Laboratorio #13

Roberto Blanco

Escaneo de vulnerabilidades

Documento: Solución de Casos según ISO 31000

CASO 1: Robo de credenciales por phishing en una entidad educativa

1. Activos críticos identificados:

- Sistema académico web.
- Credenciales de acceso de estudiantes y personal.
- Registros de notas y datos académicos.

2. Amenazas y vulnerabilidades:

- Amenaza: Ataque de phishing mediante correo fraudulento.
- Vulnerabilidades:
  - Falta de autenticación de dos factores (2FA).
  - Ausencia de filtros antispam y análisis de enlaces.
  - Usuarios sin capacitación en ciberseguridad.

3. Impacto y probabilidad:

- Impacto: Alto (modificación no autorizada de registros académicos).
- Probabilidad: Media-Alta (depende de la exposición a campañas de phishing).

4. Nivel de riesgo: Alto (impacto alto + probabilidad media-alta).

5. Riesgo aceptable: No.

6. Plan de tratamiento:

- Implementar autenticación de dos factores (2FA).
- Capacitar a usuarios en identificación de correos maliciosos.
- Instalar filtros antispam y herramientas de análisis de enlaces.
- Realizar simulaciones de phishing periódicas.

7. Responsables y tiempo estimado:

- Equipo de TI: 2 semanas para implementar 2FA.
- Área académica: 1 mes para capacitar a usuarios.

8. Mecanismos de monitoreo:

- Auditorías de acceso al sistema académico.

- Reportes mensuales de intentos de phishing detectados.

Conclusiones y recomendaciones:

- El riesgo es inaceptable debido al alto impacto en la integridad de los datos académicos.

- Se recomienda priorizar la implementación de 2FA y capacitación continua para mitigar el riesgo.

CASO 2: Ransomware en una clínica odontológica

1. Activos críticos identificados:

- Archivos clínicos (historias médicas).

- Datos financieros y administrativos.

- Estaciones de trabajo y servidores.

2. Amenazas y vulnerabilidades:

- Amenaza: Infección por ransomware mediante archivo adjunto malicioso.

- Vulnerabilidades:

  - Software antivirus desactualizado.

  - Falta de copias de seguridad automáticas.

  - Red no segmentada (propagación rápida del ransomware).

3. Impacto y probabilidad:

- Impacto: Crítico (pérdida de acceso a datos clínicos y operativos).

- Probabilidad: Media (si no se filtran correos maliciosos).

4. Nivel de riesgo: Alto (impacto crítico + probabilidad media).

5. Riesgo aceptable: No.

6. Plan de tratamiento:

- Actualizar software antivirus y parches de seguridad.

- Implementar copias de seguridad automáticas y cifradas.

- Segmentar la red para limitar la propagación de malware.

- Establecer políticas de restauración de backups.

7. Responsables y tiempo estimado:

- Equipo de TI: 1 mes para implementar backups y segmentación.

8. Mecanismos de monitoreo:

- Alertas de intrusiones en tiempo real.

- Pruebas trimestrales de restauración de backups.

Conclusiones y recomendaciones:

- El riesgo es crítico debido a la dependencia de los datos clínicos.

- Se debe priorizar la segmentación de red y backups automáticos para garantizar la continuidad operativa.

CASO 3: Acceso no autorizado a cámara IP de una empresa

1. Activos críticos identificados:

- Cámaras IP de vigilancia.

- Transmisiones de video en tiempo real.

2. *Amenazas y vulnerabilidades:

- Amenaza: Acceso remoto no autorizado a las cámaras.

- Vulnerabilidades:

  - Contraseñas predeterminadas ("admin/admin").

  - Firmware desactualizado con vulnerabilidades conocidas.

  - Uso de HTTP sin cifrado (no HTTPS).

3. Impacto y probabilidad:

- Impacto: Alto (violación de privacidad y seguridad física).

- Probabilidad: Alta (explotación de vulnerabilidades conocidas).

4. Nivel de riesgo: Alto (impacto alto + probabilidad alta).

5. Riesgo aceptable: No.

6. Plan de tratamiento:

- Cambiar contraseñas predeterminadas por credenciales robustas.

- Actualizar firmware de las cámaras.

- Habilitar HTTPS para acceso remoto seguro.

- Configurar logs de acceso y alertas de intrusiones.

7. Responsables y tiempo estimado:

- Equipo de seguridad: 1 semana para actualizar contraseñas y firmware.

8. Mecanismos de monitoreo:

- Revisión semanal de logs de acceso.
- Escaneo mensual de vulnerabilidades.

Conclusiones y recomendaciones:

- El riesgo es inaceptable debido a la exposición de video vigilancia.
- Se debe actualizar inmediatamente el firmware y eliminar contraseñas predeterminadas.

CASO 4: Uso indebido de información personal en una alcaldía

1. Activos críticos identificados:

- Bases de datos con información personal de ciudadanos.

2. Amenazas y vulnerabilidades:

- Amenaza: Acceso malintencionado por parte de contratistas.
- Vulnerabilidades:
  - Falta de registros de auditoría (logs).
  - Privilegios de acceso no gestionados.
  - Ausencia de políticas de clasificación de datos.

3. Impacto y probabilidad:

- Impacto: Alto (violación de privacidad y posibles sanciones legales).
- Probabilidad: Media (depende de controles internos).

4. Nivel de riesgo: Alto (impacto alto + probabilidad media).

5. Riesgo aceptable: No.

6. Plan de tratamiento:

- Implementar sistema de logs y auditoría de accesos.
- Establecer políticas de clasificación de datos (ej.: confidencial, público).
- Firmar acuerdos de confidencialidad con contratistas.
- Aplicar principio de mínimo privilegio en accesos.

7. Responsables y tiempo estimado:

-Área legal y TI: 2 meses para implementar políticas y auditoría.

8. Mecanismos de monitoreo:

- Alertas por accesos inusuales a bases de datos.

- Auditorías trimestrales de cumplimiento.

Conclusiones y recomendaciones:

- El riesgo es inaceptable por el incumplimiento de normativas de protección de datos.

- Se recomienda priorizar la auditoría de accesos y capacitación en manejo de datos sensibles.

CASO 5: Corte de servicio por ataque DoS a sitio web institucional

1. Activos críticos identificados:

- Servidor web institucional.

- Plataforma de inscripciones en línea.

2. Amenazas y vulnerabilidades:

- Amenaza: Ataque de denegación de servicio (DoS).

- Vulnerabilidades:

  - Ausencia de Web Application Firewall (WAF).

  - Servidor sobrecargado y sin redundancia.

  - Falta de monitoreo en tiempo real.

3. Impacto y probabilidad:

- Impacto: Alto (interrupción de servicios críticos durante horas).

- Probabilidad: Media-Alta (depende de la exposición en internet).

4. Nivel de riesgo: Alto (impacto alto + probabilidad media-alta).

5. Riesgo aceptable: No.

6. Plan de tratamiento:

- Implementar WAF y protección contra DoS.

- Configurar alta disponibilidad (balanceo de carga).

- Establecer monitoreo en tiempo real del tráfico.

- Crear protocolo de respuesta a incidentes.

7. Responsables y tiempo estimado:

- Equipo de TI: 3 semanas para implementar WAF y redundancia.

8. Mecanismos de monitoreo:

- Alertas de tráfico inusual.

- Pruebas de estrés semestrales.

Conclusiones y recomendaciones:

- El riesgo es alto debido a la dependencia del sitio web para procesos académicos.

- Se debe invertir en infraestructura resiliente y capacitar al personal en respuesta a incidentes.

Recomendaciones Generales

1.Capacitación continua:

- Todos los casos destacan la necesidad de concienciación en ciberseguridad para usuarios y empleados.

2.Monitoreo proactivo:

- Implementar herramientas de detección temprana (SIEM, WAF, antivirus).

3. Actualizaciones y parches:

- Mantener software y firmware actualizados para mitigar vulnerabilidades conocidas.

4. Cumplimiento normativo:

- Alinear controles con ISO 27001, GDPR o NIST, según aplique.