Rigoberto Márquez

Laboratorio 14 – Escenarios de Riesgo

Sesión 14: Técnicas de Mitigación de Riesgos – Análisis de Casos Reales
Empresa: Prestech S.A.S.

1. Introducción

En este taller se abordan los conceptos clave sobre la gestión de riesgos, los tipos de controles de seguridad (preventivos, detectivos y correctivos), y se aplica una metodología práctica para mitigar riesgos mediante el análisis de casos reales.

Conceptos Clave:

- **Riesgo:** Posibilidad de que un evento impacte negativamente en los activos de la organización.
- **Controles de Mitigación:**
  - **Preventivos:** Buscan evitar el incidente (ej. firewall).
  - **Detectivos:** Identifican incidentes en tiempo real (ej. IDS).
  - **Correctivos:** Restauran sistemas después del incidente (ej. respaldos).

2. Contexto de la Empresa

Prestech S.A.S. es una empresa de préstamos en línea ubicada en Medellín, Colombia. Maneja datos sensibles de sus clientes como historiales crediticios, números de cuenta y documentos de identidad. Recientemente, Prestech sufrió un ataque de phishing que evadió su firewall mal configurado, comprometiendo varios correos corporativos.

- **Tamaño:** 120 empleados
- **Personal en TI y Seguridad:** 20 personas

3. Formación de Grupos

Los participantes se dividen en los siguientes grupos:

1. **Grupo de Seguridad de la Información**
2. **Grupo de Continuidad del Negocio**
3. **Grupo de Cumplimiento Normativo**

4. **Grupo de Capacitación**

4. Escenario Analizado – Grupo de Seguridad de la Información

Escenario de Riesgo:

Un ataque de phishing dirigido a empleados del área comercial permitió que los atacantes accedieran a cuentas corporativas. El firewall no detectó los correos maliciosos debido a una mala configuración.

Activos vulnerables:

- Cuentas de correo corporativas
- Información personal de clientes
- Sistema de solicitudes de préstamos

Amenazas:

- Phishing por correo electrónico
- Configuraciones erróneas en el firewall
- Falta de capacitación del personal

5. Controles de Mitigación Seleccionados

- **Reconfiguración del firewall con reglas avanzadas**
  Costo: $10.000.000 COP | Eficacia: Alta
- **Implementación de autenticación de dos factores (2FA) para el correo**
  Costo: $6.000.000 COP | Eficacia: Alta
- **Capacitación semestral contra phishing**
  Costo: $2.500.000 COP | Eficacia: Alta
- **Sistema de filtrado de correo**
  Costo: $7.000.000 COP | Eficacia: Alta

Total estimado: $25.500.000 COP

6. Plan de Implementación

Control	Responsable	Plazo
Reconfiguración de firewall	Equipo de TI	2 semanas
Activación de 2FA	Área de sistemas	10 días
Capacitación contra phishing	Recursos Humanos	Inmediata
Filtro de correo	Infraestructura TI	1 semana

Recursos necesarios:

- Equipo técnico especializado
- Proveedor externo de formación
- Presupuesto aprobado por gerencia

7. Monitoreo y Mejora

Indicadores Clave (KPIs):

- Cantidad de correos maliciosos bloqueados
- Número de empleados capacitados
- Incidentes posteriores al 2FA
- Tasa de detección del sistema de filtrado

Revisión Periódica:

- Firewall: revisión trimestral
- 2FA: verificación mensual
- Filtros de correo: pruebas semanales
- Capacitación: actualizaciones cada 6 meses

Mejoras Propuestas:

Si los ataques de phishing persisten, se evaluará la integración de soluciones de inteligencia artificial para detección avanzada y respuesta automatizada.

8. Resultados Presentados

- **Escenario:** Phishing exitoso por fallo en el firewall
- **Controles seleccionados:** Firewall, 2FA, filtro de correo, formación del personal
- **Implementación:** Ejecución dentro del primer mes
- **Monitoreo:** KPIs definidos y plan de revisión continua

9. Conclusiones del Taller

- La combinación de medidas técnicas y humanas ofrece mayor protección.
- La planificación, implementación y monitoreo son claves para una seguridad efectiva.
- La mejora continua es esencial frente a amenazas cambiantes.