Cybersecurity in the Insurance Sector

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

KEY FIGURES

- **9% of employees** working in insurance companies would fall for a **phishing attack**.

- **All insurance companies** in the Ibex 35 have experienced a **significant ransomware incident in recent years**.

- **84% of insurers** offering Cyber Insurance would have supported the **payment of ransoms** in **ransomware incidents**.

OVERVIEW

The insurance sector is in constant evolution. Digitization is demanding organizations to adapt quickly, while the increase in threats is testing their resilience. Constantly changing regulations add an additional layer of complexity to security and privacy management. The growing interconnection of systems, especially after multiple mergers, is expanding their attack surfaces.

CHALLENGES

Risk management, cybersecurity, and continuous innovation are key elements to address these challenges and ensure the stability and efficiency of the sector. Espionage, denial-of-service attacks, or data exfiltration pose challenges alongside traditional issues like fraud, insider threats, or attacks on supply chains. With the increasing sophistication of cybercriminals, the effective implementation of cybersecurity measures becomes crucial to mitigate these risks and ensure integrity and prosperity.

SOLUTIONS

Insurance companies are heavily regulated and obligated to implement high cybersecurity measures. NIS2, National Security Frameworks, MISAR, or CCPA are some of the mandatory regulations in Europe and the United States. Zerolynx designs, implements, maintains, and operates comprehensive cybersecurity plans based on the six areas of NIST (Govern, Identify, Protect, Detect, Respond, and Recover).
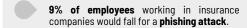
BENEFITS

Identification and Detection

We offer enhanced risk visibility through our cyber intelligence and ethical hacking services. We monitor, detect, and report various risks, such as exposed confidential data or severe vulnerabilities.
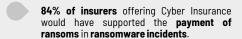
Protection and Response

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

"Zerolynx, through its Secure Development team, helped us enhance the cybersecurity of the entire lifecycle of our software products. Thanks to our collaboration, we improved our processes, technological solutions, and automation of various alert, reporting, and tracking workflows present in all phases of integration and continuous delivery"

Miguel Viedma
Head of Security Architecture
at Sanitas

TOP REFERENCES

AXA   **caser** Grupo Helvetia   **Sanitas**