ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Cybersecurity in the **Energy** Sector

OVERVIEW

Organizations dedicated to the generation of green energy, fossil-based energy, or nuclear energy form the initial stage of a process involving many other actors in refining, transportation, storage, and energy marketing. The sector represents 2% of EU GDP and is one of the most targeted by cyberattacks today, primarily due to its significance as critical infrastructure.

CHALLENGES

Industrial equipment is beginning to become obsolete. High amortization periods force organizations to extend their lifespan, maintaining industrial control systems (ICS), SCADA, HMIs, PLCs, sensors, and other OT assets that are unsupported and vulnerable to threats already addressed, such as Wannacry. The increasing interconnection of these devices, the expansion of IIoT technologies, and the overall digitization of the sector extend the attack vectors. Protecting the data of end customers of energy providers becomes crucial, facing the challenge of ensuring the security of sensitive user information, including personal data and financial transactions, exposing organizations to new security breaches.

SOLUTIONS

NIS2, GDPR, National Security Frameworks, or the Act on the Protection of Critical Infrastructure are some of the laws and regulations affecting the sector. Zerolynx designs, implements, maintains, and operates comprehensive cybersecurity plans based on the six areas of NIST (Govern, Identify, Protect, Detect, Respond, and Recover).

BENEFITS

Identification and Detection

Through our cyber intelligence and ethical hacking services, we offer a comprehensive solution, monitoring, detecting, and reporting various risks, such as exposed confidential data or severe vulnerabilities, ensuring the security of infrastructure and sensitive data.

Protection and Response

Our cybersecurity and DFIR (Digital Forensics and Incident Response) services safeguard your institution's attack surface, mitigate and respond to any threat, minimizing the impact on public services.

KEY FIGURES

- **60% of Industrial Control Systems (ICS)** are connected, and **32% are directly connected to the Internet** without additional cybersecurity measures.
- **90% of ICS** in the energy sector have experienced some form of **security breach**.
- **30% of cyber incidents** in the last year resulted in **service loss**.

"Having Zerolynx as technical experts for the internal cybersecurity audits, we conduct at the Exolum Group has allowed us to bring value to the organization by identifying areas for improvement and contributing to the strengthening of cybersecurity in corporate systems in both IT/OT and verified processes"

Gema Hernández
Deputy Director of Audit and Compliance at Exolum Corporation

TOP REFERENCES

Naturgy · RED ELÉCTRICA DE ESPAÑA · exolum

ABOUT ZEROLYNX

European Cybersecurity and Intelligence Provider.
Global Top 100 Providers ranked 2023.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE