Leitfaden

Industrial Security richtig umsetzen

Schützen Sie IT- und OT-Bereich ganzheitlich im Zusammenspiel

Erfahren Sie mehr über:

- Management Summary: Kritische Bedrohungslage, EU-Gesetzgebung, neues Zusammenspiel IT/OT, Standards
- Direkt für Ihre Praxis: Etablierte Vorgehensweisen und Konzepte gemäß des internationalen Security-Standards IEC 62443

PHOENIX CONTACT

Einleitung

Wussten Sie, dass es heutzutage gar nicht schwer ist, sich in Systeme, Anlagen und Maschinen zu hacken? Industrieunternehmen sind häufig nicht ausreichend vorbereitet, wodurch Automatisierungssysteme eine offene Tür ins Unternehmen bieten. Sei es, weil Mitarbeitende nicht sensibilisiert und geschult sind oder weil IT und OT weder ein einheitliches Verständnis zum Thema Industrial Security haben noch integriert zusammenspielen.

Traumverhältnisse für Cyber-Kriminalität mit fatalen Folgen wie Anlagenstillstand, externem Zugriff auf sensible Daten oder Eingriff in Unternehmensprozesse (oftmals vorerst unbemerkt). Die Vorfälle nehmen exorbitant zu, man kann es aus der allgemeinen Presse entnehmen. Cyber-Kriminalität ist weltweit Risiko Nr. 1 für Unternehmen[1)].

Um der kritischen Bedrohungslage entgegenzuwirken, verschärft sich die EU-Gesetzgebung. Z. B. durch den gerade verabschiedeten Cyber Resilience Act, der 2024 formal in Kraft tritt, durch die neue Richtlinie NIS 2.0 oder durch Regularien der neuen EU-Maschinenverordnung (umzusetzen ab 14. Januar 2027).

Jetzt müssen sich auch Verantwortliche von Automatisierungssystemen dem Thema der Cyber-Kriminalität im Zusammenspiel mit der IT stellen. Sei es zur Sicherung von Produktionsanlagen, Infrastrukturen, erneuerbaren Energiesystemen oder Gebäuden. Zur Umsetzung gibt es international etablierte Cyber-Security-Standards.

[1)] Quelle: Allianz Risikobarometer 2023

Verschaffen Sie sich mit Hilfe des Leitfadens 360°-Industrial-Security einen schnellen und fundierten Überblick zu zentralen Aspekten, um Ihre Anlage ganzheitlich im Zusammenspiel von IT und OT zu schützen.
Die Inhalte sind von unseren Expertinnen und Experten speziell für Betreiber und Hersteller von Maschinen aufbereitet. Sei es für das Top-Management als auch für Verantwortliche der Umsetzung.

Inhalt

Management Summary

360°-Industrial-Security – essenzielles Wissen, um Ihre Anlage zu schützen

Bedrohungslage

Die Frage ist nicht ob, sondern wann Ihr Unternehmen angegriffen wird

Cyber-Attacken sind in der Realität angekommen

- **Unternehmensrisiko Nr. 1: Cyber-Vorfälle**
  Cyber-Vorfälle, wie IT-Ausfälle, Ransomware-Angriffe oder Datenschutzverletzungen, werden – global betrachtet – im zweiten Jahr in Folge als wichtigstes Risiko eingestuft.[1)]
- **68 % der Industrieunternehmen sind Opfer**
  68 % der Industrieunternehmen in Deutschland sind bereits Opfer von Cyber-Angriffen geworden.[2)]
- **59 % Produktionsausfälle**
  59 % dieser Angriffe führen zu Produktionsausfällen.[2)]

Quelle: [1)] Allianz Risikobarometer 2023, [2)] VDMA

Zentrale Risiken durch Hackerangriffe, die ein ganzes Unternehmen zum Stillstand bringen können

- Externer Zugriff auf sensible Daten sowie deren Veränderung wie geheime Konstruktionspläne, Kundendaten – „die essenziellen Kronjuwelen eines Unternehmens“
- Externer Eingriff in Unternehmensprozesse (oft vorerst unbemerkt), schlimmstenfalls droht ein wochen- oder gar monatelanger Stillstand – auch in der Produktion oder in der Logistik
- Imageverlust und Erpressung durch Ransomware

„Die Office-IT ist in der Regel gut aufgestellt, während in der OT noch viele Gefahren schlummern. Ganzheitliche Cyber Security erfordert auch im OT-Bereich die Risiken frühzeitig zu erkennen, zu bewerten und abzuwenden.“

Torsten Gast, Director Competence Center Services,
Phoenix Contact Deutschland GmbH

Top-3-Fehleinschätzungen

1. „Unsere IT kümmert sich schon darum. Wir im OT-Bereich tragen keine Verantwortung für die Sicherheit von Informationen. Unser Hauptfokus liegt darauf, dass die Anlagen inklusive Betriebstechnik laufen und das effizient.“
2. „Automatisierungstechnik, das ist ein eigener Bereich. Das läuft schon irgendwie. Da sind wir von der IT nicht für verantwortlich. Da kennen wir uns auch nicht aus. Das macht unsere Instandhaltung.“
3. „Wir setzen Firewalls ein. Damit sind wir umfassend geschützt.“

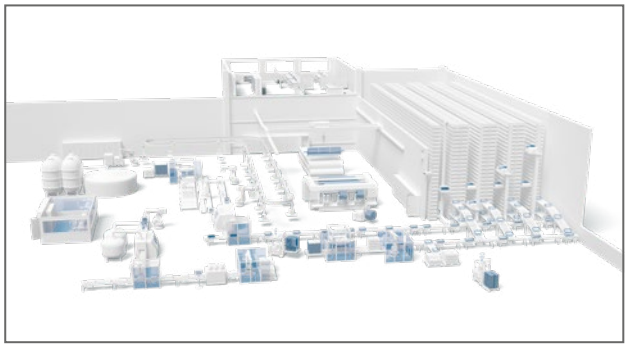
Top-3-Bedrohungen

1. Einschleusen von Schad-Software über Wechseldatenträger und mobile Systeme
2. Infektion mit Schad-Software über Internet und Intranet
3. Menschliches Fehlverhalten und Sabotage

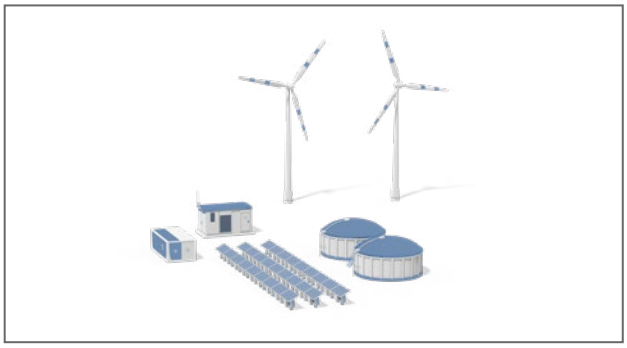
Quelle: BSI, 2022

Gesamte Liste der Top-10-Bedrohungen (BSI) einsehen

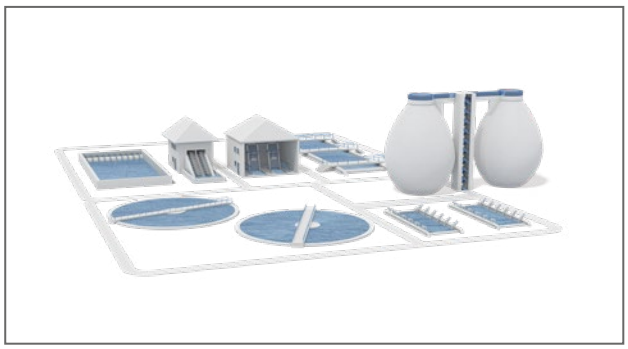
Mögliche Anwendungsbereiche von Automatisierungssystemen – schützen Sie IT- und OT-Bereich



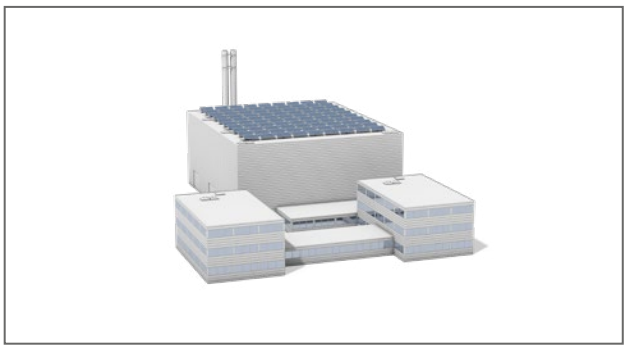
Produktionsanlagen



Erneuerbare Energien



Infrastruktur



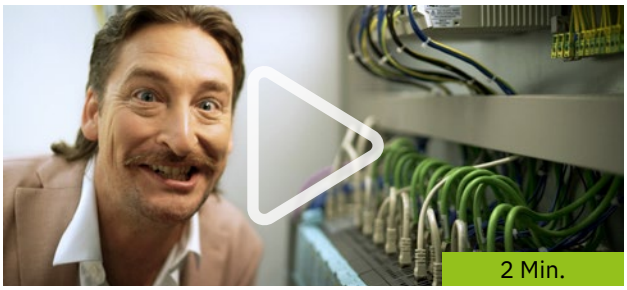
Gebäudeautomation

Cyber-Kriminalität betrifft heutzutage alle Anwendungsbereiche von Automatisierungssystemen

Warum ein Angriff auf OT-Systeme heutzutage leicht ist

Sich in Systeme, Anlagen und Maschinen zu hacken ist heutzutage gar nicht mehr so schwer. Wussten Sie, dass man dafür kaum Programmierkenntnisse benötigt?

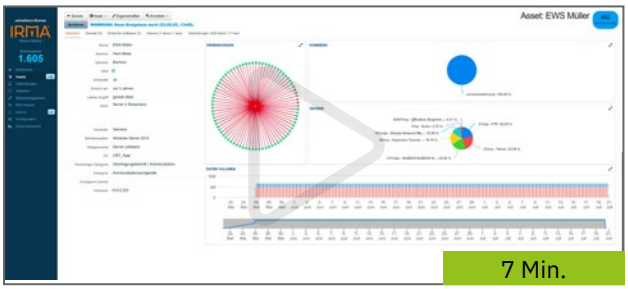
Erleben Sie, wie sich unser Hacker „Leon“ auf spielerische Art in einer Produktionsanlage kinderleicht austobt. Es gibt für ihn so viele Möglichkeiten, von außen in die Systeme zu kommen. Was hier im Video ein Spaß ist, ist im Umfeld der Industrie leider bittere Realität. Das sind Traumverhältnisse für Cyber-Kriminalität mit fatalen Folgen wie Anlagenstillstand, externem Zugriff auf sensible Daten sowie externem Eingriff in Unternehmensprozesse (oft vorerst unbemerkt).
Schützen Sie OT- und IT-Bereich ganzheitlich im Zusammenspiel.



„Warum ein Angriff auf OT-Systeme heutzutage leicht ist“: Video ansehen

Erkennen Sie Angriffe rechtzeitig durch ein OT-Monitoring

Oftmals breitet sich eine Schad-Software unbemerkt in Anlagen und ggf. in weiteren Netzwerken aus. In der Regel vergehen von der Erstinfektion bis zum Schaden mehrere Wochen bis Monate. Erste Anzeichen einer Infektion sind in den meisten Fällen schon früh erkennbar.
Empfehlung: Nutzen Sie ein Frühwarnsystem durch eine automatisierte Anomalieerkennung in Ihrem Automatisierungsnetzwerk. Wenden Sie mögliche fatale Schäden frühzeitig ab.



„Einblick in ein Anomalieerkennungssystem“: Video ansehen

EU-Gesetzgebung
Cyber-Security-Regularien verschärfen sich

Zentrale Richtlinien und Verordnungen

Um der Bedrohungslage in der Industrie zu begegnen, werden die Regularien für Cyber Security auf EU-Ebene zunehmend verschärft. Die Anforderungen für Unternehmen nehmen von gesetzlicher Seite stetig zu.

NIS 2.0 – EU-Richtlinie zur Netzwerk- und Informationssicherheit
Relevant für alle Betreiber von Maschinen aus mittleren und großen Unternehmen, die auf dem Binnenmarkt der Europäischen Union im Rahmen von wesentlichen und wichtigen Sektoren tätig sind.

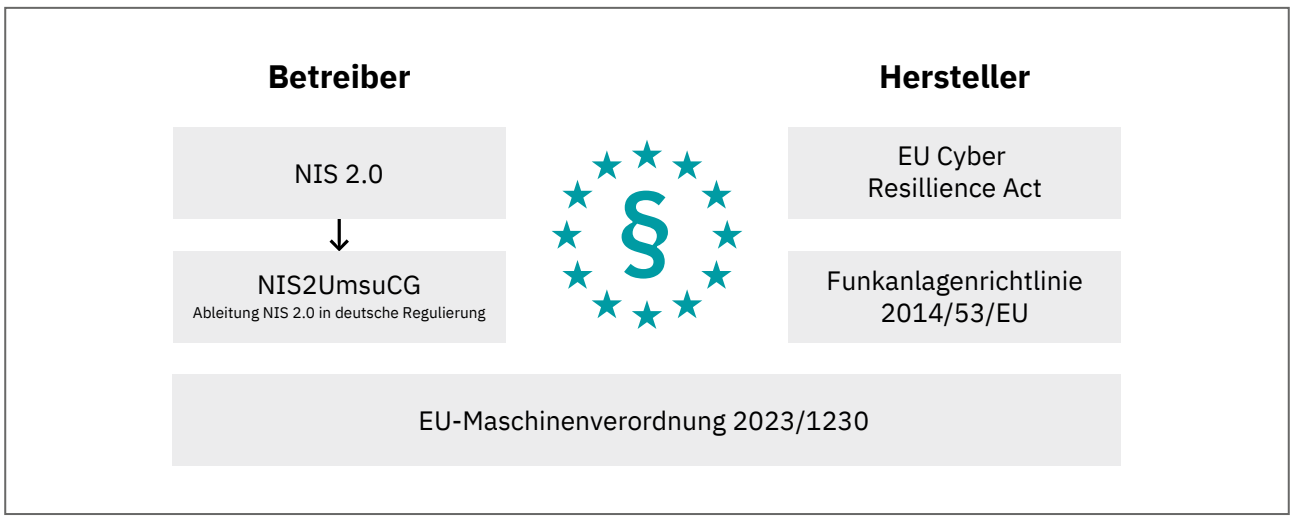
Ableitung nationales Gesetz in Deutschland (NIS2UmsuCG): NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
Die Mitgliedsstaaten haben nun bis zum 17. Oktober 2024 Zeit, sie in nationales Recht umzusetzen (Übergangsfrist bis 2026).
Mögliche Folgen für Unternehmen bei Nicht-einhaltung: Bußgelder in Höhe von bis zu zehn Millionen Euro oder zwei Prozent des gesamten, weltweit erzielten Jahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr.
Zu den verpflichtenden Maßnahmen gehört u. a. die Einführung eines Risikomanagements.

NIS2UmsuCG (NIS2-Umsetzungsgesetz)
Das Gesetz zur Umsetzung von NIS 2.0 und Stärkung der Cyber-Sicherheit, das NIS2UmsuCG, wird ab 2024 in Kraft treten. Es überführt die EU-weiten Mindeststandards für Cyber Security der EU-Direktive NIS2 in deutsche Regulierung. Fokus: KRITIS. Es erweitert die deutsche KRITIS-Regulierung von 2015 deutlich mit mehr Pflichten für einen größeren Betreiberkreis, höheren Cyber-Security-Anforderungen und mehr Befugnissen für den Staat und Regulierungsbehörden. Vom zukünftigen NIS-2.0-Umsetzungsgesetz werden in Deutschland knapp 30.000 weitere Unternehmen neu betroffen sein.

EU-Maschinenverordnung 2023/1230
Regelt ein einheitliches Schutzniveau zur Unfallverhütung für Maschinen und unvollständige Maschinen. Die neue Verordnung erstreckt sich auch auf mit Software betriebene Maschinen und verlangt Risikobeurteilungsverfahren, auch für Security-Bedrohungen.
Seit 29. Juni 2023 ist die Verordnung in Kraft, mit einem Übergangszeitraum von 42 Monaten, allerdings treten einige Punkte bereits früher in Kraft.

EU Cyber Resilience Act (digitale Produkte)
Der Cyber Resiliance Act wurde im März 2024 vom EU-Parlament angenommen und definiert Security-Anforderungen an Hersteller von Produkten mit digitalen Elementen.
Für die Umsetzung haben die Mitgliedstaaten ab Inkrafttreten 24 Monate und Hersteller 36 Monate Zeit.
Zu den Pflichten für Hersteller gehören u. a. ein Schwachstellenmanagement, Dokumentationen (wie z. B. SBOM) sowie technische Anforderungen an das Produkt. Die Konformität müssen Hersteller im Rahmen der CE-Kennzeichnung erklären.

Funkanlagenrichtlinie 2014/53/EU
Bezieht sich auf Geräte, die elektromagnetische Signale zur Kommunikation oder Ortung erzeugen bzw. empfangen können. Mit einer delegierten Verordnung vom 29. Oktober 2021 erweitert die Europäische Kommission Anwendungsbereich und Gesetzeszweck. Funkanlagen, die direkt oder indirekt mit dem Internet kommunizieren, müssen Cyber-Sicherheit und Datenschutz sicherstellen.



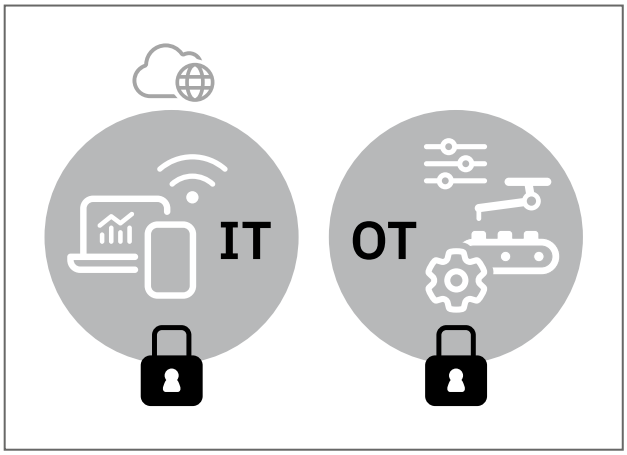
Zusammenspiel IT/OT

Unternehmensweit ist ein neues Denken und Handeln erforderlich

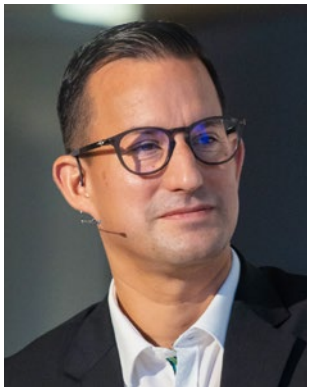
Der Trend zu einer Smart Factory stellt Verantwortliche für unternehmensweite Informationssicherheit vor erhebliche Herausforderungen.

Früher:

- Systeme zur Automatisierung (OT = Operation Technology) waren in der Regel ein vom Internet isoliertes System. Das Risiko vor Hackerangriffen war hierdurch sehr gering. Hinzu kommt, dass eine Cyber-Kriminalität, die es gezielt auf Automatisierungsnetzwerke absieht, im Markt noch kaum vorhanden war, auch weil hierfür die Mittel und das Wissen noch fehlten bzw. der Allgemeinheit noch nicht frei zugänglich waren.
- Lediglich das Büronetzwerk war mit dem Internet verbunden.
- Die Verantwortungsbereiche der IT (Information Technology) und OT waren klar definiert und wurden sowohl getrennt voneinander betrachtet sowie isoliert voneinander betrieben. Schnittmengen der beiden Tätigkeitsbereiche waren nur in wenigen Fällen erforderlich.



Der OT-Bereich war oft eine Insellösung. Das Risiko von Cyber-Kriminalität war im OT-Bereich gering, da es hier noch keine Vernetzung zu externen Netzwerken (IT und Internet) gab.



„Vor dem Hintergrund derzeitiger Bedrohungsszenarien müssen neue Automatisierungskonzepte entstehen, die gemeinsam vom Hersteller und Betreiber umzusetzen sind."

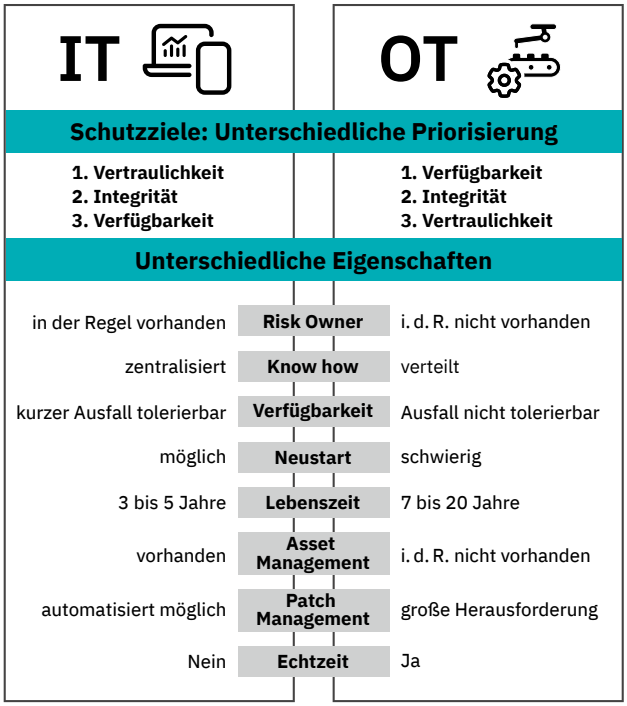
Torsten Gast, Director Competence Center Services,
Phoenix Contact Deutschland GmbH

Heute „IST“ – Chance, Potenzial:
Der Trend einer Smart Factory hält in der Industrie branchenübergreifend Einzug. Neue Technologien bieten Unternehmen entscheidende Entwicklungschancen, Aufgaben von Mensch und Maschine erheblich zu unterstützen. Das können z. B. hochautomatisierte Fertigungsprozesse sein mit intelligenten Werkstücken, die sich selbst überwachen, verifizieren und für die Vernetzung aller beteiligten Einrichtungen sowohl in als auch außerhalb der Unternehmung sorgen.
Digital Factory Transformation steht auf der Agenda höchster Unternehmensebene: Das Automatisierungsnetzwerk wird entsprechend zunehmend mit dem Internet verbunden.

Neben lukrativen Potenzialen sorgt die zunehmende Vernetzung des OT-Bereichs für erhebliche Sicherheitslücken in der IT und OT. Ein integriertes Handeln der beiden Bereiche ist gefordert.

Heute „IST“ – Risiko, Herausforderung:

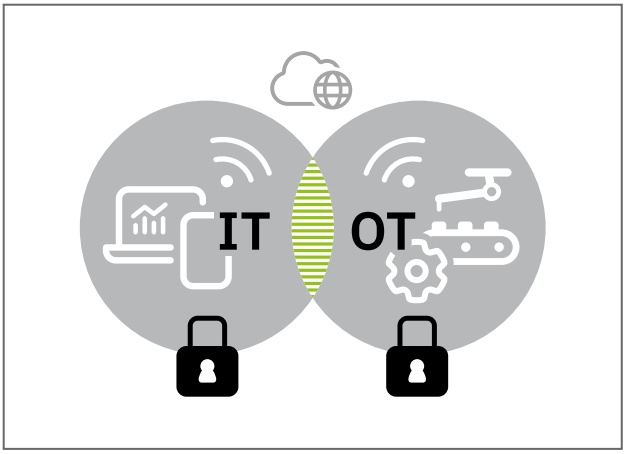
- Bestehende Strukturen der Unternehmen sind in den meisten Fällen auf diesen Trend der Digitalisierung noch nicht ausgelegt (Menschen, Prozesse, Technik). Sei es, dass eine fehlende Klarheit und Transparenz vorliegt, wer für die Informationssicherheit im Automatisierungsnetzwerk (IT ↔ OT?) verantwortlich ist. Sowie eine fehlende Sensibilisierung der Mitarbeitenden, wie unternehmenskritisch Cyber-Vorfälle sind, die im Markt exorbitant zunehmen.
  Auch der weitere Einsatz von Komponenten in alten Maschinen, die aktuelle Sicherheitsstandards nicht erfüllen, öffnet Cyber-Kriminellen oftmals unbewusst die Tür zum Unternehmen.
- Der Bereich eines Automatisierungsnetzwerks „tickt“ im Vergleich zu einem Büronetzwerk unterschiedlich. Hinzu kommt, dass sie heute oftmals noch getrennt voneinander betrachtet und betrieben werden, wodurch häufig unbewusst erhebliche Sicherheitslücken in der Unternehmung vorliegen.



Der Büro- (IT) und Automatisierungsbereich (OT) „ticken“ unterschiedlich, eine zentrale Herausforderung bei der Realisierung von unternehmensweiter Informationssicherheit.

Heute „SOLL“ – Umfassende IT- und OT-Security durch ein ganzheitliches Vorgehen

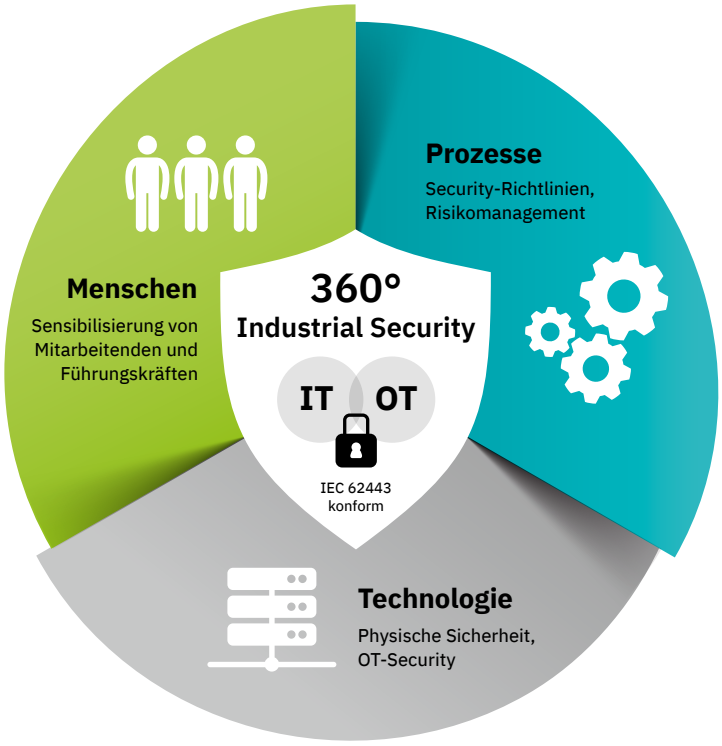
- IT und OT haben ein einheitliches Verständnis und ein gemeinsames Vorgehen zum essenziellen, übergreifenden Unternehmensziel der Informationssicherheit.
- Es ist ausgehandelt und transparent, wer für welche Aspekte der Informationssicherheit im Automatisierungsnetzwerk verantwortlich ist.
- Ein ganzheitliches Sicherheitskonzept ist in Zusammenarbeit von IT und OT unternehmensweit entwickelt und implementiert. Dieses Konzept berücksichtigt sowohl zentrale menschliche, prozessuale als auch technische Aspekte.



Für eine unternehmensweite Informationssicherheit ist es essenziell, dass IT und OT ein einheitliches Verständnis und ein gemeinsames Vorgehen haben.

360°-Industrial-Security

Unabdingbar – ein ganzheitlicher 360°-Industrial-Security-Ansatz (Menschen, Prozesse, Technologie) zur umfassenden Sicherung Ihrer Anlage.



„Unabdingbar – ein ganzheitlicher 360°-Industrial-Security-Ansatz“: Fachartikel lesen

„Der OT-Bereich steht bei unserem unternehmensweiten Ziel der Informationssicherheit seit einigen Jahren ebenfalls im Fokus. Es war von Anfang an klar, dass er eine besondere Herausforderung ist.

IT und OT dann an einen Tisch zu bekommen, war gar nicht einfach. Auch weil unterschiedliche Sprachen gesprochen und unterschiedliche Schutzziele verfolgt werden.

Seitdem wir ein gemeinsames Verständnis entwickelt haben, sind wir unseren unternehmensweiten Sicherheitszielen entscheidend näher gekommen.

Mit zahlreichen Workshops und intensiven Diskussionen war der Weg nicht einfach, gelohnt hat er sich aber für alle.“

Matthias Krause, CISO,
Phoenix Contact GmbH & Co. KG

Standards

International etablierte Cyber-Security-Normen in der IT- und OT-Welt

ISO/IEC 2700x

Standardreihe für IT-Sicherheit
Die Standardreihe ISO/IEC 2700x ist die führende international anerkannte Norm für IT-Sicherheit (Informationssicherheit) für Unternehmen und Organisationen jeglicher Art. Die Reihe beschreibt insbesondere die Planung, die Realisierung, den Betrieb und die Optimierung eines dokumentierten Informationssicherheits-Managementsystems.

Die Normenreihen ISO 2700x und IEC 62443 ergänzen sich – OT und IT im Zusammenspiel.

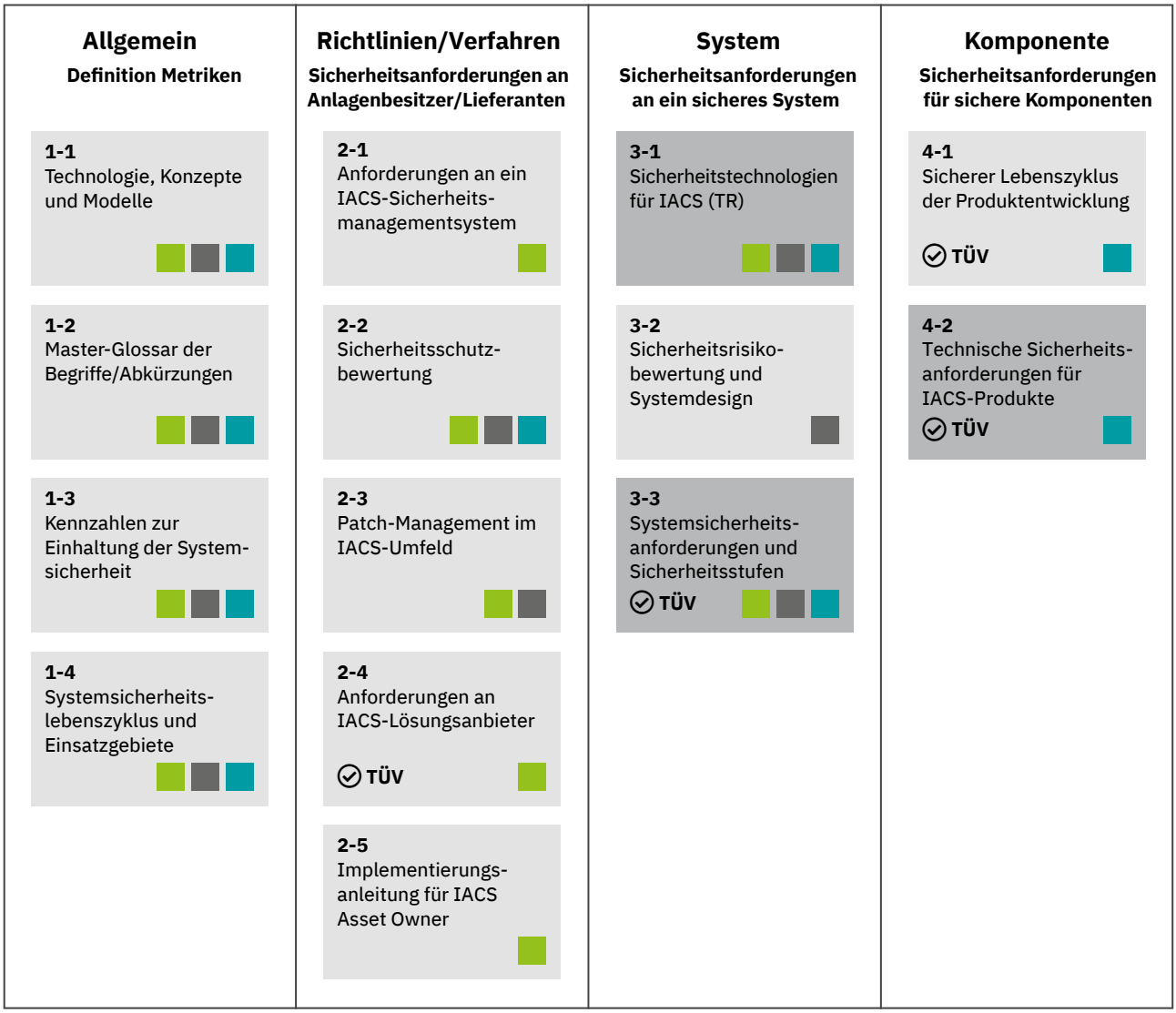
IEC 62443

Der Security-Standard der Industrie
Die IEC 62443 ist der Security-Standard der Industrie. Die Norm ist sehr breit ausgelegt. Sie stellt im Wesentlichen Methoden und Sicherheitsanforderungen für die verschiedenen Rollen in der Automatisierung bereit, sei es für Betreiber, Hersteller, Dienstleister, Systemintegratoren oder für Komponentenhersteller.
Die Normenreihen ISO 2700x und IEC 62443 ergänzen sich. ISO 2700x beschreibt das Sicherheitsmanagement für das gesamte Unternehmen. IEC 62443 detailliert die Security-Konzepte für den speziellen Bereich der Automatisierungstechnik.

„Der Security-Standard der Industrie, die IEC 62443, verständlich erklärt“: Video ansehen

Unabhängig davon, welche branchen- bzw. sektorspezifischen Security-Anforderungen erfüllt werden müssen: Mit dem risikobasierten Ansatz der IEC 62443 können grundsätzlich alle wesentlichen Themen abgedeckt werden.

Aufbau der IEC 62443



Relevant für:

- Anlagenbetreiber (z. B. Produktion, Gebäude, Windrad)
- Anlagenbauer/Dienstleister
- Komponentenhersteller

Anforderungstyp:

- Funktionale Anforderungen
- Prozessanforderungen

TÜV

Phoenix Contact ist übergreifend TÜV-zertifiziert

Direkt für Ihre Praxis

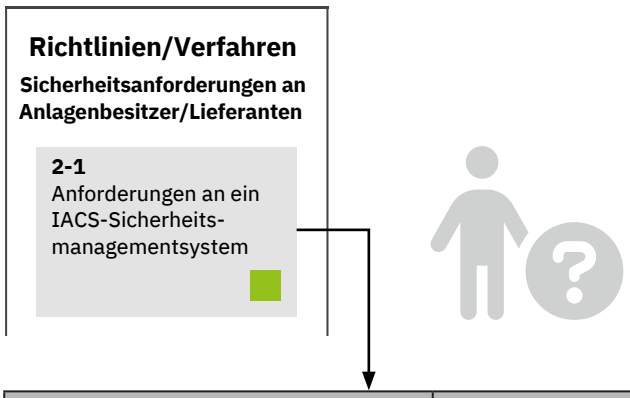
Etablierte Vorgehensweisen und Konzepte gemäß des internationalen Security-Standards IEC 62443

Anforderungen und Herausforderungen

Anforderungen an ein Sicherheitssystem und Herausforderungen bei der Realisierung

IEC 62443-2-1: Anforderungen an ein IACS-Sicherheitsmanagementsystem

› Aufbau der gesamten IEC 62443 siehe Seite 14



„Da ändert sich nur der Stecker“ – eine in der Praxis häufig anzutreffende falsche Annahme mit möglicherweise fatalen Folgen.

Anforderungen (Spezifikation SPE)	Häufige Herausforderungen bei der Realisierung	
SPE1: Organisatorische Sicherheitsmaßnahmen • ORG 1: Sicherheitsbezogene Organisation/Richtlinien • ORG 2: IT-Sicherheits-bewertungen und -prüfungen • ORG 3: Sicherheit des physischen Zugriffs	Fehlendes Bewusstsein für das unternehmenskritische Thema „Informationssicherheit“: • Wer ist verantwortlich für die Sicherheit von Informationen im OT-Bereich? Das ist oftmals nicht definiert und transparent.	
SPE2: Konfigurationsmanagement • CM 1: Inventarmanagement der IACS-Hardware/-Software-Komponenten und IACS-Netzwerkkommunikation	Fehlende Dokumentation: • Welche Komponenten gibt es, wie sind sie konfiguriert? Häufig ist weder die Netz-werkkommunikation noch die Funktionsweise der Geräte dokumentiert.	Verwendung von andersartigen Protokollen im OT-Bereich: • Einsatz von Protokollen, die im IT-Bereich komplett unbekannt sind und teilweise spezielle Anforderungen an eine Hardware vorgeben (wie PROFINET). *(Weitere Herausforderungen siehe auch SPE3, SPE4, SPE5)*

<table>
<tr><th>Anforderungen (Spezifikation SPE)</th><th colspan="2">Häufige Herausforderungen bei der Realisierung</th></tr>
<tr><td>SPE3:
Netzwerk- und Kommunikationssicherheit
• NET 1: Systemsegmentierung
• NET 2: Sicherer drahtloser Zugang
• NET 3: Sicherer Fernzugriff</td><td>• Keine Segmentierung/ flache Netzwerke.
• Kein zentral geregelter Remote-Zugriff: Keine Transparenz, wer hat von extern Zugriff auf welche Anlage?</td><td rowspan="3">(Weitere Herausforderungen siehe auch SPE2)
• Einsatz von Protokollen (wie PROFINET) ohne Sicherheitsmechanismen gegen Manipulation.
• Häufig fehlendes Grundverständnis bezüglich serieller Kommunikation (PROFIBUS oder INTERBUS) zu Ethernet bzw. PROFINET. „Da ändert sich nur der Stecker“ – eine in der Praxis häufig anzutreffende falsche Annahme mit möglicherweise fatalen Folgen.
• Mittels Ethernet-Technologie werden smarte Anwendungen möglich. Durch deren Nutzung ohne eine Berücksichtigung von Sicherheitsaspekten erfolgt oftmals unbewusst eine unsichere Verbindung in andere interne sowie externe Netzwerke.
• Protokolle aus der OT sind nicht routbar, um sie einsetzen zu können braucht man ein flaches Netzwerk.</td></tr>
<tr><td>SPE4:
Komponentensicherheit
• COMP 1: Geräte und Datenträger
• COMP 2: Schutz vor Schad-Software
• COMP 3: Patch-Management</td><td>Herausforderungen beim Schutz gegen Schad-Software:
• Antiviren-Software lässt sich nicht auf allen Komponenten installieren, Patch-Management nicht vorhanden, teilweise abgekündigte Komponenten.</td></tr>
<tr><td>SPE5:
Schutz der Daten
• DATA 1: Schutz von Daten</td><td>• Welche sensiblen Daten (z. B. geheime Rezepturen) werden in Maschinennetzwerke übertragen, wie sind sie gesichert?</td></tr>
<tr><td>SPE6:
Benutzerzugriffskontrolle
• USER 1: Identifizierung und Authentifikation
• USER 2: Autorisierung und Zugriffskontrolle</td><td colspan="2">Oftmals ist kein sicheres Berechtigungskonzept/User-Management implementiert:
• Verwendung von Default-Passwörtern und Shared User Accounts.
• Bildschirme werden oftmals nicht automatisiert gesperrt, sodass sensible Daten für Unberechtigte ohne Aufsicht einsehbar sind.
• Über ein und die gleiche Visualisierung können unterschiedliche Ausführungen gesteuert werden wie Anlagenbedienung (z. B. Teile einlegen) und Instandhaltung (z. B. Änderungen an der Maschine vornehmen).
• Oftmals liegt keine technische Möglichkeit vor, ein User-Management zu implementieren.</td></tr>
</table>

Anforderungen (Spezifikation SPE)	Häufige Herausforderungen bei der Realisierung
SPE7: Ereignis- und Vorfallmanagement • EVENT 1: Ereignis- und Vorfallmanagement	Für Security Vorfälle existiert kein Ereignis- und Vorfallmanagement: • Fehlende organisatorische Prozesse – was ist bei einem Security-Vorfall zu tun? • Fehlende technische und prozessuale Systeme zur Detektion von securityrelevanten Ereignissen wie unberechtigter Zugriff, Erkennung von neuen Geräten und Kommunikationsverbindungen.
SPE8: Systemintegrität und -verfügbarkeit • AVAIL 1: Systemverfügbarkeit und vorgesehene Funktionalität • AVAIL 2: Backup/Wiederherstellung/Archivierung	Fehlende Restore-Konzepte/Keine Backups.

Neun zentrale Schritte

Schritt für Schritt zur sicheren Anlage

Entwicklung und Realisierung eines ganzheitlichen Security-Konzepts mit Dokumentation der einzelnen Prozessschritte gemäß IEC 62443

Schritt 1: Bestandsaufnahme
Erfassung der Anlageninformationen zur Identifikation der Einsatzumgebung

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

Schritt 3: Schutzbedarfsanalyse
Ermittlung des Schutzbedarfs zur Absicherung schützenswerter Assets

Schritt 4: Bedrohungsanalyse
Identifizierung relevanter Bedrohungen für die Automatisierungslösung

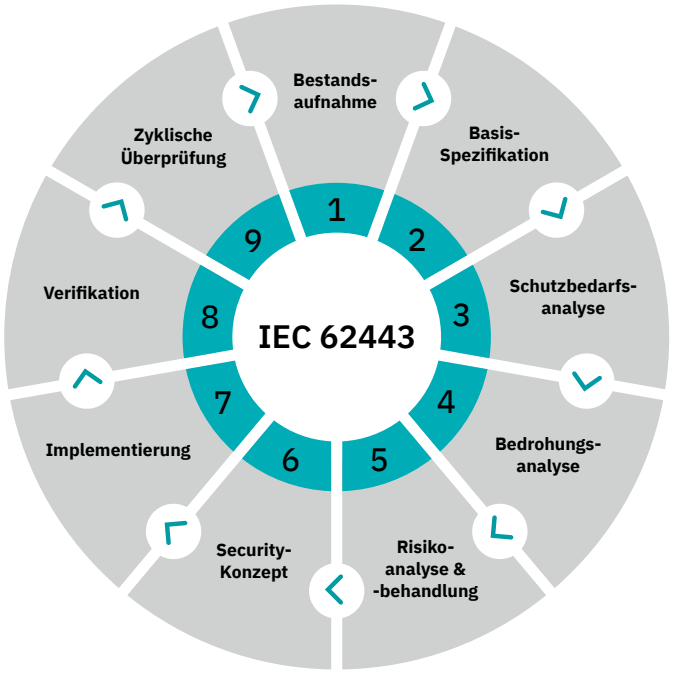
Schritt 5: Risikoanalyse/-behandlung
Erstellung einer Risikoeinschätzung inkl. Ableitung eines Maßnahmenkatalogs

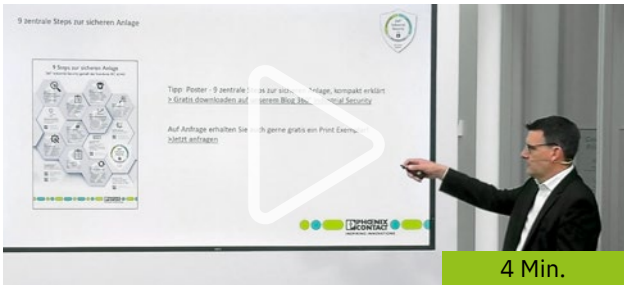
Schritt 6: Security-Konzept
Finalisierung eines individuellen und umfassenden Security-Konzepts

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

Schritt 8: Verifikation
Implementierung prüfen gem. der definierten Security-Konzeptvorgaben (→ Step 6)

Schritt 9: Zyklische Überprüfung
Stay up-to-date – vom Security-Konzept bis zum Knowledge





„Neun Schritte zur sicheren Anlage“ verständlich und kompakt erklärt. Wählen Sie für sich das passende Lernformat – gratis:

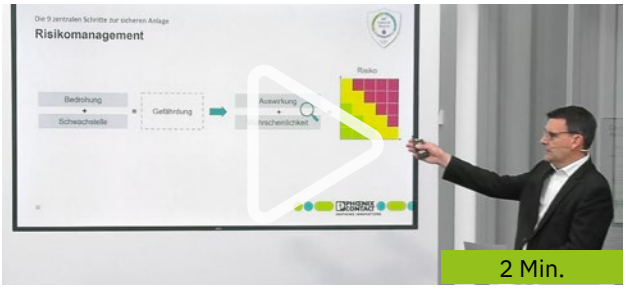
- Video ansehen
- PDF des Posters herunterladen
- Originalposter anfordern

Im Detail: Schritt 5 „Risikoanalyse und -behandlung“

Risikomanagement ist ein elementares Thema im Rahmen der Industrial Security. Zielsetzung ist, das Risiko zunächst einzuschätzen und anschließend einen passenden Maßnahmenkatalog abzuleiten.

Zentrale Schritte:

- Analyse von Wahrscheinlichkeit und Schadensausmaß
- Risikotoleranz des Betreibers festlegen
- Erkannte Bedrohungen anhand der Security-Basisspezifikation bewerten (→ Schritt 2 „Neun Schritte zur sicheren Anlage“ gemäß IEC 62443)
- Ableitung Maßnahmenkatalog zur Risikominimierung



„Risikomanagement“ einfach erklärt an einem Beispiel aus dem Alltag: Video ansehen

Defense-in-Depth-Konzept

Sicherheitssystem mehrschichtig aufbauen

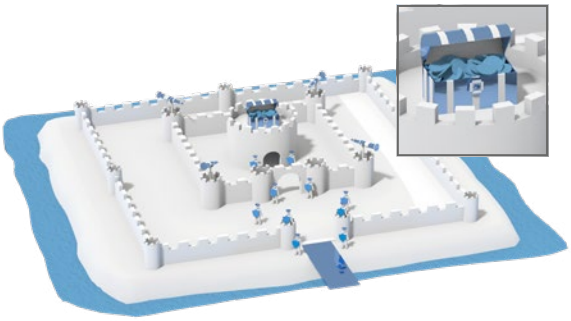
Bauen Sie Ihr Sicherheitssystem mehrschichtig auf. So wie man es schon im Mittelalter bei Burgen getan hat, um die Kronjuwelen zu schützen.

„Defense in Depth“ ist ein wesentliches Konzept der IEC 62443. Ein System gestaffelter und sich ergänzender Sicherheitsmaßnahmen auf mehreren Ebenen. Wenn einzelne Sicherheitsmaßnahmen ausfallen, nicht greifen bzw. eine Sicherheitslücke auftritt, dann ist nicht gleich das ganze Sicherheitssystem eingebrochen und somit der Angreifer nicht gleich an seinem Ziel.

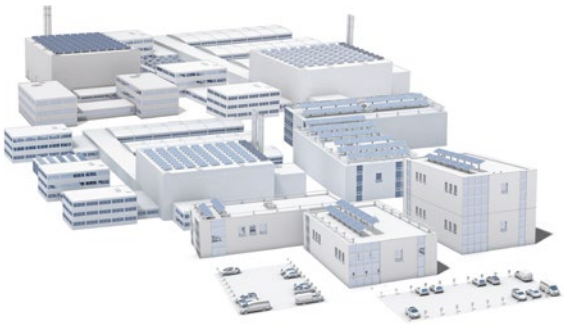
„Das Defense-in-Depth-Konzept einfach erklärt“: Video ansehen

Das Defense-in-Depth-Konzept

Mittelalter
Schutzziel: Kronjuwelen



Heute
Schutzziel: Informationen



Gestaffelte und sich ergänzende Sicherheitsmaßnahmen auf mehreren Ebenen

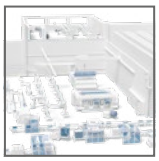
Zugbrücke – Sicherstellung, wer darf rein, wer geht raus?
Analogie zu heute: z. B. Firewall, Drehtür

Bewaffnete Ritter mit verschiedenen Funktionen
Analogie zu heute: z. B. Anomalieerkennungssystem, Berechtigungskonzept

Mauern und Wassergraben
Analogie zu heute: z. B. Netzwerksegmentierung

Wachtürme
Analogie zu heute: z. B. Anomalieerkennungssystem, Kamera

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



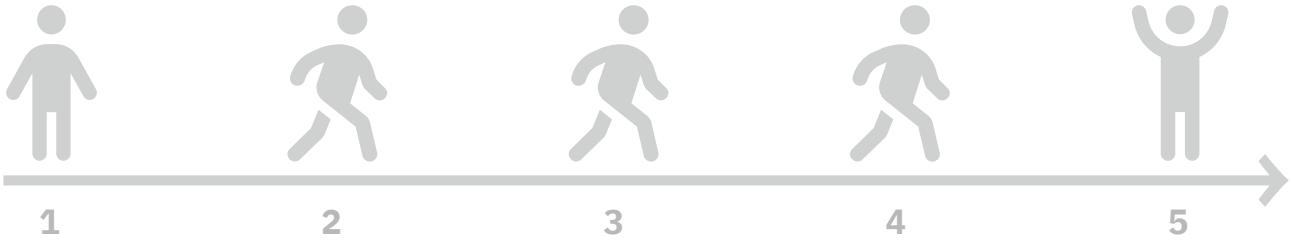
Netzwerkebene
- Netzsegmentierung (Zonen, Conduits)
- VPN
- Verschlüsselung
- Firewalls

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

Praxis-Case

Vom Schutzbedarf zum fertigen Security-Konzept

Wie sieht ein Anwendungsfall auf dem Weg zu 360°-Industrial-Security aus? Vom Schutzbedarf zum fertigen Security-Konzept gemäß IEC 62443.



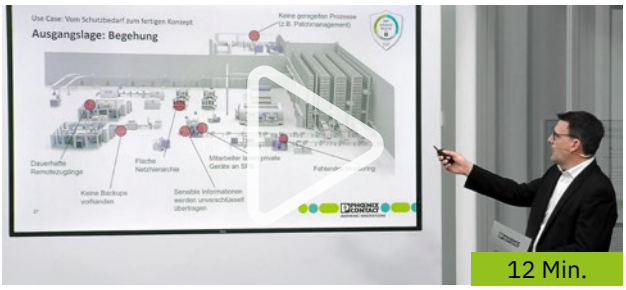
1. Ausgangssituation/Anlagenbegehung
Mögliche Schwachstellen identifizieren (wie dauerhafte Remote-Zugänge, fehlende Backups, Mitarbeitende laden private Geräte an SPS, fehlendes Monitoring, sensible Informationen werden unverschlüsselt übertragen).

2. Schutzbedarfsanalyse
- Welche Daten werden wo verarbeitet bzw. weitergeleitet?
- Schutzzielklassen/Datentypen nach individuellem Schutzbedarf aus Sicht des Betreibers festlegen (vernachlässigbar bis kritisch).
- Welche Komponenten haben mit welchem festgelegten Datentyp zu tun?

3. Bedrohungsanalyse
Welche Bedrohungen liegen vor und welche sind für meine Anlage wirklich relevant? Eine gute Basis sind die Top-10-Bedrohungen des BSI.

4. Risikoanalyse
Szenarien abschätzen:
Bedrohung + Schwachstelle = Gefährdung.
→ Auswirkung + Wahrscheinlichkeit = Risiko

5. Ganzheitliches 360°-Industrial-Security-Konzept
Gezielte Ableitung von Maßnahmen unter Berücksichtigung der Aspekte Mensch, Prozesse, Technik, um das Risiko zu reduzieren.



Vorstellung eines Use Cases: „Vom Schutzbedarf zum fertigen Security-Konzept gemäß IEC 62443“: Video ansehen

Use Case: vom Schutzbedarf zum fertigen Konzept

IEC 62443-2-4

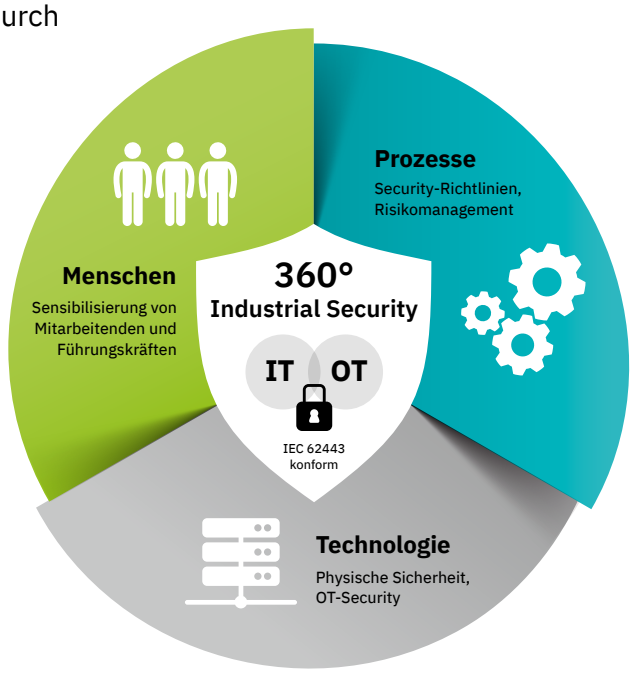
- ◯ Mitarbeitende
- ◯ Zusicherung
- ◯ Systemaufbau
- ◯ Drahtlose Verbindung
- ◯ Konfigurationsverwaltung
- ◯ Fernzugriff
- ◯ Ereignisse
- ◯ Nutzerkonten
- ◯ Schutz gegen Schad-Software
- ◯ Patch-Management
- ◯ Datensicherung und -wiederherstellung

Keine geregelten Prozesse

✓ Individuelle Abläufe wurden erarbeitet

Mitarbeitende laden private Geräte an SPS

✓ Personal wird regelmäßig durch Awareness-Maßnahmen sensibilisiert



Keine Backups vorhanden

✓ Templates und Abläufe erarbeitet

Fehlendes Monitoring

✓ IDS-System überwacht die Systeme und alarmiert in Echtzeit

Dauerhafte Remote-Zugänge

✓ Zentraler Zugang mit Schlüsselschalterlösung

Sensible Informationen sind unverschlüsselt

✓ VPN auch innerhalb der Anlage

Flache Netzhierarchie

✓ Basierend auf Funktion und Schutzbedarf segmentiert

Jetzt richtig durchstarten

Starterleistungen für jedes Sicherheits-level – setzen Sie Industrial Security ganzheitlich um (IT und OT)

Unser Starter-Angebot 360°-Industrial-Security:

- Gratis Starter-Workshop: Kompakter schneller Einstieg
- Ihr individueller Starter-Tag: Seminar und Workshop
- Angriffe frühzeitig abwenden durch Anomalieerkennung

Jetzt durchstarten

360°-Industrial-Security
Starten Sie direkt und zukunftsfähig durch

Unser Angebot für Sie:

Gratis Starter-Workshop
Ein kompakter schneller Einstieg: Neben zentralem topaktuellen Wissen erhalten Sie von unserem Expertenteam erste passende Lösungsansätze, um Ihre Anlage ganzheitlich zu sichern. Und zwar im Zusammenspiel von OT und IT. Dauer und Ort: 1 Stunde, online

Gratis Starter-Workshop: Termin vereinbaren

Ihr individueller Starter-Tag 360°-Industrial-Security
Nach Ihren Wünschen: Stark komprimiertes Fachwissen. Wie setze ich Industrial Security richtig gemäß des international etablierten Standards IEC 62443 um? Zudem: Verlässliche Antworten, Handlungsempfehlungen und Lösungsansätze, optimal auf Ihre Anlage und Unternehmung zugeschnitten.

- Format: Halbtagsseminar mit anschließendem Workshop
- Ort: Online oder direkt vor Ort

Starter-Tag: Mehr erfahren und Termin vereinbaren

Angriffe frühzeitig abwenden durch Anomalieerkennung
Nutzen Sie ein Frühwarnsystem durch eine automatisierte Anomalieerkennung in Ihrem Automatisierungsnetzwerk. Wenden Sie mögliche fatale Schäden rechtzeitig ab. Wir begleiten Sie von der Implementierung des Systems bis hin zur Auswertung erster Analysedaten. Auf Wunsch leiten wir passende Maßnahmen in Form von Handlungsempfehlungen ab.

„Anomalieerkennung in industriellen Netzwerken“: Fachbeitrag lesen

---

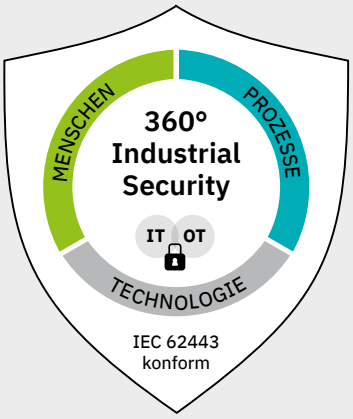
Weitere gefragte Leistungen

- Komplettpaket:
  Sichern Sie Ihre Anlage maximal ab.
- Basisabsicherung:
  Legen Sie einen fundierten Grundstein für Industrial Security.
- Sichere Fernwartung:
  Implementieren Sie Remote-Zugriffe mit maximaler Sicherheit.

Alle Leistungen im Überblick: Leistungspakete für jedes Level – ganzheitlich gesichert, zertifiziert und kosteneffizient

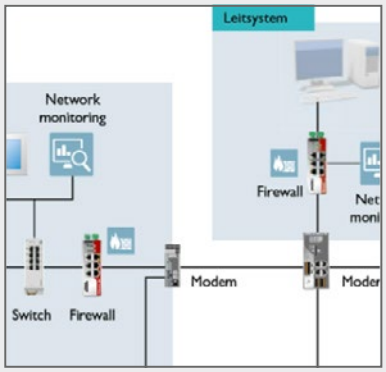
Unser Versprechen für höchste Sicherheit

Ganzheitlich gesichert: 360°-Industrial-Security
Anders als andere: Wir verfolgen konsequent einen übergreifenden 360°-Industrial-Security-Ansatz, der neben der Technik auch zentrale Aspekte von Menschen und Prozessen in Ihrem Unternehmen berücksichtigt. Solch ein übergreifendes Vorgehen ist unabdingbar und für Sie eine Garantie, dass Ihre Anlage unter der Berücksichtigung der zentralen und erfolgskritischen Industrial-Security-Faktoren umfassend und ganzheitlich gesichert wird.



Höchster Qualitätsstandard: Übergreifend zertifiziert
Phoenix Contact ist einer der wenigen Anbieter, deren Dienstleistung, Prozesse und Produktentwicklung TÜV SÜD-zertifiziert sind, gemäß der Norm IEC 62443 (IEC 62443-2-4, -3-3, -4-1 und -4-2) – dem zukunftsorientiertesten Standard für Cyber Security.
Das garantiert Ihnen, dass wir für Sie ein zentraler sowie vertrauensvoller Schlüsselpartner für Cyber Security am Markt sind, mit übergreifender und höchster Industrial-Security-Expertise. Alles mit dem Ziel, Ihre Anlage unter allen erfolgskritischen Aspekten (Mensch, Prozesse, Technik) ganzheitlich und zukunftsorientiert zu sichern.

Kosteneffizienz durch die Entwicklung eines Blueprints
Gemeinsam mit Ihnen entwickeln wir speziell für Ihren Anwendungsfall einen zentralen Blueprint gemäß der Norm IEC 62443, der sich in Ihrem Unternehmen für gleiche Anwendungen hochskalieren lässt. Das sichert Ihnen höchste Qualität und spart Ihnen gleichzeitig Zeit und Kosten ein.
Sowohl unser Vorgehen als Dienstleister als auch unsere Entwicklungsprozesse sind vom TÜV SÜD offiziell geprüft. Das sichert Ihnen eine Leistung auf höchstem Sicherheitsniveau.



Kontakt

Nehmen Sie Kontakt auf

Unser Expertenteam freut sich auf Ihre Kontaktaufnahme. Sprechen Sie uns an!

Zur Beratungsanfrage

Informieren Sie sich und bleiben Sie informiert – nutzen Sie unsere Informationsservices:

Security | Safety | CE-Kennzeichnung – auf LinkedIn folgen

Newsletter „Netzwerktechnik und Security” – zur Registrierung

Torsten Gast

Director Competence Center Services

Tel.: +49 5281 946-5555

services@phoenixcontact.de

360°-Industrial-Security – besuchen Sie auch unsere Webseite

- Zentrales Wissen – wie sichere ich meine Anlage ganzheitlich?
- Dienstleistungen – starten Sie durch mit Copilot
- Seminare – für jedes Knowledge-Level

phoenixcontact.de/industrial-security-consulting

3011480738