Interconectividad de las impresoras con otros equipos a través de Internet es foco de vulnerabilidad

4 consejos para proteger sus dispositivos de impresión de ciberataques

Las impresoras inteligentes son prácticas y funcionales, pero por algunas de sus características como permitir almacenar documentos o hasta enviar correos electrónicos, son apetecidas por los cibercriminales para vulnerarlas junto con otros equipos conectados a la red, explica Miguel Pérez, de la Escuela de Sistemas Inteligentes de Universidad CENFOTEC. Cortesía-Canva/La República

Protección a través de programas antivirus y firewalls, así como autenticación de usuarios de equipos son clave

¿Sabía que al imprimir un documento de trabajo o al escanear la copia de la cédula o el pasaporte, sin mencionar que por estos dispositivos pueden pasar datos sensibles como números de tarjeta o claves bancarias, podría estar siendo interceptado por ciberdelincuentes?

Y es que, la evolución de estos equipos que continúan formando parte de la oficina y en algunos casos del hogar, ha sido notoria a través del tiempo, siendo que la gran mayoría son capaces de conectarse a las computadoras, celulares o tabletas de forma inalámbrica a través de la red local de Internet.

Justamente esta característica de conectividad, basada en el principio del Internet de las Cosas, es lo que hace más vulnerables a estos dispositivos, frecuentemente olvidados en el plan de ciberseguridad de muchas empresas, pero que pueden convertirse en una puerta de entrada para cibercriminales mediante el robo de información confidencial o infección por archivos maliciosos.

"Es importante mencionar que una impresora WiFi multifuncional es un dispositivo más que está conectado a una red, la cual cuenta con procesos de configuración que permiten el acceso a unidades de almacenamiento compartidas en red", explica Marvin Jiménez, experto en ciberseguridad del Colegio de Profesionales en Informática y Computación.

Es así como un ciberdelincuente podría conectarse a este equipo, implantar un virus en dicha unidad e infectar los demás equipos de la red y robar datos sensibles, o bien, suplantar la dirección IP, haciéndose pasar por un dispositivo legítimo y llevar a cabo acciones maliciosas más avanzadas, según el experto.

Además de ejecutar acciones de ransomware (secuestro y encriptación de datos), tales ataques podrían conllevar otras consecuencias como la ralentización de los equipos, reducción repentina del espacio de almacenamiento, infiltración en cuentas de redes sociales y clientes de correo electrónico, aparición de ventanas emergentes con saturación de publicidad y hasta contraseñas e inicios de sesión que dejan de funcionar.

Entre las opciones para protegerse de tales escenarios destacan la protección de los equipos con programas antivirus y firewall, así como promover una cultura de prevención del riesgo en el caso de las organizaciones.

"En el caso de las impresoras inteligentes, se deben configurar para que funcione únicamente con autenticación del usuario que está solicitando el servicio de impresión o envío por medios digitales y mantener control de los usuarios autorizados, así como borrar periódicamente la caché y memorias de estos equipos para mantener la confidencialidad de la información", recomienda Miguel Pérez, director de la Escuela de Sistemas Inteligentes de Universidad CENFOTEC.

Andrei Siles
andreisiles.asesor@larepublica.net

CONSEJOS PARA BLINDAR SU IMPRESORA

Evite que los ciberdelincuentes invadan su hogar u oficina

Asegurar la red WiFi y los puntos de acceso con contraseñas robustas para evitar que personas externas puedan conectarse libremente a la red inalámbrica.

Permitir que las tareas de impresión y/o almacenamiento de la información en las unidades sea solo para personas autorizadas y que sea necesario un PIN o contraseña para poder ejecutar esas tareas.

Mantener el firmware de la impresora actualizado y en la versión recomendada por el fabricante.

Procurar mantener la impresora conectada de forma alámbrica a la computadora y no conectada a la red, en caso de tener dudas sobre la fiabilidad de esta.