SAIA BURGESS CONTROLS

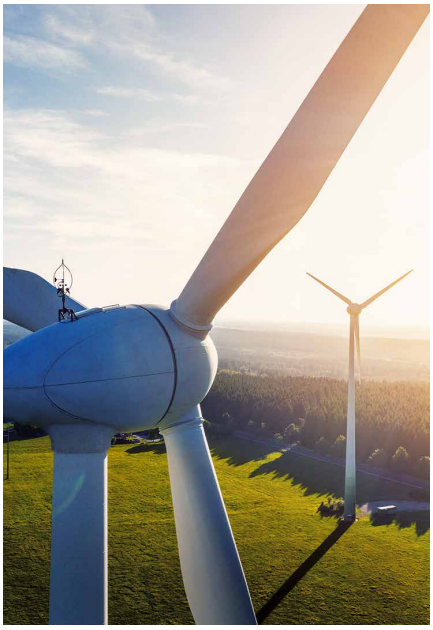
Cybersicherheit in intelligenten Gebäuden

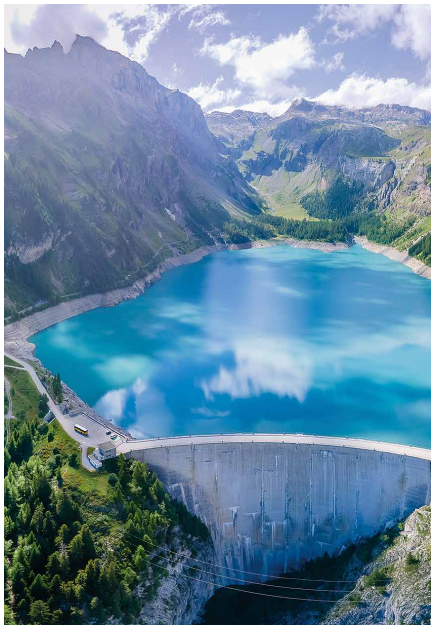
NIS2-Richtlinie – die wichtigsten Neuerungen

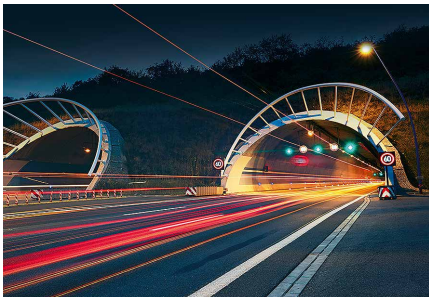
Machen Sie Ihre gewerblichen Gebäude cybersicher – mit dem Saia PCD® QronoX Controller

Mit der zunehmenden Digitalisierung steigt auch das Risiko von Cyberattacken. Um die Cyberresilienz zu stärken und eine gleichbleibend hohe Netzwerk- und Informationssicherheit zu gewährleisten, hat die EU rechtlich bindende Richtlinien veröffentlicht, die von den Mitgliedsstaaten mit dem Inkrafttreten entsprechender Umsetzungsgesetze in nationales Recht überführt werden. Eine davon ist die NIS2-Richtlinie.

Erfahren Sie, was Sie als Gebäudebetreiber jetzt beachten müssen und welche zukunftsweisenden Technologien von SBC Sie bei der Umsetzung der NIS2-Richtlinie unterstützen.



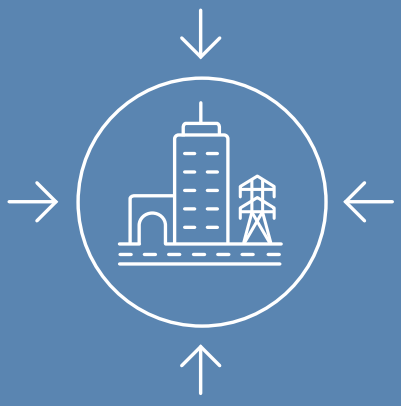




Zunehmende IT/OT-Konvergenz: Mehr Effizienz, aber auch höhere Risiken

Die zunehmende IT/OT-Konvergenz im Bereich Industrie-, Gebäude- und Infrastrukturautomation trägt dazu bei, Betriebsabläufe zu optimieren und Kosten zu senken. Dadurch sind jedoch neben IT-Anwendungen und -Systemen auch Gebäude und Infrastrukturen in zunehmendem Masse Cyberrisiken ausgesetzt. Gerade Angriffe auf kritische Infrastrukturen, beispielsweise im Bereich der Wasser- und Energieversorgung, haben in den letzten Jahren deutlich zugenommen.

Bitkom Research 2024



Um mit der zunehmenden Digitalisierung und der sich entwickelnden Bedrohungslage Schritt zu halten, trat 2023 die NIS2-Richtlinie in Kraft.

Zahlen und Fakten

8 von 10

Unternehmen in Deutschland sind von Datendiebstahl, Spionage oder Sabotage betroffen

267

Milliarden Euro Rekordschaden

2/3

aller deutschen Unternehmen fühlen sich durch Cyberangriffe in ihrer Existenz bedroht

Quelle: www.bitkom.org

Die NIS2-Richtlinie

NIS2 ersetzt die 2016 eingeführte NIS1 und zielt darauf ab, deren Schwachstellen zu beseitigen und für Einheitlichkeit zu sorgen. So sollen etwa Sicherheitsanforderungen, Meldepflichten und Sanktionen EU-weit vereinheitlicht werden. Der Gesetzgeber hat den Anwendungs-bereich von 10 auf 18 besondere und sonstige kritische Sektoren erweitert. Zusätzlich wurden zwei neue Kategorien eingeführt: wichtige und besonders wichtige Unternehmen. Sie sind für Wirtschaft und Gesellschaft von kritischer Bedeutung. Ziel dieser Änderungen ist es, Resilienz und Reaktionsfähigkeit weiter zu verbessern. Gebäudemanagementsysteme spielen dabei eine zentrale Rolle.

Infobox 1

Besonders wichtige Unternehmen

Grosse Unternehmen
- Mehr als 249 Angestellte oder mehr als 50 Millionen Euro Umsatz/Jahr, und
- tätig in einem Sektor mit hoher Kritikalität
- Betreiber kritischer Infrastrukturen jeder Grösse

Wichtige Unternehmen

Grosse Unternehmen
- In einem als kritisch definierten Sektor tätig

Mittlere Unternehmen
- Mehr als 50 Angestellte oder mehr als 10 Millionen Euro Umsatz/Jahr
- tätig in einem als „besonders kritisch“ oder „kritisch“ definierten Sektor

Besonders kritische Sektoren

- **Energie**
- **Transport**
- **Bankwesen & Finanzmärkte**
- **Gesundheit**
- **Trinkwasser & Abwasser**
- **Digitale Infrastruktur**
- **IT/IKT-Dienste im B2B-Bereich**
- **Öffentliche Verwaltung**
- **Weltraum**

Sonstige kritische Sektoren

- **Post- und Kurierdienste**
- **Abfallwirtschaft**
- **Chemikalien**
- **Lebensmittel**
- **Industrie (z. B. Maschinenbau)**
- **Digitale Dienste**
- **Forschung**

Die NIS2-Mindestanforderungen

NIS2 erweitert den Geltungsbereich von 10 auf 18 Sektoren. Betroffene Unternehmen müssen zudem auch die Sicherheit ihrer Lieferketten gewährleisten. Es werden also deutlich mehr Unternehmen in die Pflicht genommen, technische und organisatorische Maßnahmen zu ergreifen, um die Anforderungen von NIS2 zu erfüllen und somit auch ihre Gebäudesysteme entsprechend abzusichern.

Infobox 2

12 obligatorische NIS2-Massnahmen

Organisatorische Massnahmen

1. Risikomanagement (ISMS)
2. Business Continuity Management (BCM)
3. Sicherheit der Lieferketten
4. Sicherheit in der Entwicklung & Beschaffung
5. Bewertung der Effektivität
6. Schulung & Cyberhygiene

Alle hardwareseitigen Anforderungen durch Saia PCD QronoX Controller erfüllt

7. Sicherheitsvorfälle (erkennen/melden)
8. Kryptografie
9. Personal, Zugriffe & Anlagen
10. Multifaktor-Authentifizierung
11. Sichere Kommunikation
12. Sichere Notfallkommunikation

Ihre Herausforderung

Auf Sie als Gebäudebetreiber kommen nun einige Aufgaben zu. Um Ihre Gebäude in Übereinstimmung mit der NIS2-Richtlinie cybersicher zu machen, müssen Sie die Mindestanforderungen erfüllen – auch, weil mit NIS2 die Haftungsregelungen deutlich verschärft werden.

Persönliche Haftung der Geschäftsleitung – Cybersicherheit ist Chefsache

Mit der NIS-2-Richtlinie wird Cybersicherheit fest auf der Ebene der Geschäftsleitung verankert. Sie ist künftig verpflichtet

- technische und organisatorische Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit zu ergreifen,
- deren Umsetzung zu überwachen,
- sicherzustellen, dass die Erfüllung von Berichtspflichten gewährleistet ist und
- regelmäßig an Schulungen teilzunehmen

Für Gebäudebetreiber bedeutet das: Wer smarte Systeme, digitale Steuerungen oder vernetzte Infrastruktur nutzt, unterliegt mit hoher Wahrscheinlichkeit den erweiterten Pflichten. Ebenfalls wichtig:

Die Verantwortung lässt sich nicht auslagern. Auch wenn externe IT-Dienstleister eingebunden sind, bleibt die Geschäftsführung in der Pflicht – und haftet im Ernstfall persönlich für entstandene Schäden.

Geschäftsführer, die ihre Pflichten im Rahmen der NIS-2-Richtlinie verletzen, müssen mit spürbaren Konsequenzen rechnen. Neben der persönlichen und nicht delegierbaren Haftung auf Schadensersatz gegenüber dem eigenen Unternehmen – etwa bei unzureichender Überwachung von Cybersicherheitsmaßnahmen – drohen auch hohe Bußgelder. Diese können sich, angelehnt an die DSGVO, auf 7 bis zu 10 Millionen Euro oder 1,4 bis zu 2 Prozent des weltweiten Jahresumsatzes belaufen, je nachdem, welcher Betrag höher ist. Zudem soll das BSI in gravierenden Fällen künftig befugt sein, der Geschäftsleitung vorübergehend die Geschäftsführungsbefugnis zu entziehen – ein bislang beispielloser Eingriff in das Organisationsrecht.

Die wichtigsten Neuerungen auf einen Blick

Erweiterter Anwendungsbereich
Die NIS2-Richtlinie erweitert den Kreis der betroffenen Unternehmen erheblich. Neben KRITIS-Unternehmen (kritische Infrastrukturen) fallen nun auch Unternehmen aus 18 verschiedenen Sektoren unter diese Regelung. Mindestens 30.000 Unternehmen in Deutschland unterliegen damit zusätzlich den Anforderungen von NIS2.

Ihr To-Do: Prüfen Sie mit Hilfe unserer Infobox 1 (Geltungsbereich), ob Ihr Unternehmen zum Kreis der als kritisch oder besonders kritisch eingestuften Sektoren gehört.

Sicherheit der Lieferketten
Unternehmen müssen bei der Beurteilung ihres Cyberrisikos jetzt auch ihre Lieferkette berücksichtigen. Die NIS2-Richtlinie kann damit nun auch mittlere und kleinere Unternehmen betreffen, wenn sie als Zulieferer oder Dienstleister für direkt von NIS2 betroffene Unternehmen arbeiten. Sie können damit verpflichtet werden, ähnlich strenge Cybersicherheitsmassnahmen zu ergreifen, um die Sicherheit der gesamten Lieferkette zu gewährleisten.

Ihr To-Do: Prüfen Sie mit Hilfe unserer Infobox 1 (Geltungsbereich) Ihre Lieferkette auf Zugehörigkeit zum Kreis der als kritisch oder besonders kritisch eingestuften Sektoren. Prüfen Sie auch, ob Ihr Unternehmen selbst als Zulieferer oder Dienstleister betroffen ist.

Trifft einer dieser Punkte zu, müssen Sie alle Mindestanforderungen sicherstellen. Die gute Nachricht: QronoX nimmt Ihnen die Hälfte der Arbeit ab, indem er alle hardwareseitigen Anforderungen – sechs von insgesamt 12 – erfüllt (siehe Infobox 2 auf Seite 5).

Meldepflichten und -fristen bei Sicherheitsvorfällen
Sicherheitsvorfälle müssen an die zuständige Behörde gemeldet werden. In Deutschland ist dies das Bundesamt für Sicherheit in der Informationstechnik (BSI). Eine Erstmeldung muss innerhalb von 24 Stunden erfolgen, eine detailliertere Meldung binnen 72 Stunden. Das setzt entsprechende Notfallkonzepte voraus. Die verspätete, unvollständige oder unterlassene Meldung ist in der NIS-2-Umsetzung ein besonders sanktionsbewehrter Verstoss. Bußgeldadressat ist das Unternehmen, aber wie bereits erwähnt kann bei grober Pflichtverletzung die Haftung der Geschäftsleitung greifen.

So unterstützt Sie QronoX: Der QronoX-Controller protokolliert sicherheitsrelevante Ereignisse automatisiert, stellt Systemzustände transparent dar und ermöglicht durch Echtzeit-Alarmierung eine schnelle Reaktion. So können Vorfälle frühzeitig erkannt und fristgerecht gemeldet werden.

Kryptografie
Die sichere Verschlüsselung sensibler Daten – sowohl bei der Speicherung als auch bei der Übertragung – ist eine Grundanforderung der NIS-2-Richtlinie.

So unterstützt Sie QronoX: QronoX nutzt TLS-verschlüsselte Kommunikation und unterstützt sichere Protokolle wie HTTPS und WebDAV Dadurch sind Daten durchgängig kryptografisch geschützt.

Personal, Zugriffe und Anlagen
Zugriffe auf Systeme müssen kontrolliert, protokolliert und auf ein notwendiges Mass („Need-to-know-Prinzip") beschränkt werden. Auch der physische Zugang zu kritischen Anlagen ist zu schützen.

So unterstützt Sie QronoX: Der Controller ermöglicht rollenbasierte Zugriffskontrollen mit differenzierten Rechten und dokumentiert sie revisionssicher. Auch physische Schnittstellen wie Ethernet- und serielle Schnittstellen lassen sich mit Hilfe von QronoX gezielt absichern und überwachen.

Multifaktor-Authentifizierung (MFA)
Der Zugriff auf kritische Systeme muss durch mehrstufige Authentifizierungsverfahren geschützt werden.

So unterstützt Sie QronoX: QronoX unterstützt eine zweistufige Authentifizierung per Passwort und MFA. Zudem lassen sich Integrationen mit externen Authentifizierungsdiensten umsetzen.

Sichere Kommunikation
Alle Datenverbindungen – lokal wie remote – müssen gegen Manipulation und Ausspähung abgesichert sein.

So unterstützt Sie QronoX: Der QronoX-Controller nutzt durchgängig verschlüsselte Kommunikationskanäle, unterstützt IEEE 802.1X (Port Security) und schützt Schnittstellen wie BACnet/IP, Modbus TCP oder OPC UA durch Zugriffskontrolle und Zertifikate.

Sichere Notfallkommunikation
Bei einem Sicherheitsvorfall muss eine redundante, verlässliche Kommunikation mit allen relevanten Stellen sichergestellt sein.

So unterstützt Sie QronoX: QronoX erlaubt die Einbindung redundanter Kommunikationspfade, etwa über Dual-SIM-Router oder Backup-Netze. Alarmmeldungen können auch bei Ausfall der Hauptverbindung automatisiert an definierte Empfänger weitergeleitet werden.

Was Sie jetzt tun sollten

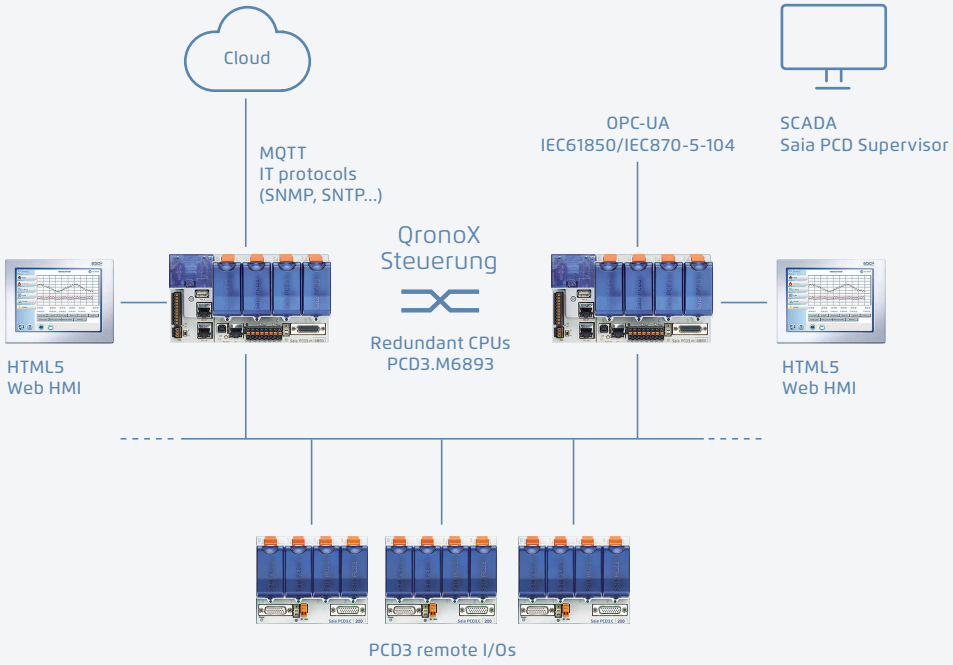
Auch wenn Sie selbst nicht direkt betroffen sind: Wie wir gesehen haben, können auch Unternehmen aus Ihrem geschäftlichen Umfeld Sie im Zuge der Sicherung ihrer Lieferketten dazu auffordern, die Vorgaben der NIS2-Richtline umzusetzen.

Handlungsempfehlung

1. Klären Sie, ob Ihr Unternehmen in irgendeiner Weise von NIS2 betroffen sein könnte
2. Beschäftigen Sie sich mit den Anforderungen der NIS2-Richtlinie
3. Lassen Sie Ihre Cyberrisiken und Sicherheitsanforderungen analysieren und Ihre Sicherheitsstufe einschätzen
4. Stellen Sie Ihre internen Cybersicherheitskonzepte für IT und OT unter Berücksichtigung der NIS2 und der IEC 62443, dem führenden Cybersicherheitsstandard im OT-Bereich, auf den Prüfstand
5. Entwickeln Sie ein individuelles und ganzheitliches Handlungskonzept für Ihr Unternehmen

Cyber-Resilienz – IT & OT mit SBC schützen

Bei der Auseinandersetzung mit der Normenreihe IEC 62443 wird deutlich, dass Cybersicherheit bereits auf Steuerungsebene beginnt. Hier können cybersichere SPS-Systeme, die mit der neuesten Generation kryptographisch gesicherter PCD-Steuerungen wie dem Saia PCD QronoX Controller von Saia Burgess Controls ausgestattet sind, gute Dienste leisten, um aktuellen Standards zu entsprechen und Cyberangriffe bereits auf Steuerungsebene abzuwehren.



Ideal geeignet für Automation kritischer Infrastruktur

Erfahren Sie mehr über Saia PCD QronoX

https://sbc.do/qronox_ger

Unsere Lösung für Ihre NIS2-Compliance

Höchste Cybersicherheit

Der universell einsetzbare Saia PCD QronoX Controller ist software- und hardwareseitig nach neusten IEC 62443-Standards abgesichert und bietet somit ein hohes Mass an Cybersicherheit (Security Level 3).

Kompatibilität & Programmierbarkeit

Der Saia PCD QronoX Controller bietet eine flexible, objektorientierte Hochsprachenprogrammierung nach IEC 61131-3.

Sichere Kommunikation & Datenverschlüsselung

Sein Betriebssystem, das alle Anwendungs- und Kommunikations-programme umfasst, ist signiert und verschlüsselt und verhindert so einen unautorisierten Zugriff auf das Prozesssteuerungssystem.

Perfekt für anspruchsvolle & kritische Anwendungen

Der QronoX Controller verfügt über zwei getrennte Netzwerkschnitt-stellen und stellt so die im Rahmen von NIS2 geforderte Netzwerk-segmentierung zur strikten Isolation kritischer Systeme sicher.
Er ist redundant und hochverfügbar und gewährleistet so einen sicheren, unterbrechungsfreien Betrieb.

Saia PCD QronoX Controller

Der zukunftsfähige Saia PCD QronoX Controller sorgt bereits auf Steuerungsebene für maximale Cybersicherheit, wie sie etwa in NIS2 für Unternehmen gefordert wird. Das ist gerade bei kritischen Infrastrukturen wichtig und sorgt für höchste Betriebs- und Rechtssicherheit.

Saia-Burgess Controls AG
Route Jo-Siffert 4
1762 Givisiez
Schweiz

T +41 26 580 30 00
info.ch@saia-pcd.com
www.sbc-support.com
www.saia-pcd.com

SBC Deutschland GmbH
Strahlenbergerstraße 110–112
63067 Offenbach am Main
Deutschland

T +49 69 80 640 40
info.de@saia-pcd.com
support.de@saia-pcd.com
www.saia-pcd.de

Saia Burgess Controls Österreich
Handelskai 388
1023 Wien
Österreich

info.at@saia-pcd.com
support.at@saia-pcd.com
www.saia-pcd.at

Swiss Design

GER01 | 06.2025