AUDITORÍA

Encontrarlo Antes que un Tercero: Qué Revisa una Auditoría

Muchos informes de seguridad se leen como una lista de miedos. Decenas de hallazgos, todos en rojo, ninguno con contexto. Sirven para justificar una compra, no para decidir por dónde empezar un lunes.

Una revisión que sirve responde tres preguntas en lenguaje llano: qué puede pasar, qué tan probable es en tu caso y cuánto cuesta cerrarlo.

Por Dónde Empezamos

- Lo que está expuesto a internet sin que nadie recuerde haberlo publicado.
- Accesos de gente que ya no trabaja contigo, y claves compartidas entre varios.
- Actualizaciones pendientes en lo que sostiene el negocio, no en todo el inventario.
- Copias de seguridad: si existen, si se pueden restaurar, y cuándo se probó por última vez.

Pentesting No Es lo Mismo que Auditoría

Una auditoría mira configuración y acuerdos. Un pentest intenta, con permiso y alcance por escrito, aprovechar lo que encuentre para mostrar hasta dónde se llega. El segundo tiene sentido cuando el primero ya está ordenado. Si no, pagas por confirmar lo evidente.

Qué Entregamos

Un informe corto y priorizado: qué encontramos, qué lo hace posible y qué recomendamos hacer primero. Y una conversación para revisarlo, porque lo que más cuesta de un informe es entender qué significa para tu operación.

> *Trabajamos con alcance y autorización por escrito, sobre sistemas del propio cliente. No hay hallazgos garantizados: hay una revisión honesta de lo que apareció en ese alcance.*

Una Comprobación Concreta

Pregunta qué evidencia permite cerrar un hallazgo. Para el acceso de una persona que dejó la empresa, una captura con el nombre eliminado es menos concluyente que comprobar, dentro del alcance autorizado, que el permiso se rechaza. Acuerda antes la cuenta de prueba, el entorno y las acciones permitidas. El informe debe distinguir lo observado, lo inferido y lo que queda sin probar.

Documentación de apoyo: Guía de OWASP sobre pruebas de autorización.
https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

Para seguir leyendo: La Web Antigua que Nadie Recuerda Puede Seguir en Línea.
https://systems.kavaliero.com/blog/la-web-antigua-que-nadie-recuerda-sigue-en-linea

Si necesitas ayuda con este trabajo, consulta el alcance de Auditoría y Pentesting Corporativo.
https://systems.kavaliero.com/soluciones/auditoria-pentesting