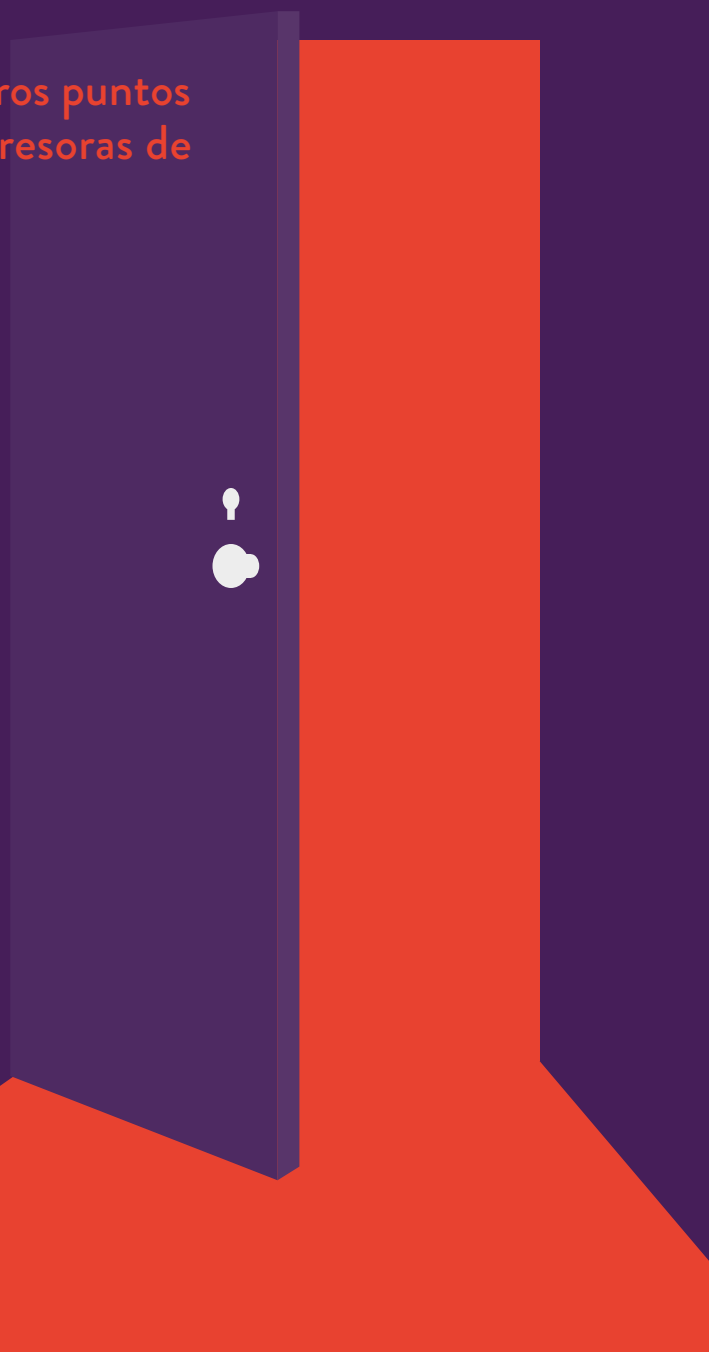
NOTAS DEL PRODUCTO

PUERTAS DESPROTEGIDAS

LA INVESTIGACIÓN INDICA QUE LAS IMPRESORAS SIGUEN ESTANDO DESPROTEGIDAS ANTE LOS CIBERATAQUES

Mientras los equipos de TI se centran en otros puntos finales, se descuida la seguridad de las impresoras de las empresas



Las impresoras son objetivos fáciles: Hay demasiadas impresoras conectadas a la red que carecen de restricciones y no están protegidas.

Sin embargo, la amenaza es real y no debe ignorarse. Las impresoras de categoría empresarial se han convertido en dispositivos potentes y conectados a la red con las mismas vulnerabilidades que cualquier otro punto final de su red. Estos puntos de entrada, que normalmente están desprotegidos, presentan una alta probabilidad de recibir ciberataques. Además, pueden ofrecer acceso a la información confidencial y financiera de su empresa con verdaderas consecuencias para la empresa.

Pese a ello, una reciente encuesta de Spiceworks realizada a más de 300 responsables en la toma de decisiones empresariales de TI, muestra que solo el 16 % de los encuestados piensa que las impresoras tienen un alto riesgo de amenaza o ataque, un porcentaje significativamente inferior en comparación con los equipos de sobremesa/portátiles y dispositivos móviles.[1] Esta percepción ha perjudicado el modo en que el personal de TI está abordando la seguridad de la red. Si bien casi tres de cada cinco organizaciones cuentan con prácticas de seguridad para las impresoras, este porcentaje se encuentra muy por debajo del de otros puntos finales y deja a las impresoras en una situación de vulnerabilidad aunque existan soluciones sencillas para proteger este particular punto de entrada.

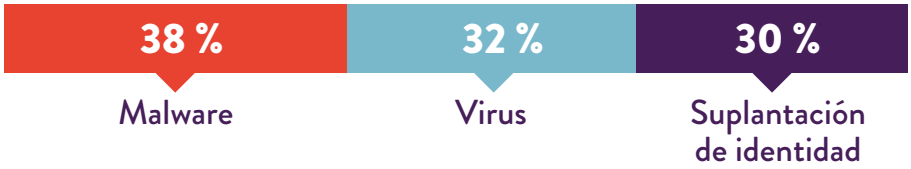
Estas notas del producto ofrecen información sobre la seguridad de las impresoras basada en la encuesta de Spiceworks, los efectos de las brechas de seguridad y algunas de las modernas funciones integradas relativas a la seguridad de las impresoras que se han diseñado para ofrecer protección frente a los ciberataques.

SOLO EL 16 % DE LOS ENCUESTADOS PIENSA QUE LAS IMPRESORAS PRESENTAN UN ALTO RIESGO DE AMENAZA/ATAQUE.[1]

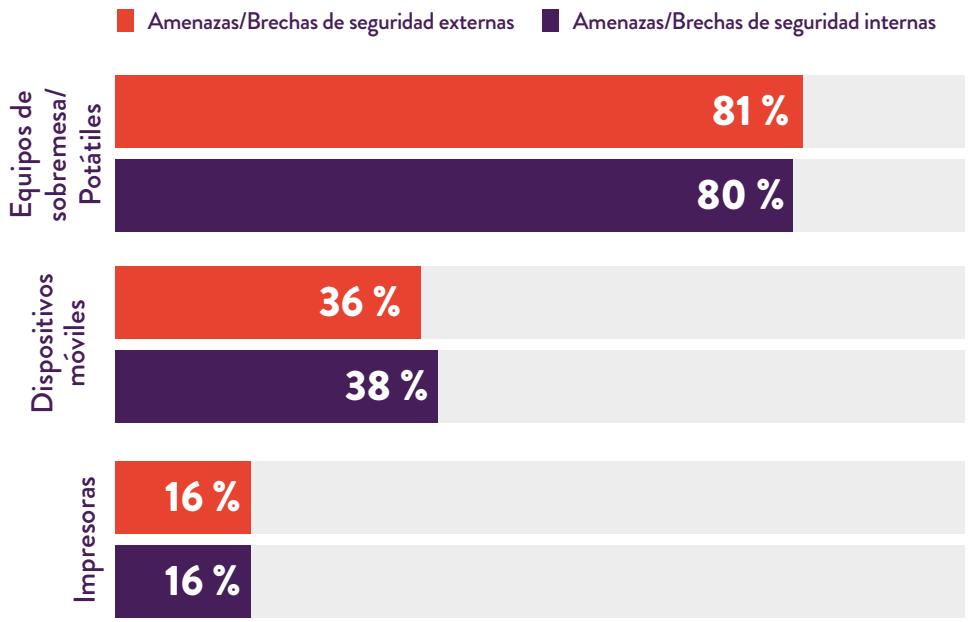
LA PUERTA DE ENTRADA DE LOS ATAQUES

En la encuesta de Spiceworks, el 74 % de los encuestados (neto) indicó que sus organizaciones experimentaron al menos un tipo de amenaza o ataque de seguridad externo el pasado año. Y el 70 % (neto) experimentó un tipo de amenaza o ataque de seguridad de TI interno, generalmente debido al error de un usuario, el uso de dispositivos personales por motivos de trabajo, o a la utilización por parte de empleados de una red doméstica o pública por motivos de trabajo.[1]

LAS PRINCIPALES AMENAZAS/BRECHAS DE SEGURIDAD DE TI EXTERNAS EXPERIMENTADAS



Las amenazas más importantes suelen afectar a los equipos de escritorio y portátiles, mientras que el resto de amenazas suelen afectar a dispositivos móviles e impresoras.[1] (El 16 % de las amenazas que afectan a las impresoras constituye una cifra notablemente superior con respecto al 4 % descubierto en un estudio similar de Spiceworks de 2014). Asimismo, es posible que se subestime el número de ataques dirigidos a impresoras, debido a que no se suelen supervisar las impresoras tan de cerca como los ordenadores y dispositivos móviles.



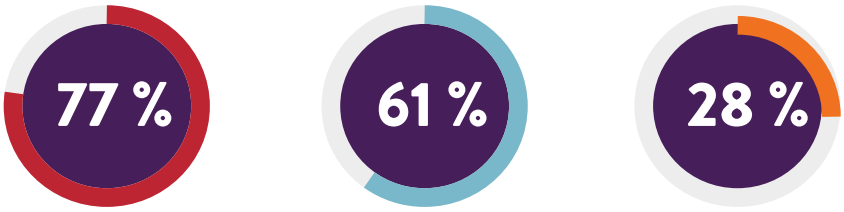
ESTAMOS DESCUIDANDO NUESTRAS IMPRESORAS

En cualquier caso, la encuesta de Spiceworks deja claro que la seguridad de las impresoras suele ser con frecuencia una reflexión tardía.

Las organizaciones son sumamente conscientes de la importancia de la seguridad de la red, los punto finales y los datos. De hecho, más de las tres cuartas partes de los encuestados utilizan la seguridad de red, el control y gestión del acceso, la protección de los datos, la seguridad de los puntos finales, o bien una combinación de todo lo anterior.[1]

No obstante, estas soluciones suelen implementarse con menor frecuencia en las impresoras. Mientras que el 83 % de los encuestados utiliza la seguridad de red en equipos de sobremesa y portátiles, y el 55 % en dispositivos móviles, solo el 41 % la emplea en impresoras.[1]

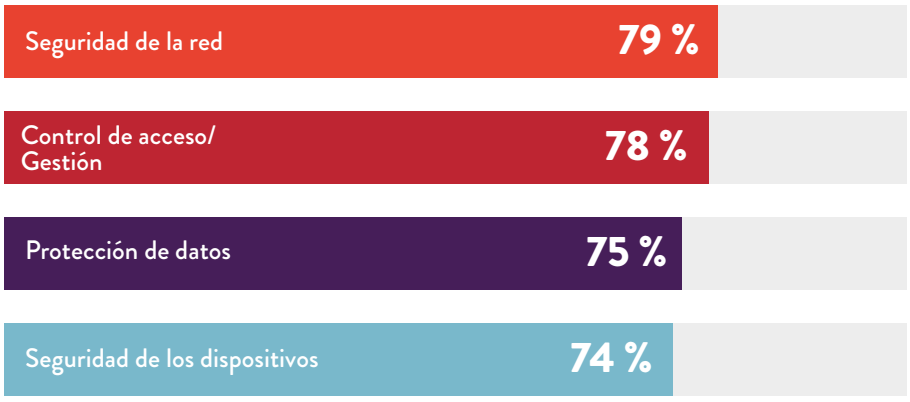
Esta disparidad es incluso más acusada en la seguridad de los puntos finales:



Ordenadores | Dispositivos móviles | Impresoras

Además, ni siquiera una tercera parte (28 %) de los encuestados implementa certificados de seguridad para impresoras, mientras que el 79 % sí lo hace en el caso de ordenadores, y el 54 % en dispositivos móviles.[1]

PRINCIPALES PRÁCTICAS DE SEGURIDAD DE PUNTOS FINALES



Entre los tipos de protección empleados en dispositivos generales de puntos finales, las medidas de seguridad más utilizadas para impresoras fueron la seguridad de los documentos, la seguridad de la red y el control del acceso. No obstante, menos de la mitad de los encuestados manifestó que sus organizaciones utilizaban cualquiera de ellas en sus impresoras.[1]

Algunas empresas disponen de prácticas de seguridad específicas para impresoras, pero incluso en estos casos, las prácticas son muy diversas. Tan solo un 40 % de las organizaciones ha implementado la autenticación de usuario y menos del 40 % ha utilizado contraseñas de administrador para la interfaz de configuración web.[1] Con el fin de contar con una fuerte protección, las organizaciones deberían utilizar una combinación de todas estas estrategias, además de otras.

PRINCIPALES PRÁCTICAS DE SEGURIDAD ESPECÍFICAS PARA IMPRESORAS

Cuando se trata del cumplimiento de los puntos finales y de las prácticas de auditoría, los controles de seguridad de las impresoras son muy inferiores a casi todos los demás puntos finales. Cerca del 90 % de las organizaciones cuenta con una política de seguridad de la información, pero esta política, por lo general, no incluye las impresoras. Por ejemplo, mientras que el 57 % de los encuestados manifestó que contaba con protección contra malware en sus ordenadores, solo el 17 % la había implementado en las impresoras.[1]

CASI 9 DE CADA 10 PROFESIONALES DE TI DECLARAN QUE SU ORGANIZACIÓN DISPONE DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEBIDO A LO SIGUIENTE:

Indudablemente, las organizaciones no se están tomando lo suficientemente en serio la seguridad de las impresoras, pero deberían hacerlo.

«Muchas impresoras incluyen todavía las contraseñas predeterminadas, o incluso no incluyen ninguna contraseña, o bien, existen casos en los que diez impresoras utilizan la misma contraseña», declara Michael Howard, asesor principal de seguridad de HP para Computerworld en junio. «Una impresora sin protección con contraseña es una mina de oro para un hacker. Uno de los ataques que solemos ver a menudo es el llamado «ataque man-in-the-middle». Consiste en tomar el control de una impresora y desviar [los documentos entrantes] a un portátil antes de que se impriman. Pueden ver todo lo que el director general está imprimiendo».[2]

EL IMPACTO POTENCIAL DE LAS INTRUSIONES EN LAS IMPRESORAS

Bogdan Botezatu, analista sénior de ciberataques de Bitdefender, explica que las amenazas representan una considerable brecha potencial en la seguridad. «Obtenemos una gran cantidad de telemetría en nuestros laboratorios de evaluación de vulnerabilidades. El enrutador ya no es el peor dispositivo de Internet. Ahora es la impresora».[3]

Esta vulnerabilidad puede tener efectos considerables en una empresa.

Una sola impresora sin protección podría provocar que toda una red de dispositivos fuera vulnerable a un ataque, otorgando a los hackers la capacidad de espiar los dispositivos en red y, a su vez, de poner en riesgo la seguridad de toda la red.

Todos hemos comprobado los efectos de las brechas de seguridad. En la encuesta de Spiceworks, los encuestados manifestaron que los cinco principales impactos de un ataque son:[1]

1. Incremento de las llamadas al centro de asistencia técnica y del tiempo dedicado a la asistencia

2. Reducción de la productividad/ eficiencia

3. Incremento del tiempo de inactividad del sistema

4. Incremento del tiempo empleado en las llamadas de asistencia

5. Incremento de la aplicación de políticas de usuario final

No obstante, el ataque a una impresora puede ser incluso más grave, especialmente si se utiliza una impresora multifunción capaz de almacenar datos impresos electrónicamente. Los trabajos de impresión almacenados en la memoria caché de una impresora permiten que los hackers obtengan acceso a información confidencial, tanto personal como empresarial.

Es incluso todavía más preocupante que los hackers puedan obtener acceso a una red empresarial más amplia a través de una impresora sin protección y robar información como los números de la Seguridad Social, la información financiera, o las memorias y documentos internos. La información robada puede afectar no solo a los empleados, sino también caer en manos de la competencia, o dañar seriamente la reputación de una empresa.

LA SOLUCIÓN MÁS SENCILLA: FUNCIONES DE SEGURIDAD INTEGRADAS

Sin lugar a dudas, las empresas deben abordar la seguridad incluso en sus impresoras. Algunas de las impresoras empresariales más modernas cuentan con un sistema de seguridad fácil de usar e integrado que le protege de las amenazas. Este sistema incluye:

- Detección de ataques, protección y recuperación automáticas
- Seguimiento del uso para prevenir el uso no autorizado
- Opciones simples de inicio de sesión, como PIN o tarjetas inteligentes
- Un lector de tarjetas de proximidad que permite a los usuarios realizar rápidamente la autenticación e imprimir de forma segura con una impresora que utiliza una credencial de identificación
- Impresión cifrada segura para documentos confidenciales

Siempre que se plantee cuál será su siguiente impresora, tanto si es de escritorio como multifunción, estudie los distintos modos de protección integrados y asegúrese de activarlos. Siempre y cuando disponga de funciones sencillas y específicas para la impresora, no tendrá que preocuparse de la seguridad que le ofrecen sus impresoras. Después de todo, con el Internet de las cosas, existen muchos otros puntos de acceso de los que preocuparse. **No hay razón para que sus impresoras sean uno de ellos.**

¿ESTÁ BUSCANDO IMPRESORAS MÁS SEGURAS?

MÁS INFORMACIÓN ›

Fuentes:

[1] Encuesta de Spiceworks realizada a 309 responsables en la toma de decisiones de TI en Norteamérica, EMEA y APAC, en nombre de HP, en noviembre de 2016.

[2] «Printer Security: Is your company's data really safe?» (Seguridad de las impresoras: ¿están los datos de su empresa realmente protegidos?) Computerworld, 1 de junio de 2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] «Printers Now the Least-secure Things on the Internet» (Las impresoras son ahora los dispositivos menos seguros de Internet) The Register, 8 de septiembre de 2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/