Demystifying the NIS 2 directive: Ensuring cybersecurity compliance for a safer digital landscape

White paper

This white paper navigates the evolving cybersecurity regulatory landscape, focusing on the impending NIS 2 directive and the penalties of non-compliance. Underscoring the importance of security architecture design, this paper addresses aspects like authentication, access control, encryption, and continuous monitoring. The paper also highlights the role of Role-Based Access Control (RBAC) in improving security and outlines priorities to avoid costly fines.

Contents

Journey through regulatory history and the NIS 2 revolution

IT technologies including 5G have revolutionized the way people and countries work, but it has also brought new cybersecurity risks. To address such cyber-risks, the council of the European Union and the European Parliament has released a newer Network Information Services (NIS) Directive known as NIS 2 in November 2022 which adapts the previous NIS to current needs. The new directive covers a wider scope compared to the former one and increases the number of entities and controls required for an adequate cybersecurity risk management program.

The NIS Directive imposes specific security technical practices, measures, and requirements for EU essential entities including communication networks, communication services, cloud service providers and content network delivery providers who deliver services electronically due to a recipient's request.

The all-hazards approach used to combat NIS risks include:

- Policies on cybersecurity risk management
- Incident handling
- Business continuity
- Supply chain security
- Network and information systems acquisition, development and maintenance, vulnerability handling
- Basic cyber hygiene practices
- Cryptography use
- Human resource security

To maintain solid cybersecurity risk management programs, entities need to assess the effectiveness of policies, security systems, and cybersecurity training.

By following these measures, NIS 2 aims to improve the security protection of both network and information systems from incidents, thereby safeguarding the economies and people using these systems and the services.

NIS 2 and the next frontier of connectivity

The NIS 1 Directive required digital service providers - like telecommunication operators - to meet digital security standards and report any cyber incidents. But with the NIS 2 Directive, several new security measurements are specified, and Nokia has identified the relevance and applicability for essential entities using 5G technologies.

Risk Management and Risk Analysis are the foundation of this new approach. No essential entities should launch a new technology (eg 5G core) or service (eg Slicing) without understanding the risks, threats, and potential impacts.

5G-Ensure research provides a starting point. But it's also essential for customers to conduct service-specific Risk Analysis to define the network's security (e.g., safeguards, encryption) and create an inventory mapped to risks, and other essential measurements. Without a cataloged inventory of your network's safeguards, any future security management, incident detection, or other mandatory measurements may become challenging or not possible. This can be more challenging for modern 5G networks with capabilities such as automated scaling, orchestration and slicing.

When it comes to network security linked to 5G technology, there are at least three areas worth paying special attention. Firstly, cloud security - since 5G networks and services run on hybrid clouds, it demands relevant security measurements. Secondly, application security, as there are more APIs and applications interworking. Thirdly, digital identities (e.g., keys, tokens, certificates) are often used for proper strong authentication. We'll cover the latter one more later, though it's worth stressing that network security like zoning, traffic segregation, and communication filters remain critical.

After identifying the security "framework" measures for assessing and protecting, it's essential to map security measures for detecting and responding to 5G technologies as operators evolve. AIOps, service orchestration, and slicing capabilities are all based on agile, elastic, and automated processes and functions – many of which are necessary as operators evolve. But all these benefits are nullified if security isn't given the attention it demands.

Article 18.2 in the NIS 2 Directive is critical for preventing, detecting, and responding to incidents in 5G networks. To achieve this, a robust security management system or security operation centers must integrate threat intelligence for 5G network functions, alongside response capabilities that do not conflict with network or service orchestration systems. It's important to note that future orchestration and provisioning are automatically executed, and there's no manual execution. This means that 5G operators and service providers must prioritize the NIS 2 mandate for their technology to function with maximum efficiency.

Exploring non-compliance consequences and penalties

Ensuring accountability for non-compliance is a key component of effective cybersecurity risk management. Under Article 20 in the NIS 2 Directive, covered entities are required to implement technical, operational, and organizational measures to manage network and information security risks, which must be approved by the management body. Under this directive, management bodies can be held liable for infringements, making risk management a legal imperative for organizations.

So, what are the Cybersecurity Risk Management measures and why should you implement effective security controls and procedures? Under Article 21 in the NIS 2 Directive, entities are required to implement appropriate and proportionate measures to manage risks in network and information systems. These measures can range from basic cyber hygiene to security controls and procedures like zero trust principles, software updates, user access, identity management, and more. Agile and effective risk management can boost incident prevention and detection, ultimately keeping companies safe from cyberattacks.

The UK's Telecommunications Security Act (TSA) and the EU's NIS 2 Directive share common ground in enhancing cybersecurity and managing risks, but TSA is specifically targeted at telecommunication operators in the UK. Both regulations require risk management, incident reporting and supply chain security. Complying with relevant legislation is mandatory for telecommunication operators, and failure to do so can result in heavy penalties.

Although TSA operates independently of the EU's NIS 2 Directive, their complementary goals and requirements ensure a broader alignment of cybersecurity standards across the UK and the EU.

While risk management is critical for important entities, companies must comply with the new NIS 2 Directive or risk facing higher penalties than those outlined in the NIS 1 Directive. Non-compliance for critical entities could result in fines of €10 million, or 2% of total worldwide turnover, and fines of €7 million, or 1.4% of total worldwide turnover for significant entities (whichever is higher).

Adopting responsible cybersecurity practices goes beyond compliance - it is key to ensuring a secure environment for the data of your company and customer base.

The critical role of security architecture design and NIS 2

As 5G technology becomes ubiquitous across Europe and we rely more heavily on digital connections, it's crucial to prioritize the security of our networks. In conjunction with the NIS 2 Directive, it is crucial to take proactive measures to protect the integrity, confidentiality, and availability of data and services.

Protect the future of your communication with key security architecture design elements tailored for 5G and the NIS 2 Directive. Proactive measures to safeguard the future of communication are listed as follows:

Threat landscape

Designing a proactive security architecture strategy is essential in today's ever-evolving threat landscape. With the increased attack surface presented by 5G technology and the growing sophistication of cyber threats, identifying potential risks and vulnerabilities is imperative.

To understand the risks and ensure compliance with NIS 2 regulations, three key practices come into play: threat modeling, risk assessment, and intelligence sharing. By adopting a comprehensive approach to threat identification, organizations can create effective security measures that protect their networks and data.

Secure-by-design principles

5G networks and NIS 2 compliance frameworks demand that security be prioritized from the get-go. Implementing secure-by-design principles ensures that security considerations are incorporated from the early stages of system design and development. By conducting security assessments, adhering to industry best practices, and following international standards, the foundation for a robust security architecture can be established. The principles of confidentiality, integrity, and availability must be preserved throughout the lifecycle of 5G networks and NIS 2 compliance initiatives.

Authentication and Access Control: Security architecture design for 5G needs identity management, authentication, and access control mechanisms to be compliant under the NIS 2 Directive. As IoT devices and complex network ecosystems spread, preventing unauthorized access requires a robust authentication framework.

Multi-factor authentication, biometrics, and secure identity protocols enhance the overall security posture. Access control mechanisms should also be granular and dynamic, facilitating fine-grained authorization based on user roles, device types, and contextual factors to better manage security.

Encryption and privacy

Organizations can enforce technical and organizational measures through the implementation of cryptography and encryption. This technology allows encrypted data to be accessed only with additional information (a cryptographic key), giving organizations greater control over their cloud-based assets.

Encryption and Key Management Systems (KMS) are technical measures and are managed by organizations, not the cloud provider and are defined as organizational measures.

Crucial to securing data and communications within 5G networks, end-to-end encryption techniques, strong encryption algorithms, cryptographic key management, and secure protocols protect data in transit and at rest.

Privacy-enhancing technologies, such as differential privacy and data anonymization, can help preserve individuals privacy rights while facilitating the analysis of aggregated and anonymized data. Compliance with data protection regulations, including NIS 2 guidelines, is essential to maintaining user trust and ensuring the confidentiality of sensitive information.

Continuous monitoring and incident response

To ensure timely detection and mitigation of threats, a robust monitoring and incident response framework is critical. This involves using Security Orchestration Analytics and Response (SOAR), Intrusion Detection and Prevention Systems (IDPS), and behavior analytics for real-time visibility into network activities and anomalies. If a security incident does occur, having a well-defined incident response plan, regular vulnerability assessments and trained personnel can minimize the impact and facilitate a swift recovery.

As 5G networks and the NIS 2 compliance framework continue to shape the future of communication, the design of a comprehensive security architecture becomes indispensable. By acknowledging the evolving threat landscape, adhering to secure-by-design principles, implementing robust authentication and access control mechanisms, ensuring strong encryption and privacy measures, and establishing continuous monitoring and incident response capabilities, organizations can effectively mitigate risks and safeguard the integrity, confidentiality, and availability of data and services.

The significance of role-based access control (RBAC) in the NIS 2 era

In 5G networks, Role-Based Access Control (RBAC) is one of the security measures that is a must for securing the network. In fact, it is listed as a relevant security measure in the risk management and incident response compliance requirements of the NIS 2 Directive.

Role-Based Access Control (RBAC) is a security model that restricts system access based on the roles assigned to users - an absolute must for securing the 5G network. In 5G technology, RBAC plays a vital role in ensuring that users are only granted access to the resources necessary for their job functions based on least-privilege principle. User data privacy concern is paramount with the quantity of confidential data passing through the control plane from network operations, as well as through the data plane from users/consumers, the implementation of RBAC has become mandatory.

RBAC effectively reduces the risk of unauthorized access to sensitive information. And organizations can guarantee that users can only gain access to functions on the network based on their roles and profiles following a zero-trust model.

To further security levels with RBAC, features like password rotation and access governance help organizations to manage their security in a more systematic way. Organizations can, for instance, override old passwords through password rotation and renew them automatically. Access governance ensures that granted access is only assigned to network functions on demand, reducing the risk of security breaches.

Of course, in 5G technology, it's important to adopt the NIS 2 Directive to stay compliant and prevent data breaches and unauthorized access to sensitive information. One way to stay compliant under the NIS 2 Directive is to encrypt data in transit and using strong authentication mechanisms such as two-factor authentication. This will enable organizations to protect their network from any potential vulnerabilities.

Priorities for enhancing security posture and avoiding costly fines

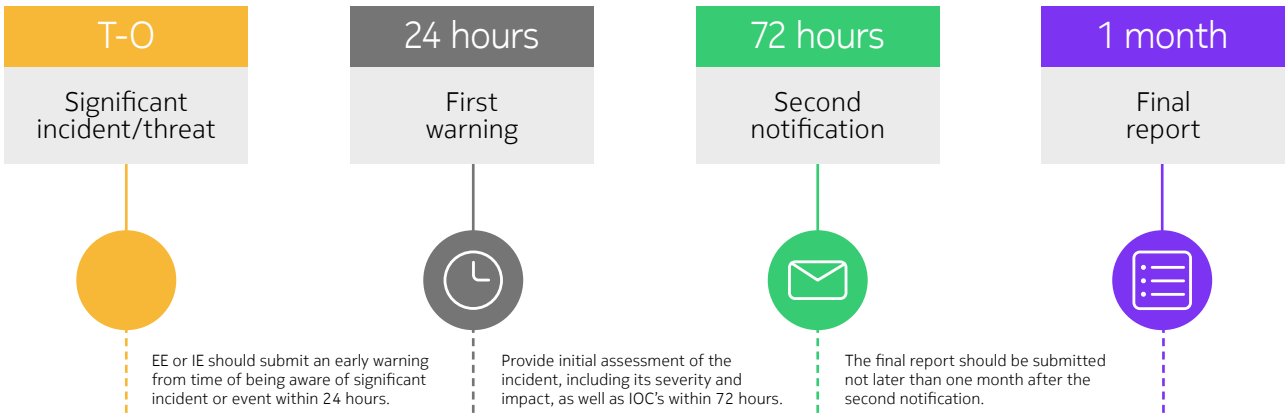
All entities in the telco sector including CSP's, vendors, and technology providers are subject to be compliant under the NIS 2 Directive and will have to prepare themselves. They must meet the requirements and enhance their security posture to avoid heavy fines.

To do this, CISOs must focus on three key priorities emphasized by the NIS 2 Directive:

- The overall information security governance
- Incident detection, handling & response
- Securing assets to improve resiliency

Incident detection & response has always been a major challenge and often a turning point for an organization's cybersecurity posture. A significant incident tests a company's ability to carry on with business operations while containing and recovering from the event to limit financial, reputational and operational impacts. After facing a major breach, the company should review its incident management plans, security budget and programs to set action plans to improve the incident response process. Cross border ramifications could loom after a major cybercrime incident as the NIS 2 Directive comes with precise obligations for incident reporting and information sharing.

The guidelines do more than set strict timelines for raising warnings during an event, but requires continuous updates, throughout the incident handling and response process such as providing initial assessments, IOCs (within 72 hours) and a final report within a month.



According to IBM's latest report on "Cost of Data Breach," companies are typically slow in identifying (average of 207 days) and containing (70 days) data breaches. CISOs and CSIRT are usually far from being ahead of the curve when it comes to incident detection and response.

To comply with NIS 2, CISOs need to review their cyber incident reporting and response processes, but more importantly, they must focus on incident detection and intelligence. By adopting both manual skills like HUMINT and cutting-edge incident response automation and machine learning solutions like Nokia NetGuard Cybersecurity Dome and NetGuard Endpoint Detection and Response (EDR), they can develop a proactive security posture.

Conclusion

In conclusion, the NIS 2 Directive become effective in January 2023 and imposes specific security requirements for EU companies including essential enterprise services (OES) operators and digital service providers (DSPs) who deliver services electronically due to a recipient's request. To avoid heavy fines, entities in the telco sector must meet the requirements under the NIS 2 Directive and prioritize information security governance, incident detection, handling & response and secure assets to improve resiliency.

However, in order to be truly proactive against cyber threats, organizations should also invest in the best solutions available on the market for detecting and responding to incidents. With the right incident response solutions, CISO's and CSIRTs can be confident that their organizations are prepared for whatever comes their way.

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID213413 (June)