100 Jahre Leidenschaft für Technologie und Innovation

Willkommen

OT-Security – Warum muss meine WEA gegen Cyber-Angriffe schützen?

Torsten Gast
PHOENIX CONTACT Deutschland GmbH

09. November 2023
Spreewindtage

PHOENIX CONTACT

Unternehmensvorstellung

PHOENIX CONTACT GmbH & Co KG

Partner für produktunabhängige Dienstleistungen für die Sicherheit in der Industrie

11
Produktionsstandorte
Deutschland | China | Taiwan | Indien | Polen | Schweden | Schweiz | Türkei | Argentinien | Griechenland | USA

100.000
Produkte

75%
Umsatz im Ausland

25%
Umsatz in Deutschland

22.000
Mitarbeitende Weltweit

10.200
Mitarbeitende Deutschland

1923
Gründung in Deutschland

HEUTE
In über 100 Ländern vertreten

Group Executive Board:
Frank Stührenberg (CEO)
Axel Wachholz (CFO)
Frank Possel-Dölken (CDO)
Dirk Görlitzer (COO, President BA ICE)
Torsten Jaroschek (COO, President BA DC)
Ulrich Leidecker (COO, President BA IMA)

Phoenix Contact ist ein **1923** gegründetes Unternehmen in **Privatbesitz** mit **hoher Wertschöpfungstiefe** und **unabhängig** in seiner **unternehmerischen Entscheidungsfreiheit**.

Torsten Gast

PHOENIX CONTACT Deutschland GmbH

Industry Management and Automation

Director Competence Center Services

Dringenauer Str. 30

31812 Bad Pyrmont

Mobil: 0049 173 2592 411

Email: torsten.gast@phoenixcontact.de

LinkedIn: linkedin.com/in/torsten-gast-8441827a

Hinweis: Urheberrechtsschutz und Disclaimer

Die Informationen und Beispiele dieser Präsentation dienen als Hilfestellung zur Umsetzung der Richtlinien und Normen. Sie erheben keinerlei Anspruch auf Rechtsverbindlichkeit und Vollständigkeit. PHOENIX CONTACT übernehmen keinerlei Haftung für etwaige Fehler, die in den Seminaren mündlich oder schriftlich übermittelt werden oder in den Unterlagen enthalten sind.

Agenda

- Warm up
- Gesetzliche Anforderungen
- Gefahren in der Digitalen-Welt
- Was ist das Defense of Depth Konzept?
- IEC 62443 in der Praxis
- Zusammenfassung

Warm up

Die Unterschiede zwischen IT & OT

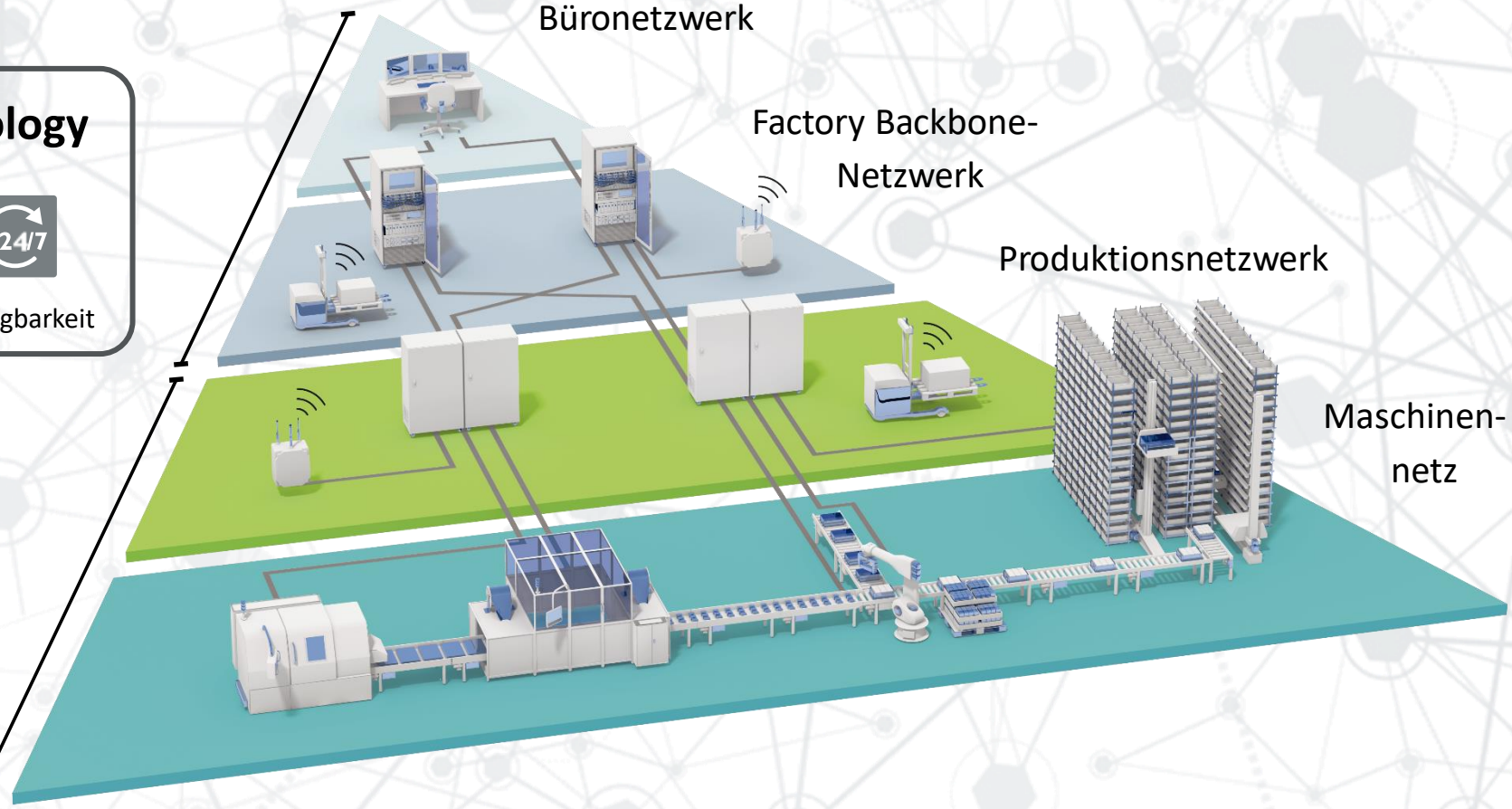
Information Technology

Vertraulichkeit | Integrität | Verfügbarkeit

≠

Operation Technology

Verfügbarkeit | Integrität | Vertraulichkeit



Warm up

OT-Security vs. IT Security

Unterschiedliche Prioritäten der Schutzziele

Verfügbarkeit
Integrität
Vertraulichkeit

OT-Security

Eigenschaften		
Ausfall nicht tolerierbar	**Verfügbarkeit**	Kurzzeitige Unterbrechungen tolerierbar
Systemspezifische Verkabelung Montage im Feld Komponenten in Industriequalität Ersatzteilverfügbarkeit: 10-20 Jahre Linien und Ring Topologien	**Installation**	Fest verlegte Verkabelung Vorkonfigurierte Leitungen Büro Komponenten Einsatzzeit: max. 5 Jahre Stern und Baum Topologien
Kleine Datenpakete Zyklische Datenkommunikation Echtzeit Höchste Netzwerkverfügbarkeit	**Echtzeit**	Große Datenpakete Azyklische Datenkommunikation Keine Echtzeit Hohe Netzwerkverfügbarkeit
Hohe Umgebungstemperaturen Staub, Luftfeuchtigkeit, Vibration Hohe EMV Belastung	**Umgebung**	Normale Umgebungstemperaturen Normales Umgebungsumfeld Niedrige EMV Belastung
Aufwendige Tests auf Interoperabilität	**Patch Management**	Automatisierter Patch Prozess
Schwierig Nur in Wartungsfenstern möglich	**Neustart**	möglich

Vertraulichkeit
Integrität
Verfügbarkeit

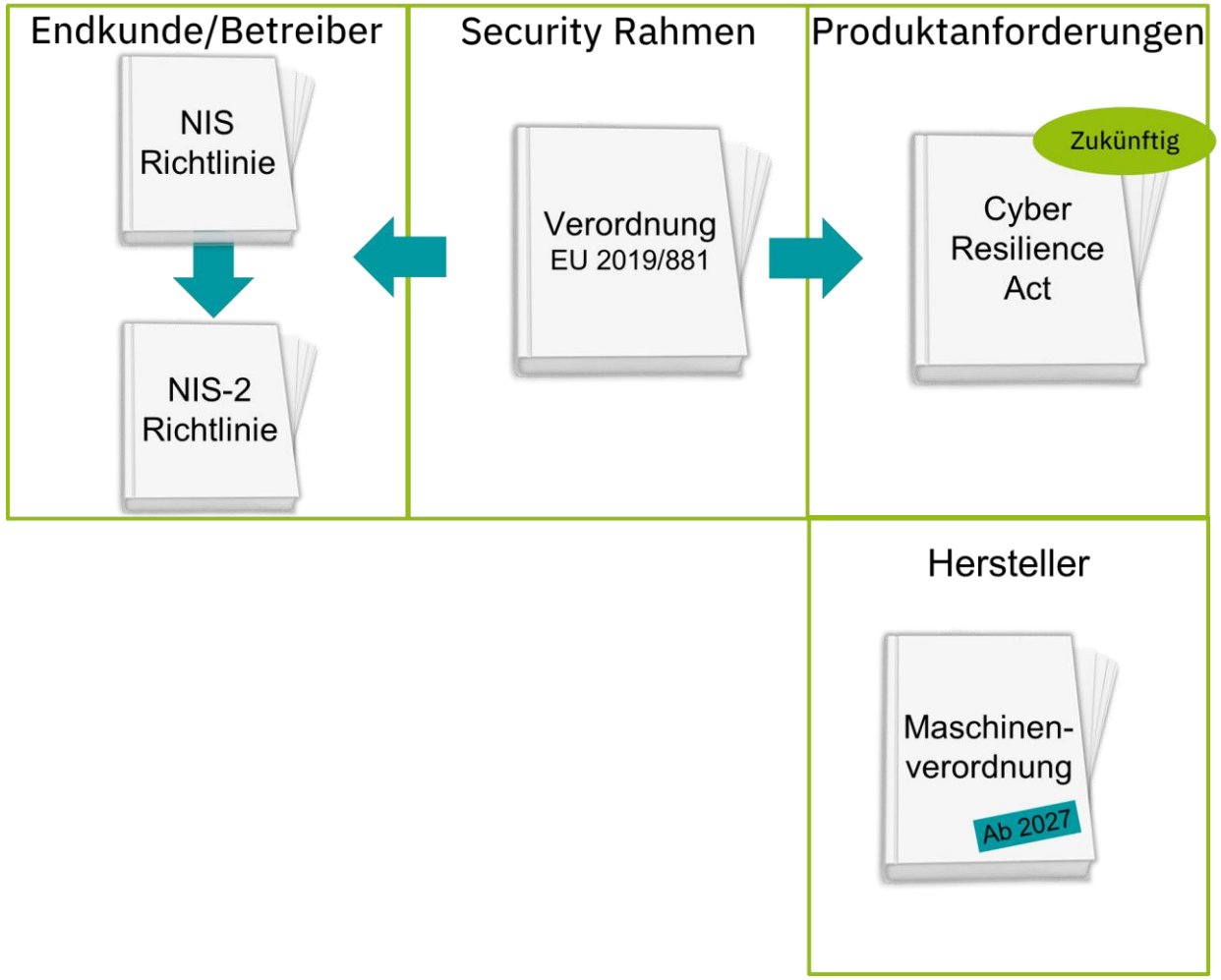
IT-Security

Agenda

- Warm up
- Gesetzliche Anforderungen
- Gefahren in der Digitalen-Welt
- Was ist das Defense of Depth Konzept?
- IEC 62443 in der Praxis
- Zusammenfassung

Gesetzliche Übersicht

- EU-Kommission sieht vermehrt die Notwendigkeit, dass Anforderungen an die Cybersicherheit gesetzlich geregelt werden müssen.
- Neben der Vergrößerung des Anwenderkreises im Bereich der kritischen Infrastruktur, werden zukünftig auch wichtige Unternehmen von der Regierung benannt, die auch die Anforderungen an die Cybersicherheit erfüllen müssen.
- Anforderungen an alle Netzwerkfähigen Produkte stellt zukünftig der CRA.
- Richtlinien und Verordnungen gibt es aber auch für spezielle Produktegruppen (z.B. Funkanlagenrichtlinie).



EU NIS 2 Directive

Network and Information Security Directive

Grundanforderungen und Zeitplan

- Die EU-Mitgliedstaaten sind **verpflichtet**, nationale Cybersicherheitsstrategien zu verabschieden:
  - zuständige Behörden und Cyber-Krisenmanagement-Behörden müssen benannt werden
  - Reaktionsteams für Computer-Sicherheitsvorfälle (CSIRTs) müssen aufgestellt werden;
- Festlegung von Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit und Meldepflichten
- Regeln und Verpflichtungen zum Austausch von Cybersicherheitsinformationen
- Aufsichts- und Durchsetzungspflichten der Mitgliedstaaten.
- Zeitplan:
  - Veröffentlichung des endgültigen Textes erfolgte am 16. Januar 2023
  - Nationale Gesetze müssen am **18. Oktober 2024** verfügbar sein
  - Nationale Stellen müssen bis zum 17. April 2025 identifiziert werden
  - 1,5-2 Jahre nationale Übergangsphase bis **zum Inkrafttreten (2026/2027)**

Wer ist von NIS 2 betroffen?

- Die NIS 2 konzentrieren sich auf ***Betreiber öffentlicher*** oder ***privater Einrichtungen***, die mehr als **50 Mitarbeiter** beschäftigen und einen Umsatz von 10 Millionen Euro erzielen.
- Die EU-Mitgliedsstaaten müssen bis zum **17. April 2025** eine Liste der Unternehmen vorlegen, die zu den **wesentlichen** und **wichtigen** Einrichtungen gehören.
- **Wesentliche** Unternehmen sind in kritischen Infrastrukturen tätig:
  - Strom-/Gas-/Wasserstofferzeugung, -speicherung und -übertragung,
  - Transport auf Wasser/Straße/Schiene,
  - Trinkwasser/Abwasser
  - digitale Infrastruktur.
- **Wichtige** Unternehmen werden aus einer Liste von 7 Sektoren auf der Grundlage ihrer Kritikalität für ihren Wirtschaftszweig und die Art der Dienstleistung ausgewählt, z. B:
  - Herstellung, Produktion und Vertrieb von Lebensmitteln und Chemikalien
  - Herstellung von elektrischen Geräten/Maschinen/Fahrzeugen.

Maßnahmen zum Risikomanagement der Cybersicherheit

- Festlegung geeigneter **technischer, betrieblicher** und **organisatorischer Maßnahmen** zur Bewältigung von Risiken für die Sicherheit von Netz- und Informationssystemen.
- Alle Bedrohungen müssen durch folgende Maßnahmen geschützt werden, z.B.:
  - Risikoanalyse und Sicherheitsrichtlinien.
  - Behandlung von Zwischenfällen, Umgang mit Schwachstellen und deren Offenlegung
  - Geschäftskontinuität, z. B. Backup-Management und Notfallwiederherstellung sowie Krisenmanagement.
  - Sicherheit bei der Beschaffung, Entwicklung und Wartung
  - Richtlinien und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen zum Management von Cybersicherheitsrisiken.
  - Richtlinien und Verfahren für den Einsatz von Kryptographie und Verschlüsselung

Cybersicherheit Meldepflichten und Überwachung

- **Bedeutende Sicherheitsvorfälle** müssen dem nationalen CSIRT **gemeldet werden**:
  - 24 Stunden: Frühwarnung muss übermittelt werden
  - 72 Stunden: Informationen über Schweregrad, Auswirkungen und Indikatoren für eine Gefährdung
  - 1 Monat: Abschlussbericht mit einer detaillierten Beschreibung des Vorfalls, seines Schweregrads, seiner Auswirkungen, der Art der Bedrohung und der Abhilfemaßnahmen
- **Die oberste Führungsebene** wird für die Umsetzung der Risikomanagementmaßnahmen verantwortlich gemacht.
- Die nationalen Behörden überwachen die in der NIS 2 festgelegten Maßnahmen und setzen sie durch.
- Geldbußen von 7 Mio. EUR oder 1,4% (wichtige Unternehmen) bis 10 Mio. EUR 2% (wesentlichen und wichtigen Einrichtungen) des gesamten weltweiten Jahresumsatzes im vorangegangenen Steuerjahr.
- Für die sichere Gestaltung von Produkten und Systemen sind Normen erforderlich.

EU CRA

Cyber Resilience Act

Gesetzliche Anforderungen - CRA

DER Cyber Resilience Act

DAS GESETZ WIRD:

- sicherstellen, dass in der EU in Verkehr **gebrachte Produkte mit digitalen Elementen** von vornherein weniger Schwachstellen aufweisen und dass **die Hersteller** über den **gesamten Lebenszyklus** ihrer Produkte für die **Cybersicherheit verantwortlich** bleiben.
- für eine größere **Transparenz** in Bezug auf die Sicherheit von Hardware- und Softwareprodukten sorgen.
- dafür sorgen, dass gewerbliche Nutzer und Verbraucher einen besseren Schutz genießen.

Mit dem Gesetz über Cyber-Resilienz werden verbindliche Cybersicherheitsanforderungen für Hardware- und Softwareprodukte für deren gesamten Lebenszyklus eingeführt.

Gesetzliche Anforderungen - CRA

Zeitrahmen

2024?

Das Europäische Parlament und der Rat prüfen das vorgeschlagene Gesetz über Cyberresilienz.

?

Nach der Verabschiedung haben Wirtschafts-teilnehmer und Mitgliedstaaten zwei Jahre Zeit, um sich auf die neuen Anforderungen einzustellen. Die Meldepflicht für aktiv ausgenutzte Schwachstellen und Vorfälle wird schon nach einem Jahr gelten.

x+2

Die Kommission wird das Gesetz über Cyberresilienz regel-mäßig überprüfen und über seine Funktions-weise Bericht erstatten.

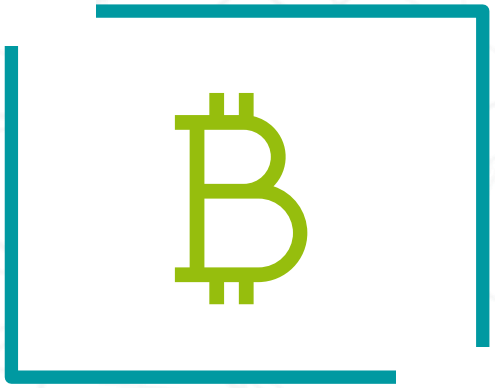
Agenda

- Warm up
- Gesetzliche Anforderungen
- Gefahren in der Digitalen-Welt
- Was ist das Defense of Depth Konzept?
- IEC 62443 in der Praxis
- Zusammenfassung

Gefahren in der Digitalen-Welt

Bedrohungslage

Alle 11 Sekunden findet in der EU eine **Ransomware Attacke** statt



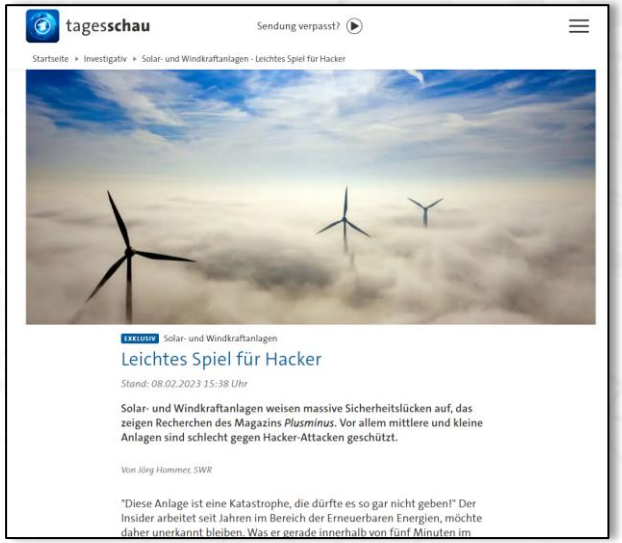
Die Kosten für Ransomware Attacken beziffern sich auf ungefähr **20 Milliarden Euro** in 2021

Die weltweiten jährlichen Kosten der Cyberkriminalität wurden für das Jahr 2021 auf 5,5 Billionen EUR geschätzt.

Quelle: Gesetz über Cyberresilienz – Factsheet

Gefahren in der Digitalen-Welt

Bedrohungslage



tagesschau

Sendung verpasst?

Startseite ▸ Investigativ ▸ Solar- und Windkraftanlagen - Leichtes Spiel für Hacker

EXKLUSIV Solar- und Windkraftanlagen

Leichtes Spiel für Hacker

Stand: 08.02.2023 15:38 Uhr

Solar- und Windkraftanlagen weisen massive Sicherheitslücken auf, das zeigen Recherchen des Magazins *Plusminus*. Vor allem mittlere und kleine Anlagen sind schlecht gegen Hacker-Attacken geschützt.

Von Jörg Hommer, SWR

"Diese Anlage ist eine Katastrophe, die dürfte es so gar nicht geben!" Der Insider arbeitet seit Jahren im Bereich der Erneuerbaren Energien, möchte daher unerkannt bleiben. Was er gerade innerhalb von fünf Minuten im

Quelle: Solar- und Windkraftanlagen - Leichtes Spiel für Hacker | tagesschau.de

NORDEX

Hackerangriff bei Windturbinenhersteller Nordex

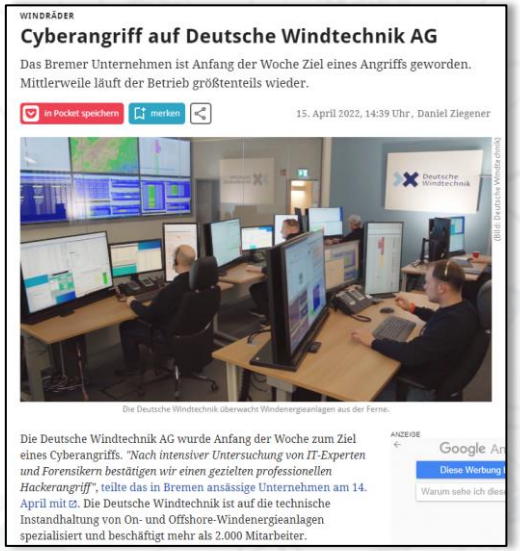
Stand: 04.04.2022 18:59 Uhr

Der Windkraftanlagenbauer Nordex mit Sitz in Hamburg und Rostock ist zum Ziel einer Cyberattacke geworden. Vorsorglich seien die IT-Systeme mehrerer Geschäftsbereiche an verschiedenen Standorten abgeschaltet worden.

Nach dem Hackerangriff auf die Nordex Group gibt es noch immer Probleme am Rostocker Standort der Firma. Das Unternehmen ist weiterhin nicht erreichbar. Außerdem wird nach Informationen des NDR an dem Standort offenbar nicht gearbeitet. Die Mitarbeiterinnen und Mitarbeiter seien für viele Arbeiten auf die IT-Systeme angewiesen. Nordex hat nach dem Hackerangriff nach NDR Recherchen bei der Staatsanwaltschaft Hamburg Anzeige erstattet. Netzbetreiber berichten derweil, dass die Windkraftanlagen von Nordex weiter laufen und Strom ins Netz einspeisen.

Unternehmen bemerkte Angriff am Wochenende

Quelle: Hackerangriff bei Windturbinenhersteller Nordex | NDR.de - Nachrichten - Mecklenburg-Vorpommern



WINDRÄDER

Cyberangriff auf Deutsche Windtechnik AG

Das Bremer Unternehmen ist Anfang der Woche Ziel eines Angriffs geworden. Mittlerweile läuft der Betrieb größtenteils wieder.

in Pocket speichern | merken

15. April 2022, 14:39 Uhr, Daniel Ziegener

Die Deutsche Windtechnik überwacht Windenergieanlagen aus der Ferne.

Die Deutsche Windtechnik AG wurde Anfang der Woche zum Ziel eines Cyberangriffs. *"Nach intensiver Untersuchung von IT-Experten und Forensikern bestätigen wir einen gezielten professionellen Hackerangriff"*, teilte das in Bremen ansässige Unternehmen am 14. April mit. Die Deutsche Windtechnik ist auf die technische Instandhaltung von On- und Offshore-Windenergieanlagen spezialisiert und beschäftigt mehr als 2.000 Mitarbeiter.

ANZEIGE

Google Ar

Diese Werbung

Warum sehe ich dies

Quelle: Windräder: Cyberangriff auf Deutsche Windtechnik AG - Golem.de

Nach Cyberangriff: Störung bei Windkraft-Fernwartung behoben

Stand: 29.04.2022 17:48 Uhr

Die Fernwartung Tausender Windräder in Europa war seit dem 24. Februar infolge eines mutmaßlichen Cyberangriffs gestört. Jetzt funktioniert sie laut Hersteller Enercon in Aurich wieder weitgehend.

Rund 95 Prozent der 1.281 betroffenen Windparks sind nach Angaben eines Enercon-Sprechers wieder an die Satellitenkommunikation angebunden. Dies soll in Kürze auch mit den noch verbliebenen 64 Windparks geschehen.

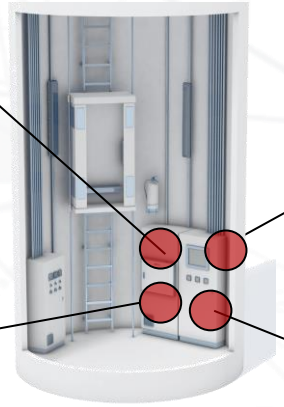
Fernüberwachung von 5.800 Windkraftanlagen gestört

Quelle: Nach Cyberangriff: Störung bei Windkraft-Fernwartung behoben | NDR.de - Nachrichten - Niedersachsen

Gefahren in der Digitalen-Welt

Bedrohungslage

Mitarbeiter laden private Geräte an SPS



Keine Backups vorhanden

Dauerhafte Remotezugänge

Keine geregelten Prozesse (z.B. Patchmanagement)

Fehlendes Monitoring

Flache Netzhierarchie

Sensible Informationen werden unverschlüsselt übertragen

Agenda

- Warm up
- Gesetzliche Anforderungen
- Gefahren in der Digitalen-Welt
- Was ist das Defense of Depth Konzept?
- IEC 62443 in der Praxis
- Zusammenfassung

Was ist das Defense of Depth Konzept?

Gesetzlicher & Normativer Rahmen

Regulatorien erfüllen
Beschreiben was getan werden muss

IT-Sicherheitsgesetz (2.0)

Bundesministerium des Innern

- **Meldepflicht** für Zwischenfälle
- Betreiber von kritischen Infrastrukturen müssen ein **ISMS** aufbauen und zertifizieren lassen
- Erfüllung von technischen Mindestanforderungen

EU NIS 2.0

Definiert Anforderungen für Betreiber kritischer Infrastrukturen + „important Entities“
ab 50 MA
-> Schwellwerte entfallen!

Empfehlungen beachten
Beschreiben was getan werden sollte

Bundesamt für Sicherheit in der Informationstechnik

BSI IT-Grundschutz-kompendium/ B3S
(Betreiber/Gerätehersteller)

Standards entsprechen
Beschreiben wie es umgesetzt werden sollte

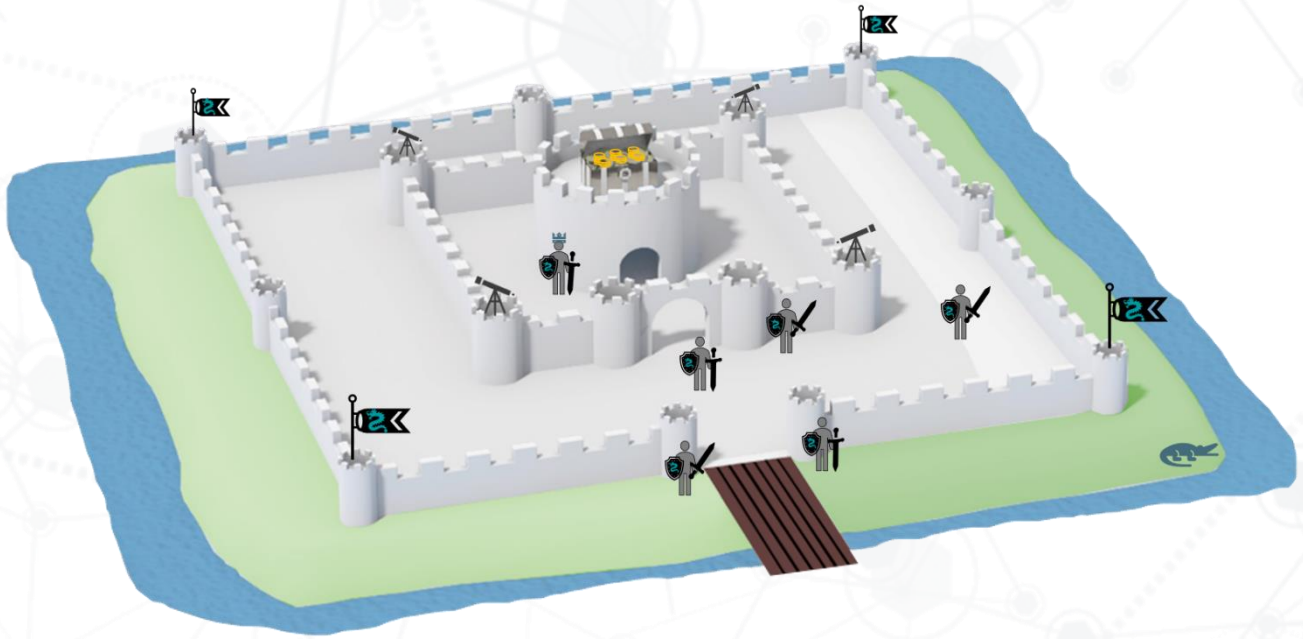
IEC 62443 IT-Sicherheit für industrielle Automatisierungssysteme
(Fokus: Betreiber, Integratoren & Gerätehersteller)

ISO/IEC 2700X Sicherheitsmanagement
(Fokus: Betreiber)

ISMS Informations-**S**icherheits-**M**anagement-**S**ystem

Was ist das Defense of Depth Konzept?

Das „Defense in Depth“ Konzept



Was ist das Defense of Depth Konzept?

Aufbau der IEC 62442

Allgemein	Richtlinien und Verfahren	System	Komponente
1-1 Technologie, Konzepte und Modelle	2-1 Anforderungen an ein IACS-Sicherheitsmanagementsystem	3-1 Sicherheitstechnologien für IACS (TR)	4-1 Sicherer Lebenszyklus der Produktentwicklung
1-2 Master-Glossar der Begriffe und Abkürzungen	2-2 Sicherheitsschutzbewertung	3-2 Sicherheitsrisikobewertung und Systemdesign	4-2 Technische Sicherheitsanforderungen für IACS-Produkte
1-3 Kennzahlen zur Einhaltung der Systemsicherheit	2-3 Patch-Management im IACS-Umfeld (TR)	3-3 Systemsicherheits-anforderungen und Sicherheitsstufen	
1-4 Systemsicherheits-lebenszyklus und Einsatzgebiet	2-4 Anforderungen an IACS-Lösungsanbieter		
	2-5 Implementierungsanleitung für IACS Asset Owner		
Definitionen Metriken	Sicherheitsanforderungen an Anlagenbesitzer und Lieferanten	Sicherheitsanforderungen an ein sicheres System	Sicherheitsanforderungen für sichere Komponenten

Funktionale Anforderungen

Prozessanforderungen

Betreiber

Integrator

Hersteller

Was ist das Defense of Depth Konzept?

Security Level – die Security „Quantifizierung“ der 62443

Schütz vor:	
SL-0	Kein Schutz
SL-1	Durchschnittlichen Internet-Nutzern
SL-2	Interessierten Einzelpersonen und Firmen mit allgemeinen Security-Kenntnissen
SL-3	Experten und Firmen, die mit klaren Zielen effektive, jedoch kostenorientierte Angriffsszenarien entwickeln und einsetzen
SL-4	Staatlichen Organisationen, bei denen die Erreichung des spezifisch ausgewählten Angriffsziels um fast jeden Preis im Vordergrund steht

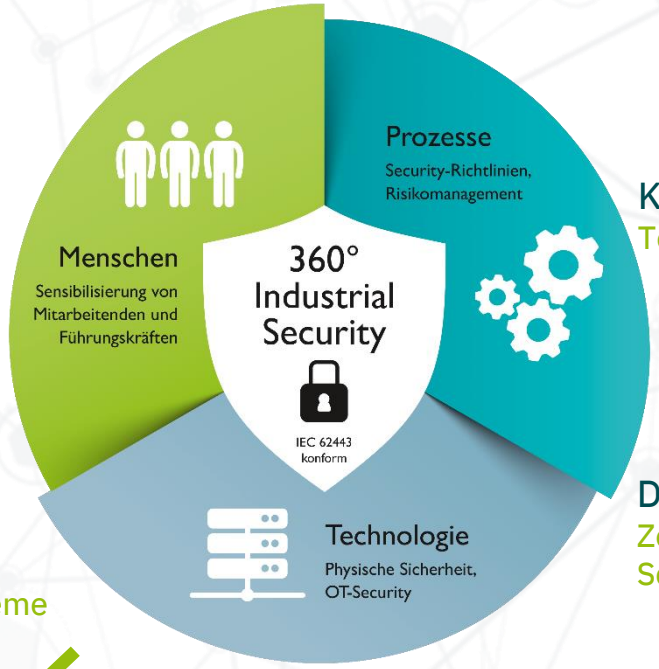
Was ist das Defense of Depth Konzept?

Konzept

IEC 62443-2-4
Mitarbeiter
Zusicherung
Systemaufbau
Drahtlose Verbindungen
SIS (Safety Instrumented System)
Konfigurationsverwaltung
Fernzugriff
Ereignismanagement
Nutzerkonten
Schutz gegen Schadsoftware
Patch Management
Datensicherung und Wiederherstellung

Keine geregelten Prozesse
Individuelle Abläufe wurden erarbeitet

Mitarbeiter laden private Geräte an SPS
Personal wird regelmäßig durch Awareness-Maßnahmen sensibilisiert



Keine Backups vorhanden
Templates und Abläufe erarbeitet

Dauerhafte Remotezugänge
Zentralen Zugang mit Schlüsselschalterlösung

Fehlendes Monitoring
IDS-System überwacht die Systeme und alarmiert in Echtzeit

Sensible Informationen sind unverschlüsselt
VPN auch anlagenintern

Flache Netzhierarchie
Basierend auf Funktion und Schutzbedarf segmentiert

Agenda

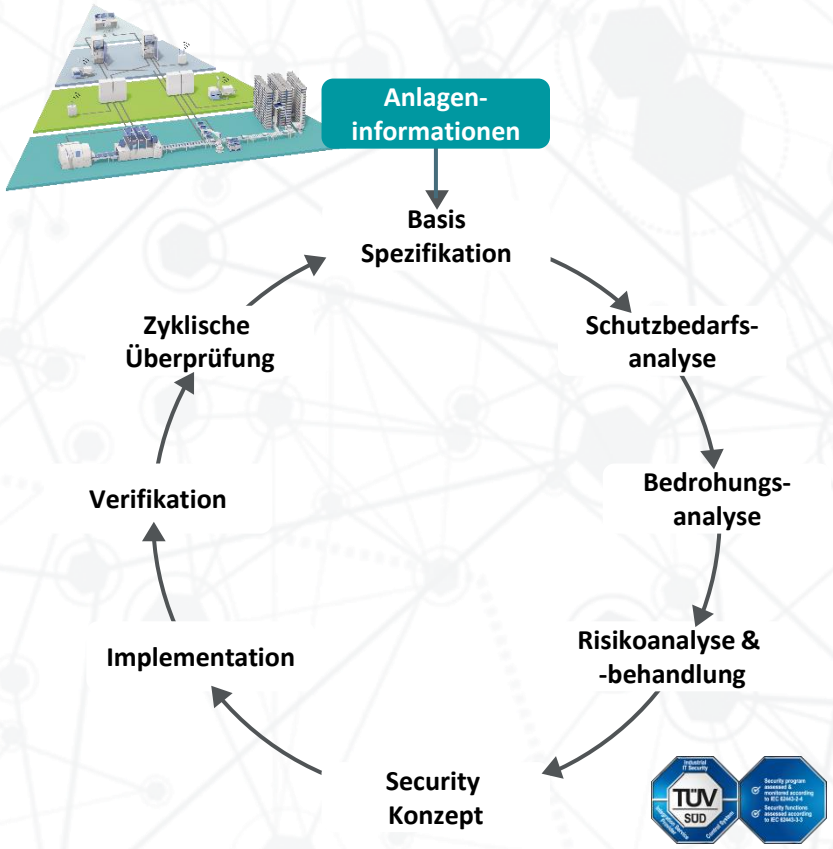
- Warm up
- Gesetzliche Anforderungen
- Gefahren in der Digitalen-Welt
- Was ist das Defense of Depth Konzept?
- IEC 62443 in der Praxis
- Zusammenfassung

IEC 62443 in der Praxis

Die Vorgehensweise im Detail (1/9)

Aktivitäten

- Bestimmung der Einsatzumgebung
- Bestimmung der Assets mit allen notwendigen Informationen zur Erstellung einer Asset Liste
- Festlegung der Netzwerkinfrastruktur
- Ermittlung der Abläufe in der Produktionsanlage.
- Festlegung welche Informationen/Daten und Kommunikationsbeziehungen schützenswert sind



IEC 62443 in der Praxis

Asset Aufnahme

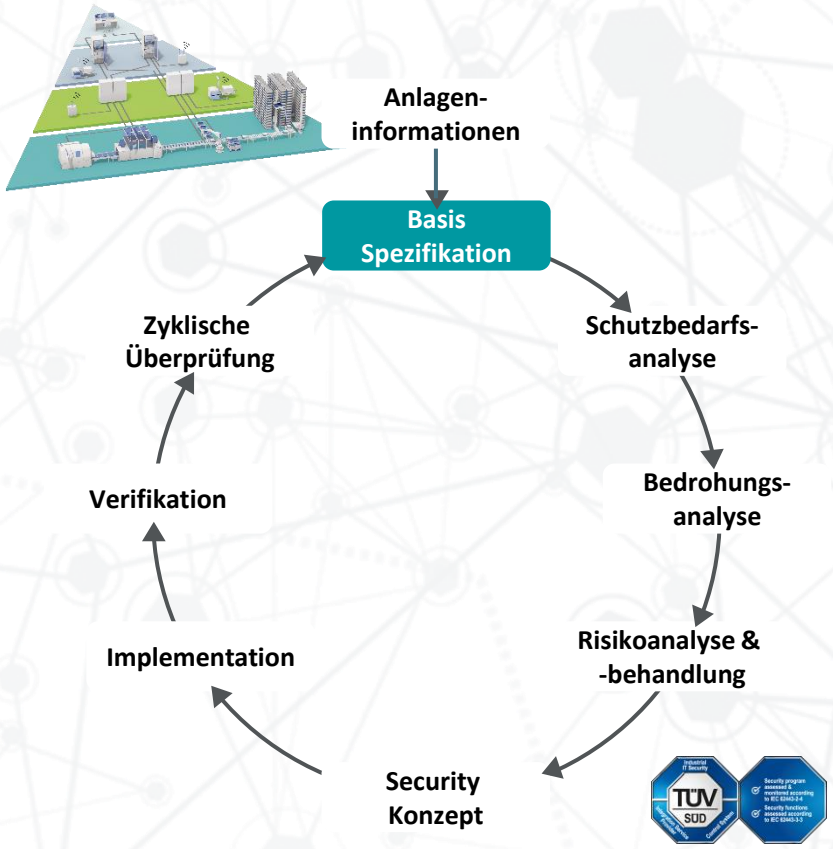
Das Anomalieerkennungssystem IRMA®

- ✓ Passives scannen der Teilnehmer
- ✓ Erfassung aller OT-Assets
- ✓ Kontinuierliche Überwachung
- ✓ Aufzeichnung der Verbindungen
- ✓ Validierung jeder Verbindung / jedes Teilnehmers
- ✓ Risiko Management
- ✓ Alarme bei Anomalien, neuen Teilnehmern im Netzwerk
- ✓ Reporting über den Zustand der Anlage

Die Vorgehensweise im Detail (2/9)

Aktivitäten

- Erstellung einer Assetliste
- Spezifizieren von Basisanforderungen für ein ganzheitliches Security Konzept zu den Themen:
  - Netzwerk-Architektur
  - Wireless
  - Configuration Management
  - Remote Zugänge
  - Event Management
  - Account Management
  - Malware Protection
  - Patch Management
  - Backup & Restore



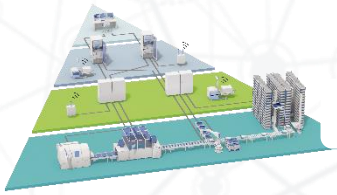
Die Vorgehensweise im Detail (3/9)

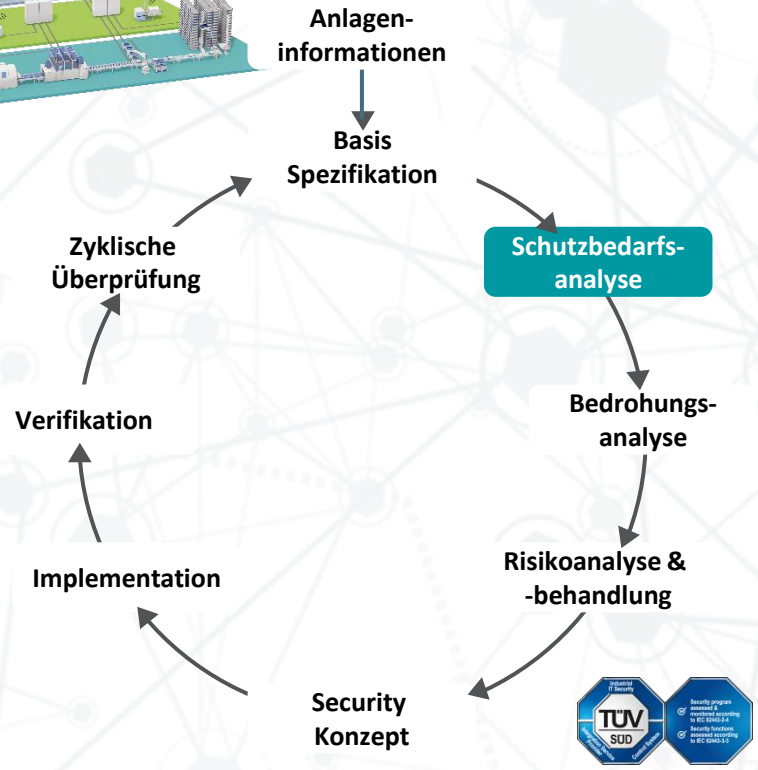
Aktivitäten

Ermittlung des Schutzbedarfes zur individuellen Absicherung besonders schützenswerter Assets

- Ermittlung der Schutzziele für
  - die Datenklassen in den Anlagenteilen und auf den logischen Kommunikationswegen
  - die logischen Kommunikationswege
  - die einzelnen Assets

Festlegung der Zonen und Conduits





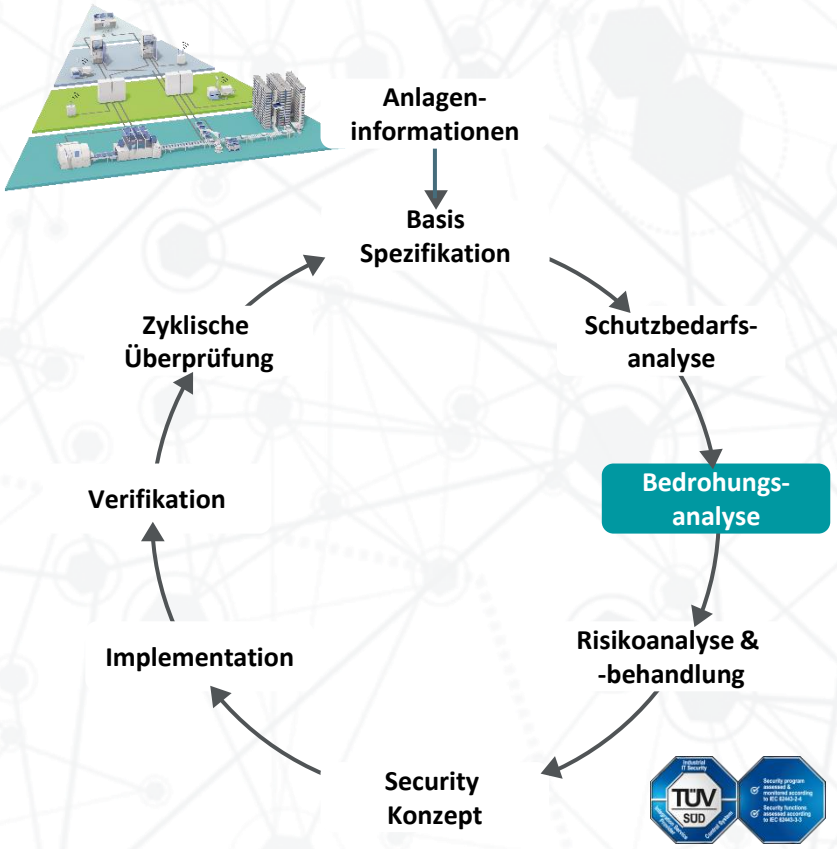
IEC 62443 in der Praxis

Die Vorgehensweise im Detail (4/9)

Aktivitäten

Identifizierung relevanter Bedrohungen für die Automatisierungslösung

- Abstimmung und ggf. Erweiterung des Bedrohungskatalogs mit dem Betreiber
- Bewertung der Bedrohungen bezüglich der Relevanz für die Automatisierungslösung

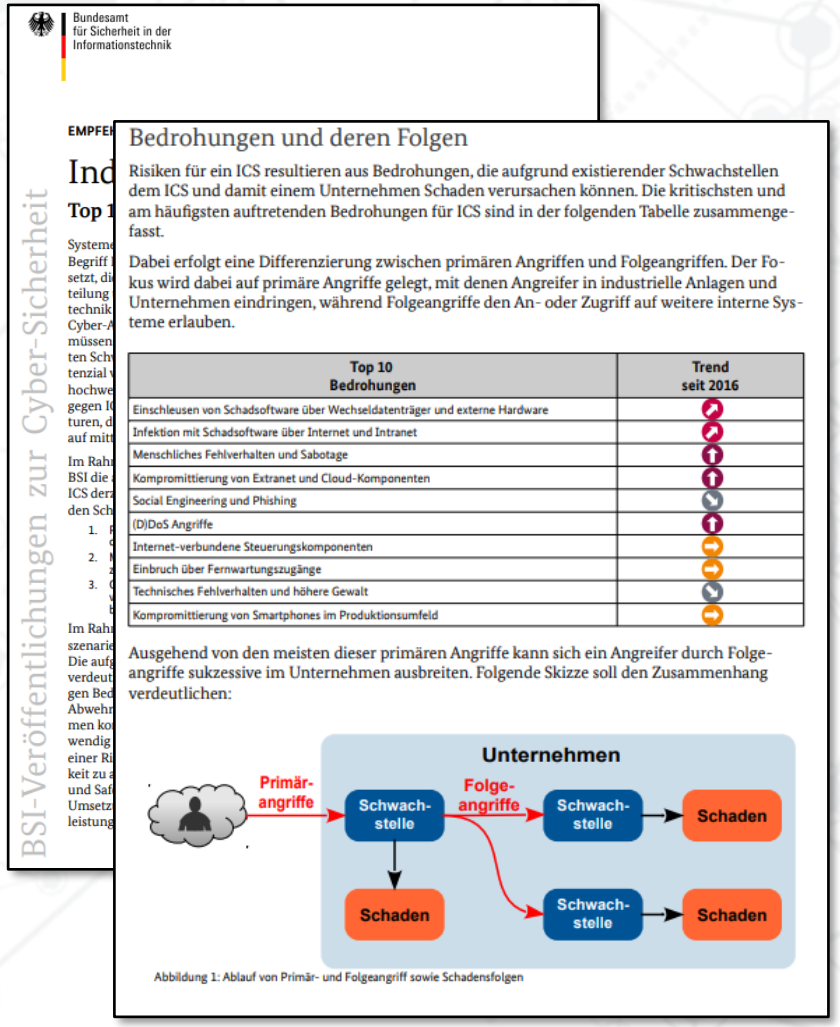


IEC 62443 in der Praxis

BSI – die TOP 10 Bedrohungen (2022)

Top 10 Bedrohungen	Trend seit 2019
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	→
Infektion mit Schadsoftware über Internet und Intranet	↑
Menschliches Fehlverhalten und Sabotage	→
Kompromittierung von Extranet und Cloud-Komponenten	↗
Social Engineering und Phishing	→
(D)DoS Angriffe	→
Internet-verbundene Steuerungskomponenten	↗
Einbruch über Fernwartungszugänge	↗
Technisches Fehlverhalten und höhere Gewalt	→
Soft- und Hardwareschwachstellen in der Lieferkette	↑

Quelle: BSI



Bundesamt für Sicherheit in der Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

Bedrohungen und deren Folgen

Risiken für ein ICS resultieren aus Bedrohungen, die aufgrund existierender Schwachstellen dem ICS und damit einem Unternehmen Schaden verursachen können. Die kritischsten und am häufigsten auftretenden Bedrohungen für ICS sind in der folgenden Tabelle zusammengefasst.

Dabei erfolgt eine Differenzierung zwischen primären Angriffen und Folgeangriffen. Der Fokus wird dabei auf primäre Angriffe gelegt, mit denen Angreifer in industrielle Anlagen und Unternehmen eindringen, während Folgeangriffe den An- oder Zugriff auf weitere interne Systeme erlauben.

Top 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	→
Infektion mit Schadsoftware über Internet und Intranet	↑
Menschliches Fehlverhalten und Sabotage	→
Kompromittierung von Extranet und Cloud-Komponenten	↗
Social Engineering und Phishing	→
(D)DoS Angriffe	↗
Internet-verbundene Steuerungskomponenten	→
Einbruch über Fernwartungszugänge	→
Technisches Fehlverhalten und höhere Gewalt	→
Kompromittierung von Smartphones im Produktionsumfeld	↓

Ausgehend von den meisten dieser primären Angriffe kann sich ein Angreifer durch Folgeangriffe sukzessive im Unternehmen ausbreiten. Folgende Skizze soll den Zusammenhang verdeutlichen:

Abbildung 1: Ablauf von Primär- und Folgeangriff sowie Schadensfolgen

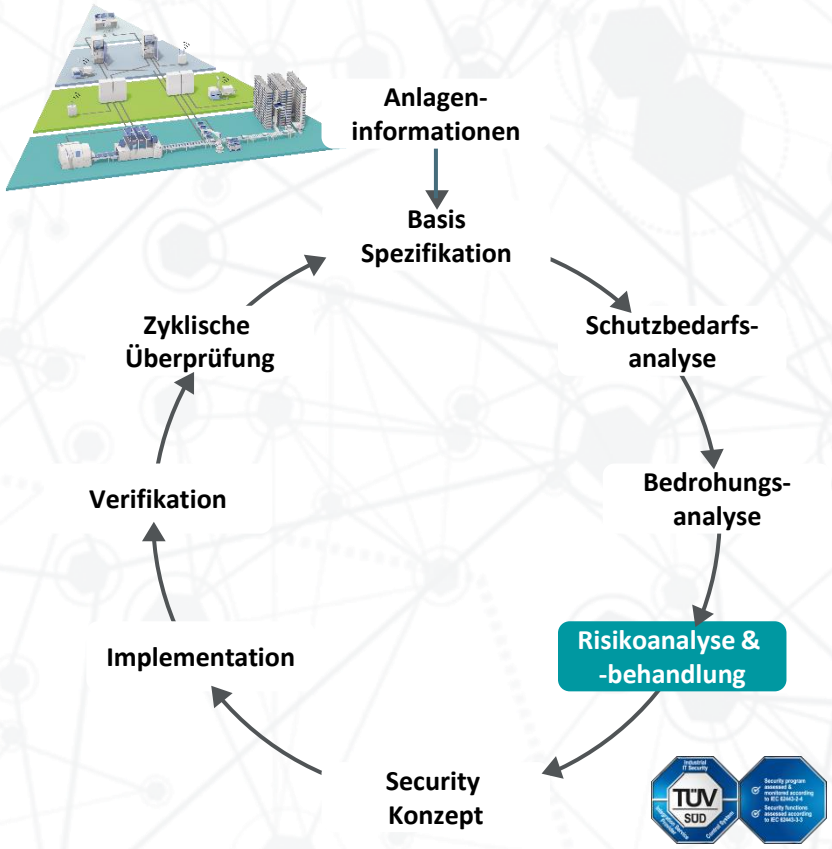
IEC 62443 in der Praxis

Die Vorgehensweise im Detail (5/9)

Aktivitäten

Erstellung eines Risk Assessments in dem folgenden Punkte erfasst sind:

- Ermittlung der Risikotoleranz des Betreibers
- Bewertung der erkannten Bedrohungen auf Basis der Security Spezifikation
- Maßnahmenvorschläge zur Risikominimierung



IEC 62443 in der Praxis

Risikomanagement

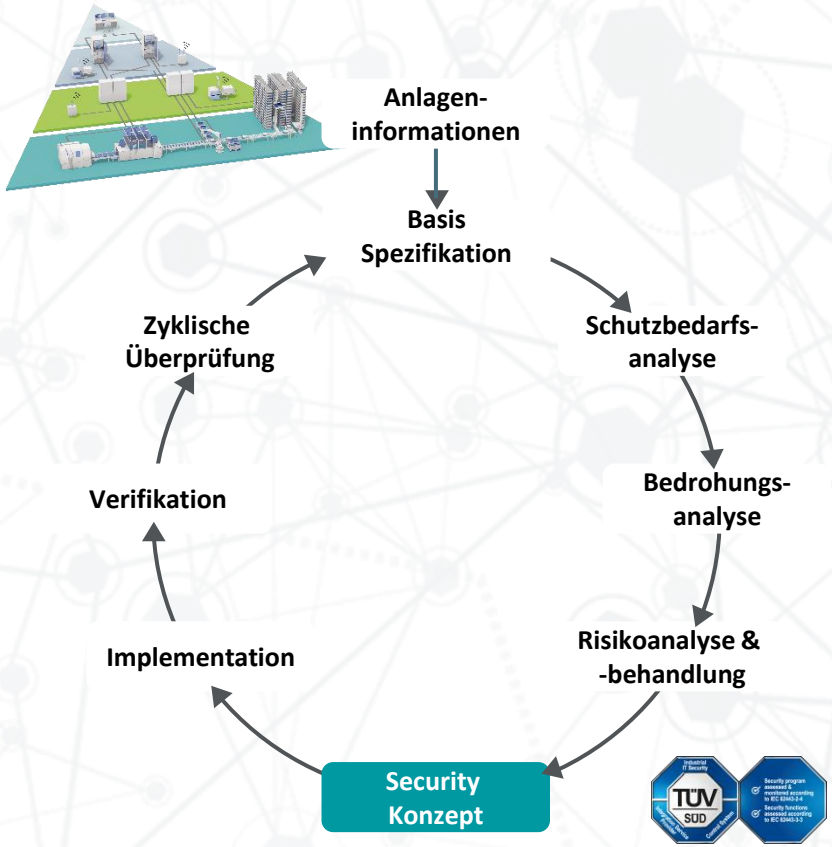
TID	Bedrohung - Szenario	Risiko ohne Maßnahmen	Risiko mit Maßnahmen	Maßnahmen	Kosten Schätzung	Risk Owner	Status	Frist zur Umsetzung
1	<Hier werden die Bedrohungen aus der Bedrohungsanlayse eingefügt>	Hoch	Gering	<Maßnahmen zur Risikominderung definieren>	<Kostensc hätzung>	<Verantwortlic hen einfügen>	Umgesetzt	Offen
2	<Hier werden die Bedrohungen aus der Bedrohungsanlayse eingefügt>	Hoch	Mittel	<Maßnahmen zur Risikominderung definieren>	<Kostensc hätzung>	<Verantwortlic hen einfügen>	Risiko akzeptiert	Offen

Die Vorgehensweise im Detail (6/9)

Aktivitäten

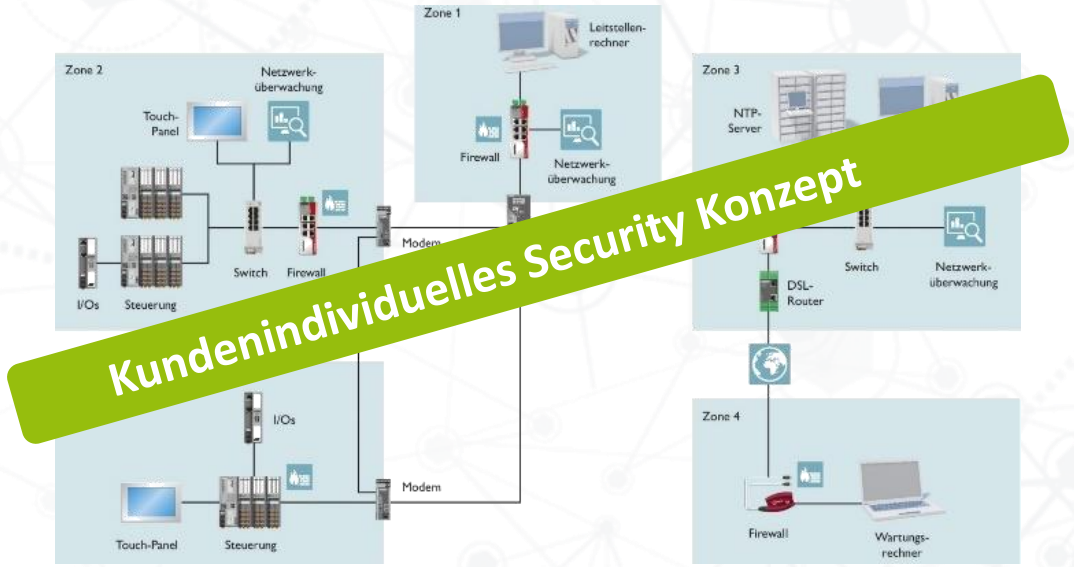
Ergänzung der Security Basis Spezifikation um individuelle Maßnahmen, auf Basis der Risikoanalyse:

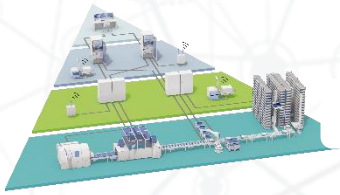
- Erstellung einer generischen Security Test Spezifikation für die Überprüfung der Implementierung
- Alle Maßnahmen basieren, zu dem Zeitpunkt der Durchführung, auf dem aktuellen Stand der Technik und die Ergebnisse sind dokumentiert

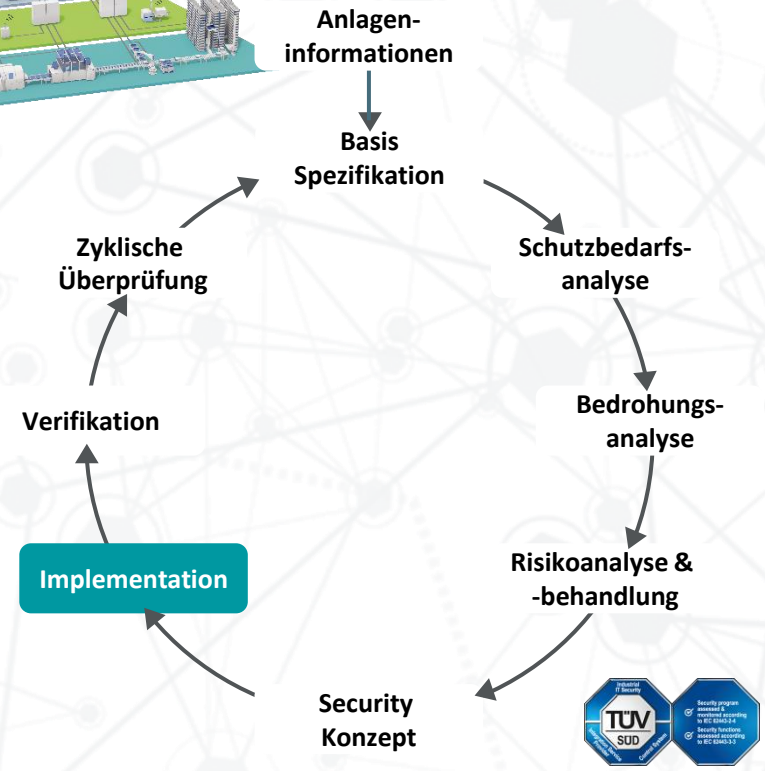


Die Vorgehensweise im Detail (7/9)

Aktivitäten





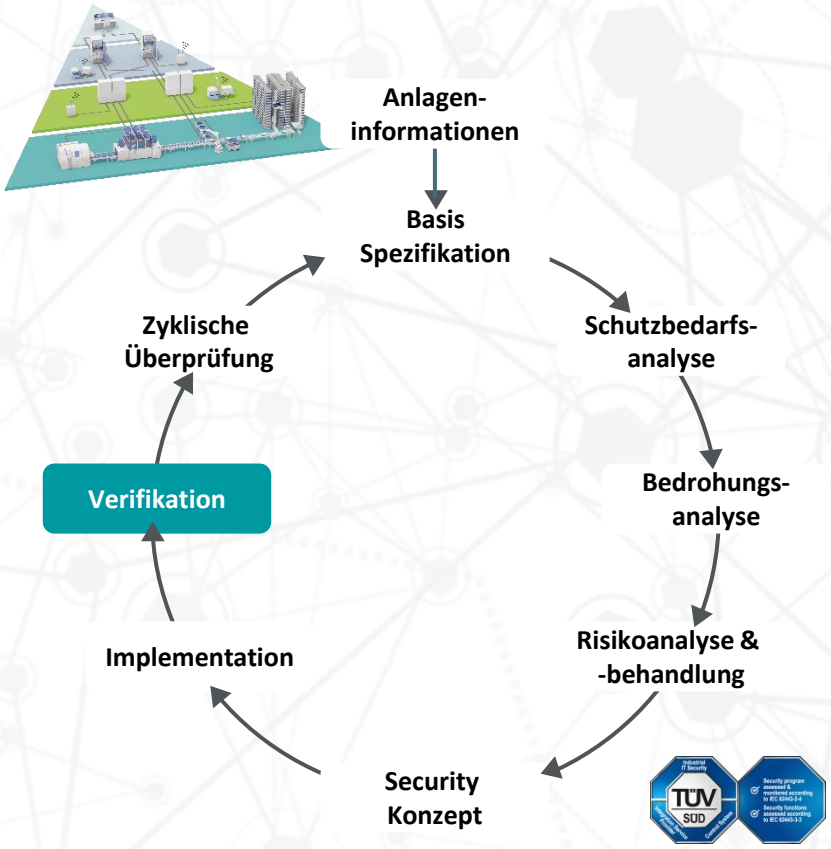


IEC 62443 in der Praxis

Die Vorgehensweise im Detail (8/9)

Aktivitäten

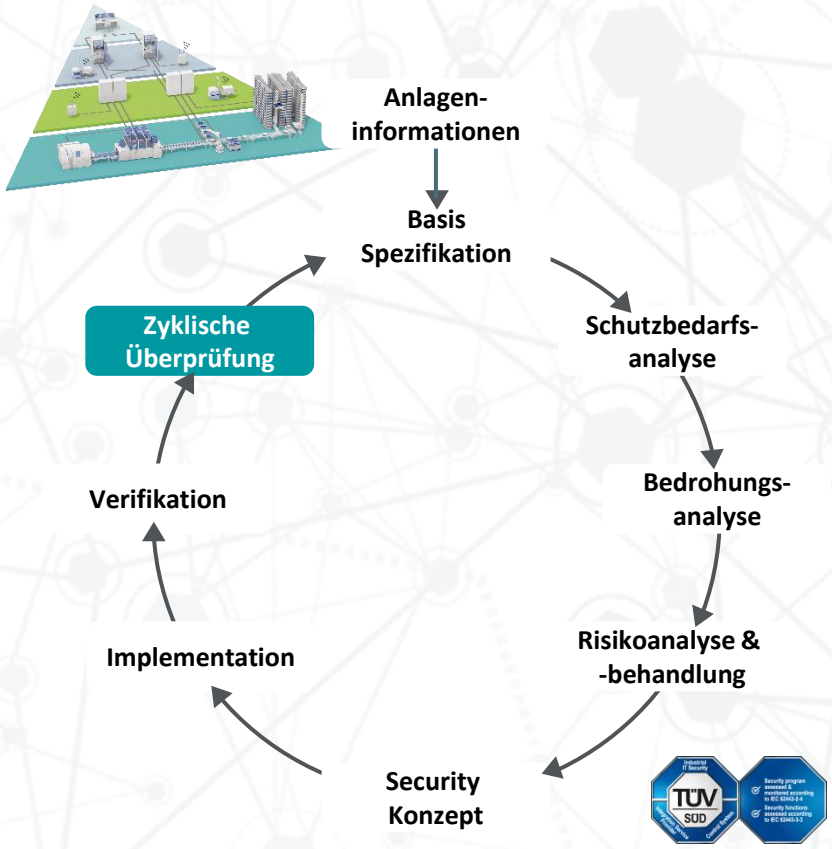
Auf Basis der generischen Security Testspezifikation erfolgt gemeinsam mit dem Systemintegrator im Rahmen eines Security-Audits die Überprüfung der Implementierung.



Die Vorgehensweise im Detail (9/9)

Aktivitäten

Um alle Maßnahmen auf dem Stand der Technik zu halten, empfehlen wir in regelmäßigen Abständen eine detaillierte Überprüfung der Security Spezifikation und deren Wirksamkeit durchzuführen.



Agenda

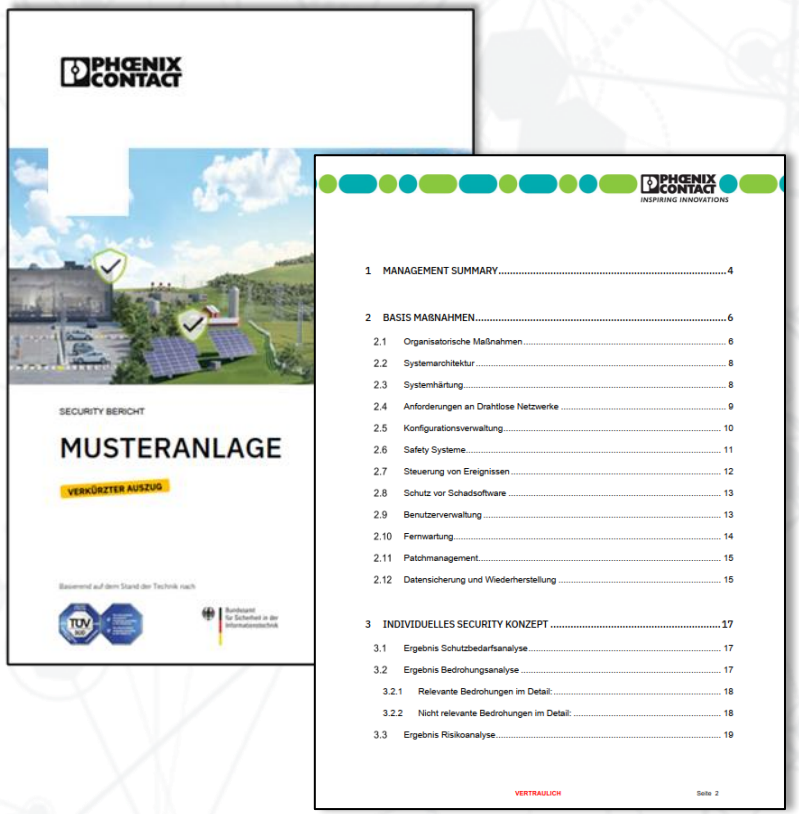
- Warm up
- Gesetzliche Anforderungen
- Gefahren in der Digitalen-Welt
- Was ist das Defense of Depth Konzept?
- IEC 62443 in der Praxis
- Zusammenfassung

Zusammenfassung

Schritt für Schritt

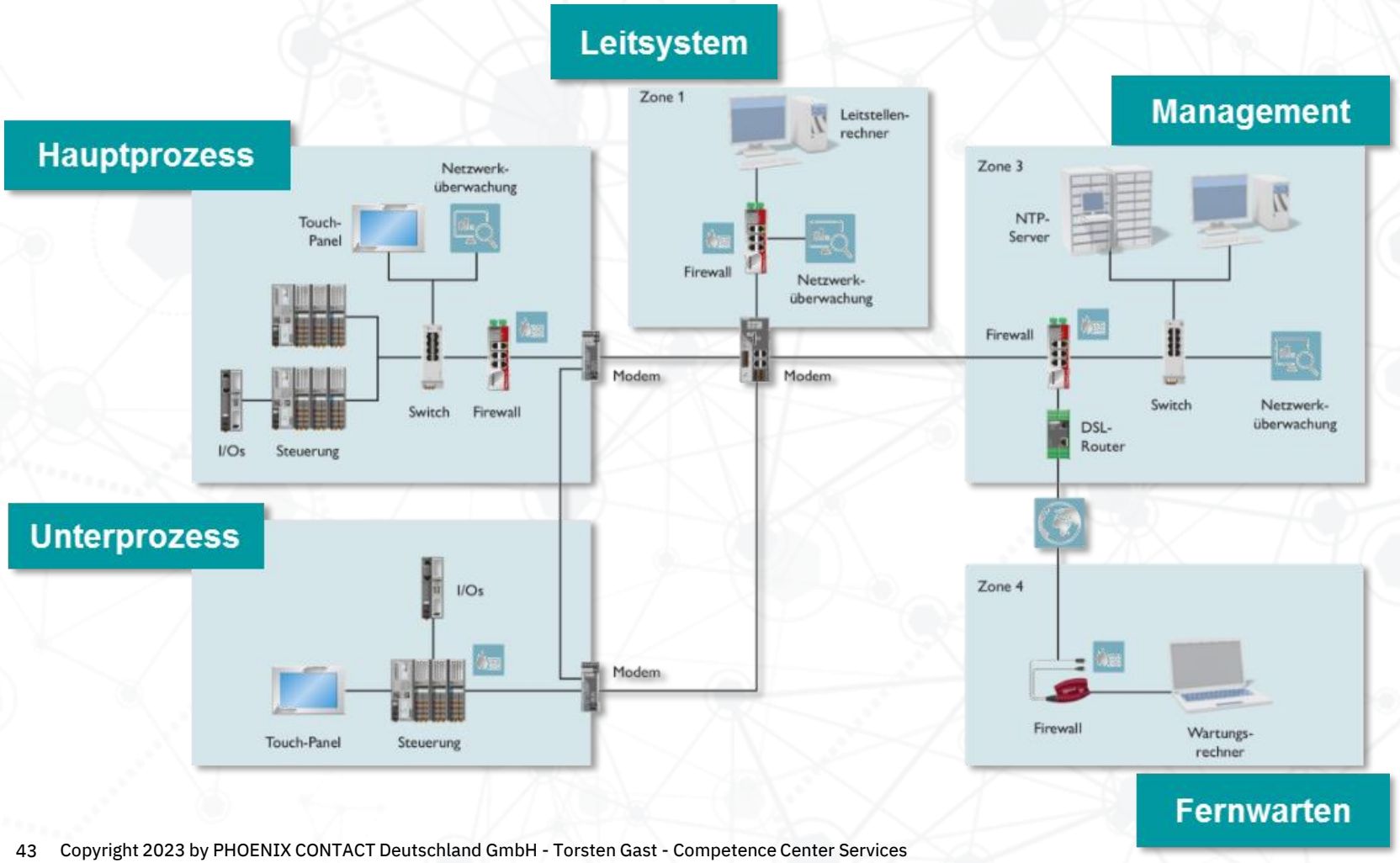
- Unternehmen müssen ihre Produktionsanlagen in das **ganzheitliche Security Konzept** mit aufnehmen.
- IT muss Kompetenzen im Bereich der OT-Security aufbauen
- Anforderungen der ISO 2700X reichen **nicht** für den Produktions- und Gebäudeautomatisierungsbereich aus!

➢ **Für ein 360° Grad Konzept im Industriellen Umfeld sollte der Standard IEC 62443 angewendet werden.**



Zusammenfassung

Der generische Blueprint – Referenzarchitektur



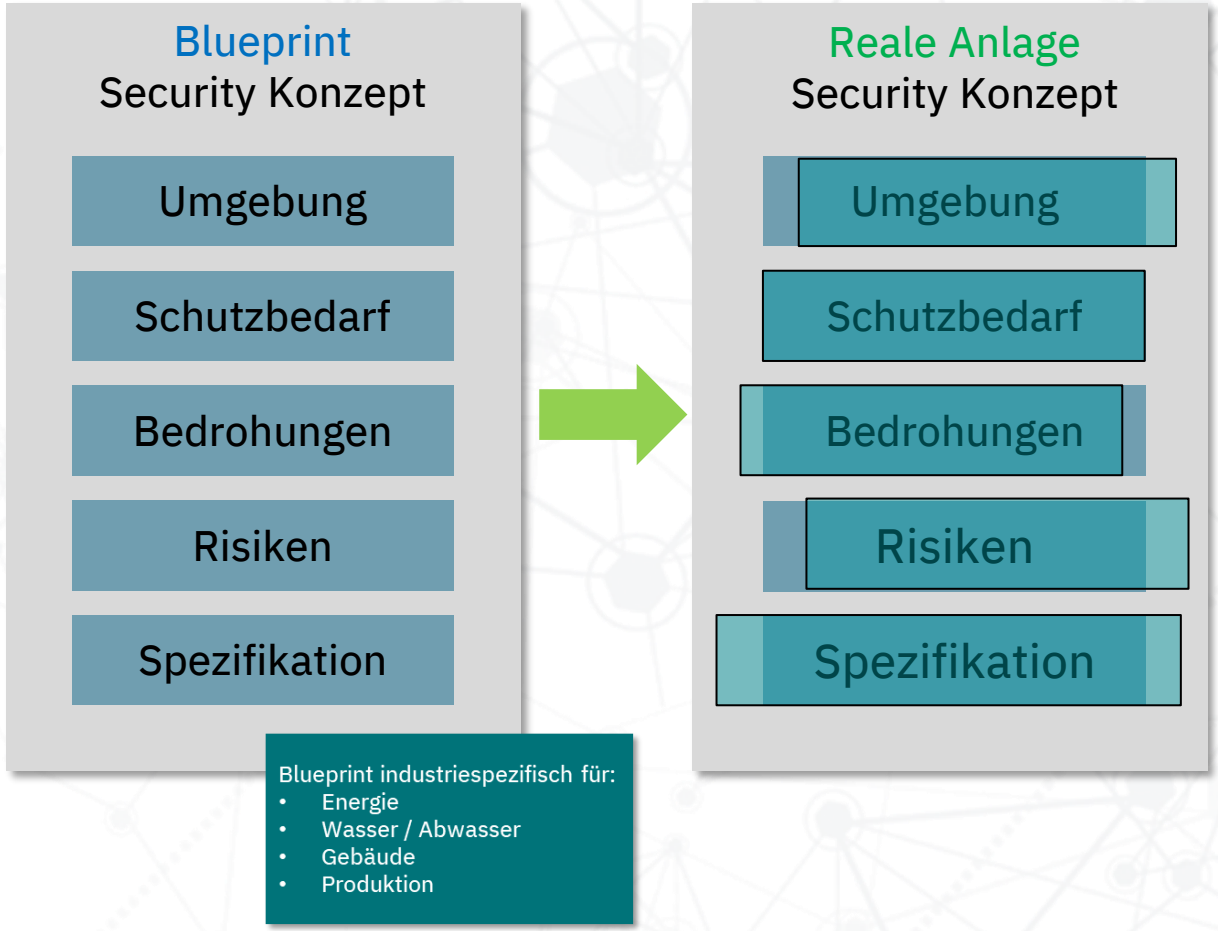
Anwendung des Defense in Depth Konzepts durch Segmentierung in Zonen

Sie als Kunde finden sich mit Ihrer Anlage in der Architektur wieder.

Visuelle Darstellung eines zertifizierten Security Designs

Zusammenfassung

Vom Security Blueprint zu einer realen Anlage



- Der Blueprint ist die Vorlage für alle weiteren realen Anlagen.
- Sollten bei den realen Automatisierungslösungen Abweichungen bei Umfeld, Schutzbedarf, Bedrohungen und Risiken vorhanden sein, dann werden **nur** für diese Abweichungen die Security Betrachtungen erweitert.

Zusammenfassung

Unser Angebot für Sie direkt zum Durchstarten

9 Schritte zur sicheren Anlage

1) Bestandsaufnahme
2) Security Basisspezifikation
3) Schutzbedarfsanalyse
4) Bedrohungsanalyse
5) Risikoanalyse
6) Security-Konzept
7) Implementierung
8) Verifikation
9) Zyklische Überprüfung

+ STARTER Workshop
oder
+ vor Ort Gratis Erstgespräch mit First-Security Check

Competence Center Services

Ihr Partner für Produktunabhängige Dienstleistungen

OT-Security Service Provider nach IEC 62443

CERT@VDE

Linked in Industrial Services - Security | Safety | CE

www.phoenixcontact.de/services

Danke
für Ihr Interesse!

Wie Sie jetzt auch noch Ihre Produktion sicher bekommen

Torsten Gast

Email: torsten.gast@phoenixcontact.de
Telefon: 0173 / 25 92 411

PHOENIX CONTACT
INSPIRING INNOVATIONS