AUDITORÍA DE PARQUE DE CÓMPUTO · SEGURIDAD EMPRESARIAL

REVISAMOS TODAS LAS COMPUTADORAS DE LA EMPRESA. NO HABÍA UN LADRÓN: HABÍA UNA CASA CON LAS VENTANAS ABIERTAS.

LA SEGURIDAD INFORMÁTICA NO SE DECLARA: SE VERIFICA

> **UN ANTIVIRUS AL DÍA SOBRE UN SISTEMA SIN ACTUALIZAR ES UN GUARDIÁN CON UNA PARED ROTA A LA ESPALDA.**

Imagen forense de cada equipo con su huella, y un historial por máquina: la radiografía completa de una empresa.

EL PROBLEMA

Hay encargos que son la radiografía completa de una empresa: revisar no una máquina sospechosa, sino todo el parque de cómputo. Una compañía lo pidió exactamente así — todas sus computadoras, de dos plataformas distintas, con una imagen forense de cada una y su huella de integridad.

El resultado fue un documento que la dirección no olvidó: no encontramos un ladrón; encontramos una casa entera con las ventanas abiertas, y dos invitados que no deberían estar.

LA INTERVENCIÓN

El barrido fue equipo por equipo: disco, usuarios, ejecutables, software instalado y desinstalado, archivos sospechosos verificados contra las bases mundiales de reputación, servicios, puertos, firewall, actualizaciones y registros de uso. En la carpeta de software compartido vivían los dos invitados: un instalador reportado por más de veinte firmas antivirus como malicioso, con actividad de puertos que su versión legítima no necesita, y un segundo con la conducta del manual del malware profesional — se calla cuando sospecha que lo están observando. Y un tercer archivo marcado como sospechoso resultó, al probarlo en ambiente aislado, un falso positivo: dos amenazas reales y una que no era nada — la diferencia entre leer una alerta y hacer forense.

Después, las puertas: todas las máquinas podían recibir conexiones de control remoto con un protocolo obsoleto, repetido equipo tras equipo. Los registros contaban su uso: una máquina acumulaba eventos un orden de magnitud por encima de cualquier otra — un número que no acusa pero exige explicación — y otra aparecía en el inventario con una sola anotación: formateada semanas antes de la intervención.

Y la seguridad de fachada: antivirus actualizado pero sin activar sus opciones de detección, ni un solo sistema parchado, puertos USB bloqueados como medalla — mientras los empleados se compartían el trabajo por nubes privadas, anulando el bloqueo por completo: la información no salía en memorias, salía por internet, sin registro ni control.

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

CUANDO UNA REVISIÓN ASÍ SE ANUNCIA, LA FECHA DE UN FORMATEO SE VUELVE EL DATO MÁS INTERESANTE DEL EXPEDIENTE.

ANTIVIRUS, BLOQUEO DE USB Y RED COMPARTIDA — Y DESPROTEGIDA POR LOS CUATRO COSTADOS

QUÉ SE LOGRÓ

Gracias a la auditoría completa del parque de cómputo, la dirección obtuvo su radiografía real en la investigación interna: dos amenazas reales detectadas y un falso positivo absuelto, control remoto obsoleto en toda la flotilla, sistemas sin parchar, una máquina formateada justo antes de la revisión y la fuga cotidiana por nubes personales documentada.

> **La enseñanza que toda dirección debería escuchar una vez al año: una empresa puede tener antivirus, bloqueo y red compartida, y estar desprotegida al mismo tiempo. La seguridad no se declara: se verifica.**

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 nunca ha revisado todo su parque de cómputo, la radiografía está pendiente. Somos su aliado digital.

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