Universidad Politécnica de San Luis Potosí

Ingeniería en Tecnologías de la Información

Actividad 02

Evaluación de servicios de seguridad en escenarios actuales

Alumna: Karina Mendoza Aguado

Matrícula: 179859

Asignatura: CNG V: Seguridad informática

Docente: Mtro. Servando López Contreras

San Luis Potosí, S.L.P.

1. Marco conceptual

La protección de la información dentro de organizaciones modernas exige modelos que permitan clasificar los incidentes y comprender su impacto. La recomendación ITU-T X.800 propone un conjunto de servicios de seguridad que sirven como referencia para identificar qué propiedad fundamental debe preservarse. Por su parte, el RFC 4949 aporta un vocabulario común que ayuda a describir amenazas y eventos de manera uniforme entre especialistas. Utilizar ambos marcos de forma conjunta facilita el análisis estructurado, la comunicación entre equipos técnicos y la definición de estrategias de mitigación acordes al riesgo.

2. Escenarios propuestos

Intrusión mediante malware en correo electrónico

Servicios afectados: autenticación, confidencialidad y disponibilidad. Descripción: un archivo adjunto malicioso permite el acceso remoto al equipo de la víctima. Impacto: interrupción de operaciones y posible fuga de datos. Controles: filtros de correo, capacitación y respaldo frecuente.

Exposición accidental de almacenamiento en la nube

Servicios afectados: confidencialidad y control de acceso. Descripción: permisos mal asignados dejan información accesible públicamente. Impacto: riesgo legal y reputacional. Controles: auditorías automáticas y principio de mínimo privilegio.

Compromiso de proveedor de software

Servicios afectados: integridad. Descripción: una actualización distribuida incluye componentes alterados. Impacto: propagación masiva del incidente. Controles: verificación de firmas y monitoreo continuo.

Campaña de ingeniería social

Servicios afectados: autenticación. Descripción: usuarios entregan credenciales en sitios falsos. Impacto: accesos indebidos a recursos internos. Controles: MFA y programas de concientización.

Borrado intencional de información crítica

Servicios afectados: disponibilidad e integridad. Descripción: después de obtener privilegios elevados, el atacante elimina activos clave. Impacto: recuperación lenta o imposible. Controles: copias offline y segregación de funciones.

3. Conclusiones

Los servicios definidos por X.800 continúan siendo una guía útil para determinar la naturaleza del daño en incidentes contemporáneos. Complementariamente, la terminología del RFC 4949 favorece reportes claros y comparables. La adopción de estas referencias permite fortalecer la gestión de riesgos y mejorar la toma de decisiones en ambientes reales.