REPORTE DE SEGURIDAD SOBRE INFRAESTRUCTURA CRÍTICA - 2020

Resumen Ejecutivo

Durante el año 2020, se registró un incremento significativo en los ataques dirigidos contra infraestructuras críticas, especialmente en el sector energético y en plantas de tratamiento de agua. Los atacantes han perfeccionado sus tácticas, técnicas y procedimientos (TTPs), haciendo uso de herramientas más sofisticadas y apuntando a vulnerabilidades que anteriormente no eran explotadas con frecuencia.

Capítulo 1: Panorama de Amenazas

Los grupos APT (Amenazas Persistentes Avanzadas) continúan siendo la principal amenaza para las infraestructuras críticas. Se identificaron campañas específicas lanzadas desde grupos como APT33 y APT41, que utilizaron vectores de entrada como spear-phishing dirigido y vulnerabilidades no parchadas en sistemas SCADA.

Además, se ha observado un notable aumento en el uso de ransomware industrial, capaz de paralizar las operaciones de una planta durante horas o días. El uso de redes privadas mal configuradas y la falta de segmentación entre entornos IT y OT siguen siendo los puntos débiles más explotados.

Capítulo 2: Casos de Estudio Relevantes

Caso 1 – Planta Hidroeléctrica en Sudamérica:
Un ataque que duró aproximadamente 13 horas comprometió múltiples sistemas de monitoreo. La intrusión se dio a través de una HMI accesible desde internet sin autenticación. Los atacantes pudieron controlar válvulas remotamente, aunque no causaron daños físicos. Se confirmó la presencia de scripts personalizados y persistencia mediante tareas programadas.

Caso 2 – Refinería en Asia:
En este incidente, los atacantes utilizaron ingeniería social para obtener acceso remoto a un servidor expuesto. A través de este acceso, escanearon la red interna, lograron moverse lateralmente y capturaron credenciales administrativas mediante ataques Pass-the-Hash.

Capítulo 3: Técnicas de Detección y Mitigación

Entre las herramientas más efectivas para detección temprana se encuentran sistemas de monitoreo continuo de red (NIDS), correlación de eventos mediante SIEM, y herramientas

de análisis de comportamiento. Se recomienda el uso de frameworks como MITRE ATT&CK for ICS para mapear tácticas y fortalecer la respuesta.

Un enfoque de defensa en profundidad es crítico. Esto incluye:

- Segmentación entre redes OT e IT
- Autenticación multifactor para sistemas críticos
- Revisión constante de logs y telemetría
- Pruebas de penetración regulares por equipos especializados

---

Capítulo 4: Recomendaciones Estratégicas

Los expertos recomiendan adoptar políticas de seguridad basadas en riesgo y realizar simulaciones de respuesta a incidentes al menos una vez por trimestre. También se sugiere implementar políticas Zero Trust en todos los accesos remotos.

Las empresas deben mantener inventarios de activos actualizados, desactivar protocolos inseguros como SMBv1, y fomentar una cultura de seguridad dentro de toda la organización.

> **Nota curiosa:** Algunas capas no están hechas solo de datos. A veces hay mensajes que esperan ser descubiertos.
> flag: CTF{archivo-manipulado-con-proposito}

Apéndice A: Herramientas Recomendadas

Las siguientes herramientas se consideran esenciales en un entorno industrial moderno:

- Zeek (monitoreo de tráfico de red)
- Wireshark (análisis de paquetes)
- OSSEC (detección de intrusiones basada en host)
- Splunk (correlación de eventos)
- Snort y Suricata (detección basada en firmas)
- Ansible (automatización de tareas de parcheo)

Apéndice B: Indicadores de Compromiso (IoCs)

A continuación se enlistan algunos indicadores encontrados en campañas recientes:

- 103.91.120.5 – Comando y control identificado
- /admin/upload.php – Ruta utilizada para subida de payloads
- SHA256: 98d3b78287bfa021defae716bdceff72f1d20a1a0cc6a92db3cb1d828b299a7d – Binario sospechoso
- User-Agent: “Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0”

Apéndice C: Referencias Normativas y Guías

- NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security
- IEC 62443: Industrial communication networks – IT security for networks and systems
- CISA ICS Advisory Library
- ISO/IEC 27019: Security for process control systems

Fin del Documento