UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

Actividad 02

CNO V Seguridad Informática

Casos de estudio

Introducción

Este documento presenta diez escenarios de incidentes reales o posibles, mostrando cómo afectan aspectos clave como la confidencialidad, la integridad y la disponibilidad de los sistemas. A través de una tabla comparativa, se describen las amenazas, sus causas, el impacto que generan y las medidas de control que pueden aplicarse. El propósito es ofrecer una visión clara y práctica que ayude a comprender mejor los problemas de seguridad y cómo prevenirlos.

Escenario 01.

En múltiples incidentes atribuidos al grupo LockBit, organizaciones públicas y privadas han sufrido el cifrado masivo de servidores tras un acceso inicial no

autorizado. Antes de ejecutar el ransomware, los atacantes exfiltraron información sensible y posteriormente amenazaron con su publicación, evidenciando un

compromiso simultáneo de la confidencialidad, la integridad y la disponibilidad.

Desde el enfoque del RFC 4949, el incidente se clasifica como un multi-stage attack con data breach y availability attack, donde la indisponibilidad del sistema

es solo una fase final del daño. La ausencia de respaldos inmutables y de detección temprana permitió que el impacto fuera total.

Escenario 02.

En diversos casos documentados, bases de datos completas quedaron accesibles públicamente debido a errores de configuración en servicios de

almacenamiento en la nube. No existió una explotación técnica sofisticada, sino una falla en el control de acceso, lo que derivó directamente en la pérdida de

confidencialidad de los datos. El RFC 4949 describe este tipo de incidentes como misconfiguration y exposure, subrayando que la amenaza no siempre

implica malware o intrusión activa. El impacto suele ser legal y reputacional, aun cuando no se pueda demostrar acceso malicioso.

Escenario 03.

Un proveedor legítimo de software fue comprometido y distribuyó una actualización que incluía código malicioso, afectando a cientos de organizaciones que

confiaban en él. Este escenario refleja una violación grave de la integridad de los sistemas y, en muchos casos, de la confidencialidad, al permitir accesos no

autorizados posteriores. El RFC 4949 lo identifica como supply chain attack, destacando el abuso de relaciones de confianza. El daño es particularmente crítico

porque rompe el supuesto de legitimidad del software firmado.

Escenario 04.

Mediante campañas de phishing, atacantes obtuvieron credenciales válidas y accedieron a sistemas corporativos durante meses sin levantar alertas. Aunque la

autenticación funcionó técnicamente, el servicio de autenticación fue comprometido al basarse en credenciales robadas, afectando también el control de

acceso. Según el RFC 4949, se trata de un credential compromise con authentication failure conceptual, no técnica. La falta de MFA y de monitoreo de

comportamiento facilitó la persistencia del atacante.

Escenario 05.

En ataques de ransomware avanzados, los atacantes eliminaron o cifraron los respaldos antes de afectar los sistemas productivos. Este hecho compromete

directamente la disponibilidad y la integridad de la información, al impedir la recuperación. El RFC 4949 clasifica este comportamiento como data destruction

y availability attack, evidenciando intención deliberada de maximizar el daño. La inexistencia de respaldos offline o inmutables convierte el incidente en

catastrófico.

Escenario 06.

Un empleado con acceso legítimo extrajo bases de datos completas y las vendió a terceros, sin explotar vulnerabilidades técnicas. El servicio afectado fue

principalmente la confidencialidad, junto con fallas en el control de acceso por exceso de privilegios. El RFC 4949 define este escenario como insider threat,

destacando que el riesgo interno puede ser tan grave como el externo. La carencia de monitoreo y de políticas de mínimo privilegio fue determinante.

Escenario 07.

Tras un ataque, los registros del sistema quedaron cifrados o alterados, impidiendo reconstruir la secuencia de eventos. Esto compromete la integridad de los

datos y el no repudio, ya que no es posible demostrar qué ocurrió ni quién fue responsable. Desde el RFC 4949, se trata de una violación de evidentiary

integrity y del audit trail. El impacto no solo es técnico, sino también probatorio y legal.

Escenario 08.

Una actualización mal ejecutada provocó la caída simultánea de múltiples servicios críticos a nivel global. Aunque no existió un atacante, el servicio de

disponibilidad fue gravemente afectado. El RFC 4949 contempla estos eventos como operational failure, recordando que la seguridad también se ve afectada

por errores internos. La falta de pruebas previas y planes de reversión amplificó el impacto.

Escenario 09.

Atacantes replicaron sitios y correos oficiales para engañar a ciudadanos y obtener información sensible. Este escenario afecta la autenticación, al suplantar

identidades legítimas, y la confidencialidad de los datos recolectados. El RFC 4949 lo clasifica como masquerade y phishing, subrayando el componente de

ingeniería social. La ausencia de mecanismos de autenticación del dominio y de concientización facilitó el éxito del ataque.

Escenario 10.

En algunos incidentes, tras exfiltrar información, los atacantes ejecutaron acciones destructivas para borrar sistemas completos y eliminar rastros. Se produce

un compromiso total de la confidencialidad, la integridad y la disponibilidad, configurando uno de los peores escenarios posibles. El RFC 4949 describe este

patrón como destructive attack, donde el objetivo no es solo el lucro, sino el daño irreversible. La detección tardía impidió cualquier contención efectiva.

Análisis de servicios de seguridad

Escenario	Servicios X.800 comprometidos	Definiciones RFC 4949	Tipo de amenaza	Vector de ataque	Impacto técnico	Medida de control
01	Confidencialidad, Integridad, Disponibilidad	Multi-stage attack, Data breach, Availability attack	Externa (acceso no autorizado)	Ransomware, exfiltración	Impacto total por falta de respaldos inmutables y detección temprana	Respaldos inmutables, detección temprana, segmentación de red.
02	Confidencialidad	Misconfiguration, Exposure	Interna (error humano)	Falla de configuración en nube	Pérdida de confidencialidad , impacto legal y reputacional	Auditorías, revisión de permisos
03	Integridad, Confidencialidad	Supply chain attack	Externa (compromiso de proveedor)	Distribución de software malicioso	Violación de integridad y confidencialidad	Validación de firmas, control de versiones, monitoreo de integridad
04	Autenticación, Control de acceso	Credential compromise, Authentication failure	Externa (phishing)	Robo de credenciales válidas	Persistencia sin alertas, fallo conceptual de autenticación	MFA, monitoreo de comportamiento, alertas de acceso
05	Disponibilidad, Integridad	Data destruction, Availability attack	Externa (ransomware avanzado)	Eliminación de respaldos	Daño catastrófico, pérdida de recuperación	Respaldos offline/inmutables, detección proactiva
06	Confidencialidad, Control de acceso	Insider threat	Interna (empleado malicioso)	Venta de datos con acceso legítimo	Compromiso de confidencialidad y control de acceso	Políticas de mínimo privilegio, monitoreo, DLP
07	Integridad, No repudio	Evidentiary integrity, Audit trail	Externa (ataque destructivo)	Alteración/cifrado de logs	Pérdida de no repudio, impacto técnico y legal	Protección de logs, almacenamiento seguro, monitoreo continuo
08	Disponibilidad	Operational failure	Interna (error de actualización)	Actualización mal ejecutada	Caída de servicios críticos	Pruebas previas, planes de reversión, gestión de cambios
09	Autenticación, Confidencialidad	Masquerade, Phishing	Externa (ingeniería social)	Suplantación de identidad	Robo de datos personales	Autenticación de dominio, capacitación, filtros antiphishing
10	Confidencialidad, Integridad, Disponibilidad	Destructive attack	Externa (ataque deliberado)	Exfiltración seguida de destrucción	Daño irreversible, compromiso total de CIA	Detección temprana, segmentación, respuesta ante incidentes

Conclusiones

En conclusión, los escenarios analizados muestran que los problemas de seguridad pueden tener distintos orígenes, desde errores humanos hasta ataques planeados, pero todos pueden afectar gravemente a las organizaciones. Más allá de la complejidad técnica, lo importante es reconocer que la prevención, la preparación y la respuesta rápida son claves para reducir el daño.

Referencias

Shirey, R. W. (2007). *RFC 4949: Internet Security Glossary, Version 2, IEFT*. Obtenido de datatracker: https://datatracker.ietf.org/doc/html/rfc4949

The International Telegraph and Telephone Consultative Commitee. (1991). Obtenido de Union Internacional de Telecomunicaciones: https://www.itu.int/rec/t-rec-x.800-199103-i/es