ELATEC
RFID Systems

LOGICAL ACCESS CONTROL

NIS2 introduces stricter requirements for logical/digital access control to limit access to digital systems, data and networks.

8 STEPS FOR NIS2 COMPLIANCE IN DIGITAL AND PHYSICAL ACCESS

User authentication and access control for both digital and physical assets are critical components of Network and Information Security Directive 2 (NIS2) compliance. NIS2 mandates stricter security measures to ensure that only authorized individuals can access sensitive systems, data and physical infrastructure. By securing both physical and digital entry points, organizations can better safeguard their operations and meet the directive's rigorous requirements.

01

Implement Strong Password Policies of Passwordless Authentication

Ensure all systems have strict password policies. Enforce the use of complex passwords, require regular updates, and prohibit easily guessable passwords. For enhanced security, consider moving to passwordless authentication methods, such as Radio-Frequency Identification (RFID) badges/tokens or mobile credentials on the smartphone using Near-Field Communication (NFC).

02

Adopt Multi-Factor Authentication (MFA)

Implement multi-factor authentication (MFA) for accessing sensitive data and systems. MFA should include a combination of factors such as passwords, PINs, one-time codes, biometric data, and RFID badges/NFC mobile credentials. For maximum security, implement phishing-resistant MFA, such as RFID/NFC with PIN or a mobile credential with biometrics on the smartphone.

03

Use Strong Identity-Based Access Management

Implement a unified Identity and Access Management (IAM) and Privileged Access Management (PAM) system to control who can access systems, applications and data. Use a centralized access management system to control access levels and permissions based on user roles. Maintain up-to-date access permissions as people change roles or leave the organization.

04

Secure Single Sign-On (SSO) Solutions

Ensure that Single Sign-On (SSO) solutions are protected by secure phishing-resistant MFA to minimize the risk of unauthorized access through a single compromised login. While SSO simplifies user access, if not paired with appropriate security measures, it can become a single point of failure for multiple systems.

05

Use Appropriate Encryption for Access Control Systems

Ensure that strong encryption, such as AES-256 or advanced Elliptic Curve Cryptography (ECC), is applied across all physical and digital access control points to protect user authentication data. Encrypt sensitive data such as login credentials, biometric data, and RFID/mobile credentials during both storage and transmission. Implement end-to-end encryption for communication between devices and access management systems to safeguard against data interception or unauthorized access.

For more information contact our Application Specialists at the locations below:

elatec.de

EMEA
Puchheim, Germany
+ 49 89 552 9961 0
sales-rfid@elatec.com

AMERICAS
Palm City, Florida, USA
+1 772 210 2263
americas-info@elatec.com

ASIA PACIFIC
Shenzhen, China
+86 755 2394 6014
apac-info@elatec.com

ELATEC
RFID Systems

PHYSICAL ACCESS CONTROL (PAC)

While NIS2 primarily emphasizes cybersecurity, physical security also plays a crucial role in protecting essential services and infrastructure.

8 STEPS FOR NIS2 COMPLIANCE IN DIGITAL AND PHYSICAL ACCESS

06

Consider Physical Access as Part of Cybersecurity

NIS2 requires organizations to adopt a holistic risk management approach that includes both physical and digital security measures. This means that organizations must secure their physical facilities to prevent unauthorized access that could compromise sensitive systems or data. Ensure that physical access credentials (e.g., RFID cards, mobile credentials) are securely managed and regularly updated to prevent unauthorized entry.

07

Use MFA to Secure Sensitive Locations

MFA should be used as part of a PAC solution for highly sensitive locations such as server rooms and data centers. For physical access applications, that is most commonly accomplished via an RFID reader with a keyboard for PIN entry. Biometrics are an alternative in some cases, for example by combining a mobile credential with biometric capabilities on the smartphone.

08

Implement Tamper-Proofing for Access Control Systems

Ensure that all physical access control (PAC) components, such as RFID readers and door locks, are tamper-proof. This prevents unauthorized individuals from physically manipulating or bypassing these systems to gain entry.

Other Considerations for NIS2 Compliance

A comprehensive and compliant plan for access management also includes:

- Regular auditing of cybersecurity measures, including access control, to ensure compliance.
- Ongoing continuous monitoring of access systems for login activities, access events and real-time anomaly detection.
- An incident response plan to handle security breaches, including reporting to relevant authorities.
- Integration of PAC with other elements of physical security, such as intrusion detection and surveillance systems.
- Supply chain management to ensure access systems for third-party vendors and service providers are compliant.

Questions about NIS2-Compliant Access Solutions?

Organizations must take a risk-based approach to physical and logical access control and tailor solutions to their unique risk profiles and threats. ELATEC can help you evaluate your current physical and digital access control systems and design a modern, compliant solution that meets all NIS2 requirements. A **unified access system** that integrates both logical and physical access simplifies management and compliance while increasing convenience for end users.

Talk to an access control expert today.

For more information contact our Application Specialists at the locations below:

elatec.de

EMEA
Puchheim, Germany
+ 49 89 552 9961 0
sales-rfid@elatec.com

AMERICAS
Palm City, Florida, USA
+1 772 210 2263
americas-info@elatec.com

ASIA PACIFIC
Shenzhen, China
+86 755 2394 6014
apac-info@elatec.com