FUGA DE INFORMACIÓN · FORENSE CORPORATIVO

BLOQUEARON TODAS LAS PUERTAS Y LA INFORMACIÓN SALIÓ POR LA VENTANA.

EL CORREO PERSONAL ABIERTO EN EL EQUIPO DE TRABAJO: EL CANAL QUE NINGÚN FIREWALL DETIENE

> **QUIEN PLANEA UNA FUGA PIENSA EN CÓMO SACAR LOS ARCHIVOS; CASI NUNCA PIENSA EN QUE EL SISTEMA LLEVA UN DIARIO DE CADA PUERTA QUE ABRIÓ.**

Investigación interna con métrica de riesgo, vía por vía, documentada y replicable.

EL PROBLEMA

Una empresa sospechaba que un empleado se había llevado información confidencial, pero su defensa parecía razonable: las memorias USB estaban bloqueadas por política en todos los equipos y un firewall empresarial bloqueaba los sitios de almacenamiento en la nube. Si la información no podía salir por memoria ni por nube, ¿por dónde?

El encargo fue revisar el equipo del empleado y una «aplicación virtual» que la empresa operaba. Ambas respuestas resultaron más interesantes de lo que nadie esperaba.

LA INTERVENCIÓN

La revisión recorrió cada vía con una métrica de riesgo. Las defensas funcionaban: sin USB de almacenamiento, nube bloqueada. Pero el empleado tenía un correo personal abierto en el equipo, y un buzón personal permite adjuntar documentos y enviarlos — un canal de extracción que el firewall no filtra porque, para él, es solo correo.

Después, los números: borrado masivo de archivos desde el primer día de uso; un pico exacto de datos enviados un día concreto, y tres días después el historial del navegador borrado selectivamente — limpieza deliberada, que requiere pasos intencionados. Y en la máquina virtual de la empresa, los testigos mudos que el usuario nunca supo que existían: el sistema guarda un registro la primera vez que cada carpeta es visitada, y ese mismo día el empleado entró por primera vez a carpetas de trabajo que no le correspondía consultar.

No se pudo dictaminar qué se llevó —el borrado lo impidió— pero sí cuándo, por dónde y con qué preparación.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.

LAS DEFENSAS FUNCIONARON.
LA VENTANA ESTABA ABIERTA.

LAS CARPETAS QUE ALGUIEN ABRE POR PRIMERA VEZ QUEDAN MARCADAS PARA SIEMPRE

QUÉ SE LOGRÓ

Gracias al análisis forense, la empresa obtuvo certeza técnica sobre la fuga en su investigación interna: la extracción por USB no fue posible y las defensas perimetrales funcionaron, pero el correo personal ofreció un canal sin restricciones, el consumo de red tuvo su pico el mismo día en que el empleado accedió por primera vez a información que no le correspondía, y los historiales fueron borrados intencionalmente.

> **La lección para toda dirección de tecnología: bloquear las puertas conocidas no es seguridad si quedan ventanas cotidianas. Los sistemas registran la verdad incluso cuando el usuario ya se fue.**

POR QUÉ DURIVA ES LA MEJOR OPCIÓN

≡

EFICIENCIA

Metodología propia probada en miles de dictámenes, con equipos que trabajan en paralelo sobre la evidencia.

TIEMPO

Respuesta ágil en escenarios de urgencia procesal, con la misma calidad técnica y documentación completa.

18

TRAYECTORIA

Más de 18 años de cómputo forense en México y América Latina. Creador del primer sistema operativo forense latinoamericano, presidente del Consejo Americano de Ciberseguridad y Cómputo Forense, autor de seis libros especializados.

Si sospecha que alguien se llevó información, el equipo lo recuerda todo. Somos su aliado digital.

Caso anonimizado para proteger la identidad de las partes. Los detalles técnicos se describen a nivel general.