Cybersecurity in the Telecommunications Sector

ZEROLYNX | **OSANE CONSULTING** A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

KEY FIGURES

- The **Telecommunications** Sector accounted for **10% of cyber incidents last year.**

- The **average time** for a cybercriminal to **access a system** was **1 hour and 24 minutes.**

- **43% of cyber attacks** on the **Telecommunications** sector were carried out by **organized groups**.

OVERVIEW

The Telecommunications Sector faces constant challenges in a dynamic and ever-evolving environment. The rapid expansion of emerging technologies like 5G, the demand for increasingly robust and costly infrastructures, and cybersecurity are central concerns for a heavily regulated business with fierce competition.

CHALLENGES

As critical infrastructure, companies in the sector face constant and highly complex challenges. The cybersecurity of 5G, 4G, VoLTE, or LTE networks, and the supporting infrastructures under frameworks and protocols like IMS or SIP, requires in-depth technical knowledge and market understanding. The growing interconnection of all these elements, the expansion of IIoT technologies, and the inherent digitization in the sector itself are increasing the attack surface, raising the chances that cybercriminals could identify a vulnerability to exploit. MVNOs must protect customer data and prevent fraud in service activation. This is essential for maintaining customer trust and compliance with regulations.

SOLUTIONS

NIS2, GDPR, National Security Frameworks, and the Acts on the Protection of Critical Infrastructure are some of the laws and regulations that affect 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.

"Orange has maintained a strong alliance with Zerolynx for over 5 years, being one of our preferred partners for providing cybersecurity services to large accounts. Additionally, Zerolynx supports us in our internal cybersecurity, participating in multiple projects across various branches. Zerolynx is certainly a highly recommended ally"

José Ramón Monleón
CISO of Orange Espagne

TOP REFERENCES

orange™   **Jazztel**   **euskaltel**

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

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE™