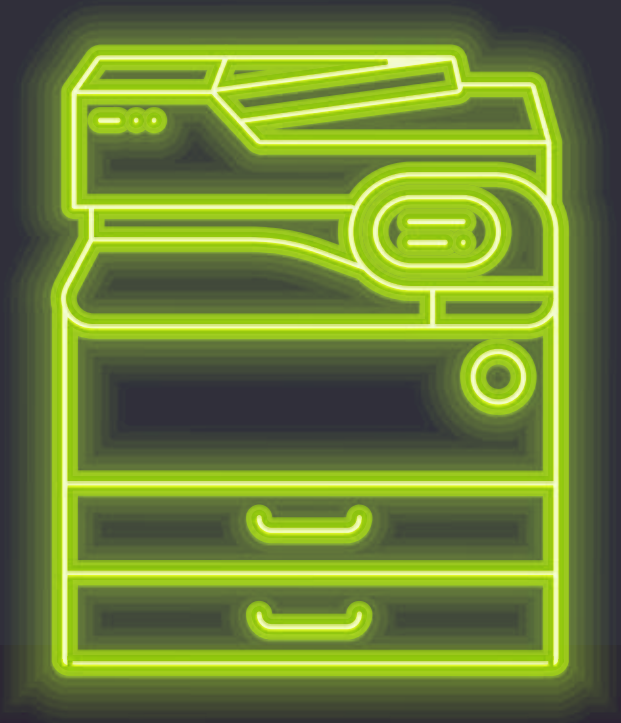
Seguridad de las impresoras: El nuevo imperativo de TI

Los estudios muestran que la «humilde impresora» permanece como un punto ciego de la seguridad



Índice

Introducción

A pesar de que aumentan las amenazas a la seguridad de TI, los esfuerzos por proteger el hardware no suelen estar a la altura. El problema más evidente es con las impresoras. Aunque los profesionales de TI son cada vez más conscientes de los peligros que plantean para la red las impresoras desprotegidas, estas siguen ocultas en el punto ciego de la seguridad, la mayoría operando sin protección.

«Se están exponiendo vulnerabilidades en todo tipo de dispositivos conectados a la red, incluida la humilde impresora de red», declara Ben Vivoda, director de sistemas de impresión para HP Pacífico Sur. **«Normalmente, vemos cómo la impresora se deja fuera, se ignora y a menudo queda expuesta. Las empresas ya no pueden permitirse ignorar la impresión al diseñar una estrategia global de ciberseguridad de TI».**[1]

De hecho, según un estudio reciente realizado por Spiceworks, las impresoras son el origen de un número cada vez mayor de amenazas a la seguridad. Hoy en día, una impresora tiene un 68 % más de probabilidades de ser el origen de una amenaza o infracción externa que en 2016; una cifra que alcanza el 118 % en el caso de amenazas o infracciones internas.

Y sin embargo, tan solo el 30 % de los profesionales de TI reconoce que las impresoras suponen un riesgo de seguridad. Aunque esta cifra se ha duplicado desde 2016, sigue siendo demasiado baja y refleja una realidad peligrosa. Muchos profesionales de TI parecen mantener una perspectiva obsoleta de la seguridad de las impresoras, posiblemente fundada en la antigua percepción de que las impresoras están seguras dentro del perímetro de la red.

Incluso aquellos profesionales de TI que reconocen el riesgo, con frecuencia otorgan la máxima prioridad a proteger la superabundancia de dispositivos de usuarios finales, dejando las impresoras totalmente abiertas y, a su vez, las redes vulnerables.[2] Aunque es comprensible que la seguridad de las impresoras se haya relegado a un segundo plano con respecto a otros puntos de conexión del pasado, resulta esencial que las organizaciones de TI empiecen a enfrentarse a los riesgos que las impresoras no protegidas plantean tanto para su infraestructura de TI más amplia como para la gobernanza general de la empresa.

El riesgo para la empresa

¿Son las impresoras realmente un problema? En una palabra: sí. En una era en la que emergen nuevas amenazas para la seguridad cada hora, una impresora puede ser un objetivo fácil. «Las impresoras modernas son esencialmente hosts de red avanzados y especializados. Como tales, debería prestarse el mismo nivel de atención a su seguridad que a la de los ordenadores tradicionales», declara Kevin Pickhardt en *Entrepreneur*[2]. «Las impresoras de oficina no son solo fuentes potenciales de pérdida de datos y problemas de confidencialidad, sino también vectores de ataque que pueden explotar los hackers». Ejemplo: según nuestras fuentes, el año pasado, un hacker informático utilizó una secuencia de comandos automatizada para acceder a 150 000 impresoras públicamente accesibles, entre las que se incluía un gran número de impresoras para imprimir recibos, y les ordenó que ejecutaran un trabajo de impresión fraudulento[3].

Los analistas del sector coinciden. Según IDC: «La mayoría de las impresoras tienen acceso sin restricciones a una red interna. **Un atacante que ponga en peligro una impresora, puede obtener un acceso sin restricciones a la red, las aplicaciones y los activos de datos de una organización».**[4]

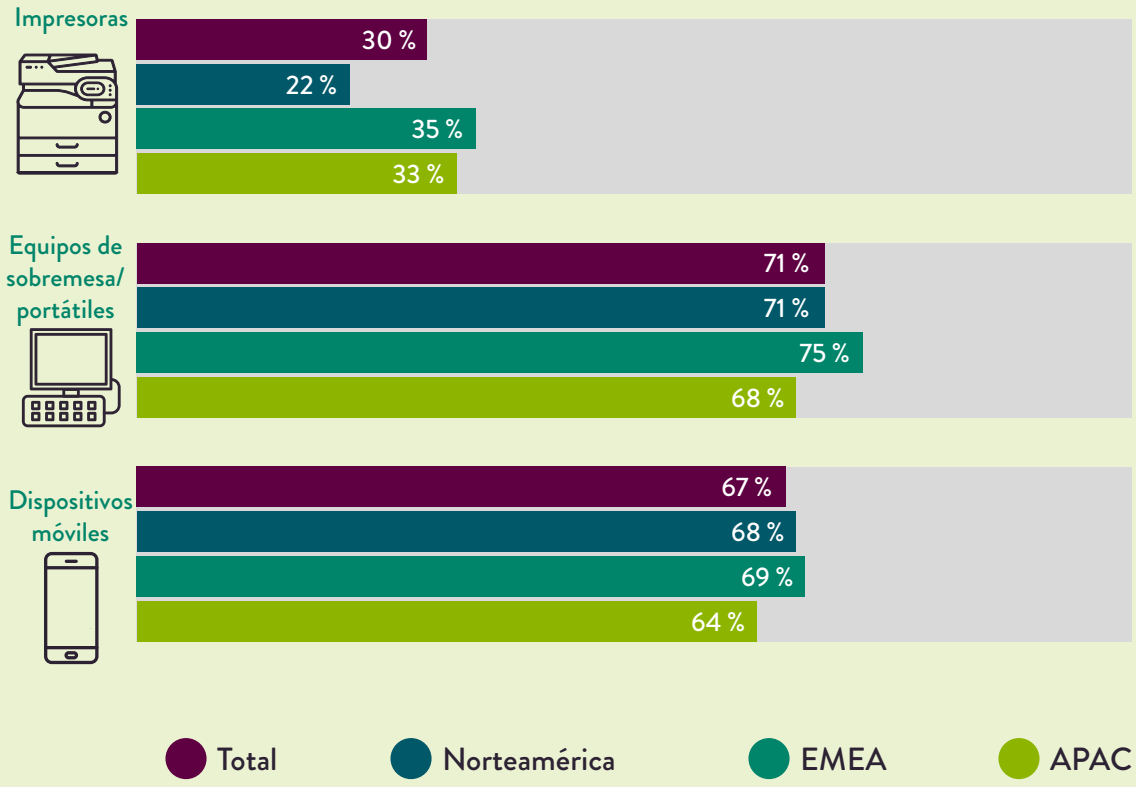
¿Qué aspecto tiene una impresora de red sin protección? No está protegida y, por tanto, está abierta a una amplia gama de protocolos de red.
No requiere controles de acceso (a menudo, ni siquiera se define una contraseña de administrador). Permite imprimir documentos confidenciales sin autenticación,
de modo que pueden permanecer en una bandeja de salida durante horas. Envía datos no cifrados a la red. Ejecuta firmware obsoleto, o no se supervisa en busca de amenazas a la seguridad.

Todos estos fallos de seguridad tendrán consecuencias. Gartner predice que, en 2020, más de la mitad de los proyectos del Internet de las cosas (IoT) expondrán información sensible por no aprovechar las funciones de seguridad del hardware, frente a tan solo un 5 % actual.[4]

Un problema de percepción

No obstante, y a pesar de los estudios, los profesionales de TI siguen sin reconocer los riesgos que plantean las impresoras. En Norteamérica, ni siquiera una cuarta parte de los profesionales de TI (22 %) reconoce a las impresoras como un riesgo de seguridad, mientras que en Europa, Oriente Medio y África (EMEA), esa cifra representa algo más de un tercio del total, con un 35 %.

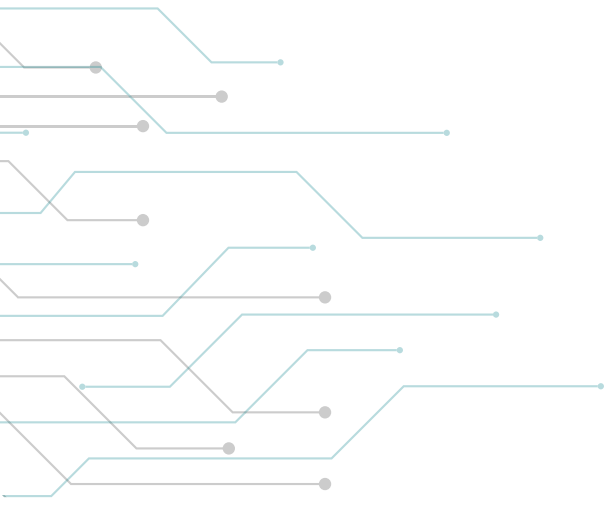
Nivel percibido de riesgo para la seguridad



Por el contrario, un 71 % de los profesionales de TI reconoce la amenaza que plantean los equipos de sobremesa y portátiles, y un 67 % la que suponen los dispositivos móviles.

El estudio de Spiceworks muestra además que los profesionales de TI que sí adoptan medidas preventivas, han adoptado enfoques incompletos. No es de extrañar, si tenemos en cuenta la amplitud de los requisitos de seguridad. Ninguna solución por sí sola es suficiente; implementar un cortafuegos por sí solo no basta, por ejemplo. Como con cualquier dispositivo de red, la seguridad de las impresoras debe enfocarse desde varios ángulos. Y como con cualquier estrategia de seguridad, las soluciones más eficaces deberán integrarse y automatizarse, y ser fáciles de usar y gestionar.

Para complicar todavía más el desafío, se debe tener en cuenta que cada marca de impresora presenta su propio software y sistema operativo patentado. Cabe esperar que muchos profesionales de TI no cuenten con el conocimiento suficiente para configurar el software de sus impresoras con el fin de que cumpla sus políticas de seguridad.



Prácticas actuales

Los profesionales de TI están adoptando diversos enfoques con respecto a la seguridad de las impresoras, que crean una combinación personalizada de prácticas y funciones de seguridad basadas en las herramientas de las que disponen y su comprensión de las mismas. No obstante, a grandes rasgos, los enfoques de la seguridad de las impresoras actuales pueden dividirse en seis grupos.

El porcentaje de encuestados que aplica actualmente las siguientes prácticas de seguridad para las impresoras

42 % Seguridad de los documentos

31 % Seguridad de los dispositivos

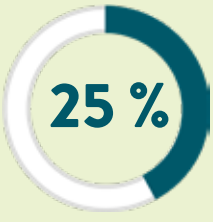
40 % Seguridad de la red

30 % Supervisión de la seguridad

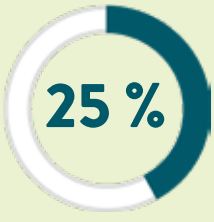
39 % Control de acceso

28 % Protección de datos

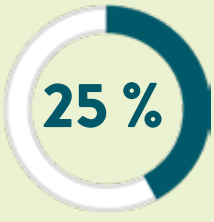
El estudio reveló que los profesionales de TI están adoptando una serie de pasos de seguridad fundamentales dentro de estas categorías, pero, desgraciadamente, a un ritmo muy lento.



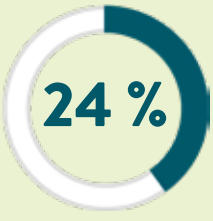
Cierre de puertos abiertos no utilizados



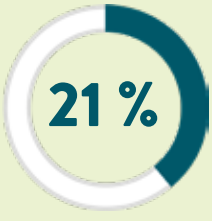
Activación de la función «enviado desde»



Protección del acceso a la impresora para reparaciones



Implementación de la impresión («pull») con privacidad

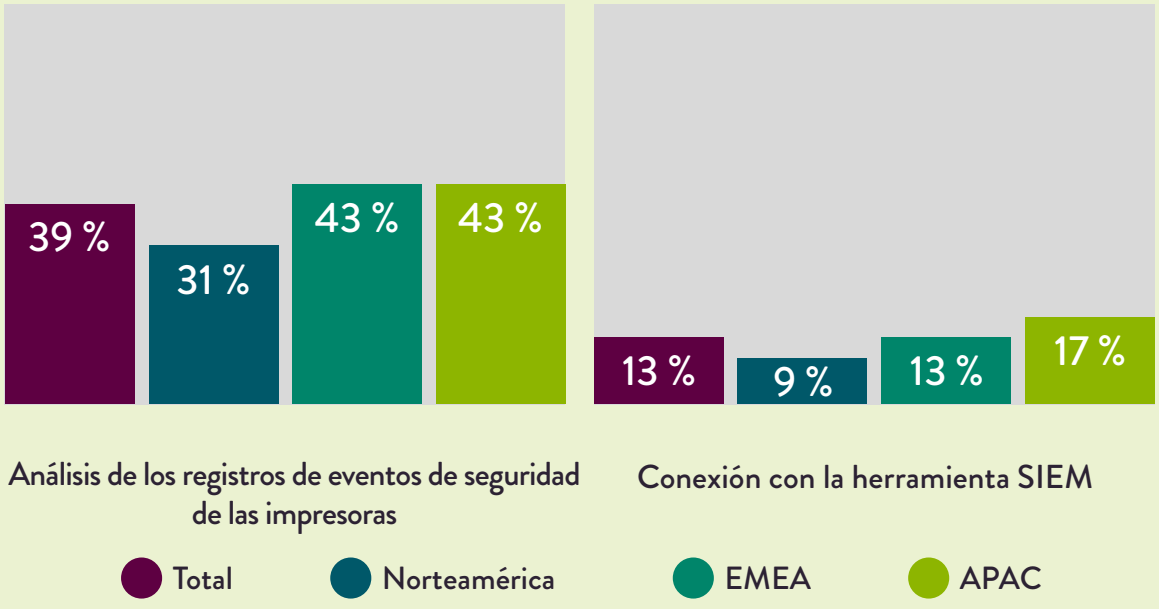


Borrado rutinario de los discos duros de las impresoras

Un número todavía menor de profesionales de TI cierra o purga trabajos de forma programada, exige acceso de administrador para realizar cambios en la configuración, o automatiza la gestión de certificados.

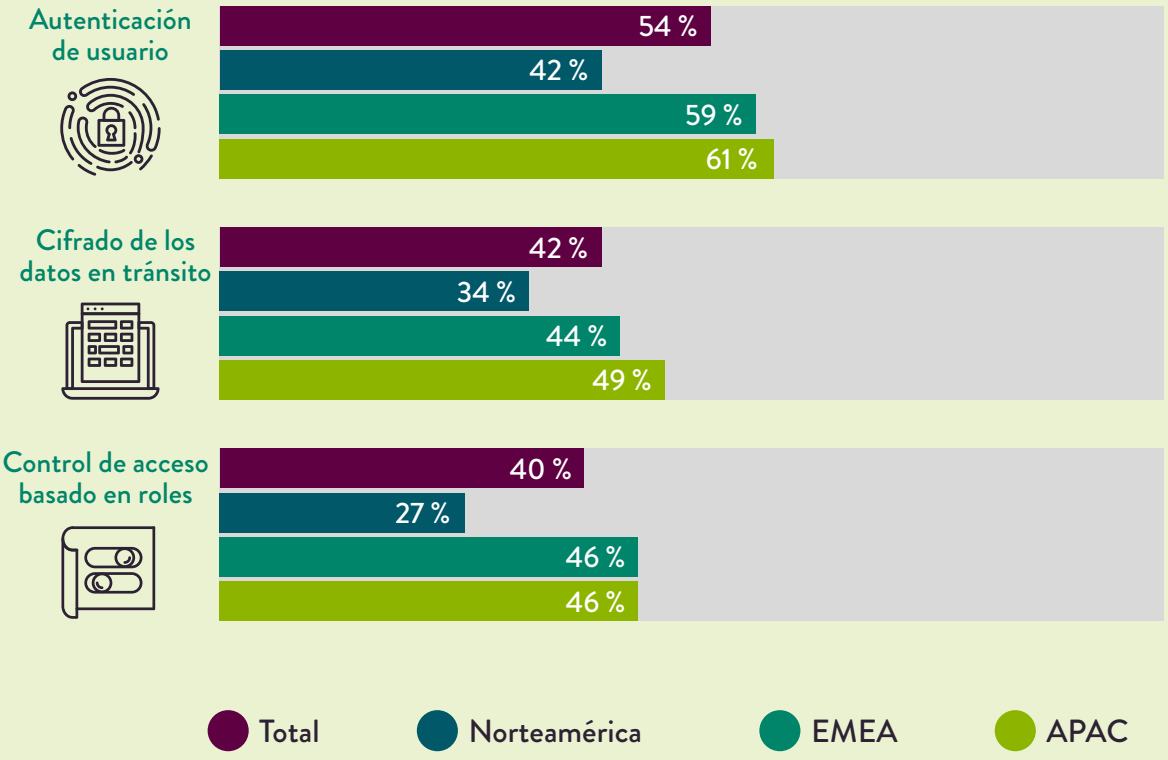
Los profesionales de TI *sí* están implementando la supervisión de la seguridad de las impresoras con más frecuencia que otras actividades, pero los índices siguen siendo bajos; tan solo el 39 % declara analizar periódicamente los registros de la impresora, y en Norteamérica, únicamente el 31 %. En cuanto a la conexión de las impresoras a herramientas de SIEM, tan solo el 13 % indica haberlo hecho. El hecho de no supervisar los registros de las impresoras y de no integrarlas con SIEM, deja a los profesionales de TI a oscuras, sin conocimiento de los ciberdelincuentes que pueden estar utilizando la infraestructura no supervisada para ocultarse en una red y exfiltrar datos.

Supervisión de impresoras



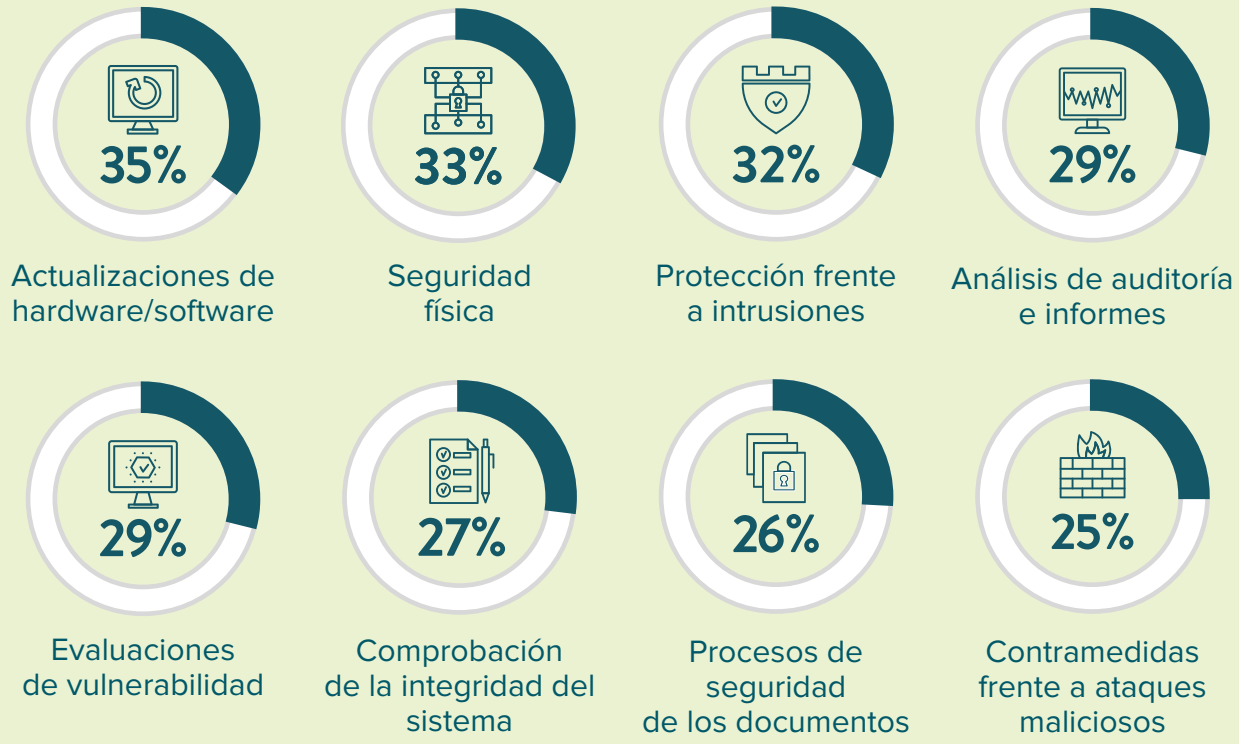
El estudio desvela otras diferencias geográficas con respecto a determinadas áreas de la seguridad de las impresoras, donde, una vez más, Norteamérica se queda atrás. Ello resulta especialmente cierto en el caso de los controles de acceso y el cifrado. Los profesionales de TI en el área de Asia y el Pacífico son mucho más proclives que los de Norteamérica a cifrar los datos en tránsito, solicitar identificación en el dispositivo, e implementar controles de acceso basados en los roles de los usuarios.

Prácticas de seguridad de las impresoras implementadas



Por último, a la hora de satisfacer las normativas de privacidad de los datos, los profesionales de TI confían de nuevo en multitud de enfoques y, en ocasiones, los controles de las impresoras quedan absorbidos por la estrategia de cumplimiento de TI global. El estudio de Spiceworks preguntó a los profesionales de TI qué controles de cumplimiento habían implementado, sobre la base de los «Controles de CIS V7» del Centro para la seguridad de Internet (CIS, por sus siglas en inglés).[5]

Controles de cumplimiento en uso



Estos datos muestran que los profesionales de TI a menudo ignoran las precauciones de seguridad de las impresoras más básicas, como la actualización del firmware; tan solo en torno a un tercio de los encuestados, había convertido esta actividad en parte rutinaria de sus actividades de cumplimiento. Los estudios del sector coinciden. Según IDC, las impresoras no se actualizan con el firmware más reciente porque las organizaciones subestiman el riesgo.[4] Además, es posible que no dispongan del tiempo necesario para analizar, probar y aceptar el nuevo firmware en todas las impresoras de la flota.

Hacia la seguridad completa de las impresoras

Del 84 % de profesionales de TI que declara disponer de una política de seguridad, solo el 64 % indica que incluye la impresión. En el caso de Norteamérica, la cifra es de tan solo el 52 %. Este es uno de los motivos por los que resulta tan importante buscar controles de seguridad integrados y automatizados para las impresoras, así como implementarlos realmente. Las impresoras con funciones de seguridad integradas permiten minimizar el riesgo, mientras maximizan la inversión en TI.

Los analistas de IDC también han considerado esta declaración como cierta: «Las impresoras son mucho más difíciles de proteger una vez se envían, lo que subraya la importancia de seleccionar dispositivos que se envíen con funciones de seguridad básicas y avanzadas ya integradas».[4] Gartner indica: «Para explotar las dinámicas de los mercados de impresión emergentes, los planificadores tecnológicos estratégicos deben diseñar un portfolio completo de soluciones de seguridad de las impresoras, utilizando niveles de soluciones que vayan más allá de las mejores prácticas del sector. Esas soluciones deben integrarse con el ecosistema más amplio de soluciones de seguridad»[6].

Los proveedores de servicios gestionados de impresión están ampliando sus servicios para cubrir aquellos departamentos de TI cuyas plantillas carecen de la amplitud de conocimientos necesarios para responder a la seguridad de las impresoras. Según IDC: «Los proveedores ofrecen una amplia gama de servicios de protección tanto para dispositivos como para datos, muchos de los cuales se han diseñado para integrarse con los sistemas de gestión de documentos y contenido empresarial existentes con el fin de ofrecer una mayor protección y responder a los problemas de gobernanza y conformidad normativa».[7]

Por suerte para los profesionales de TI, las impresoras avanzadas de hoy en día ofrecen docenas de funciones de seguridad integradas para su portfolio de seguridad, incluidas la detección de amenazas, protección, notificación y recuperación automática, lo que facilita más que nunca la protección de uno de los puntos de conexión más vulnerables de su red: la humilde impresora.

Es el momento de fortalecer la seguridad de sus impresoras.

Más información

Acerca del estudio

HP encargó un estudio a Spiceworks en mayo de 2018, dirigido a los responsables de la toma de decisiones de TI, incluidos directores, responsables y resto de personal de TI, para comprender las prácticas actuales de seguridad de las impresoras e identificar las áreas de riesgo. Los resultados del estudio presentaron las respuestas de unos 500 participantes de Norteamérica, EMEA y APAC, pertenecientes a organizaciones de 250 empleados o más.

Fuentes

1 McLean, Asha, «Unsecured printers a security weak point for many organisations: HP» (Las impresoras no protegidas son un punto débil para muchas organizaciones: HP), *ZDNet*, 18 de abril de 2017.
https://www.zdnet.com/article/unsecured-printers-a-security-weak-point-for-many-organisations-hp/

2 Pickhardt, Kevin, «Why Your Innocent Office Printer May Be a Target For Hackers» (Por qué su inocente impresora de oficina puede ser un objetivo para los hackers), *Entrepreneur*, 31 de enero de 2018.
https://www.entrepreneur.com/article/308273

3 Peyser, Eve, «Hacker Claims He Hacked 150,000 Printers to 'Raise Awareness' About Hacking» (Un hacker declara que pirateó 150 000 impresoras para «concienciar» sobre la piratería), *Gizmodo*, 6 de febrero de 2017.
https://gizmodo.com/hacker-claims-he-hacked-150-000-printers-to-raise-aware-1792067012

4 Brown, Duncan, et al., «IDC Government Procurement Device Security Index 2018» (Índice de seguridad de los dispositivos adquiridos por el gobierno en 2018), *IDC*, mayo de 2018.

5 «Controles de CIS», *Centro para la seguridad de Internet*, marzo de 2018.
https://www.cisecurity.org/controls/

6 Von Manowski, Kristin Merry y Deborah Kish, «Market Insight: IoT Security Gaps Highlight Emerging Print Market Opportunities» (Visión del mercado: las brechas de seguridad del IoT desvelan oportunidades en el emergente mercado de la impresión), *Gartner*,
31 de octubre de 2017
https://www.gartner.com/doc/reprints?id=1-4OCKFKG&ct=180110&st=sb

7 Palmer, Robert y Allison Correia, «IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment» (IDC MarketScape: evaluación de servicios y soluciones de seguridad en todo el mundo de los proveedores de copias impresas de 2017), IDC, 2017.