LABORATORIO TEÓRICO – Mitigación de Riesgos en Ciberseguridad

Título:

Análisis y mitigación de riesgos ante amenazas de malware en entornos corporativos.

Identificación del riesgo

-Cuál es el riesgo principal?

El riesgo principal es la infección por ransomware que cifró archivos compartidos en la red, interrumpiendo el acceso al sistema de historias clínicas y afectando la operatividad de la empresa.

-Qué activos están comprometidos?

- Equipos conectados a la red institucional.
- Archivos compartidos en la red (específicamente historias clínicas).
- Sistema de historias clínicas (disponibilidad e integridad de los datos).

¿-tipo de amenaza representa este evento?

Es una amenaza de tipo malware (ransomware), que se propaga a través de un archivo ejecutable (.exe) descargado por error por un empleado.

-Qué vulnerabilidades se evidencian?

- Falta de capacitación en concienciación de seguridad para empleados.
- Ausencia de filtrado web o bloqueo de descargas de archivos ejecutables desde correos personales.
- Falta de segmentación de red para limitar el impacto del ransomware.
- Copias de seguridad no verificadas o accesibles durante el incidente.

Selección de controles de mitigación

Se proponen 4 controles, uno por categoría:

Preventivo:

Control: Implementar un firewall con filtrado web para bloquear descargas de archivos ejecutables (.exe) desde correos no corporativos.

Justificación: Evita la descarga inicial de malware.

Detectivo:

Control: Desplegar un sistema de detección de intrusos (IDS) para monitorear comportamientos anómalos en la red, como cifrado masivo de archivos.

Justificación: Permite identificar rápidamente actividades sospechosas.

Correctivo:

Control: Restaurar sistemas afectados mediante copias de seguridad automatizadas y verificadas, almacenadas fuera de la red principal.

Justificación: Minimiza el tiempo de recuperación y pérdida de datos.

Plan de implementación:

Capacitación obligatoria en ciberseguridad para empleados, enfocada en phishing y manejo seguro de correos.

- Tiempo: 2 semanas.
- Responsables: Recursos Humanos + Departamento de TI.

Plan de monitoreo

Indicadores:

- Número de alertas generadas por el IDS por semana.
- Tiempo de restauración de copias de seguridad en simulacros trimestrales.
- Número de empleados capacitados anualmente.

Frecuencia:

- Revisión semanal de alertas.
- Simulacros trimestrales de recuperación.

Herramientas:

Informes del IDS.

Plataformas de capacitación (ej. LMS).

Reflexión final

Efectividad de las medidas:

Los controles propuestos (firewall, IDS, copias de seguridad y capacitación) habrían mitigado el riesgo:

-El firewall habría bloqueado la descarga del .exe.

-La capacitación habría reducido la probabilidad de que el empleado descargara el archivo.

Medidas adicionales:

-Segmentación de red para aislar sistemas críticos (historias clínicas).

-Autenticación multifactor (MFA) para acceder a recursos compartidos.

-Simulacros de ransomware para evaluar la respuesta del equipo.

Conclusión:

en la prevención, detección y respuesta rápida es fundamental. La tecnología, capacitación y planes de contingencia reduce significativamente el impacto de amenazas similares.