

La ciberseguridad en el Sector Energético

OBJETIVOS

Las organizaciones dedicadas a la generación de energías verdes, de origen fósil o de origen nuclear forman la primera etapa de un proceso en el que intervienen otros muchos actores dedicados a la refinería, al transporte, al almacenamiento y a la comercialización de la energía. El sector representa el 2,5% del PIB y es uno de los más ciberatacados en la actualidad debido, principalmente, a su importancia como infraestructura crítica.

RETOS

El equipamiento industrial empieza a encontrarse obsoleto. Sus altos periodos de amortización obligan a las organizaciones a estirar su vida útil, manteniendo sistemas de control industrial (ICS), Scadas, HMIs, PLCs, sensores y demás activos OT fuera de soporte y vulnerables ante amenazas ya resueltas como Wannacry. La creciente interconexión de estos dispositivos, la expansión de las tecnologías IIoT, la digitalización del sector en general, amplían los vectores de ataque. La protección de los datos de los clientes finales de las comercializadoras se vuelve crucial, enfrentándose al desafío de garantizar la seguridad de la información sensible de los usuarios, que incluye datos personales y transacciones financieras, exponiendo a las organizaciones ante nuevas brechas de seguridad.

SOLUCIONES

NIS2, GDPR, el ENS o la Ley PIC, son algunas de las leyes y regulaciones que afectan al sector. Zerolynx diseña, implanta, mantiene y opera planes integrales de ciberseguridad basados en las seis funciones del NIST (Gobierno, Identificación, Protección, Detección, Respuesta y Recuperación).

BENEFICIOS

Identificación y detección

Mediante nuestros servicios de ciberinteligencia y hacking ético ofrecemos una solución integral, vigilamos, detectamos y reportamos todo tipo de riesgos, como, por ej. datos confidenciales expuestos o vulnerabilidades severas, asegurando la infraestructura y datos sensibles.

Protección y respuesta

Mediante nuestros servicios de ciberdefensa y DFIR protegemos la superficie de ataque de su institución, asegurando la continuidad de sus operaciones y la mitigación efectiva de amenazas.

CIFRAS CLAVE

- El **60%** de los sistemas **Sistema de Control Industrial (ICS)** se encuentran conectados y, un **32%**, se encuentran conectados directamente a **Internet sin medidas de ciberseguridad** adicionales.
- El **90%** de los **ICS del sector energético** han sufrido algún tipo de **brecha de seguridad**.
- El **30%** **ciberincidentes** del último año provocaron la **pérdida de servicio**.



"Contar con Zerolynx como expertos técnicos para las auditorías internas de Ciberseguridad que realizamos en el Grupo Exolum nos ha permitido aportar valor a la organización identificando nuestras áreas de mejora, y contribuir al refuerzo de la Ciberseguridad de los sistemas corporativos en las áreas de IT/OT y procesos verificados"

Gema Hernández
Subdirectora de Auditoría y Compliance
de Exolum Corporation

REFERENCIAS DESTACADAS

