



Willkommen

**IT-Sicherheitsgesetz 2.0?
Kritis? Wat nu?**

**Wie Sie die Cyber
Sicherheitsrisiken Ihres
Windparks minimieren**

PHOENIX CONTACT - Auf einen Blick

Gründung

1923 in Essen, Nordrhein-Westfalen, Deutschland

Umsatz 2020

2,4 Mrd. €

Mitarbeitende 2020

17.100 weltweit, 8.800 davon in Deutschland

Produktionsstandorte

China, Deutschland, Griechenland, Indien, Polen, Russland, Schweden, Schweiz, Taiwan/China, Türkei, USA

Vertrieb

in über 55 Tochtergesellschaften weltweit vertreten

Windenergie

Ausbau der Lösungs-, Applikations- und Produktkompetenz im Vertical-Market-Management, aufbauend auf vorhandenen Geschäftsbeziehungen



Wie Sie die Cyber Sicherheitsrisiken Ihres Windparks minimieren

Agenda

Competence Center
Services



Kompetenzfeld: Industrial Security

- 1| **Cyber Attacken als Unternehmensrisiko #1**
- 2| **Der Weg zum sicheren Windpark**
- 3| **Phoenix Contact als ICS-Security Service Provider**

IT-Sicherheitsgesetz 2.0

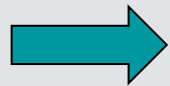
Einführung der UNBÖFI



Erweiterte Aufgaben
sowie Befugnisse
für das BSI

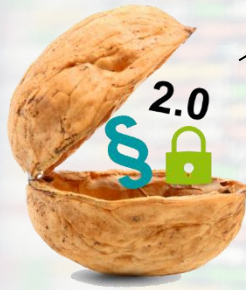


Meldepflicht
für den Einsatz von
kritischen Komponenten



Ausblick 2022 EU-Ebene: NIS 2.0

- Keine Schwellwerte, Unternehmen ab 50 MA
- IT-Sicherheitsgesetz 3.0?!



Neuer Sektor
Siedlungsabfallentsorgung



Geplant
sinkende Schwellwerte
(Kritisverordnung Entwurf)



Anforderungen + Bußgelder steigen

- Bsp. Systeme zur Angriffserkennung
- §14 bis zu 2.000.000€, kann durch Verweis auf § 30 OWiG verzehnfacht werden

Security trotzdem umsetzen?!

DIENSTAG, 02. NOV 2021

MecklenburgVorpommern

Cyberangriff: Normalbetrieb erst im kommenden Jahr



Cyberangriff: Fleischproduzent JBS stellt Produktion ein



Angriff aus dem Netz –
Wie Cyberkriminelle unsere Wirtschaft erpressen

Cyberangriff: TU Berlin rechnet mit monatelangen IT-Einschränkungen



www.ardmediathek.de

SWR >>>

Cyber Attacken sind in der Realität angekommen



#1 Unternehmensrisiko (weltweit)

Quelle: Risikobarometer der Allianz AG

68% der Industrieunternehmen in Deutschland sind bereits Opfer von Cyber Angriffen geworden.

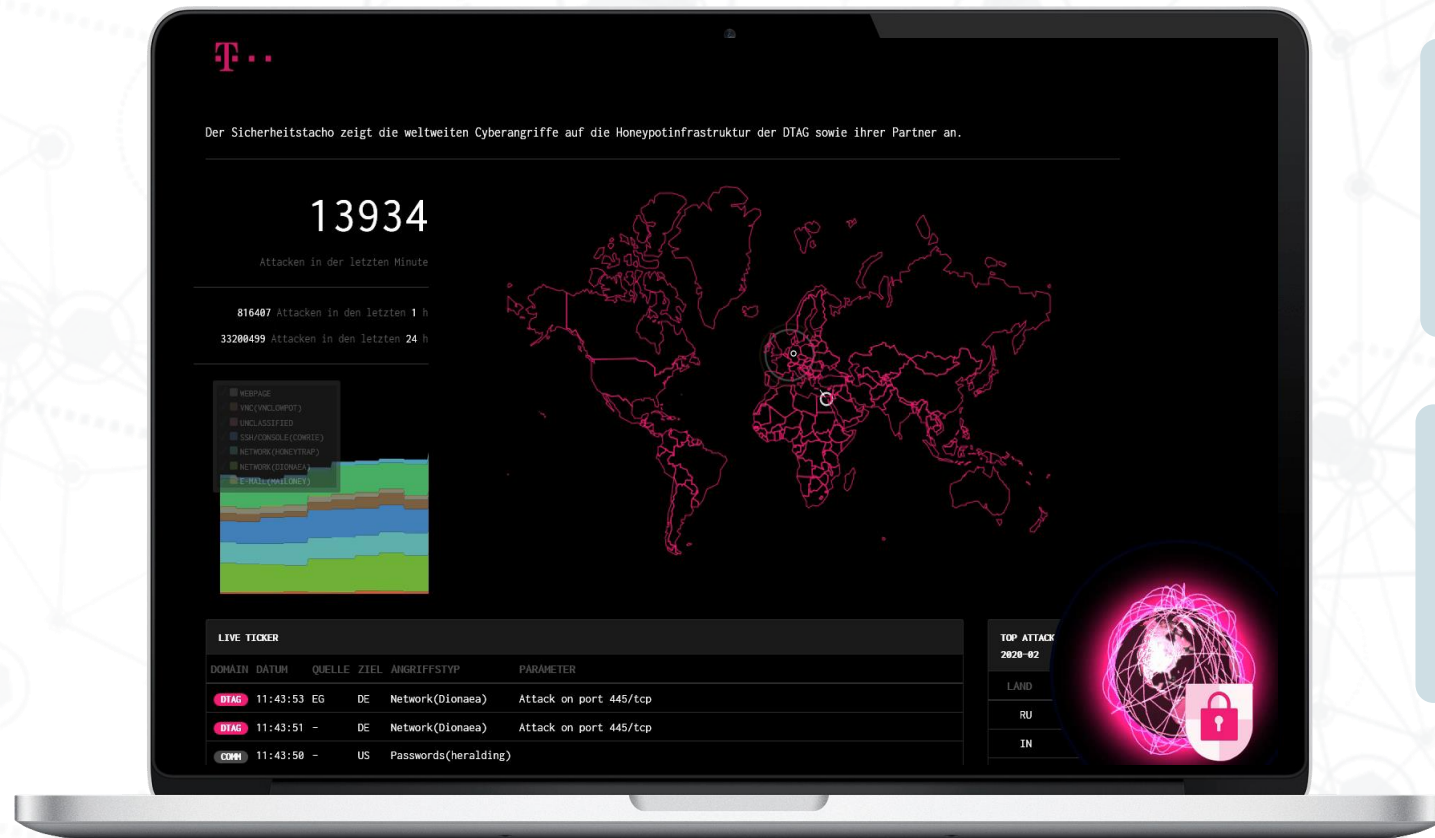
Quelle: VDMA

59% dieser Angriffe führen zu Produktionsausfällen

Quelle: VDMA

Bedrohungslage

Online Cyber Angriffe



Quelle: www.sicherheitstacho.eu

Kann man auf meine Steuerung über das www zugreifen?

- <https://www.shodan.io/>

Müssen alle Täter gute Hacker sein?

- Cyber-Crime as a Service!

Auswirkungen eines Security-Vorfalls auf Automatisierungsanlagen

Anlagenstillstand

Wie hoch sind die Wiederherstellungskosten?



Imageverlust

Wird Ihre Reputation von Partnern & Kunden in Frage gestellt?

Verlust von Know-How & sensibler Daten

Kann der Schaden wirtschaftlich quantifiziert werden?

Erpressung mit Ransomware

Wie hoch sind die Kosten für die Rekonstruktion der Daten?

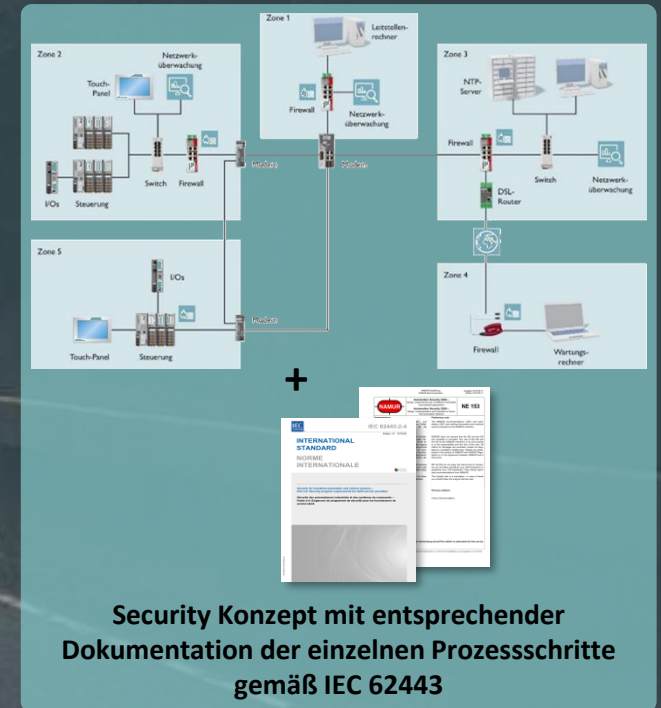
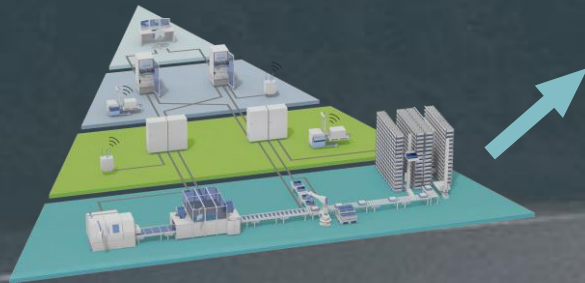
Der Weg zum sicheren Windpark

Design eines Security Konzepts für Automatisierungslösungen

Ausgangsbasis:
Kundenanlageninformation

Vorgehensweise:
Design eines Security Konzepts für Automatisierungslösungen

Ergebnis: Ganzheitliches Security Konzept durch Blueprint & Doku



Dienstleistungsportfolio – Industrial Security

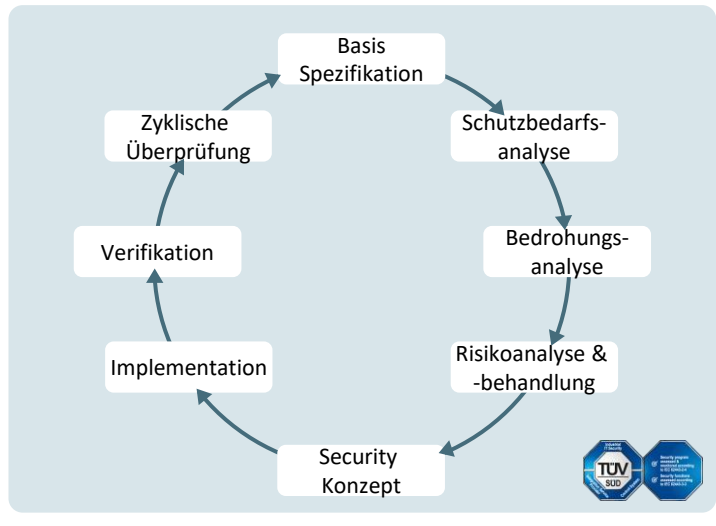


Komplettpaket

Design eines Security Konzepts für Automatisierungslösungen

C E

- Minimierung von Cyber Sicherheitsrisiken durch individuelle Absicherungsstrategie
- Sicherstellung der Anlagenverfügbarkeit & Prävention von Ausfallkosten
- Exzellente Kompetenz durch unsere Security Auditoren & Zertifizierung nach IEC 62443
- Kosteneffizienz durch Blueprint Ansatz




Beliebteste Einzelpakete

- Basis Spezifikation für Automatisierungslösungen (C)
- Sichere Fernwartung (C)
- Sicheres Netzwerkkonzept (C)
- Implementierung eines Anomalieerkennungssystems (E)



Dienstleistungsportfolio – Industrial Security







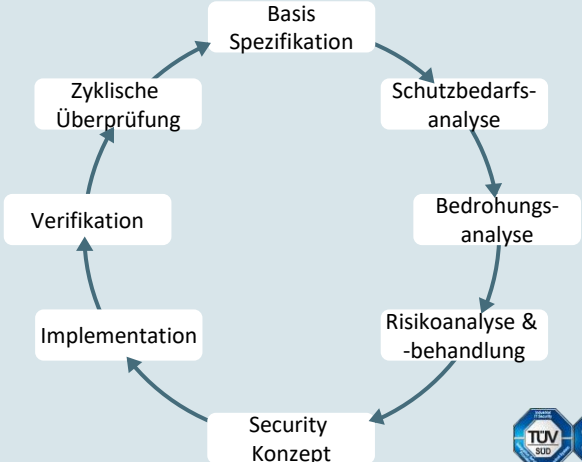
Komplettpaket


Design eines Security Konzepts für Automatisierungslösungen

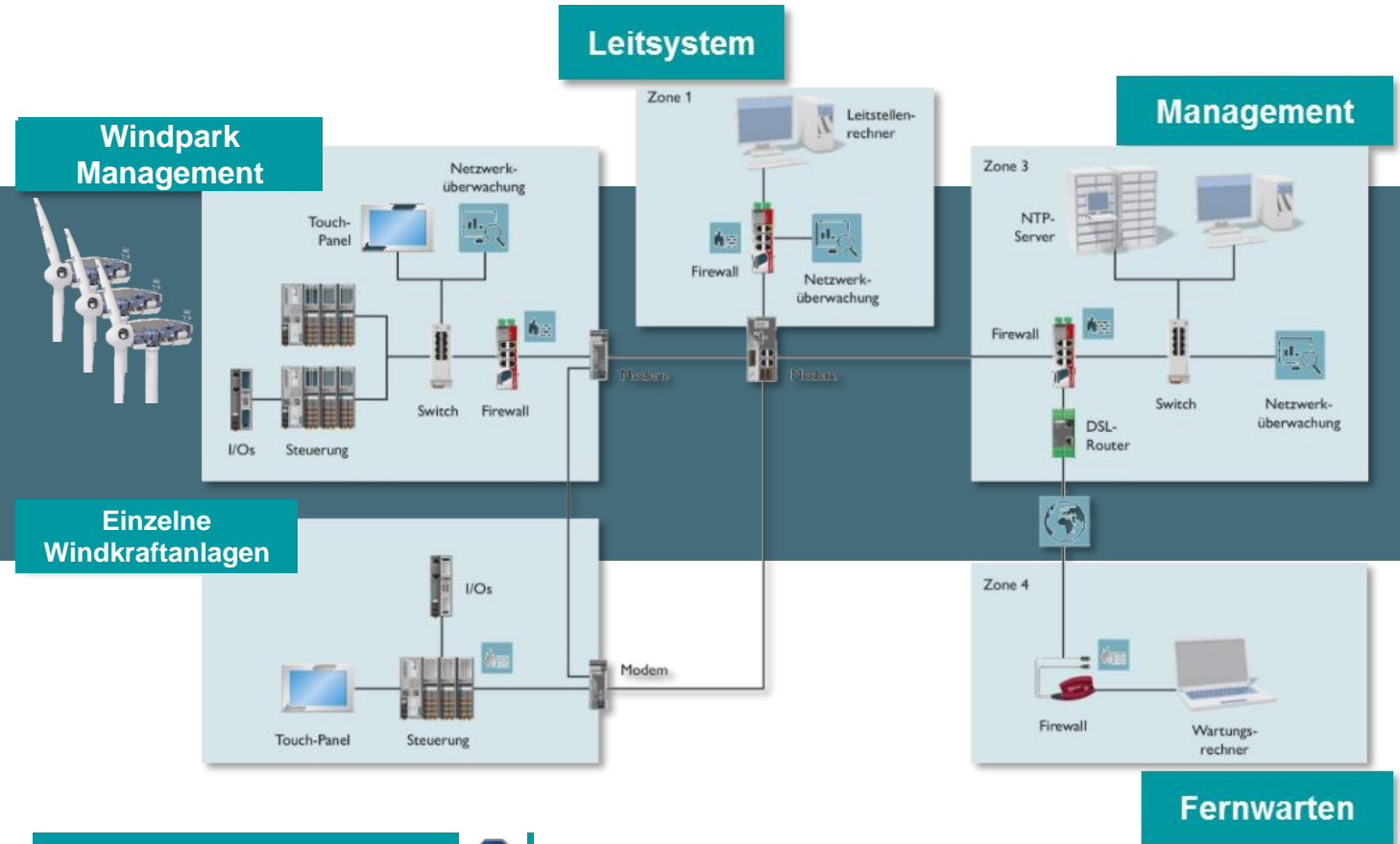
C

E


-  **Minimierung von Cyber Sicherheitsrisiken** durch individuelle Absicherungsstrategie
-  **Sicherstellung der Anlagenverfügbarkeit** & Prävention von Ausfallkosten
-  **Exzellente Kompetenz** durch unsere Security Auditoren & Zertifizierung nach IEC 62443
-  **Kosteneffizienz** durch Blueprint Ansatz







Blueprint ist nach 62443-3-3 Systemsicherheitsanforderungen und Sicherheitsstufen zertifiziert.







Phoenix Contact als ICS-Security Service Provider

Dienstleistungsportfolio – Industrial Security



Beliebteste Einzelpakete

-  Basis Spezifikation für Automatisierungslösungen **C**
-  Sichere Fernwartung **C**
-  Sicheres Netzwerkkonzept **C**
-  Implementierung eines Anomalieerkennungssystems **E**

Netzwerkarchitektur & -segmentierung

Drahtlose Datenübertragung

Fernzugriffe

Event Management

Berechtigungskonzept

Schadsoftware Schutz

Patch Management





Datensicherung/
Wiederherstellung

Phoenix Contact als ICS-Security Service Provider

Dienstleistungsportfolio – Industrial Security



Beliebteste Einzelpakete

-  Basis Spezifikation für Automatisierungslösungen **C**
-  **Sichere Fernwartung** **C**
-  Sicheres Netzwerkkonzept **C**
-  Implementierung eines Anomalieerkennungssystems **E**

Absicherung eines besonders schutzbedürftigen Bereichs

Abbilden aller Security Anforderungen auf den Scope Fernwartung

Dienstleistungsportfolio – Industrial Security



„Anforderungen zum Stand der Technik leichter umsetzen“

Beliebteste Einzelpakete



Basis Spezifikation für Automatisierungslösungen



Sichere Fernwartung



Sicheres Netzwerkkonzept



Implementierung eines Anomalieerkennungssystems



Wie Sie die Cyber Sicherheitsrisiken Ihres Windparks minimieren

Sprechen Sie uns an!

Competence Center
Services



Kompetenzfeld: Industrial Security



| Web: www.phoenixcontact.de/services



| E-Mail: services@phoenixcontact.de



| Telefon: 05281-946-5555