ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Cybersecurity in the **Retail** Sector

OVERVIEW

The Retail Sector is immersed in a constant transformation process driven by the influence of e-commerce. The rapid evolution of technology has led to the need to implement innovative solutions, such as artificial intelligence and data analysis, to better understand consumer preferences and optimize inventory management. In this dynamic context, the attack surface of companies has continued to expand, increasing the likelihood of experiencing a cyber incident.

CHALLENGES

Virtual stores are the windows to the world of an increasingly digitized sector, but they are also the doors used by cybercriminals in 33% of their incursions. Manufacturing, sorting, and distribution plants are also a target of crime. The interconnection of these through different industrial equipment (ICS) and the lack of patching and maintenance create significant cybersecurity gaps. Unsupported Scadas, HMIs, PLCs, sensors, and other OT assets expose vulnerabilities to constantly evolving threats that must be properly mitigated.

SOLUTIONS

NIS2 and GDPR 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.

KEY FIGURES

- **54% of companies** in the Retail Sector **admit to having experienced cyber incidents during the last year.**
- **One in three cyber incidents** in the sector occurred on **main websites**.
- **Employees and their devices** continue to be the **main entry point for cybercrime**, accounting for **56% of cyber incidents** in the sector.

"As an international company, BOJ Global interacts and collaborates with suppliers worldwide, which has compelled us to have cybersecurity measures in line with multiple regulations. Zerolynx has helped us raise our cybersecurity levels in this complex scenario and define and implement response plans to address any incident"

Kristina Apiñaniz
CEO of BOJ GLOBAL

TOP REFERENCES

unide · Infortisa · BOJ SINCE 1905

ABOUT ZEROLYNX

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

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE