Industrial Cyber Security

Standardisiert und zukunftssicher

PHOENIX CONTACT
INSPIRING INNOVATIONS

Industrielle Cyber Security
Vertrauen ist die Basis

Wir leben in einer Zeit, in der die Entwicklung der Kommunikationstechnologien es Millionen von Geräten ermöglicht, Informationen weltweit auszutauschen. Daraus ergibt sich die Notwendigkeit einer Strategie für Netzwerksicherheit und Anlagenverfügbarkeit. Phoenix Contact entwickelt deshalb Lösungen zum Schutz der Systeme Ihres Unternehmens, zur Sicherung des Know-hows und aller sensiblen Datenbestände, aus denen sich die Geschäfts- oder Produktionsprozesse zusammensetzen.

Mehr Informationen zum Thema

Es gibt viele Gründe, sich mit dem Thema Cyber Security auseinanderzusetzen. Diese Broschüre soll Ihnen einen grundlegenden Überblick über das Thema geben und Lösungsansätze aufzeigen.

Aktuelle Informationen zum Thema Cyber Security finden Sie jederzeit unter: https://phoe.co/cyber-security
Zusätzlich finden Sie viele hilfreiche Videos auf unserem Youtube-Channel: https://phoe.co/youtube

QR-Code scannen und mehr Informationen zu Industrial Cyber Security erhalten

Rundum sorglos

Bei uns erhalten Sie alle Werkzeuge für die Security Ihrer Maschinen und Anlagen. Stellen Sie sich aus Produkten, Dienstleistungen und Lösungen Ihr individuelles „Rundum-sorglos-Paket“ zusammen.

Inhalt

Cyber Security – In jeder Branche relevant

Egal ob Hersteller oder Betreiber, Industrie oder kritische Infrastruktur – das Thema Cyber Security geht alle etwas an. Durch die zunehmende Vernetzung und Anbindung industrieller Steuerungs- und Automatisierungssysteme (ICS) an das Internet sind diese zunehmend Cyber-Angriffen und ungewollten Veränderungen ausgesetzt.

Die ICS-Security nimmt daher immer stärker an Bedeutung zu.

Maschinenhersteller

Security steigert die Zuverlässigkeit und Verfügbarkeit Ihrer Maschinen. Für eine Fernwartung beim Kunden ist außerdem eine sichere Fernverbindung Voraussetzung.

Anlagenbetreiber

Security sichert nicht nur die Verfügbarkeit und den zuverlässigen Ablauf Ihrer Anlagen und Prozesse, sondern schützt auch Ihr Produktions-Know-how.

Automobilindustrie

Die Verfügbarkeit Ihrer Anlagen ist Ihr wichtigstes Gut. Security-Mechanismen sichern die Verfügbarkeit Ihrer Produktionsstraßen und können sie möglicherweise sogar erhöhen.

Energiewirtschaft

Unternehmen in der Energiewirtschaft spielen eine wichtige Rolle in der Grundversorgung der Menschen. Aus diesem Grund verpflichtete der Gesetzgeber in vielen Ländern die Betreiber von Anlagen der kritischen Infrastruktur, ihre Anlagen gegen einen unberechtigten Zugriff zu schützen.

Wasser/Abwasser

Ihre höchste Aufgabe ist die Sicherstellung der stetigen Trinkwasserversorgung und Abwasserreinigung. Mit Security sichern Sie Ihren Fernzugriff auf entlegene Pumpen- und Aufzugsstationen und schützen Ihre Automatisierungssysteme vor den zunehmenden Cyber-Angriffen aus dem Internet.

Öl und Gas

Insbesondere in explosiven und leicht entflammbaren Bereichen ist Security inzwischen als Safety-Voraussetzung anzusehen.
Denn eine gehackte Anlage kann schnell nicht nur zu einem finanziellen Risiko, sondern auch zum Sicherheitsrisiko Ihrer Mitarbeiter werden.

Was soll schon passieren? Mögliche Folgen eines Security-Vorfalls

Unternehmen sind nur dann erfolgreich, wenn ihre Produktionsanlagen sicher und störungsfrei arbeiten. Ausfälle, Sabotage oder Datenverlust können einen hohen wirtschaftlichen Schaden verursachen. Denn Stillstandzeiten bedeuten nicht nur einen finanziellen Verlust, sondern gefährden zudem Liefertermine und folglich die Reputation. In einer Standort- und Prozessanalyse können Sie die relativen Risiken Ihres Industriesystems und seine Wechselwirkung mit dem Anlageninformationssystem abschätzen.

Verlust von Know-how

Ein Wettbewerber kann auf Ihre sensiblen Produktionsdaten zugreifen. Können Sie den Schaden wirtschaftlich quantifizieren?

Datenverlust

Plötzlich gehen unternehmenskritische Daten verloren. Wie hoch sind der Aufwand und die Kosten für die Rekonstruktion dieser Daten?

Anlagenstillstand

Aufgrund von Sicherheitsproblemen muss die Produktion für einige Stunden oder Tage gestoppt werden. Wie hoch sind die Kosten eines solchen Produktionsausfalls?

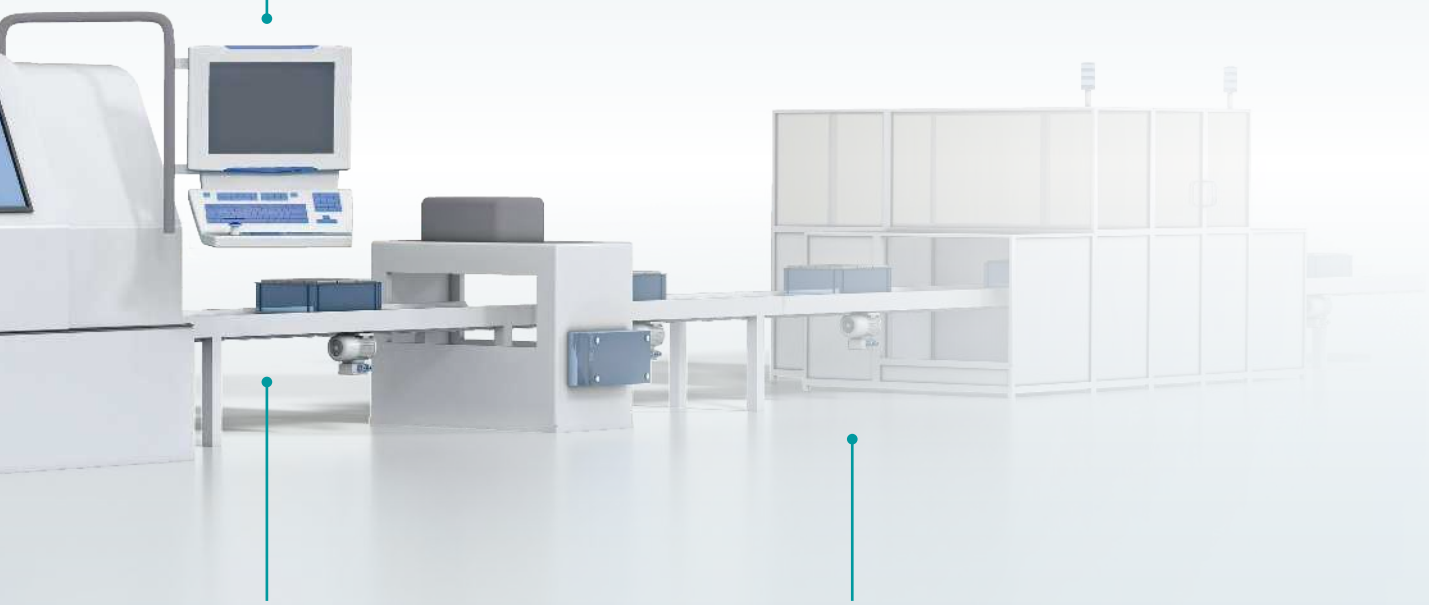
Was schon passiert ist

Die Liste von Security-Zwischenfällen in der Industrie wird immer länger: Begonnen mit „Stuxnet“, einem Schadprogramm speziell für SCADA-Systeme, über den Virus „Industroyer“ (2016) und „TRITON“ (2017), einem gezielten Angriff auf Sicherheitssteuerungen, bis zur Erpressersoftware „WannaCry“ (2017), die weltweit über 230.000 Systeme befallen hatte.

Aktuelle Informationen zu Security-Themen erhalten Sie jederzeit über unsere Social-Media-Kanäle und Newsletter.

Ansehen

Was passiert, wenn Partner und Kunden Ihren Ruf in Bezug auf die Zuverlässigkeit und Sicherheit der Daten Ihres Unternehmens in Frage stellen?



Erpressung mit Ransomware

Totale Blockade von Produktion und Dateien. Wie hoch sind die Kosten für das Lösegeld, das für die Reaktivierung des Produktionsprozesses erforderlich ist?

Personalkosten

Wie viele Arbeitsstunden der Mitarbeiter sind erforderlich, um den Schaden zu beheben, der durch unzureichende Sicherheitsmaßnahmen verursacht wurde?

360° Security
Unser Qualitätsanspruch

Phoenix Contact bietet standardisierte Security in Produkten, Industrielösungen und Dienstleistungen für den zukunftssicheren Betrieb von Maschinen, Anlagen und Infrastrukturen. Security ist im gesamten Lebenszyklus unserer Produkte und Lösungen verankert. Unser Anspruch: moderne Security handhabbar machen, z. B. durch eine einfache Konfiguration, integrierte Security-Funktionen, ausgereifte Komplettlösungen und unterstützende Beratungsleistungen. Die langjährige Verfügbarkeit notwendiger Updates ermöglicht außerdem eine lange Nutzungsdauer unserer Komponenten.

Vollständiges Angebot für Rundum-sorglos-Security

Ihre Daten sind bei uns sicher

Wir kennen uns mit dem Thema Security aus und können Ihnen daher versichern, dass Ihre Daten bei uns stets vertraulich behandelt werden. Phoenix Contact unterhält ein Informationssicherheits-Managementsystem („ISMS“), das entsprechend den Anforderungen aus der ISO/IEC 27001 u. a. den Umgang mit sensiblen Daten und Informationen festlegt.

Sichere Produkte

Phoenix Contact führt einen sicheren Entwicklungsprozess ein. Dabei werden auf Basis einer Bedrohungsanalyse Security-Maßnahmen implementiert, verifiziert und dokumentiert. Darüber hinaus verfügen unsere Produkte über verschiedene Sicherheitsfunktionen wie eine verschlüsselte Kommunikation oder Firewall-Funktionen. Zusätzlich werden Security-Schwachstellen konsequent geprüft und Security-Updates bereitgestellt.

Sichere Dienstleistungen

Ohne die korrekte Implementierung von Security-Mechanismen und die Aufmerksamkeit jedes einzelnen Mitarbeiters kann Security nicht umgesetzt werden. Daher bietet Ihnen Phoenix Contact verschiedene unterstützende Dienstleistungen: von der Einschätzung Ihres individuellen Security-Niveaus, über die Beratung zur Verbesserung Ihrer Security, bis zur Mitarbeiterschulung. Alle Services erfolgen dabei unter Einhaltung höchster Security-Standards. Ihr Anliegen ist bei uns sicher.

Sichere Lösungen

Phoenix Contact verbindet sichere Produkte und Dienstleistungen zu ganzheitlichen Lösungen und Security-Architekturen. Neben sicheren Produkten können wir Ihnen also auch für unterschiedlichste Anforderungen und Branchen sichere Automatisierungslösungen anbieten.

Laufende Verbesserung

Unser Product Security Incidente Response Team (PSIRT) sammelt und analysiert permanent mögliche Sicherheitslücken in unseren Produkten und Prozessen. Sollte eine Sicherheitslücke bekannt werden, sind wir somit in der Lage, sie schnell zu schließen und Ihnen maximale Security zu garantieren.

Alle Meldungen finden Sie unter:
https://phoe.co/ PSIRT

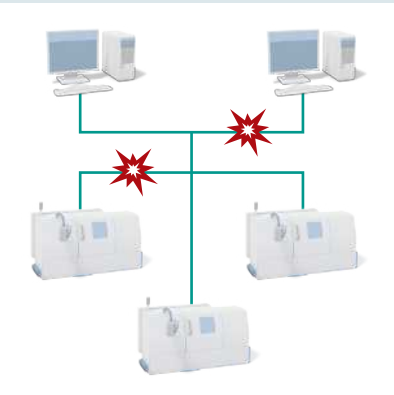
Zertifizierte Security

Phoenix Contact wurde als eines der ersten Unternehmen vom TÜV SÜD nach der IEC 62443 im Teil 4-1:2018 Edition 1.0 zertifiziert. Dies bestätigt, dass wir für die Entwicklung von Security-by-Design-Produkten einen sicheren Entwicklungsprozess zugrunde legen. Auch als Dienstleister für das Design sicherer Automatisierungslösungen sind wir nach der Norm im Teil 2-4 zertifiziert. Darüber hinaus arbeiten wir laufend an weiteren Zertifizierungen für unsere Security-Angebote.

Typische Sicherheitsrisiken und Lösungen

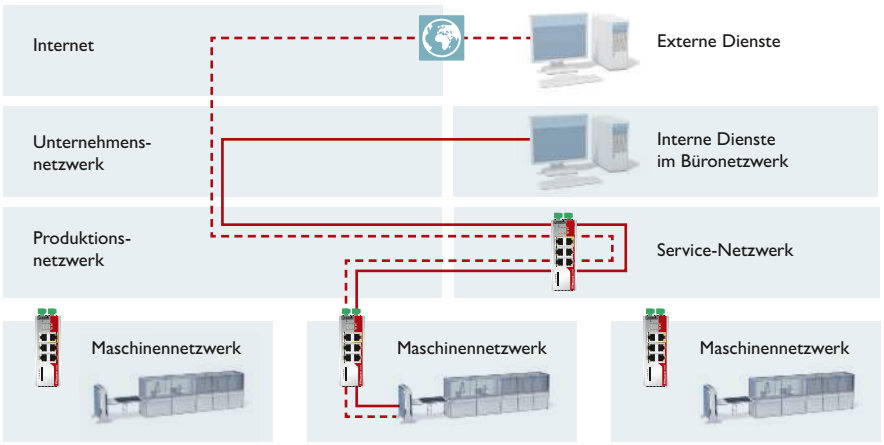
Risiko: Störungen aus dem Office

Störungen und Viren, z. B. aus dem Office-Umfeld, können direkt in den Produktionsbereich übertragen werden.



Lösung: Netzwerksegmentierung

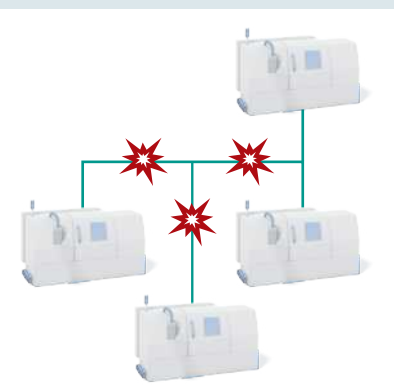
Durch die Aufteilung großer Netzwerke in kleine Segmente kann der Datenaustausch zwischen den verschiedenen Zonen, z. B. zwischen Produktion und Office oder zwischen verschiedenen Anlagenteilen, gesteuert werden. Die Trennung der einzelnen Segmente kann mit Hilfe von VLANs oder Firewalls erfolgen. Für die Kommunikation zwischen den einzelnen Netzwerksegmenten müssen dann Router oder Layer 3 Switches eingesetzt werden. Diese Geräte fangen typische Netzwerkfehler auf, sodass sie sich nicht weiter im restlichen Netzwerk verbreiten können.



Netzwerksegmentierung mit mGuard-Security-Routern

Risiko: Befall mit Schad-Software

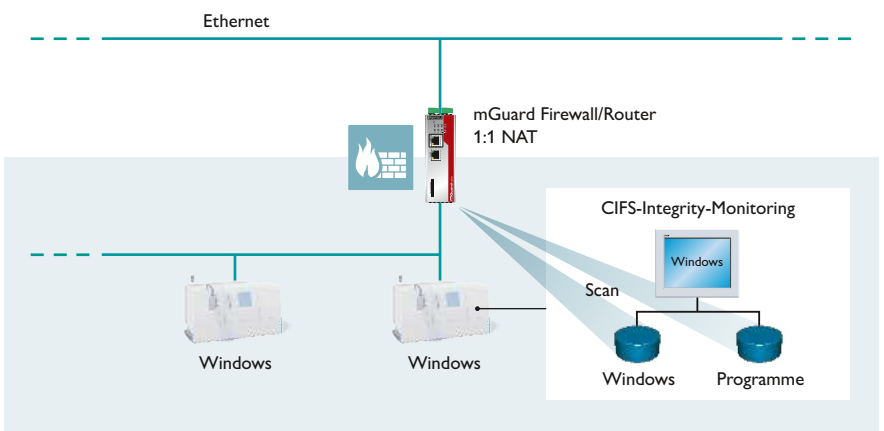
Häufig ist Schad-Software so konzipiert, dass sie versucht, sich auf benachbarte Systeme auszubreiten und diese auch zu befallen. Beispiel hierfür ist die WannaCry-Schad-Software, die ungepatchte Windows-Systeme befallen hat.



Lösung: Eingrenzung der Kommunikation

Durch die Verwendung von Firewalls kann die Verbreitung entsprechender Schad-Software begrenzt oder verhindert werden. Wenn alle Kommunikationsmöglichkeiten unterbunden werden, die nicht technisch notwendig sind, sind viele Angriffe gar nicht mehr möglich.

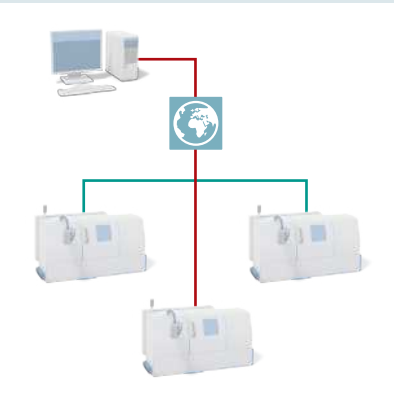
Zusätzlich hilft ein industrietaugliches Integrity Monitoring (z. B. CIM), Veränderungen und Manipulationen an Windows-basierten Systeme wie Steuerungen, Bedieneinheiten oder PCs frühzeitig zu erkennen und einzudämmen.



CIFS-Integrity-Monitoring

Risiko: Hackerangriffe

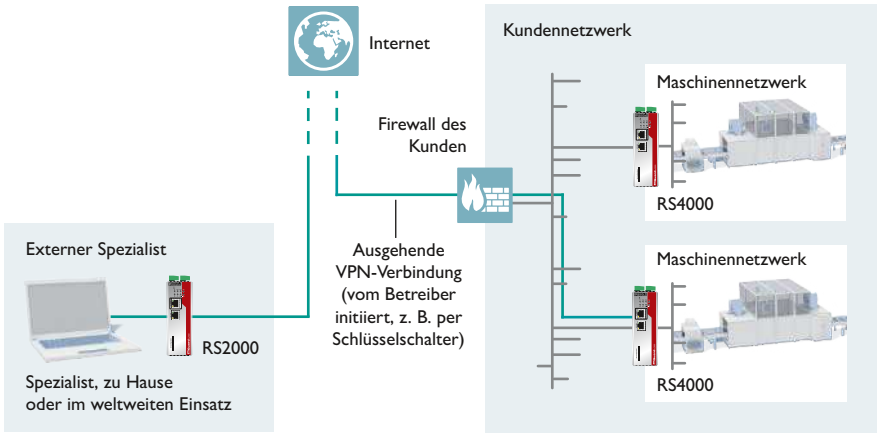
Kriminelle können über eine offene Internetverbindung Daten kopieren oder Änderungen an der Anlage durchführen.



Lösung: Verschlüsselte Datenübertragung

Automatisierungssysteme sollten vom Internet aus nicht zugänglich sein. Dies wird durch eine Firewall am Internetzugang erreicht, die allen eingehenden aber auch den ausgehenden Verkehr auf notwendige und zugelassen Verbindungen beschränkt.

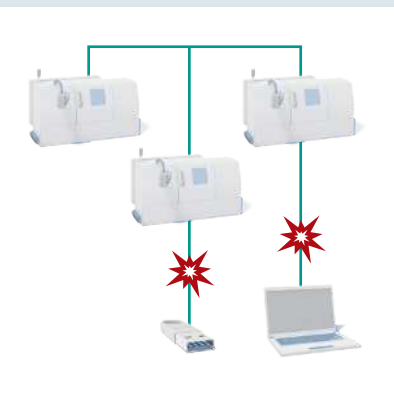
Alle Weitverkehrsverbindungen sollten verschlüsselt durchgeführt werden, z. B. durch VPN mit IPsec.



Sichere Fernwartung mit verschlüsselter Datenübertragung

Risiko: Infizierte Hardware

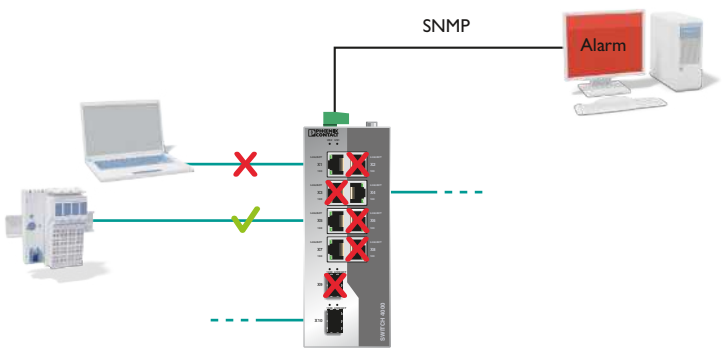
Infizierte Hardware wie USB-Stick oder Laptops können Schad-Software ins Netzwerk übertragen.



Lösung: Ports absichern

Über die Funktion Port Security können Sie direkt an Ihren Netzwerkkomponenten einstellen, dass unerwünschte Teilnehmer keine Daten mit dem Netzwerk austauschen dürfen. Darüber hinaus sollten Sie freie Ports, die nicht benötigt werden, abschalten.

Einige Komponenten bieten zusätzlich die Möglichkeit, Sie via SNMP und Meldekontakt zu alarmieren, wenn ein unberechtigter Zugriff auf das Netzwerk registriert wird.

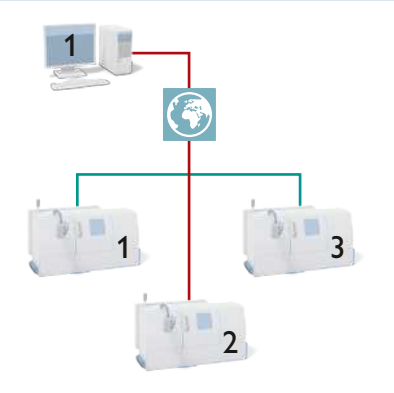


Port-Abschaltung und Alarmierung über SNMP

Typische Sicherheitsrisiken und Lösungen

Risiko: Unberechtigter Zugriff auf Anlagen

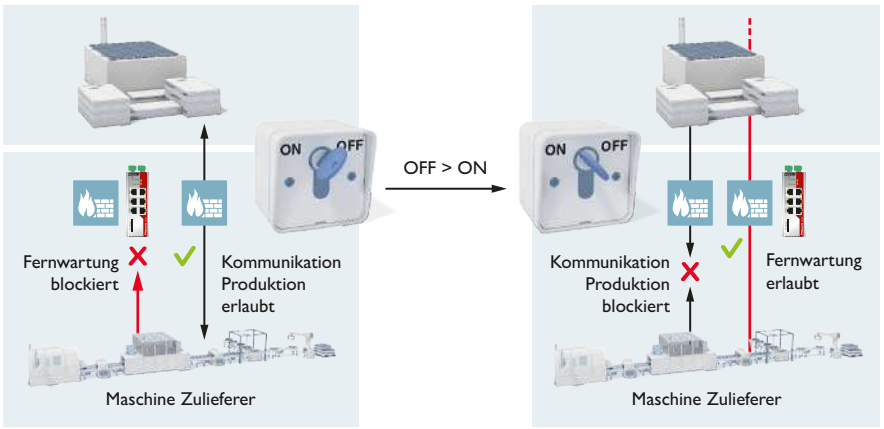
Aus der Ferne werden versehentlich Änderungen am falschen System durchgeführt.



Lösung: Sicherer Fernzugriff

Der sichere Fernzugriff auf eine oder mehrere Maschinen kann mit unterschiedlichen technologischen Lösungen realisiert werden. Zum einen wird die Kommunikation nach außen verschlüsselt, z. B. über IPsec oder OpenVPN. Zum anderen kann über einen Schlüsselschalter an der Maschine die Fernwartung initiiert werden.

So wird sichergestellt, dass nur an der Maschine Änderungen vorgenommen werden, an der dies beabsichtigt ist. Gleichzeitig können über den Schlüsselschalter die Kommunikationsregeln im Netzwerk für die Zeit der Fernwartung blockiert werden.



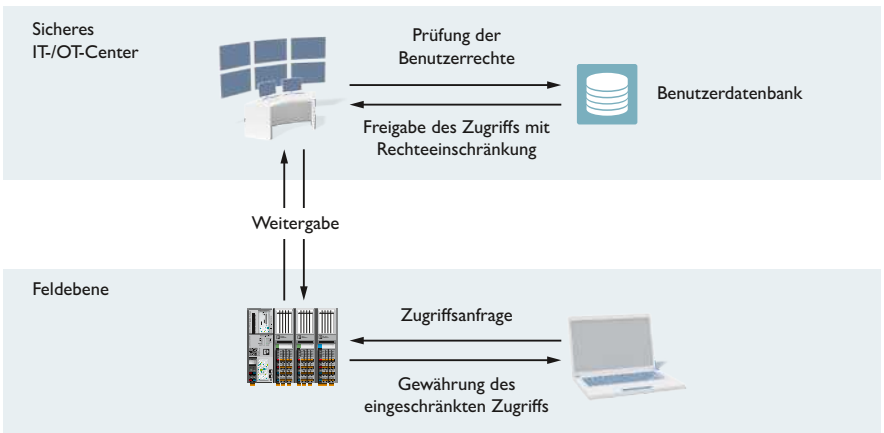
Steuerung der Fernwartung mit Hilfe eines Schlüsselschalters

Risiko: Unzureichendes Benutzermanagement

Häufig werden Sammelpasswörter für Benutzerzugänge genutzt. Verlassen Mitarbeiter das Unternehmen, werden Passwörter nicht geändert oder Zugänge nicht abgeschaltet. Das Sammelpasswort ist dadurch zu vielen Mitarbeitern bekannt und kann missbraucht werden.

Lösung: Zentrale Benutzerverwaltung

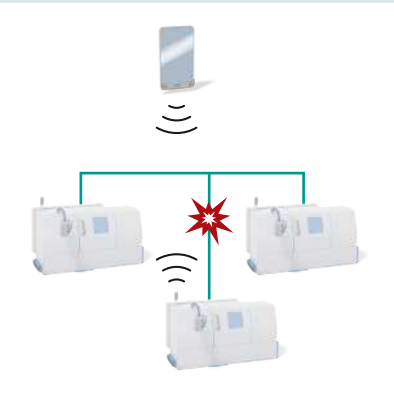
Durch eine zentrale Benutzerverwaltung, die jedem Mitarbeiter einen individuellen Zugang zuweist, kann dieses Problem gelöst werden. Viele Phoenix Contact Geräte unterstützen die Einbindung in ein zentrales Benutzermanagement.



Zentrales Benutzermanagement mit individueller Rechtevergabe

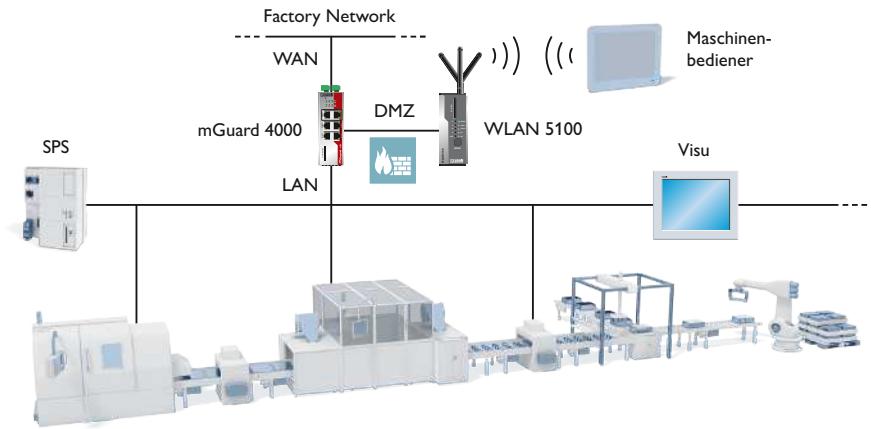
Risiko: Mobile Endgeräte

Nicht autorisierte Smart Devices verbinden sich über die WLAN-Schnittstelle.



Lösung: Sichere WLAN-Passwortvergabe

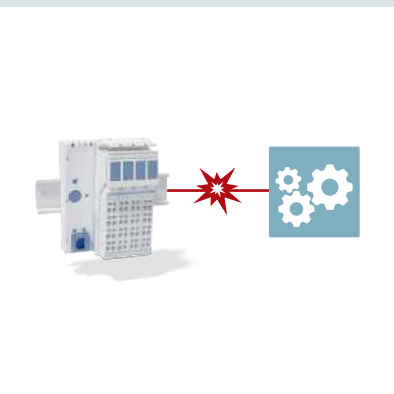
Sind WLAN-Passwörter bekannt und über längere Zeit unverändert, ermöglicht das auch einen unkontrollierten Zugriff Dritter auf das Maschinennetzwerk. WLAN-Komponenten von Phoenix Contact ermöglichen daher ein automatisiertes Schlüsselmanagement durch die Maschinensteuerung. So lassen sich sichere WLAN-Maschinenzugänge in Form von Einmalpasswörtern einfach realisieren. Zusätzlich kann die WLAN-Kommunikation über eine demilitarisierte Zone (DMZ) abgesichert und vom restlichen Netzwerk isoliert werden.



Sichere Einbindung von mobilen Endgeräten mit Einmalpasswörtern und DMZ

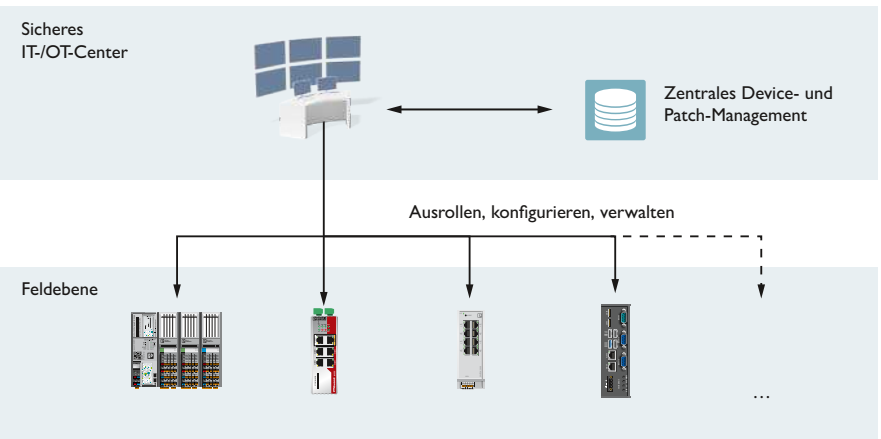
Risiko: Unsichere oder falsche Gerätekonfiguration

Standardkonfigurationen von Geräten sind darauf ausgelegt, dass die Komponenten korrekt funktionieren und sich leicht in Betrieb nehmen lassen. Sicherheitsmechanismen spielen dabei oft eine untergeordnete Rolle.



Lösung: Device- und Patch-Management

Bei der Verwaltung mehrerer Geräte kann ein intelligentes und effizientes Device- und Patch-Management zeitaufwändige Prozesse automatisieren und die Risiken einer Fehlkonfiguration reduzieren. Es unterstützt beim Konfigurieren, Ausrollen und Verwalten von Geräten und reduziert Sicherheit- und Compliance-Risiken durch die Verkürzung von Patch- und Upgrade-Zyklen. Das Device- und Patch-Management ermöglicht die zentrale Erstellung und Verwaltung aller sicherheitsrelevanten Geräteeinstellungen und unterstützt bei Firmware-Upgrades.



Zentrales Patch- und Device-Management

Unser Ziel: Informationssicherheit schaffen

Nachhaltige organisatorische und technische Maßnahmen, orientiert am Lebenszyklus Ihrer Anlage, minimieren das Risiko von möglichen Angriffen. Damit Sie eine möglichst hohe Stabilität und Transparenz Ihrer Infrastruktur erlangen, unterstützen wir Sie bei der Auswahl der passenden und notwendigen Hardware, bei der Ausarbeitung individuelle Schutzkonzepte und auch bei der Umsetzung praxisnaher Schulungen.

Auf Wunsch kombinieren wir unsere Erfahrung, Produkte und Dienstleistungen zu gesamtheitlichen Industrielösungen.

Produkte

Sicher von der Entwicklung bis zum Patch-Management

Die Integration von Security ist integraler Bestandteil unserer Produktentwicklung. Dies beginnt bereits bei einem sicheren Entwicklungsprozess.

Außerdem bieten unsere viele unserer Produkte Security-Funktionen wie z. B. eine sichere Benutzerauthentifizierung, eine Netzwerksegmentierung, Netzwerkmonitoring- und Firewall-Funktionen oder die Nutzung sicherer und verschlüsselter Kommunikationsprotokolle. Darüber hinaus werden unsere Produkte über ihren Lebenszyklus hinweg über ein Schwachstellenmanagement (PSIRT) auf Sicherheitslücken hin geprüft und mit Sicherheitspatches und Updates versorgt.

mGuard Security
Die mGuard-Security-Router bilden das zentrale Security-Rückgrad Ihrer Anlage. Sie bieten spezielle Firewall-Funktionen für die Industrie wie z. B. Conditional Firewall und User Firewall, Deep Packet Inspection für Industrieprotokolle und sichere Netzwerkzugänge für Servicetechniker. Mit der mGuard Secure Cloud erhalten Sie zusätzlich ein System zur einfachen, sicheren Fernwartung.

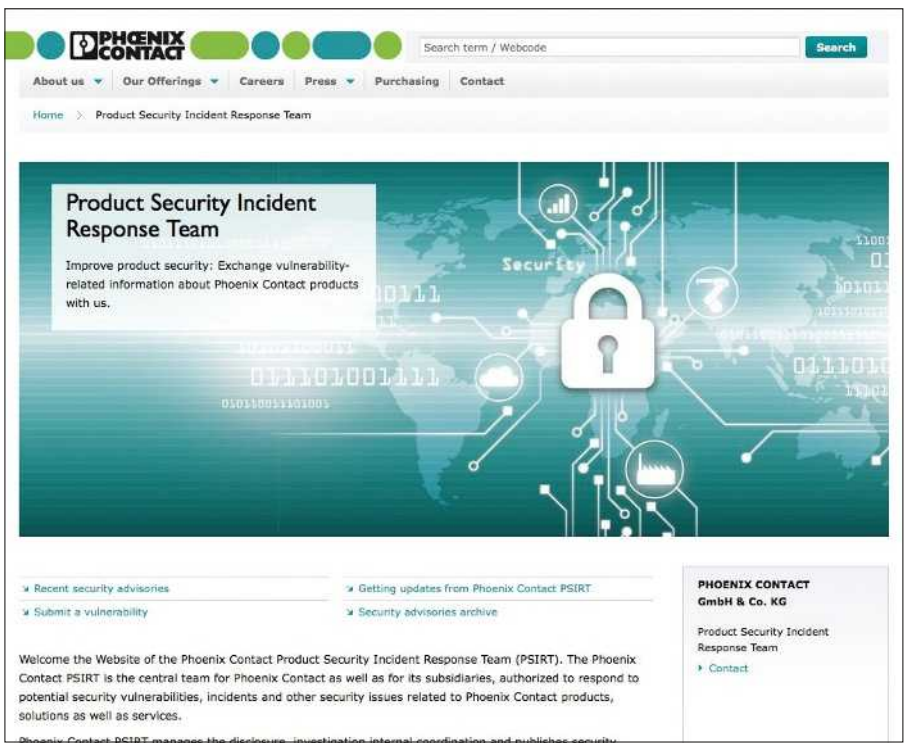
PLCnext Security
Die PLCnext-Steuerungen wurden nach Security-by-Design-Kriterien entwickelt. Die Entwicklungsprozesse sind entsprechend der IEC 62443-4-1 zertifiziert. Die Verwendung eines Trusted Platform Modules (TPM), Nutzung eines konfigurierbaren Linux-Kerns, die Verwendung der Linux-Firewall und die Implementierung eines Crypto Stores für Zertifikate und Schlüssel sind u. a. wichtige Security Maßnahmen.

Schwachstellenmanagement: PSIRT

Um Ihre Sicherheit jederzeit optimal zu gewährleisten, hat Phoenix Contact ein Product Security Incident Response Team (PSIRT) etabliert. Das Team

- reagiert auf potenzielle Sicherheitslücken, Vorfälle und andere Sicherheitsprobleme im Zusammenhang mit Produkten, Lösungen sowie Diensten von Phoenix Contact
- leitet die Offenlegung, Untersuchung und interne Koordination von Sicherheitshinweisen
- veröffentlicht Sicherheitshinweise zu bestätigten Sicherheitslücken, bei denen Maßnahmen zur Abschwächung oder Behebung verfügbar sind.

Alle aktuellen und vergangenen Sicherheitshinweise kommunizieren wir transparent auf unserer Webseite: https://phoenixcontact.com/psirt



PSIRT-Newsletter abonnieren und Sicherheitslücken melden

Dienstleistungen

Bewertung und Planung

Auf Basis des Branchenstandards erarbeiten wir für Sie individuelle Lösungen und Konzepte
- für ausfallsichere Netzwerkstrukturen,
- zur Absicherung oder Fernwartung Ihrer Maschine,
- für leistungsfähige Funknetzwerke

Wir begehen gemeinsam Ihre Anlage und analysieren Ihre individuelle Bedrohungs- und Risikolage, Dokumentationen und Abläufe.

Ergebnis:
Sie erhalten einen ausführlichen Bericht mit Schwachstellen, Handlungsempfehlungen sowie eine Auflistung von erforderlichen Maßnahmen zur Standardabsicherung Ihrer Anlage die dem IT-Grundschutz entsprechen.

Umsetzung

Damit Sie weiterhin den Fokus auf Ihre Kernkompetenzen legen können, übernehmen wir für Sie die Umsetzung Ihrer Security- und Netzwerkanforderungen:
- Konfiguration und Dokumentation
- Einführung von Managementsystemen
- Erkennen und Beseitigen von Anomalien
- Netzwerk Maintenance
- Testen der in Betrieb genommenen Systeme

Ergebnis:
Die Kommunikationsbeziehungen Ihres Netzwerks sind optimiert und erhöhen dessen Performance und Verfügbarkeit.

Wartung und Support

Um die Verfügbarkeit Ihrer Anlage zu gewährleisten, müssen regelmäßig Updates installiert, die Regeln der Firewall angepasst und Meldungen ausgewertet werden.
Wir unterstützen Sie bei
- der Fehlersuche (z. B. fehlerhafte Gerätekonfiguration)
- dem Erkennen von Anomalien
- dem Troubleshooting vor Ort
- dem individuellen Produkt-Support

Ergebnis:
Als Anwender haben Sie einen geringen administrativen Aufwand und erfüllen gleichzeitig die Nachweispflicht zur Umsetzung von Maßnahmen zum Stand der Technik.

Seminare

Informationssicherheit betrifft in Ihrem Unternehmen alle Mitarbeiter.
Wir bieten Ihnen
- Security-Grundlagenschulungen
- Security-Awareness-Schulungen
- Ethernet-Grundlagenschulungen
- Produktschulungen
- individuelle Praxistrainings, zugeschnitten auf Ihre individuellen Anforderungen

Ergebnis:
Durch sicherheits- und verantwortungsbewusstes Handeln können Ausfälle und Schäden in Ihren Anlagen vermieden werden und somit zum Unternehmenserfolg beitragen.

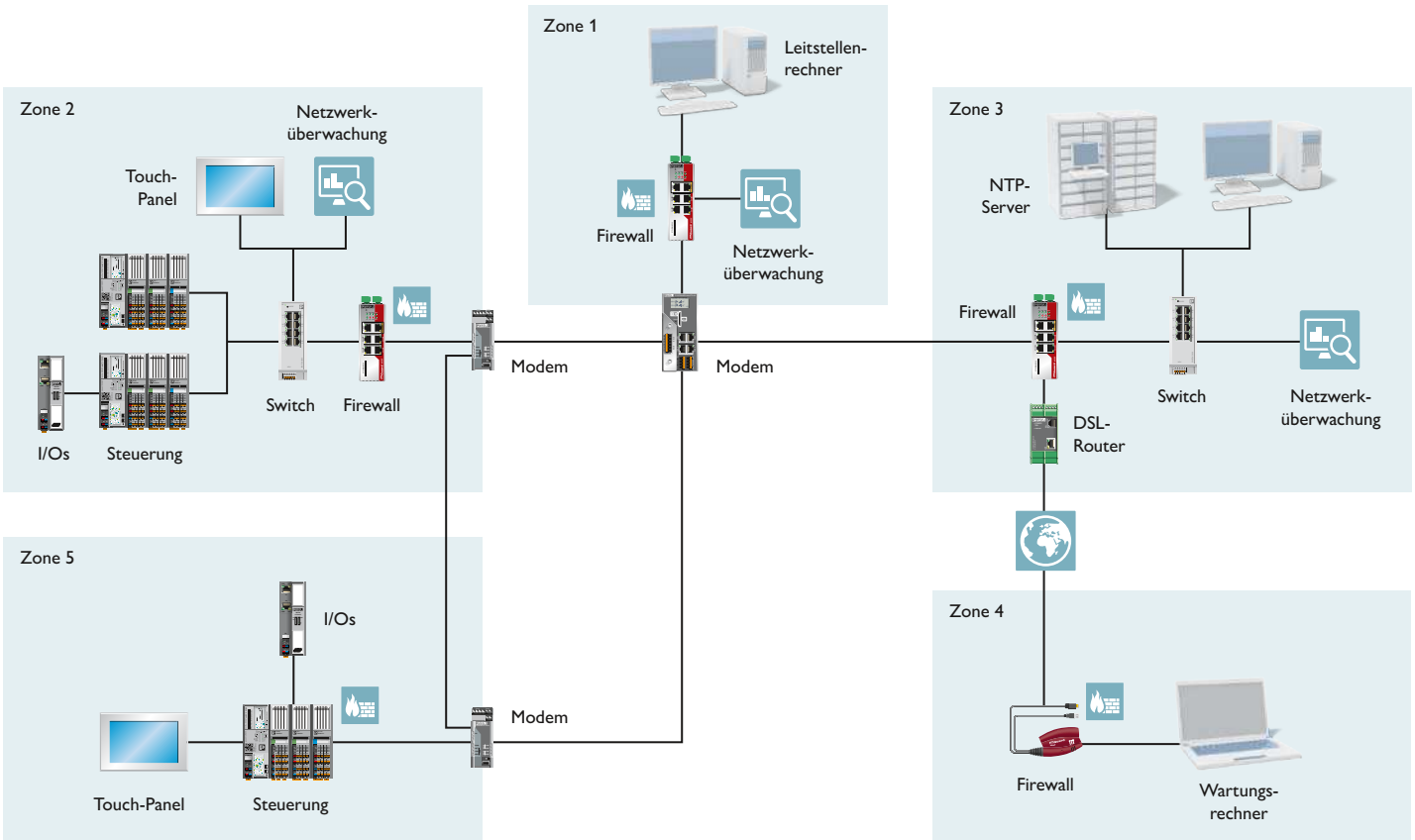
Lösungen

Sichere Automatisierungslösungen

Phoenix Contact verfügt über die Fähigkeiten, sichere Automatisierungslösungen unter Berücksichtigung des internationalen Standards IEC 62443-2-4 zu entwickeln und in Betrieb zu nehmen.
Im Rahmen einer Schutzbedarfsanalyse und den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit entwickeln wir sichere Automatisierungslösungen. Eine Bedrohungsanalyse sowie eine Security Risikoanalyse gehören ebenfalls zum Leistungsangebot.

Security by Design bedeutet für uns:

- Schutzbedarf ermitteln
- Bedrohungs-/Risikoanalyse durchführen
- Entwicklung eines sicheren Netzwerkkonzepts, mit Zonen und Conduits, unter Berücksichtigung der IEC 62442
- Auswahl von sicheren Automatisierungsprodukten
- Dokumentation und Inbetriebnahme der Anlage sowie
- Anlagenbegleitende Dienstleistungen (z. B. Patch-Management) über den Lebenszyklus der Anlage.



Standardisierte Datensicherheit:

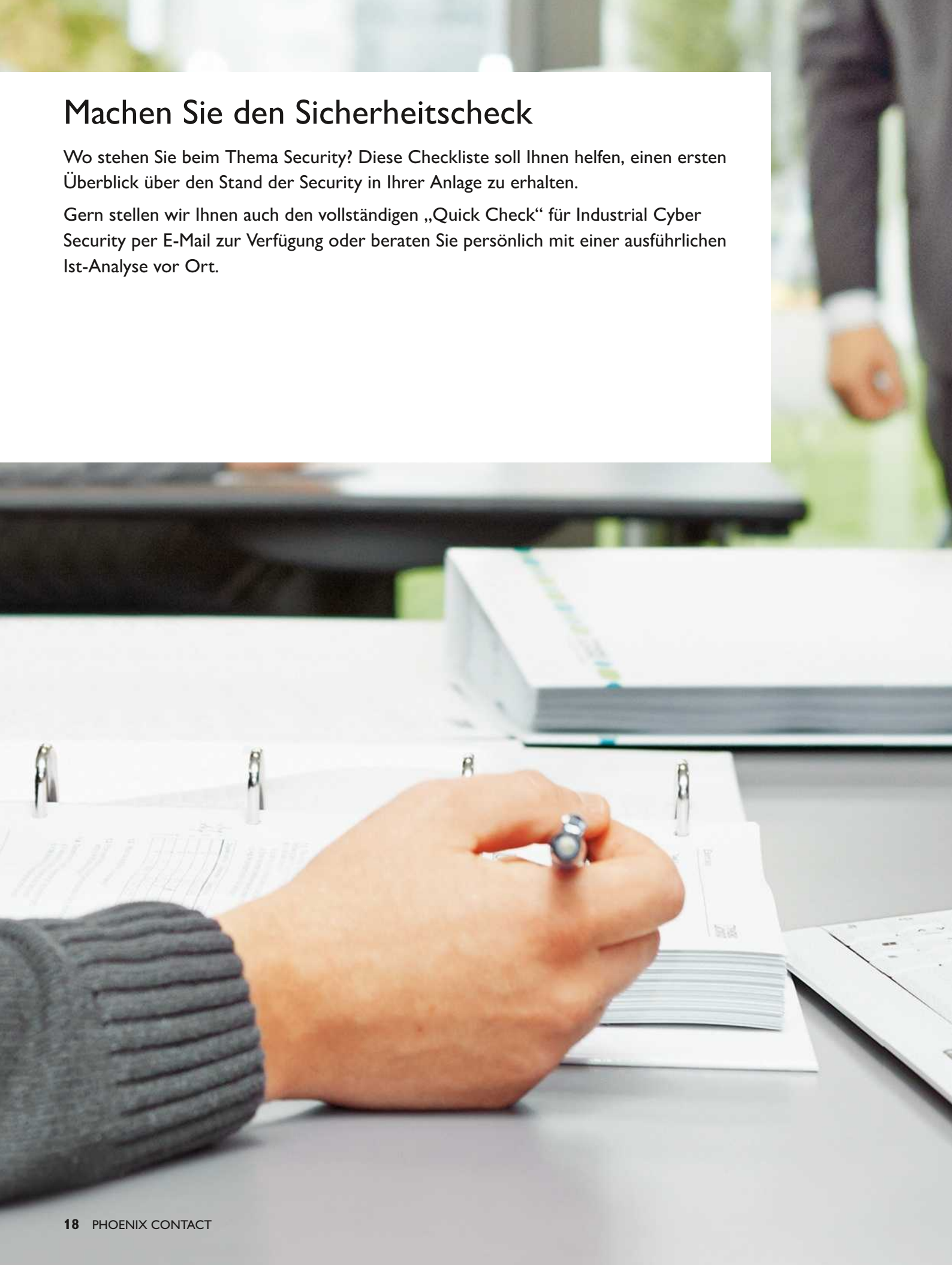
Phoenix Contact unterhält ein Informationssicherheits-Managementsystem („ISMS“), das entsprechend den Anforderungen aus der ISO/IEC 27001 aufgebaut ist. Durch das ISMS wird u. a. der Umgang mit sensiblen Daten und Informationen festgelegt, von der IT-Sicherheit über den Umgang mit sensiblen Daten und Kundendaten bis zur Netzwerksicherheit.

Darüber hinaus ist die Phoenix Contact Energy Automation GmbH, als erstes Unternehmen der Phoenix Contact-Gruppe bereits nach der ISO/IEC 27001 zertifiziert.

Machen Sie den Sicherheitscheck

Wo stehen Sie beim Thema Security? Diese Checkliste soll Ihnen helfen, einen ersten Überblick über den Stand der Security in Ihrer Anlage zu erhalten.

Gern stellen wir Ihnen auch den vollständigen „Quick Check“ für Industrial Cyber Security per E-Mail zur Verfügung oder beraten Sie persönlich mit einer ausführlichen Ist-Analyse vor Ort.



Checkliste

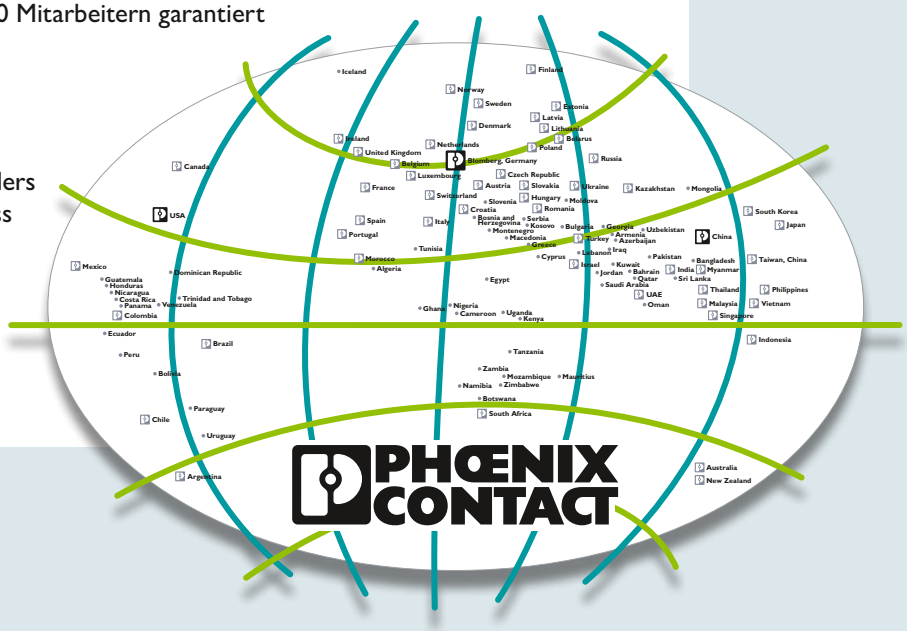
Anforderungen	Ja	Nein	Anmerkungen
Haben alle internen und externen Mitarbeiter eine schriftliche Vertraulichkeitserklärung abgegeben?	☐	☐	
Wurde festgelegt, welche Zutrittsrechte an welche Personen im Rahmen ihrer Funktionen vergeben wurden?	☐	☐	
Werden Passwörter individualisiert und regelmäßig geändert?	☐	☐	
Werden die Mitarbeiter regelmäßig zu Themen der Informationssicherheit geschult bzw. sensibilisiert?	☐	☐	
Ist die private Nutzung dienstlicher Hardware und Software verboten?	☐	☐	
Ist die Einbindung mobiler Datenträger (USB-Sticks, USB-Festplatten u. a.) in IT- oder Automatisierungssysteme in einer Richtlinie dokumentiert und reglementiert?	☐	☐	
Sind Ihre Netzwerke segmentiert?	☐	☐	
Haben Sie Firewalls eingerichtet, die die Datenkommunikation im Netzwerk filtern und Zugriffsrechte regeln?	☐	☐	
Ist der Fernwartungszugang im Normalbetrieb deaktiviert und wird nur im Einzelfall freigeschaltet? Ist diese Anforderung dokumentiert?	☐	☐	
Ist die Kommunikation nach außen verschlüsselt, z. B. über einen VPN-Tunnel?	☐	☐	
Werden Ihre Systeme regelmäßig auf Schwachstellen geprüft und aktualisiert?	☐	☐	
Wissen die Mitarbeiter, was im Fall eines Sicherheitsvorfalls zu tun ist? Gibt es hierzu Richtlinien, in denen beschrieben ist, wie nach einer schwerwiegenden Störung der ordnungsgemäße Betrieb wiederhergestellt werden kann?	☐	☐	

Falls Sie eine oder mehrere Fragen mit Nein beantworten mussten, wenden Sie sich an Phoenix Contact.
Wir beraten Sie gern und unterstützen Sie mit passenden Beratungsdienstleistungen und Produkten.

Weltweit im Dialog mit Kunden und Partnern

Phoenix Contact ist ein weltweit agierender Marktführer mit Unternehmenszentrale in Deutschland. Die Unternehmensgruppe steht für zukunftsweisende Komponenten, Systeme und Lösungen in der Elektrotechnik, Elektronik und Automation. Ein globales Netzwerk in mehr als 100 Ländern mit 17.400 Mitarbeitern garantiert die wichtige Nähe zum Kunden.

Mit einem breitgefächerten und innovativen Produktportfolio bieten wir unseren Kunden zukunftsfähige Lösungen für unterschiedliche Applikationen und Industrien. Das gilt besonders für die Bereiche Energie, Infrastruktur, Prozess und Fabrikautomation.



Unser komplettes Produktprogramm finden Sie unter:

phoenixcontact.de

(D) PHOENIX CONTACT Deutschland GmbH
Flachsmarktstraße 8
32825 Blomberg, Deutschland
Tel.: +49 5235 3-12000
Fax: +49 5235 3-12999
E-Mail: info@phoenixcontact.de
phoenixcontact.de

(A) PHOENIX CONTACT GmbH
Ada-Christen-Gasse 4
1100 Wien, Österreich
Tel.: +43 1 68076
Fax: +43 1 68076-20
E-Mail: info.at@phoenixcontact.com
phoenixcontact.at

(CH) PHOENIX CONTACT AG
Zürcherstrasse 22
8317 Tagelswangen, Schweiz
Tel.: +41 5235 45555
Fax: +41 5235 45699
E-Mail: infoswiss@phoenixcontact.com
phoenixcontact.ch

(L) PHOENIX CONTACT s.à r.l.
10a, z.a.i. Bourmicht
8070 Bertrange, Luxemburg
Tel.: +352 4502 35-1
Fax: +352 4502 38
E-Mail: info@phoenixcontact.lu
phoenixcontact.lu

Printed in Germany

AI 05-19.000.L3
MNR 1101728/2019-03-15/00

INSPIRING INNOVATIONS