UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

CARRERA: INGENIERIA EN TECNOLOGIAS DE LA INFORMACION

MATERIA: Seguridad informática

Actividad 2

PARCIAL: 1

Rodriguez Moreno Cristian Alejandro/ Matrícula:181641

Profesor: Servando López Contreras

Fecha de entrega: 27 de enero de 2026

Introducción

El presente trabajo nos habla sobre dos estándares que son fundamentales para entender la seguridad informática hoy en día, pues nos ayudan a comprender qué es lo que pasa realmente cuando ocurre un incidente. Por una parte, tenemos el modelo X.800, el cual nos indica los servicios de seguridad que debemos proteger, como la confidencialidad o la integridad; y por otra parte, utilizamos el RFC 4949, que funciona como un diccionario técnico para ponerle el nombre exacto a cada amenaza. Esto es muy importante, pues al analizar los incidentes me di cuenta de que muchas veces confundimos los términos o no sabemos explicar el impacto real. Entonces, el objetivo de esta actividad es aprender a identificar bien qué servicio falló y usar la terminología correcta del RFC, para así poder documentar vulneraciones en contextos reales de forma profesional.

Una vez explicado el contexto de los estándares, a continuación se muestra la tabla con el análisis detallado de cada escenario.

	Servicios de X.800 comprometidos	Definición(es) aplicable(es) RFC 4949	Tipo de amenaza.	Vector de ataque	Impacto Técnico/ Operativo.	Medida de control recomendada
1	Confidencialidad, Integridad y Disponibilidad.	Nos habla sobre un Ransomware que causó un Data Breach y también un Availability attack.	Externa (Maliciosa).	Pues todo comenzó con la explotación de una vulnerabilidad y luego ejecutaron el malware para cifrarlo todo.	El impacto fue que se pararon las operaciones y se filtraron datos, entonces la reputación de la empresa quedó muy mal.	Se recomienda tener respaldos inmutables y segmentar la red para que no pase a mayores.
2	Confidencialidad y Control de Acceso.	Aquí se trata de una Misconfiguration que provocó una Exposure de los datos.	Interna (Error humano).	Fue un error al configurar los permisos en la nube, pues cualquiera podía entrar a ver los archivos.	Se perdió la privacidad de los datos masivamente y pues eso trae problemas legales fuertes aunque no hackearan nada.	Hay que auditar las configuraciones seguido y cifrar los datos para evitar que se vean.
3	Integridad y Autenticación de origen.	El RFC nos define esto como un Supply Chain Attack y uso de Malicious Logic.	Externa (Indirecta).	Los atacantes infectaron el software original del proveedor antes de que le llegara al cliente.	Afectó a muchas empresas que confiaban en el proveedor, entonces el daño fue crítico porque nadie sospechaba.	Se debe verificar el hash de los archivos y vigilar a los proveedores siempre.
4	Autenticación y Control de Acceso.	Es un Credential Compromise mediante Phishing, lo que causó un Unauthorized Access.	Externa (Ingeniería Social).	Comenzó con correos falsos para robar las contraseñas, pues los usuarios pensaron que eran reales.	Los atacantes estuvieron dentro sin que nadie se diera cuenta, robando información poco a poco.	Activar el doble factor (MFA) para que aunque tengan la clave, no puedan entrar.
5	Disponibilidad e Integridad.	Aquí nos habla de Data Destruction y	Externa (Destructiva).	Se metieron hasta los servidores de respaldo para	Pues la empresa no se pudo recuperar	Tener respaldos fuera de línea (offline) para

		un Availability Attack intencional.		borrarlos antes de soltar el ataque principal.	y perdió toda su información, fue algo catastrófico para el negocio.	que nadie los pueda tocar remotamente.
6	Confidencialidad y Control de Acceso.	Se define como Insider Threat y hubo un Misuse of Privilege.	Interna (Intencional).	El empleado aprovechó que tenía permisos legítimos para sacar la información y venderla.	Se fugaron datos sensibles y nadie sospechó nada porque el acceso parecía normal en el sistema.	Monitorear lo que hacen los usuarios y dar solo los permisos necesarios (Mínimo Privilegio).
7	No Repudio e Integridad.	Se trata de una falla en la Evidentiary Integrity y modificación del Audit Trail.	Interna o Externa.	Borraron los registros (logs) después de entrar para que no supieran quién fue ni qué hizo.	No se puede saber qué pasó ni culpar a nadie, entonces falla el análisis forense legal.	Mandar los logs a un servidor aparte en tiempo real para que no los puedan borrar.
8	Disponibilidad.	El RFC lo marca como Operational Failure y System Crash.	Interna (Error de proceso).	Una actualización salió mal y tumbó los servidores, pues no la probaron bien antes de lanzarla.	Se cayeron los servicios en todo el mundo y se perdió mucho dinero por estar parados tanto tiempo.	Probar bien las actualizaciones antes de lanzarlas a todos los equipos.
9	Autenticación y Confidencialidad.	Nos habla de Masquerade y Spoofing para engañar a la gente.	Externa (Engaño).	Crearon sitios web idénticos a los originales para que la gente se confiara y pusiera sus datos.	Los usuarios dieron sus datos pensando que era real, entonces les robaron su identidad y dinero.	Usar certificados válidos y enseñar a la gente a revisar bien las direcciones web.
10	Disponibilidad, Integridad y Confidencialidad.	Es un Destructive Attack usando herramientas tipo Wiper.	Externa (Ciberguerra).	Usaron un malware diseñado solo para borrar todo lo que encontraba a su paso en los discos duros.	Se destruyó todo el sistema y hubo que empezar desde cero, pues el daño fue total e irreversible.	Tener planes de recuperación ante desastres (DRP) bien ensayados para levantar el servicio.

Conclusión

Al terminar de analizar estos escenarios me puse a pensar en que muchas empresas se confían y cuando les llega un ataque no saben qué hacer. El problema es claro también aquí, pues los riesgos cambian todo el tiempo y hay que adaptarnos. El uso del RFC 4949 y el X.800 nos sirve para no solo decir "me hackearon", sino para entender técnicamente qué pasó, si fue la integridad o la disponibilidad lo que falló. En mi opinión, si aprendemos a usar bien estos términos, podremos defendernos mejor y aplicar controles reales, alejándonos del miedo a lo desconocido y actuando con más seguridad en el entorno laboral.

Bibliografía

International Telecommunication Union. (1991). Security Architecture for Open Systems Interconnection for CCITT Applications (X.800).

Shirey, R. (2007). Internet Security Glossary, Version 2 (RFC 4949). The Internet Society.