NIS2-Anforderungen für Unternehmen: Wie Firmen mit digitaler Zutrittskontrolle ihre cyberphysische Resilienz erhöhen können

ASSA ABLOY
Opening Solutions

www.assaabloy.com/de

Experience a safer
and more open world

Inhalt

Die jährlich durch Datendiebstahl, Spionage und Sabotage verursachten Schäden für die deutsche Wirtschaft sind enorm. Allein im Jahr 2023 beliefen sich die Verluste laut einer durch den Digitalverband Bitkom beauftragten Studie auf 206 Milliarden Euro. Einen neuen Höchststand erreichten dabei die Cyberattacken mit einem Anteil von nahezu drei Vierteln. Bestätigt wird dieser Trend durch den Bericht zur Lage der IT-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Auch in Österreich verzeichnen BMI und Bundeskriminalamt einen bedeutenden Anstieg von Attacken auf IT-Systeme. 2022 wurde hier mit über 60.000 Angriffen ein neuer Spitzenwert registriert, der einer Zunahme von 30,4 Prozent entspricht.

Die Behörde stuft die Bedrohungslage als so hoch wie nie zuvor ein und verweist darauf, dass neben kritischen Infrastrukturen vermehrt auch kleine und mittlere Unternehmen, Behörden sowie Bildungs- und Wissenschaftseinrichtungen in den Fokus der Kriminellen geraten. Eine möglichst breit angelegte Strategie zur Stärkung der Widerstandsfähigkeit von Unternehmen und Organisationen ist somit das Gebot der Stunde.

NIS2 bringt höhere Mindestanforderungen für deutlich mehr Betriebe

*In Österreich rechnet das BMI damit, dass sich die Zahl der dort von NIS2 betroffenen Unternehmen von derzeit ca. 100 auf 3.000 bis 4.000 erhöhen wird.

Die NIS2-Richtlinie verfolgt einen entsprechenden Ansatz. Das EU-weite Cybersicherheitsgesetz ersetzt die ursprüngliche NIS-Richtlinie zur Informationssicherheit (Network and Information Security) aus dem Jahr 2016. Die Gesetzesnovelle verschärft die Mindestanforderungen an die IT-Sicherheit kritischer Infrastrukturen und erweitert diese um zusätzliche Sektoren. Das bedeutet, dass von der Umsetzung von NIS2 in deutsches Recht zum Stichtag am 17.10.2024 deutlich mehr Bereiche und Betriebe betroffen sein werden als bisher.

Der Gesetzgeber geht dabei von rund 30.000 Unternehmen* in verschiedenen Gruppen aus. Gut zu wissen: Die neue Cybersicherheits-Richtlinie fordert einen gefahrenübergreifenden Ansatz. Verantwortliche sollten also nicht nur digitale Sicherheitsmaßnahmen ergreifen, sondern auch Vorkehrungen zum physischen Schutz ihrer Infrastrukturen implementieren. Für welche Unternehmen NIS2 gilt, welche konkreten Anforderungen damit verbunden sind und wie Firmen sich vorbereiten können, erfahren Sie im vorliegenden Whitepaper.

Wer ist von NIS2 betroffen?

Ob die NIS2-Richtlinie auf ein Unternehmen anwendbar ist, hängt zunächst von dessen Zugehörigkeit zu einem von insgesamt 18 Sektoren ab. Diese werden in zwei Anlagen beschrieben und teilen sich in Sektoren mit „hoher Kritikalität“ sowie „sonstige“ kritische Sektoren auf, welche der Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE) folgen:

Diese Zusammenstellung orientiert sich an dem NIS2-Referentenentwurf vom September 2023 und der hieraus abgeleiteten Darstellung auf der Online-Informationsplattform OpenKRITIS. Es handelt sich dabei um eine vorläufige Bestandsaufnahme, die leicht von den in der EU-Direktive definierten Sektoren abweicht. Bis zur finalen Fassung des NIS2-Umsetzungsgesetzes, mit der erst im Oktober 2024 gerechnet wird, können sich ebenfalls noch einmal geringe Änderungen ergeben. Experten gehen davon aus, dass sich Österreich bei der Zuordnung der Sektoren an diesem Modell orientieren wird. Änderungen sind indessen auch hier noch möglich.

Sektoren und Teilsektoren mit hoher Kritikalität (Anhang I)	Sonstige kritische Sektoren und Teilsektoren (Anhang II)
Energie Stromversorgung, Fernwärme/-kälte, Kraftstoff/Heizöl, Gas	
Transport / Verkehr Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr	**Transport / Verkehr** Post und Kurier
Finanz / Versicherung Banken, Finanzmarkt-Infrastruktur	**Chemie** Herstellung, Handel, Produktion
Gesundheit Dienstleistungen, Referenzlabore, F&E, Pharma (NACE C Abt. 21), Medizinprodukte	**Forschung** Forschungseinrichtungen
Wasser / Abwasser	**Verarbeitendes Gewerbe** Medizin / Diagnostika; DV, Elektro, Optik (NACE C Abt. 26 und 27); Maschinenbau (NACE C 28), Kfz/Teile (NACE C 29), Fahrzeugbau (NACE C 30)
Informationstechnik und Telekommunikation IXPs, DNS, TLD, Cloud Provider, RZ-Dienste, CDNs, TSP, elektronische Kommunikation/ Dienste, Managed Services und Security Services	**Digitale Dienste** Marktplätze, Suchmaschinen, soziale Netzwerke
Weltraum Bodeninfrastrukturen	
	Lebensmittel Großhandel, Produktion, Verarbeitung
	Entsorgung Abfallbewirtschaftung

Für die Zuordnung sind neben diesen Tätigkeitsbereichen auch die Größe und Wirtschaftsleistung entscheidend. In Abhängigkeit dieser Faktoren unterscheidet NIS2 zwischen „besonders wichtigen“ und „wichtigen Einrichtungen“. Als besonders wichtig wird eine Einrichtung demzufolge eingestuft, wenn ihre Tätigkeit in einem Sektor mit hoher Kritikalität (Anhang 1) stattfindet, mehr als 250 Mitarbeiter beschäftigt und einen Umsatz von mehr als 50 Millionen Euro erwirtschaftet. In die Kategorie der wichtigen Einrichtungen fallen alle anderen Einrichtungen der Anlagen 1 und 2, wenn sie mehr als 50 Beschäftigte oder einen Jahresumsatz von mehr als 10 Millionen Euro haben:

Besonders wichtige Einrichtung	Wichtige Einrichtung
Sektor in Anhang I mit mindestens 250 Beschäftigten oder über 50 Mio. Jahresumsatz sowie einer Bilanzsumme von über 43 Mio. Euro	Sektoren in Anhang I + II mit mindestens 50 Beschäftigten oder über 10 Mio. Euro Jahresumsatz und Bilanzsumme
Bestimmte Sonderfälle, z. B. qTSP, TLD, DNS, TK-Anbieter, kritische Anlagen, Zentralregierung	Vertrauensdienste / Trust Service Provider (TSP)

Für alle Unternehmen, die in den Sektoren aufgelistet sind und einen Jahresumsatz von 10 Millionen Euro überschreiten, gilt die NIS2!

Davon abgesehen, können auch kleinere Betriebe von NIS2 betroffen sein. Dies ist der Fall, wenn ihr Ausfall erhebliche Auswirkungen auf Wirtschaft und öffentliche Versorgung hätte. Dazu zählen unter anderem bestimmte digitale Dienste, die durch die eIDAS-Verordnung geregelt werden. Nicht betroffen sind hingegen alle Kleinstbetriebe, mit weniger als 9 Beschäftigten und einem Umsatz unter 2 Millionen Euro.

Anforderungen von NIS2 und Bedeutung des physischen Schutzes

Grundsätzlich müssen besonders wichtige und wichtige Einrichtungen gemäß NIS2 Artikel 21 „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme [...] zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.“ Der Stand der Technik ist hierbei ebenso zu berücksichtigen wie die individuelle Gefährdungslage. Von großer Bedeutung ist in diesem Zusammenhang, dass die Schutzvorkehrungen einem gefahrenübergreifenden Ansatz („all hazards approach“) folgen. Es gilt also, nicht nur digitale Gefährdungen von den Netz- und Informationssystemen fernzuhalten, sondern auch die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen.

Dass die neue Richtlinie diesen Aspekt so deutlich herausstellt, kommt nicht von Ungefähr. So verweist etwa die Agentur der Europäischen Union für Cybersicherheit (ENISA) in ihrer aktuellen Auswertung der Bedrohungslage explizit auf die Zunahme sogenannter cyberphysischer Angriffe. Im Zuge der zunehmenden Vernetzung von Produkten im „Internet der Dinge“ (IoT) bieten dort bestehende Schwachstellen mögliche Angriffspunkte, um sich beispielsweise Zugang zu physischen Hochsicherheitsbereichen zu verschaffen. Trotz bestehender hybrider Pläne für Cyber- und physische Sicherheit seitens der Unternehmen stuft die Cyberagentur den physischen Zugang als „größte Hintertür“ ein, deren Bedeutung immer noch vernachlässigt werde. Besonders vulnerabel sind in diesem Zusammenhang frei zugängliche Terminals, Arbeitsspeicher oder Monitore, die so zu besonders leichten Zielen für Vandalismus-Attacken werden, beispielsweise durch „böswillige USB-Geräte“.

Der physische Zugang gilt als größte Hintertür für Cyberkriminelle!

Darüber hinaus müssen mindestens diese Anforderungen erfüllt sein:

- Ausgearbeitete Konzepte für die Risikoanalyse und Sicherheit von IT-Systemen sowie zur Bewältigung von Sicherheitsvorfällen
- Maßnahmen zur Aufrechterhaltung des Betriebs (Business Continuity Management) durch Krisenmanagement und Backup-Maßnahmen zur Datenwiederherstellung
- Sicherheit in der Lieferkette (Umgang mit Geschäftspartnern und Dienstleistern, Sicherheitsmaßnahmen bei Erwerb und Entwicklung von Informationssystemen)
- Sicherheit in der Beschaffung, Entwicklung und Wartung von IT und Netzwerk-Systemen inklusive Schwachstellen-Management
- Vorgaben zur Messung von Cyber- und Risikomaßnahmen
- Schulungen zur IT-Sicherheit und grundlegende Verfahren der Cyberhygiene (z. B. Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement oder Sensibilisierung der Nutzer […]; s. NIS2 Vorwort, Punkt 89)
- Kryptographie und Verschlüsselung von Daten
- Sicherheit des Personals einschließlich Konzepten für Zugriffskontrolle und Anlagenmanagement (ISMS / Informationssicherheitsmanagementsystem)
- Sichere Authentifizierung und Kommunikation

Umsetzung der NIS2-Vorgaben – der Countdown läuft!

Anders als bei einer Verordnung, die von allen EU-Ländern vollumfänglich umgesetzt werden muss, ist es bei Richtlinien wie der NIS2 Sache der einzelnen Länder, eigene Rechtsvorschriften zur Verwirklichung der darin festgelegten Ziele zu erlassen. Derzeit liegt das NIS2-Umsetzungsgesetz als Referentenentwurf vor, der bis zum Ablauf der Frist am 17. Oktober 2024 die Gesetzgebung auf Bundesebene durchlaufen haben muss. Unternehmen, die zu den wichtigen oder besonders wichtige Einrichtungen zählen, sollten jedoch schon jetzt mit den Vorbereitungen beginnen, denn eine Übergangsphase für die Umsetzung ist nicht vorgesehen, und: Risikoanalysen, Lieferkettenkontrolle, Sicherheitsmaßnahmen und die Auswahl geeigneter Produkte brauchen erfahrungsgemäß ihre Zeit!

Mögliche Schwachstellen in der Schließtechnik aufspüren und schließen

Je eher Betriebe also mit ihrer NIS2-Vorbereitung beginnen, desto besser und Vorkehrungen zum physischen Schutz der Anlagen spielen dabei eine zentrale Rolle. Bei ihrer Bestandsaufnahme sollten sich Sicherheitsverantwortliche intensiv mit bereits bestehenden Sicherheitsvorkehrungen und Schließlösungen befassen und deren Zukunftsfähigkeit bestimmen. Besonders ältere mechanische Schließanlagen können für Betreiber zu einem Haftungsrisiko werden, wenn beispielsweise der Patentschutz abgelaufen ist. Ist dies der Fall, müssen Fachgeschäfte keinen Kontakt mehr zum Hersteller aufnehmen und Schlüsselkopien können ohne Rückfragen angefertigt werden: Ein enormes Sicherheitsrisiko, bei dem Unternehmen die Folgekosten für etwaige Versorgungsausfälle selbst tragen müssen, da sie keine ausreichenden Schutzmaßnahmen nachweisen können. Erfahrungsgemäß wird es proportional zum Alter solcher Schließanlagen auch zunehmend komplexer, die Anzahl der im Umlauf befindlichen Schlüssel im Auge zu behalten und ein zeitnahes Reagieren auf

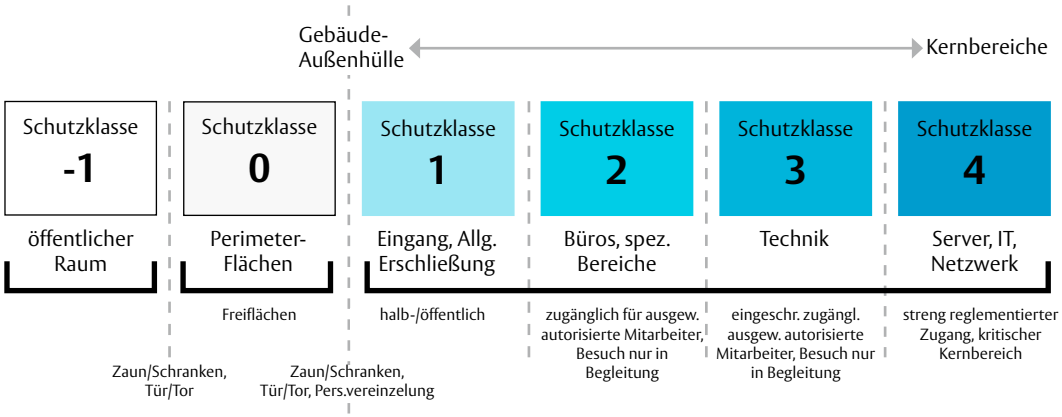
Schlüsselverluste kaum möglich. Handelt es sich bereits um ein elektronisches System, das per Kabel angeschlossen ist, gilt es sicherzustellen, dass auch bei Unterbrechungen der Stromzufuhr die Funktionalität weiterbesteht. Anhand der folgenden Checkliste lässt sich erkennen, ob bei der Schließanlage akuter Handlungsbedarf besteht.

Checkliste: Wie zukunftssicher ist mein Schließsystem?

- Verfügt mein Schließsystem über einen gültigen Patentschutz?
- Entspricht das Schließsystem dem aktuellen Stand der Technik?
- Ist die Türtechnik aktuell (Türschließer, Schlösser etc.)?
- Ist ein Betrieb bei Unterbrechung der Stromzufuhr (Blackout) gewährleistet?
- Sind Zutrittsereignisse nachvollziehbar und werden diese dokumentiert?
- Existiert ein ausgearbeitetes Sicherheitskonzept?
- Wie umfassend ist die Schlüsselorganisation?
- Befinden sich möglicherweise nicht autorisierte Schlüssel im Umlauf?
- Wie schnell kann auf Schlüsselverluste reagiert werden?

Ganzheitlicher Schutz Ihrer Daten vor physischen Bedrohungen

Ob in der Industrie, der öffentlichen Verwaltung oder im Gesundheitswesen: Als Schalt- und Speicherzentralen für den elektronischen Informationsaustausch bilden moderne Datenzentren das Herzstück vieler Unternehmen und Organisationen. Die effektive Sicherung der dort konzentrierten physischen und digitalen Vermögenswerte ist von zentraler Bedeutung für die Aufrechterhaltung der kritischen betrieblichen Funktionen und die Reputation eines Unternehmens. Die zur Absicherung dieser sensiblen Bereiche bereits etablierten Normen und „Best Practices“ bilden eine gute Ausgangsbasis für entsprechende Maßnahmen entlang der gesamten betrieblichen Infrastruktur, wie sie die NIS2 vorsieht. Zur ersten Orientierung empfiehlt sich daher die europäische Normenreihe EN 50600 „Einrichtungen und Infrastrukturen von Rechenzentren“, die einen stufenweisen Aufbau der Absicherungsmaßnahmen nach dem „Zwiebelschalenprinzip“ beschreibt. Schicht um Schicht bauen dabei unterschiedliche sicherheitsrelevante Klassen aufeinander auf und steigern sich von außen nach innen. Ein typischer Aufbau folgt beispielsweise diesem Schema:



Synergien von elektronischer Schließanlage und Zutrittskontrollsystem nutzen

Um ein entsprechendes Sicherheitskonzept aufzuspannen, bieten digitalisierte und vernetzte Sicherheitslösungen klare Vorteile gegenüber mechanischen Systemen. Das beginnt mit der einfachen Verwaltung von Zutrittsrechten und Berechtigungen einzelner Mitarbeiter und geht über den Diebstahlschutz bis hin zum Brandschutz. Gerade bei der physischen Absicherung – also beim Schutz von Mitarbeitern, Inventar sowie analogen und digitalen Daten vor äußeren Gefahren und Ereignissen – können vernetzte Schließanlagen und Zutrittskontrollsysteme ein Mehr an Komfort und Sicherheit generieren. Zwei Sicherheitslösungen, die dabei mit großer Flexibilität punkten, sind das schlüsselbasierte elektronische Schließsystem eCLIQ und die Zutrittskontrolle SCALA von ASSA ABLOY.

eCLIQ - Flexible Schließlösung für jede Anforderung und Gebäudegröße

Vom Einfahrtstor eines Firmengeländes über die Briefkastenanlage und den Aufzug bis zum Aktenschrank: Alles, was abschließbar ist, lässt sich mit über 60 verfügbaren Zylindertypen in eine eCLIQ-Schließanlage integrieren. Das rein elektronische System bietet hohen Schutz gegen Manipulation und intelligente Angriffe und eignet sich zur Auslegung von Schließanlagen in jeder Größenordnung und in Objekten aller Art. Veränderte Zugangsberechtigungen lassen sich mit eCLIQ flexibel durch die Vergabe von Rechten festlegen. Ziehen Mitarbeiter oder eine ganze Abteilung um, ist es nicht notwendig, die Zylinder auszuwechseln. Verlorene Schlüssel stellen keine Sicherheitslücke mehr dar, da sie einfach deaktiviert werden. Und auch zeitlich und räumlich begrenzte Berechtigungen sind möglich, beispielsweise um Technikern eine individuelle Autorisierung für einen konkreten Auftrag zu erteilen. Bei großen Unternehmen kann es sinnvoll sein, zeitlich begrenzte Zugangsberechtigungen zu erteilen. Um am darauffolgenden Tag wieder in das Gebäude zu gelangen, ist eine erneute Validierung der auf dem Schlüssel gespeicherten Zutrittsberechtigungen an einem Updateterminal erforderlich.

Weitere Vorteile von eCLIQ:

- Einfache Installation dank „Plug and Play“-Lösung: Die Installation erfordert keine Verkabelung oder bauliche Maßnahmen.
- Langlebige Schließlösung: Die Zylinder sind komplett wartungsfrei. Zusammen mit den robusten und wasserdichten eCLIQ-Schlüsseln ist das Schließsystem auch für anspruchsvolle Umweltbedingungen geeignet.
- Die Energieversorgung erfolgt allein über eine leicht auszuwechselnde Standard-Batterie im Schlüssel, die werkzeuglos gewechselt werden kann.

Zutrittskontrolle SCALA – Jede Tür jederzeit im Blick haben

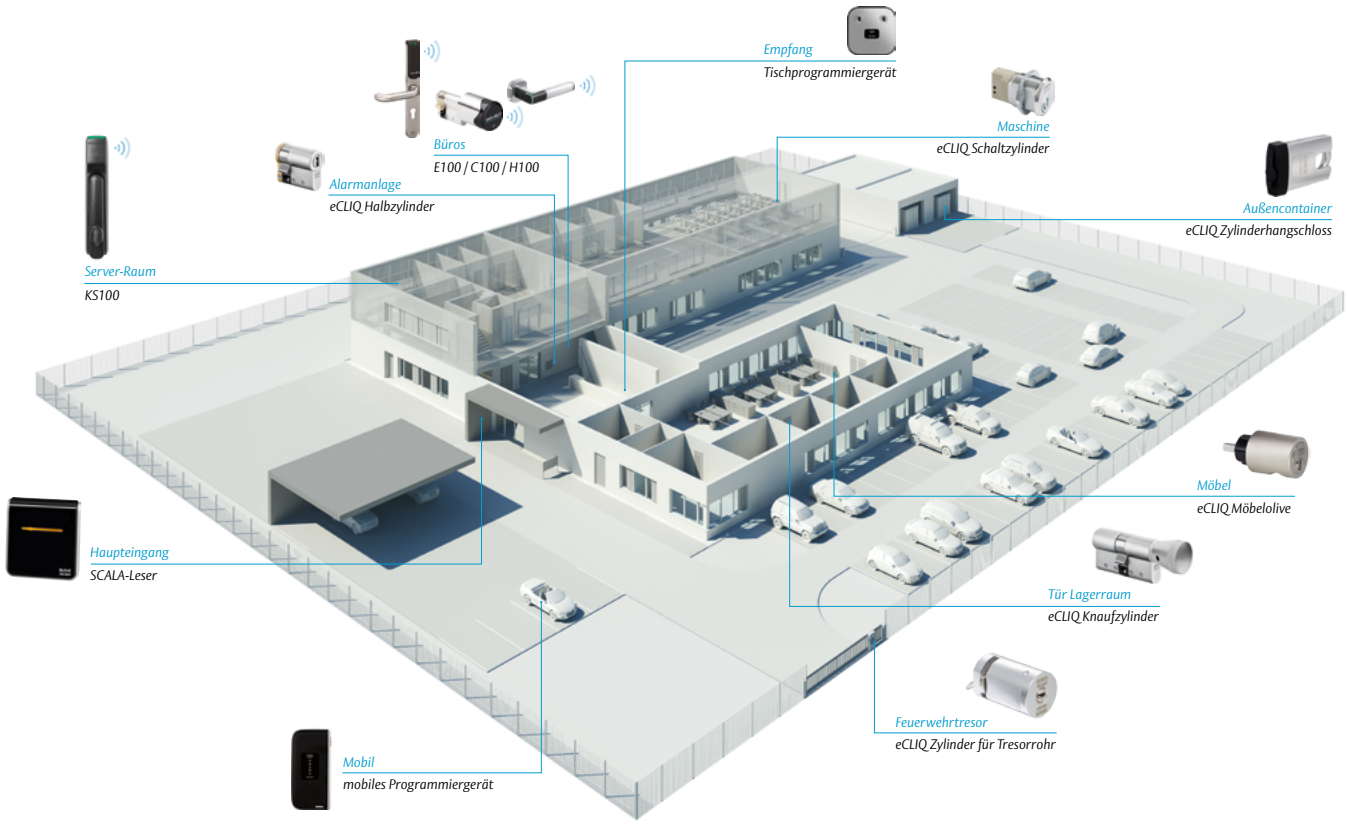
Anders als beim schlüsselbasierten elektronischen Schließsystem lässt sich mit einem digitalen Zutrittskontrollsystem zusätzlich auch der Türzustand zu jedem Zeitpunkt überwachen und regeln. Wird ein RFID-basiertes Medium (Schlüsselanhänger, Karte oder Smartphone) an den Leser gehalten, überprüft das System in Echtzeit die Identifikation des Nutzers. Der Türzustand wird an eine Zentrale gemeldet und kann von dort von Sicherheitsverantwortlichen überwacht werden. Nach Bedarf – beispielsweise, wenn eine Tür zu lange offensteht – kann gehandelt werden. Ob online verdrahtet oder offline: die SCALA Zutrittskontrolle von ASSA ABLOY bietet für jeden Einsatzbereich die passende Lösung. Das komfortable Zutrittskontrollsystem beginnt bei der kleinsten Variante SCALA solo mit nur einer Hardware-Komponente und reicht bis zur Client-Server-Lösung SCALA net für beliebig viele Türen.

Die Vorteile von SCALA im Überblick:

- SCALA ist das komfortable Zutrittskontrollsystem, das mit nur einer Hardware-Plattform frei skalierbar ist, von einer Einzeltür bis hin zu jeder gewünschten Türenanzahl.
- Ein Update auf eine größere Version ist dadurch jederzeit möglich. ASSA ABLOY SCALA ist die perfekte Lösung für kleine Objekte, mittelgroße Unternehmen sowie große Unternehmen mit komplexen Anforderungen.
- SCALA net erlaubt eine in ein Netzwerk integrierte Anlagenstruktur und bietet den vollen Funktionsumfang einer Zutrittskontrolllösung, beispielsweise Zeitschaltung, Zonenüberwachung oder Aufzugssteuerung. Dank des modularen Aufbaus lässt sich die Lösung durch die Vergabe von Lizenzen leicht erweitern.

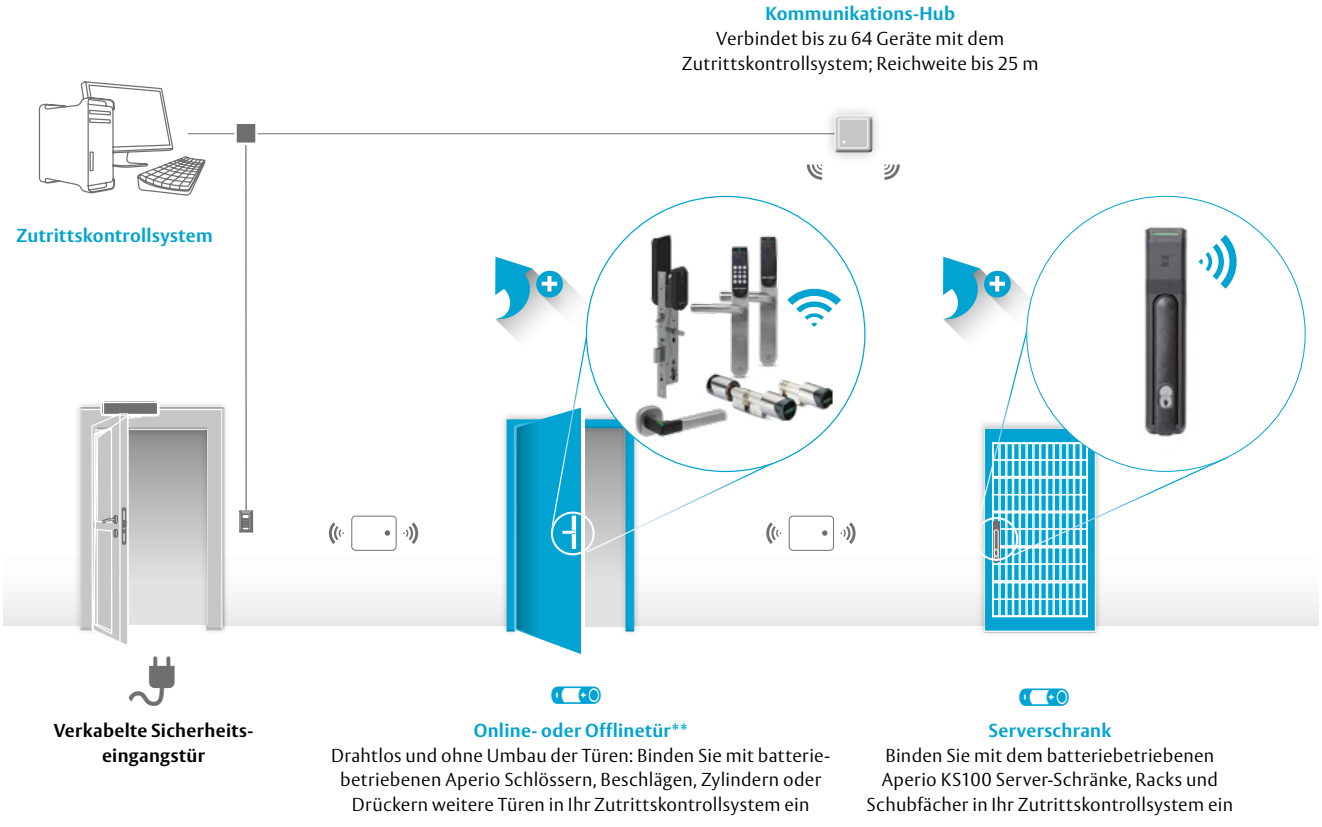
Vorteile von Karte und Schlüssel in einer gemeinsamen Oberfläche verwalten

Gerade bei größeren Objekten werden oft karten- und schlüsselbasierte Systeme zugleich genutzt. Ein solches Vorgehen bewährt sich beispielsweise bei sehr unterschiedlichen Nutzergruppen – je nachdem, ob Nutzer häufig wechseln, zusätzliche Kartenfunktionen verwendet werden oder ein Zutritt auch im Notfall möglich sein soll. In solchen Fällen werden Türen dann mit beiden Zutrittslösungen ausgestattet und die Nutzer erhalten dementsprechend Karte oder Schlüssel oder eine Kombination aus beidem. Auf diese Weise lassen sich hochspezifische Sicherheitsstufen für jede Tür und jeden Nutzer definieren und flexibel auswählen. Mit der CLIQ® Web-Manager-Integration in SCALA net hat ASSA ABLOY eine Lösung geschaffen, solche redundanten Systeme in einer einzigen Nutzeroberfläche zu verwalten.



Sicherheit von der ersten bis zur letzten Verteidigungslinie

Mit der drahtlosen Aperio-Technologie, die sich ebenfalls über SCALA net verwalten lässt, ist es möglich, die Zutrittskontrolle an einer Vielzahl von Türen aufzurüsten – unabhängig davon, ob Sie sich für eine Online- oder Offline-Integration entscheiden. Das umfassende Sortiment an zertifizierter, batteriebetriebener Schließtechnik ermöglicht die Sicherung der Außenhaut des Datenzentrums, des Serverraums und einzelner Serverschränke bei voller Einbindung in das vorhandene Zutrittskontrollsystem.



Racks sind die letzte Verteidigungslinie gegen physische Zugriffe auf IT-Ausstattung und Daten, bleiben aber häufig ohne Überwachung. Das Aperio KS100 Serverschrank-Schloss hilft, die Schutzvorgaben in Datenzentren und Colocation-Einrichtungen zu erfüllen, indem es eine Echtzeit-Zugangskontrolle für einzelne Serverschrank-Türen innerhalb eines Zutrittskontrollsystems bietet. So erhalten Sicherheitsverantwortliche auch auf Serverschrankebene ohne Zeitverzögerung Berichte über mögliche Sicherheitsvorfälle und können schnell Gegenmaßnahmen einleiten.

Hand in Hand zu mehr cyberphysischer Resilienz – mit dem richtigen Partner

Unabhängig davon, ob Ihr Unternehmen von den Vorgaben der NIS2-Richtlinie betroffen ist oder nicht: Die Investition in ein modernes Zutrittskontroll-System trägt dazu bei, den Schutz eigener sowie kundenspezifischer Informationen und Vermögenswerte zu erhöhen. Da die Konzeption einer Schließanlage ein komplexes Verfahren ist, unterstützen Sie unsere geschulten Experten dabei gerne. Profitieren Sie von unserer jahrzehntelangen Erfahrung im Bereich Sicherheitstechnik und der Innovationskraft unseres international agierenden Unternehmens, das in rund 70 Ländern aktiv ist, und nehmen Sie Kontakt auf unter: www.assaabloy.com/de und www.assaabloy.com/at

Die ASSA ABLOY Gruppe ist der Weltmarktführer in Zugangslösungen. Jeden Tag helfen wir Menschen sich sicherer und geborgener zu fühlen und eine offenere Welt zu erleben.

ASSA ABLOY
Opening Solutions

ASSA ABLOY Sicherheitstechnik GmbH
Attilastraße 61–67
12105 Berlin
DEUTSCHLAND
Tel. +49 30 8106-0
berlin@assaabloy.com

www.assaabloy.com/de

ASSA ABLOY Austria GmbH
Hütteldorfer Straße 216 c
1140 Wien
ÖSTERREICH
Tel. +43 (0) 1 212 51 11
wien@assaabloy.com

www.assaabloy.com/at