Folleto

Ayude a sus clientes a imprimir de una forma más segura

Muchas empresas han implementado una estrategia de seguridad para su red y puntos finales, que incluye una rigurosa política de seguridad en los ordenadores. Sin embargo, la mayoría de las estrategias de seguridad informática no contemplan los dispositivos de imagen e impresión. Si no se protegen como es debido, las impresoras y equipos multifunción pueden suponer un riesgo de seguridad para la red. Las empresas tienen que integrar las necesidades de protección de su entorno de imagen e impresión en su estrategia de seguridad de IT más amplia.

Las impresoras y equipos multifunción HP LaserJet disponen de aproximadamente 200 funciones de seguridad que sus clientes pueden usar para proteger sus datos y dispositivos. Gracias a la tecnología moderna, se puede alcanzar un equilibrio entre la usabilidad y la seguridad. Como cada empresa es única, las impresoras y equipos multifunción de HP vienen preparadas de fábrica para responder a las necesidades de una amplia variedad de usuarios. Sin embargo, debido al gran número de ajustes posibles, puede parecer una tarea de gran envergadura.

El propósito de esta guía es ayudarle a comprender algunos de los ajustes básicos de los dispositivos que todas las empresas, independientemente de su tamaño o sector, deberían implementar para proteger los dispositivos de imagen e impresión en red. Al explicar para qué sirve cada ajuste y el riesgo que supone dejarlo desprotegido, puede ayudar a su cliente a poner en marcha una estrategia de seguridad para su entorno de imagen e impresión.

Ajustes recomendados de los dispositivos para una flota de impresión HP

Los clientes necesitan su ayuda para conocer qué ajustes de seguridad deben tener en cuenta a la hora de proteger sus datos. Hemos seleccionado estos ajustes entre las más de 200 configuraciones que permiten los dispositivos. Se trata de ajustes de seguridad básicos que todas las empresas, independientemente de su tamaño o sector, deberían implementar. HP recomienda aplicar estos ajustes de seguridad mínimos para evitar los problemas de seguridad más comunes.

Es importante tener en cuenta que el entorno de cada cliente es único. Cada cliente debe buscar un equilibrio entre la seguridad y la productividad de los usuarios finales. Configurar un equipo multifunción para usarlo en una red puede requerir algunos ajustes en esta configuración. Su cliente debe valorar las configuraciones adecuadas para su entorno de red.

Riesgos potenciales de no proteger un dispositivo

- Pérdida de productividad de los empleados porque los ajustes del dispositivo han cambiado y ya no es posible imprimir, copiar, escanear o usar el fax
- Acceso no autorizado a datos confidenciales
- Exposición potencial de los ajustes del dispositivo, incluidas las credenciales
- Más llamadas al soporte técnico que consumen un valioso tiempo del personal de IT

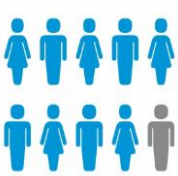
Recomendaciones a su cliente antes de empezar

- Actualizar el dispositivo con la última versión del firmware para asegurar que tiene las capacidades más recientes.
- Verificar que la impresora o equipo multifunción está detrás de su cortafuegos para mantenerlo protegido. Algunas soluciones de HP requieren que el dispositivo tenga acceso a Internet para funcionar adecuadamente.

Para evitar el riesgo de...	Ajuste de seguridad	Acción	Propósito del ajuste
Cualquiera puede cambiar los ajustes o botones del dispositivo en el panel de control (por ejemplo para deshabilitar funciones del producto)	Contraseña de administrador para el HP Embedded Web Server (EWS)	Configurar una contraseña	Controla el acceso a los parámetros de configuración del HP EWS.
Cualquiera puede cambiar los ajustes del panel de control	Contraseña del Lenguaje de Trabajo de la Impresora (PJL)	Configurar una contraseña	Los comandos PJL proporcionan una comunicación bidireccional con la impresora y se pueden usar para cambiar los ajustes del panel de control.
Cualquiera puede cambiar los ajustes de la impresora si está habilitada la "escritura" en SNMPv1/v2	SNMPv1/v2 Protocolo Simple de Administración de Red	Configurar como "Solo lectura"	Estos ajustes ofrecen compatibilidad con herramientas de gestión antiguas que se basan en SNMPv1/v2 para detectar los dispositivos y verificar su estado.
Cualquiera puede detectar un dispositivo de la red y cambiar sus ajustes si se deja abierto SNMPv3	SNMPv3	Habilitar; crear una cuenta en el dispositivo	SNMPv3 emplea un modelo de seguridad basado en el usuario que incluye autenticación y privacidad de los datos mediante el cifrado. Es un método más seguro que SNMPv1/v2.
Si se deja abierto, cualquiera puede actualizar el firmware, lo cual permitiría volver a una versión menos segura y afectaría al funcionamiento de las soluciones existentes	Actualización del firmware FTP	Deshabilitar	Es un método para actualizar el firmware del dispositivo de forma remota.
Si se deja abierto, cualquiera puede actualizar el firmware de forma remota, lo cual permitiría volver a una versión menos segura y afectaría al funcionamiento de las soluciones existentes	Actualización remota del firmware (RFU)	Deshabilitar Nota: habilitar para actualizar el firmware de forma remota, deshabilitar cuando haya terminado la actualización.	Es otra manera de actualizar el firmware del dispositivo de forma remota.
Si la información no está cifrada, alguien podría rastrear el tráfico de la red y ver los datos	Requiere una redirección HTTPS	Habilitar	Cifra los datos que se transmiten del dispositivo al ordenador cuando se accede al servidor web integrado del dispositivo.
Si los protocolos se dejan habilitados, alguien podría acceder al dispositivo y cambiar su configuración	Desactivar los protocolos que no se utilizan • Telnet • Protocolo de Transferencia de Archivos (FTP) • Novell (IPX/SPX) • Appletalk	Deshabilitar	Estos protocolos permiten enviar o recibir información de un dispositivo de la red. Normalmente, los protocolos no utilizados se dejan habilitados para las aplicaciones antiguas.
Los usuarios podrían acceder a archivos y manipularlos como si estuvieran guardados localmente en su propio disco duro	Evitar el acceso a los archivos • Sistemas de Archivos de Red • Lenguaje de Gestión de la Impresora • Lenguaje de Trabajo de la Impresora • Postscript	Deshabilitar; marcar todas las casillas	Permite a todos los usuarios de la red acceder de forma remota a los archivos guardados en el disco duro de la impresora.

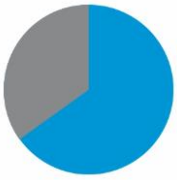
Aplique fácilmente políticas de seguridad a toda su flota de dispositivos HP

Casi el 90%



de las empresas ha sufrido por lo menos una pérdida de datos debido a la falta de seguridad en la impresión[1]

El 65%



de las brechas en la seguridad de los datos se deben a accidentes, negligencias de los empleados o fallos en los procesos de IT o de trabajo[2]

6,88 M € en total

El coste medio de una brecha en la seguridad de los datos es de 123 euros por registro puesto en peligro y 6,88 millones de euros en total[2]

Por qué las políticas de seguridad son importantes

Su cliente genera continuamente datos confidenciales valiosos que son esenciales para el funcionamiento del negocio. Y probablemente utiliza varios métodos de seguridad (incluida la autenticación, el cifrado y la supervisión) para proteger estos datos en sus redes, ordenadores y servidores. ¿Pero su entorno de impresión e imagen es tan seguro como el resto de su infraestructura?

Las brechas de seguridad pueden provocar una peligrosa exposición de datos confidenciales:

- Los dispositivos de imagen e impresión almacenan los archivos en unidades de memoria o discos duros internos, a través de los cuales cualquiera puede tener acceso a información confidencial.
- Los equipos multifunción permiten capturar y enviar trabajos a varios destinos con facilidad, lo cual puede exponer potencialmente datos confidenciales.

Los ajustes de seguridad pueden no estar actualizados o no cumplir las regulaciones de seguridad:

- En algunos países, las empresas se exponen a sanciones si sus ajustes de seguridad no cumplen la ley.

Con los ajustes básicos indicados en la página 2, puede ayudar a su cliente a poner en marcha una estrategia de seguridad en su entorno de imagen e impresión.

Preguntas de orientación

Para determinar las necesidades del cliente, empiece por hacer preguntas relacionadas con su entorno de trabajo, como por ejemplo:

- ¿Qué políticas de seguridad de IT tiene implementadas actualmente?
- ¿Sus políticas de seguridad incluyen los dispositivos de imagen e impresión?
- ¿Es consciente de que las impresoras de su red son un punto de vulnerabilidad?
- ¿Sabe cómo configurar estos ajustes de seguridad en su dispositivo?
- ¿Sabía que HP dispone de una solución que le permite crear una política de seguridad y aplicarla a todos los dispositivos de su flota?

HP JetAdvantage Security Manager

HP JetAdvantage Security Manager es una potente herramienta para crear y editar políticas de seguridad en toda una flota de dispositivos de imagen e impresión de HP[3]. HP Security Manager ofrece la máxima seguridad sin que los administradores tengan que ser expertos en seguridad.

Los dispositivos de impresión se pueden proteger de uno en uno mediante el Embedded Web Server (EWS), pero no resulta muy práctico cuando se trata de proteger una flota entera de dispositivos. Gestionar los ajustes de seguridad en toda su flota no tiene por qué ser complicado ni requerir mucho tiempo. Los ajustes de seguridad indicados en la página 2 son la configuración mínima recomendada por HP para evitar la mayoría de los problemas de seguridad. Se trata de una selección de los ajustes que forman parte de la política básica de seguridad incluida en HP Security Manager.

A medida que su cliente empiece a proteger la red, puede crear su propia política de seguridad con estos ajustes mínimos e ir añadiendo más configuraciones con el tiempo. En los dispositivos compatibles con HP JetAdvantage Security Manager e Instant-On, su cliente puede habilitar ajustes de seguridad importantes desde el momento en que conecte una nueva impresora a la red.

HP Security Manager
Proteja su flota de impresión HP con la solución considerada como pionera por Buyers Laboratory (BLI)[4].

Cómo HP JetAdvantage Security Manager protege su flota

HP Security Manager ayuda a agilizar el proceso para aplicar las políticas de seguridad que ha definido el cliente a una flota de dispositivos de imagen e impresión HP, así como para supervisar y mantener su cumplimiento. HP Security Manager permite identificar fácilmente qué dispositivos no cumplen las políticas y restablece automáticamente los ajustes de seguridad definidos. HP Instant-on Security simplifica la protección de los nuevos dispositivos HP en cuanto se añaden a la red. Facilite a los administradores de IT la gestión del proceso de certificados y ahorre tiempo y dinero a su cliente.

A diferencia de las herramientas tradicionales para gestionar dispositivos en red que se usan generalmente para supervisar y controlar el rendimiento de los dispositivos conectados, HP JetAdvantage Security Manager es la solución de impresión segura más completa del mercado, ya que ofrece un enfoque eficaz basado en políticas para proteger los dispositivos de impresión e imagen de HP[5].

Para empezar ahora mismo con una prueba gratuita durante 60 días, visite: software.hp.com/kiosk.

Nombre de usuario: HPSM_TRIAL60_KIOSK
Contraseña: hpsm60020112

Más información

Para obtener más información sobre cómo convertir HP Security Manager en parte de la estrategia de seguridad de IT integral de su empresa o conseguir una versión de prueba, visite hp.com/go/securitymanager.

[1] "Panorama de Servicios de Impresión Gestionados, 2014", Quocirca, junio de 2014.
[2] "Informe Global 2014 sobre el Coste del Cibercrimen", Ponemon, octubre de 2014.
[3] HP JetAdvantage Security Manager se vende por separado. Para obtener más información o conseguir una prueba gratuita, visite hp.com/go/securitymanager.
[4] Fuente: Informe sobre las soluciones HP JetAdvantage Security Manager 2.1 de Buyers Laboratory LLC, febrero de 2015. Para obtener más información, visite hp.com/go/securitymanager o buyerslab.com.
[5] Basado en datos internos de seguridad de HP (Comparativa de seguridad de dispositivos en enero de 2015) y el Informe sobre las soluciones de HP JetAdvantage Security Manager 2.1 de Buyers Laboratory LLC en febrero de 2015.

Regístrese para recibir novedades
hp.com/go/getupdated

4AA5-8727ESE, julio de 2015