ELATEC
RFID Systems

ZUGANGSKONTROLLE

Die NIS-2-Richtlinie führt strengere Anforderungen für die digitale Zugangskontrolle ein, um den Zugang zu digitalen Systemen, Daten und Netzwerken zu begrenzen.

8 SCHRITTE ZUR KONFORMITÄT MIT DER NIS-2-RICHTLINIE BEI ZUGANG UND ZUTRITT

Benutzerauthentifizierung und Zugangskontrolle sowohl für digitale als auch für physische Assets sind kritische Komponenten, um die Konformität mit der zweiten EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) zu erzielen. Die NIS-2-Richtlinie schreibt strengere Sicherheitsmaßnahmen vor, um sicherzustellen, dass nur befugte Personen Zugang zu sensiblen Systemen, Daten und physischer Infrastruktur haben. Durch die Absicherung von physischen als auch digitalen Zugangspunkten können Organisationen ihre Abläufe besser schützen und die strengen Anforderungen der Richtlinie erfüllen.

01 **Implementierung starker Passwortrichtlinien für die Authentifizierung ohne Passwörter**

Stellen Sie sicher, dass für alle Systeme strenge Passwortrichtlinien gelten. Setzen Sie die Verwendung komplexer Passwörter durch, fordern Sie regelmäßige Updates und verbieten Sie leicht zu erratende Passwörter. Für erhöhte Sicherheit sollten Sie den Wechsel zu Authentifizierungsmethoden ohne Passwörter in Erwägung ziehen, wie z. B. RFID-Ausweise/Tokens oder digitale Berechtigungsnachweise auf dem Smartphone mittels Near-Field Communication (NFC).

02 **Einführung der Multifaktor-Authentifizierung (MFA)**

Systemen. Die MFA sollte eine Kombination aus Faktoren wie Passwörtern, PINs, Einmalcodes, biometrischen Daten und RFID-Badges/digitalen Berechtigungsnachweisen mit NFC umfassen. Für höchste Sicherheit empfiehlt sich die Implementierung einer Phishing-resistenten MFA, z. B. RFID/NFC mit PIN oder einem digitalen Berechtigungsnachweis mit Biometrie auf dem Smartphone.

03 **Verwendung eines starken identitätsbasierten Zugriffsmanagements**

Implementieren Sie ein vereinheitlichtes IAM-System für Identitäts- und Zugriffsmanagement und ein PAM-System (Privileged Access Management), um zu kontrollieren, wer Zugang zu Systemen, Anwendungen und Daten erhält. Verwenden Sie ein zentralisiertes Zugangsmanagementsystem, um Zugriffsebenen und Berechtigungen basierend auf Benutzerrollen zu steuern. Halten Sie die Zugangsberechtigungen auf dem neuesten Stand, wenn Personen ihre Rollen ändern oder die Organisation verlassen.

04 **Sichere Single Sign-On (SSO) Lösungen**

Stellen Sie sicher, dass SSO Lösungen durch eine sichere, Phishing-resistente MFA geschützt werden, um das Risiko eines unbefugten Zugangs durch eine einzige kompromittierte Anmeldung zu minimieren. SSO vereinfacht zwar den Zugang für die Benutzer, muss aber mit geeigneten Sicherheitsmaßnahmen kombiniert werden, da die Lösung anderenfalls zu einem Single Point of Failure für mehrere Systeme werden kann.

05 **Verwendung einer geeigneten Verschlüsselung für Zutritts- und Zugangskontrollsysteme**

Stellen Sie sicher, dass an allen Zutritts- und digitalen Zugangskontrollpunkten eine starke Verschlüsselung wie AES-256 oder fortgeschrittene Elliptic Curve Cryptography (ECC) zum Schutz der Daten zur Benutzerauthentifizierung eingesetzt wird. Verschlüsseln Sie sensible Daten wie Berechtigungsnachweise zur Anmeldung, biometrische Daten und RFID/digitale Berechtigungsnachweise sowohl bei der Speicherung als auch bei der Übertragung. Implementieren Sie eine durchgängige Verschlüsselung für die Kommunikation zwischen Geräten und Zugangsmanagementsystemen, um Schutz gegen das Abfangen von Daten oder vor unbefugtem Zugriff zu gewährleisten.

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

ZUTRITTSKONTROLLE (PAC)

Auch wenn der Schwerpunkt der NIS-2-Richtlinie auf der Cybersicherheit liegt, spielt auch die physische Sicherheit eine entscheidende Rolle beim Schutz wichtiger Dienste und Infrastrukturen.

8 SCHRITTE ZUR KONFORMITÄT MIT DER NIS-2-RICHTLINIE BEI ZUGANG UND ZUTRITT

06

Berücksichtigung des Zutritts als Teil der Cybersicherheit

Die NIS-2-Richtlinie fordert von Organisationen ein ganzheitliches Risikomanagement, das sowohl Maßnahmen für die physische als auch digitale Sicherheit beinhaltet. Dies bedeutet, dass Organisationen ihre physischen Einrichtungen absichern müssen, um unbefugten Zugang zu verhindern, der sensible Systeme oder Daten gefährden könnte. Stellen Sie sicher, dass Berechtigungsnachweise für den Zutritt (z. B. RFID-Karten, digitale Berechtigungsnachweise) sicher verwaltet und regelmäßig aktualisiert werden, um unbefugten Zutritt zu verhindern.

07

Verwendung von MFA zur Absicherung sensibler Standorte

MFA sollte als Teil einer PAC-Lösung für hochsensible Standorte wie Serverräume und Rechenzentren verwendet werden. Bei Zutrittsanwendungen wird dies in der Regel über einen RFID-Leser mit einer Tastatur für die PIN-Eingabe umgesetzt. In einigen Fällen ist Biometrie eine Alternative, zum Beispiel durch die Kombination digitaler Berechtigungsnachweise mit biometrischen Funktionen auf dem Smartphone.

08

Implementierung eines Manipulationsschutzes für Zutritts- und Zugangskontrollsysteme

Stellen Sie sicher, dass alle Komponenten der Zutrittskontrolle (PAC) wie RFID-Leser und Türschlösser manipulationssicher sind. Dies verhindert, dass Unbefugte diese Systeme physisch manipulieren oder umgehen können, um sich Zugang zu verschaffen.

Weitere Überlegungen zur Konformität mit der NIS-2-Richtlinie

Zu einem umfassenden und konformen Plan für das Zugangsmanagement gehört auch Folgendes:

- Regelmäßige Überprüfung der Maßnahmen zur Cybersicherheit, einschließlich der Zugangskontrolle, um die Einhaltung der Vorschriften zu gewährleisten.
- Kontinuierliche Überwachung der Zugangssysteme auf Anmeldeaktivitäten, Zugangsereignisse und Erkennung von Anomalien in Echtzeit.
- Plan für die Reaktion auf Sicherheitsverletzungen, einschließlich der Berichterstattung an die zuständigen Behörden.
- Integration von PAC mit anderen Elementen der physischen Sicherheit, wie Einbruchmelde- und Überwachungssysteme.
- Lieferkettenmanagement, um sicherzustellen, dass die Zugangssysteme für Drittanbieter und Dienstleister konform sind.

Haben Sie Fragen zu NIS-2 konformen Zugangslösungen?

Organisationen müssen bei der Zutritts- und Zugangskontrolle einen risikobasierten Ansatz verfolgen und Lösungen auf ihre individuellen Risikoprofile und Bedrohungen abstimmen. ELATEC kann Ihnen bei der Bewertung Ihrer derzeitigen Zutritts- und digitalen Zugangskontrollsysteme helfen und eine moderne, konforme Lösung entwickeln, die alle Anforderungen der NIS-2-Richtlinie erfüllt. Ein vereinheitlichtes Zugangssystem, das sowohl den Zugang als auch den Zutritt integriert, vereinfacht das Management und die Einhaltung von Vorschriften und erhöht gleichzeitig den Komfort für die Endnutzer.

Sprechen Sie noch heute mit einem Experten für Zugangskontrolle.

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