NOTICIAS DESTACADAS DEL MERCADO DE IDC

El punto ciego del RGPD: por qué las impresoras suponen una debilidad para su cumplimiento

Julio de 2017

Por Duncan Brown

Con el patrocinio de HP

Este informe sobre las noticias destacadas del mercado de la International Data Corporation (IDC) pone de relieve la naturaleza vulnerable de las impresoras en las redes empresariales y, en particular, cómo esta vulnerabilidad afecta a un programa de cumplimiento centrado en el Reglamento General de Protección de Datos (RGPD) y en otras legislaciones futuras. El documento también informa sobre cuáles son los pasos para reducir el riesgo que representan las impresoras no seguras para la empresa.

Introducción

La atención que se le daba a la seguridad del Internet de las cosas (IoT, por sus siglas en inglés) creció significativamente después de una serie de ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés) de alto perfil que dirigía un enorme volumen de tráfico malicioso desde miles de cámaras de vigilancia, grabadoras de vídeo digital y otros dispositivos conectados infectados con el fin de hacer caer sitios web populares. ¿Qué dispositivo será el próximo objetivo?

Mientras buscamos otros dispositivos del IoT que compartan algunas de las características de los dispositivos utilizados en los últimos ataques, nuestra atención se centra en las impresoras de los consumidores, los pequeños negocios y las empresas. Las actualizaciones de *software* y el control de acceso, que son prioridades en los productos de tecnología informática (TI) tradicionales, a menudo se pasan por alto en las impresoras. Las impresoras pueden ser el siguiente objetivo para un gran ataque al IoT, pero también podrían representar nuevos peligros para las operaciones comerciales porque residen dentro de la red empresarial y posibilitan el robo de datos y DDoS en la parte interna de una red. Con las consecuencias empresariales de las violaciones a los datos personales que imponen el RGPD y otras normas recientes, la impresora de red es el periférico olvidado que necesita atención urgente.

Su impresora es un periférico

Analicemos la siguiente situación: se conecta un dispositivo desconocido a una red empresarial, detrás de las defensas perimetrales como los cortafuegos, los sistemas de prevención de intrusiones y otras infraestructuras de TI, de manera que el dispositivo tiene acceso sin restricciones a todos los recursos de la red corporativa. Se integra un servidor web en el dispositivo para maximizar su funcionalidad. Todos los puertos se establecen como «abiertos» de manera predeterminada y permiten un máximo de un gigabit de conectividad Ethernet para acceder al dispositivo. El dispositivo tendrá un SO potente, como Linux, para maximizar la funcionalidad. No se utilizará el escáner de vulnerabilidades de la empresa para examinarlo continuamente, ya que el servidor web incorporado probablemente active las herramientas de gestión de eventos e información de seguridad (SIEM, por

sus siglas en inglés) de la organización con falsos positivos. El escáner de vulnerabilidades se configurará para ignorar el dispositivo, lo que llevará a la conclusión, según la marca, de que el dispositivo no recibirá actualizaciones, mantenimiento ni revisiones durante su vida útil de 5 a 10 años. La protección del dispositivo consistirá en una contraseña predeterminada y en su mantenimiento por parte de terceros sin supervisión. El dispositivo será fundamental para la productividad de la organización, por lo que habrá uno por cada 10 empleados. Estos empleados no solo lo utilizarán, sino que también le enviarán activamente datos personales confidenciales y este los almacenará. Peor aún, esos datos también pueden llegar a un espectador casual, sin autenticación ni control de acceso.

Algunos podrían llamar a esto una pesadilla; otros lo podrían llamar impresora.

Hay que aclarar un punto muy importante. La «seguridad de la impresión» es una disciplina con años de desarrollo, impulsada en su mayor parte por la necesidad de seguridad de los datos. Como se puede suponer, las normas de cumplimiento desempeñan un papel importante en el impulso de la disciplina de seguridad de la impresión. En la región EMEA, esto es sinónimo del RGPD, pero también se extiende a la Directiva de Seguridad de las Redes y Sistemas de Información (NIS, por sus siglas en inglés), así como a la actualización de la Directiva de Privacidad Electrónica y la Directiva de Servicios de Pagos Revisada (PSD2, por sus siglas en inglés). Estas normas son la base para los *resultados* de seguridad, sin especificar los detalles técnicos para su cumplimiento.

Los puntos fundamentales del RGPD

El RGPD, muy esperado y bien recibido, supone una renovación de las antiguas leyes europeas de protección de datos. Sustituye a la legislación vigente que data de 1995, antes del *boom* de las puntocom, Twitter, Facebook y la nube. El RGPD actualiza la ley para tener en cuenta estos y futuros desarrollos que crean y usan datos personales.
Un beneficio adicional de este reglamento es que se aplica a todos los Estados miembros de la Unión Europea (UE).

El RGPD se promulgó en abril de 2016 y su aplicación será efectiva el 25 de mayo de 2018. Las organizaciones tienen menos de un año para garantizar su cumplimiento. Las sanciones por incumplimiento podrían alcanzar el 4 % de sus ingresos anuales mundiales o 20 millones de euros, lo que sea mayor. El RGPD también incluye la notificación obligatoria de las violaciones en la seguridad de los datos, cuyas consecuencias preocupan a las juntas ejecutivas que se inquietan por los daños que esto puede producir en su reputación corporativa.

Cabe señalar que la posible salida del Reino Unido de la UE (también conocida como Brexit) no afecta de manera significativa al amplio panorama del RGPD:

- Las empresas del Reino Unido que procesen datos personales de la UE tendrán que cumplir con el reglamento de todos modos, porque este se aplica extraterritorialmente a los datos personales de cualquier persona en la UE.
- Es probable que el Reino Unido aplique leyes locales como el RGPD para facilitar las transferencias de datos desde la UE, ya que se rige por las normas de "adecuación".

El RGPD va más allá de una cuestión de seguridad. Contiene una serie de medidas nuevas, que incluyen la portabilidad, el consentimiento y la revocación de los datos, la verificación de la edad y el derecho a que los datos personales no sean almacenados. Sin embargo, lograr el cumplimiento se reduce, en gran medida, a una buena seguridad. ¿Qué dice el reglamento específicamente al respecto?

Sorprende que el RGPD no sea prescriptivo sobre la definición de medidas de seguridad. De sus 99 artículos, solo el artículo 32 habla específicamente de la seguridad. Establece el requisito de que las

organizaciones tomen «las medidas técnicas y organizativas oportunas para garantizar un nivel de seguridad adecuado según el riesgo». En otras palabras, cada empresa deberá evaluar el riesgo asociado a los datos personales e implementar los controles de seguridad que considere necesarios.

Un aspecto de esta consideración es lo que el RGPD define como «última generación». Las empresas no están obligadas a implementar tecnología de vanguardia. Sin embargo, deben saber lo que esto significa y defender su posición. Una situación que las empresas deben evitar es intentar justificar por qué no implementaron un control de seguridad o una técnica en particular que les condujo directamente a una violación de datos.

Una de las pruebas claves que probablemente serán aplicadas por los reguladores del RGPD es lo que IDC llama la prueba de «¿Hasta dónde llegó su esfuerzo?». No conocer una vulnerabilidad es algo malo. Conocerla y no hacer nada es aún peor. Ignorar la vulnerabilidad de seguridad de una impresora podría dar lugar a una violación de los datos personales que, de ser grave, podría hacer que un regulador se pregunte si se han implementado las medidas técnicas y de organización adecuadas para proteger la información.

Es importante destacar que el alcance material del RGPD es «el procesamiento total o parcial de datos personales por medios automatizados y el procesamiento no automatizado de datos personales que forman parte de un sistema de archivo o que están destinados a formar parte de un sistema de archivo». En otras palabras, los datos no necesitan estar en formato electrónico para estar bajo su ámbito. Las copias impresas de los datos también se deberían proteger.

La Directiva de Seguridad de las Redes y Sistemas de Información

La UE entiende que, en una era de ataques cibernéticos cada vez mayores, es necesario proteger los servicios importantes, especialmente los que se consideran críticos para el funcionamiento económico o social. Para lograr la coherencia en todos los Estados miembros con respecto a la protección contra ataques cibernéticos, la UE aprobó esta directiva conocida como NIS, por sus siglas en inglés.

La NIS prácticamente no menciona detalles en lo que respecta a requisitos de seguridad. Hay un enfoque amplio en la protección de la infraestructura, que incluye los activos físicos y hace hincapié en la resiliencia (gestión de incidentes, gestión de la continuidad del negocio, etc.). Incluye una cláusula obligatoria de notificación de violaciones (véase el artículo 16), pero no hay multas prescritas para casos de incumplimiento.

Dado que la NIS es una directiva, debe ser transpuesta por un Estado miembro y ratificada por su asamblea legislativa. La NIS entró en vigor en agosto de 2016. Los Estados miembros tienen hasta el 10 de mayo de 2018 para incorporar la directiva a sus leyes nacionales y seis meses más para identificar a los operadores de los servicios esenciales.

Los beneficios de la seguridad de las impresoras

La seguridad de las impresoras, en contraposición a la seguridad de la impresión, se centra únicamente en los dispositivos físicos asociados con la impresión y es una disciplina de la seguridad de redes. La seguridad de las impresoras ve a la impresora como un periférico y la trata con el mismo cuidado que a cualquier otro periférico, como portátiles, servidores y dispositivos móviles. Aunque comparten un lenguaje común y tienen algunas áreas afectadas relacionadas, la seguridad de la impresión y la seguridad de las impresoras son disciplinas diferentes.

¿Cómo de vulnerables son las impresoras en red?

Las impresoras reciben volúmenes considerables de datos, algunos de los cuales son datos personales.
Pocos usuarios, expertos en el cumplimiento de las normas o administradores de TI tienen en cuenta la seguridad de dichos datos cuando se transmiten y almacenan en las impresoras. El artículo 5.f del RGDP exige «una seguridad adecuada de los datos personales, que incluye la protección contra el procesamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas». Sin embargo, son pocas las organizaciones que tienen en cuenta la seguridad de los datos en una impresora.

Además, es habitual ver los documentos impresos olvidados en las bandejas de papel de la impresora. Según el RGPD, las soluciones de impresión ascendente podrían convertirse en un componente esencial para salvaguardar la pérdida accidental de datos personales, en particular, para aquellas organizaciones cuyo tratamiento primario de datos personales implica la impression.

Las impresoras son un objetivo jugoso para los ciberdelincuentes, en parte porque no se consideran parte de la TI y, por lo tanto, no requieren mucha atención del personal de seguridad. La gestión de las impresoras se considera a menudo como parte de las funciones de la gestión de las instalaciones. Cuando las impresoras se convirtieron en dispositivos conectados en red, siempre y cuando los dispositivos estuvieran protegidos por el cortafuegos de la empresa, se consideraron en su mayor parte «de bajo riesgo». La vulnerabilidad de los periféricos de impresión permaneció como algo poco identificado.

Además, las máquinas combinadas con impresora/escáner/fax son cada vez más sofisticadas. Estos dispositivos tienen ordenadores generales instalados en su interior para controlar todo lo que hacen. Los sistemas Windows y Linux suelen estar integrados en muchas impresoras modernas. Debido a que los controladores de estos ordenadores tienen poca seguridad y no se presta demasiada atención a las revisiones, a menudo son vulnerables. Además, la funcionalidad requiere conectividad, lo que provoca que muchas impresoras se envíen con muchos puertos abiertos para mantener su funcionalidad.

La falta de atención que se conjuga con una alta potencia de procesamiento y un popurrí de opciones de conexión hace que los atacantes puedan acceder a las impresoras de varias maneras, p. ej., a través de un módem, un punto de acceso inalámbrico o accedan desde los escritorios infectados con *spyware* (programas espías). Después de acceder, los atacantes pueden usar esta potencia para atacar a otras máquinas en su red interna o participar en una denegación de servicio distribuido. La mayoría de las impresoras tienen acceso sin restricciones a una red interna. Un atacante que accede a una impresora puede escanear todo en busca de sistemas que se puedan aprovechar.

Al igual que otros dispositivos periféricos que requieren protección, las impresoras no solo son una «puerta de acceso», sino también un objetivo para los ciberdelincuentes. Las impresoras suelen almacenar documentos confidenciales en su cola de impresión. A menudo se combinan también con un escáner de documentos, y estos se almacenan en el archivo de escaneo durante mucho más tiempo de lo que la mayoría de la gente espera.

Consideraciones

Si su organización no ha prestado atención a la seguridad de las impresoras, IDC tiene algunas recomendaciones sobre por dónde empezar.

Todo comienza con la visibilidad

Como con cualquier periférico que requiera seguridad, comience con lo básico: el primer paso es siempre la visibilidad. Haga un inventario completo de todas las impresoras, en el que se incluya la marca, el modelo, las características y las configuraciones. La creación de esa lista puede ser problemática porque la iniciativa individual coloca a menudo a las impresoras en lugares no identificados (TI en la sombra). Los laboratorios, las oficinas ejecutivas o las oficinas de servicios de campo suelen colocar una impresora en la red por comodidad o la conectan directamente a un PC, independientemente de las implicaciones de seguridad.

Lo ideal sería un inventario de periféricos que incluyera a las impresoras y que derivara de un controlador de acceso a red (NAC, por sus siglas en inglés) o una herramienta de gestión de activos que detectara a los dispositivos como funcionalidad principal. Lograr una visibilidad realmente completa de las impresoras es extremadamente difícil sin un NAC. Por supuesto, algunos modelos de impresora pueden tener la función de autodetección cuando están conectadas a red. Si su entorno de red no tiene la suerte de incluir una base instalada homogénea de este tipo de impresoras, un NAC es la solución.

Proteja sus impresoras periféricas

Las impresoras dentro de una organización se deben gestionar como cualquier otro periférico conectado. Desactive todos los servicios innecesarios que ofrece la impresora, como un protocolo de transferencia de archivos (FTP, por sus siglas en inglés). La mayoría de las organizaciones no necesitan acceso FTP a sus impresoras y, a menudo, puede causar más perjuicios que beneficios. Por ejemplo, algunas impresoras permiten a un atacante realizar solicitudes de FTP y eliminar trabajos de una cola de impresión de forma anónima. Además, muchos servicios FTP en impresoras modernas están sujetos a ataques de rebote FTP. Con una herramienta como Nmap (cartógrafo de redes), un atacante puede ocultar el origen de un escaneo de puertos, convenciendo así a un servidor FTP compatible para que permita conexiones FTP *proxy*. Si bien dichos escaneos de rebote FTP son viejas técnicas, una cantidad importante de servidores de impresión completamente nuevos es susceptible a estos ataques.

Sin embargo, la actividad más importante en la protección de periféricos de impresión es la gestión de contraseñas.
El error más atroz cometido por las organizaciones es no cambiar las contraseñas predeterminadas. De acuerdo con el *Informe 2016 de Investigación de Violaciones de Datos* de Verizon, el 63 % de las violaciones de datos confirmadas implicaban el uso de contraseñas débiles, predeterminadas o robadas. Si las impresoras se gestionan a través de instalaciones o de proveedores, la comodidad es primordial (para ellos). Cuando un dispositivo necesita mantenimiento, encontrar una contraseña puede ser un problema. Cuando hay una impresora por cada 10 empleados, una organización con 10 000 empleados puede tener que mantener 1000 contraseñas. La seguridad, por lo tanto, da paso a la comodidad. La gestión de contraseñas no es solo un fallo del personal no técnico. El segundo error más flagrante que se comete es tener el nombre de usuario y la contraseña con libre acceso en texto sin cifrar, disponible para cualquier persona con una conexión http://.

Mantenimiento y revisiones

La mayoría de las violaciones se dan por una falta de higiene. De acuerdo con el *Informe de 2016 de Investigación de Violaciones de Datos* de Verizon, las 10 vulnerabilidades atacadas en 2015 representaron el 85 % del tráfico que se vulneró con éxito. Las vulnerabilidades más atacadas son conocidas y divulgadas públicamente. Los ciberdelincuentes usarán lo que funciona y maximizarán la inversión que han realizado en sus herramientas de *malware* (programas maliciosos).

El mantenimiento y las revisiones de las periféricas de impresión harán de usted un objetivo más difícil y empujarán a los ciberdelincuentes a utilizar sus herramientas en organizaciones que no han hecho un mantenimiento de sus sistemas.

En lo que respecta a revisiones, no todas las impresoras son iguales. Algunos fabricantes ofrecen conjuntos de herramientas de gestión que le permiten supervisar, gestionar y revisar algunas marcas y modelos de impresoras. Estos conjuntos de herramientas son extremadamente valiosos porque el escáner de vulnerabilidades de una empresa probablemente tendrá problemas con las impresoras debido al servidor web incorporado. Si, por casualidad, usted tiene estas impresoras con herramientas de gestión sólidas, tiene suerte. Si no es así, es posible que tenga que revisar manualmente cada impresora, ya que quizás sea difícil improvisar una solución automatizada.

Además, para evitar el «ruido» de la importación a las herramientas SIEM, las organizaciones a menudo configuran los detectores de vulnerabilidades para que ignoren a las impresoras. Esto supone un problema tanto con SIEM y las herramientas de gestión de vulnerabilidad como con las impresoras. Quizás sea complicado configurar estas herramientas para que acepten solo ciertos mensajes de las impresoras, pero a corto plazo, este esfuerzo ayudará a proteger la red de infecciones transmitidas por las impresoras.

Conexión segura

Reduzca los protocolos de gestión utilizados para la impresora. La mayoría de las impresoras modernas admiten algún tipo de gestión a través de HTTP y/o HTTPS, y algunas incluso admiten Telnet o Secure Shell (SSH, por sus siglas en inglés). Elija cuidadosamente un protocolo de gestión que proporcione cifrado, como HTTPS o SSH, e inhabilite cifrados débiles o inservibles como SSLv3.

Por último, asegúrese de que las impresoras no tengan acceso abierto al resto de su red interna. La segmentación de redes empresariales es una práctica recomendada de seguridad de redes y las impresoras deben incluirse en la iniciativa. Se pueden utilizar certificados para segmentar de forma lógica el acceso a los recursos de la red y para cifrar el tráfico. Sin embargo, tenga en cuenta que estas medidas de seguridad adicionales pueden perjudicar la funcionalidad de la impresora, como la restricción del acceso a los servicios de directorio (por ejemplo, Active Directory) y la gestión y la supervisión basadas en la nube. Lograr el equilibrio entre asegurar bien las impresoras y preservar la funcionalidad del negocio es siempre una cuestión de criterio y evaluación del riesgo empresarial.

Conclusión

Las impresoras no han recibido la atención dada a otros vectores de amenazas a la seguridad cibernética. La vulnerabilidad y su correspondiente amenaza son muy reales. Las organizaciones, sin importar su tamaño, deben tomar medidas para abordar el problema y hacerlo con rapidez. Los ciberdelincuentes son imitadores voraces. Una vez que un actor malintencionado ha aprovechado un vector de amenaza para ganar, otros lo siguen rápidamente.

Las consecuencias financieras y aquellas que afectan a la reputación producidas por ignorar la seguridad de las impresoras están a punto de subir al nivel directivo con el RGPD. Sería desafortunado ver a una organización que cumple, que ha trabajado duro en sus procesos y tecnologías de seguridad de la información, fallar por un punto ciego: la impresora.

A C E R C A D E E S T A P U B L I C A C I Ó N

IDC Custom Solutions produjo esta publicación. La opinión, el análisis y los resultados de la investigación presentados aquí se extraen de investigaciones y análisis más detallados realizados y publicados por IDC independientemente, a menos que se especifique el patrocinio específico de los proveedores. IDC Custom Solutions pone a disposición el contenido de IDC en una

amplia variedad de formatos para su distribución por diversas empresas. La licencia para distribuir contenido de IDC no implica la aprobación de o la opinión sobre el titular de la licencia.

Más información sobre IDC en www.idc.com. Más información sobre IDC Custom Solutions en http://www.idc.com/prodserv/custom_solutions/index.jsp.

Sede central: 5 Speen Street Framingham, MA 01701 EE. UU. P.508.872.8200 F.508.935.4015 www.idc.com