ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Cybersecurity in the **Healthcare** Sector

OVERVIEW

Hospitals, laboratories, pharmaceutical companies, insurers, public and private healthcare, and all sector suppliers in general, collect and process a vast amount of confidential health data. Digitization, the use of connected medical devices, and IoT are expanding the attack surface. Low patching levels, unsupported systems, and the deployment of few security measures enable cybercrime to exploit multiple vulnerabilities to steal personal data, disrupt services, and even cause physical harm.

CHALLENGES

Medical equipment is beginning to become obsolete. High amortization periods force organizations to extend their lifespan, maintaining magnetic resonance imaging, ultrasound, X-ray, or CT scan systems 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, including new video consultation systems and patient portals, are exposing organizations to new security breaches.

SOLUTIONS

As critical infrastructures, healthcare entities are heavily regulated and obligated to implement high-security measures. HIPAA, NIS2, HITECH, GDPR, or National Security Frameworks are some of the 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

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.

KEY FIGURES

- In 2023, the **Hospital Clinic of Barcelona** suffered a **ransomware incident** in which the criminals demanded a **4.5 million € ransom**.
- The **Healthcare Sector** is among the **top 3 most targeted sectors of cyberattacks**.
- **93% of the medical equipment** in use is **unpatched and out of support**.

"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

Sanitas · PharmaMar · Osakidetza

ABOUT ZEROLYNX

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

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE