LA SEGURIDAD CIBERNÉTICA Y SU EMPRESA

Cuánto cuestan los delitos cibernéticos y cómo proteger sus datos

Brought to you by

CONTENIDO

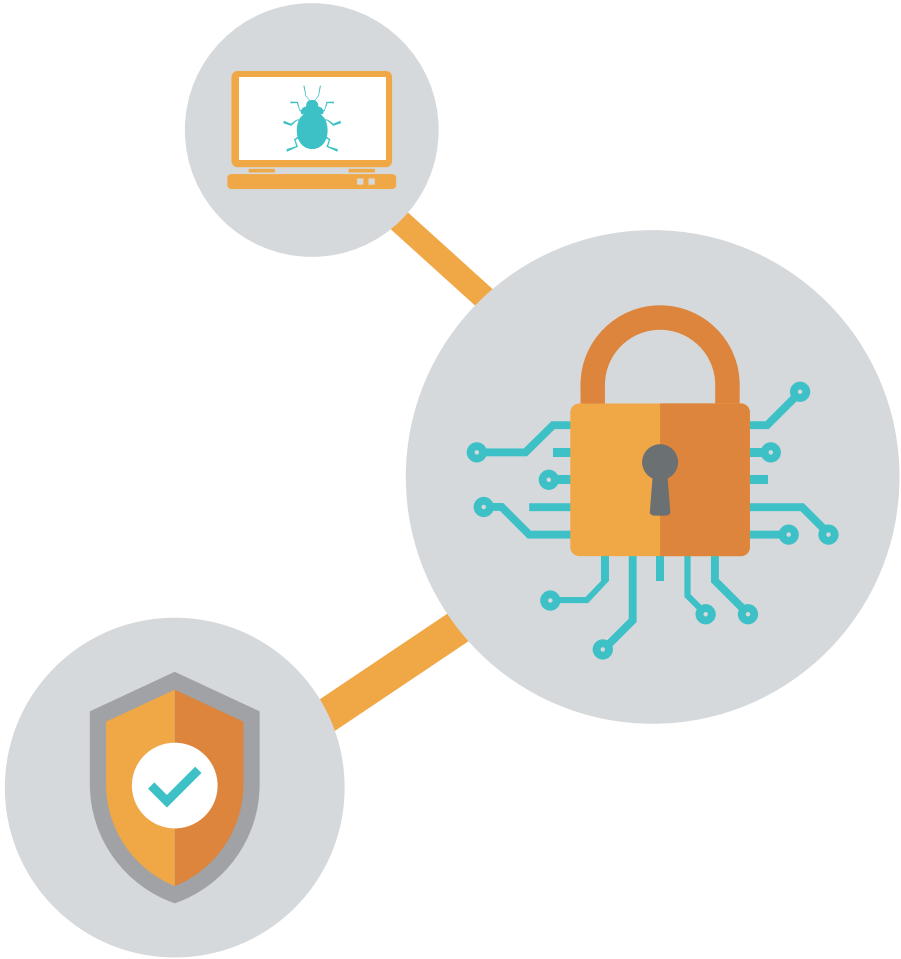
INTRODUCCIÓN

"Muchos ejecutivos afirman que los delitos cibernéticos definirán nuestra generación". – Dennis Chesley, Global Risk Consulting Leading, PwC[1]

La seguridad cibernética no es una preocupación reciente. Pero sí que va a más. Los piratas informáticos son cada vez mejores. Y disponen de más puntos por donde filtrarse a una red. El internet de las cosas está multiplicando el número de dispositivos terminales, que a menudo son la forma más sencilla de acceder a una red. Los objetivos son cada vez mayores y los problemas de red son cada vez más comunes.

El 21 de octubre de 2016, el proveedor estadounidense de DNS Dyn sufrió el mayor ataque de negación de servicio (DDoS) de la historia. Algunos de los mayores sitios web del mundo – incluidos Netflix,[2] Amazon y Twitter – estuvieron caídos 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, hubo muchos rumores de que el causante había sido un ataque DDoS.[3]



Fuente: [1] PwC: The Global State of Information Security Survey 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 infracciones de seguridad suponen algo más que mala publicidad. Cuestan dinero.

Según el informe Printer Security Survey Report 2016 de Spiceworks, el 34 % de las organizaciones dijeron que una infracción de seguridad implicaba el aumento de las llamadas al servicio de asistencia técnica y del tiempo de asistencia, el 29 % dijeron que las infracciones de seguridad reducían la productividad/efectividad y el 26 % dijeron que los aumentos del tiempo de inactividad en el sistema suponían un problema.[4]

Casi el 60 % de los jefes de seguridad entrevistados para una Evaluación de Jefes de Seguridad (CSO) de IBM dijeron que la sofisticación de los atacantes superaba la sofisticación de las defensas de sus organizaciones.[5]

Los responsables de seguridad (CIO), preocupados por el problema, llevan indicando desde hace 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 son evitables. En las siguientes páginas hablaremos sobre creencias falsas habituales en torno a la ciberseguridad, estudiaremos detalladamente el impacto que tienen los delitos cibernéticos en las empresas, y también hablaremos sobre qué puede hacer usted para defenderse de estos ataques. Por último, veremos qué nos depara el futuro y hablaremos sobre lo que está por venir y cómo prepararnos.

Sources: [4] HP Printer Security Research 2016, Spiceworks [5] IBM CSO Assessment 2014 [6] SIM IT Trends Survey 2015

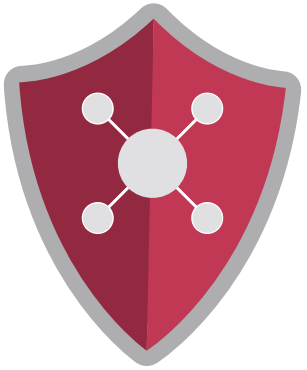
CINCO CREENCIAS FALSAS HABITUALES
QUE PUEDEN PROVOCAR QUE SU EMPRESA SUFRA DELITOS CIBERNÉTICOS

Cuando se produce una filtración de datos, las firmas más conocidas son las que acaparan los titulares. Sin embargo, ningún organismo está libre de esta amenaza. A continuación, incluimos cinco mitos sobre ciberseguridad que dejan a las empresas a merced de los piratas informáticos.

Violación de la seguridad

Fuga de Información

Prácticas de Seguridad



Software Antivirus

Ciberataques

1 LAS EMPRESAS SE RECUPERAN RÁPIDAMENTE DE CUALQUIER FILTRACIÓN

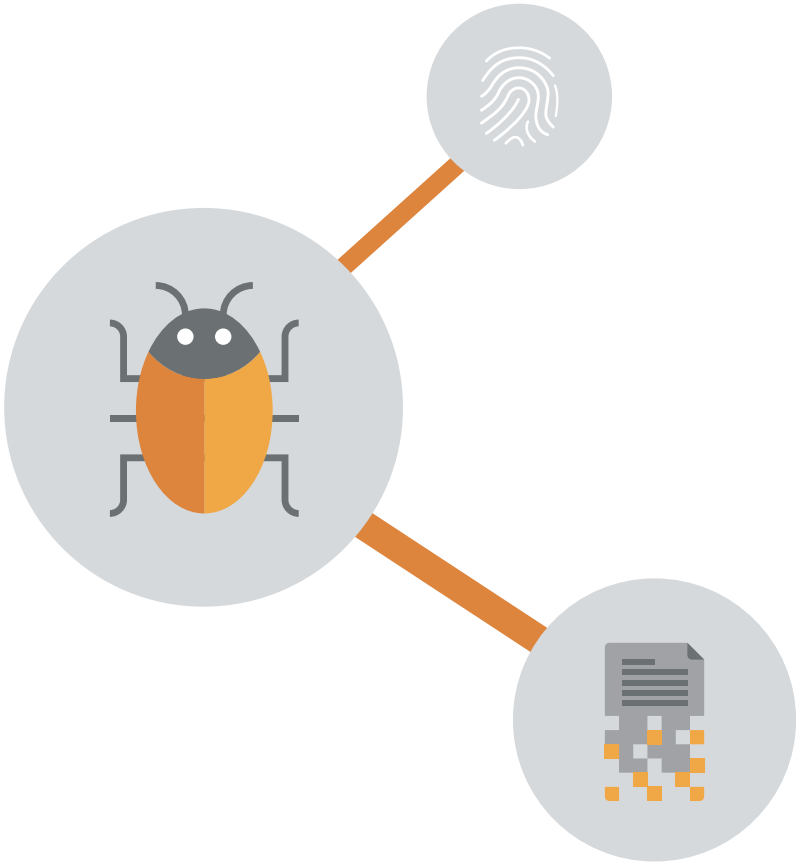
Para los organismos comerciales sigue siendo muy difícil medir el coste de las infracciones de seguridad. Antes existía la creencia de que el impacto de los delitos informáticos se veía reflejado en un descenso en el precio de las acciones.

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 en incluso gastos legales.

Tras sufrir un ataque informático, todos estos factores pueden poner en jaque a las empresas durante largo periodos de tiempo.
Y los costes van en aumento. Un reciente estudio de Ponemon[7] reveló que los costes anuales medios de una infracción de seguridad pasaron de **7,7 millones de USD** en 2015 a **9,5 millones de USD** en 2016.[8]

Fuente: [7] 2016 Cost of Cyber Crime Study & the Risk of Business Innovation [8] Ponemon Institute Cost of Cyber Crime Study 2016

2 LA VIOLACIÓN DE LAS MEDIDAS DE SEGURIDAD ES ALGO POCO FRECUENTE, POR LO QUE NO ES NECESARIA UNA PROTECCIÓN ACORDE



IDC descubrió[9] que la proporción de empresas que sufren vulneraciones de seguridad llegó al 99 % en 2016, si bien 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 (Cyber Threat Report 2016, CyberEdge).[10]

Es muy probable que estas cifras tiren por lo bajo. Las empresas no suelen informar de los ataques informáticos que sufren a fin de evitar la mala prensa.

El otro punto que se salta este mito es el impacto debilitador que puede tener una violación de red. Puede que su empresa solo sufra una violación de seguridad. Pero esto es más que suficiente para provocar problemas a la larga.

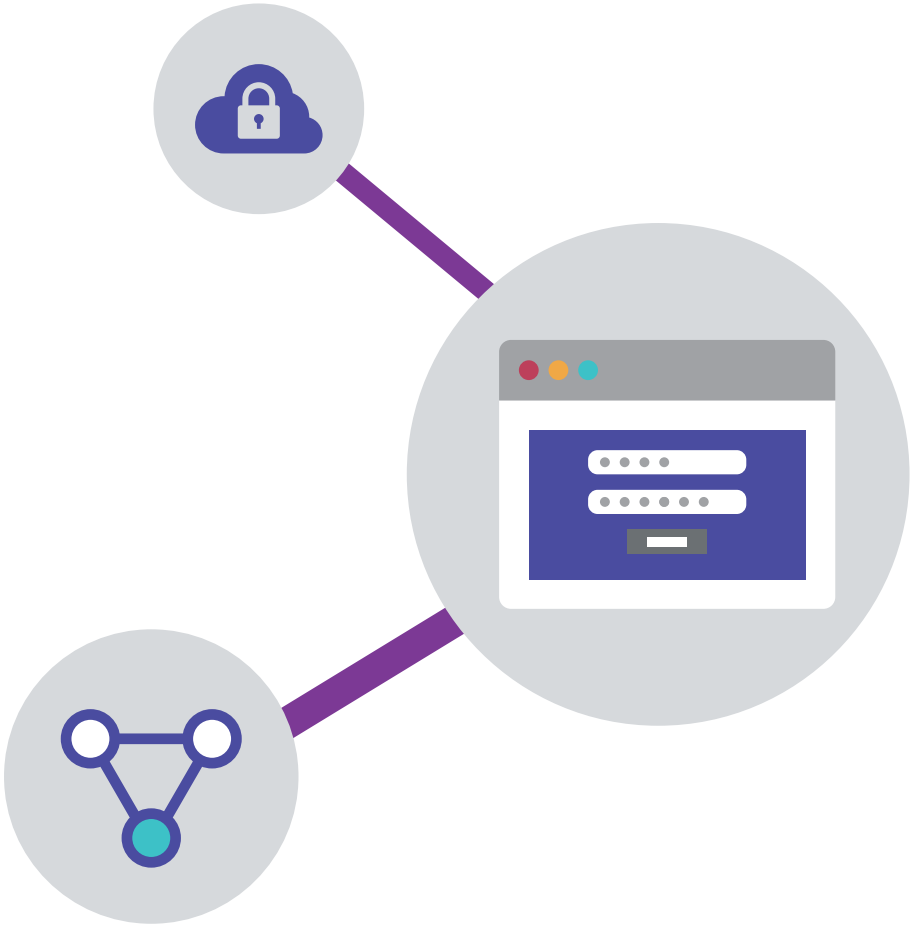
Fuente: [9] IDC [10] Ponemon Institute Cost of Cyber Crime Study 2016

3 HEMOS CONTRATADO A UN ESPECIALISTA EN IT ENCARGADO DE LA SEGURIDAD, NO HAY DE QUÉ PREOCUPARSE

Si bien contratar a un experto es una buena idea, todos los empleados de una empresa deberían tener formación en buenas prácticas en seguridad cibernética.

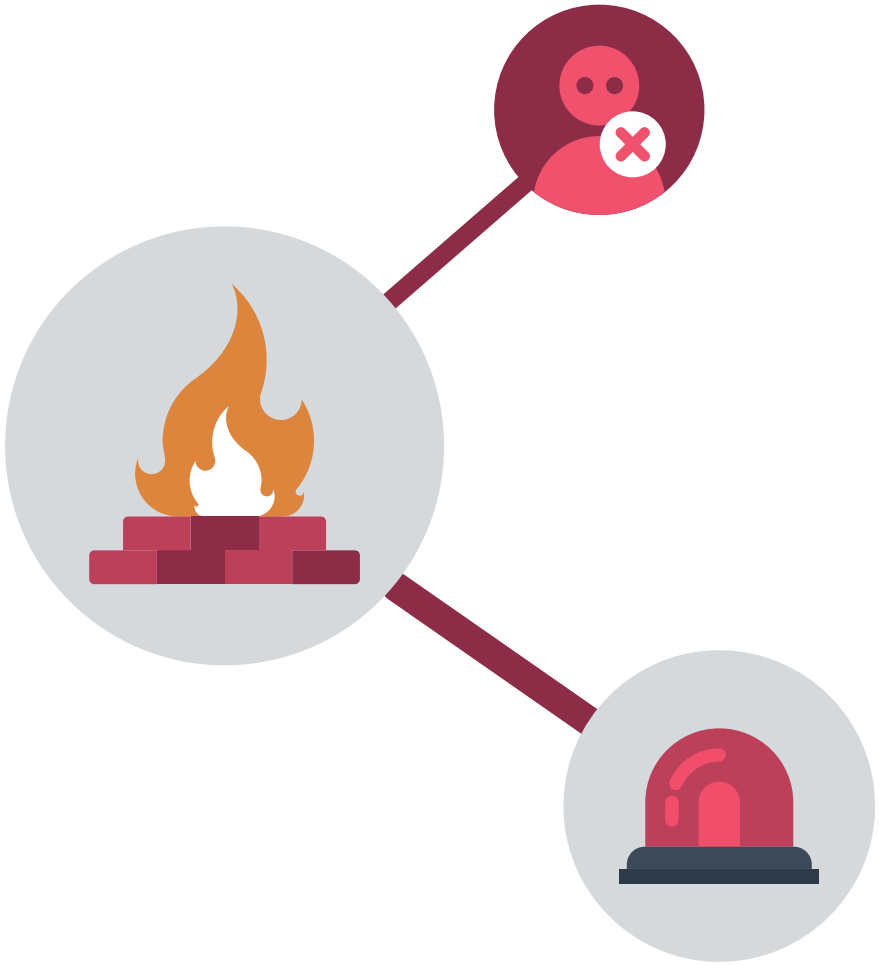
Piense en el empleado que, ignorando lo que conlleva, descarga los archivos adjuntos malignos de un correo electrónico o visita un sitio web peligroso, infectando la red de una empresa con malware que ralentiza los ordenadores o envía información sensible a un delincuente cibernético.

Según el informe Cyber Threat Report 2016 de CyberEdge, las organizaciones dijeron que la 'baja conciencia de los empleados en temas de seguridad' era el principal problema que les impedía defenderse frente a las amenazas de seguridad. Para las empresas, esto resulta más preocupante que la 'falta de presupuesto' o la 'falta de personal cualificado'.[11]



Fuente: [11] Ponemon Institute Cost of Cyber Crime Study 2016

4 NUESTROS SISTEMAS DISPONEN DE UN POTENTE ANTIVIRUS, ESTAMOS BIEN PROTEGIDOS



Los antivirus rastrean los sistemas en busca de malware descargado de sitios web o correos electrónicos. Pero los delincuentes cibernéticos cuentan con otros medios para sortear esta protección.

Un software antivirus es incapaz de bloquear los siguientes ciberataques: ataques de negación 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 consiguen acceder a un sitio mediante dispositivos robados.

5 SI SE CUELA UN INTRUSO, LO NOTAREMOS ENSEGUIDA

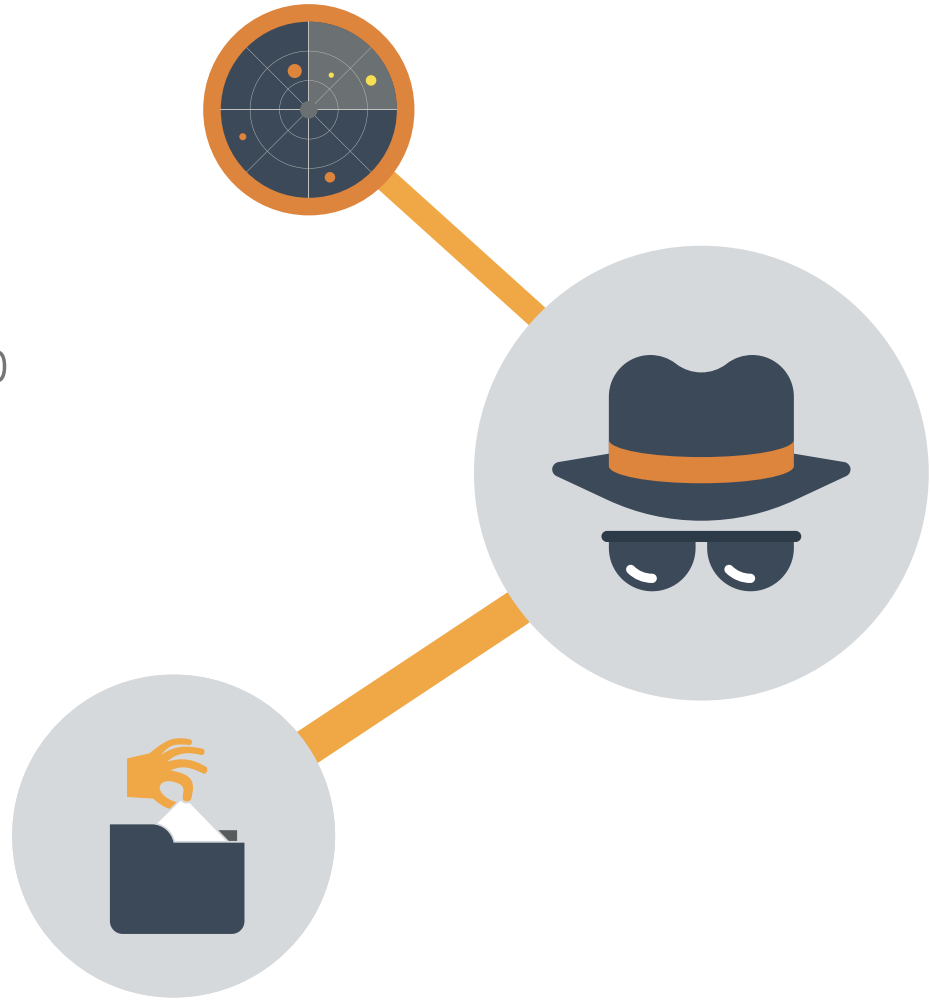
Detectar un ciberataque no es sencillo. El malware que se filtra en un sistema no altera las operaciones inmediatamente; en lugar de ello, puede espiar el sistema y darle información al hacker para que orqueste ataques más definidos, a menudo para conseguir acceso a toda la red.

Tales ataques contra 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:
Controlar 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 —de ese modo detiene las infracciones de seguridad antes de que los datos se vean comprometidos.

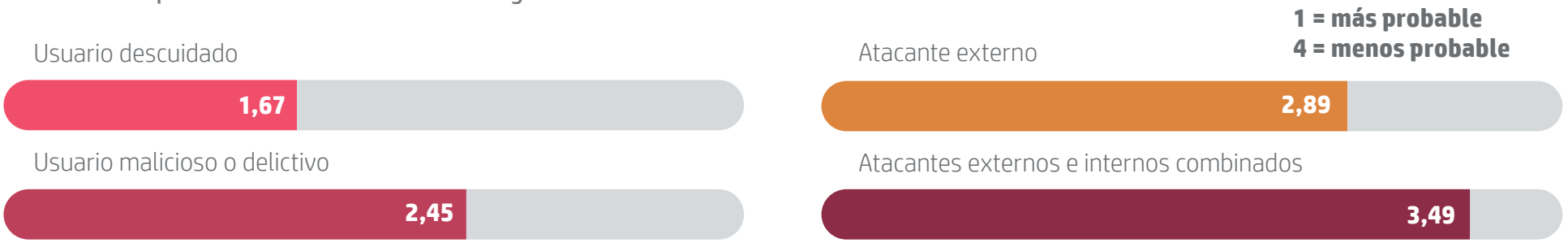


¿DE DÓNDE PROVIENEN LAS AMENAZAS?

Proteger una red comienza por conocer sus puntos más débiles.

La causa más probable de una infracción de seguridad:[12]

1 = más probable
4 = menos probable



Tipos de amenazas externas más comunes:

- **30%** Phishing
- **32%** Virus
- **38%** Malware

Cómo ocurren las infracciones de seguridad internas:[13]

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

Fuente: [12] http://www.kilpatricktownsend.com/_assets/Kilpatrick%20Townsend%20Report%20Final.pdf [13] Ponemon Institute Cost of Cyber Crime Study 2015

¿CUÁNTO CUESTA RECUPERARSE DE UN DELITO CIBERNÉTICO?

Los tipos de ciberataque más costosos son:

Recuperarse de un ciberataque tiene un coste estimado de 907 053 USD —una cantidad que resulta muy superior para las grandes empresas[14]

25 %

Un millón de GBP

Código malicioso y malware

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

24 %

960 000 GBP

Ataques de denegación de servicios

Los ataques “DDoS” son torrentes de seguimiento web que tumban el sitio web y los servidores de una empresa

16 %

640 000 GBP

Ataques web

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

13 %

520 000 GBP

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 GBP

Suplantación de identidad e ingeniería social

Correos electrónicos o mensajes emergentes que se hacen pasar como solicitudes de acceso legales

9 %

360 000 GBP

Abuso de información privilegiada

Empleados que ceden información sensible

4 %

160 000 GBP

Botnets

Redes de ordenadores infectados controlados por actividades maliciosas, como el seguimiento

Fuente: [14] 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 coste del delito en sí

Las infracciones de seguridad conllevan un precio muy alto. A grandes rasgos, existen tres formas de que una infracción de seguridad perjudique las finanzas de su empresa.

Recursos empresariales

Obviamente, las cosas tendrán que volver a ponerse en orden. Esto conlleva una dedicación de tiempo considerable por parte de los empleados y otros costes. Lo que significa que habrá 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 UE el próximo año, las empresas que no cumplan con la normativa podrían verse obligadas a pagar una multa total del 4 % de su facturación global. Podría acabar incluso en los tribunales en el caso de que una filtración derivase en un compromiso de la confidencialidad del clientey.

Reputación dañada

Puede que este sea uno de los impactos más perjudiciales de una infracción de seguridad. Las infracciones de seguridad permanecen durante mucho tiempo en la memoria colectiva. Recuperar la confianza puede llevar mucho tiempo.

ANATOMÍA DE UN HACK INFORMÁTICO INESPERADO

Cuando Sony Pictures fue atacado en 2014, los hackers entraron por la puerta principal.[15]

Según "Lena", del grupo de hackers Guardianes de la Paz (Guardians of Peace, GOP) —quienes 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, plantaron un malware que tomo 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, correos electrónicos, documentos financieros y mucho más —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 sensible tras la violación de seguridad inicial.

Como escribió el experto en seguridad Bruce Schneier tras el ataque, "Todas las redes son vulnerables frente 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 contra las infracciones de seguridad para cada departamento, desde el de IT hasta el de atención al cliente, a fin de minimizar el tiempo de recuperación.

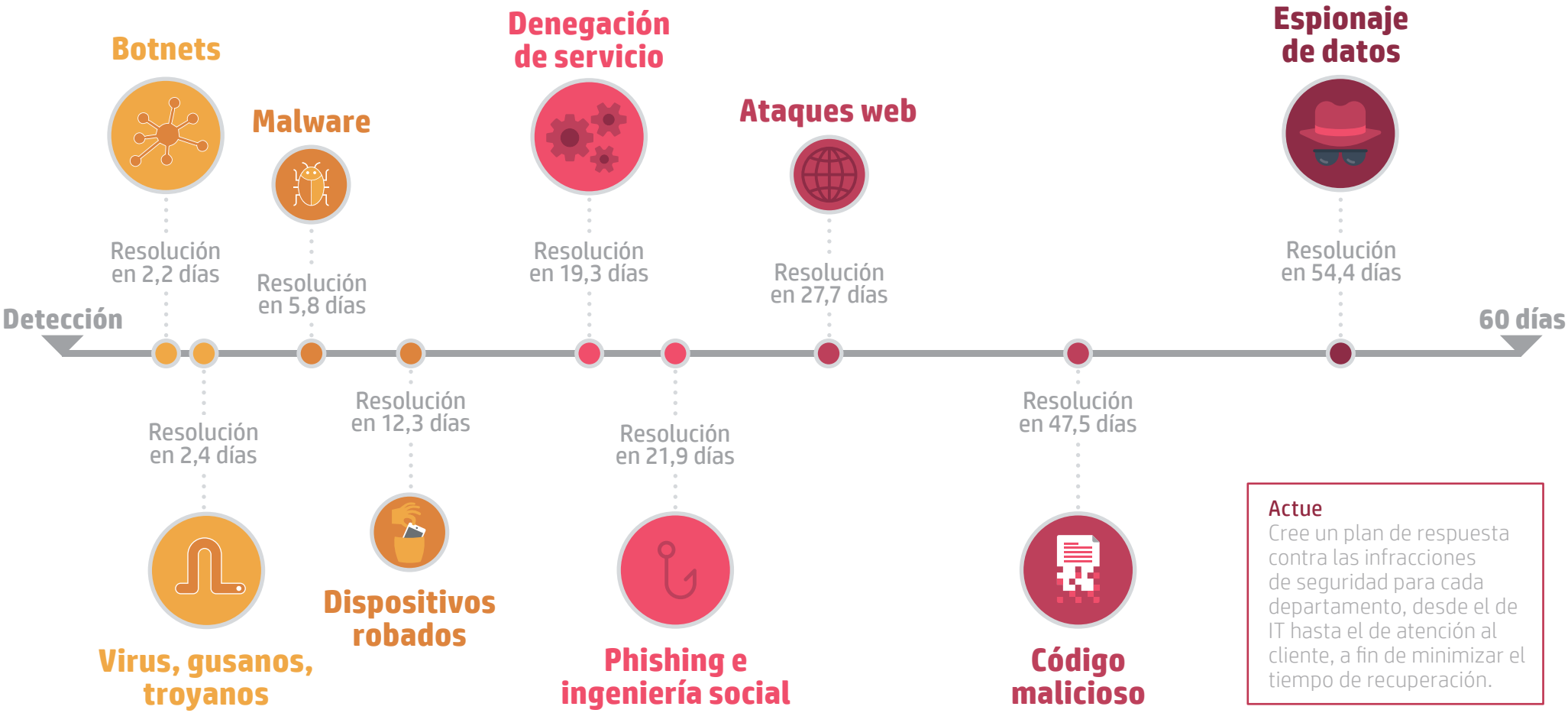
CONSEJO:
Los archivos adjuntos de los correos electrónicos son uno de los principales canales de transmisión de malware. Forme a su personal para que reconozca los archivos sospechosos camuflados como documentos legales.

- Coste estimado de los delitos cibernéticos en las empresas británicas: 21 mil millones de GBP[16]
- Coste medio de los delitos cibernéticos por empresa británica en 2016: 5,7 millones de GBP[17]
- Porcentaje de empresas británicas que sufrieron una violación de seguridad o ataque cibernético en el periodo 2015-2016: 66 %[18]

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



Actue
Cree un plan de respuesta contra las infracciones de seguridad para cada departamento, desde el de IT hasta el de atención al cliente, a fin de minimizar el tiempo de recuperación.

Fuente: [19] Ponemon Institute Cost of Cyber Crime Study 2015

CÓMO PROTEGER SU EMPRESA DE LOS DELITOS CIBERNÉTICOS

Consejos y estrategias esenciales en seguridad cibernética para empresas

Aquí indicamos los seis objetivos comunes que los hackers utilizan para violar los sistemas de seguridad de una empresa, y también qué se puede hacer al respecto hoy en día.

Bases de datos de clientes

Servicios en la nube

Smartphones y tablets de los empleados

Errores de los empleados

Prepárese para el 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 tabletas hasta impresoras con wifi— que proporcionan un número creciente de puntos de acceso para los hackers.

1 BASES DE DATOS DE CLIENTES

Los datos económicos no son el único objetivo de los atacantes: datos como nombres y direcciones de correo electrónico puede utilizarse para suplantar la identidad, hacer spam o hackear otras cuentas.

Para los hackers, atacar empresas que sirven a empresas todavía más grandes supone un premio aún mayor. Véalo como el equivalente digital de colarse en una tienda informática únicamente para acceder a la pared del sótano lindante 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 los clientes de, a su vez, clientes más grandes. ¿Cómo puede verse comprometida su base de datos de clientes? Virus, gusanos y troyanos, descargados de sitios maliciosos o correos electrónicos, 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, correos electrónicos y terminales.
- Actualice siempre el software de seguridad para bloquear el malware más actual.
- Descargue las actualizaciones de software de sus programas, pues los programas más antiguos son más vulnerables ante 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 fuerte 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, tal como un código de Smartphone y una contraseña, para realizar cambios en los datos de nube, como descargar, eliminar o mover archivos.

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

La tecnología Cloud se ha vuelto fundamental dentro de la infraestructura de una empresa. La encuesta Cloud Computing Survey 2016 de IDG descubrió que el 70 % de las empresas tienen al menos una parte de su infraestructura en la nube,[20] mientras que Tripwire descubrió que el 90 % utiliza la nube para guardar infraestructura y/o almacenar datos, incluidos los más importantes.[21]

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

Por eso, 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,[22] solo el 7 % de los servicios de nube de las empresas (grandes y pequeñas) sufrió violaciones de seguridad graves, por lo general como resultado de permisos de acceso o contraseñas insuficientes. Una nube segura necesita unos controles de seguridad internos fuertes. Piense en la puerta delantera de Sony.

Fuente:
[20] https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey#fullscreen&from_embed
[21] https://www.tripwire.com/state-of-security/security-data-protection/enterprise-impressions-of-cloud-security-in-2016/ (and for following stat)
[22] 2015 Small Business Survey. Department for Business, Innovation & Skills

3 SMARTPHONES Y TABLETS DE LOS EMPLEADOS

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

Las políticas BYOD (siglas en inglés de "traiga su propio dispositivo") suponen una forma efectiva de aprovechar los smartphones de los empleados. Esta es una tendencia al alza; de hecho, el 53,2 % de las organizaciones está implementando una política BYOD para los próximos dos años.[23] (Cyber Threat Report 2016, CyberEdge). 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 saltar a los archivos y sistemas de una empresa y así controlar sus actividades o robar información.

Esta es una amenaza que va en aumento: un 64,9 % de las organizaciones dice que el número de amenazas contra sus dispositivos móviles ha aumentado (Cyber Threat Report 2016, CyberEdge).[24]

Los empleados a quienes les hayan robado sus teléfonos también pueden actuar, inconscientemente, como una puerta de entrada para los hackers. Pongamos que un ladrón de teléfonos le vende un dispositivo a un comprador en el mercado negro, quien lo quiere para obtener información con el fin de violar la seguridad de la empresa de la víctima, o para penetrar en los sistemas de un cliente más grande. Las organizaciones puntuaron con un 3,54 sobre 5 su capacidad para defenderse contra amenazas de seguridad originadas desde dispositivos móviles. Esta fue la puntuación más baja de entre todos los orígenes potenciales de amenazas que se preguntaron (Cyber Threat Report 2016, CyberEdge).[25]

Cómo asegurar los dispositivos de los empleados

- Instale una herramienta de detección de amenazas como X-Ray, de Duo Labs, para dispositivos Android, y facilitar de ese modo el rastreo de aplicaciones no autorizadas y códigos sospechosos.
- Pida a los empleados que habiliten los barridos remotos (gratis 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.
- Pídales a los empleados que habiliten el cifrado de dispositivo en sus smartphones para la protección de datos (esta característica viene por defecto en teléfonos iOS y Android).

Fuente: [23] Cost of Cyber Crime Study 2015, Ponemon Institute [24] ibid [25] ibid

4 ERRORES DE LOS EMPLEADOS

Cómo ayudar a los empleados

- Forme a su personal en las mejores prácticas de seguridad cibernética e imparta formación cada cierto tiempo para que conozcan 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 es disponer de una buena política de contraseñas. Aun así, el 31 % de las peores infracciones de seguridad de 2015 fue resultado de un incidente relacionado con los empleados.

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

5 PREPÁRESE PARA EL INTERNET DE LAS COSAS

La empresa de investigaciones 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 que se estimaba (Turnaround and transformation in cybersecurity, PwC).[26]

Si bien los ordenadores de oficina están asegurados al menos con contraseñas, e idealmente con software de seguridad, las colas de impresión y las tareas de impresión no suelen recibir los mismos protocolos de seguridad. Además, el auge de los dispositivos móviles y el incremento del teletrabajo hacen que no todos los dispositivos personales estén tan asegurados como deberían.

Las impresoras no aseguradas (y otro hardware en red) pueden caer presa de "programas de rastreo", capaces de registrar las tareas de impresión y el tráfico de red, nombres de usuarios e información de contraseñas, y enviarlo todo al servidor del delincuente cibernético.

Aquí cabe mencionar que la famosa vulneración de seguridad de Dyn estaba supuestamente ligada a una red de cámaras de vigilancia habilitadas en la red, hecha por una única empresa, XiongMai Technologies. Según la empresa de seguridad Flashpoint.

Esto demuestra que todos los dispositivos de una red son un terminal, y que una red es tan segura como el dispositivo menos seguro. El 97 % de las organizaciones tienen prácticas de seguridad para ordenadores de escritorio/portátiles, el 77 % para dispositivos móviles, pero tan solo el 57 % tienen prácticas de seguridad para impresoras.[27] La única manera que tienen los negocios de mantenerse seguros es la implementación de prácticas de seguridad para todos sus dispositivos.

Cómo prepararse para el Internet de las cosas.

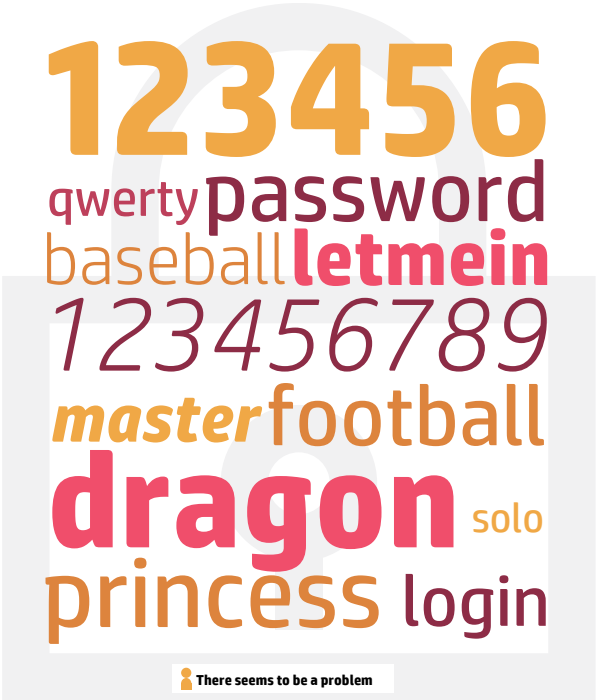
- Elimine o deshabilite las funcionalidades innecesarias del hardware, ya que, a más funciones, más puertas de entrada se abren para los atacantes.

Fuente: [26] PwC: The Global State of Information Security Survey 2016 [27] HPI Printer Security Research, 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 descodificación de sistemas protegidos por contraseña, logró penetrar en 8000 sitios protegidos por contraseñas, de los más 16 000 que intentó 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 llamado Cryptolocker que afectó a miles de usuarios y llegó a llamar la atención de la Agencia Nacional contra el Delito del Reino Unido y su Unidad Nacional contra el Delito Informático. Así es como se producen este tipo de ataques:

1. Instalación	El código malicioso se instala en el ordenador tras ser descargado inadvertidamente por el usuario, puede ser mediante un correo electrónico o a través de un sitio web malintencionado.
2. Alerta a su sede de procedencia	El ransomware se conecta con su servidor y establece una conexión cifrada.
3. Encriptación de los archivos del usuario	El ransomware escanea los archivos de la red del usuario y los encripta, 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.

* Splashdata

6 ENTRADAS DE RED

Cuando los hackers quieren penetrar en una red, tienen que desencadenar un ataque DDoS, donde miles de máquinas infectadas con malware se unen para generar tanto tráfico basura que la red cae bajo el peso del ataque.

A menudo, los atacantes DDoS distraen a los administradores de los sitios con un sistema congelado mientras roban datos o instalan malware, a fin de planificar robos de datos futuros. Parte de los ataques DDoS son también resultado de “script kiddies”, hackers novatos que tan solo quieren echar abajo un sitio de internet porque pueden. Que un sitio web esté caído solo unas horas puede ser devastador 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 asegurar 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. Los propietarios de las empresas utilizan plataformas de computación de nube y externalizan los servicios técnicos clave. Y casi cuatro millones de británicos trabajan desde casa. La seguridad cibernética se complica cuando no hay un control sobre el dispositivo, la infraestructura ni el espacio de trabajo.

Al mismo tiempo, los smartphones 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 públicas de wifi para procesar enormes cantidades de datos personales y empresariales, a menudo mediante smartphones que apenas están protegidos. Los delincuentes son conscientes de esta tendencia.

La seguridad se ve comprometida cuando no cuidamos nuestro entorno de trabajo.

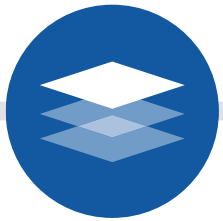
En los años venideros, esto implicará mucho más que la simple instalación de un antivirus en nuestros dispositivos o la actualización de nuestras contraseñas cada seis meses. En cambio, las empresas tendrán que adoptar medidas de seguridad optimizadas que funcionen igual de bien a distancia que como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

Para las organizaciones distribuidas del mañana, la seguridad cibernética dependerá de los análisis sofisticados que aíslen comportamientos infrecuentes y de la seguridad por niveles 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 que tiene unos patrones. Utilizar herramientas analíticas que midan y registren la actividad puede facilitar el diagnóstico cuando algo vaya mal. En primera instancia, estas herramientas rastrean y documentan un comportamiento normal a 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.



Encubrimiento por capas: un paso por delante de los atacantes

En ocasiones llamada “defensa en profundidad”, la seguridad por capas protege todos los puntos de acceso de diversas formas. Los métodos comunes incluyen certificados SSL de validación extendida que dificultan la falsificación de las credenciales necesarias para entrar en una red segura. También puede ser de utilidad respaldarlo con una autenticación multifactorial que obligue a los invasores a craquear algo más que una contraseña.

Independientemente de la tecnología específica de su oficina, el principio subyacente al encubrimiento por capas es que todas las áreas sensibles 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 no son más que pequeñeces a cambio de la seguridad de una empresa.

Actúe ahora

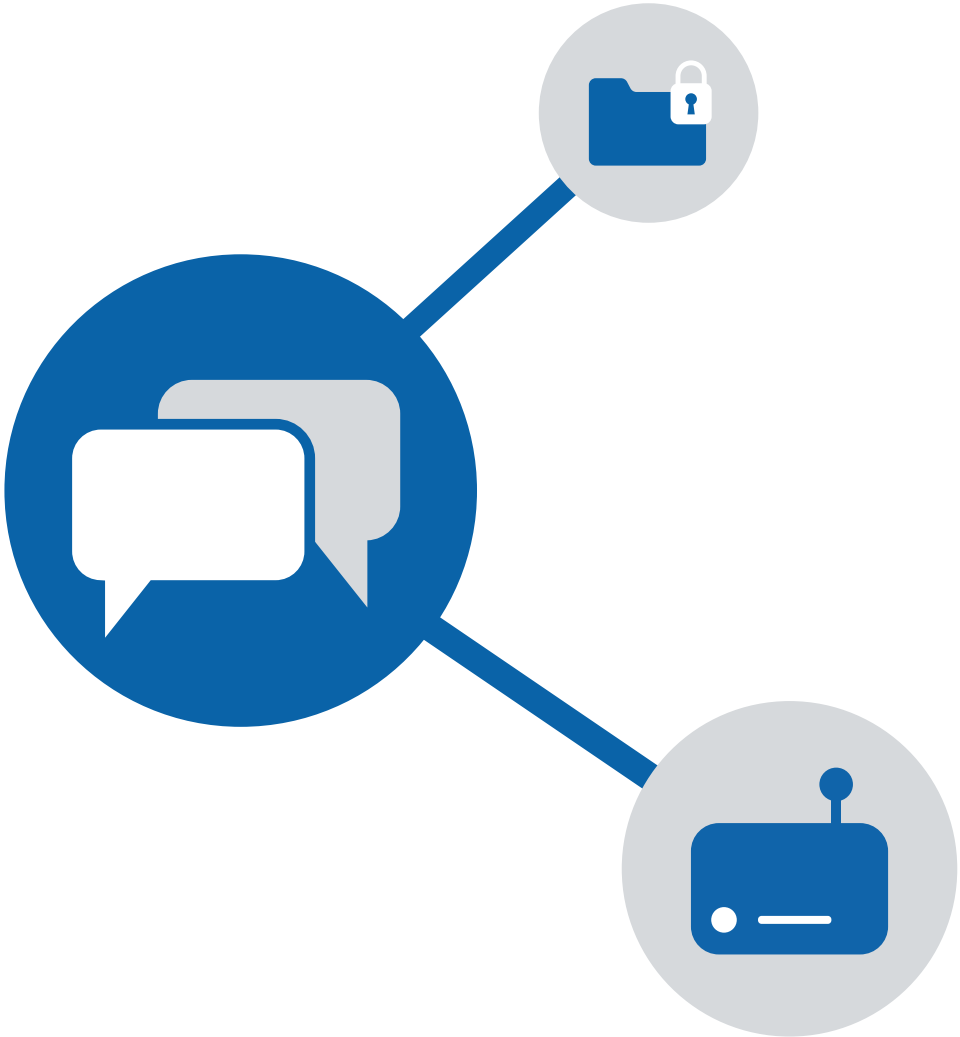
Invertir en software de seguridad y en formación son las mejores defensas. Comience por efectuar una auditoría de sus sistemas e infraestructura. ¿Se está haciendo lo suficiente? ¿Qué se podría mejorar?

Por último, también puede ponerse en contacto con nuestros expertos en Hewlett Packard Inc. Nuestra base de conocimiento colectivo se centra en ir por delante de las amenazas, no solo en responder a ellas. Para saber más, visítenos en HP.com.

CONSEJO:
Rastree y documente un comportamiento normal en primera instancia, a fin de detectar anomalías posteriormente.

CONSIDERACIONES DE SEGURIDAD PARA DISPOSITIVOS TERMINALES

Asegurar todos y cada uno de los dispositivos de su red



Un informe de seguridad elaborado por Spiceworks[28] reveló que los principales orígenes de amenazas para 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

¿Cuál de estas amenazas habría que asegurar antes? Muy sencillo: todas. Si bien esto puede parecer muy obvio, un número alarmante de organizaciones siguen dudando respecto a qué dispositivos asegurar.

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

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

Fuente: [28] HP Printer Security Research 2016, Spiceworks

HP: ABRIENDO CAMINO HACIA UN NUEVO PANORAMA

La seguridad cibernética está cambiando. Disponemos de las herramientas para ayudar a su defensa

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

En HP, la seguridad es lo primero. Nuestra gama HP Elite presenta funciones de seguridad líderes en el mercado, no disponibles en ningún otro sitio, como HP SureStart, la primera BIOS con capacidad de auto-reparación del mundo, y la pantalla de privacidad HP SureView.

La gama de dispositivos HP Premium Elite presenta características de seguridad líderes en el mercado, que no encontrará en ningún otro sitio. Nuestros dispositivos están diseñados pensando en la seguridad, y en combinación con servicios y soluciones gestionados, son la defensa más proactiva y robusta contra la piratería. Descubra nuestras características únicas a continuación:

HP equipa sus dispositivos con:

- **Cierre de Bluetooth:** La máquina apaga automáticamente la conexión Bluetooth cuando nos marchamos y lo enciende cuando volvemos.
- **Seguridad biométrica:** Reconocimiento facial y dactilar que da acceso s olo a usuarios autentificados biométricamente.
- **Pantallas HP SureView*:** Los monitores oscurecidos evitan que los mirones vean nuestras pantallas y protegen el material confidencial cuando estemos trabajando sobre la marcha.
- **BIOS auto-reparador de HP SureStart:** Los HP Elite controlan su BIOS cada 15 minutos. En caso de que detecten alguna anomalía, resetean el PC a su estado original, expulsando de ese modo a los posibles intrusos.

Los HP Elite no protegerán su empresa por sí solos. Pero sí que constituirán una sólida primera línea. Visite **www8.hp.com** para saber más sobre la completa gama HP Elite.

Consulte **HP Device as a Service** para conseguir un fácil acceso a todos los dispositivos y servicios que necesita su negocio. Se trata una solución informática inteligente y sencilla para el mundo actual, que incluye:

- **Una analítica excepcional y capacidad de gestión proactiva –** Una solución inteligente para la gestión de una flota moderna, optimizando los activos y recursos informáticos.
- **Planes flexibles** – Planes sencillos a la vez que flexibles, ampliables según sus necesidades.
- Experiencia en la gestión **del ciclo de vida a escala global**

* Modelos seleccionados

GLOSARIO Y LECTURAS COMPLEMENTARIAS

Acceso a herramientas de control

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

Botnet:
Generalmente hace referencia a un tipo de programa automatizado, diseñado para acceder y controlar ordenadores conectados a internet a espaldas del propietario. A menudo los ordenadores se ven infectados con malware. Los hackers utilizan los botnets para provocar un **ataque de negación 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 dispositivos.

Gusanos:
Al contrario que los virus, que se propagan al compartir un archivo del host, los gusanos pueden reproducirse independientemente de un archivo del host, como un documento de Word o una hoja de Excel, y por tanto no necesitan más interacción humana para causar estragos. Los sistemas de mensajería instantáneos 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:
Se refieren a iniciativas amplias y coordinadas en el interior de una empresa, destinadas a gestionar y regir las operaciones de tal modo que cumplan con las normativas y que, como resultado, reducen los riesgos.

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

Ingeniería social:
En donde 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 desmantelar otros sistemas. Virus, gusanos y troyanos son ejemplos de malware. También, con objetivo del estudio de Ponemon citado en este eBook, el malware es distinto a los virus, los cuales menciona que “residen en los terminales y todavía no se han infiltrado en una red”.

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

GLOSARIO Y LECTURAS COMPLEMENTARIAS

Sistemas inteligentes de seguridad:
Una amplia variedad de inteligencia de seguridad puede ayudar a reunir y sintetizar información relacionada con 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 muy a favor de varios tipos de cifrado en los últimos años. Recientemente, el gobierno se ha visto obligado a c**ambiar su postura en cuanto a la tecnología de cifrado** como consecuencia de las duras críticas.

Tecnologías cortafuegos:
Otro término general que describe un estilo de dispositivo que utiliza algoritmos y otras técnicas para impedir al tráfico y a los 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 las diferencias 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 borrar archivos o crear una “entrada trasera” que el hackers utilizará después.

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