brother
at your side

Informe de Seguridad Brother

Septiembre 2016

LAS AMENAZAS OCULTAS QUE PLANTEA TU EQUIPO DE IMPRESIÓN

(Y LO QUE PUEDE HACERSE AL RESPECTO)

El parque instalado de impresoras y escáneres de las empresas de todo tipo disponen de una versatilidad y potencia crecientes. Pero todos estos avances vienen acompañados de mayores riesgos para la seguridad y son pocas las organizaciones que toman suficientes medidas para protegerse.

Las medidas de seguridad en el trabajo constituyen una parte habitual de nuestra vida cotidiana. Para proteger los activos, las organizaciones utilizan de forma rutinaria elementos que van desde las tarjetas o claves de identificación, hasta el control de acceso físico, desde el uso de software de seguridad de la red hasta la protección del acceso a la información. Incluso la idea de tener una cuenta de correo electrónico sin contraseña nos parece completamente temeraria.

La forma en la que equipos informáticos, tales como impresoras y escáneres, se conectan a redes teóricamente seguras también ha de ser tenida en cuenta para evitar puntos débiles de seguridad en las organizaciones.

En 2015 Brother realizó un estudio[1] sobre los desafíos a los que se enfrentan las empresas, en el que participaron más de 2.500 pymes. El 75% indicó que consideraban que la seguridad de la información constituía un elemento muy importante para su organización, mientras que el 59% convino en que la seguridad de la información afecta a las decisiones sobre la gestión de documentos e impresión.

Estas preocupaciones están cobrando relevancia como respuesta a un creciente número de problemas relacionados con la seguridad en todos los sectores de actividad. Un estudio de Quocirca[2] sobre una muestra de 200 empresas que también se llevó a cabo en 2015 reveló que, por primera vez, la seguridad está entre las máximas prioridades, con un 75% de respuestas que indicaban que era un factor importante o muy importante (con una puntuación media de 4,01 sobre 5). En términos globales, el 74% de las organizaciones ya ha puesto en marcha o tiene planificado implantar soluciones de impresión segura.

¿En qué consisten exactamente las amenazas?

Básicamente, hay cuatro formas en las que los equipos de impresión o escáneres en red pueden representar una amenaza para una organización.

1. **MEDIANTE LA FILTRACIÓN ACCIDENTAL DE INFORMACIÓN CONFIDENCIAL IMPRESA**
2. **MEDIANTE LA FILTRACIÓN ACCIDENTAL DE INFORMACIÓN CONFIDENCIAL ESCANEADA**
3. **AL PERMITIR QUE SE PRODUZCAN INTRUSIONES EN LA RED A TRAVÉS DE UN NIVEL DE SEGURIDAD REDUCIDO**
4. **AL PERMITIR EL ACCESO FÍSICO DE USUARIOS NO AUTORIZADOS A DISPOSITIVOS NO VIGILADOS**

Para ayudar a las organizaciones a eliminar estas amenazas comunes para la seguridad, Brother ha elaborado un resumen de los riesgos específicos que los administradores deberían tener en cuenta, así como el tipo de tecnología que se ha desarrollado expresamente y que puede integrarse con la seguridad existente, a fin de mejorar el nivel de protección.

1. FILTRACIÓN ACCIDENTAL DE INFORMACIÓN CONFIDENCIAL IMPRESA

¿Cuáles son los peligros?

Independientemente del nivel de eficacia de la política de seguridad de su organización, si alguien puede ir a una impresora, coger páginas que no se hayan recogido e irse con ellas, sus datos están en peligro.

El puesto de trabajo de la mayoría de personas no está justo delante de la impresora que utilizan, de modo que siempre existe el riesgo de que los trabajos de impresión no recogidos, que potencialmente pueden contener información sensible, queden expuestos a cualquiera que pase por delante.

¿Qué pueden hacer las organizaciones al respecto?

La mejor forma de combatir eficazmente este riesgo es realizar la impresión cuando el usuario autorizado llegue a la máquina, y el modo ideal de hacerlo es por medio de un código PIN o un lector de tarjetas de seguridad. En función del tamaño de la organización y de sus requisitos, Brother recomienda distintas soluciones. La primera es la **Impresión segura**, una funcionalidad diseñada principalmente para personas que imprimen documentos confidenciales de forma ocasional. La Impresión segura permite a los usuarios iniciar el proceso efectivo de impresión cuando estén físicamente delante del equipo. Por lo tanto, si es necesario imprimir algún documento confidencial, solo hay que asignar un código PIN a la tarea en el controlador de impresión al enviarla al dispositivo. Pero si se imprimen documentos confidenciales a menudo, la identificación por **Active Directory** resultará más efectiva. Esta funcionalidad restringe completamente el acceso físico a cualquier función del equipo, fundamentalmente mediante el bloqueo de toda persona no autorizada. Para desbloquear el equipo de impresión y recuperar el documento, los usuarios deben autenticarse previamente por medio del nombre de usuario y contraseña de Active Directory de Windows® ya creados. En este caso y en el de Impresión segura, la tarea se almacena en la memoria interna del equipo de impresión hasta que se recoge.

Para implementar la funcionalidad Active Directory, la organización debe estar utilizando ya Active Directory de Microsoft®. No obstante, en el caso de las organizaciones que no lo hagan, existen soluciones como la Impresión segura con servidores de bases de datos de usuarios, compatibles con LDAP. Esta opción funciona de la misma forma que Active Directory, pero se comunica con un servidor mediante el protocolo LDAP habilitado.

Para añadir un nivel de seguridad adicional con las funciones de Active Directory o LDAP, los administradores pueden especificar un límite de tiempo durante el que las tareas de impresión no recogidas se conservan en la memoria de los dispositivos. De este modo, los documentos confidenciales no permanecen indefinidamente en la máquina.

En el caso de entornos en los que las necesidades de impresión de información confidencial varían en función de los usuarios, resultará más adecuado una **configuración basada en red**, una solución que almacene los documentos en un servidor central en lugar de en los dispositivos. Esto permite recoger los documentos en cualquier equipo de impresión del edificio que esté conectado al servidor a través de un código PIN o, cuando sea compatible, mediante la autenticación con tarjetas NFC. Además, los administradores pueden monitorizar más de cerca la utilización de los equipos por parte de los usuarios.

Aun en el caso de que se apliquen estas medidas, sigue existiendo un punto débil: con el software adecuado, es posible interceptar los datos durante su transmisión al equipo. Para protegerse de ello, Brother recomienda el **cifrado de TLS (Transport Layer Security) y de SSL (Secure Socket Layer):** la misma tecnología que se utiliza en el comercio electrónico para proteger los datos bancarios y de tarjetas de crédito. De este modo, los archivos más confidenciales se pueden cifrar con claves de hasta 256 bits durante su transmisión a través de la red.

2. FILTRACIÓN ACCIDENTAL DE INFORMACIÓN CONFIDENCIAL ESCANEADA

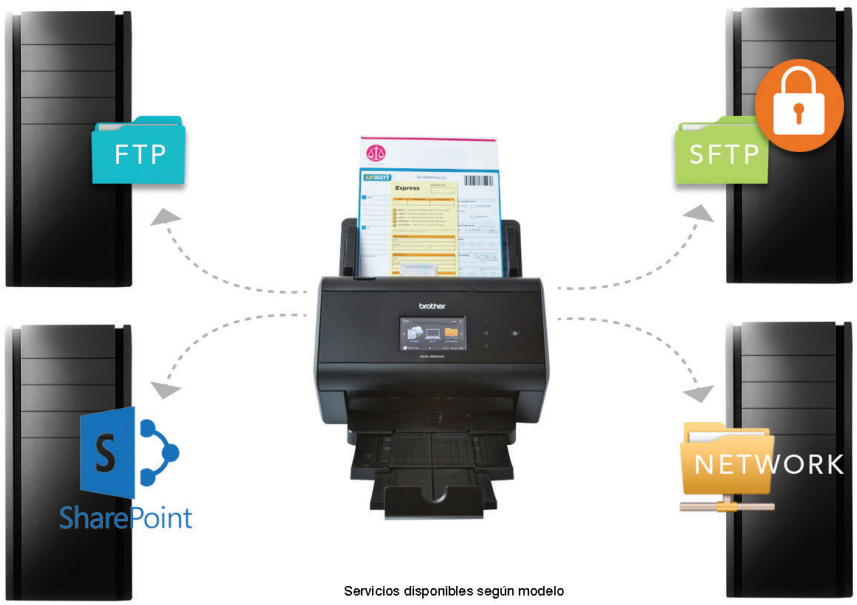
¿Cuáles son los peligros?

Aunque tu equipo de impresión o escaneado sea seguro, existe otro riesgo de filtración potencial no muy extraño: a través de los documentos escaneados. Después de escanear un documento confidencial, los usuarios disponen de diversas opciones para almacenarlo o compartirlo. Compartir documentos escaneados por correo electrónico o cargarlos a la web son estrategias que entrañan un alto riesgo para la información sensible, ya que los documentos pueden caer muy rápidamente en manos no deseadas si se comete un error relativamente pequeño. Y lo que es peor, no hay límite respecto a la cantidad de copias que se pueden realizar.

¿Qué pueden hacer las organizaciones al respecto?

La solución más sencilla pasa por convertir el documento escaneado en un **PDF Seguro** protegido con un código PIN, de modo que nadie pueda abrirlo sin su permiso.

Alternativamente, pueden utilizar la función **escanear a SFTP (Secure File Transfer Protocol)**. El protocolo seguro de transferencia de archivos establece un flujo de datos privado y seguro. Mediante un control de acceso a los servidores SFTP más estricto, las organizaciones pueden contribuir a mantener toda su red aún más segura mediante el cierre completo de una puerta de entrada y salida de su sistema.



Servicios disponibles según modelo

3. POSIBLES INTRUSIONES EN LA RED A TRAVÉS DE UN NIVEL DE SEGURIDAD REDUCIDO

¿Cuáles son los peligros?

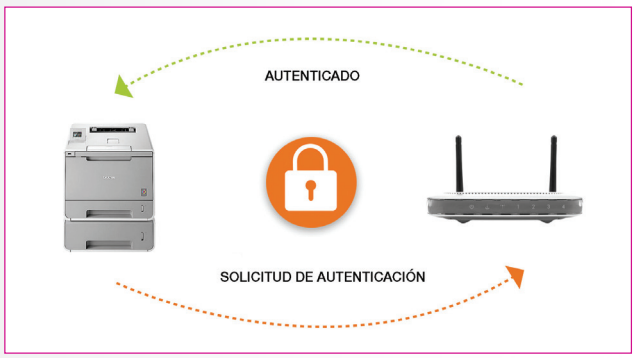
La exigencia de proporcionar certificados, nombres de usuario y contraseñas para conectar tabletas y portátiles a una red segura constituye una práctica estándar. Pero normalmente no se espera que sea necesario hacer lo mismo con los equipo de impresión o escaneado, a pesar de que su punto de conectividad puede representar el mismo nivel de amenaza para la seguridad que el conjunto de la red.

¿Qué pueden hacer las organizaciones al respecto?

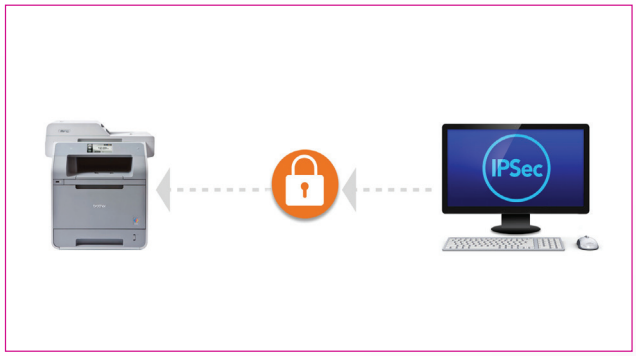
Amenazas externas

Como sus dispositivos cuentan con diversos tipos de cifrado integrado, Brother puede sugerir varias formas de mejorar la seguridad y cubrir posibles fugas.

802.1x: es un estándar IEEE para un acceso de red autenticado a redes Ethernet por cable y redes 802.11 inalámbricas. IEEE 802.1X mejora la seguridad y la implementación al proporcionar la compatibilidad con la identificación de usuarios, la autenticación, la administración de claves dinámicas y la creación de cuentas de manera centralizada. Se usa con los dispositivos que ya están conectados por medio de un cable o formen parte de la infraestructura inalámbrica de la organización.



IPsec: Internet Protocol security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado. Permite conectar varios dispositivos directamente a entornos seguros internos o externos a través de IPsec, lo que permite ahorrar tiempo y dinero. Como los equipos Brother llevan IPsec integrado, no hay necesidad de instalar software intermedio o hardware de terceros para conectar los dos extremos.



SNMPv3: es un protocolo de la capa de aplicación que facilita el intercambio de información de gestión entre dispositivos de red. Este protocolo es parte del conjunto de protocolos TCP/IP y permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas.

Los dispositivos Brother, que están diseñados para cumplir políticas de seguridad de red estrictas, son capaces de interpretar todas las instrucciones que reciben en las versiones 1, 2 y 3 (MD5 y SHA1) de SNMP cifrado, incluso durante la configuración remota y el mantenimiento rutinario.

Las organizaciones que utilicen su propia herramienta de gestión del parque de impresoras para la gestión centralizada de sus dispositivos, también deben implementar medidas de seguridad para prevenir un acceso no autorizado a la herramienta.

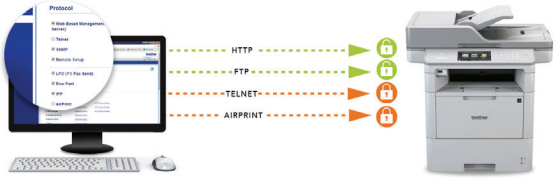
Amenazas internas

Si bien el cifrado ofrece protección contra las amenazas externas, si el personal interno puede acceder remotamente a equipos conectados a la red, ésta puede ser vulnerable. Para evitar cualquier problema derivado de ello, los equipos de impresión o escaneado con **servidores Web integrados, deben tener protección por contraseña**, que dejarán de estar disponibles tras un periodo de inactividad de cinco minutos.

También es recomendable la función de **bloqueo de IP**, que impide el acceso al dispositivo a través de la red. En este ejemplo, la impresora solo aceptará conexiones de usuarios de las direcciones IP siguientes: 10.45.12.1, 12.45.12.45, 10.45.12.46 y 10.45.12.47

Si se desea una solución menos restrictiva, el **Control de protocolos** permite a los administradores deshabilitar protocolos que no sean necesarios, sin bloquear por completo el acceso a todos los elementos, como el FTP o el SMTP.

Con el Control de protocolos los administradores pueden deshabilitar protocolos que no sean necesarios sin bloquear por completo el acceso a todos los elementos, como el FTP o el SMTP. En el ejemplo siguiente se muestra cómo el administrador del sistema ha deshabilitado las funciones siguientes: Telnet, AirPrint, Proxy y el servidor FTP.



4. ACCESO FÍSICO NO AUTORIZADO A DISPOSITIVOS SIN VIGILANCIA

¿Cuáles son los peligros?

A pesar de contar con todas estas funciones de seguridad, a menos que los equipos de impresión o escaneado estén protegidos físicamente en salas seguras, las personas pueden acercarse a ellas e intentar extraer información de las mismas. En el caso de pequeñas y medianas empresas con escasa o ninguna infraestructura informática, resulta especialmente importante disponer de algún tipo de seguridad física.

En el estudio realizado por Brother en 2015, dos terceras partes de los responsables de la toma de decisiones indicaron que la seguridad afecta a las decisiones sobre la gestión de documentos e impresión y que, entre las cuestiones que les preocupan, se encuentra el modo en el que se conservan los documentos en el equipo de impresión.

¿Qué pueden hacer las organizaciones al respecto?

Para este tipo de organizaciones, recomendamos funciones de seguridad que evitan que personas no autorizadas puedan manipular los equipos.

Bloqueo de configuración: restringe el acceso a la configuración del dispositivo a través del panel de control. Es ideal para organizaciones que no deseen limitar la forma en la que las personas utilizan las funciones, pero que quieran impedir que los usuarios no autorizados puedan modificar ninguna configuración.

Bloqueo Seguro de Funciones va un paso más allá, ya que impide el acceso tanto a la configuración del dispositivo como a determinadas funciones. Esto permite a los administradores decidir quién puede hacer qué con cada máquina. Por ejemplo, controlando qué usuarios pueden enviar faxes y escanear documentos, o implantando límites mensuales a través de códigos PIN o tarjetas de acceso NFC únicas.

La captura de pantalla que se incluye a continuación corresponde a la página de configuración de Bloqueo Seguro de Funciones desde el servidor Web integrado del dispositivo. Muestra que todas las funciones están bloqueadas para los usuarios no autorizados, lo que aparece en la primera fila, llamado Modo público. El Usuario 1, tal como se muestra en la primera fila, tiene acceso no restringido a todas las funciones.

	LISTA DE USUARIOS / FUNCIONES RESTRINGIDAS	FUNCIONES					LÍMITES DE PÁGINAS (*)		
		IMPRIMIR	COPIA	ESCANEAR	FAX		ACTIVADO	PÁGINAS MÁX.	IMPRESIÓN A COLOR
					Enviar	Recibir			
	Modo público	✓	✓	✓	✓	✓	☐	0	✓
1	Usuario 1	✓	✓	✓	✓	✓	☐	0	✓
2	Usuario 2	✓	✓	✓	☐	☐	✓	100	✓
3									

El Usuario 2, tal como se muestra en la segunda fila, no puede enviar ni recibir faxes y tiene un límite de impresión de 100 páginas. Este límite puede ser ajustado y reiniciado por un administrador o configurarse para que se reinicie de forma periódica.

En el caso de organizaciones en las que varios usuarios comparten equipos de impresión o escaneado, o bien es necesario colocarlas en lugares públicos, puede resultar difícil establecer un control del uso abusivo sin obstaculizar el uso normal. Sin embargo, con las opciones de Active Directory o de autenticación LDAP, el personal puede utilizar de forma sencilla sus credenciales de inicio de sesión ya existentes para obtener acceso a los equipos sobre la marcha.

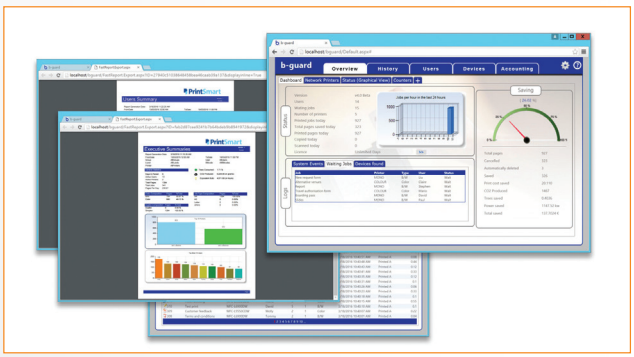
Recomendaciones

No cabe duda de que hay muchas organizaciones de todos los sectores que deben tomarse en serio las amenazas para la seguridad de datos y redes que plantean los equipos de impresión y escáneres, pero no existe una solución única. Los administradores de sistemas tienen que seleccionar las soluciones adecuadas para las características particulares de sus riesgos, infraestructuras y seguridad existentes.

En resumen, una organización debe asegurarse de:

1. **Garantizar la seguridad de sus dispositivos**
2. **Proteger los datos en tránsito y tras la impresión**
3. **Proteger su red de los intrusos**

Una vez hecho esto, podrá confiar en que sus sistemas de impresión y escaneado contarán con una protección adecuada frente a las amenazas para la seguridad en el futuro próximo.



[1]Fuente: estudio sobre pymes para Brother realizado por B2B International entre 2502 empresas de Reino Unido, Francia, Alemania y Estados Unidos

[2]Fuente: Quocirca Managed Print Services Landscape (Panorama de los servicios de impresión gestionada de Quocirca), 2015. Encuesta a 200 organizaciones con 1000 empleados o más de Reino Unido, Francia, Alemania y Estados Unidos