FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

CARRERA DE COMPUTACIÓN

MATERIA:

CRIPTOGRAFÍA Y SEGURIDAD DE LA INFORMACIÓN

DOCENTE:

ING. GIOVANNY MOCAYO

INTEGRANTES:

- Andino John
- Borja Diego
- Cajamarca Anthony
- Cruz Kevin
- Jami Mateo

TEMA:

Ejemplos de Ataques Reales a la Seguridad Empresarial

FECHA DE ENTREGA:

19 de enero del 2026

Caso 1: Ciberataque al Registro Civil del Ecuador

Fecha del incidente

El ataque fue detectado días antes del 29 de enero de 2025. La denuncia oficial se presentó el 28 de enero de 2025.

Nombre de la empresa / institución

Dirección General del Registro Civil, Identificación y Cedulación del Ecuador.

Ubicación geográfica de la empresa

Quito, provincia de Pichincha, Ecuador.

¿Qué fue lo que se afectó?

Se vio comprometida la disponibilidad de los servicios digitales, uno de los principios fundamentales de la seguridad de la información.

Las plataformas afectadas fueron la Agencia Virtual y el sitio web institucional, especialmente el sistema de agendamiento de turnos para cédulas y pasaportes, provocando interrupciones e imposibilidad temporal de acceso para los ciudadanos.

La vulnerabilidad estuvo asociada a una insuficiente capacidad de protección frente a tráfico masivo no legítimo, permitiendo la saturación de los servidores.

¿Qué técnica de explotación se usó?

Se utilizó un ataque de denegación de servicio distribuido (DDoS) de tipo volumétrico, basado en la generación de miles de solicitudes simultáneas desde múltiples direcciones IP ubicadas en el exterior (principalmente Brasil, México y Colombia), con el fin de colapsar los recursos del sistema.

¿Qué buena práctica de seguridad informática se recomienda implementar?

Se recomienda implementar mecanismos avanzados de mitigación de ataques DDoS, tales como:

- Firewalls de aplicaciones web (WAF).
- Sistemas de detección y mitigación de tráfico malicioso en tiempo real.
- Infraestructura escalable con balanceo de carga.
- Monitoreo continuo del tráfico de red.

Argumentación:

Los ataques DDoS afectan directamente la disponibilidad de servicios críticos. En una institución pública, la interrupción de plataformas digitales impacta derechos ciudadanos y la confianza en el Estado. La adopción de soluciones especializadas permite absorber picos de tráfico, identificar patrones anómalos y garantizar la continuidad operativa, reduciendo significativamente el impacto de este tipo de amenazas.

Referencia

[1] El Comercio, “Registro Civil denuncia presunto ciberataque a su Agencia Virtual,” ene. 2025. [En línea]. Disponible en: https://www.elcomercio.com/actualidad/seguridad/registro-civil-denuncia-presunto-ciberataque-agencia-virtual/

Caso 2: Ciberataque a Jaguar Land Rover

Fecha del incidente

El ciberataque fue detectado el 31 de agosto de 2025 y confirmado oficialmente el 2 de septiembre de 2025.

Nombre de la empresa

Jaguar Land Rover (JLR).

Ubicación geográfica de la empresa

Sede principal en el Reino Unido, con plantas afectadas en Solihull y Halewood (Reino Unido) y Nitra (Eslovaquia).

¿Qué fue lo que se afectó?

El ataque comprometió la disponibilidad de los sistemas logísticos e industriales, afectando directamente la cadena de suministro y provocando una paralización parcial de la producción.

La dependencia total de sistemas informáticos interconectados evidenció una vulnerabilidad crítica en la infraestructura tecnológica industrial y de proveedores.

¿Qué técnica de explotación se usó?

Aunque no se ha confirmado oficialmente, los expertos señalan que el vector de ataque más probable fue un ransomware, un tipo de malware que bloquea sistemas críticos para exigir un rescate económico, afectando tanto a la red interna como a los sistemas de proveedores estratégicos.

¿Qué buena práctica de seguridad informática se recomienda implementar?

Se recomienda fortalecer la seguridad de infraestructuras industriales (OT) y de la cadena de suministro, mediante:

- Segmentación de redes IT/OT.
- Sistemas de detección de intrusiones industriales (IDS).
- Actualizaciones seguras y gestión de parches.
- Cumplimiento de estándares internacionales como ISO/SAE 21434 y UNECE R155.
- Evaluaciones periódicas de seguridad a proveedores.

Argumentación:

La industria automotriz moderna depende de sistemas digitales altamente interconectados. Un ataque a un proveedor puede propagarse rápidamente y detener la producción global. Implementar estándares de seguridad industrial y controles en la cadena de suministro reduce la superficie de ataque, mejora la detección temprana de incidentes y minimiza el impacto económico y operativo de ciberataques de gran escala.

Referencia

[2] Cadena SER, “El ciberataque a las fábricas de Jaguar Land Rover deja la producción británica en mínimos,” oct. 2025. [En línea]. Disponible en: https://cadenaser.com/andalucia/2025/10/30/el-ciberataque-a-las-fabricas-de-jaguar-land-rover-deja-la-produccion-britanica-en-minimos-y-pone-en-evidencia-las-brechas-del-sector-ser-malaga/