Checklist

5 señales de que tu organización tiene exposición al riesgo sin saberlo

mtp DIGITAL BUSINESS ASSURANCE

Checklist | 5 señales de que tu organización tiene exposición al riesgo sin saberlo

Durante años, muchas organizaciones han enfocado su estrategia de seguridad en la identificación de vulnerabilidades técnicas. Sin embargo, el entorno digital actual ha cambiado radicalmente y la exposición al riesgo ya no depende únicamente de la existencia de vulnerabilidades, sino de cómo estas se combinan con la superficie de ataque, los accesos disponibles y la criticidad de los activos.

Este checklist permite identificar señales tempranas de exposición al riesgo que muchas organizaciones aún no visualizan.

1. NO EXISTE UN INVENTARIO COMPLETO DE ACTIVOS DIGITALES

Muchas organizaciones no tienen una visibilidad clara de todos los activos que forman parte de su ecosistema digital.

Esto incluye:
- Sistemas on-premise
- Servicios en la nube
- Aplicaciones SaaS
- APIs expuestas a internet
- Integraciones con terceros
- Identidades con acceso a recursos críticos

Cuando no existe un inventario actualizado de activos, es imposible entender realmente la superficie de ataque de la organización.

Preguntas clave:
- ¿Tenemos visibilidad de todos los activos expuestos a internet?
- ¿Sabemos qué aplicaciones están conectadas a nuestros sistemas críticos?
- ¿Tenemos claro quién es responsable de cada activo?

2. LAS VULNERABILIDADES SE PRIORIZAN SOLO POR SEVERIDAD TÉCNICA

Muchas organizaciones priorizan vulnerabilidades utilizando métricas técnicas como CVSS. Sin embargo, la severidad técnica no siempre refleja el riesgo real.

Por ejemplo:
- Una vulnerabilidad crítica en un sistema aislado puede representar un riesgo bajo
- Una vulnerabilidad media en un sistema crítico expuesto a internet puede representar un riesgo alto

Sin contexto de negocio, las organizaciones pueden invertir tiempo resolviendo problemas que no reducen significativamente su exposición.

Preguntas clave:
- ¿Priorizamos vulnerabilidades considerando la criticidad del activo?
- ¿Entendemos qué vulnerabilidades pueden afectar procesos críticos del negocio?

3. SEGURIDAD IDENTIFICA PROBLEMAS, PERO NO CONTROLA LA REMEDIACIÓN

En muchas organizaciones existe una separación clara entre quienes identifican los riesgos y quienes deben resolverlos.

El equipo de seguridad identifica vulnerabilidades, pero la remediación depende de:
- Infraestructura
- Cloud
- Desarrollo
- Operaciones

Cuando no existe un proceso claro de priorización y coordinación, muchas vulnerabilidades permanecen abiertas durante largos periodos.

Preguntas clave:
- ¿Existe un proceso claro de remediación de riesgos?
- ¿Se asignan responsables específicos para resolver vulnerabilidades críticas?

4. LAS EVALUACIONES DE SEGURIDAD SON PERIÓDICAS, NO CONTINUAS

Las pruebas de penetración y los análisis de vulnerabilidades suelen realizarse de forma periódica. Sin embargo, el entorno tecnológico cambia constantemente.

Cada día pueden aparecer:
- Nuevos activos
- Nuevas configuraciones
- Nuevas integraciones
- Nuevas identidades

Esto significa que una evaluación realizada hace algunos meses puede no reflejar la exposición actual.

Preguntas clave:
- ¿Con qué frecuencia evaluamos nuestra superficie de ataque?
- ¿Tenemos visibilidad continua de los cambios en el entorno?

5. NO EXISTE VISIBILIDAD SOBRE POSIBLES RUTAS DE ATAQUE

Una vulnerabilidad aislada puede no representar un riesgo significativo. Pero cuando varias vulnerabilidades se combinan, pueden crear una ruta de ataque que permita comprometer sistemas críticos.

Por ejemplo:
Acceso externo → credencial comprometida → movimiento lateral → acceso a información sensible

Muchas organizaciones no tienen visibilidad sobre estas rutas de ataque potenciales.

Preguntas clave:
- ¿Podemos identificar cómo un atacante podría moverse dentro de nuestra red?
- ¿Entendemos qué activos podrían ser utilizados como punto de entrada?

REFLEXIÓN FINAL

Si tu organización se identifica con varias de estas señales, es probable que exista una exposición al riesgo mayor de la que actualmente se percibe.

La seguridad moderna no se trata únicamente de identificar vulnerabilidades. Se trata de entender qué tan expuesta está realmente la organización frente a un posible ataque.