Simons Voss technologies

UPDATE NIS-2

Physische Sicherheit im Fokus

Inhalt

Aktueller Stand in Deutschland

Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) (im Folgenden: NIS-2-Umsetzungsgesetz) ist eine europäische Verordnung mit dem Ziel, die Cybersicherheit in der Europäischen Union zu stärken, indem sie einen umfassenderen und einheitlicheren Rahmen für den Schutz kritischer Infrastrukturen und digitaler Dienste schafft. Die Richtlinie verlangt von Mitgliedstaaten, Unternehmen und Organisationen, strengere Sicherheitsmaßnahmen zu implementieren und eine bessere Zusammenarbeit im Falle von Cyberangriffen zu gewährleisten. Dies umfasst unter anderem eine erweiterte Meldepflicht für Sicherheitsvorfälle, eine stärkere Regulierungsaufsicht und höhere Strafen für die Nichteinhaltung der Vorschriften. NIS-2 soll somit einen wesentlichen Beitrag zur Resilienz und Sicherheit der digitalen Landschaft Europas leisten.

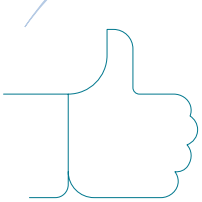
Das NIS-2-Umsetzungsgesetz trat am 14. Dezember 2022 in Kraft und verpflichtete die EU-Mitgliedstaaten, die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen. Doch seitdem das novellierte NIS-2-Umsetzungsgesetz im Amtsblatt der Europäischen Union veröffentlicht wurde, konnte keine Umsetzung in deutsches Recht erreicht werden. Die Ampel-Regierungskoalition hatte vorgesehen, die NIS-2-Richtlinie durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz bis März 2025 in deutsches Recht zu überführen, doch das parlamentarische Verfahren zum Gesetz konnte nicht abgeschlossen werden.

Endgültig in Kraft trat das NIS-2-Umsetzungsgesetzt in Deutschland am 06.12.2025 und setzt die EU-Richtlinie für ein höheres Cybersicherheitsniveau um. Es betrifft Unternehmen ab 50 Mitarbeitern oder 10 Mio. € Umsatz in 18 Sektoren. Die Geschäftsführung trägt direkte Verantwortung für IT-Sicherheit, und betroffene Einrichtungen mussten sich bis zum 06.03.2026 beim BSI registrieren.

„Seit das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) gilt, müssen alle Pflichten eingehalten werden. Betroffene Unternehmen haben daher keine Wahl. Sie müssen sich mit den Inhalten des jüngsten Entwurfs auseinandersetzen und mit der Abarbeitung der formulierten Anforderungen sofort beginnen.

Ich gehe sogar einen Schritt weiter, NIS-2 ist nicht nur eine rechtliche Vorgabe, sondern ein Versprechen: ein Versprechen an uns alle, einen sichereren Raum zu schaffen, in dem unsere Gesundheit, unser Wohlstand und unsere Werte geschützt sind.“

ULRICH IRNICH,
Executive Tech Advisor und früherer CIO von Vodafone Germany



DER SCHUTZ KRITISCHER INFRASTRUKTUREN BETRIFFT SOWOHL DIE DIGITALE WIE AUCH DIE PHYSISCHE UMGEBUNG. MIT SIMONS VOSS HABEN SIE EINEN VERLÄSSLICHEN PARTNER FÜR DEN PHYSISCHEN SCHUTZ IHRER INFRASTRUKTUR AN DER HAND.

Simons Voss technologies

Wer ist von NIS-2 betroffen?

Das NIS-2-Umsetzungsgesetz betrifft eine breitere Palette von Unternehmen und Organisationen im Vergleich zur ursprünglichen NIS-Richtlinie. Betroffen sind hauptsächlich zwei Kategorien von Betreibern: wesentliche und wichtige Diensteanbieter. Diese Kategorien umfassen verschiedene Sektoren und Branchen. Hier eine detaillierte Übersicht:

1. Wesentliche Diensteanbieter

Diese Unternehmen und Organisationen erbringen Dienstleistungen, die für die Aufrechterhaltung von wichtigen gesellschaftlichen und wirtschaftlichen Aktivitäten unerlässlich sind. Zu den wesentlichen Diensteanbietern gehören:

Energie
- :: Strom- und Gaserzeugung, -übertragung und -verteilung
- :: Erdölproduktion, -raffinierung, -lagerung und -transport

Transport
- :: Fluggesellschaften und Flughäfen
- :: Eisenbahngesellschaften und Bahnhöfe
- :: Schifffahrtsunternehmen und Häfen
- :: Straßenverkehrsunternehmen

Bankwesen
- :: Kreditinstitute

Finanzmarktinfrastrukturen
- :: Börsen und zentrale Gegenparteien

Gesundheitswesen
- :: Krankenhäuser und andere Gesundheitseinrichtungen
- :: Pharmazeutische Unternehmen

Trinkwasserversorgung und -verteilung

Digitale Infrastruktur
- :: Internet Exchange Points (IXPs)
- :: Domain Name System (DNS)-Dienste
- :: Cloud-Computing-Dienste

2. Wichtige Diensteanbieter

Diese Unternehmen und Organisationen erbringen Dienstleistungen, die ebenfalls bedeutend sind, aber nicht denselben kritischen Einfluss wie die wesentlichen Dienste haben. Zu den wichtigen Diensteanbietern gehören:

Post- und Kurierdienste

Abfallwirtschaft
- :: Entsorgung und Recycling von Abfällen

Chemische Industrie
- :: Herstellung von Chemikalien

Lebensmittelindustrie
- :: Produktion und Vertrieb von Lebensmitteln

Herstellung
- :: Herstellung von medizinischen Geräten und Arzneimitteln

3. Weitere betroffene Sektoren

Das NIS-2-Umsetzungsgesetz erweitert auch den Fokus auf Sektoren wie:

Öffentliche Verwaltung
- :: Nationale, regionale und lokale Behörden

Digitale Dienste
- :: Online-Marktplätze
- :: Suchmaschinen
- :: Social Media Plattformen

Quellen:
PwC Deutschland (https://www.pwc.de/de/cyber-security/europaeische-nis-2-richtlinie-implikationen-fuer-unternehmen-und-institutionen.html#:~:text=Die%20NIS%2D2%2DRichtlinie%20ist,2024%20in%20nationales%20Recht%20umsetzen.)

Welche Herausforderungen gibt es und wie können Sie diese meistern?

Mit der Anpassung des NIS2-Umsetzungsgesetzes ergeben sich Herausforderungen für Unternehmen, die einzelne Branchen besonders betreffen. Insgesamt erfordert das NIS2-Umsetzungsgesetz von Unternehmen ein höheres Maß an Aufmerksamkeit und Investition in Sicherheit, um den gesetzlichen Anforderungen gerecht zu werden und Systeme, Zugriffe und Daten besser zu schützen.

„Umso wichtiger ist ein mehrschichtiger Sicherheitsansatz wie die „Defense in Depth"-Strategie. Die physische Sicherheit stellt dabei eine eigene Verteidigungsebene dar. Physische Sicherheitsmaßnahmen schützen vor Diebstahl, Sabotage, Manipulation und anderen physischen Angriffen auf IT-Systeme."

VALERI MILKE,
CEO von VamiSec |
IT Security & Compliance Consulting

Der Ansatz der „Defense in Depth" basiert auf der Annahme, dass kein einzelnes Sicherheitsinstrument oder eine einzelne Sicherheitsmaßnahme absolut sicher ist. Daher werden mehrere Schichten von Schutzmaßnahmen implementiert, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu minimieren.

Physische Sicherheitsmaßnahmen verstärken die Wirksamkeit anderer Schichten in einem „Defense in Depth-Ansatz". Durch die Verwendung mehrerer Verteidigungsebenen, einschließlich physischer Sicherheitsmaßnahmen, wird sichergestellt, dass bei einem Ausfall einer Ebene andere verfügbar sind, um Bedrohungen zu stoppen.

Unternehmen, die die Anforderungen der NIS-2 erfüllen wollen, können das Defense-in-Depth-Modell als Grundlage nutzen, um ein robustes und widerstandsfähiges Sicherheitskonzept zu entwickeln.

Erweiterter Anwendungsbereich und höhere Sicherheitsanforderungen:

Unternehmen, die bisher nicht betroffen waren, müssen nun Compliance-Maßnahmen ergreifen. Striktere Sicherheitsmaßnahmen müssen eigenverantwortlich implementiert werden, um ihre Netzwerke und Informationssysteme zu schützen. Dies umfasst sowohl technische als auch organisatorische Maßnahmen. Oft fehlt inhouse das Know-how dafür.

Wir empfehlen: Es ist für Sie sinnvoll, Ihre aktuelle Infrastruktur (digital sowie physisch) kritisch zu hinterfragen, auch wenn Sie bisher nicht betroffen waren. Ggfs. binden Sie einen Experten ein, um Ihren Status Quo zu bewerten und sich Handlungsempfehlungen geben zu lassen.

Laut einem Bericht von KPMG gaben etwa **15 % der befragten Unternehmen** an, dass sie physische Sicherheitsvorfälle (einschließlich unbefugtem Zutritt) erlebt haben, während 85 % von digitalen Sicherheitsvorfällen betroffen waren.

Quelle: KPMG Cybersecurity Annual Report

Meldepflichten:

Das NIS-2-Umsetzungsgesetz verlangt eine schnellere und detailliertere Meldung von Sicherheitsvorfällen an die zuständigen nationalen Behörden. Unternehmen müssen sicherstellen, dass sie Mechanismen zur schnellen Erkennung und Meldung solcher Vorfälle haben.

Wir empfehlen: Diskutieren Sie vorab mit allen wichtigen Stakeholdern einen Krisenplan. Entwickeln Sie Maßnahmen für den Notfall und stimmen Sie diese mit einem Experten ab. Regelmäßige Workshops und Schulungen sichern einen reibungslosen Ablauf im Notfall.

Erhöhte Sanktionen:

Das NIS-2-Umsetzungsgesetz sieht strengere Sanktionen für die Nichteinhaltung vor. Dies kann zu hohen Geldstrafen führen, was einen erheblichen finanziellen und reputationsschädigenden Einfluss auf Unternehmen haben kann und die Geschäftsführung ist in der Haftung.

Wir empfehlen: Planen Sie vorausschauend und nicht erst hinterher. So sparen Sie Nerven, Energie und Kosten.

Kooperation und Informationsaustausch:

Ggf. müssen Sie mit nationalen und europäischen Behörden sowie anderen Unternehmen zusammenarbeiten, um Cyber-Bedrohungen zu bekämpfen. Dies erfordert einen effektiven Informationsaustausch und koordinierte Maßnahmen.

Wir empfehlen: Entwerfen Sie eine Checkliste für den Notfall. So wissen Sie, was im Ernstfall zu tun ist und verlieren keine Zeit oder können wichtige Aufgaben schnell delegieren. Definieren Sie Verantwortliche für bestimmte Aufgaben. Fehlt Ihnen inhouse das Know-how, können Sie für die Erstellung eines Krisenplans einen Experten beauftragen.

Compliance und Audits:

Unternehmen müssen möglicherweise regelmäßige Audits und Bewertungen ihrer Sicherheitsmaßnahmen durchführen lassen, um die Einhaltung des NIS-2-Umsetzungsgesetz nachzuweisen. Dies kann zusätzlichen administrativen Aufwand und Kosten bedeuten.

Wir empfehlen: Investieren Sie in Systeme, die Ihnen den administrativen Aufwand abnehmen. Digitale Zutrittskontrollsysteme beispielsweise protokollieren Zutritte und Zugriffe für alle Türen, Schränke oder Aufzüge. So können Sie jederzeit nachvollziehen, wer wann in welchen Bereichen Ihres Unternehmens war. Ähnliche Systeme gibt es auch für digitale Infrastrukturen. Informieren Sie sich vorab über die Angebote und vergleichen Sie passende Lösungen.

Technologische Anpassungen:

Die Einführung neuer Sicherheitsanforderungen kann technologische Anpassungen und Upgrades in den bestehenden IT-Infrastrukturen erfordern. Dies kann zu zusätzlichen Kosten und technischen Herausforderungen führen.

Wir empfehlen: Investieren Sie in digitale Schließsysteme, die auf- und abwärtskompatibel sind. Ändern sich Ihre Anforderungen an physische Zutritte, können Sie flexibel reagieren, anstatt neue Systeme kaufen zu müssen. So sparen Sie Kosten und schützen Ihre Investitionen. Im digitalen Bereich können Sie Ihre Bestandssysteme optimieren und weiterentwickeln und so ebenfalls bereits getätigte Investitionen schützen.

Physische Zugriffe:

Bedenken Sie, dass es Räume gibt, die besonders schützenswert sind, da sie Zugriff auf sensible Daten bieten. Dazu gehören z. B. Arbeitsplätze oder IT- & Serverräume, Schränke mit sensiblen Kunden- oder Patientendaten und Ähnliches.

Wir empfehlen: Investieren Sie in digitale Schließsysteme, die garantieren, dass nur befugte Personen mit entsprechendem Identifikationsmedium bestimmte Räume betreten können. Intelligentes Door Monitoring wird Sie außerdem informieren, wenn Türen nicht abgeschlossen sind oder länger als gewöhnlich offenstehen. Personelle Änderungen oder Schlüsselverlust können Sie außerdem mit wenigen Klicks bewältigen und so die Sicherheit für Ihr Unternehmen erhöhen und trotzdem flexibel bleiben. So beugen Sie Datenmissbrauch durch nicht autorisierten Zugang effektiv vor.

Beispiele für Herausforderungen, die ein digitales Schließsystem auf einfache Weise löst:

Wer wann und wo zutrittsberechtigt ist
(Es gibt keine „schwarzen“ Schlüssel oder Ähnliches)

Registrierung von Besuchern

Authentifizierung von bestimmten Mitarbeitern
für den Zugang zu vertraulichen Informationen

Protokollierung jedes Zutritts

Besondere Maßnahmen für externe Personen

Kontinuierliche Bewertung, Aktualisierung
und, falls erforderlich, Entzug von Zugangsrechten

„Wir sind derzeit im Zusammenhang mit Verschluss-Sachen (VS) der einzige Anbieter für digitale Schließtechnik, der einen Schließzylinder verwendet, der den Anforderungen des Bundesamts für Sicherheit in der Informationstechnik entspricht.“

DIEGO LA MARCA,
Experte für digitale Schließtechnik
bei SimonsVoss

Warum sich eine Investition in Ihre Sicherheit lohnt?

Investitionen in Sicherheit sind nicht nur eine Reaktion auf gesetzliche Anforderungen, sondern auch eine strategische Maßnahme, um die langfristige Stabilität und den Erfolg eines Unternehmens zu sichern. Durch die Implementierung von digitalen und physischen Sicherheitsmaßnahmen, die den Anforderungen des NIS-2-Umsetzungsgesetzes entsprechen, können Sie Ihre Netzwerke und physischen Zugriffe vor Datenverlust, Betriebsunterbrechungen und finanziellen Schäden schützen.

Außerdem ist das NIS-2-Umsetzungsgesetz eine verbindliche Vorgabe. Unternehmen, die diese Anforderungen nicht erfüllen, riskieren hohe Geldstrafen und rechtliche Konsequenzen. Durch frühzeitige Investitionen in Sicherheit können Sie rechtliche Risiken minimieren. Auch die DSGVO sieht vor, dass Daten- und Auftragsverarbeiter eigenverantwortlich geeignete technische und organisatorische Maßnahmen ergreifen, um sensible Daten vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung zu schützen (Art. 32, DSGVO).

Langfristige Kostenersparnis:

Präventive Maßnahmen zur Sicherung von Netzwerken, Informationssystemen und physischen Zugriffen können langfristig kostengünstiger sein als die Bewältigung der Folgen eines erfolgreichen Cyberangriffs.

Erhöhung der Resilienz:

Sicherheitsinvestitionen erhöhen die Widerstandsfähigkeit eines Unternehmens gegenüber zukünftigen Bedrohungen und helfen dabei, schneller auf Sicherheitsvorfälle zu reagieren und sich davon zu erholen. Dies verbessert die allgemeine Krisenbewältigungsfähigkeit.

Business Continuity:

(Zu Deutsch „Geschäftsfortführung“:) Strategien, Maßnahmen und Prozesse, die in einem Krisenfall (z. B. ausgelöst durch Cyberangriffe) den unterbrechungsfreien IT-Betrieb sichern oder nach einem Ausfall umgehend wiederherstellen. Um das Überleben eines Unternehmens zu sichern, sind geeignete Präventivmaßnahmen zu treffen, die zum einen die Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Reagieren in einer Krise ermöglichen.

(Quelle: https://www.myrasecurity.com/de/knowledge-hub/business-continuity-management/)

„Auf digitale Schließsysteme von SimonsVoss gibt es 5 Jahre lang Gewährleistung. Bevor Sie also hinterher die Kosten für die Konsequenzen eines Sicherheitsvorfalls tragen, empfiehlt es sich, frühzeitig sinnvoll zu investieren.“

SEBASTIAN SCHITTENBERGER,
Vertriebsleiter Österreich bei SimonsVoss

SimonsVoss technologies

Welche Konsequenzen gibt es für Ihr Unternehmen, wenn Sie nicht handeln?

Die Nichteinhaltung des NIS-2-Umsetzungsgesetzes kann für Unternehmen schwerwiegende Konsequenzen haben, die über finanzielle Strafen hinausgehen. Um diese Risiken zu vermeiden, ist es entscheidend, dass Unternehmen die erforderlichen Maßnahmen ergreifen, um den Anforderungen der Richtlinie zu entsprechen. Dies umfasst die Implementierung geeigneter Sicherheitsmaßnahmen, regelmäßige Überprüfung der Sicherheitsvorkehrungen und Schulung der Mit arbeiter. Die Einhaltung des NIS2-Umsetzungsgesetzes trägt nicht nur zur rechtlichen und finanziellen Absicherung bei, sondern stärkt auch die allgemeine Sicherheit und Resilienz des Unternehmens.

>> Kosten für Bußgelder, Strafen (Haftung der Geschäftsführung) und Geschäftsschäden

>> Betriebsunterbrechungen

>> Datenverlust

>> Vertrauensverlust von Kunden, Geschäftspartnern und Öffentlichkeit

>> Erhöhter Versicherungsbeitrag

>> Verlust von Geschäftsmöglichkeiten

Unsere Lösungen für physische Sicherheit: Die Vorteile von digitalen Schließsystemen

Zutrittskontrollsysteme:

Digitale Schließsysteme können mit Zutrittskontrollsystemen kombiniert werden, die den Zugang basierend auf individuellen Berechtigungen regeln. Dies reduziert das Risiko unbefugten Zugangs erheblich.

Kosteneffizienz:

Die Implementierung und Wartung digitaler Schließsysteme kann langfristig kosteneffizienter sein, da der Bedarf an physischen Schlüsselkopien und -austauschen reduziert wird.

Zentrale Verwaltung:

Digitale Schließsysteme ermöglichen eine zentrale Verwaltung der Zutrittsberechtigungen. Berechtigungen können einfach und schnell vergeben, geändert oder entzogen werden, ohne physische Schlüssel austauschen zu müssen.

Integration mit anderen Sicherheitssystemen:

Digitale Schließsysteme können mit Alarmanlagen, Überwachungskameras und anderen Sicherheitstechnologien kombiniert werden, um ein umfassendes Sicherheitsnetzwerk zu schaffen.

Protokollierung und Überwachung:

Moderne digitale Schließsysteme bieten umfassende Protokollierungsfunktionen, die genau aufzeichnen, wer wann Zugang zu welchen Bereichen hatte. Diese Protokolle können in Echtzeit überwacht und ausgewertet werden.

Schnelle Reaktion auf Sicherheitsvorfälle:

Bei Verlust oder Diebstahl eines digitalen Identmediums kann diese sofort deaktiviert werden, ohne dass physische Schlösser ausgetauscht werden müssen.

„Eine typische Angst ist, dass eine Umrüstung auf eine digitale Schließanlage sehr komplex wäre. Jedoch ist genau das Gegenteil der Fall: Bevor Sie eine defekte mechanische Tür reparieren, rüsten Sie diese doch auf. Sie können die Umrüstung nach und nach vornehmen – Kosten und Aufwand minimieren sich."

SEBASTIAN SCHITTENBERGER,
Vertriebsleiter Österreich bei SimonsVoss

SimonsVoss technologies

Konkrete Anwendungsbeispiele für digitale Schließanlagen

... in der öffentlichen Verwaltung:

In öffentlichen Einrichtungen müssen öffentliche und nicht-öffentliche Bereiche getrennt werden. Zum Beispiel sollte ein Lehrerzimmer in einer Schule stets verschlossen sein. Friedhöfe müssen nachts verschlossen sein. Für Sporthallen oder Versammlungsräume sollte die Nutzung möglichst flexibel sein. Schließsysteme für öffentliche Verwaltungsgebäude sollten auch zeitlichen Anforderungen oder einer spontanen Umnutzung der Räume gerecht werden.

... für das Gesundheitswesen:

Gerade in Krankenhäusern ist eine strikte Trennung in öffentliche und nicht-öffentliche Bereiche sowie eine sichere Zutrittskontrolle erforderlich. Dazu kommen hoch sensible Bereiche wie zum Beispiel Medikamentenschränke und Dienstzimmer. Schließsysteme für das Gesundheitswesen sollten auch rechtlichen Anforderungen und Personalfluktuation gerecht werden.

Unsere digitalen Schließanlagen decken auch die individuellen Bedürfnisse von folgenden Branchen ab:

:: Energie

Große Energieunternehmen müssen den Zugang zu zahlreichen Standorten und Anlagen verwalten. Dies umfasst die Verwaltung von Schlüsseln, die Zuordnung von Zugangsrechten und das Nachverfolgen von Zugangshistorien. Ein digitales Schließsystem übernimmt diese Aufgaben zuverlässig.

:: Transport / Verkehr

Die Sicherung von Fahrzeugen (z.B. LKWs, Lieferwägen) und Frachtcontainern gegen Diebstahl und unbefugten Zugang ist eine zentrale Aufgabe. Traditionelle **mechanische Schlösser** können leicht geknackt oder mechanische Schlüssel dupliziert werden, was das Risiko für Diebstahl und unbefugten Zugriff erhöht. Im Falle eines Notfalls oder Sicherheitsvorfalls kann der Zugang zu Fahrzeugen oder Containern mithilfe digitaler Zutrittskontrolle aus der Ferne gesperrt oder freigegeben werden.

:: Entsorgung

Entsorgungsanlagen und Recyclinghöfe beherbergen oft wertvolle Materialien und Ausrüstungen, die vor Diebstahl und Vandalismus geschützt werden müssen. Die Verwaltung des Zugangs für verschiedene Mitarbeitergruppen und externe Dienstleister ist eine Herausforderung, die effektiv von digitalen Schließsystemen gelöst werden kann.

:: Finanzsektor

Im Finanzsektor sind die Anforderungen an die physische Sicherheit besonders hoch, da dieser Sektor sensible Informationen und große Geldmengen verwaltet. IT-Räume, Datenzentren und Archivräume sollten besonders vor unbefugtem Zugang geschützt werden. Tresorräume und Geldautomaten sind attraktive Ziele für Diebstahl und Einbruch. Traditionelle mechanische Schlösser bieten nicht immer ausreichenden Schutz und können manipulierbar sein.

Digitale Schließsysteme bieten die Möglichkeit, alle Zutrittsversuche zu protokollieren. So können Zutritte in Echtzeit überwacht werden. Dies ermöglicht eine sofortige Reaktion bei unbefugten Zugriffsversuchen und hilft bei der Nachverfolgung im Falle eines Sicherheitsvorfalls. Digitale Schließsysteme können außerdem in bestehende Sicherheitsinfrastrukturen integriert werden, sodass unbefugte Zugriffsversuche sofort erkannt und entsprechende Maßnahmen ergriffen werden können.

:: Informationstechnik und Telekommunikation

Rechenzentren und Serverräume beherbergen die wichtigsten IT-Infrastrukturen eines Unternehmens, einschließlich Server, Netzwerkgeräte und Datenbanken. Der Zugang zu diesen Bereichen muss streng kontrolliert werden, um unbefugten Zugriff und potenzielle Sicherheitsvorfälle zu verhindern. Mit digitalen Schließsystemen können Zugangsrechte individuell vergeben und verwaltet werden: Jeder Mitarbeiter erhält nur Zugang zu den Bereichen, die für seine Arbeit erforderlich sind. Dies minimiert das Risiko von Insider-Bedrohungen.

:: Digitale Dienste

Unternehmen, die digitale Dienste anbieten, müssen ihre Bürogebäude und insbesondere die Entwicklungsbereiche, in denen vertrauliche Softwareentwicklungen und sensible Daten bearbeitet werden, vor unbefugtem Zugang schützen. Die Verwaltung von Zugangsberechtigungen für Mitarbeiter und Besucher ist dabei besonders wichtig. Mit digitalen Schließlösungen können Berechtigungen zentral verwaltet und bei Bedarf sofort angepasst werden. Dies ist besonders nützlich bei Personaländerungen oder Änderungen in den Projektanforderungen.

:: Raumfahrt

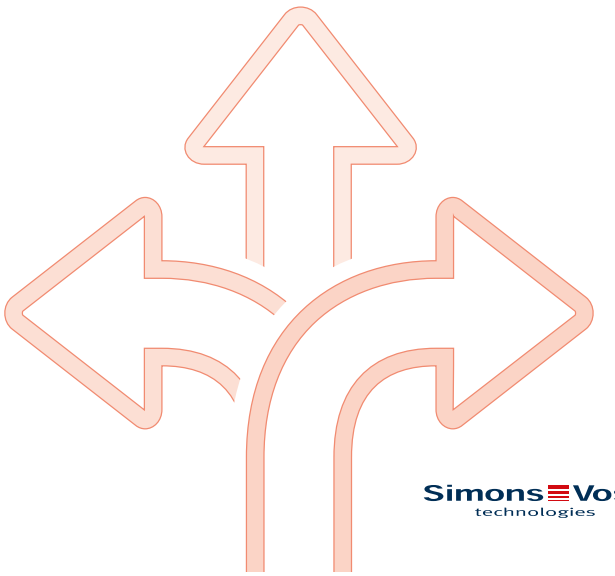
Raumfahrtunternehmen betreiben Forschungseinrichtungen und Technologiezentren, in denen hochentwickelte Technologien, sensitive Daten und Prototypen entwickelt und getestet werden. Der Zugang zu diesen Einrichtungen muss streng kontrolliert werden, um die Integrität der Projekte und die Sicherheit der Technologien zu gewährleisten.

:: Lebensmittel

Lebensmittelproduktionsstätten und Lagerhäuser müssen vor unbefugtem Zugriff geschützt werden, um die Sicherheit und Qualität der Lebensmittel zu gewährleisten. Zudem müssen sensible Bereiche wie Kühlräume, in denen verderbliche Waren gelagert werden, streng kontrolliert werden. Digitale Schließsysteme ermöglichen es, Zugangskontrollen für verschiedene Bereiche wie Produktionslinien, Lagerbereiche, Kühlräume und Verwaltungsbüros individuell zu verwalten und minimieren so den manuellen Aufwand und erhöhen die Sicherheit.

:: Verarbeitende Industrie / Gewerbe

Digitale Schließsysteme ermöglichen eine differenzierte Vergabe von Zugangsrechten basierend auf den Rollen und Verantwortlichkeiten der Mitarbeiter. Zum Beispiel erhalten Produktionsmitarbeiter Zugang zu spezifischen Maschinen und Anlagen, während Wartungspersonal Zugang zu den entsprechenden Wartungsbereichen hat.



Simons Voss technologies

So funktioniert digitales Schließen und Öffnen

ZENTRALE SYSTEMSTEUERUNG

Die Zutrittsberechtigungen werden mit der bewährten LSM Software oder der zukunftsweisenden AXM Software verwaltet.

IDENTMEDIEN

Transponder, FORTLOX Key, SmartCards und Co. bündeln die Zutrittsrechte ihres Besitzers. Existiert eine Zutrittsberechtigung, kann die entsprechende Schließkomponente bedient werden.

SYNCHRONISATION

Die Berechtigungen werden per SmartStick, SmartRelais oder per Smartphone übertragen.

Bluetooth

25 kHz B-Feld

DIGITALE SCHLIESSKOMPONENTEN

Je nach Einsatzbereich stehen unterschiedliche Komponenten zur Verfügung – für Indoor- und Outdoor-Anforderungen.

Wie können Sie starten?

Wir sind erfahren im Umgang mit digitalen Schließlösungen für unterschiedlichste Geschäftsbereiche: Elektronische Zylinder und smarte Türschlösser sind genauso schnell und einfach eingebaut wie herkömmliche Ausführungen. Die Montage ist absolut problemlos und sauber.

SEBASTIAN SCHITTENBERGER

Vertriebsleiter Österreich
bei SimonsVoss

DIEGO LA MARCA

Experte für digitale Schließtechnik
bei SimonsVoss

info-simonsvoss@allegion.com

Lassen Sie sich gerne von einem unserer Experten beraten oder laden Sie sich HIER kostenlos unsere Einsteigerbroschüre für digitales Schließen herunter.

Oder rufen Sie uns einfach an:
+49 (0)89 99 228 440

Worauf Sie sich bei einem SimonsVoss Schließsystem verlassen können:

Mehr Kontrolle und Sicherheit

Sicherheit bedeutet, dass unsere elektronischen Identifikationsmedien vor unerlaubtem Kopieren geschützt sind. Dass Sie sensible Bereiche mit kabelfreier Türüberwachung (Door Monitoring) zentral kontrollieren können. Und dass jeder Zutritt dokumentierbar ist.

Made in Germany

Seit wir als Pionier der digitalen Schließanlagen begonnen haben, fertigen wir sämtliche Bauteile an unserem eigenen Produktionsstandort in Deutschland. Qualität Made in Germany heißt bei uns: hohe Lebensdauer und Zuverlässigkeit mechanischer Bauteile, störungsfreier Betrieb – und nicht zuletzt minimaler Energieverbrauch. Wir erfüllen die DIN-Norm 15684 um das 7,5-fache und unsere Zylinder können bis zu 1,5 Millionen Mal betätigt werden.

Investitionssicherheit & Kompatibilität

Es ist seit jeher unser Credo, dass jede SimonsVoss Schließanlage kostengünstig und auch noch nach vielen Jahren problemlos mit neuer Software und neuen Bauteilen erweitert werden kann. Auf- und Abwärtskompatibilität unserer Produkte und Systeme bringt Investitionssicherheit.

Mehr Service

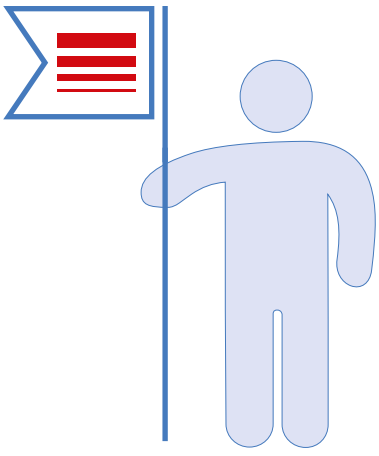
Zuverlässigkeit ist Vertrauenssache. Ganz egal, ob über Hotline, vor Ort oder remote: unsere bestens geschulten Service-Teams sind für Sie da.

Flexibilität

Auch wenn Sie zunächst nur einzelne Bereiche mit unseren Produkten sichern möchten, ist dies kein Problem: Sie können die Anlage jederzeit erweitern – übrigens auch gebäude- und standortübergreifend. Ihre bestehenden Systeme können integriert werden, seien es Zeit-/Zahlsysteme, Rolltore oder Ihr Lift.

„Von der Produktpräsentation bis zum Servicetermin gewährleistet SimonsVoss schnelle Terminabsprachen, Servicetermine vor Ort oder remote mit klarer Struktur und den gewünschten Informationen. Ich bin sehr zufrieden und empfehle das in unseren Betriebsstätten eingesetzte Produkt „Locking System Management Software (LSM)“ und die digitalen Schließzylinder für anspruchsvolle, variable Einsätze in besonderen Objekten.“

HEINER HEUMANN,
Staatstheater Braunschweig



SimonsVoss technologies

Das ist SimonsVoss

SimonsVoss, der Pionier funkgesteuerter, kabelloser Schließtechnik, bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, kleine und große Unternehmen sowie öffentliche Einrichtungen. SimonsVoss-Schließsysteme verbinden intelligente Funktionalität, hohe Qualität und preisgekröntes Design Made in Germany.

Als innovativer Systemanbieter legt SimonsVoss Wert auf skalierbare Systeme, hohe Sicherheit, zuverlässige Komponenten, leistungsstarke Software und einfache Bedienung. Damit wird SimonsVoss als ein Technologieführer bei digitalen Schließsystemen angesehen.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs.

Sie möchten mehr erfahren?

Unsere Experten beraten Sie gern.
Nehmen Sie am besten gleich Kontakt mit uns auf!

So erreichen Sie uns:

SimonsVoss Technologies GmbH
Münchner Straße 16
85774 Unterföhring
Deutschland

Tel. +49 (0)89 99 228 440

info-simonsvoss@allegion.com

www.simons-voss.com I www.allegion.com

SimonsVoss
technologies