Lecciones Aprendidas – Incidentes de Seguridad 2024 (Sede Barcelona)

Durante el año 2024, TechSys Solutions – sede Barcelona enfrentó múltiples incidentes relacionados principalmente con:

- Infecciones por troyanos recurrentes en distintos equipos.
- Problemas de sincronización en el servidor de MFA y correo electrónico.
- Accesos no autorizados provenientes de IPs externas.
- Fallos persistentes en copias de seguridad, VPN y controladores de red.

A partir del análisis de estos eventos, se destacan las siguientes lecciones aprendidas:

1. **Refuerzo de autenticación multifactor (MFA):** varios incidentes se relacionaron con errores o fallos en el servidor MFA. Se programó su actualización y revisión de configuración.
2. **Concienciación sobre ciberseguridad:** se detectó malware de tipo troyano en usuarios de distintos departamentos. Se fortalecieron las campañas internas de concienciación.
3. **Fortalecimiento del perímetro de red:** se observaron múltiples accesos sospechosos desde IP externas. Se reforzaron políticas de firewall y monitorización con SIEM.
4. **Revisión de procesos de backup:** algunos errores estaban relacionados con software de backup desactualizado. Se programaron auditorías técnicas y pruebas de restauración.
5. **Comunicación y escalado:** se identificaron diferencias en los tiempos de detección y resolución. Se mejoraron los canales de reporte y respuesta.

Lecciones Aprendidas – Incidentes de Seguridad 2025 (Sede Barcelona)

A lo largo de 2025, los incidentes de seguridad informática registrados en la sede de Barcelona reflejan tendencias similares al año anterior, con algunos cambios notables. Se identificaron los siguientes puntos clave:

1. **Persistencia de errores de configuración:** varios incidentes estuvieron relacionados con configuraciones incorrectas del servidor de correo, de MFA o de VPN. Esto resalta la necesidad de revisar y auditar configuraciones críticas de forma periódica.

2. **Mejora en la capacidad de respuesta:** los tiempos de resolución fueron más rápidos en comparación con 2024, lo cual sugiere una mayor madurez en la gestión operativa de incidentes y uso efectivo del SIEM.

3. **Reincidencia de infecciones por troyanos:** aunque menos frecuentes que el año anterior, las infecciones siguen presentes, lo cual indica que es necesario reforzar tanto las políticas de navegación como las actualizaciones del antivirus.

4. **Accesos no autorizados y MFA:** se repiten incidentes relacionados con accesos sospechosos desde IP externas y fallos en la autenticación multifactor. Se requiere revisar las políticas de geobloqueo, accesos remotos y autenticación avanzada.

5. **Conectividad y proveedores:** cortes recurrentes de conexión y errores relacionados con el proveedor de Internet sugieren la conveniencia de establecer medidas de contingencia adicionales (enrutamiento alternativo, redundancia o acuerdos SLA más exigentes).