INSTITUCIONES EDUCATIVAS · RESPUESTA A INCIDENTES

EL INTRUSO NO HACKEÓ LA SESIÓN: ENTRÓ POR UNA PUERTA QUE LA ESCUELA DEJÓ ABIERTA.

DOS CONFIGURACIONES QUE SE CORRIGEN EN DIEZ MINUTOS SEPARAN A UNA INSTITUCIÓN DE UN ESCÁNDALO

> **EL ATACANTE CASI NUNCA ROMPE LA PUERTA: ENCUENTRA LA QUE DEJARON ABIERTA POR COMODIDAD.**

Reconstrucción del incidente con métrica de riesgos y registro completo de actividades.

EL PROBLEMA

Una escuela vivió la pesadilla moderna de cualquier institución educativa: en plena sesión informativa en línea, con aspirantes y familias conectados, la transmisión fue atacada. El encargo fue preciso: analizar el equipo que organizaba la sesión y determinar bajo rigor científico el origen del ataque — ¿un atacante conectado al equipo, o el incidente venía de otro método?

El equipo quedó puesto a la vista, con la evidencia sellada con sus valores de integridad desde el primer momento.

LA INTERVENCIÓN

El primer hallazgo fue el equipo mismo: una máquina de uso comunal, con un único usuario general, perfiles de varias personas y contraseñas guardadas en el navegador, accesibles para cualquiera que la usara — en un equipo compartido, ninguna credencial guardada es realmente de nadie. El segundo fue la puerta trasera institucionalizada: una aplicación de escritorio remoto configurada de la peor manera posible — sin contraseña de uso, con inicio automático cada vez que el equipo encendía y con permisos por encima del propio antivirus.

El tercero fue el mecanismo exacto del espectáculo: la carpeta de materiales no contenía nada inapropiado que hubiera podido proyectarse por error —pero la sesión tenía habilitada la opción de compartir pantalla para todos los invitados, y la plataforma coloca en pantalla principal, automáticamente, a quien comparte. Un intruso no necesitaba hackear nada: entraba como invitado, compartía su pantalla, y la plataforma lo ponía en grande frente a todas las familias.

Y el dictamen respondió con datos: en las fechas y horas de las sesiones implicadas, sí existieron conexiones remotas al equipo. Las dos vías quedaron documentadas — la puerta trasera del escritorio remoto sin contraseña y la puerta delantera de la pantalla compartida abierta a todos.

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

CUANDO EL INCIDENTE YA OCURRIÓ, LA RESPUESTA NO ES EL PÁNICO: ES EL PERITAJE.

RECONSTRUIR QUÉ PASÓ, CON QUÉ VECTOR Y CON QUÉ EVIDENCIA, PARA CERRAR LA PUERTA CORRECTA

QUÉ SE LOGRÓ

Gracias a la investigación forense, la escuela obtuvo la explicación completa del incidente en su investigación interna: el equipo comunal con credenciales expuestas, el escritorio remoto abierto de par en par, el mecanismo de la transmisión secuestrada y las conexiones remotas documentadas en las fechas implicadas — con las recomendaciones de fondo para que no vuelva a ocurrir.

> **La enseñanza para toda institución que abre salas en línea: una sesión donde «todos pueden compartir pantalla» es un escenario entregado al primer intruso.**

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 institución abre salas en línea, cierre las dos puertas antes de que alguien las encuentre. Somos su aliado digital.

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