Whitepaper

IEC 62443 als Erfolgsfaktor für ganzheitliche Security-Konzepte

Schutz vor Cyber-Attacken und Erfüllung der neuen gesetzlichen Anforderungen

Erfahren Sie mehr über:

- → Die Umsetzung von Cyber Security in der Automatisierung
- → Die neuen gesetzlichen Richtlinien NIS 2, CRA und die neue Maschinenverordnung
- → Das 360°-Security-Konzept

PHOENIX CONTACT

Einleitung

Können nach IEC 62443 zertifizierte Komponenten und Systeme umfassend vor Cyber-Angriffen schützen und gleichzeitig gesetzliche Anforderungen der EU, wie die NIS 2, der Cyber Resilience Act (CRA) und die neue Maschinenverordnung, erfüllen?

Die Digitalisierung und Vernetzung von Produktions-, Produkt- und Kundendaten ist der entscheidende Faktor zur Steigerung der Wertschöpfung von Unternehmen und damit auch eine Basis der wirtschaftlichen Entwicklung von globalen Regionen. Dies hat die EU-Kommission erkannt und bereits im Dezember 2020 die EU-Cyber-Security-Strategie veröffentlicht. Sie definiert die Anforderungen zur Resilienz und Angriffsabwehr an Hersteller von Komponenten und Systemen als auch für alle wesentlichen fertigenden Unternehmen.

Die internationale Normenreihe IEC 62443 beschreibt grundlegende Anforderungen zur Vermeidung von Sicherheitsrisiken für Komponentenhersteller, Systemintegratoren und Betreiber. Sie ist die führende Norm für die Umsetzung von Security-by-Design in Produkten und Systemen.

„Die IEC 62243 ist ein Erfolgsfaktor zur Erfüllung aktueller Cyber-Security-Richtlinien.“

Boris Waldeck, Master Specialist Security PLCnext Technology

Inhalt

1 Wertschöpfung als Ziel

Zunehmende Digitalisierung und Vernetzung erhöhen die Angriffsflächen für Cyber-Attacken. Zusätzlich werden die Angreifenden und die Angriffsmethoden immer professioneller. Ziel der Cyber Security ist es, die Wertschöpfung und individuelle Sicherheitsziele eines Unternehmens abzusichern. Hierzu zählen u. a. der Schutz von Know-how – z. B. Entwicklungsergebnisse oder Vertragskonditionen – und die Einhaltung gesetzlicher Vorschriften, z. B. des Datenschutzes.

In fertigenden Unternehmen ist die Produktions- und Lieferfähigkeit von offensichtlicher Wichtigkeit. Über diese konkreten Angriffsschäden hinaus gibt es weitere, die oft im Vorfeld unterschätzt werden.

So führen Cyber-Angriffe häufig auch zu Imageschäden, da sie das Vertrauen der Kunden, Partner, Investoren und der Öffentlichkeit in das betroffene Unternehmen beeinträchtigen können. Für kritische Infrastrukturen sind gesetzliche Vorgaben zur Umsetzung der Cyber Security schon längst etabliert, diese werden jetzt von der EU durch die NIS 2.0-Richtlinie auf viele weitere Unternehmen ausgedehnt.

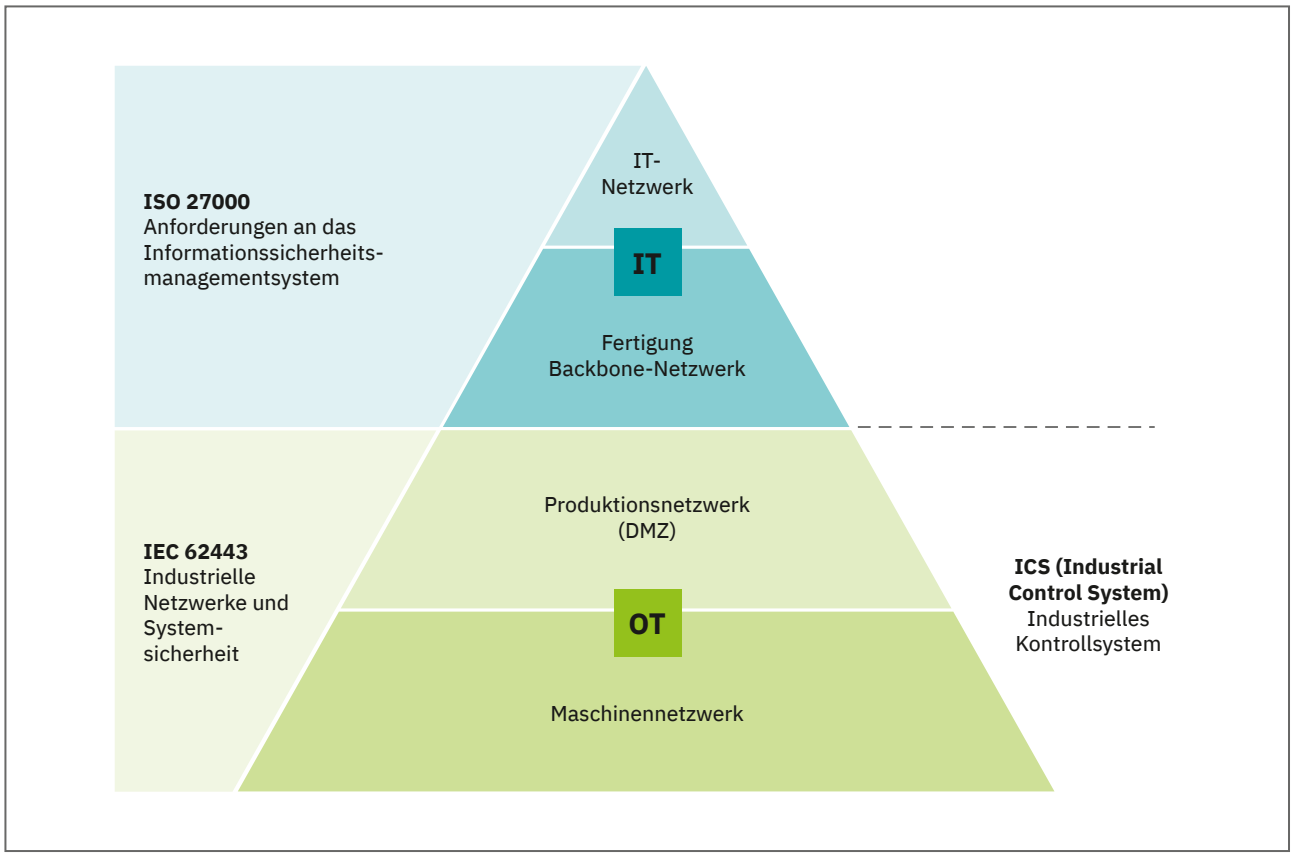
Sicherstellung der Wertschöpfung ist das oberste Ziel von Cyber Security.

2 Umsetzung in der Automatisierung

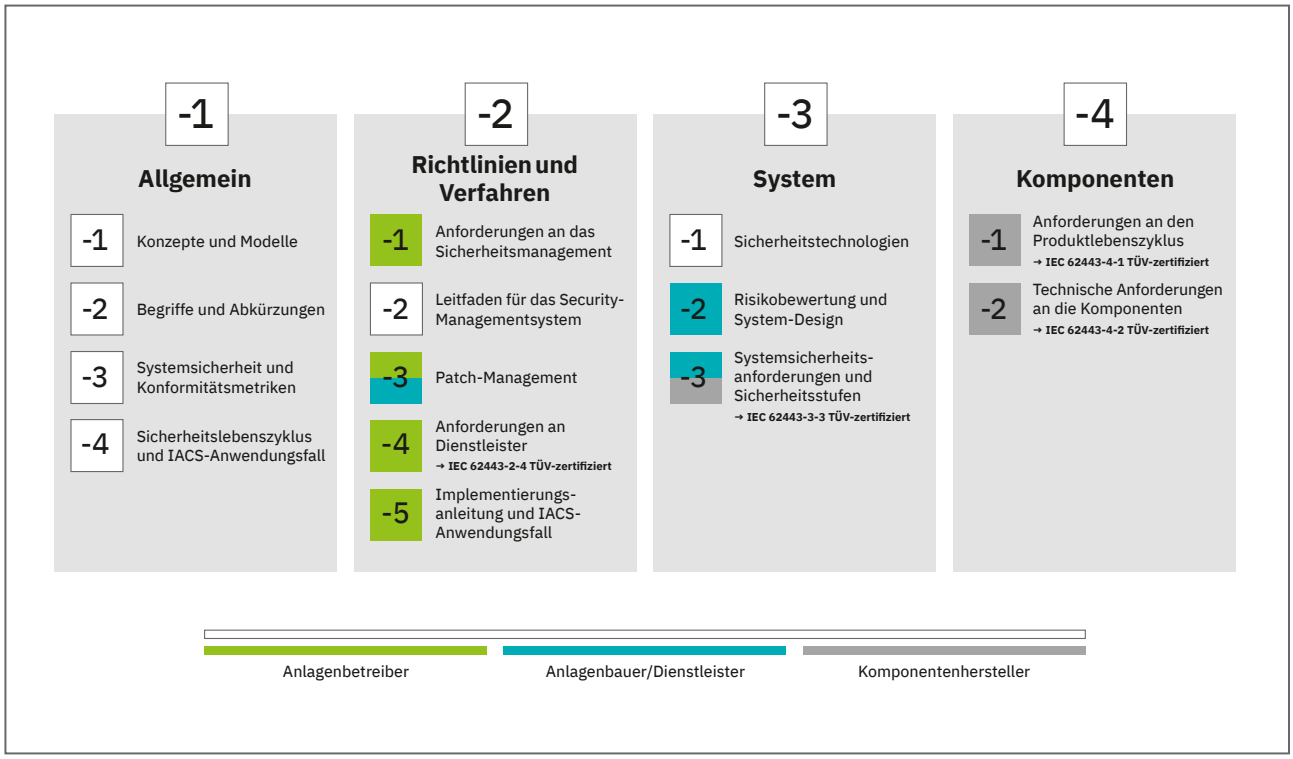
Die Sicherheit eines Unternehmens befindet sich in zwei Welten: IT (Information Technology) und OT (Operational Technologie). Zum Schutz beider Welten wird deshalb ein Informationssicherheits-Managementsystem (ISMS) nach ISO 27001/2 in der IT eingeführt, das in Richtung der OT erweitert wird. Die Anforderungen eines ISMS enthalten sowohl technische als auch organisatorische Anforderungen. Die technischen Anforderungen lassen sich mit Hilfe der IEC 62443-2-1 auf Maßnahmen in der OT, der IACS-Umgebung (Industrial Automation Control System) referenzieren. Die IEC 62443 ergänzt somit die Norm ISO 27001. Gemeinsam bieten die beiden Normen einen ganzheitlichen Ansatz zum Schutz vor Cyber-Bedrohungen.

Maßnahmen, die die Normenreihe IEC 62443 beschreibt, sind u. a.:

- Konfiguration und Segmentierung der Netzwerke
- Schutz der Daten bei der Speicherung und Übertragung
- Authentifizierung von Benutzerinnen und Benutzern
- Überwachung und Protokollierung der Aktionen von Benutzenden und Systemen
- Security-Härtung der eingesetzten Geräte
- Konfiguration, Updates, Backup und Restore
- Organisatorische Anforderungen an das Handling des Systems



Cyber Security in der IT und OT



Aufbau der IEC 62443

Die konkreten Maßnahmen der IEC 62443 werden für unterschiedliche Sichtweisen adressiert:

Komponenten

4-1 Sicherer Prozess zur Entwicklung und dem Lebenszyklus von Komponenten (Produkten)

4-2 Security-Anforderungen für Komponenten

System

3-3 Security-Anforderungen für Systeme

Betreiber

2-1 Security-Managementsystem

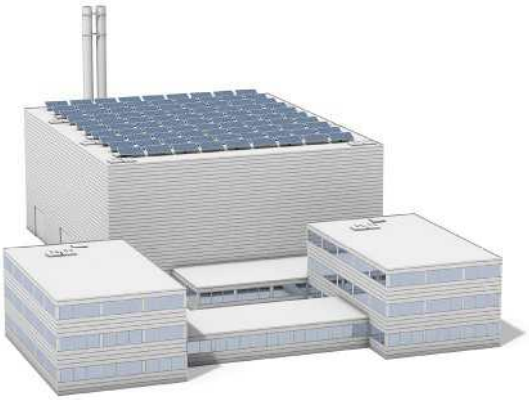
2-3 Patch-Management

2-4 Security-Anforderungen an Systemintegratoren (Dienstleister)

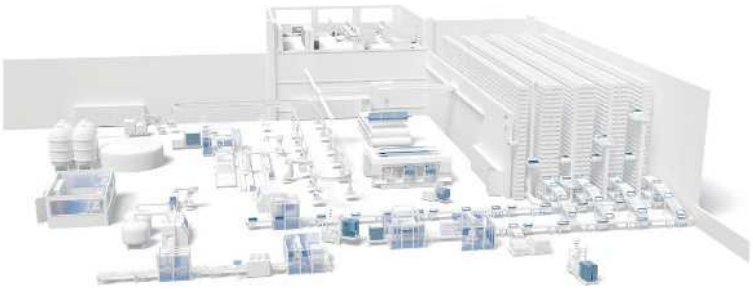
Das besondere Element der IEC 62443 ist der ganzheitliche Security-by-Design-Ansatz, der von Anforderungen an die Betriebsprozesse über Anforderungen an die Systeme bis hin zu den Produkten reicht und sowohl prozessuale als auch technische Maßnahmen und Anforderungen darlegt.

Ein entscheidendes Security-Konzept der IEC 62443 ist „Defense in Depth“, durch die Staffelung mehrerer Sicherheitsmechanismen hintereinander wird es den Angreifenden schwerer gemacht. So muss z. B. bei einem Angriff über das Netzwerk erst eine oder mehrere Firewalls überwunden werden, bevor die Angreifenden an die Zielkomponente herankommen. Dort muss dann eine Benutzeranmeldung bezwungen werden, um dann noch durch interne Sicherheitsmechanismen aufgehalten zu werden.

Defense in Depth



Unternehmensebene:
- Physische Maßnahmen
- Berechtigungskonzept (Zutritt, Zugang, Zugriff)
- Awareness-Schulungen
- ISMS-Prozesse



Netzwerkebene:
- Netzsegmentierung (Zonen, Conduits)
- VPN
- Verschlüsselung
- Firewalls
- Angriffserkennung

Produktebene:
- Security Features
- Systemhärtung
- „Security by Design“-Komponenten

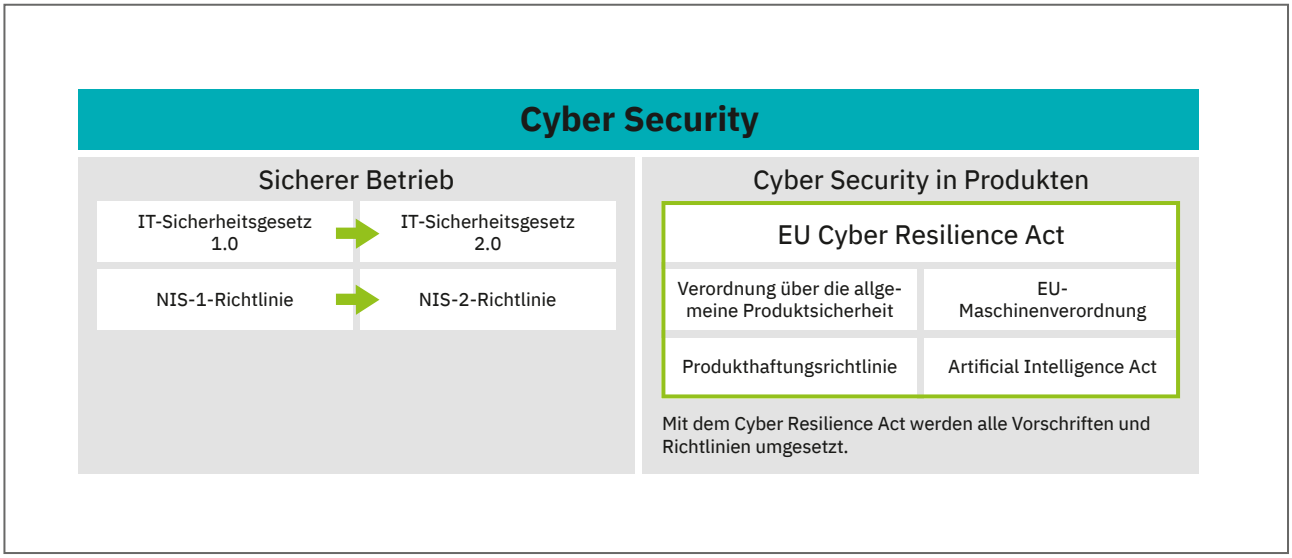
3 Gesetzliche Richtlinien

Cyber-Security-Maßnahmen waren bisher nur für die kritischen Infrastrukturen gesetzlich vorgeschrieben und wurden zusätzlich bei großen, meist international tätigen Anlagenbetreibern umgesetzt. Mit der neuen NIS-2-Richtlinie der EU ändert sich dies jetzt deutlich.

NIS-2-Richtlinie

Um ihre Systeme gegen Cyber-Attacken abzusichern, verpflichtet die europäische NIS-2-Richtlinie (Netz- und Informationssicherheit) Betreiber öffentlicher oder privater Einrichtungen passende Sicherheitsinstrumente einzuführen. Sie weitet im Vergleich zur bestehenden NIS 1 ihre Vorschriften auf mittelgroße Unternehmen mit mehr als 50 Mitarbeitenden und über zehn Millionen Euro Umsatz aus. Sie gilt für wesentliche und wichtige Einrichtungen in der EU.
Unter den Begriff „wesentliche Einrichtungen“ fallen Unternehmen, die in kritischen Infrastrukturen tätig sind, z. B. den Bereichen Strom-/Gaserzeugung, -speicherung und -übertragung, Transport auf dem Wasser sowie der Straße und Schiene, Trinkwasser- und Abwasseranlagen als auch der digitalen Infrastruktur. Wichtige Einrichtungen werden aus einer Liste von sieben Sektoren gewählt, auf der Grundlage ihrer Kritikalität für ihren Geschäftsbereich und die Art der Dienstleistung. Als Beispiel sind die Herstellung und der Vertrieb von Lebensmitteln und Chemikalien sowie die Produktion von elektrischen Geräten, Maschinen und Fahrzeugen genannt.

Die NIS-2-Richtlinie trat am 16. Januar 2023 in Kraft und muss bis zum 18. Oktober 2024 durch die EU-Staaten in nationales Recht umgesetzt werden.
Diese Anforderungen lassen sich jedoch nur schwer erfüllen, wenn die eingesetzten Produkte nicht nach Security-by-Design entwickelt worden sind. Um diese Herausforderung zu lösen, wurde durch die EU der Cyber Resilience Act (CRA) definiert.



Überblick über die neuen gesetzlichen Richtlinien

Cyber Resilience Act (CRA)

Der CRA nimmt die Hersteller in die Pflicht Security-by-Design-Produkte zu entwickeln. Produkte, die unter den CRA fallen, bekommen in Zukunft kein CE-Kennzeichen mehr, wenn sie nicht den gesetzlichen Regelungen entsprechen. Es werden Security-Mindestanforderungen für die Umsetzung der Security-Maßnahmen definiert. Je nach Produktklasse müssen sie durch eine Produktkonformitätsprüfung durch benannte Stellen z. B. TÜV oder durch den Einsatz einer harmonisierten Norm beim Hersteller selbst nachgewiesen werden.

Die essenziellen Anforderungen des CRA müssen bei der Konzeption, Entwicklung und Herstellung berücksichtigt werden, also auf einem sicheren Entwicklungsprozess basieren. Gefordert wird u. a. ein Zugriffsschutz, den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit sowie einen sicheren Auslieferungszustand.
Ein zusätzlicher Bestandteil ist das Schwachstellenmanagement und Regelungen für die Dauer, in der die Hersteller Security-Updates für ihre Produkte zur Verfügung stellen müssen. Der Textentwurf des CRA ist im September 2022 veröffentlicht worden. Die dazugehörigen Trilog-Abstimmungen sind abgeschlossen.
Als EU-ACT muss er nicht in nationales Recht umgesetzt werden, sondern ist nach der Veröffentlichung im Access the Official Journal gültig. Die Umsetzung der CRA ist voraussichtlich bis 2027 verpflichtend.

Die IEC 62443 deckt sowohl den geforderten sicheren Entwicklungsprozess als auch die technischen Anforderungen an einzelne Produkte und Systeme ab. Daraus folgt, das die IEC 62443 oder eine abgeleitete Sektornorm ein aussichtsreicher Kandidat für eine harmonisierte Norm des CRA ist.
Um die Anforderungen an das Schwachstellenmanagement zu erfüllen, ist es wichtig, dass für alle Produkte ein standardisierter Software Bill of Material (SBOM), eine Liste, die alle Software-Komponenten eines Produkts beschreibt, zur Verfügung steht. Zusätzlich müssen bekannte Schwachstellen in einem standardisierten digitalen Format wie Common Security Advisory Framework (CSAF) zur Verfügung stehen. Nur so wird die Einhaltung der Fristen für die Berichterstattung und der Behebung von Schwachstellen gewährleistet.

EU-Maschinenverordnung (MVO)

Um Menschen und Umwelt vor negativen Folgen z. B. vor Verletzung oder Verunreinigung zu schützen, müssen Maschinen mit funktionaler Sicherheitstechnik mit der Maschinenrichtlinie 2006/42/EG konform sein. Dieser Standard bedarf eines Updates, da Risiken neuer Technologien und neue Regelungen zur Produktsicherheit berücksichtigt werden müssen. Zusätzlich hat sich gezeigt, dass durch die Richtline (Umsetzung in nationales Recht) teilweise unterschiedliche Regelungen gefordert werden. Auch das Thema funktionale Sicherheit in Kombination mit Cyber Security muss zukünftig berücksichtigt werden. Aus diesen Anforderungen entstand die Maschinenverordnung 2023.

Die MVO ist eine Ergänzung zum CRA, der auch Maschinen als Produkt sieht. Für Maschinen mit funktionaler Sicherheit ist jedoch die MVO die führende Sicht.

4 Umsetzung von Cyber Security bei Phoenix Contact

Bei Phoenix Contact wurde mit der Umsetzung der IEC 62443 im Jahr 2017 begonnen. Es wurde das „360°-Security-Konzept“ etabliert, dass den Leitsatz „Security ist im gesamten Lebenszyklus unserer Produkte und Lösungen verankert“ umsetzt.

Sicherer Entwicklungsprozess

Die für Entwicklung und den gesamten Lebenszyklus der Produkte ist der sichere Entwicklungsprozess nach IEC 62443-4-1 die Voraussetzung. Er definiert die Entwicklung nach den gängigen Cyber-Security-Verfahren Security-by-Design, Defense-in-Depth, stellt aber auch die Überwachung von Schwachstellen sicher und sorgt für regelmäßige Security-Updates.

Sichere Produkte

Sichere Produkte sind nach dem 4-1-Entwicklungsprozess entwickelt und erfüllen die funktionalen Security-Anforderungen der 4-2. Dies sind z. B. Schutz vor DDoS-Angriffen (Distributed Denial of Service), User-Management, Vertraulichkeit der Daten bei der Übertragung oder Speicherung. Als erste Steuerung im Markt ist 2021 PLCnext Control nach IEC 62443-4-1 ML3 /4-2 SL2 Feature Set zertifiziert. Weitere sichere Produkte befinden sich zurzeit in der Entwicklung oder werden zertifiziert.

Weitere Informationen zu den Produkten →

Phoenix Contact hat IEC-62443-konforme Cyber Security umgesetzt

PLCnext Control: IEC 62443 zertifizierte Safety und Security

Als Teil des 360°-Security-Konzepts wurde PLCnext Control als erste Steuerung im Markt nach IEC 62443-4-1 ML3 /4-2 SL2 Feature Set durch den TÜV SÜD zertifiziert. Diese Zertifizierung wird fortlaufend für weitere PLCnext Steuerungen ergänzt. Zum Beispiel wurde diese Zertifizierung 2022 um die funktional sicheren Steuerungen der PLCnext Control-Familie erweitert.

Die IEC 62443-Zertifizierung der PLCnext Control enthält u. a. umfangreiche Security-Funktionen:

- Security-Profil als Konfiguration der geringsten Funktionalität
- Firewall und Netzwerksegmentierung sowie die Überwachung und Limitierung der Netzlast
- TLS-Security für eine zugriffssichere Kommunikation
- Zertifikatsverwaltung zur asymmetrischen Kryptografie und Schlüsselverwaltung
- Benutzerverwaltung, rollenbasiert lokal und Anbindung an zentrale Benutzermanagementsysteme
- Event-Logging-Systeme mit lokaler und zentraler Ankopplung
- PSIRT überwacht automatisch bekannte Schwachstellen der verwendeten Software-Komponenten und veröffentlicht Security Advisories
- Device and Updatemanagement App als zentrale Verwaltung der Geräte für Security-Updates (Firmware und Applikation) als auch dem Management des Backups und Restore
- SBOM im standardisierten Format und digitale Security Advisories nach Common Security Advisory Framework (CSAF) sind in Vorbereitung

Der zertifizierte Funktionsumfang wird im PLCnext Security Info Center dokumentiert.

→ **Mehr erfahren:**
phoenixcontact.com/security-infocenter

mGuard-Security-Router: Leistungsstarker Schutz für industrielle Netzwerke

Die mGuard-Security-Router schützen industrielle Netzwerker dank umfangreichen Security-Funktionen vor unautorisierten Zugriffen oder Schad-Software. Die bewährte mGuard-Security-Technologie ermöglicht die Kontrolle und Absicherung der Kommunikation innerhalb des Maschinen- oder Produktionsnetzwerk. Die Produkte sind Teil unseres vollständigen 360°-Security-Konzepts.

Die industriellen Router wurden nach dem zertifizierten Entwicklungsprozess nach IEC 62443-4-1 ML3 entwickelt und verfügen über die umfangreichen Security-Funktionen:

- Intelligente Firewall mit unterschiedlichem Funktionsumfang je nach Anwendung:
  - Bedingte Firewall
  - DNS-namensbasierte Firewall
  - Benutzer-Firewall
  - Firewall-Redundanz
  - Router mit NAT und 1:1 NAT
- IPsec VPN-Funktionalität:
  - Zertifikatsbasiert
  - Umschaltbar über I/Os
- Lokale und zentralisierte (RADIUS) Benutzerverwaltungskonfiguration
- Lokale und zentralisierte Sicherheitsprotokollierung
- NTP: Netzwerkweite Zeitsynchronisation
- Geräte- und Update-Management mit dem mGuard Device Manager
- Systembenutzungsbenachrichtigung

Die Cyber Security der PLCnext Control kann systemisch durch die bekannte mGuard-Technologie gut ergänzt werden. Je nach Anwendungsfall und Risikoanalyse der Anlage können zusätzliche Geräte zur Segmentierung, als weitere Firewall oder als Absicherung von Zugriffen durch VPN (z. B. Fernwartung oder Cloud-Zugriffen) eingesetzt werden. Ein Zusammenspiel beider Lösungen ist zur ganzheitlichen Absicherung von Anlagen- oder Maschinennetzwerke sinnvoll.

Weitere Informationen zu den mGuard-Security-Routern

→ **Mehr erfahren:**
phoenixcontact.com/mguard

Sichere Dienstleistungen

Um zusammen mit Systemintegratoren und Betreibern Security-Lösungen zu diskutieren, beraten, installieren und zu warten, müssen die Teams die entsprechenden Cyber Security-Fähigkeiten besitzen und nachweisen. Die entsprechenden Teams, auch in ausgewählten Ländergesellschaften von Phoenix Contact, sind nach IEC 62443-2-4 zertifiziert.

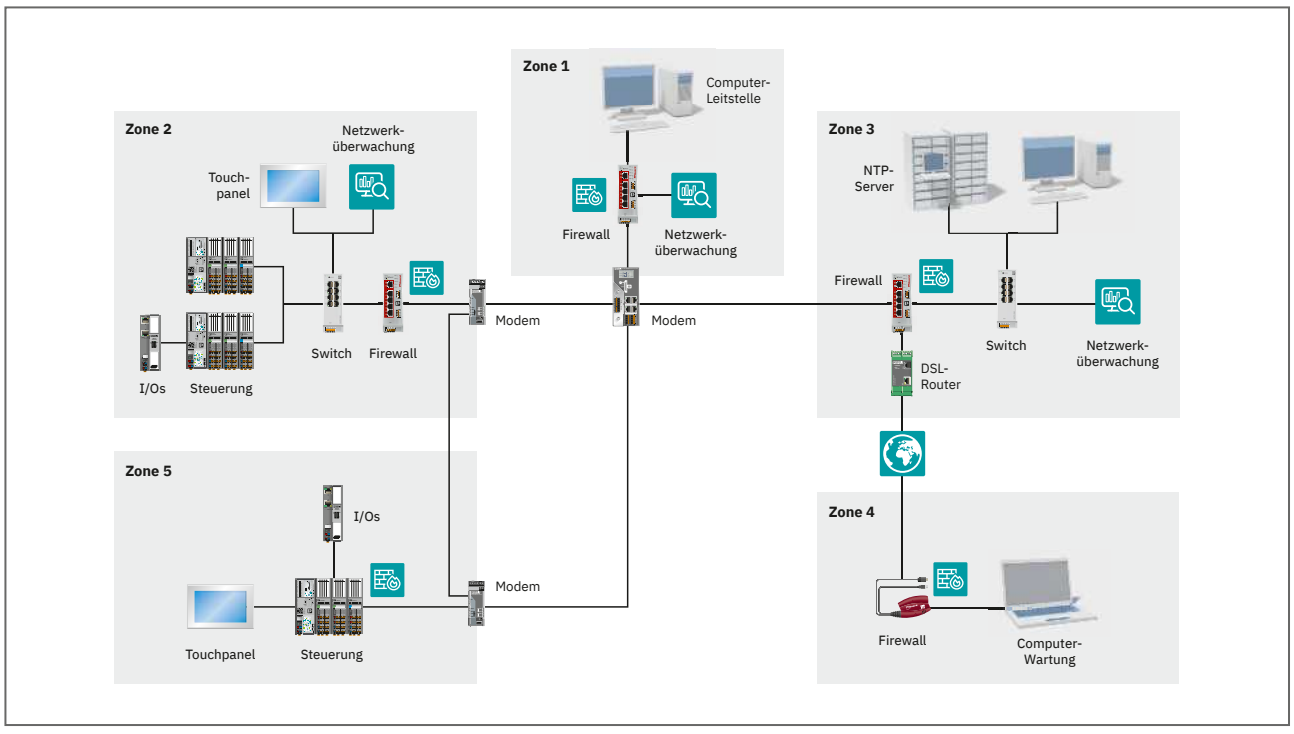
Sichere Lösungen

Für unterschiedliche Lösungen und Märkte sind Templates (Blueprints) entwickelt und wenn sinnvoll nach IEC 62443-3-3 zertifiziert worden. Sie erleichtern die Diskussion und die Konzeptarbeit einerseits und weisen andererseits das Know-how von Phoenix Contact nach, Lösungen mit Kunden zu zertifizieren.

PSIRT

Das Produkt Security Incidence Response-Team (PSIRT) ist das zentrale Team dessen Aufgabe es ist, auf potenzielle Sicherheitslücken, Vorfälle und andere Sicherheitsprobleme im Zusammenhang mit Produkten, Lösungen sowie Diensten von Phoenix Contact zu reagieren. Das PSIRT leitet die Offenlegung, Untersuchung und interne Koordination und veröffentlicht Sicherheitshinweise zu bestätigten Sicherheitslücken.

Die oben genannten Zertifizierungen werden alle durch jährliche Audits vom TÜV SÜD überwacht.

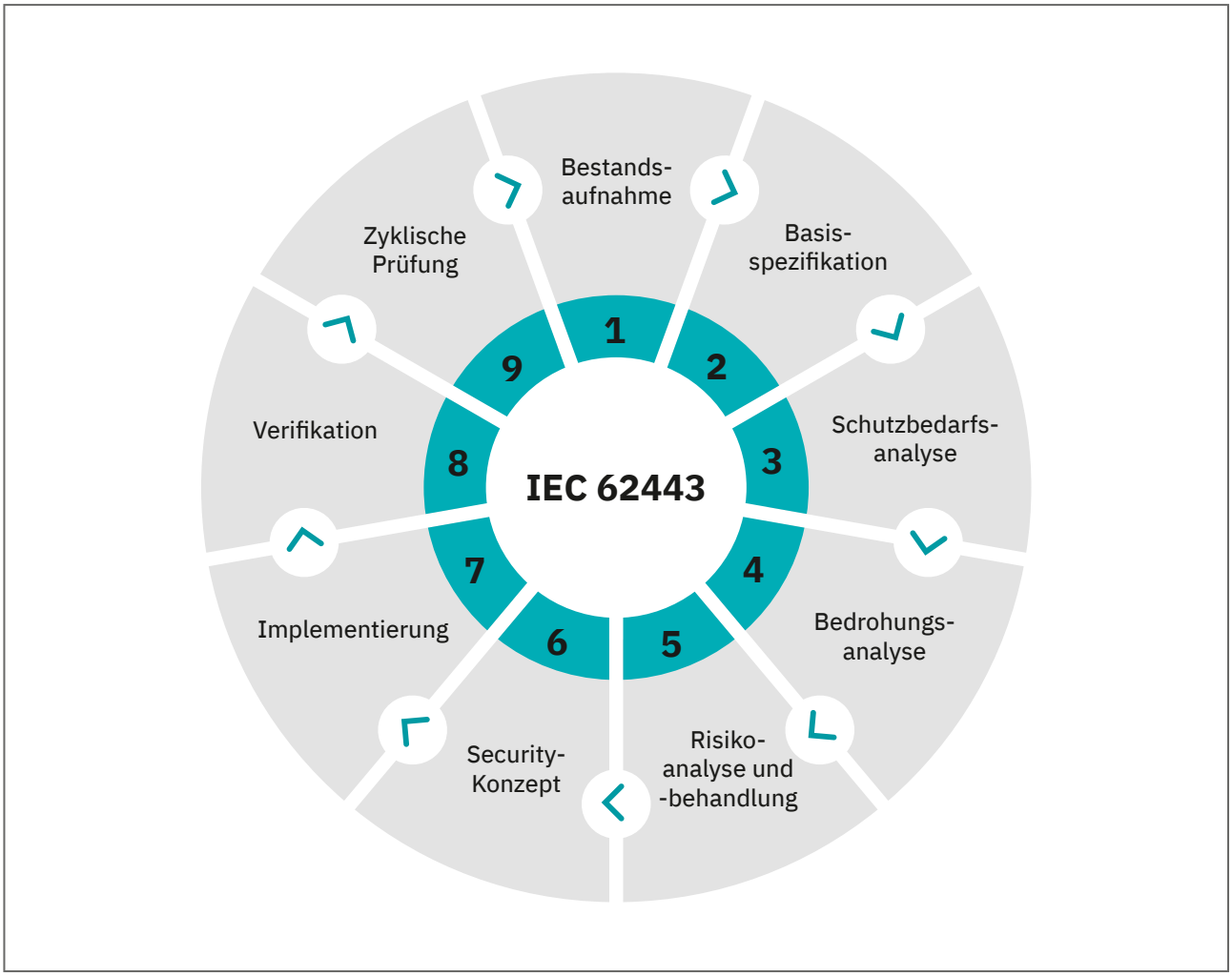


Unser vom TÜV SÜD gemäß IEC 62443-3-3 zertifizierter Blueprint „Remote-Monitoring and -Control“

5 Fazit: Phoenix Contact als Partner für Cyber Security

Die NIS 2, der CRA und die MVO befinden sich im Gesetzgebungsverfahren der EU oder in der Umsetzung in nationales Recht. Wendet man die typischen Übergangsfristen an, werden alle voraussichtlich im Jahr 2027 vollumfänglich geltendes Recht sein. Berücksichtigt man die Komplexität der Cyber-Security-Normen und der Gesetze wird schnell deutlich, dass sowohl bei den Herstellern von Produkten, Systemintegratoren als auch bei den Betreibern dringender Handlungsbedarf besteht.

Phoenix Contact ist durch die langjährige Erfahrung des 360°-Security-Konzept gut aufgestellt und bietet über die Produkte und Systeme hinaus auch Betreibern und System-integratoren beim Design und Betrieb von Anlagen Dienstleistung nach IEC 62443 an. Das 360°-Security-Konzept beginnt mit der Vorgehensweise „Neun Steps zur sicheren Anlage“ die Systemintegratoren und Be-treibern ermöglicht Security-by-Design für ihre spezifische Lösung zu erfüllen.



360°-Industrial-Security: Neun Schritte zur sicheren Anlage

Security-by-Design-Automatisierungslösungen nach IEC 62443 müssen einem strikten Vorgehensmodell folgen. Sie sind im Folgenden in den „Neun Schritten zur sicheren Anlage“ definiert:

1 Bestandsaufnahme:
Erfassung der Anlageninformationen zur Identifikation der Einsatzumgebung

2 Security-Basisspezifikation:
Planung von Basismaßnahmen zur Grundabsicherung der Anlage

3 Schutzbedarfsanalyse:
Ermittlung des Schutzbedarfs zur Absicherung schützenswerter Assets

4 Bedrohungsanalyse:
Identifizierung relevanter Bedrohungen für die Automatisierungslösung

5 Risikoanalyse/-behandlung:
Erstellung einer Risikoeinschätzung inkl. Ableitung eines Maßnahmenkatalogs

6 Security-Konzept:
Finalisierung eines individuellen und umfassenden Security-Konzepts

7 Implementierung:
Umsetzung des Security-Konzepts – von der Theorie in die Praxis

8 Verifikation:
Prüfung der Implementierung gemäß der definierten Security-Konzeptvorgaben aus Schritt 6

9 Zyklische Prüfung:
Stay up-to-date – vom Security-Konzept bis zum Know-how

Kontakt

Sind Sie auf die neuen gesetzlichen Richtlinien vorbereitet?

Wir helfen Ihnen, die neuen Anforderungen der gesetzlichen Richtlinie für Ihr Unternehmen umzusetzen und sich selbst vor Cyber-Angriffen zu schützen.
Gemeinsam setzen wir ein 360°-Security-Konzept für Sie um!

Mehr Informationen unter:
phoenixcontact.com/cybersecurity

Boris Waldeck
Master Specialist Security
PLCnext Technology
bwaldeck@phoenixcontact.com

Andreas Fuß
Product Marketing
Network Security
afuss@phoenixcontact.com

3011401267