FUGA DE INFORMACIÓN · INVESTIGACIÓN CONFIDENCIAL

LA FUGA RARA VEZ ES UN HACKER ENTRANDO: ES UN EMPLEADO SALIENDO.

CON LAS LLAVES DE LA COMPETENCIA GUARDADAS EN SU PROPIO CORREO

MIENTRAS EL ÁREA DE SISTEMAS VIGILA LA PUERTA EQUIVOCADA.

Copias forenses de varios equipos y un teléfono, sin que nadie en la empresa lo supiera.

EL PROBLEMA

Una empresa encargó una investigación confidencial —sin que sus empleados lo supieran— por una posible fuga de información hacia la competencia. Las palabras clave venían del propio informe interno: el nombre de una distribuidora externa, dos personas y términos de producto.

Se hicieron copias forenses de varios equipos de cómputo y un teléfono, sin tocar los originales. La métrica del análisis: riesgo bajo, medio o alto, equipo por equipo.

LA INTERVENCIÓN

El primer golpe fue de los que no se olvidan: en un equipo, guardados con usuario y contraseña, estaban los accesos a dos cuentas de correo del dominio de la distribuidora externa — una con el nombre del propio empleado. Un empleado de la empresa con llaves de la competencia, y correspondencia que lo vinculaba con otra entidad del mismo ecosistema.

El segundo equipo tenía software anti-forense instalado —de los que borran sin dejar recuperación— y correos eliminados de los que solo sobrevivían las cabeceras; ambos equipos tenían escritorio remoto, canales legítimos que en manos equivocadas son puertas traseras. Y el teléfono completó el mapa: conversaciones pidiendo a un directivo de la distribuidora el detalle de pagos, y otra sobre la creación de los dominios de esa empresa — cerrando con la decisión del nombre del dominio y de las cuentas que después aparecieron en el primer equipo.

El análisis también midió lo que no había: coincidencias irrelevantes por una palabra clave —el cuidado de no acusar por coincidencia fonética— y un tercer equipo que quedó limpio.

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

RIESGO REAL, RIESGO POTENCIAL Y EQUIPO LIMPIO: TODO DOCUMENTADO.

LAS CONCLUSIONES SE ORDENAN POR EQUIPO, NO POR SOSPECHA

QUÉ SE LOGRÓ

Gracias a la investigación confidencial, la empresa obtuvo el mapa completo de la fuga en su investigación interna: el equipo con credenciales de la competencia como riesgo real, el de anti-forense como riesgo potencial, el tercero sin hallazgos, y la línea financiera a seguir entre el dueño del teléfono y la distribuidora externa.

> **La recomendación de higiene inmediata: políticas sobre escritorio remoto y sobre cuentas personales en equipos de trabajo — porque la fuga casi nunca fuerza la puerta; usa las llaves que la empresa misma dejó.**

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 una fuga, investigue en silencio y con método: la evidencia decide equipo por equipo. Somos su aliado digital.

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