Riesgos Cibernéticos

FUENTE: James Tuplin, Head of Cyber & TMT, International Financial Lines en XL Catlin

La impresora de la oficina: ¿un punto débil en su estrategia de seguridad?

"Primero me hice con el control de sus impresoras. Después, con el de su red. A continuación, con sus datos... Y no es lo único que he robado en esta empresa. Esta gente tiene todas las papeletas para pasarlo muy mal".

Esto es un extracto del cortometraje El lobo, producido por HP y protagonizado por Christian Slater. El lobo muestra cómo una inocente impresora de oficina, la primera "cosa" del Internet de las cosas (IoT, por sus siglas en inglés), puede llegar a ser una amenaza de seguridad por la que introducirse fácilmente.

- **Abierto de par en par**

Hoy en día, la mayoría de las impresoras están conectadas vía wifi. En muchas de ellas la conexión está abierta por defecto, lo que equivale a aparcar un Ferrari en un garaje y anunciar con un letrero luminoso que está ahí, que la puerta está abierta y que las llaves están en la guantera.

- **¿Le suena exagerado?**

En 2009 se lanzó al mercado el programa Shodan, diseñado para detectar dispositivos conectados a Internet, en particular aquellos con fallos de seguridad. Shodan despertó mucho interés cuando se supo que era capaz de encontrar webcams vulnerables, lo que permitía a los hackers acceder a imágenes de vídeo sin que los dueños de los aparatos se den cuenta.

Recientemente unos investigadores han desarrollado en Singapur dos aplicaciones móviles basadas en Shodan que buscan dispositivos wifi abiertos. Las impresoras son el principal objetivo. La idea consiste en equipar un dron con un smartphone que tenga instalada una de estas aplicaciones y utilizarlo para buscar conexiones wifi abiertas en edificios de oficinas.

Riesgos Cibernéticos

FUENTE: James Tuplin, Head of Cyber & TMT, International Financial Lines en XL Catlin

Una de las versiones, llamada Cybersecurity Patrol, es benévola. Cuando la aplicación encuentra una impresora abierta, crea un punto de acceso falso y envía un mensaje de advertencia a la impresora para alertar a la empresa de su vulnerabilidad.

Con la versión malévola, el punto de acceso falso puede usarse para interceptar documentos dirigidos a la impresora. Dichos documentos, que pueden contener información confidencial o privada, pueden enviarse a la cuenta Dropbox del hacker gracias a la conexión 3G o 4G del teléfono. Una vez descargados, la aplicación puede reenviarlos a la impresora "real" para que nadie se percate de la intrusión.

Además de para la extracción directa de datos, los hackers pueden utilizar las impresoras y fotocopiadoras para acceder a todo el servidor de archivos de la empresa. Empleando el dispositivo comprometido como puente, los cibercriminales son capaces de instalar un malware en la red de la empresa y causar daños de todo tipo, filtrar datos o incluir la red en una botnet para perpetrar un ataque de denegación de servicio distribuido (DDoS).

❖ Tome medidas

Las redes wifi desprotegidas no son la única vía de acceso a los sistemas y datos de la empresa a través de las impresoras.

❖ Dé la voz de alarma

Aunque los métodos que utilizan los hackers para introducirse a través de las impresoras son de sobra conocidos, las amenazas de seguridad a menudo se pasan por alto.

Según un estudio del Instituto Ponemon publicado en 2015, el 56 % de las empresas no incluye a las impresoras de oficina en los análisis de seguridad. Resulta aún más llamativo que nada menos que un 60 % hayan sufrido una filtración de datos a través de la impresora y tardaron una media de 46 días en resolver el problema.

Es más, según un estudio de HP publicado en 2016, solo el 18 % de los encuestados mostraron preocupación por la seguridad de sus impresoras, mientras que el 91 % se mostró preocupado por la seguridad de sus ordenadores.

Riesgos Cibernéticos

FUENTE: James Tuplin, Head of Cyber & TMT, International Financial Lines en XL Catlin

❖ Reconocer la amenaza

Proteger una impresora de los hackers no cuesta demasiado trabajo y a menudo basta con tomar medidas básicas y de sentido común. Lo más difícil suele ser garantizar que las impresoras de red se incluyan en los programas de ciberseguridad.

Los expertos en seguridad recomiendan a las empresas que solo adquieran dispositivos con funciones de seguridad integradas, como software de detección. Cada vez son más los modelos de impresoras que incluyen potentes medidas de seguridad, pero sigue habiendo muchos que carecen de ellas.

Otra medida consiste en analizar qué dispositivos están conectados a su red. Con la ayuda de un inventario exhaustivo, los encargados de seguridad pueden desconectar los dispositivos que no requieren conexión a Internet y tomar las precauciones necesarias respecto a los que sí (por ejemplo, cambiar la conexión inalámbrica a una por cable siempre que sea posible).

Además, se deben cambiar siempre las contraseñas por defecto cuando se incorpore un nuevo dispositivo a la infraestructura de la empresa. Mientras que en los ordenadores es habitual hacerlo, los periféricos como las impresoras, los aparatos de aire acondicionado y las cámaras de circuito cerrado suelen funcionar con la contraseña de administrador proporcionada por el fabricante.

Por último, como ocurre con todos los ciberriesgos, es importante saber que la tecnología de seguridad tiene sus límites. Las empresas pueden aplicar los últimos sistemas y procedimientos de seguridad, pero la clave para reducir las amenazas siguen siendo los usuarios.