ACTIVIDAD 02 Análisis de servicios de seguridad (X.800 y RFC 4949).

Edgar Omar Rodriguez Hernandez.

177888.

Seguridad informática

UPSLP.

Servando López Contreras.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

ESCENARIO 1

Elemento	Respuesta
Servicios X.800 comprometidos.	**Confidencialidad:** Por la exfiltración de datos sensibles. **Integridad:** Por la alteración (cifrado) no autorizado de los archivos. **Disponibilidad:** Por el bloqueo de acceso a los servidores y sistemas críticos.
Definición(es) aplicable(s) RFC 4949.	**Multi-stage attack:** Serie de acciones dirigidas que se ejecutan en pasos sucesivos para lograr un objetivo. **Data breach:** Entrada no autorizada en un sistema que resulta en la pérdida o exposición de datos. **Availability attack:** Acción que impide a los usuarios autorizados acceder a los servicios del sistema. **Exfiltration:** Transferencia no autorizada de datos desde dentro de un sistema hacia un destino externo.
Tipo de amenaza.	Externa, intencionada y persistente (Grupo de ciberdelincuencia organizada).
Vector de ataque.	Acceso inicial no autorizado seguido de movimiento lateral y exfiltración de datos.
Impacto técnico / operativo.	Pérdida total de control sobre los activos de información, interrupción de la continuidad del negocio y daño reputacional por la amenaza de publicación de datos.
Medida de control recomendada.	Implementación de respaldos inmutables, despliegue de soluciones EDR/XDR para detección temprana, y una arquitectura de Zero Trust para limitar el movimiento lateral.

ESCENARIO 2

Elemento	Respuesta
Servicios X.800 comprometidos.	**Confidencialidad:** El servicio principal afectado, ya que los datos quedaron expuestos a terceros no autorizados. **Control de acceso:** Fallo en los mecanismos que restringen quién puede ver o usar los recursos.
Definición(es) aplicable(s) RFC 4949.	**Misconfiguration:** Error en la configuración de un sistema que debilita o anula sus controles de seguridad. **Exposure:** Incidente de seguridad en el que datos sensibles se vuelven disponibles para personas que no tienen autorización para acceder a ellos. **Data Leak:** Liberación accidental de información privada hacia un entorno externo.
Tipo de amenaza.	Interna y accidental (derivada de un error humano o de gestión por parte del administrador).
Vector de ataque.	Falta de controles de seguridad en servicios de almacenamiento y ausencia de auditorías de configuración.
Impacto técnico / operativo.	Filtración masiva de bases de datos, vulnerabilidad ante el cumplimiento de leyes de protección de datos y pérdida de confianza del cliente.
Medida de control recomendada.	Implementación de herramientas de Cloud Security Posture Management (CSPM), automatización de políticas de "Denegar por defecto" y auditorías de seguridad periódicas.

ESCENARIO 3

Elemento	Respuesta
Servicios X.800 comprometidos.	**Integridad:** El software original fue alterado con código malicioso antes de su distribución. **Confidencialidad:** El acceso no autorizado posterior permitió la extracción de datos sensibles. **Autenticación:** Se vulneró la confianza en la identidad del proveedor y la validez de la firma digital.
Definición(es) aplicable(s) RFC 4949.	**Supply chain attack:** Ataque que aprovecha las vulnerabilidades en la cadena de suministro de un producto para comprometer a sus usuarios finales.

	Malicious logic: Código (como un caballo de Troya) insertado deliberadamente para realizar funciones no autorizadas. **Trust relationship:** Relación en la que un sistema depende de otro para decisiones de seguridad o legitimidad.
Tipo de amenaza.	Externa e intencionada.
Vector de ataque.	Inyección de código malicioso en el ciclo de vida de desarrollo de software (SDLC) o compromiso de los servidores de actualización del proveedor.
Impacto técnico / operativo.	Ejecución de código arbitrario en cientos de redes corporativas simultáneamente y ruptura total del modelo de confianza en software firmado.
Medida de control recomendada.	Implementación de análisis de composición de software (SCA), verificación rigurosa de hashes en entornos aislados y segmentación de red para limitar el impacto de actualizaciones comprometidas.

ESCENARIO 4

Elemento	Respuesta
Servicios X.800 comprometidos.	**Autenticación:** Se vulneró la seguridad al suplantar la identidad de usuarios legítimos mediante credenciales robadas. **Control de acceso:** El sistema permitió la entrada y el movimiento de sujetos que no eran los propietarios reales de las cuentas.
Definición(es) aplicable(s) RFC 4949.	**Credential compromise:** Situación en la que los datos de autenticación (como contraseñas) son conocidos por un atacante. **Authentication failure:** En este contexto, una falla conceptual donde el sistema acepta una identidad falsa como válida. **Phishing:** Técnica de ingeniería social para engañar a los usuarios y obtener su información sensible.
Tipo de amenaza.	Externa e intencionada (con uso de credenciales válidas para evadir defensas perimetrales).
Vector de ataque.	Ingeniería social (Phishing) para la obtención de credenciales y posterior inicio de sesión en sistemas corporativos expuestos.
Impacto técnico / operativo.	Acceso persistente no detectado, posible exfiltración silenciosa de datos y compromiso de la integridad de los registros de acceso.

Medida de control recomendada.	Implementación de MFA (Autenticación de Múltiples Factores) robusto, monitoreo de comportamiento de usuarios y políticas de Conditional Access.

ESCENARIO 5

Elemento	Respuesta
Servicios X.800 comprometidos.	**Disponibilidad:** El daño principal, al eliminarse la única vía de recuperación de los sistemas productivos. **Integridad:** Los datos de respaldo fueron alterados o borrados de forma no autorizada.
Definición(es) aplicable(s) RFC 4949.	**Data destruction:** Alteración o eliminación deliberada de datos para que ya no sean legibles o recuperables. **Availability attack:** Acción que impide o inhibe el uso o gestión legítima de los recursos de información. **Ransomware:** Tipo de malware que utiliza criptografía para retener datos como "rehén" a cambio de un pago.
Tipo de amenaza.	Externa, intencionada y de alto impacto.
Vector de ataque.	Movimiento lateral con escalada de privilegios administrativos para acceder a las consolas de gestión de copias de seguridad.
Impacto técnico / operativo.	Incapacidad de recuperación ante desastres, pérdida permanente de activos digitales y paralización indefinida de la operación.
Medida de control recomendada.	Implementación de la regla de respaldo 3-2-1 con al menos una copia fuera de línea (offline) o inmutable, y segregación estricta de privilegios para la administración de backups.

ESCENARIO 6

Elemento	Respuesta
Servicios X.800 comprometidos.	**Confidencialidad:** Se vulneró al exponer datos privados a terceros no autorizados.

	Control de acceso: Fallo en la restricción de privilegios, permitiendo que el usuario realizara acciones más allá de sus necesidades laborales.
Definición(es) aplicable(s) RFC 4949.	**Insider threat:** Una entidad con acceso legítimo que utiliza dicho acceso para dañar el sistema o la organización. **Data Exfiltration:** El retiro no autorizado de información sensible de un sistema. **Privilege Abuse:** Uso deliberado de privilegios de acceso para fines distintos a los autorizados.
Tipo de amenaza.	Interna e intencionada.
Vector de ataque.	Abuso de privilegios legítimos preexistentes y falta de controles de salida de datos.
Impacto técnico / operativo.	Pérdida de propiedad intelectual, exposición de datos de clientes y posibles sanciones legales masivas por incumplimiento de custodia.
Medida de control recomendada.	Aplicación del Principio de Mínimo Privilegio (PoLP), implementación de soluciones DLP (Data Loss Prevention) y monitoreo de comportamiento mediante UEBA.

ESCENARIO 7

Elemento	Respuesta
Servicios X.800 comprometidos.	**Integridad:** Los registros (logs) fueron modificados o eliminados, perdiendo su veracidad. **No repudio:** Al perderse la evidencia, un atacante o usuario puede negar haber realizado las acciones.
Definición(es) aplicable(s) RFC 4949.	**Audit trail:** Un registro cronológico de las actividades del sistema que permite reconstruir eventos. **Evidentiary integrity:** La seguridad de que la evidencia digital no ha sido alterada y es admisible. **Anti-forensics:** Técnicas usadas para omitir, corromper o engañar a las herramientas de análisis forense.

Tipo de amenaza.	Externa o interna, intencionada.
Vector de ataque.	Escalada de privilegios para obtener permisos de escritura/borrado sobre los archivos de log del sistema o de la aplicación.
Impacto técnico / operativo.	Incapacidad de realizar un análisis de causa raíz, pérdida de validez legal de las pruebas y dificultad para determinar el alcance real de la intrusión.
Medida de control recomendada.	Implementación de Centralized Logging (SIEM) con transferencia de logs en tiempo real y uso de almacenamiento de solo lectura para registros críticos.

ESCENARIO 8

Elemento	**Respuesta**
Servicios X.800 comprometidos.	**Disponibilidad:** El servicio fue interrumpido de manera masiva, impidiendo el acceso legítimo a los recursos del sistema.
Definición(es) aplicable(s) RFC 4949.	**Operational failure:** Un evento interno donde un sistema no realiza su función debido a errores en procesos o configuración. **Service Outage:** Interrupción del servicio que hace que los recursos no estén disponibles para los usuarios. **Reliability:** La propiedad de un sistema de comportarse de manera consistente según sus especificaciones.
Tipo de amenaza.	Interna y accidental (Falla técnica o error humano en la implementación).
Vector de ataque.	Proceso de despliegue defectuoso y carencia de pruebas de regresión en entornos controlados.
Impacto técnico / operativo.	Caída global de servicios, interrupción de la continuidad del negocio y posible corrupción de datos por cierres inesperados de procesos.

Medida de control recomendada.	Implementación de Planes de Rollback automáticos, despliegues escalonados y protocolos de QA (Quality Assurance) más estrictos.

ESCENARIO 9

Elemento	Respuesta
Servicios X.800 comprometidos.	**Autenticación:** Se vulnera la identidad de la entidad legítima mediante suplantación. **Confidencialidad:** La información sensible de los ciudadanos es recolectada por terceros no autorizados.
Definición(es) aplicable(s) RFC 4949.	**Masquerade:** Una entidad se hace pasar por otra para obtener privilegios o acceso no autorizado. **Phishing:** Engaño mediante comunicaciones electrónicas que parecen provenir de una fuente confiable. **Social Engineering:** Manipulación de personas para que realicen acciones o divulguen información confidencial.
Tipo de amenaza.	Externa e intencionada (Fraude digital).
Vector de ataque.	Replicación de sitios web, correos electrónicos falsos y uso de dominios similares.
Impacto técnico / operativo.	Robo masivo de identidad, compromiso de credenciales de ciudadanos y pérdida de reputación/confianza en las instituciones oficiales.
Medida de control recomendada.	Implementación de protocolos de autenticación de correo, uso de certificados SSL/TLS con validación extendida y campañas de concientización en ciberseguridad.

ESCENARIO 10

Elemento	Respuesta
Servicios X.800 comprometidos.	**Confidencialidad:** Por la exfiltración previa de datos. **Integridad:** Por la alteración y borrado deliberado de archivos del sistema.

	Disponibilidad: Por la destrucción total de los activos, dejando los sistemas inoperativos.
Definición(es) aplicable(s) RFC 4949.	**Destructive attack:** Ataque diseñado para dañar, destruir o denegar el uso de recursos informáticos. **Wiper:** Tipo de malware cuyo único objetivo es borrar el disco duro de la víctima. **Anti-forensics:** Acciones ejecutadas para eliminar rastros (logs, registros) y dificultar la investigación.
Tipo de amenaza.	Externa e intencionada.
Vector de ataque.	Explotación de vulnerabilidades para obtener privilegios de superusuario (root/admin) y ejecución de scripts de borrado masivo.
Impacto técnico / operativo.	Destrucción irreversible de la infraestructura digital, pérdida total de datos y rastro forense, y cese completo de actividades.
Medida de control recomendada.	Implementación de segmentación de red (microsegmentación), monitoreo de integridad de archivos en tiempo real y mantenimiento de backups inmutables fuera del dominio principal.

Conclusión

Haber analizado estos escenarios muestra que la SI requiere un doble enfoque, el ITU-T X.800 sirve de mapa para identificar qué reglas de seguridad han sido violentadas, el RFC 4949 nos da el lenguaje técnico exacto para explicar cómo es que ocurrió el ataque. Al combinar ambos, se pueden dar explicaciones más profesionales y precisas y no tan generales, esto también nos ayuda mucho al momento de documentarlo.

Bibliografías

https://datatracker.ietf.org/doc/html/rfc4949