NOTICIAS DESTACADAS DEL MERCADO DE IDC

La seguridad de la infraestructura de impresión es esencial para la transformación digital

Diciembre de 2016

Por Robert Palmer, director de investigación de IDC, soluciones de creación de imágenes, impresión y documentos

Con el patrocinio de HP Inc.

Un plan de seguridad de TI en cualquier organización es una prioridad evidente para garantizar una protección y respuesta adecuadas ante potenciales amenazas y brechas. La seguridad de la impresión debe formar parte de este plan, especialmente en la era de la informática de tercera plataforma (movilidad, nube, macrodatos y redes sociales). Por lo tanto, cualquier plan integral que permita abordar la seguridad del entorno de impresión de la organización, debe incluir soluciones y servicios que se encarguen de la seguridad de los datos y de los dispositivos. Este estudio analiza la importancia de la protección de la infraestructura de impresión y de los documentos, y el papel que los servicios gestionados de impresión desempeñan en la consecución de este objetivo.

Introducción

Los problemas relacionados con la seguridad y la privacidad de los datos llevan más de una década ocupando los primeros puestos en la lista de los directores de informática y directores de TI. La propia investigación de IDC muestra que la seguridad se ha convertido ahora en una prioridad para la mayoría de las empresas, solo ligeramente por debajo de otra iniciativa empresarial clave: la transformación digital. Si bien ambos pueden considerarse factores diferenciadores empresariales esenciales, es importante comprender cómo la transformación digital y la seguridad están íntimamente relacionadas.

Las organizaciones hacen frente a una amplia gama de amenazas en lo que respecta a la seguridad de su infraestructura de TI. Una gran parte de las organizaciones con conocimientos informáticos ha priorizado la seguridad centrándose en problemas como la protección de la red frente a los ataques externos, la seguridad de los dispositivos de la red, la gestión del acceso a dispositivos conectados y la prevención de la divulgación de información confidencial.

A primera vista, resulta fácil ver cómo todos estos problemas giran en torno a la necesidad de proteger los activos más importantes de la organización: la información empresarial y los datos de los clientes. Las empresas invierten miles de millones de dólares en la gestión de documentos y software de gestión de contenido empresarial (ECM), lo que supone realizar importantes inversiones en sistemas para obtener el control del contenido esencial para la empresa. A este complicado reto se suma una creciente tendencia hacia la movilidad y la informática en la nube. Los denominados «trabajadores del conocimiento» de hoy en día exigen un acceso ininterrumpido a la información, lo que significa que el contenido debe poder moverse libremente desde el interior al exterior del cortafuegos corporativo.

US41987416

Curiosamente, la infraestructura de impresión y documentos de una organización se posiciona de manera exclusiva justo en la intersección entre la transformación digital y la seguridad de TI. Sin embargo, una gran parte de las empresas no puede reconocer las vulnerabilidades de seguridad asociadas a su entorno actual de impresión y de documentos. En el trasfondo de todo este asunto se encuentra el papel que desempeña la impresora multifunción inteligente, que se ha convertido en un centro de procesamiento empresarial inteligente utilizado como rampa de acceso a la información empresarial, tanto si se almacena en el dispositivo y en la red corporativa, como si se almacena en papel o en la nube.

Una amenaza desconocida y sin gestionar

La impresora multifunción conectada supone un riesgo de seguridad potencial como un dispositivo conectado sin gestionar. No obstante, la impresora multifunción también se puede utilizar como un activo de primera línea para la protección del acceso a la red, la gestión de la seguridad de los datos y la protección del acceso a la información.

Según la investigación llevada a cabo por IDC *«User Perspectives on Print Security» (Perspectivas del usuario sobre la seguridad de impresión)* en 2015, más del 30 % de las organizaciones no ha implementado políticas de seguridad para gestionar el acceso y controlar los derechos de uso de las impresoras e impresoras multifunción que se encuentren en la red. Al mismo tiempo, más de la mitad de los encuestados muestra un alto grado de preocupación en lo que respecta al uso no autorizado de fotocopiadoras o impresoras multifunción.

Existen inconsistencias similares en lo que respecta al modo en que los negocios perciben sus prácticas de seguridad de TI actuales. Según el *estudio de referencia de MaturityScape: La seguridad de la impresión en los Estados Unidos (2016)* de IDC, más del 70 % de los encuestados indica que la seguridad de la impresión ejerce un alto nivel de influencia en la compra o alquiler de impresoras e impresoras multifunción. Curiosamente, sin embargo, el porcentaje de encuestados que indicó que la seguridad de la impresión era «muy importante» fue del 26 % o inferior con respecto a aquellos que mostraron preocupación por la seguridad de TI en general.

Un gran número de directores de seguridad y de TI han asumido que los sistemas que se utilizan para proteger la red se ampliarían a otros periféricos conectados. Sin embargo, la seguridad en torno al perímetro de la red se desmorona y cada dispositivo conectado a la red es ahora un riesgo de seguridad de punto final: impresoras e impresoras multifunción incluidas.

La amenaza es real, con posibles brechas de seguridad que se producen mediante ataques maliciosos que utilizan una impresora conectada a la red o una impresora multifunción como punto de entrada, o simplemente debido a un uso negligente de los dispositivos por parte de los empleados. Teniendo en cuenta que el entorno de impresión es único debido a que gestiona específicamente datos, documentos e información, tanto en formato digital como impreso, el contenido crítico de la empresa queda expuesto y resulta vulnerable de muy diversas maneras. Si no se protege el entorno de impresión como parte de una estrategia de TI global, la organización puede permanecer en una situación de vulnerabilidad parecida a la no adopción de medidas de seguridad en torno a la TI.

El resultado final de una brecha de seguridad en la infraestructura de impresión y documentos es el mismo que el de cualquier otro fallo de seguridad: altos costes relacionados con el tiempo de inactividad para identificar y reparar una brecha de seguridad, sanciones asociadas con el cumplimiento normativo y gubernamental, pérdida de clientes y otros daños a la reputación de la empresa.

Servicios de impresión segura

Los retos relacionados con la seguridad de la impresión y documentos son fácilmente identificables. Sin embargo, se ha comprobado que el desarrollo de una estrategia de impresión segura puede resultar difícil para muchas empresas. Uno de los problemas hace referencia a las distintas partes interesadas de la organización. La seguridad de los dispositivos tiende a englobarse en el área de TI y suele incluir el departamento de TI, el director de seguridad, el departamento de asistencia técnica, la seguridad de punto final y la seguridad de la red. Además, cualquier debate relacionado con la seguridad de las impresoras e impresoras multifunción involucra a menudo la gestión de los centros.

Por otro lado, la seguridad del contenido se considera frecuentemente relacionada con los problemas en torno al cumplimiento normativo y las partes interesadas tienden a percibirla como parte del área de riesgo y gobernanza corporativa. También pueden participar los representantes de aplicaciones ERP, de clústeres de bases de datos, de gestión del contenido y otros directores de líneas de negocio (LOB, por sus siglas en inglés). Generalmente, la seguridad del contenido y de las impresoras se gestiona por separado, lo que lleva a una falta de integración y a una mayor situación de vulnerabilidad. Al mismo tiempo, las empresas desconocen a menudo las distintas soluciones de impresión segura y servicios profesionales que se encuentran disponibles en el mercado.

Esta es un área en la que los servicios gestionados de impresión (MPS, por sus siglas en inglés) pueden desempeñar un papel importante en el desarrollo de la seguridad de la impresión y de los documentos. Si bien un gran número de empresas han contratado ya a un proveedor de servicios gestionados de impresión (MPS) para optimizar su infraestructura de impresión, lograr procesos más eficientes y reducir los costes de producción, la seguridad de la impresión y el contenido han sido en gran medida desatendidos en la mayoría de los acuerdos contractuales de servicios de impresión. Hoy en día, algunos proveedores de MPS cuentan con la capacidad, las herramientas y los recursos necesarios para permitir que las empresas puedan identificar y priorizar las amenazas actuales a la seguridad. Parte de este proceso podría incluir una evaluación de la seguridad inicial, algo esencial en la identificación de las carencias de la infraestructura actual de contenido y dispositivos. Posteriormente, las empresas podrían colaborar con el proveedor de servicios para desarrollar e implementar servicios gestionados de impresión segura que aborden las vulnerabilidades actuales, refuercen la infraestructura de los documentos y mitiguen los riesgos de seguridad futuros.

El proveedor de MPS también puede reunir a las partes interesadas para ofrecer servicios de impresión contractuales en los departamentos y líneas de negocio, lo que resulta esencial para implementar un enfoque integral en la seguridad del contenido y de los dispositivos. Este enfoque también beneficia al desarrollo de un plan de seguridad que abarque la estrategia de transformación digital propia de la organización. Los servicios de impresión segura pueden abordar desde la seguridad básica para proteger el equipo y los datos, hasta medidas más avanzadas que son significativamente más complejas en lo que respecta a su implementación y permiten ofrecer un nivel superior de seguridad para los dispositivos y una protección del contenido.

Conclusión: De reactivo a proactivo

La conclusión es que la infraestructura de impresión y de documentos no ha recibido el nivel de atención que se ha otorgado a otras amenazas de la red y a la ciberseguridad. Las brechas generan miedo e inseguridad y el impacto en los costes operativos, rendimiento y reputación de la empresa puede ser enorme.

Las organizaciones deben adoptar medidas proactivas para abordar las preocupaciones en torno a la seguridad de la infraestructura de impresión y de los documentos, y se debe considerar al proveedor de MPS como a un socio importante en esta tarea. Cuando busque proveedores de servicios de impresión, tenga en cuenta a aquellos que puedan demostrar competencias básicas en la evaluación de los niveles de amenazas y en sus capacidades de reparación.

Asimismo, elija a socios con hardware y soluciones integradas en torno a un ecosistema de seguridad con el fin de abordar las siguientes vulnerabilidades en la infraestructura de documentos:

- Autenticación y autorización de usuarios
- Gestión de dispositivos
- Protección frente al malware de los dispositivos
- Actualizaciones de firmware y gestión de contraseñas
- Seguridad del contenido, privacidad e integridad de los datos
- Capacidades para abordar el factor humano involucrado en la instalación, configuración y uso del equipo

Las soluciones de MPS también se deben diseñar de forma que se integren con la gestión de documentos de terceros y sistemas ECM para que ofrezcan una mayor protección y faciliten los requisitos de gobernanza y cumplimiento normativo.

Mediante la adopción de un enfoque integral, las empresas pueden empezar a contener las vulnerabilidades y reforzar la protección en los entornos de impresión y de documentos, que son probablemente los eslabones de seguridad más débiles de su organización.

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