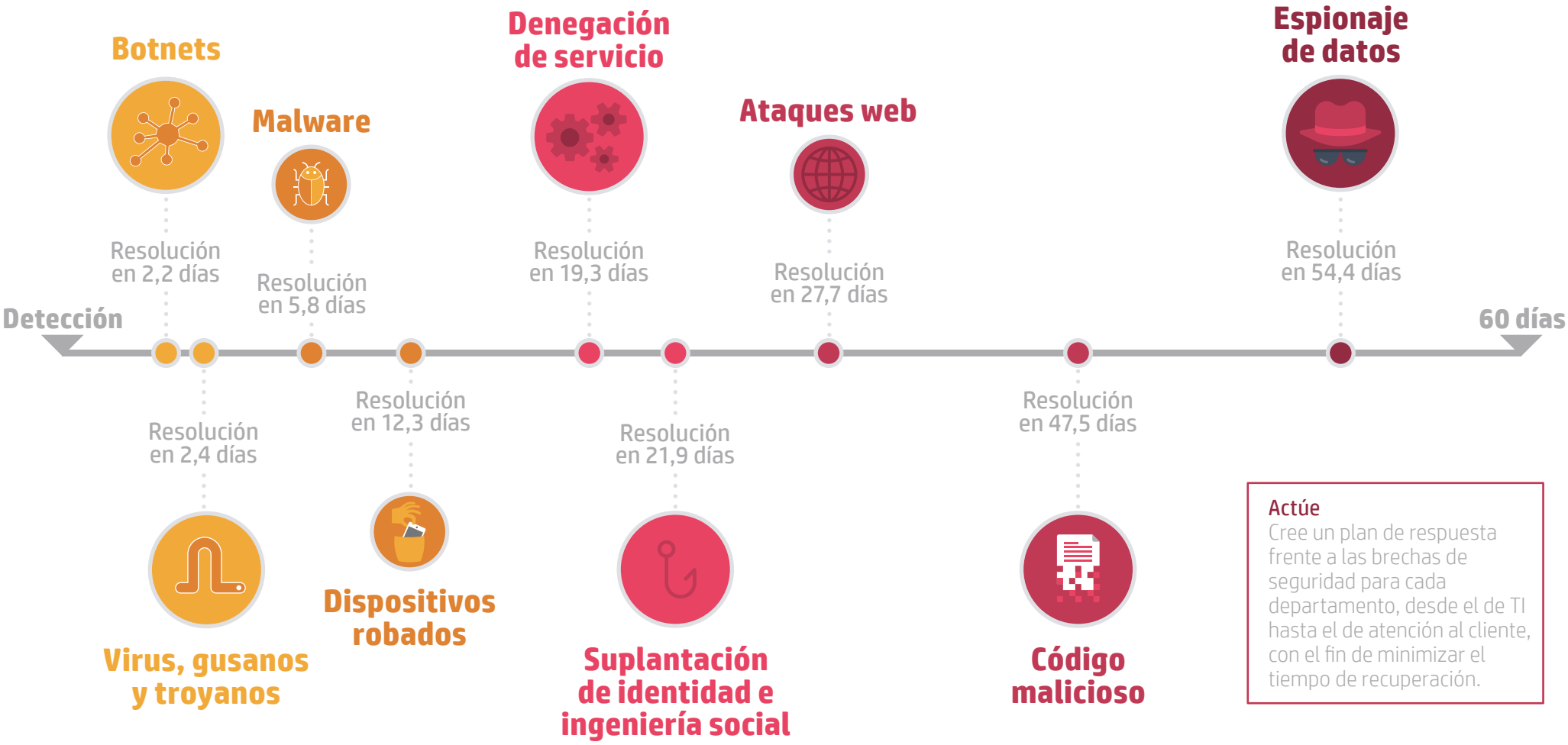
CONSEJO:
Los archivos adjuntos de los mensajes de correo electrónico son uno de los principales canales de transmisión de malware. Forme a su personal para que reconozca los archivos sospechosos camuflados como documentos legítimos.

- Coste estimado de los delitos cibernéticos en las empresas británicas: 21 000 millones de libras esterlinas[15]
- Coste medio de los delitos cibernéticos por empresa británica en 2016: 5,7 millones de libras esterlinas[16]
- Porcentaje de empresas británicas que sufrieron una brecha de seguridad o ataque cibernético en el periodo 2015-2016: 66 %[17]

Fuente: [14] http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?IR=T [15] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[16] https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/ Stat is $7.21m – have converted to £
[17] https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year

Crimen cibernético: el tiempo de recuperación

¿Cuánto se tarda en reparar el daño ocasionado por una brecha de datos? Ponemon Institute señala un promedio de 46 días. Una cifra potencialmente muy perjudicial para las PYMES británicas que dependen de la continuidad de sus operaciones.



Actúe
Cree un plan de respuesta frente a las brechas de seguridad para cada departamento, desde el de TI hasta el de atención al cliente, con el fin de minimizar el tiempo de recuperación.

Cómo proteger su empresa de los delitos cibernéticos

Consejos y estrategias esenciales en seguridad cibernética para empresas

A continuación indicamos seis objetivos comunes que utilizan los hackers para piratear los sistemas de seguridad de una empresa y qué se puede hacer al respecto.

Bases de datos de clientes

Servicios en la nube

Teléfonos y tablets de los empleados

Errores de los empleados

Internet de las cosas

Entradas de red

Conforme avanzamos hacia un mundo cada vez más digital, donde los datos tienen cada vez más valor, los delitos cibernéticos pueden adoptar muchas formas. Los delincuentes cibernéticos codician la información. Cada vez hay más dispositivos conectados a Internet en los lugares de trabajo, desde teléfonos inteligentes y tablets hasta impresoras con Wi-Fi, que proporcionan un número creciente de puntos de acceso a los hackers.

1 Bases de datos de clientes

Los datos financieros no son el único objetivo de los atacantes: se pueden utilizar datos como nombres y direcciones de correo electrónico para suplantar la identidad, generar correo no deseado o hackear otras cuentas.

Para los hackers, el ataque a empresas que ofrecen sus servicios a empresas todavía más grandes, supone un premio aún mayor. Digitalmente, esto puede equiparse a colarse en una tienda informática únicamente para acceder a la pared del sótano que se comunica con la cámara acorazada de un banco.

Una vez que los atacantes están dentro de un sistema más pequeño, se encuentran mejor situados para acceder a los datos de clientes que albergan los datos de clientes más importantes. ¿Cómo puede afectar esto a su base de datos de clientes? Los virus, los gusanos y los troyanos que se descargan de sitios web o mensajes de correo electrónico maliciosos, pueden revelar el código necesario para que un hacker entre y robe datos.

Cómo proteger los datos de sus clientes

- Utilice software de seguridad especial para empresas, que ofrece protección para redes, mensajes de correo electrónico y puntos de conexión.
- Actualice siempre el software de seguridad para bloquear el malware más actual.
- Descargue las actualizaciones de software de los programas del sistema, dado que los programas más antiguos pueden ser más vulnerables a los ataques.

2 Servicios en la nube

Cómo proteger la información en la nube

- Cifre la información más importante con herramientas como la tecnología Smartcrypt de PKWARE, que utiliza políticas de acceso para determinar la complejidad de un cifrado. De ese modo, los usuarios autorizados ven los datos que deberían ver, y los usuarios no autorizados no ven nada.
- Cree una contraseña segura para su cuenta en la nube. Del mismo modo, en la configuración de la cuenta en la nube, defina bien quién puede acceder a los datos y qué puede hacer con ellos.
- Solicite autenticación de dos factores, como un código de teléfono y una contraseña, para realizar cambios en los datos en la nube, como descargar, eliminar o mover archivos.

La informática en la nube se ha vuelto fundamental dentro de la infraestructura de una empresa.

La encuesta sobre informática en la nube de 2016 de IDG[18] reveló que el 70 % de las empresas tiene al menos una parte de su infraestructura en la nube, mientras que Tripwire reveló que el 90 % utiliza la nube para la infraestructura y/o para almacenar datos, incluidos los más importantes.[12]

Sin duda, la seguridad es una preocupación; sin embargo, los datos suelen estar más seguros en la nube, almacenados en servidores externos por una empresa cuya reputación dependa de mantenerlos a salvo.

De este modo, el 64 % de las empresas encuestadas por Tripwire consideran más segura la nube que los sistemas convencionales.

Por suerte, esta confianza no está fuera de lugar: según la encuesta BIS de 2015,[19] solo el 7 % de las empresas (grandes y pequeñas) ha experimentado brechas de seguridad importantes en sus servicios en la nube, por lo general, como resultado de permisos de acceso o contraseñas insuficientes. Sin embargo, una nube segura necesita unos estrictos controles de seguridad internos. Piense en la puerta delantera de Sony.

Fuente:

[12] Ponemon Institute Cost of Cyber Crime Study 2015 (Ponemon Institute: Estudio sobre el coste de los delitos informáticos de 2015)

[18] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey

[19] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/

3 Teléfonos y tablets de los empleados

Muchas personas utilizan sus dispositivos personales para realizar labores de oficina.

Las políticas BYOD («Traiga su propio dispositivo») suponen una forma efectiva de aprovechar los teléfonos de los empleados. Esta es una tendencia al alza; de hecho, el 53,2 % de las organizaciones quiere implementar una política BYOD en los próximos dos años.[20] Pero estos dispositivos son objetivos fáciles para los hackers.

Se estima que una de cada cinco aplicaciones Android es portadora de algún tipo de malware invasivo que podría pasar a los archivos y sistemas de una empresa y controlar sus actividades o robar información.

Esta es una amenaza que va en aumento: un 64,9 % de las organizaciones declara que el número de amenazas contra sus dispositivos móviles ha aumentado.[20]

Aquellos empleados a los que les hayan robado sus teléfonos también pueden ser, inconscientemente, una puerta de entrada para los hackers. Supongamos que un ladrón de teléfonos le vende un dispositivo a un comprador en el mercado negro con el fin de infringir la seguridad de la empresa de la víctima o adentrarse en los sistemas de un cliente más grande. Las organizaciones puntuaron con un 3,54 sobre 5 su capacidad para defenderse de las amenazas de seguridad originadas desde dispositivos móviles. Esta fue la puntuación más baja de entre todos los orígenes potenciales de amenazas que se abordaron.[20]

Cómo proteger los dispositivos de los empleados

- Instale una herramienta de detección de amenazas, como X-Ray de Duo Labs, para dispositivos Android con el fin de facilitar el seguimiento de aplicaciones no autorizadas y códigos sospechosos.
- Solicite a los empleados que habiliten los barridos remotos (gratuitos para Android, iPhone y Windows Phone, y con subscripción para Blackberry); de ese modo, en caso de pérdida, podrán eliminarse los datos confidenciales personales y de la empresa.
- Solicite a los empleados que habiliten el cifrado de dispositivo en sus teléfonos para la protección de datos (esta función se incluye de forma predeterminada en los nuevos teléfonos iOS y Android).

Fuente: [20] Ponemon Institute Cost of Cyber Crime Study 2015 (Ponemon Institute: Estudio sobre el coste de los delitos informáticos de 2015)

4 Errores de los empleados

Cómo ayudar a los empleados

- Forme a su personal en materia de mejores prácticas de seguridad cibernética e imparta formación cada cierto tiempo para que conozca las últimas amenazas.
- Desarrolle un protocolo de seguridad adaptado a su empresa y a los tipos de datos que procesa.
- Cree un equipo para que comunique la política de seguridad cibernética tanto a empleados como a clientes y socios.

El principio básico de la seguridad cibernética consiste en disponer de una buena política de contraseñas. El 31 % de las peores brechas de seguridad de 2015 fue ocasionado por un incidente relacionado con los empleados.

Los atacantes suelen sacar partido de los errores humanos, desde hackear contraseñas poco seguras hasta robar documentos enviados por correo electrónico a través de una conexión insegura, o suplantar la identidad de un mensaje de correo electrónico destinado a un empleado en concreto.

5 Prepárese para el Internet de las cosas

IDC predice que el número de dispositivos conectados a Internet llegará a los 30 000 millones en 2020, por encima de los 13 000 millones previstos.[21]

Si bien los ordenadores de oficina están protegidos al menos con contraseñas, e idealmente con software de seguridad, las colas de impresión y los trabajos de impresión no suelen estar protegidos con protocolos de seguridad similares.

Las impresoras no seguras (y otro hardware en red) pueden ser una presa fácil de los «programas de rastreo», capaces de registrar las tareas de impresión y el tráfico de red, nombres de usuario e información sobre contraseñas, y enviarlo todo al servidor del delincuente cibernético.

Debemos mencionar que la famosa brecha de seguridad de Dyn estaba supuestamente relacionada con una red de cámaras de vigilancia habilitadas en la web de una única empresa denominada, XiongMai Technologies, según la empresa de seguridad Flashpoint.

Esto demuestra que todos los dispositivos de una red son un punto de acceso, y que una red es tan segura como el dispositivo menos seguro. El 97 % de las organizaciones ofrece prácticas de seguridad para ordenadores de sobremesa/portátiles, el 77 % para dispositivos móviles, pero tan solo el 57 % ofrece prácticas de seguridad para impresoras.[22] La única manera que tienen las empresas de mantenerse seguras es mediante la implementación de prácticas de seguridad en todos sus dispositivos de puntos de conexión.

Cómo prepararse para el Internet de las cosas.

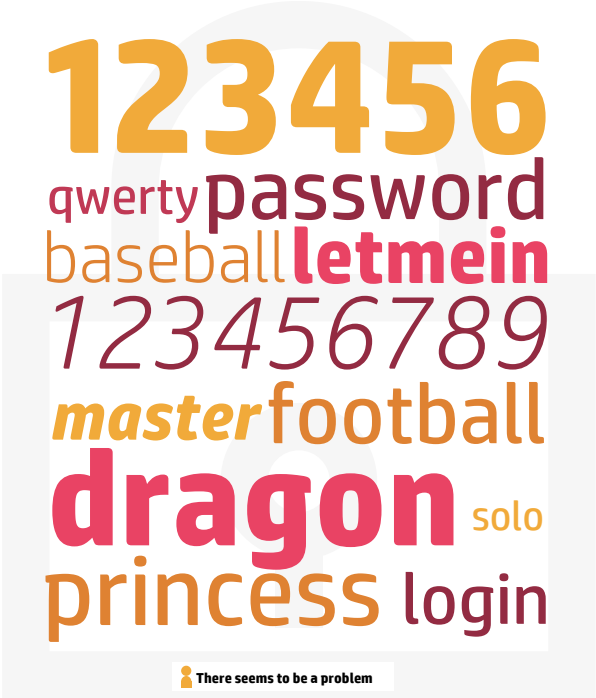
- Elimine o deshabilite las funcionalidades innecesarias del hardware, ya que cuantas más funciones haya, más puertas de entrada se abren para los atacantes.

Fuente: [21] PwC: The Global State of Information Security Survey 2016 (PwC: Encuesta sobre el estado global de la seguridad de la información de 2016)
[22] HPI Printer Security Research (investigación sobre la seguridad de las impresoras de HP), Spiceworks 2016

Contraseñas y ransomware

Las contraseñas más usadas

A principios de 2013, un periodista de Ars Technica que nunca había cometido delitos informáticos ni tenía experiencia alguna en vulneración de sistemas protegidos por contraseña, logró descifrar 8000 de más 16 000 contraseñas cifradas, en un solo día*. ¿Qué posibilidades tiene una contraseña excesivamente simple de resistir la acción de un hacker?



¿Qué es un ransomware?

Los delincuentes informáticos están haciendo un uso cada vez mayor del ransomware, una forma de malware (programa malicioso) que bloquea el acceso a un sistema que solo podrá ser liberado mediante el pago de un rescate en dinero electrónico o bitcoin. En 2013, se produjo la invasión de un troyano denominado Cryptolocker, que afectó a miles de usuarios y llegó a llamar la atención de la agencia nacional contra el crimen del Reino Unido y su unidad nacional contra el delito informático. Así es como se lleva a cabo este tipo de ataques:

1. Instalación	El código malicioso se instala en el ordenador después de una descarga imprevista realizada por el usuario, sirviéndose de un mensaje de correo electrónico o de un sitio web malicioso.
2. Alerta a la sede	El ransomware se conecta al servidor y establece una conexión cifrada.
3. Cifrado de los archivos de usuario	El ransomware escanea los archivos de la red del usuario y los cifra, haciéndolos inaccesibles.
4. Extorsión	Generalmente, aparece un mensaje en la pantalla del usuario indicando un tiempo límite y una cantidad que debe pagar para liberar los archivos o, en caso contrario, serán borrados.
5. Pago	La empresa se ve obligada a comprar una cierta cantidad en moneda electrónica como bitcoin y transferirla al hacker, con la esperanza de que libere los archivos secuestrados.

* Miscelánea de datos

6 Entradas de red

Cuando los hackers quieren adentrarse en una red, pueden desencadenar un ataque DDoS en el que miles de máquinas infectadas con malware se unen para generar tal cantidad de tráfico basura que la red sucumbe al ataque.

A menudo, los atacantes DDoS distraen a los administradores de los sitios con un sistema congelado mientras roban datos o instalan malware, con el fin de planificar robos de datos futuros. Parte de los ataques DDoS son también el resultado de «script kiddies», hackers novatos que tan solo quieren interrumpir la actividad de un sitio de Internet porque pueden. La interrupción de la actividad de un sitio web, aunque solo sea durante pocas horas, puede ser devastadora para el resultado y la reputación de una empresa.

CONSEJO:
Invierta en hardware que ofrezca protección integrada, como autenticación avanzada y herramientas de cifrado.

Cómo proteger una red

- Cree sistemas que controlen el tráfico que entra y sale de la red. Los picos repentinos pueden significar un ataque, mientras que una actividad constante pero inexplicable puede significar que un troyano está enviando datos a su matriz.
- Filtre todo el tráfico, de modo que solo acabe en nuestra red el tráfico necesario para el funcionamiento de nuestra empresa.
- Asegúrese de que todos los enrutadores, conmutadores u otros dispositivos de red funcionan con el mismo software y funcionalidades básicos, y descargue siempre las actualizaciones de software.

El futuro de la seguridad cibernética empresarial

Las empresas dependen tanto de Internet que la construcción de sólidas defensas de seguridad cibernética se ha convertido en un asunto de vital importancia

Hoy en día, los trabajadores traen sus propios dispositivos al trabajo. Las empresas utilizan plataformas informáticas en la nube y externalizan los servicios técnicos clave. Y cada vez hay más gente que trabaja de forma remota. La seguridad cibernética se complica cuando no existe ningún tipo de control sobre el dispositivo, la infraestructura o el espacio de trabajo.

Al mismo tiempo, los teléfonos nos han enseñado que se pueden hacer negocios donde sea y cuando sea. Una cafetería es un lugar tan bueno para trabajar como una oficina. Utilizamos redes Wi-Fi públicas para procesar enormes cantidades de datos personales y empresariales, a menudo mediante el uso de teléfonos que apenas están protegidos. Los delincuentes son conscientes de esta tendencia. La seguridad se ve afectada cuando no cuidamos nuestro entorno de trabajo.

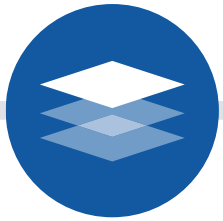
En los años venideros, esto implicará mucho más que la simple instalación de un programa antivirus en nuestros dispositivos o la actualización de nuestras contraseñas cada seis meses. En cambio, las empresas tendrán que adoptar medidas de seguridad optimizadas que funcionen tanto de forma remota como lo harían en una oficina gestionada por un administrador de TI.

Para las organizaciones distribuidas del mañana, la seguridad cibernética dependerá de sofisticados análisis que aíslen comportamientos infrecuentes y de la seguridad por capas que proteja todos los puntos de acceso.

El futuro de la seguridad cibernética empresarial

Analítica: el detective de seguridad cibernética

Aunque su sitio web no tenga demasiado tráfico, sí tendrá unos patrones. La utilización de herramientas analíticas que evalúen y registren la actividad, puede facilitar el diagnóstico cuando algo vaya mal. En primera instancia, estas herramientas realizan un seguimiento y documentan el comportamiento normal con el fin de detectar anomalías posteriormente. Una vez detectadas, los administradores pueden pasar a la ofensiva y eliminar los ataques antes de que estos tengan la oportunidad de desatar un caos cibernético.



Multicapa: un paso por delante de los atacantes

En ocasiones denominada «defensa en profundidad», la seguridad por capas protege todos los puntos de acceso de diversas formas. Los métodos comunes incluyen certificados SSL de validación ampliada que dificultan la falsificación de las credenciales necesarias para entrar en una red segura. También puede ser de utilidad una autenticación multifactor que obligue a los invasores a descifrar algo más que una contraseña.

Independientemente de la tecnología específica de su oficina, el principio subyacente a la protección por capas es que todas las áreas confidenciales de su red estén cerradas de algún modo. Puede que sus usuarios y socios necesiten más tiempo y esfuerzo para acceder a los datos más importantes, pero estos inconvenientes merecen la pena si priorizamos la seguridad de una empresa.

Actúe ahora

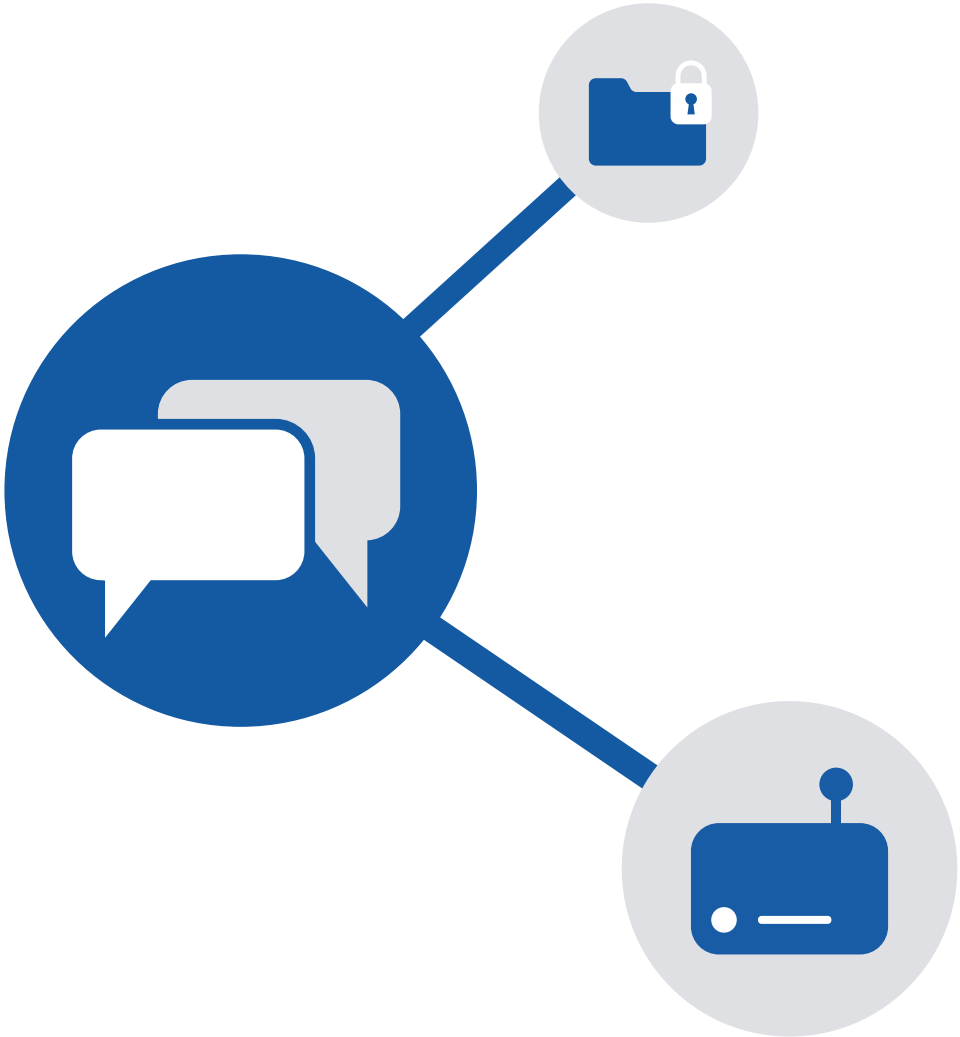
La inversión en software de seguridad y en formación es la mejor defensa. Comience por efectuar una auditoría de sus sistemas e infraestructura. ¿Se está haciendo lo suficiente? ¿Qué se podría mejorar?

Por último, también puede ponerse en contacto con los expertos de Hewlett Packard Inc. Nuestra base de conocimiento colectivo se centra en adelantarnos a las amenazas, no solo en responder a las mismas. Para obtener más información, visítenos en HP.com.

CONSEJO:
Realice un seguimiento y documente el comportamiento normal en primera instancia, con el fin de detectar anomalías posteriormente.

Consideraciones de seguridad para dispositivos de puntos de conexión

Protección para todos y cada uno de los dispositivos de su red



Un informe de seguridad elaborado por Spiceworks[4] reveló que los principales orígenes de las amenazas a la seguridad a las que se enfrentaban las empresas eran:

- Portátiles y ordenadores de sobremesa: 81 % externos y 80 % internos
- Dispositivos móviles: 36 % externos y 38 % internos
- Impresoras: 16 % externas y 16 % internas

De estas amenazas, ¿cuál debería solucionarse antes? Muy sencillo: todas. Si bien esto puede parecer muy obvio, un número alarmante de organizaciones sigue dudando con respecto a qué dispositivos debe proteger.

Para HP, todo dispositivo conectado a una red debe estar protegido. Es así de simple: una red es tan segura como el dispositivo menos seguro conectado a la misma.

Es posible que la lógica intuitiva nos diga que la protección de una impresora conectada no es tan importante como la protección de toda la flota de portátiles. Pero el riesgo es el mismo. Los hackers son famosos por centrarse en impresoras, o en cualquier dispositivo inteligente conectado a una red, porque saben que estos dispositivos no suelen estar bien protegidos y además ofrecen el mismo nivel de acceso a una red.

Fuente: [24] HP Printer Security Research 2016 (Investigación sobre la seguridad de las impresoras de HP de 2016), Spiceworks

HP: liderando el camino hacia un nuevo entorno

La seguridad cibernética está cambiando. Disponemos de las herramientas necesarias para ayudarle a protegerse.

En lo que respecta a la seguridad cibernética, las soluciones inmediatas no existen. Una defensa sólida requiere un enfoque que englobe redes, dispositivos y personas. La elección de la tecnología adecuada es un buen comienzo.

En HP, la seguridad es lo primero. Nuestra gama HP Premium Elite presenta funciones de seguridad líderes en el mercado, como HP SureStart, la primera BIOS con capacidades de recuperación automática del mundo.

HP equipa sus dispositivos con:

- **Bloqueo de Bluetooth:** la máquina apaga automáticamente la conexión Bluetooth cuando se marcha, y la enciende cuando vuelve.
- **Seguridad biométrica:** reconocimiento facial y dactilar que ofrece acceso únicamente a usuarios autentificados biométricamente.
- **Pantallas HP SureView*:** los monitores oscurecidos evitan que otras personas vean las pantallas y protegen el material confidencial cuando se trabaja durante los desplazamientos.
- **HP SureStart:** los dispositivos HP Elite controlan su BIOS cada 15 minutos. En caso de que se detecte alguna anomalía, restablecen el ordenador a su estado original, expulsando de ese modo a los posibles intrusos.

Los dispositivos HP Elite no protegen su empresa por sí solos. Pero sí que constituyen una sólida primera línea. Visite www8.hp.com para obtener más información sobre la completa gama HP Elite.

* Modelos seleccionados

HP: liderando el camino hacia una nueva perspectiva en la impresión

Defienda su red con la impresión más segura del mundo*

«Resultado de su permanente inversión en seguridad de impresión, HP cuenta con el portfolio más amplio y mejor constituido del mercado en soluciones y servicios de seguridad».

– Quocirca, enero de 2017**

HP equipa sus dispositivos con:

- **Intrusión en tiempo real:** la detección de intrusiones en tiempo real de HP ayuda a proteger los dispositivos mientras están en funcionamiento y conectados a la red, precisamente cuando se producen la mayoría de los ataques.
- **Jet Advantage Security Manager:** ofrece al administrador de sistemas de TI una manera sencilla y directa de evaluar y, si es necesario, corregir ajustes de seguridad en toda la flota de dispositivos para cumplir las políticas de seguridad previamente establecidas por la empresa.
- **HP SureStart:** durante el reinicio, HP SureStart detecta y previene la ejecución de códigos maliciosos y repara la BIOS automáticamente. Se reinicia a partir de una copia «perfecta» integrada.
- **Listas blancas:** aseguran que solo se cargue en la memoria el código HP auténtico y conocido como válido. Si se detecta una anomalía, el dispositivo se reinicia a un estado seguro sin conexión y notifica la situación a TI.

Fuentes: *5 La declaración de la «Impresión más segura» se basa en la revisión de HP de 2016 sobre las funciones de seguridad publicadas de las impresoras de la competencia de la misma categoría. Solo HP ofrece una combinación de funciones de seguridad que pueden supervisar para detectar y detener de forma automática un ataque y, a continuación, autovalidar la integridad del software en un reinicio. **Quocirca: «Print security: An imperative in the IoT era» (Seguridad de la impresión: un imperativo en la era de IoT), quocirca.com/content/print-security-imperative-iot-era, enero de 2017.

Glosario y lecturas complementarias

Acceso a herramientas de gobernanza

Ataques web:
A menudo, un ataque web implica redirigir un navegador a un sitio web malicioso.

Botnet:
Generalmente, hace referencia a un tipo de programa automatizado, diseñado para acceder y controlar ordenadores conectados a Internet sin conocimiento del propietario. A menudo, los ordenadores se ven infectados con malware. Los hackers utilizan los botnets para provocar un **ataque de denegación de servicio** en un sitio web.

Controles de perímetro:
Una categoría general que describe la defensa cibernética en el punto donde el Internet público u otra red pública coincide con una red privada gestionada y de titularidad local. **Suelen estar involucradas** distintas capas y tipos de dispositivo.

Gusanos:
Al contrario que los virus, que se propagan al compartir un archivo portador, los gusanos pueden reproducirse independientemente de un archivo portador, como un documento de Word o una hoja de Excel y, por tanto, no necesitan una interacción humana adicional para causar estragos. Los sistemas de mensajería instantánea son conocidos por propagar gusanos. Skype los sufrió en 2012.

Herramientas de gestión de políticas:
En términos generales, las herramientas de gestión de políticas establecen un estándar para lo que pueden y no pueden ver ciertos usuarios, y después aplican esa política a toda una red. La consistencia da seguridad (al menos en teoría).

Herramientas GRC:
Hacen referencia a iniciativas amplias y coordinadas dentro de una empresa, destinadas a gestionar y regir las operaciones de tal modo que cumplan con las normativas y que, como resultado, reduzcan los riesgos.

Herramientas para evitar la pérdida de datos:
Una amplia categoría de software cuyo objetivo es controlar los datos confidenciales y bloquear los intentos de acceso o copia por parte de personal no autorizado. Existen distintos métodos que permiten proteger el punto de acceso mientras atraviesa una red, o en un sistema de datos. Gartner estimó que este mercado **crecería un 25 %** en 2013.

Ingeniería social:
Un atacante trabaja para coaccionar a un usuario autorizado y hacer que comparta información que no debería, otorgando acceso a un atacante.

Malware:
Una amplia categoría de software que puede provocar daños o incluso inutilizar otros sistemas. Virus, gusanos y troyanos son ejemplos de malware. En relación con el estudio de Ponemon citado en este libro electrónico, el malware se considera distinto a los virus que «residen en los puntos de conexión y todavía no se han infiltrado en una red».

Suplantación de identidad:
A menudo se lleva a cabo por correo electrónico, donde un atacante solicita información de identificación en un cuadro de diálogo con aspecto legítimo.

Glosario y lecturas complementarias

Sistemas inteligentes de seguridad:
Una amplia variedad de inteligencia de seguridad puede ayudar a reunir y sintetizar información relacionada con las amenazas. Los sistemas varían desde gestores de registros hasta sistemas para detectar anomalías en la red.

Tecnologías de cifrado:
Herramientas que **hacen ilegibles los datos** sin ningún tipo de decodificador. El comisionado de información del Reino Unido se ha pronunciado **sumamente a favor** de varios tipos de cifrado en los últimos años. Recientemente, el gobierno se ha visto obligado a **cambiar su postura en cuanto a la tecnología de cifrado** como consecuencia de las duras críticas.

Tecnologías de cortafuegos:
Otro término general que describe un estilo de dispositivo que utiliza algoritmos y otras técnicas para impedir al tráfico y usuarios no autorizados el acceso a una red. **Las próximas versiones** de estos dispositivos serán potentes gracias a la combinación de funciones de las que antes se encargaban varios dispositivos. La detección de intrusos, por ejemplo. También suelen reconocer las aplicaciones y, por lo tanto, conocen la diferencia entre el tráfico web de una implementación salesfore.com y de una página de Facebook.

Troyano:
Con un impacto similar al de un virus o gusano, es el usuario quien instala el troyano, por lo que este suele estar hábilmente oculto. Sus efectos varían desde cambios en la configuración del ordenador, hasta la eliminación de archivos o la creación de una «entrada trasera» que el hacker utiliza después.

Virus:
Código malicioso que es capaz de reproducirse y expandirse por una red.

4AA7-1085ESE