Building Trust in Messaging Technology: Ensuring Top-Tier Security and Compliant Solutions

The more data exchanged online, the greater the risk of data breaches.

RORSCHACH, SWITZERLAND, November 26, 2024 / EINPresswire.com/ -- The amount of customer data captured online nowadays is growing at an exponential rate. Whether it's opening a bank account, buying a train ticket, or communicating with local government authorities, users are required to share basic personal information, including payment details, email addresses, and home addresses. The more data exchanged online, the greater the risk of data breaches.

In 2023 alone, over 2,800 reported data theft incidents compromised more than 8 billion records. Such breaches have a profound impact on consumer trust, which is the cornerstone of customer loyalty. According to PCI Pal, 83% of consumers would stop spending with a business for months following a security breach, and 21% might never return.

For messaging technology providers like HORISEN, adhering to and even exceeding security standards is essential for maintaining the trust and ensuring the highest level of data protection for our customers' businesses. Although we, as technology providers, are not directly obligated to comply with these standards, the impact of non-compliance can be significant for our customers. Therefore, as a trusted provider to telecom, governmental, and banking sectors, HORISEN's security experts rigorously monitor the latest updates and standards and prioritize aligning with the latest security frameworks such as the NIS 2 Directive for cybersecurity and the Digital Operational Resilience Act (DORA) to protect our clients' interests and ensure robust, compliant operations.

What is the NIS-2 Directive?

The Network and Information Security Directive 2 (NIS-2) establishes an EU-wide cybersecurity

framework, created in response to escalating threats. Published in December 2022, it replaces the original NIS Directive, setting higher standards for network and information system security across EU member states. NIS-2 requires essential and significant entities to implement robust measures to manage and mitigate risks, enhancing the resilience of critical sectors and supporting a secure EU digital landscape.

What is DORA?

The Digital Operational Resilience Act (DORA) is EU legislation focused on strengthening the cybersecurity resilience of financial institutions. It closes regulatory gaps with specific requirements for managing ICT incidents, business continuity, and third-party risk, while mandating threat-led penetration testing. DORA takes a systemic approach to resilience across Europe, prioritizing the financial sector and taking precedence where its requirements overlap with those of NIS-2.

Raising the Bar in Security and Compliance: HORISEN's Commitment to Excellence

HORISEN is deeply committed to upholding high security and compliance standards recognizing that robust security is essential to building customer trust. Our foundation in GDPR, ISO/IEC 27001, and ISO/IEC 27002 compliance not only ensures data protection but also enables us to align closely with new regulatory frameworks, such as NIS-2 and DORA, which demand more stringent cybersecurity measures and operational resilience.

Through an in-depth analysis, HORISEN identified specific areas requiring enhancement to fully comply with these evolving standards. Although ISO 27001 covers nearly all NIS-2 requirements, additional measures were necessary to address areas like crisis management and comprehensive incident reporting, as outlined in NIS-2. To meet these requirements, we have expanded our incident response capabilities to include rapid, structured reporting and a formalized crisis management approach.

For DORA compliance, which emphasizes rigorous ICT risk management, incident reporting, and resilience testing, HORISEN is implementing ISO 22301 standards to strengthen our business continuity management, ensuring resilience during disruptions. Additionally, DORA's focus on supply chain security led us to adopt ISO 27036, fortifying our vendor risk management process, especially with critical providers like data centres and ISPs. By managing most key services in-house, we retain greater control over our supply chain and reduce potential security risks.

Furthermore, HORISEN's proactive security testing practices, including annual third-party penetration tests, align with DORA's stringent resilience testing requirements, ensuring that our systems remain secure and resistant to emerging threats. Beyond these updates, we also continuously improve employee training programs and have integrated multi-factor authentication (MFA) in line with NIS-2's cybersecurity expectations.

Through these targeted enhancements and rigorous compliance measures, HORISEN upholds a comprehensive approach to data security, meeting today's regulatory standards and laying a robust foundation for the future.

Setting the Standards for Safe and Reliable Messaging

In the messaging industry that is growing rapidly, security is not just an obligation - it's a competitive advantage. At HORISEN, we take pride in our proactive approach to security, ensuring that we meet and exceed industry standards to protect the data of our customers and their clients. HORISEN recognizes the importance of staying ahead of security standards and regulations. We adhere to these high standards not out of obligation, but because our commitment to our customers' security and business growth drives us. Our priority is to ensure the most secure and reliable services, reflecting our dedication to their success.

This commitment extends to ensuring that our suppliers, such as data centres, also comply with these high standards. Our cloud services are hosted in Tier IV data centres in Switzerland, demonstrating this commitment through their advanced security concepts that meet the highest requirements. These partnerships enhance platform reliability, ensuring the utmost integrity and safeguarding clients' data with unparalleled diligence while complying with privacy laws. Additionally, we conduct annual penetration tests to ensure that our systems remain resilient against potential threats and vulnerabilities.

By adhering to GDPR, ISO/IEC 27001/27002, NIS 2, and DORA, along with hosting our cloud services in most secure environment, we provide a secure foundation for our customers to build their own trusted services. This comprehensive approach ensures the highest levels of protection and reliability, supporting our customers in delivering secure and trustworthy services to their clients.

For an in-depth look at these standards, our gap analysis, and the steps to achieve full alignment with NIS-2 and DORA, check out our paper, Meeting NIS 2 and DORA Requirements in the CPaaS Industry, available on our website.

Una Zecic
HORISEN
+381 69 699031
email us here
Visit us on social media:
LinkedIn