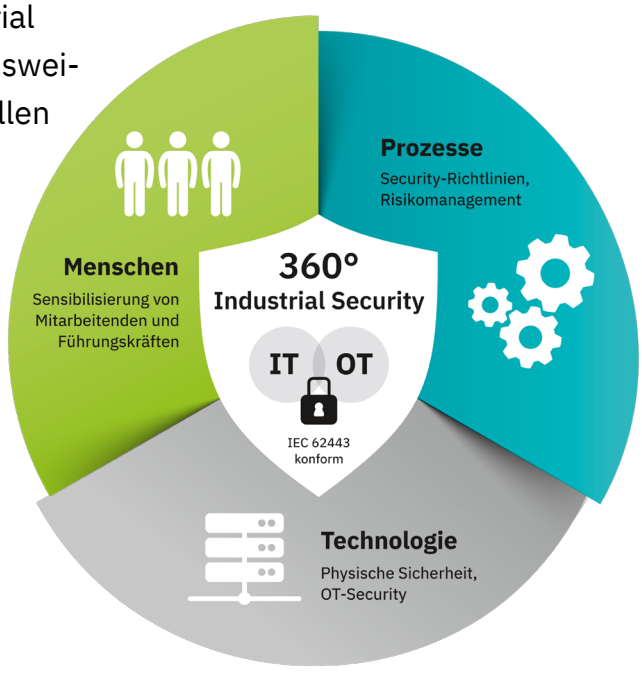
QUICK Check gratis für Informationssicherheit

Wie sicher ist Ihre Anlage?

Verschaffen Sie sich durch unseren Service „QUICK Check gratis“ einen ersten Überblick zum Status der Informationssicherheit in Ihrem Unternehmen – und zwar ganzheitlich auf Basis des 360° Industrial Security-Ansatzes. Neben Fragestellungen zu „Technologie“ werden zusätzlich die zentralen Sicherheitsaspekte „Menschen“ und „Prozesse“ berücksichtigt.

Entscheidend beim Angang des Themas Industrial Security: Nur durch eine ganzheitliche Vorgehensweise kann Ihre Anlage umfassend vor Cyber-Vorfällen gesichert werden.



Anleitung und wichtige Anmerkungen zum QUICK Check

Ermitteln Sie anhand der folgenden Checkliste zu den Handlungsfeldern „Menschen“, „Prozesse“ und „Technologie“ den individuellen Schutzgrad Ihres Unternehmens.

Bewerten Sie bitte objektiv Ihren Informationsverbund und tragen Sie ihn in die Tabelle ein:

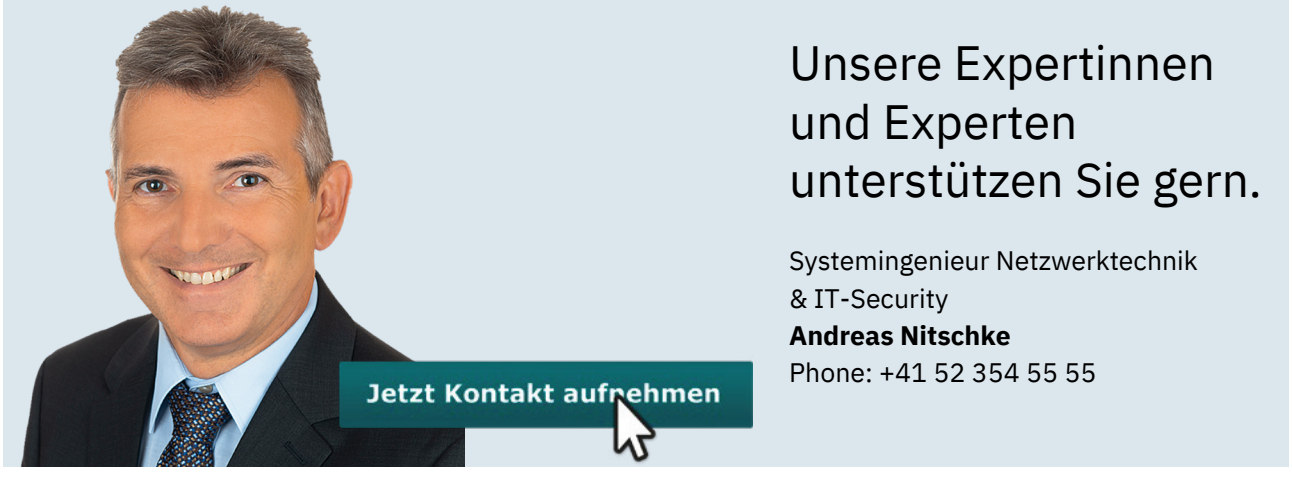
- Ja: Die Umsetzung ist durchgeführt.
- Teilweise: Die Umsetzung ist teilweise durchgeführt oder bereits in Planung.
- Nein: Die Umsetzung ist nicht durchgeführt.

Sollte eine Frage für Sie nicht zutreffen (z. B. eine Frage zum Fernwartungszugang – im Unternehmen existiert ggf. jedoch kein Fernwartungszugang), kreuzen Sie bitte „ja“ an.
Nach der Auswertung des Fragebogens erhalten Sie einen Überblick, wie Sie im Bereich Informationssicherheit aufgestellt sind.

Der QUICK Check kann und darf eine ganzheitliche Betrachtung der Informationssicherheit nicht ersetzen. Sollten Sie alle Fragen mit „ja“ beantworten, ist das noch kein Garant dafür, dass Sie in allen Teilen Ihres Informationsverbundes sicher aufgestellt sind. Er dient vielmehr als Orientierungshilfe für eine strukturierte Vorgehensweise im Bereich der IT-Sicherheit.

Sie benötigen Unterstützung bei der Beantwortung der Fragen?
Oder möchten das Thema Industrial Security für Ihr Unternehmen noch genauer beleuchten?

Sichern Sie sich ein gratis Erstgespräch.



QUICK Check jetzt starten

Zentrale Fragestellungen zum Sicherheitsaspekt **Menschen**

Die sichere Verarbeitung von Informationen ist heutzutage für alle Unternehmen von existenzieller Bedeutung. Informationen existieren sowohl auf Papier, in Datenverarbeitungssystemen oder als Know-how der Mitarbeitenden. Für den Schutz der Informationen reicht es daher nicht aus, nur technische Sicherheitslösungen einzusetzen. Ein angemessenes Sicherheitsniveau kann nur durch eine geplante und strukturierte Vorgehensweise aller Beteiligten erreicht und aufrechterhalten werden.

	Nein	Teilweise	Ja	Punkte
Gibt es eine von der Geschäftsführung verabschiedete Leitlinie zur Informationssicherheit und sind alle Mitarbeitenden darauf hingewiesen worden?	☐ 0	☐ 2	☐ 4	0 ____
Ist eine IT-Sicherheitsbeauftragte oder ein IT-Sicherheitsbeauftragter benannt?	☐ 0	☐ 2	☐ 4	0 ____
Gibt es Seminare und Sensibilisierungskonzepte zur Informationssicherheit?	☐ 0	☐ 2	☐ 4	0 ____
Wissen die Mitarbeitenden, was im Fall eines Sicherheitsvorfalls zu tun ist?	☐ 0	☐ 1	☐ 3	0 ____
Gibt es eine von der Leitungsebene verabschiedete aktuelle Leitlinie zum Notfallmanagement?	☐ 0	☐ 2	☐ 4	0 ____
Werden regelmässig und anlassbezogen Überprüfungen der Notfallmassnahmen durchgeführt?	☐ 0	☐ 2	☐ 4	0 ____
Gibt es hierzu Richtlinien, in denen beschrieben ist, wie nach einer schwerwiegenden Störung der ordnungsgemässe Betrieb wieder hergestellt werden kann?	☐ 0	☐ 2	☐ 4	0 ____
			Punkte Sicherheitsaspekt Menschen	0 ____

Zentrale Fragestellungen zum Sicherheitsaspekt **Prozesse**

Für die Informationssicherheit muss eine geeignete Organisationstruktur im Unternehmen existieren, damit Sicherheitsprozesse erfolgreich geplant, umgesetzt und aufrechterhalten werden können.

	Nein	Teilweise	Ja	Punkte
Existieren in allen Bereichen Vertretungsregelungen?	☐ 0	☐ 1	☐ 2	0 ____
Haben alle internen und externen Mitarbeitenden eine schriftliche Vertraulichkeitserklärung abgegeben?	☐ 0	☐ 1	☐ 2	0 ____
Werden externe Mitarbeitende geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet?	☐ 0	☐ 1	☐ 3	0 ____
Werden betriebsfremde Personen auf dem Betriebsgelände begleitet oder beaufsichtigt?	☐ 0	☐ 2	☐ 4	0 ____
Wurde festgelegt, welche Zutrittsrechte an welche Personen im Rahmen ihrer Funktionen vergeben wurden?	☐ 0	☐ 2	☐ 4	0 ____
Sind diese Zutrittsberechtigungen vollständig dokumentiert und werden diese aktualisiert?	☐ 0	☐ 1	☐ 2	0 ____
Werden Mitarbeitende angewiesen, bei Abwesenheit ihr Büro zu verschliessen oder ihre Arbeitsunterlagen wegzuschliessen?	☐ 0	☐ 1	☐ 2	0 ____
Wird sporadisch überprüft, ob Büros beim Verlassen verschlossen werden?	☐ 0	☐ 1	☐ 2	0 ____
Werden tragbare IT-Systeme außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt?	☐ 0	☐ 1	☐ 2	0 ____
Gibt es eine Richtlinie wie bei Verlust bzw. Diebstahl eines mobilen Gerätes vorgegangen werden muss?	☐ 0	☐ 1	☐ 2	0 ____
Sind zur Entsorgung von schutzbedürftigem Material (Dokumente, Speichermedien usw.) geeignete Entsorgungseinrichtungen wie z. B. Aktenvernichter vorhanden?	☐ 0	☐ 1	☐ 2	0 ____

Fortsetzung auf nächster Seite →

Fortsetzung:
Zentrale Fragestellungen zum Sicherheitsaspekt **Prozesse**

	Nein	Teilweise	Ja	Punkte
Werden die Mitarbeitenden regelmäßig zu Themen der Informationssicherheit geschult bzw. sensibilisiert?	☐ 0	☐ 2	☐ 4	0 ____
Werden die Mitarbeitenden regelmässig für die Belange des Datenschutzes sensibilisiert?	☐ 0	☐ 2	☐ 4	0 ____
Werden Mitarbeitende, die eine Aufgabe neu übernehmen sollen, ausreichend geschult?	☐ 0	☐ 1	☐ 2	0 ____
Ist die private und zugleich berufliche Nutzung von Hardware und Software untersagt?	☐ 0	☐ 1	☐ 3	0 ____
			Punkte Sicherheitsaspekt Prozesse	0 ____

Zentrale Fragestellungen zum Sicherheitsaspekt **Technologie**

Vernetzte IT-Systeme sind heute für die Realisierung von Geschäftsprozessen eine technische Grundlage und daher kaum entbehrlich. Die auf ihnen verarbeiteten und gespeicherten Informationen stellen einen wesentlichen Wert für das Unternehmen dar und müssen angemessen geschützt werden.

	Nein	Teilweise	Ja	Punkte
Gibt es ein Schutzkonzept, wie IT-Systeme abgesichert werden müssen?	☐ 0	☐ 1	☐ 3	0 ____
Existieren dokumentierte Richtlinien für Hard- und Software?	☐ 0	☐ 1	☐ 2	0 ____
Ist die Nutzung von nicht freigegebener Hard- und Software geregelt und dokumentiert und sind alle Mitarbeitenden darüber informiert?	☐ 0	☐ 1	☐ 3	0 ____
Ist sichergestellt, dass nur berechtige Personen auf Anwendungen und IT-Systeme zugreifen können? (Vergabe von Zugriffsrechten)	☐ 0	☐ 1	☐ 3	0 ____
Werden nur die Zugriffsrechte vergeben, die für die jeweiligen Aufgaben erforderlich sind?	☐ 0	☐ 1	☐ 3	0 ____
Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?	☐ 0	☐ 1	☐ 3	0 ____
Sind die Benutzenden angewiesen, dem Schutzbedarf angemessene Passwörter mit ausreichender Komplexität zu verwenden?	☐ 0	☐ 2	☐ 4	0 ____
Sind die Benutzenden angewiesen, ihr Passwort geheim zu halten?	☐ 0		☐ 2	0 ____
Wird regelmäßig überprüft, ob die Vorgaben zur Passwortkomplexität noch dem Stand der Technik entsprechen?	☐ 0	☐ 1	☐ 3	0 ____
Ist der Datentransport über mobile Datenträger zwischen IT-Systemen, die nicht miteinander vernetzt sind, gemäss Unternehmensrichtlinie geregelt?	☐ 0	☐ 1	☐ 2	0 ____
Ist die Einbindung mobiler Datenträger (USB-Sticks, USB-Festplatten u. a.) in IT- oder Automatisierungssysteme in einer Richtlinie dokumentiert und reglementiert?	☐ 0	☐ 2	☐ 4	0 ____
Ist der Einsatz mobiler Datenträger gemäß Unternehmensrichtlinie nicht zulässig, sind Vorkehrungen getroffen, die das Anschließen von mobilen Datenträgern direkt an Rechner des Automatisierungssystems unterbinden?	☐ 0	☐ 2	☐ 4	0 ____

Fortsetzung auf nächster Seite →

Fortsetzung:
Zentrale Fragestellungen zum Sicherheitsaspekt **Technologie**

	Nein	Teilweise	Ja	Punkte
Existiert ein Prozess, nach dem kritische Systemaktualisierungen in der Automatisierungsanlage getestet, freigegeben und eingebracht werden? Ist dieser Prozess dokumentiert und erprobt?	☐ 0	☐ 2	☐ 4	0
Wird der Status von IT- bzw. Automatisierungssystemen von einem System zur Anomalieerkennung erfasst?	☐ 0	☐ 1	☐ 2	0
Werden bei Komponenten des Automatisierungssystems die Standardpasswörter auf individuelle Passwörter abgeändert und ist dieses Vorgehen in einer Richtlinie dokumentiert?	☐ 0	☐ 1	☐ 3	0
Sind wichtige IT-Systeme, wie z. B. Server oder Netzwerkverteiler in Räumen mit Zutrittsbeschränkung untergebracht?	☐ 0	☐ 1	☐ 3	0
Wird eine regelmäßige Datensicherung der wichtigsten Unternehmensdaten durchgeführt?	☐ 0	☐ 2	☐ 4	0
Sind Viren-Schutzprogramme auf allen IT-Systemen installiert, auf denen dies laut Sicherheitskonzept vorgesehen ist?	☐ 0	☐ 1	☐ 3	0
Wird sichergestellt, dass sowohl Scan-Programme als auch Signaturen stets auf dem aktuellsten Stand sind?	☐ 0	☐ 1	☐ 3	0
Werden heruntergeladene Dateien mit einem Viren-Schutzprogramm geprüft, bevor sie geöffnet bzw. gestartet werden?	☐ 0	☐ 1	☐ 3	0
Ist der Fernwartungszugang im Normalbetrieb deaktiviert, wird dieser nur im Einzelfall freigeschaltet und ist diese Anforderung dokumentiert?	☐ 0	☐ 1	☐ 3	0
Entsprechen bei verwendetem WLAN die eingesetzten Passwörter und Verschlüsselungsalgorithmen dem Stand der Technik?	☐ 0	☐ 1	☐ 3	0
			Punkte Sicherheitsaspekt Technologie	0
			Gesamtpunkte	0

Auswertung

Basierend auf Ihrer Einschätzung und der hier erzielten Gesamtsumme lässt sich bei einer Selbstauswertung nur eine sehr grobe Einschätzung zum Erfüllungsgrad Ihrer IT-Sicherheit treffen.

Leiten Sie den Fragebogen für eine kostenlose Auswertung an unsere E-Mail-Adresse: anitschke@phoenixcontact.com weiter. Sie erhalten anschließend eine detaillierte Rückmeldung zu Ihrem IT-Sicherheitsniveau, aus der Sie erste Massnahmen ableiten können.

Unabhängig vom erzielten Ergebnis beraten und unterstützen wir Sie vertrauensvoll, umfassend und kompetent bei der Einführung und Umsetzung von IT-Sicherheitsstandards im industriellen Umfeld.

Im jeweiligen Feld ist eine Punktzahl angegeben. Übertragen Sie diese in die Spalte „Punkte“ und addieren Sie die erzielten Punktzahlen. Anhand der Summe lassen sich folgende pauschale Aussagen Ihres aktuellen Standes ableiten:

- Haben Sie weniger als 70 Punkte erzielt, besteht akuter Handlungsbedarf. Werden Sie hier umgehend aktiv und informieren Sie sich zum Thema Informationssicherheit.
- Liegt Ihr Ergebnis zwischen 70 bis 120 Punkten, kann davon ausgegangen werden, dass bereits ein Ansatz der Informationssicherheit Anwendung findet. Hier besteht aber voraussichtlich in einigen Bereichen erhebliches Verbesserungspotenzial. Auch hier sollten Sie sich zu aktuellen IT-Sicherheitsstandards im industriellen Umfeld informieren.
- Bei einem Ergebnis über 120 Punkte lässt sich erkennen, dass Ihr Unternehmen bereits verantwortungsvoll mit dem Thema IT-Sicherheit umgeht. Dies bedeutet jedoch keinesfalls einen verlässlichen Schutz gegen Cyber-Angriffe. Sie sollten den Weg zu einem systematischen und ganzheitlichen Ansatz wie IT-Grundschutz, ISO/IEC 27001 oder IEC 62443 verfolgen.

Sollten Sie noch Fragen zu unserem QUICK Check oder zum Themengebiet IT-Sicherheit im industriellen Umfeld haben, stehen wir Ihnen gern als kompetenter Ansprechpartner zur Verfügung.

Tipp

STARTER-Workshop –
Starten Sie schnell, professionell und zukunftsorientiert durch mit Co-Pilot

Zentrale Fragestellungen gleich beim Start vollständig einkreisen und richtig angehen.

STARTER Workshop – 360° Industrial Security

Jetzt mehr erfahren

Tipp

Know more –
Zentrales Industrial Security-Wissen für jedes Level

Whitepaper, Webinare, Infographiken: zentrales Security-Wissen für Sie kompakt zusammengefasst.

Alle Themen im Überblick

Bleiben Sie immer up-to-date!
News, Trends und Handlungsempfehlungen – topaktuelles Industrial-Security-Wissen direkt von unseren Expertinnen und Experten

Folgen Sie uns auf den Industrial-Security-Kanälen von Phoenix Contact.

Industrial-Security-Newsletter:
Jetzt registrieren

Industrial-Security-LinkedIn-Kanal:
Jetzt folgen

Sichern Sie sich ein Gratis-Erstgespräch

Unsere Expertinnen und Experten unterstützen Sie gern.

Systemingenieur Netzwerktechnik & IT-Security
Andreas Nitschke
Phone: +41 52 354 55 55

phoenixcontact.ch