Análisis y conclusiones sobre las actualizaciones de firmware y sus repercusiones negativas

El firmware es el sistema operativo esencial de una impresora y merece el mismo cuidado que un servidor o un ordenador. Proponemos un enfoque proactivo y preventivo.

01 CONTROL DE ACTUALIZACIONES

Cómo gestionamos el firmware de una flota

Tomando como ejemplo una Xerox AltaLink C8245, nuestro equipo monitoriza los avisos del fabricante y aplica los parches de seguridad siguiendo un proceso controlado:

01

Avisos de seguridad

Revisión de los boletines del fabricante.

02

Pruebas

Validación en entornos controlados antes del despliegue.

03

Despliegue

Automatizado o semiautomatizado en toda la flota.

04

Monitorización

Integración con SIEM para detectar accesos o cambios no autorizados.

02 VULNERABILIDADES

Lo que corrigen las actualizaciones

Un ejemplo conocido es PrintNightmare, la vulnerabilidad de los sistemas de impresión de Windows. También existen riesgos en la cadena de suministro.

Accesos no autorizados

Al dispositivo y a la red.

Escalada de privilegios

Ejecución de código malicioso

Denegación de servicio

Protocolos inseguros

Como LPD o IPP.

Manipulación de ajustes

Como la autenticación.

03 CONSECUENCIAS DE NO ACTUALIZAR

Una impresora desactualizada es una puerta de entrada a tu red

- **Ransomware** y propagación de malware.
- **Phishing** enviado desde direcciones internas.
- **Incumplimiento normativo** (RGPD).
- **Fugas de datos**.
- **Denegación de servicio**.
- **Daño reputacional**.

¿Hablamos de tu caso?

Reprise · Xerox Platinum Partner desde 1987 · más de 35 años · info@reprise.es · 910 220 142 · 934 093 260 · reprise.es/contact