RANSOMWARE · RESPUESTA A INCIDENTES Y RECUPERACIÓN DE DATOS

SU EMPRESA AMANECIÓ SIN PODER ABRIR UN SOLO DOCUMENTO.

CÓMO SE RECONSTRUYE UN ATAQUE MINUTO A MINUTO — Y CÓMO SE RECUPERA LA INFORMACIÓN

> **UN RANSOMWARE CASI NUNCA ES MALA SUERTE: ES LA SUMA DE PUERTAS ABIERTAS QUE NADIE CERRÓ.**

Investigación forense con evidencia sellada, replicable por cualquier especialista.

EL PROBLEMA

Una empresa amaneció sin poder abrir un solo documento: su sitio web, sus bases de datos y los archivos de trabajo de años, todo cifrado por un programa malicioso de rescate. La pregunta que se nos encargó responder no era solo si se podía recuperar la información. Era quién había sido: ¿un empleado con acceso físico al servidor, o un atacante desde fuera de la red?

De esa respuesta dependían decisiones serias: un despido justificado o un juicio laboral, una reclamación de seguro procedente o negada. La empresa no pagó el rescate y entregó el disco del servidor para el análisis forense.

LA INTERVENCIÓN

Lo primero fue no tocar nada: se generó una copia forense bit a bit del disco, sellada con sus huellas digitales de integridad, y todo el trabajo se hizo sobre la copia. Los registros del propio servidor contaron la película completa: durante horas, una máquina del exterior probó contraseñas sin descanso —decenas de miles de intentos— y el servidor no bloqueó ni uno. En la madrugada, el atacante consiguió entrar por un canal de red que debía estar cerrado; segundos después ya tenía las manos en el teclado, y un minuto más tarde arrancó el cifrado.

La autopsia de cuentas explicó por qué pudo pasar: el servidor tenía dos administradores con permisos totales y contraseñas de años sin rotar, no limitaba los intentos de acceso, no bloqueaba direcciones atacantes y era alcanzable directamente desde internet, cuando un servidor con datos críticos debe vivir detrás de un control de accesos.

Sobre la copia forense —nunca sobre el original— fue posible recuperar la práctica totalidad de la información: el sitio web, las bases de datos y los documentos, cada archivo entregado con su huella de integridad.

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

EL SERVIDOR GRABÓ SU PROPIA DERROTA.

LA PREGUNTA «¿EMPLEADO O ATACANTE EXTERNO?» SE RESPONDE CON EVIDENCIA, NO CON SOSPECHAS

QUÉ SE LOGRÓ

Gracias a la investigación forense se probó que el ataque vino de fuera, por una puerta que la propia empresa tenía abierta: el servidor grabó su propia derrota intento por intento, y los registros que nadie vigiló antes del ataque fueron los que permitieron reconstruirlo después. La empresa recuperó su información y salió con un plan de remediación ordenado por prioridad.

> **La pregunta que todo director debería hacerse no es «¿y si nos atacan?», sino cuántas veces puede fallar un extraño tratando de entrar a su servidor antes de que el sistema lo expulse. Si la respuesta es «las que quiera», el ataque ya está en camino.**

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 su empresa amaneció cifrada, no negocie a ciegas: documente. Somos su aliado digital.

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