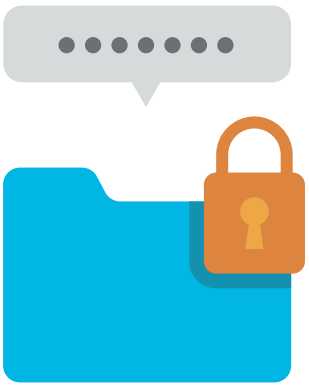
Business white paper

La seguridad comienza en los terminales

La priorización de la seguridad en los terminales

Brought to you by

Resumen ejecutivo



El 82 % de las empresas han sufrido alguna amenaza/vulneración de la seguridad cibernética en los últimos 12 meses.[1] Los delitos cibernéticos aumentan en frecuencia, gravedad y costes.

El paradigma de prevención y protección de la seguridad mediante la defensa con cortafuegos de un perímetro de red está obsoleto. La detección y respuesta son medidas mucho más efectivas.

No obstante, los presupuestos de TI no bastan para cubrir el entorno cambiante de la seguridad cibernética. El 77 % sigue invirtiéndose en prevención y protección[2] y solo el 36 % de los gerentes de seguridad informática piensa que tiene un presupuesto suficiente como para implementar una seguridad efectiva en sus terminales.[3]

Una protección sólida de los datos es posible: con la tecnología adecuada —desde soluciones de seguridad de detección y respuesta hasta dispositivos individuales— la estrategia adecuada y los recursos suficientes, las empresas pueden protegerse de los delincuentes cibernéticos.

Al no aumentar las inversiones en seguridad cibernética ni modificar dichas inversiones para conseguir una defensa realmente efectiva, la frecuencia de las infracciones de seguridad aumenta y conlleva unos costes más elevados para la empresa.

Introducción

Seguridad cibernética en la era de las redes desestructuradas
El 60 % de los líderes de TI opina que el aumento del volumen y la sofisticación de los delitos cibernéticos supera sus defensas. El 80 % de los jefes de seguridad considera las amenazas persistentes avanzadas (Advanced Persistent Threats, APT), las organizaciones delictivas, y a los hackers y "hacktivistas" financiados por los estados como los mayores desafíos para la seguridad informática.[4]

No se equivocan: el gobierno del Reino Unido eleva el coste económico de los delitos cibernéticos hasta los 27 mil millones de GBP, una cifra "significativa y en posible aumento", y unas pérdidas empresariales de 21 mil millones de GBP.[5] En el Informe sobre el estado de los terminales de Ponemon de 2016, el 78 % de las empresas informaron sobre un aumento de la gravedad de los ataques con malware, en comparación con el 47 % de 2011.

Sin embargo, centrarse en las amenazas externas es un error que puede tener como resultado una concentración quijotesca de recursos de prevención y protección en la defensa del perímetro.

Pese a la mayor incidencia de ataques externos (virus, malware, phishing), los ataques internos generan costes superiores.[6] Además, la mayoría de esos ataques externos son producto de vulnerabilidades internas: empleados negligentes que ignoran los protocolos de seguridad o dispositivos no seguros conectados a la red (que el 81 % de los participantes en la encuesta de Ponemon identificaron como las mayores amenazas de seguridad).

Esta situación va en aumento. El terminal es el punto más débil de cualquier red y, con el aumento de las políticas BYOD (siglas en inglés de "traiga su propio dispositivo"), el trabajo remoto y el Internet de las cosas, el número de terminales no para de crecer. En consecuencia, el número de puertas de acceso disponibles para los hackers también se multiplica.

Las redes actuales están desestructuradas y poco tienen que ver con las antiguas redes controladas de los ordenadores de sobremesa conectados por Ethernet; ahora se han convertido en una maraña de dispositivos personales y profesionales que acceden a los datos desde múltiples nodos Wi-Fi, tanto en línea como de forma local.

Esta situación no es inabordable: basta con adoptar una nueva estrategia en materia de seguridad cibernética, enfoques novedosos que respondan al nuevo rostro de la delincuencia cibernética, y una nueva tecnología con la capacidad de bloquear la sofisticación cada vez mayor de la creciente amenaza.

En este informe blanco, examinamos la naturaleza y el alcance de la amenaza (para conocer mejor a nuestro enemigo) antes de abordar la cuestión de cómo afrontar la seguridad cibernética en la era de los dispositivos múltiples, las redes no seguras y la nube.

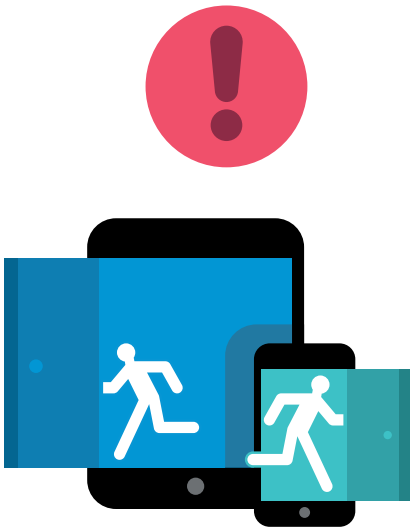
[1] HPI Printer Security Research 2016 (Spiceworks)
[2] PAC Incident Response Management 2015: https://www.pac-online.com/download/19443/155514
[3] Ponemon 2016 State of the Endpoint Report
[4] IBM CISO Assessment 2014
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf
[6] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic

El alcance de la amenaza

Recuperarse de una infracción de seguridad cuesta a las empresas una media de 907 503 USD con un 13 % adicional de pérdida de ingresos. De media, las empresas tardan nueve semanas en recuperarse.[7]

Aproximadamente el 85 % de las empresas encuestadas en el HP Printer Security Report de 2015 afirmaron que habían sufrido amenazas/infracciones de seguridad en los 12 meses anteriores. El 80 % de los profesionales encuestados preveían un aumento de las amenazas en los próximos tres años.[8]

Los delitos cibernéticos cuestan dinero real: pérdida del importe de lo robado o deteriorado, pérdida de ingresos por el daño a la reputación y recursos invertidos en la recuperación y en la implementación de nuevas políticas de seguridad lo que se traduce en pérdida de productividad, pérdida de tiempo en servicio técnico, pérdidas de personal y otras respuestas internas; además de multas y sanciones por parte de los organismos reguladores y una bajada del precio de las acciones.



La amenaza aumenta a medida que aumenta el número de dispositivos conectados a la red. Gracias al Internet de las cosas, Gartner predice que para 2018 habrá 11,400 mil millones de dispositivos conectados, en comparación con los 6,4 mil millones de 2016. En 2020, más del 25 % de los ataques identificados a empresas estarán relacionados con el Internet de las cosas, aunque se le dedicará menos del 10 % del presupuesto en seguridad.[9]

La amenaza de la delincuencia cibernética es grande y sigue en aumento.

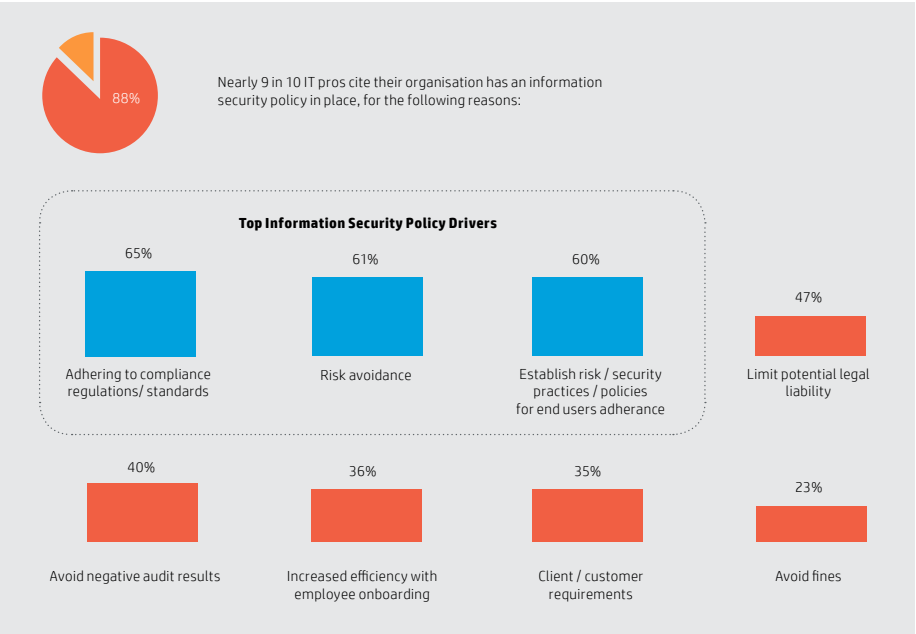
La forma de la amenaza

Las empresas sufren numerosos ataques cibernéticos cada día. La mayoría se trata de virus de bajo nivel y malware. El 99 % de las empresas encuestadas por Ponemon en 2016 había sufrido malware en los 12 meses anteriores. Esta clase de ataques web externos son relativamente benignos y cuestan a las empresas un promedio de 4639 USD.[10]

Sin embargo, los ataques más graves son cada vez más frecuentes. El 51 % de las empresas encuestadas en 2015 había sufrido ataques DDoS, que pueden ser devastadores, y estos costaron un promedio de 127,000 USD. Todavía más inquietante es el hecho de que el 35 % sufrió un ataque malicioso desde dentro, con un coste medio de 145,000 USD.[9]

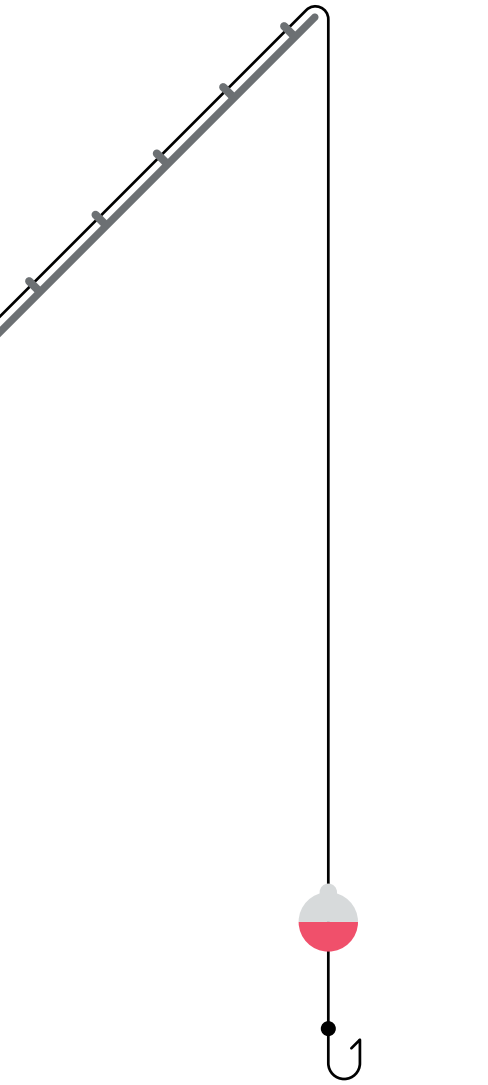
La nueva perspectiva presenta ataques menores incesantes desde el exterior junto con ataques de más envergadura que, aunque menos frecuentes, pueden suceder con sorprendente frecuencia; ambos son producto de negligencias desde el interior o, incluso, intencionados. El 62 % de las empresas ha sufrido phishing/ataques de ingeniería social, que se aprovechan de la debilidad de los empleados y cuestan 86,000 USD de media.[11]

Un informe aparte de Spiceworks, en nombre de HP, desglosa los ataques sufridos en 2014-2015 por 90 empresas del Reino Unido.[12]



[7] NTT Security Risk:Value Report 2016
[8] HP 2Printer Security Report 2015
[9] http://www.gartner.com/newsroom/id/3291817
[10] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf
[11] https://digitalguardian.com/blog/insiders-vs-outsiders-whats-greater-cybersecurity-threat-infographic
[12] HPI Printer Security Research, Spiceworks 2016

Causas de las vulneraciones



Los titulares nos hablan de hackers que atraviesan las redes de seguridad más sofisticadas de gobiernos y empresas, pero la realidad es mucho más mundana.

Los virus pueden aprovecharse de las redes comprometidas, pero el uso de malware solo es posible a partir de un error del usuario. El phishing y los ataques de ingeniería social dependen de ellos. Los ataques DDoS y el robo de información a gran escala también suelen ser el resultado de una negligencia del usuario.

El infame hackeo a Dropbox fue supuestamente el resultado de un descuido de un empleado de Dropbox que utilizaba la misma contraseña para los sistemas internos que para su cuenta de LinkedIn.[13] El supuesto hackeo ruso al DNC se llevó a cabo gracias a que John Podesta, antiguo asesor de la señora Clinton, hizo clic en el enlace de un correo electrónico de phishing erróneamente marcado como seguro por un ayudante.[14]

Los hackers no necesitan una asistencia activa para tener éxito. Ignorar o desconocer los protocolos de seguridad es igual de peligroso. El uso de los dispositivos personales de los empleados en el trabajo y la utilización de software de nube comercial supone una amenaza cada vez mayor, ya que introducen elementos no seguros en una red protegida que están fuera del control del equipo de TI de las empresas y crean vulnerabilidades que pasan desapercibidas.

La mayoría de las veces, los hackers no necesitan emplear sofisticados algoritmos ni lo último en tecnología: basta con que alguno de nosotros sea un poco descuidado.

El cortafuegos está obsoleto

Hasta hace poco, los puntales de la seguridad cibernética eran los antivirus y cortafuegos: prevenir, proteger y crear un perímetro de seguridad. En el entorno de trabajo actual, han dejado de ser una estrategia efectiva.

El 81 % de los encuestados por Ponemon afirma que los dispositivos móviles de sus redes han sido objetivo de ataques de malware. Otros aumentos de los riesgos de seguridad incluyen el uso por parte de los empleados de aplicaciones comerciales de nube (citado por el 72 % de los encuestados), BYOD (69 %) y empleados que trabajan desde casa u otros lugares distintos de la oficina (62 %).[15]

Básicamente, el uso de un cortafuegos tenía sentido cuando el administrador de red podía controlar qué dispositivos había conectados a la red. No obstante, en una era donde los empleados utilizan sus dispositivos personales en el trabajo (normalmente, más de uno y sin conocimiento del departamento de TI) y con un número cada vez mayor de trabajadores que se conectan de forma remota, es imposible proteger el perímetro. Todos los dispositivos sin examinar son puntos vulnerables que los hackers pueden explotar.

[13] https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

[14] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0

[15] Ponemon 2016 State of the Endpoint Report

La perspectiva de HP: dar un paso más allá en seguridad de redes

Michael Howard, jefe de asesoría de seguridad de HP a nivel mundial, habla sobre la seguridad de los terminales

Un asunto actual y primordial es la preocupación de las empresas por asegurar todos los terminales, debido al desconocimiento sobre ciertos dispositivos y los riesgos que conllevan. Se sienten seguros protegidos por un cortafuegos, a pesar de que ya no baste para protegerse frente a los ataques. Los equipos de seguridad deben estar al tanto de todos los terminales de la infraestructura y garantizar que todos ellos tienen múltiples capas de protección para salvaguardar frente a unos ataques cada vez más sofisticados.

Es fundamental que los equipos de seguridad investiguen todos los rincones de las infraestructuras de TI de sus empresas y construyan una capa adicional de protección por encima de los perímetros de red estándar. Por sí solo, un cortafuegos no puede soportar ataques sofisticados, y una política de defensa con múltiples capas de protección en cada terminal es fundamental para garantizar que tu empresa cumpla con los requisitos normativos y para evitar multas elevadas.

La política de HP consiste en desarrollar la seguridad de cada nueva solución, servicio o producto que se ofrece en primer lugar. Los equipos de desarrollo saben que deben dar respuesta a las cuestiones de seguridad y deben saber cómo implementarlas en una red de forma segura.

Ahora más que nunca, la seguridad debe ser lo primero, no un extra. Esta ha sido la política de HP durante años.

Seguridad en capas

El nuevo enfoque en materia de seguridad cibernética debe ser multicapa.
La seguridad de red sigue siendo importante, pero debe componerse de redes discretas. Muchas vulneraciones residen en un acceso inicial que da acceso a todo el sistema. Recuerda el tropiezo de John Podesta. Es fundamental cercar la información sensible en múltiples niveles de acceso, para que la irrupción en una sala no suponga la conquista de la fortaleza.

Se debe llevar un control de los dispositivos. Un problema clave para los jefes de TI es garantizar que todos los dispositivos conectados a la red están protegidos frente a virus, malware y spyware por un software de seguridad que se actualice regularmente, y que se analicen con frecuencia en busca de anomalías. Todavía mejor sería utilizar los propios dispositivos como sensores que recopilen información en tiempo real para alertar de cualquier vulneración en el perímetro de red en la que se vean envueltos.

Hay que llevar a cabo un control exhaustivo de la seguridad en el que todos los empleados tengan formación en protocolos de seguridad. Los errores humanos (desde un clic en un enlace falso hasta conectarse con un dispositivo de usuario) son la principal amenaza de las redes. Los errores humanos pueden reducirse mediante la formación.

Seguridad de los dispositivos

Controlar todos los dispositivos que tienen acceso a la red es quizás el tema principal al que se enfrenta la seguridad cibernética en la actualidad.
La primera y más sencilla solución que suele adoptarse es utilizar redes Wi-Fi diferentes para visitantes y empleados; de esta forma, los dispositivos externos sin seguridad no tienen acceso a la red principal. Esta acción debe realizarse de forma conjunta con la formación de los empleados en el uso de dicha red con sus dispositivos personales.

La segunda solución consiste en asegurarse de que se tiene el control de los dispositivos de los empleados. Hay que introducir este asunto en las políticas BYOD y CYOD de la empresa, y es un argumento de peso en favor de las políticas CYOD, que dan mayor control sobre qué dispositivos se utilizan, para elegir los que tienen mejores prestaciones de seguridad, cómo están configurados, y la gestión y el control de dichos dispositivos.

Por ejemplo, el uso de ordenadores de la línea HP Elite es preferible al de portátiles de bajo coste. Todos los ordenadores HP Elite incorporan la tecnología HP SureStart, que analiza la BIOS cada cuarto de hora y restaura la configuración original de la máquina al detectar una anomalía para bloquear a los intrusos indeseados. Por esta y otras muchas prestaciones, los dispositivos de la serie HP Elite 800 han sido declarados “los ordenadores más seguros del mundo”.[16] Sin embargo, es poco probable que los propios empleados tengan ordenadores HP Elite.

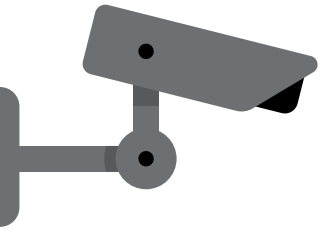
Los empleados suelen preferir el uso de sus propios dispositivos por dos motivos:
1. La tecnología de usuario suele ser mejor que la facilitada por la empresa
2. Los empleados prefieren utilizar tecnología que les resulte familiar

Al ofrecer una política CYOD bien provista, que ofrezca lo último en dispositivos y los actualice regularmente, las empresas pueden equipar a sus empleados con mejores dispositivos que los suyos y mantener un control superior sobre su seguridad. Por este motivo, HP ofrece la solución de Dispositivo como servicio (HP DaaS).

Es fundamental incluir todos los dispositivos en la estrategia de seguridad, incluidos los que suelen pasarse por alto. En una encuesta del IDC, el 80 % de los participantes afirmó que la seguridad de TI es importante para sus empresas, pero solo el 59 % reconoce la importancia de la seguridad de impresión, a pesar de que más de la mitad ha sufrido vulneraciones relacionadas con la seguridad de sus impresoras en los 12 meses anteriores. Las impresoras suponen un punto ciego evidente.

El promedio de vulneraciones de seguridad antes de implementar la seguridad de impresión ascendía a 9,9 al año y costaba una media de 521,000 USD (incluyendo sanciones). Tras la puesta en práctica de la seguridad de impresión, el promedio de vulneraciones descendió hasta 1,5, con un ahorro de 200 horas de trabajo de los empleados por año y 250,000 USD de costes derivados, incluyendo auditorías y cumplimiento normativo.[17]

[16] http://www8.hp.com/us/en/campaign/computersecurity/
[17] IDC The Business Value of Printer Security 2015



Detección y respuesta proactivas

Según un estudio de PAC, el 77 % del gasto en seguridad se destina a tecnología de prevención y protección, como antivirus y cortafuegos. Sin embargo, esta estrategia es poco eficaz. Este informe descubrió también que el 67 % de las firmas encuestadas había sufrido una vulneración de la seguridad en los 12 meses anteriores, y el 100 % de ellas en algún momento de su historia.[18]

En concreto, el software antivirus es especialmente ineficaz. Damballa llevó a cabo unas pruebas donde atacan una red deliberadamente para medir la respuesta del antivirus. Pasaron más de seis meses hasta que se identificó el 100 % de los archivos maliciosos.[19] Esta información coincide con otro descubrimiento de PAC, según el cual las empresas tardan entre uno y seis meses en averiguar que han sufrido un ataque.

La seguridad de los terminales ya no reside en la prevención. El número cada vez mayor de incidentes causados por virus/malware, además de la falta de seguridad inherente de las políticas BYOD/trabajo remoto, convierten las infracciones de seguridad en algo inevitable. Nadie está sugiriendo que la prevención y protección deban abandonarse por completo, pero la detección y la respuesta oportuna deben cobrar mayor importancia.

La vigilancia continuada y en tiempo real es necesaria, idealmente mediante el uso de los propios terminales como sensores que alerten al resto de la red cuando sufran una infracción. Así se permite una respuesta remota de la seguridad de TI, que incluye procesos como los siguientes:

- Apagado remoto de dispositivos
- Finalización de un proceso infectado o que extienda el malware
- Puesta en cuarentena de un archivo o grupo de archivos específicos
- Interrupción de las redes de comunicaciones para aislar los dispositivos infectados[20]

Aceptar que las vulneraciones van a ocurrir y adoptar protocolos de respuesta adecuados, además de implementar la tecnología necesaria para llevarlos a cabo, es la única manera de garantizar la seguridad cibernética cuando la prevención ha quedado obsoleta.

> "No hay tecnología capaz de ofrecer seguridad si los usuarios la quebrantan."
>
> – Joseph Steinberg [21]

Seguridad de los empleados

Salvaguardar a las personas que utilizan los dispositivos es tanto o más importante que asegurar los propios dispositivos.
Todos los empleados deben recibir formación en materia de seguridad cibernética, y deben estar al corriente de los riesgos del phishing, de las webs sospechosas y de la descarga de archivos adjuntos sospechosos. Además, deben estar al tanto de la política de seguridad de contraseñas, utilizando contraseñas seguras y únicas cada vez que tengan que iniciar sesión para acceder a información confidencial y haciendo uso del gestor de contraseñas adecuado para almacenarlas.

Deben ser conscientes de la importancia de mantener el software de seguridad de sus dispositivos actualizado para facilitar la vigilancia de TI. Deben estar alerta sobre el uso de dispositivos seguros para acceder a las redes de la empresa y evitar la utilización de sus dispositivos personales en redes externas y sin protección para acceder a datos sensibles.

Numerosos expertos de alto nivel en seguridad cibernética recomiendan simular ataques phishing, incluso mediante la creación de sitios web de phishing para entrenar a todos los empleados, y llevar la formación en seguridad cibernética a un nivel superior. Y es que la mayoría de los ataques depende de puntos débiles humanos, ya sea mediante negligencias o de forma intencionada.

Las personas son el eslabón más débil de cualquier red.

[18] PAC Incident Response Management 2015
[19] https://www.damballa.com/time-to-fix-malware-strategies-2/
[20] The Essential Endpoint Detection Checklist – HP Now
[21] https://digitalguardian.com/blog/data-security-experts-answer-what-biggest-misconception-companies-have-about-endpoint-security

Conclusión

El gasto en seguridad informática debería centrarse en la detección y respuesta, en vez de en la prevención y la protección

La defensa de los datos empresariales en el entorno informático actual, que se enfrenta cada vez a más amenazas cibernéticas y a una pérdida de control del perímetro de la red, requiere dos acciones: un salto conceptual y mayores recursos.

El concepto de red necesita modificarse: la idea de una red como una valla que rodea un grupo de dispositivos ha perdido vigencia. Es hora de afrontar la realidad: "la red" es una masa desestructurada. Está formada por dispositivos conectados que actúan como terminales. Asegurar la red significa asegurar dichos terminales, que constan de dos elementos: el dispositivo y su usuario. Ambos deben tenerse en cuenta.

Sin embargo, implementar una seguridad efectiva en este nuevo paradigma es mucho más complicado que hacerlo en el entorno del pasado, donde los ordenadores de sobremesa se conectaban por Ethernet. Se necesitan mayores recursos que hay que impulsar, según admite el 61 % de los encuestados por Ponemon.

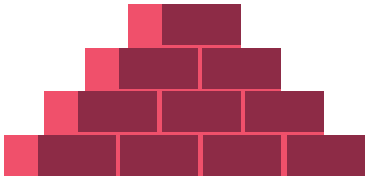
La clave reside en involucrar al resto de la organización. Solo el 36 % de los encuestados opina que dispone de presupuesto y personal para implementar seguridad en los terminales. El 69 % dice que el departamento de TI no puede copar la demanda de los empleados para ofrecer mayor soporte. El 71 % asegura que las políticas de seguridad en los terminales son difíciles de implementar.[22]

El 80 % de los directores de seguridad informática opina que el cumplimiento normativo es la mejor forma de justificar el presupuesto de sus programas de seguridad, pero también cree que dicho cumplimiento es el área menos importante en la que invertir recursos. El cumplimiento normativo consiste en alcanzar los mínimos exigidos.[23]

Los encargados de las decisiones informáticas deben cooperar con los mandos superiores para resaltar la importancia de la seguridad. Dejar claros los costes de una seguridad laxa (los gastos de recuperación, la pérdida de ingresos y un valor bursátil menguado) y subrayar los ahorros a largo plazo. La mayoría de soluciones de seguridad también origina mejoras en otras áreas. Considera la mejora de productividad al implementar seguridad de impresión, y los beneficios en la productividad al ofrecer una tecnología actualizada con regularidad dentro de un programa CYOD flexible ofrecido por una empresa externa (como HP DaaS). Un caso de negocio claro puede ser construido.

El desafío es formidable y, con el paso del tiempo, gracias al aumento desmesurado de los dispositivos en la era del Internet de las cosas y el aumento de la sofisticación de los delitos cibernéticos, será cada vez más grande, aunque no insuperable. Con la tecnología, la estrategia y los recursos adecuados, podemos defender nuestros terminales y mantener la seguridad de nuestros datos.

Para más información sobre los Dispositivos como servicio de HP (HP DaaS) y cómo pueden ayudarte a poner en marcha un programa CYOD exhaustivo, flexible y seguro, visita **www.hp.com/go/daas.**



Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA7-1089ESE

[22] Ponemon 2016 State of the Endpoint Report

[23] https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697