Hauke Kästing Competence Center Services

Willkommen

Best Practice – von der Risikoanalyse zum Security Konzept

PHOENIX CONTACT
INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

Hauke Kästing

PHOENIX CONTACT Deutschland GmbH

Industry Management and Automation

Competence Center Services

Industrial Security & Netzwerk

Dringenauer Str. 30

31812 Bad Pyrmont

Fon: +49 5281 946- 2113

Email: hauke.kaesting@phoenixcontact.de

INSPIRING INNOVATIONS

Die zwei Security Welten IT & OT

360° Industrial Security
MENSCHEN
PROZESSE
TECHNOLOGIE
IEC 62443 konform

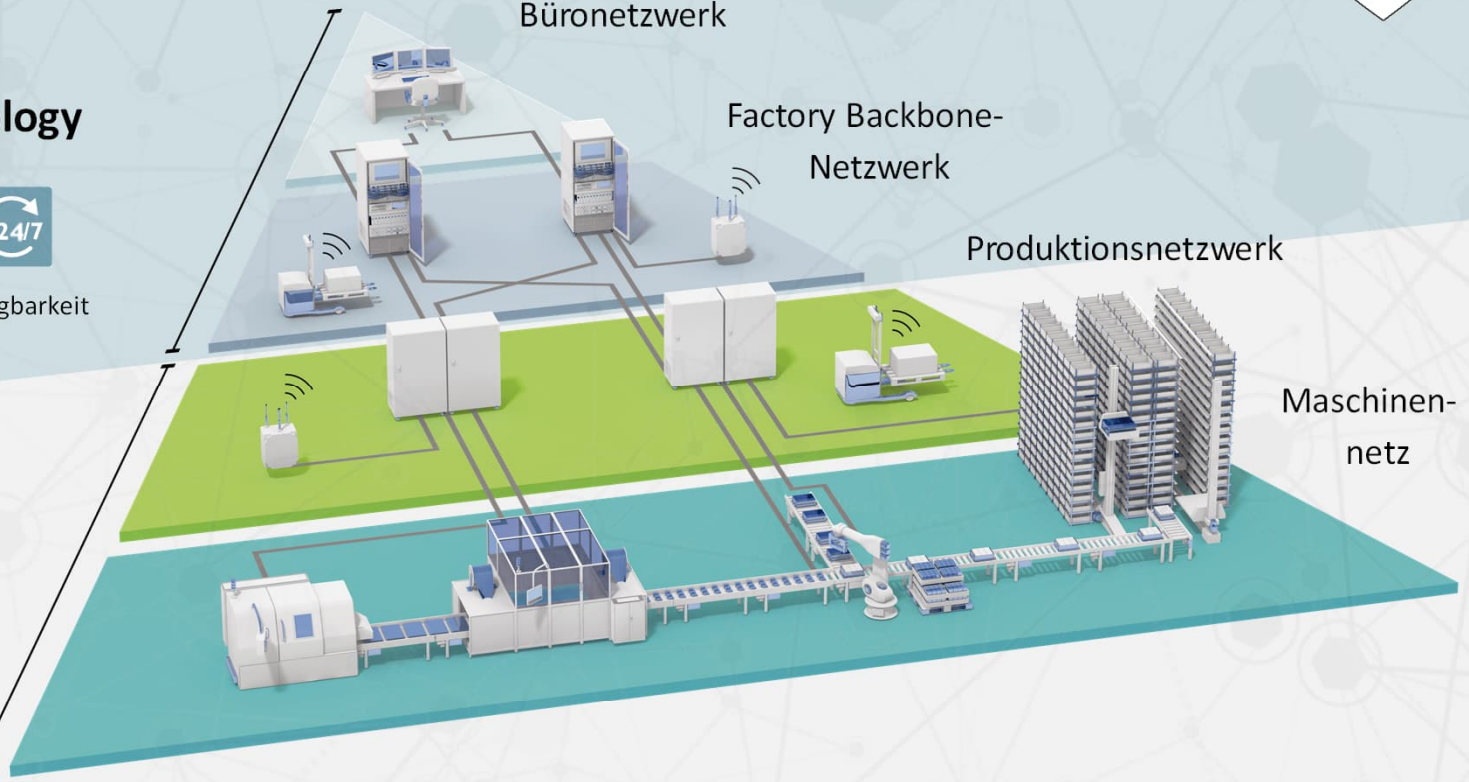
Information Technology

Vertraulichkeit | Integrität | Verfügbarkeit

≠

Operation Technology

Verfügbarkeit | Integrität | Vertraulichkeit



PHOENIX CONTACT
INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

IEC 62443: Aufbau

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 Systemsicherheitslebenszyklus 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

INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

Anforderungen an einen Systemintegrator IEC 62443-2-4

Wert	SP-Anford.-ID	Beschreibung
Mitarbeiter	SP.01.XX	Anforderungen an die Zuweisung von Personal durch den Dienstleister für Tätigkeiten in Zusammenhang mit der „Automatisierungslösung“
Zusicherung	SP.02.XX	Anforderungen an das Vertrauen, dass die IT-Sicherheitsleitlinien für die „Automatisierungslösung“ durchgesetzt werden
Systemaufbau	SP.03.XX	Anforderungen an die Auslegung der „Automatisierungslösung“
Drahtlose Verbindung (drahtlos)	SP.04.XX	Anforderungen an die Verwendung von Drahtlose Verbindungen in der „Automatisierungslösung“
SIS	SP.05.XX	Anforderungen an die Integration von PLT-Sicherheitseinrichtungen in die „Automatisierungslösung“
Konfigurationsverwaltung	SP.06.XX	Anforderungen an die Konfigurationssteuerung der „Automatisierungslösung“
Fernzugriff	SP.07.XX	Anforderungen an den Fernzugriff auf die „Automatisierungslösung“
Behandlung von Ereignissen	SP.08.XX	Anforderungen an die Behandlung von Ereignissen in der „Automatisierungslösung“
Verwaltung von Nutzerkonten	SP.09.XX	Anforderungen an die Verwaltung von Nutzerkonten in der „Automatisierungslösung“
Schutz gegen Schadsoftware	SP.10.XX	Anforderungen an den Einsatz von Anti-Malware in der „Automatisierungslösung“
Patch-Management	SP.11.XX	Anforderungen an die IT-Sicherheitsaspekte der Genehmigung und Installation von Softwarepatches
Datensicherung/ -wiederherstellung	SP.12.XX	Anforderungen an die IT-Sicherheitsaspekte der Datensicherung und Wiederherstellung

- Anforderungen an den Personaleinsatz
  - Kompetenz
  - Rollen/Verantwortung
  - Prozesse
  - Leitlinien
- Anforderungen an die Automatisierungslösung
  - Prozesse
  - Funktionen
  - Dokumentation

PHOENIX CONTACT
INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

IEC 62443-3-3: Die 7 Foundational Requirements (FR)

1. Identifizierung und Authentifikation (Identification and authentication control (IAC))
2. Nutzungskontrolle (Use control (UC))
3. Systemintegrität (System integrity (SI))
4. Vertraulichkeit der Daten (Data confidentiality (DC))
5. Eingeschränkter Datenfluss (Restricted data flow (RDF))
6. Rechtzeitige Reaktion auf Ereignisse (Timely response to events (TRE))
7. Verfügbarkeit der Ressourcen (Resource availability (RA))

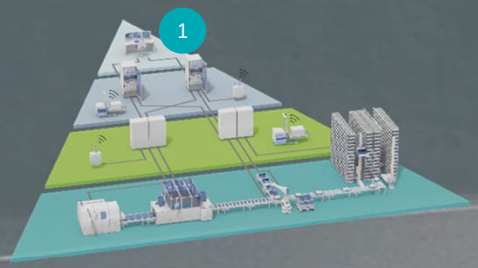
PHOENIX CONTACT
INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

Design eines Security Konzepts für Automatisierungslösungen

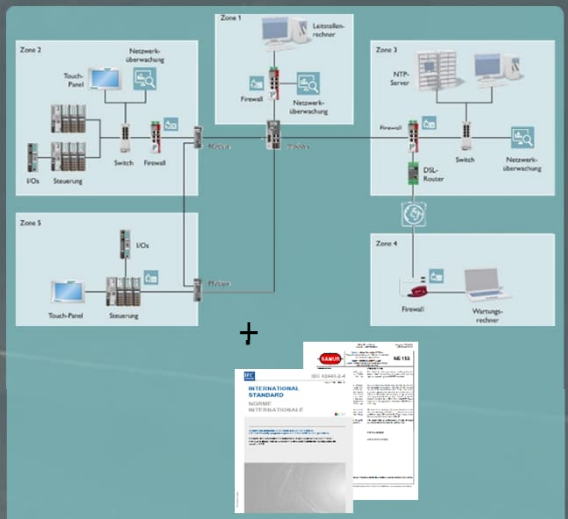
360° Industrial Security – MENSCHEN – PROZESSE – TECHNOLOGIE – IEC 62443 konform

Ausgangsbasis:
Kundenanlageninformation



Vorgehensweise:
Design eines Security Konzepts für Automatisierungslösungen

Ergebnis:
Ganzheitliches Security Konzept

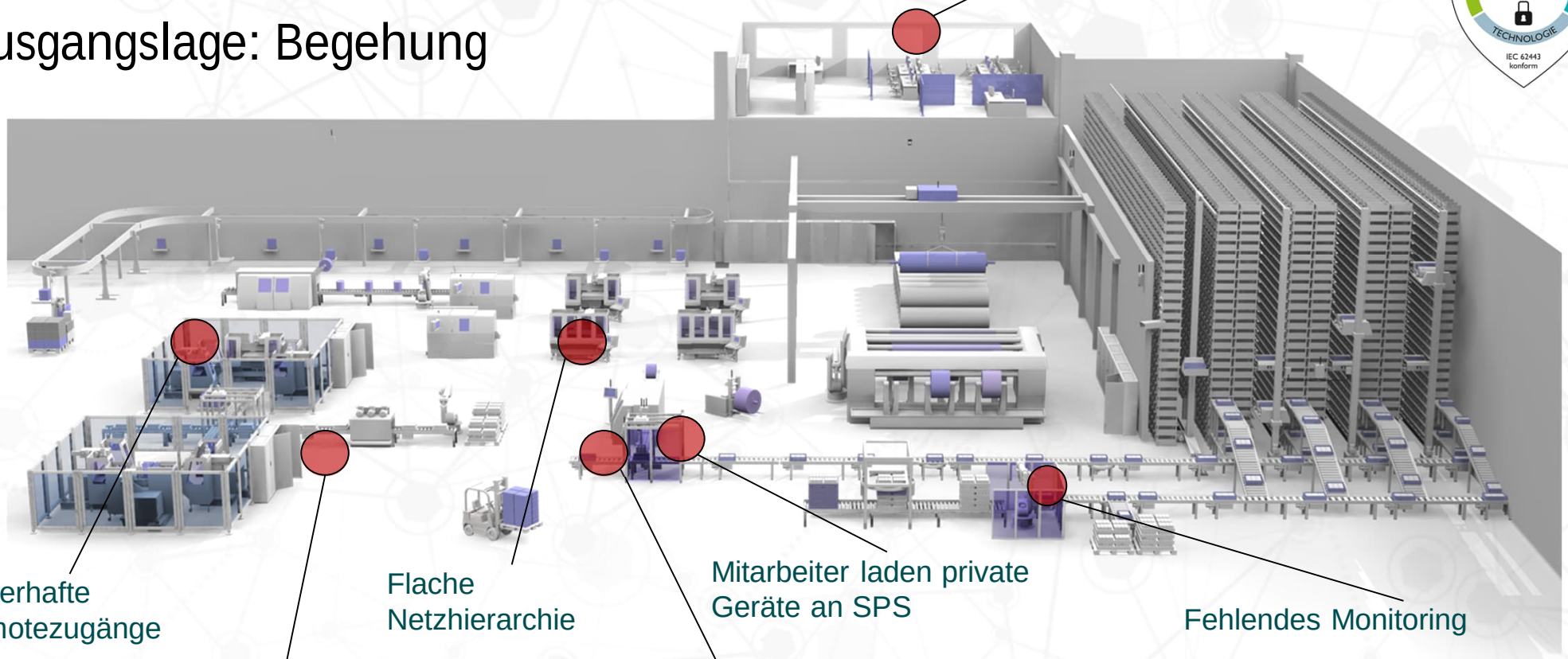


Security Konzept mit entsprechender Dokumentation der einzelnen Prozessschritte gemäß IEC 62443

PHOENIX CONTACT
INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

Ausgangslage: Begehung



Use Case: Vom Schutzbedarf zum fertigen Konzept

Anlageninformationen/ Strukturanalyse

„Ich kann nur schützen, was ich auch kenne“

- Unkenntnis der Anlage/ Bedrohungen (insb. Brownfield)
- Keine Basisabsicherung/ Grob fahrlässige Schwachstellen
- Beweispflicht gegen interne/ externe Manipulation

PHOENIX CONTACT
INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

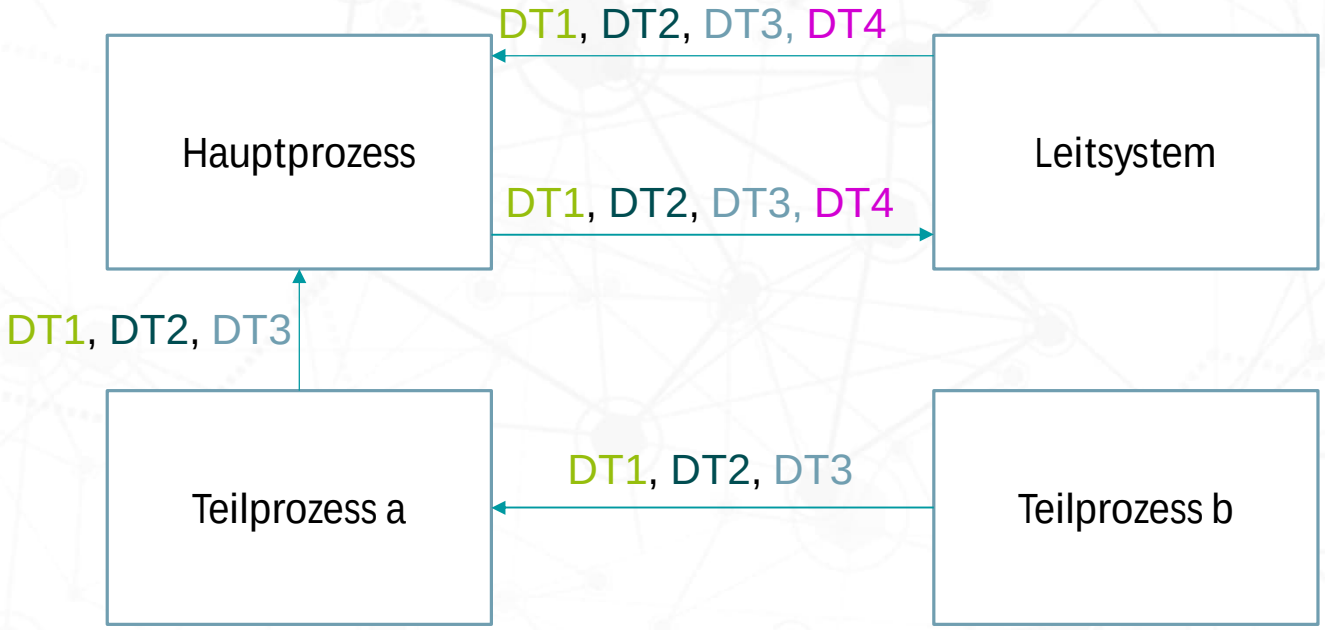
Schutzbedarfsanalyse

Fahrrad = 5000€ Schutzbedarf = hoch

Fahrrad = 50€ Schutzbedarf = niedrig

Use Case: Vom Schutzbedarf zum fertigen Konzept

Schutzbedarfsanalyse



Schutz Klasse	Schutzbedarf
1	Vernachlässigbar
2	Moderat
3	Hoch
4	Kritisch

Datentyp	Schutzbedarf
DT1	2
DT2	2
DT3	2
DT4	3

Use Case: Vom Schutzbedarf zum fertigen Konzept

Bedrohungsanalyse

Bedrohung
(Fahrraddieb)

+

Schwachstelle
(Fahrrad)

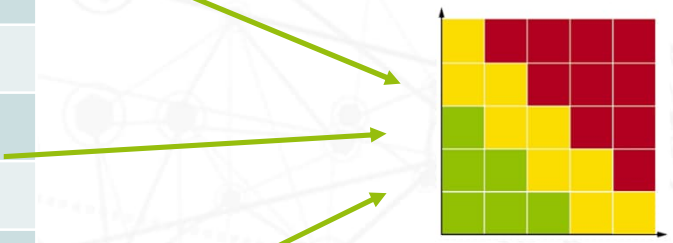
=

Gefährdung
(€-Schaden)

Use Case: Vom Schutzbedarf zum fertigen Konzept

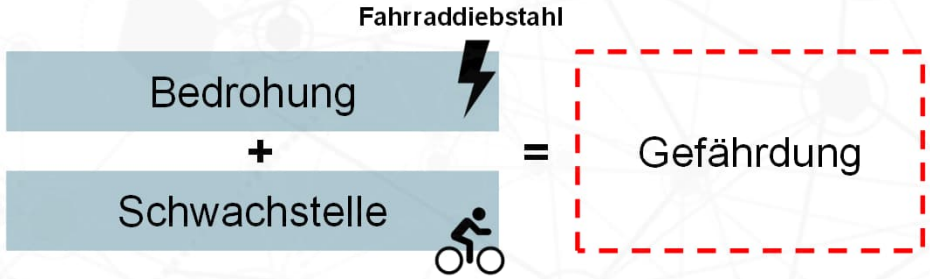
Bedrohungsanalyse

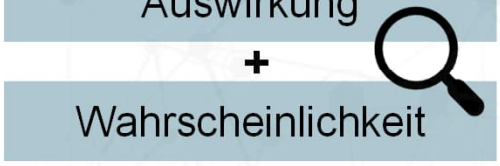
Bedrohung	Relevant
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	✓
Infektion mit Schadsoftware über Internet und Intranet	✓
Menschliches Fehlverhalten und Sabotage	✓
Kompromittierung von Extranet und Cloud Komponenten	✗
Social Engineering und Phishing	✓
(D)DoS Angriffe	✓
Internet-verbundene Steuerungskomponenten	✗
Einbruch über Fernwartungszugänge	✓
Technisches Fehlverhalten und höhere Gewalt	✓
Kompromittierung von Smartphones im Produktionsumfeld	✓



Use Case: Vom Schutzbedarf zum fertigen Konzept

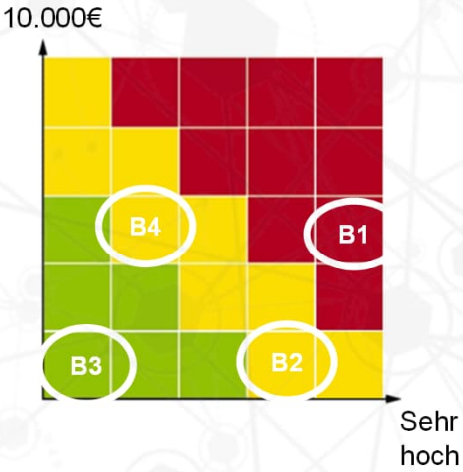
Risikoanalyse





=

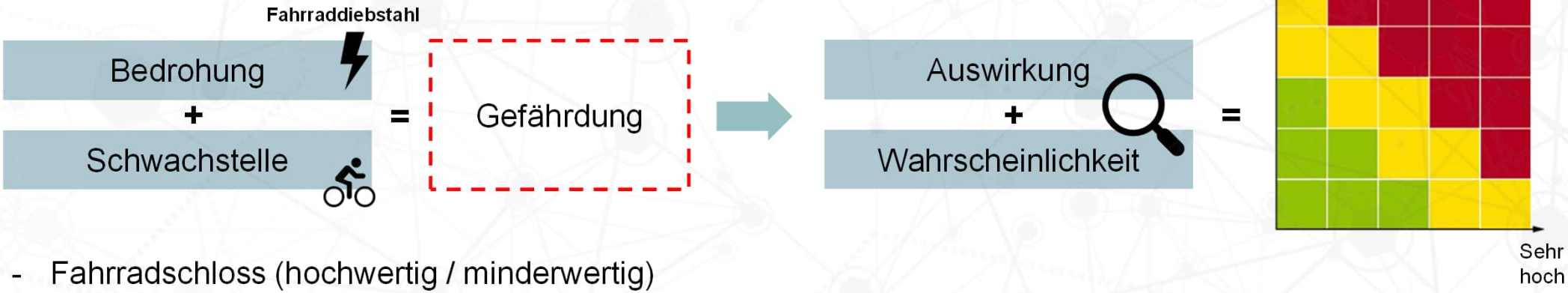
Risiko



Beispiel 1: 5000€ Fahrrad - abgestellt am Bahnhof	Risiko → sehr hoch
Beispiel 2: 50€ Fahrrad - abgestellt am Bahnhof	Risiko → mittel
Beispiel 3: 50€ Fahrrad - abgestellt in abgeschlossener Garage	Risiko → gering
Beispiel 4: 5000€ Fahrrad - abgestellt in abgeschlossener Garage	Risiko → mittel

Use Case: Vom Schutzbedarf zum fertigen Konzept

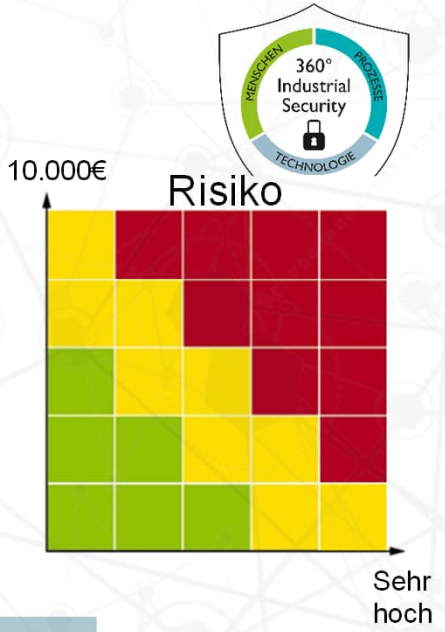
Risikobehandlung



- Fahrradschloss (hochwertig / minderwertig)
- Bus zum Bahnhof
- Versicherung
- Kamera / Alarmanlage an der Garage
- jemanden beauftragen aufzupassen
- Fahrrad verkaufen
- Risiko akzeptieren

Use Case: Vom Schutzbedarf zum fertigen Konzept

Securitykonzept



- Fahrradschloss (hochwertig / minderwertig) **[Basis-Absicherung]**
- Bus zum Bahnhof
- Versicherung
- Kamera / Alarmanlage an der Garage
- jemanden beauftragen aufzupassen
- Fahrrad verkaufen
- Risiko akzeptieren

Durchführen	Nicht Durchführen
x	-
-	x
x	-
x	-
-	x
-	x
?	?

Risk-Tool

PHOENIX CONTACT
INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

Risikoanalyse

IST (ohne Maßnahmen)

				Risikobewertung					
TID	Bedrohung - Szenario	betroffene Assets	Schaden	Wahrscheinlichkeit					Risiko
				Angriffsweg	Komplexität	Benötigte Rechte	Zeitfenster		
1	**Schadsoftware durch Wechseldatenträger**	Anlage	Beträchtlich	Anlage	Mittel	Keine	Mittel	Häufig	**Hoch**

SOLL (mit Maßnahmen)

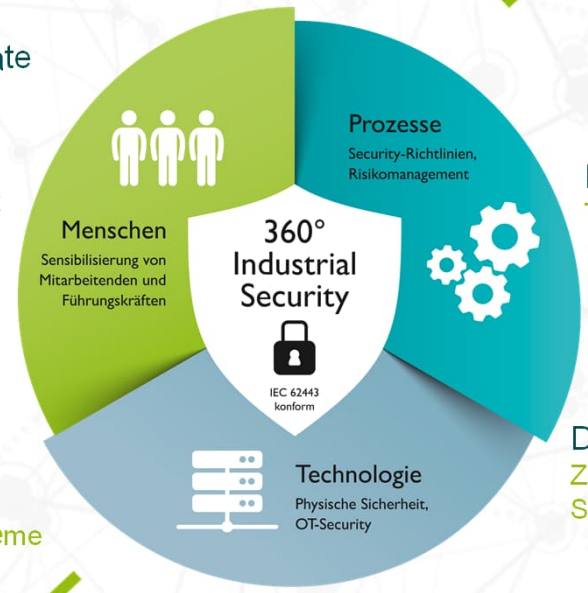
				Risikobewertung					
TID	Bedrohung - Szenario	betroffene Assets	Schaden	Wahrscheinlichkeit					Risiko
				Angriffsweg	Komplexität	Benötigte Rechte	Zeitfenster		
1	**Schadsoftware durch Wechseldatenträger**	Anlage	Begrenzt	Anlage	Hoch	User	Kurz	Mittel	**Gering**

PHOENIX CONTACT
INSPIRING INNOVATIONS

Use Case: Vom Schutzbedarf zum fertigen Konzept

Konzept

IEC 62443-2-4
Mitarbeiter
Zusicherung
Systemaufbau
Drahtlose Verbindungen
SIS (Safety Instrumented System)
Konfigurationsverwaltung
Fernzugriff
Ereignisse
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

Flache Netzhierarchie
Basierend auf Funktion und Schutzbedarf segmentiert

Sensible Informationen sind unverschlüsselt
VPN auch anlagenintern

Bei weiterführenden **Fragen** oder **Informationen** zu den Themen

Industrial Security, **Netzwerktechnik** oder **produktunabhängige Dienstleistungen**

Kompetenzfeld: Industrial Security

| Web: www.phoenixcontact.de/services

| E-Mail: services@phoenixcontact.de

| Telefon: 05281 946 5555

Vielen Dank

PHOENIX CONTACT
INSPIRING INNOVATIONS