LAYER SEVEN SECURITY

NIS2 COMPLIANCE FOR SAP SOLUTIONS

EUROPEAN UNION DIRECTIVE FOR NETWORK AND INFORMATION SECURITY

NIS2 COMPLIANCE FOR SAP SOLUTIONS

EUROPEAN UNION DIRECTIVE FOR NETWORK AND INFORMATION SECURITY

CONTENTS

INTRODUCTION

The Directive for Network and Information Security (NIS2) released by the European Union in December 2022 expands upon the original NIS Directive released in 2016. It mandates strict standards for cybersecurity including risk management, corporate accountability, reporting obligations and business continuity for essential and important organizations in critical sectors. The Directive takes effect on October 17 2024 and carries severe penalties for non-compliance.

This white paper discusses the requirements of the NIS2 Directive. It provides guidance for complying with the Directive with a specific focus on the impact for business-critical SAP applications. This includes managed solutions in SAP RISE. It provides a clear path to compliance for SAP customers with recommendations for managing cyber risks, ensuring compliance, and detecting and reporting security breaches in SAP solutions.

REQUIREMENTS

The NIS2 Directive is targeted at essential and important organisations in specific sectors that are considered part the supply chain for critical infrastructure in member states of the European Union. It applies to organizations with more than 50 employees and annual revenue exceeding 10M euros within a broad range of sectors deemed critical in the Directive. This includes energy, transportation, banking, financial market infrastructure, digital infrastructure, technology, health, water and waste management, chemicals, food supply, manufacturing, and public administration. Organizations in some sectors are required to comply with NIS2 regardless of size. The Directive applies equally to organizations based in the member states of European Union and overseas organizations that provide services within the EU. There are some exemptions for non-EU organizations such as digital services providers, DNS/ TLS registries, and cloud computing/ data centre providers.

The Directive includes requirements for the security of network and information systems in organisations within the target sectors. Network and information systems are defined in Article 6 (1) of the Directive as devices used to store, process, retrieve or transmit digital data. Security is defined in 6 (b) as "the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data". Note that the definitions detailed in Article 6 of the Directive do not provide for any limitation of the requirements to specific forms of data such as Personally Identifiable Information (PII). The Directive applies to all forms of data in network and information systems.

Article 21 (2) defines the following specific measures that organizations must apply to protect network and information systems.

a) Policies on risk analysis and information system security
b) Incident handling
c) Business continuity, such as backup management and disaster recovery, and crisis management
d) Supply chain security
e) Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
f) Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
g) Basic cyber hygiene practices and cybersecurity training
h) Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
i) Human resources security, access control policies and asset management
j) The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity

Article 21 (4) requires organizations to take "without undue delay, all necessary, appropriate and proportionate corrective measures" to comply with the measures outlined in 21 (2).

Article 23 specifies reporting obligations for cybersecurity incidents. Organizations must report significant incidents to the CSIRT in the relevant member state within 24 hours. According to the Article, an incident is considered significant if it causes or is capable of causing severe operational disruption or financial loss to the organization or other parties.

The notification for a significant incident must be followed-up with an initial assessment within 72 hours that includes disclosure of the severity and impact of the incident, and, where available, indicators of compromise. A detailed report must be filed with the CSIRT within one month of the significant incident. The report must include details of the root causes, mitigation measures applied by the organization, and, where applicable, the cross-border impact.

The Directive empowers CSIRTs to disclose significant incidents if it is in the public interest and to report incidents to law enforcement if they are suspected to be of criminal nature.

Article 32 defines enforcement measures for the Directive. It enables member states to perform information requests, audits, inspections, and security scans to validate the compliance of relevant organizations. The costs of the reviews are borne by the organizations. It also enables member states to issue binding instructions to organizations with time limits to remediate infringements. Section 5 (b) of Article 32 enables member states to request the suspension of Chief Executive Officers and other officers for the failure to comply with enforcement measures including the remediation of infringements. Section 6 establishes personal liability of the officers of the organization for compliance failures.

Article 34 details administrative fines for non-compliance. Fines for essential entities can be up to 10M Euros or 2% of annual global revenue, whichever is higher. Maximum fines for important entities are the higher of up to 7M Euros or 1.4% of annual global revenue. Essential entities are large organizations with more than 250 employees or 50M Euros in annual revenue in sectors of critical importance. Important entities are medium sized organizations with less than 250 employees or less than $50M Euros in annual revenue in sectors of critical importance and all organizations regardless of size in other critical sectors.

Member states of the European Union are required by Article 41 to implement the Directive within their territories by October 17 2024.

NIS2 COMPLIANCE FOR SAP SOLUTIONS

The requirements of the NIS2 Directive apply to all network and information systems used by organizations to store, process and transmit data and all forms of data. They also apply to all potential hazards such as natural disasters, negligence, sabotage and not just cyber threats. SAP solutions are some of the most important information systems in organizations, often storing and processing sensitive financial and personal information. Security failures that lead to data breaches, financial fraud or impact the availability of SAP systems can have a significant impact on organizations. This section provides specific guidance for organizations managing SAP solutions to meet the requirements of Articles 21 and 23 that mandate cybersecurity measures to protect network and information systems and report significant incidents.

An information security baseline should be established for SAP solutions to define minimum security standards for solutions and provide a governance framework that identifies and addresses relevant risks. This should include policies and procedures for network design, landscape architecture, data access governance, access control, system configuration, patch management, and incident detection and response. Hardening standards can be derived from recommendations provided by SAP through, for example, the SAP Security Baseline and product-specific security guides for solutions such as SAP S/4HANA. SAP RISE customers should refer to note 3250501 for information on mandatory security parameters and hardening requirements for ABAP systems in SAP Enterprise Cloud Services (ECS). The standards should include measures for the use of cryptography and encryption to protect data in transit and at rest. The Secure Storage in the File System (SSFS) should be appropriately configured to protect sensitive SAP data in the file system. Database encryption should also be applied to secure critical tables or columns. The use of insecure cryptographic algorithms should be blocked and system communications should be encrypted using SNC or TLS, depending on the SAP protocol.

NIS2 requires organizations to implement procedures to assess the effectiveness of cybersecurity risk management procedures. This should include periodic penetration testing of SAP solutions and security audits to assess system hardening. Layer Seven Security is an SAP Services Partner and a leading provider of penetration testing services for SAP solutions. The Cybersecurity Extension for SAP from Layer Seven Security automates SAP vulnerability and compliance management. It performs scheduled checks for over 4000 vulnerabilities in SAP systems and automates compliance gap analysis for frameworks such as the SAP Security Baseline, Security Guide for S/4HANA, and Security Requirements for RISE Solutions. Other supported frameworks include NIST, GDPR, PCI-DSS and SOX. The Cybersecurity Extension for SAP also identifies unapplied security patches and vulnerabilities in custom code in SAP systems. The solution supports the planning, tracking and reporting of remediation activities for the mitigation of vulnerabilities for NIS2 compliance.

In order to comply with the incident reporting requirements of NIS2, organizations must detect, analyse and report significant incidents to CISRTs within 24 hours, followed up with more detailed filings within 72 hours. This requirement can only be met for SAP solutions using automated threat detection and response.
Security-related events in SAP systems are captured in multiple disparate logs. There is no standardization of event structures across the logs. Furthermore, the high volume of events per second in SAP logs means manual detection is impractical.

The Cybersecurity Extension for SAP automates threat detection and response for SAP. It applies more than 1000 patterns to detect indicators of compromise for SAP logs in real-time. The solution filters, normalizes and enriches event logs from multiple SAP systems to support detection and forensic analysis. It triggers alerts and notifications for suspected security incidents. The alerts can be integrated with Security Event and Information Management (SIEM) solutions for centralized SOC monitoring and investigated using embedded procedures for alert handling that support incident analysis and reporting. The solution also detects anomalies in SAP systems based on unusual system and user behaviour to augment threat detection based on pattern matching.

SAP customers are responsible for securing and monitoring the application layer within SAP solutions. This includes customers using SAP solutions managed directly by SAP as part of SAP RISE. Standard RISE services do not delegate responsibility for securing applications from customers to SAP.

Additional services and packages must be purchased from SAP to extend SAP support for areas such as application-level access control, vulnerability management, patch management, and threat detection and response. For further information, please refer to the guide Security for SAP RISE from Layer Seven Security.

CONCLUSION

The NIS2 Directive imposes a considerable responsibility on a wide range of organizations both within and outside the European Union to implement robust measures to protect information systems from hazards such as cyber threats. The Directive also requires organisations to detect and report significant cybersecurity incidents within a prescribed time frame and undertake measures to remediate the incidents. NIS2 mandates severe penalties for non-compliance including substantial fines and criminal sanctions for management to ensure accountability.

NIS2 compliance requires the implementation of a comprehensive risk management framework for information systems. The measures included in the framework should address the specific risks of the technologies deployed by each organization. For SAP solutions, the measures should include adherence to security benchmarks and SAP recommendations for system hardening, security patching, and securing custom code. SAP recommendations are documented in security guides and standards for each area and product. The measures should also include mechanisms for the timely detection, investigation and reporting of security incidents captured in SAP logs. Pattern matching and anomaly detection can be deployed to effectively detect security incidents in SAP solutions.

The Cybersecurity Extension for SAP simplifies the path to NIS2 compliance. The SAP-certified solution automates vulnerability detection, compliance reporting, and custom code security to reduce the complexity and lower the cost of compliance with Article 21 of the Directive. The solution also enables organizations to meet the requirements of Article 23 for breach identification and reporting through automated threat detection and incident response for SAP applications.

LAYER SEVEN SECURITY

Layer Seven Security is an industry leading provider of security software and services for SAP solutions. The company is recognized as one of the Top Ten SAP Solution Providers of 2018, Top 25 Cybersecurity Companies of 2020, and Top Threat Intelligence Solution Providers 2023. Layer Seven Security is headquartered in Toronto, Canada.

CONTACT US

www.layersevensecurity.com
info@layersevensecurity.com

SAP Partner