AUDITORÍA CORPORATIVA

El Fallo sin Parche Ya Es la Entrada Más Común a una Brecha, según Verizon

El 19 de mayo de 2026, Verizon publicó su Data Breach Investigations Report (DBIR) de este año. Por primera vez en la historia del informe, aprovechar una vulnerabilidad superó al robo de credenciales como la vía de entrada más común a una brecha. En los casos que analiza, el atacante entró más a menudo por un fallo de software sin corregir que con una contraseña robada.

El hallazgo principal está en el comunicado de Verizon del 19 de mayo de 2026.
https://www.verizon.com/about/news/breach-industry-wide-dbir-finds

Según la reseña del informe que publicó Help Net Security, la corrección también se volvió más lenta. La mediana entre la detección de una vulnerabilidad y su parche completo pasó de 32 a 43 días. Mientras dura ese intervalo, el fallo sigue abierto para quien lo busque.

Las cifras de corrección aparecen en el resumen de Help Net Security del 20 de mayo de 2026.
https://helpnetsecurity.com/2026/05/20/verizon-2026-dbir-findings

Dos Casos en Colombia y México sin Programas Sofisticados

El 21 de julio de 2026, Kaspersky publicó dos casos de ransomware que investigaron sus equipos de respuesta a incidentes en empresas de Colombia y México, sin identificar a las víctimas. Según Kaspersky, en ninguno los atacantes recurrieron a un programa malicioso sofisticado. En Colombia, los atacantes entraron por un servicio de escritorio remoto expuesto a internet. En México, por un servidor de base de datos mal configurado y accesible desde internet, con unas credenciales que estaban en código publicado en GitHub. Kaspersky añade que en el caso mexicano el ataque empezó unos tres meses antes de ser detectado y que hubo alertas que nadie investigó. En los dos casos, el cifrado se hizo con funciones del propio Windows y las notas de rescate salieron por las impresoras de la oficina.

El análisis técnico se publicó en Securelist, el blog de investigación de Kaspersky, el 21 de julio de 2026.
https://securelist.com/new-extortion-scheme-printers-bitlocker/120718/

Un Referente Útil: La Directiva de CISA sobre Equipos de Borde

El 5 de febrero de 2026, la agencia estadounidense CISA emitió la directiva BOD 26-02. Obliga a las agencias civiles federales de Estados Unidos a inventariar los equipos de borde que ya no

reciben soporte del fabricante (firewalls, routers, switches, balanceadores de carga, puntos de acceso inalámbrico) y a retirarlos por etapas: a los 12 meses, los que ya hayan perdido el soporte para esa fecha, y a los 18 meses, todos los identificados. CISA explica que conoce campañas de explotación amplias contra esos equipos. La directiva no se aplica a ninguna empresa venezolana. Su lógica sí sirve como referencia: un equipo sin soporte no recibirá el parche que corrija su próximo fallo.

El texto completo está en la página de la directiva publicada por CISA el 5 de febrero de 2026.
https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices

Qué Revisar Esta Semana en Tu Empresa

- Haz una lista de todo lo que da a internet (firewall, VPN, router, NAS, escritorio remoto, paneles de administración, la web y su panel) y anota de cada uno el modelo, la versión, quién lo mantiene y hasta qué fecha el fabricante publica actualizaciones.
- Busca cada fabricante y producto en el catálogo de vulnerabilidades explotadas conocidas (KEV) de CISA y pon primero en la cola lo que aparezca allí o ya no tenga soporte.
- Fija un plazo máximo para aplicar correcciones críticas en esos equipos y registra la fecha real de cada parche, para conocer tu tiempo de corrección con datos propios.
- Retira de internet el escritorio remoto y las bases de datos; si un acceso remoto hace falta, que pase por una VPN con verificación en dos pasos.
- Revisa el código que la empresa o sus proveedores publicaron en GitHub o servicios parecidos, y los documentos compartidos con enlace público, en busca de contraseñas o claves; si aparece una, cámbiala primero y retira el archivo después.
- Nombra a una persona que reciba las alertas del firewall, del antivirus y de los inicios de sesión, con un horario y una instrucción clara de qué hacer con cada una.

Cómo lo Trabajamos en Auditoría y Pentesting Corporativo

Empezamos con un alcance escrito y una autorización firmada: qué direcciones, dominios y equipos son de la empresa, qué pruebas se acuerdan y en qué horario. Después revisamos la exposición externa como la vería cualquiera desde internet: servicios abiertos, versiones, paneles de administración, accesos remotos y equipos fuera de soporte. Contrastamos cada elemento con el catálogo KEV de CISA y con las fechas de soporte de su fabricante, y buscamos credenciales de la empresa en código público y documentos expuestos.

Las pruebas autorizadas comprueban qué es alcanzable y aprovechable de verdad, y se planifican para no interrumpir la operación. Cada hallazgo llega con su evidencia. El informe ejecutivo ordena

las correcciones por exposición y por explotación conocida, además de la gravedad técnica, y señala qué equipos sin soporte conviene reemplazar. Cuando tu equipo aplica los cambios, volvemos a probar para confirmar que cada corrección funciona.

> *Una auditoría describe lo encontrado dentro de un alcance y en una fecha. No garantiza que no existan otras vulnerabilidades ni sustituye la actualización continua, que depende también de que el fabricante siga publicando parches. Las cifras citadas son de Verizon y Kaspersky y describen los casos que esas empresas analizaron.*

Una Comprobación Concreta

Abre la página de administración de tu firewall, VPN o router principal y anota el modelo y la versión de firmware, sin cambiar ningún ajuste. Busca ese modelo en el sitio de soporte del fabricante para saber si todavía recibe actualizaciones y hasta cuándo. Después busca el fabricante y el producto en el catálogo de vulnerabilidades explotadas conocidas de CISA. Si el modelo ya no tiene soporte, o el catálogo recoge un fallo de ese producto y el aviso del fabricante indica que tu versión está afectada, ese equipo va primero en la lista para actualizar o reemplazar.

Documentación de apoyo: Catálogo de vulnerabilidades explotadas conocidas de CISA.
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Para seguir leyendo: La Web Antigua que Nadie Recuerda Puede Seguir en Línea.
https://systems.kavaliero.com/blog/la-web-antigua-que-nadie-recuerda-sigue-en-linea

Si necesitas ayuda con este trabajo, consulta el alcance de Auditoría y Pentesting Corporativo.
https://systems.kavaliero.com/soluciones/auditoria-pentesting