Industrial Cyber Security: Herausforderungen und Lösungen für den Mittelstand

Breakout-Session

Deutsche Messe
Technology Academy

Caroline Neufert
Senior Manager
caroline.neufert@bearingpoint.com
+49 30 88004 2230

Bernd Koberwein
Head of Security Services
bernd.koberwein@bearingpoint.com
+43 664 81 61 874

April 2022

BearingPoint®

Inhalt

Herausforderungen

Lösungen

Diskussion

BearingPoint®

BearingPoint - Management und Technologie Beratung

€780m
Revenue

78
Countries in which BearingPoint served clients

11,360
Global alliance headcount

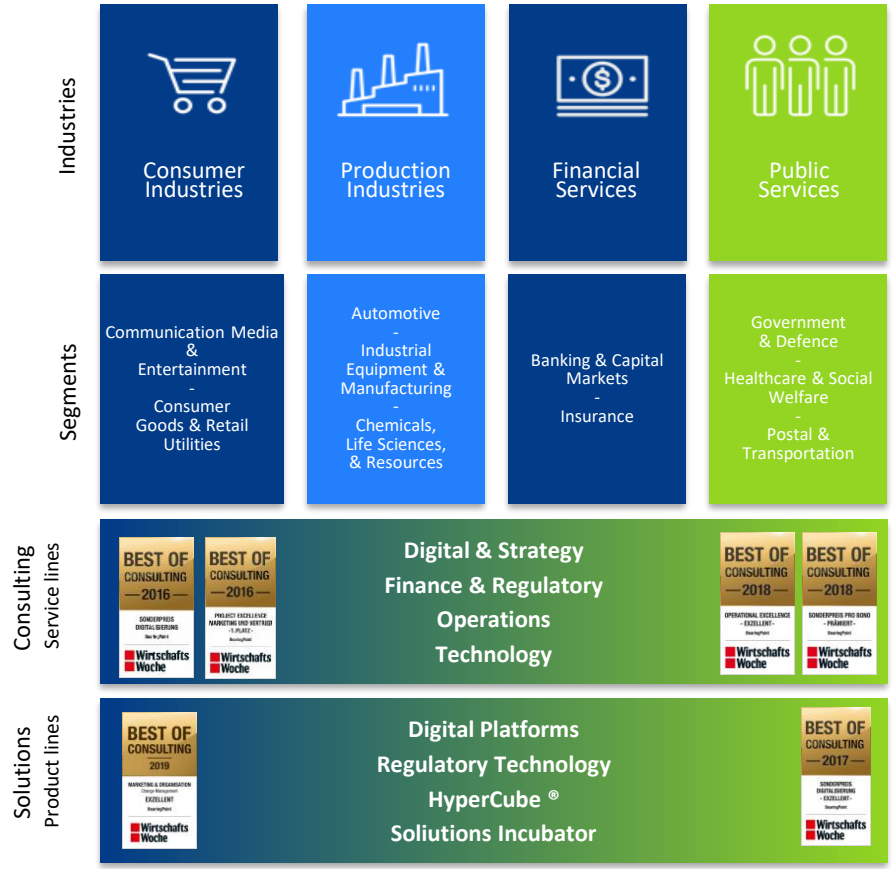
39
BearingPoint offices

174
BearingPoint Partners

22
Countries where BearingPoint has a direct presence

2009
Foundation date as BearingPoint European partnership

4,574
Global BearingPoint headcount



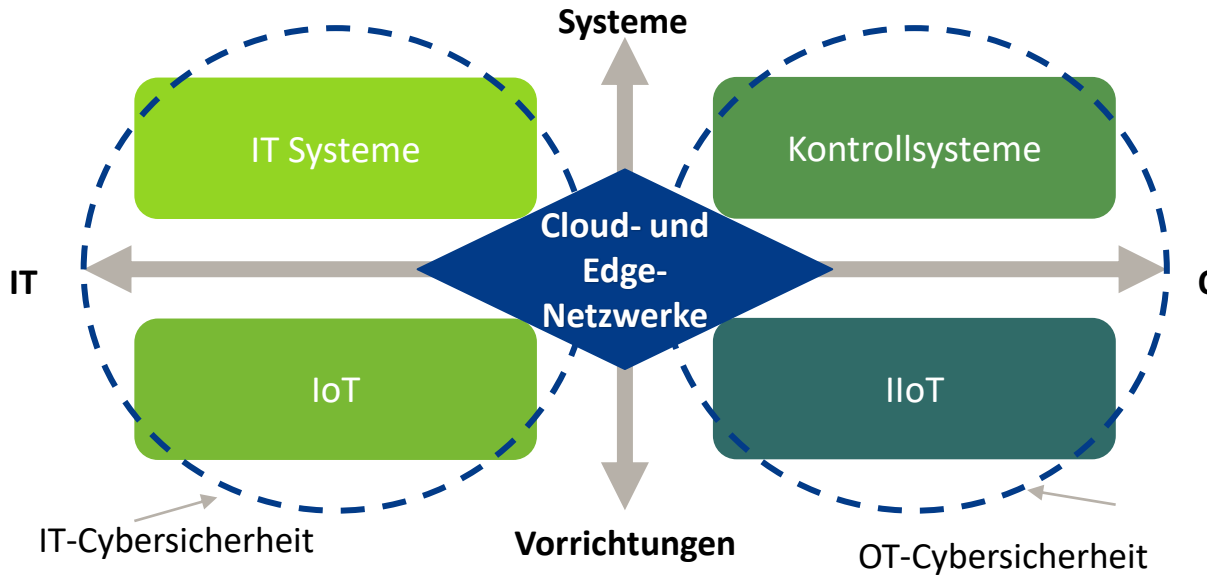
Abu Dhabi • Amsterdam • Berlin • Brussels • Bucharest • Casablanca • Chicago • Dallas • Dubai • Dublin • Düsseldorf • Frankfurt • Frederiksberg • Geneva • Graz • Hamburg • Helsinki • Iasi • Leipzig • Lisboa • London • Malmö • Milan • Moscow • Munich • Oslo • Paris • Prague • Shanghai • Sibiu • Singapore • Stockholm • Stuttgart • Timisoara • Turin • Vienna • Walldorf • Warsaw • Zurich

BearingPoint®

Unterschiede zwischen OT und IT

Informationen verwalten
Büro-PCs, Drucker, Drucker
Web/App/Daten/E-Mail-Server
TCP-Netzwerke

Tablets
Mobiltelefone
Sensor
Etc.



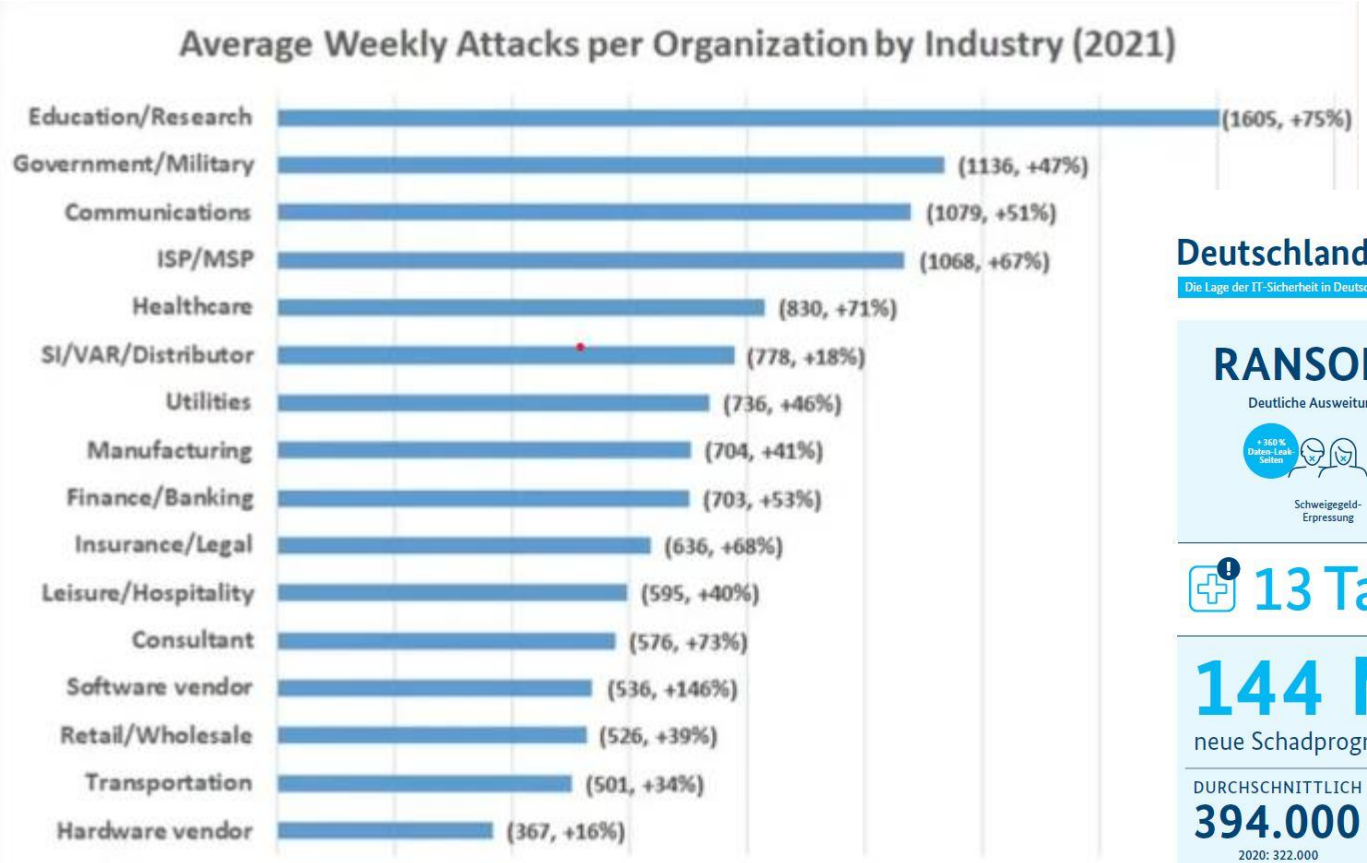
Verwaltung physischer Prozesse
Industriesteuerungen (SPS, DCS, SCADA) & I/Os
Gehärtete PCs und Server
Industrielle Netzwerke

Sensoren (Temperatur, Druck, etc.)
Kameras, Scanner, etc.
Eingebettete Systeme (Roboter etc.)

	IT	OT / ICS
Performance	Erledigt Aufgaben meist ohne garantiertes Zeitfenster Hohe Bandbreite	Erledigt Aufgaben in garantiertem Zeitfenster (Echtzeit) Geringe Bandbreite
Ressourcen	Umfassende Ressourcen wie CPU oder Speicher ermöglichen Installation von Security Software	Limitierte Ressourcen wie CPU oder Speicher erlauben nur bedingt Installation von Security Software
Verfügbarkeit	Wartungsausfall kann kurzfristig geplant werden, wenig Kosten Reboot der Systeme kein großes Problem	Wartungsausfall kann nur langfristig geplant werden, hohe Kosten Reboot im Produktionsumfeld problematisch
Safety	Spielt wenig Rolle	Spielt oft wichtige Rolle (Patchen mit Software verletzt Safety-Zertifizierungen)
Lebensdauer Komponenten	< 4 Jahre	20 – 25 Jahre

BearingPoint®

Cyberattacken auf Industrien – ein paar Statistiken I

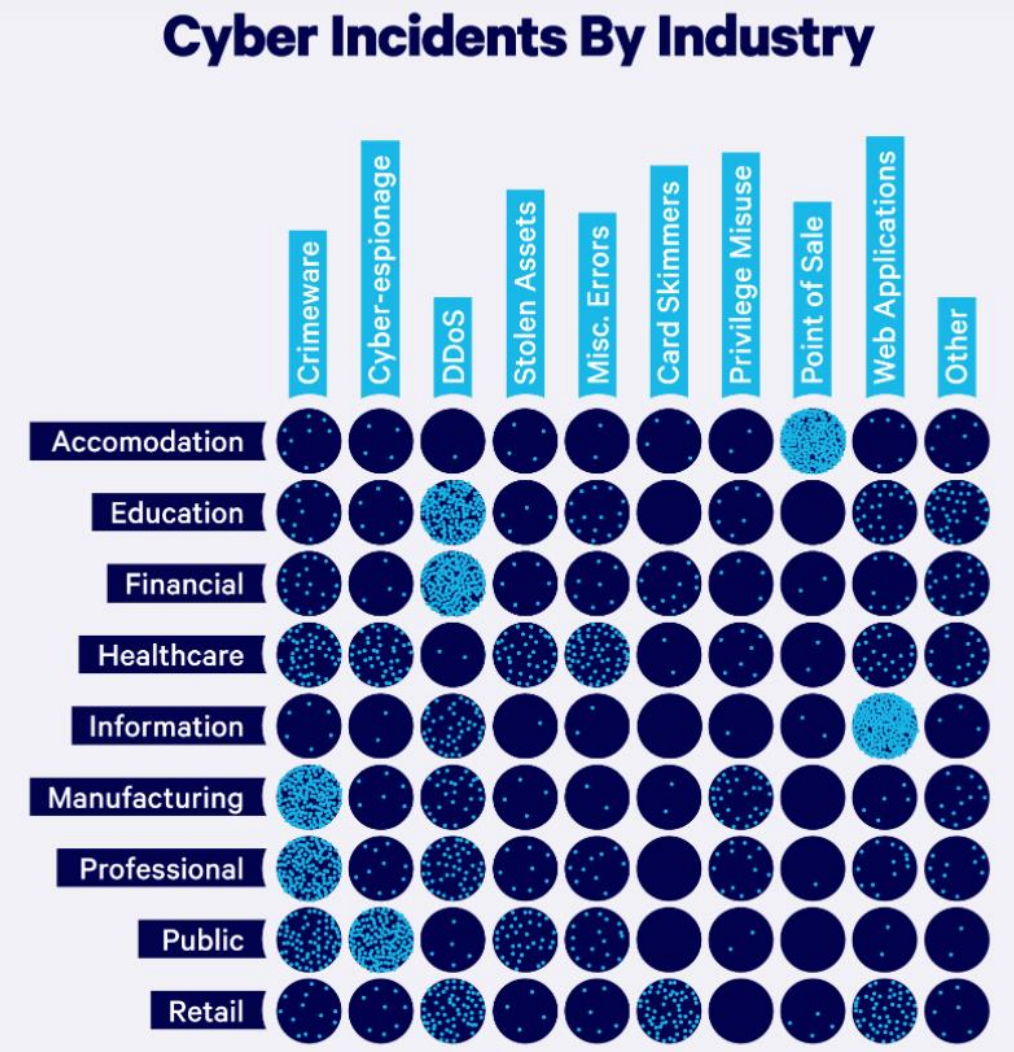


Quelle: Forbes 2022

Quelle: Lagebericht BSI, 2021

BearingPoint®

Cyberattacken auf Industrien – ein paar Statistiken II



Quelle: Ponemon, 2021

Quelle: Ponemon, 2021

BearingPoint®

Herausforderungen (Cyberrisk) für mittelständische Unternehmen

Industrial Cyber Security – eine Vielzahl von Herausforderungen:

- **regulatorischer Art**
- **organisatorischer**
- **prozessualer**
- **technischer Art**

Unklare Zuständigkeiten

Kundenumgebungen, die einer erheblichen Anzahl von Schwachstellen

(D)Dos Angriffe

Einbruch über Fernwartungszugänge

Einschleusen von Schadsoftware über externe Geräte

Infektion mit Schadsoftware über Internet oder Intranet

Kompromittierung von Smartphones im Produktionsumfeld

Technisches Fehlverhalten und höhere Gewalt

Sicherer Zugang zu Systemen und Daten
Verschiedene Betriebssysteme und Anwendungen, oft End of Life noch vorhanden
Anzahl an Netzwerken

Menschliches Fehlverhalten und Sabotage

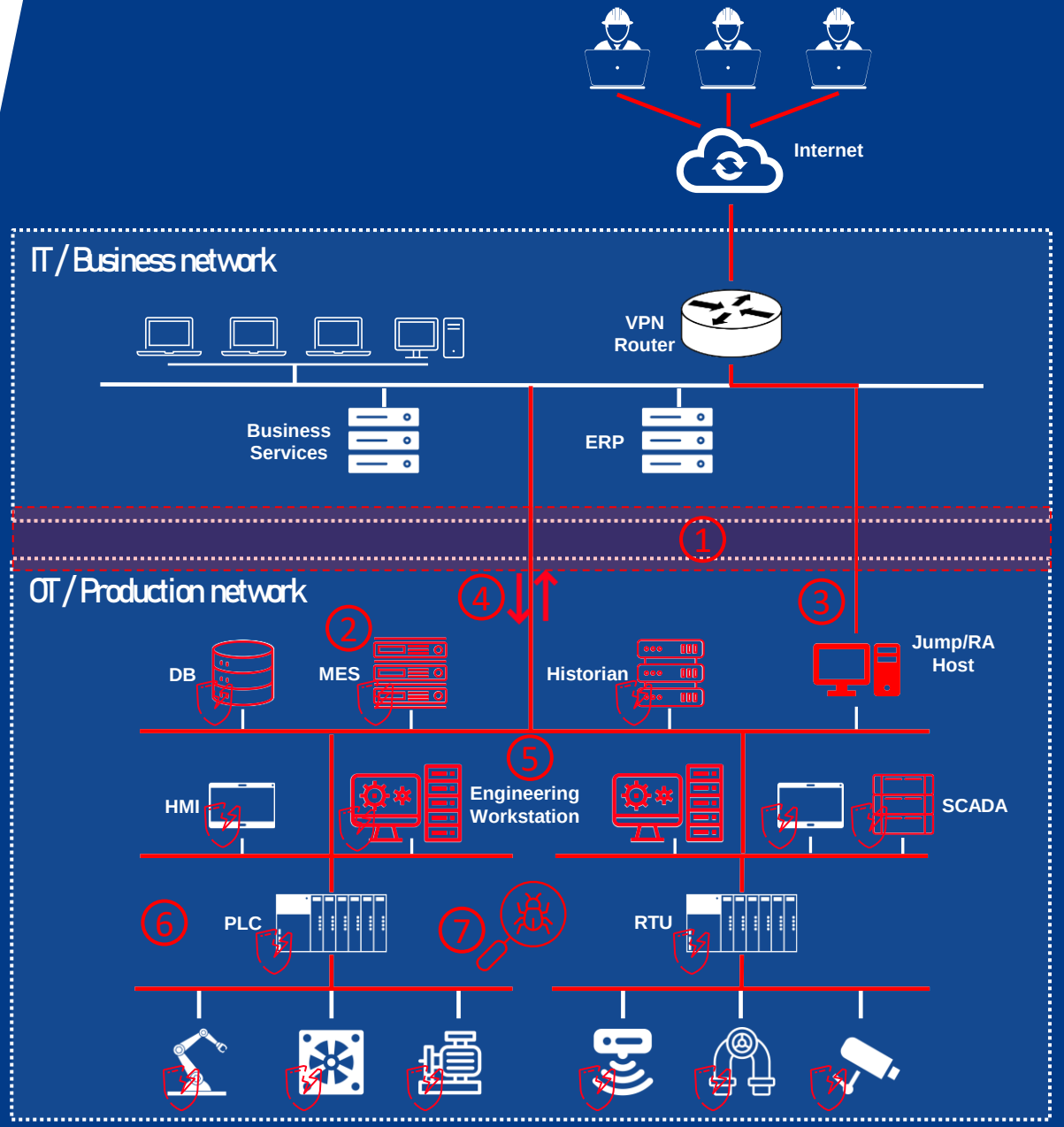
Social Engineering und Phishing/Vishing

Kompromittierung von Extranets und Cloud Komponenten

BearingPoint®

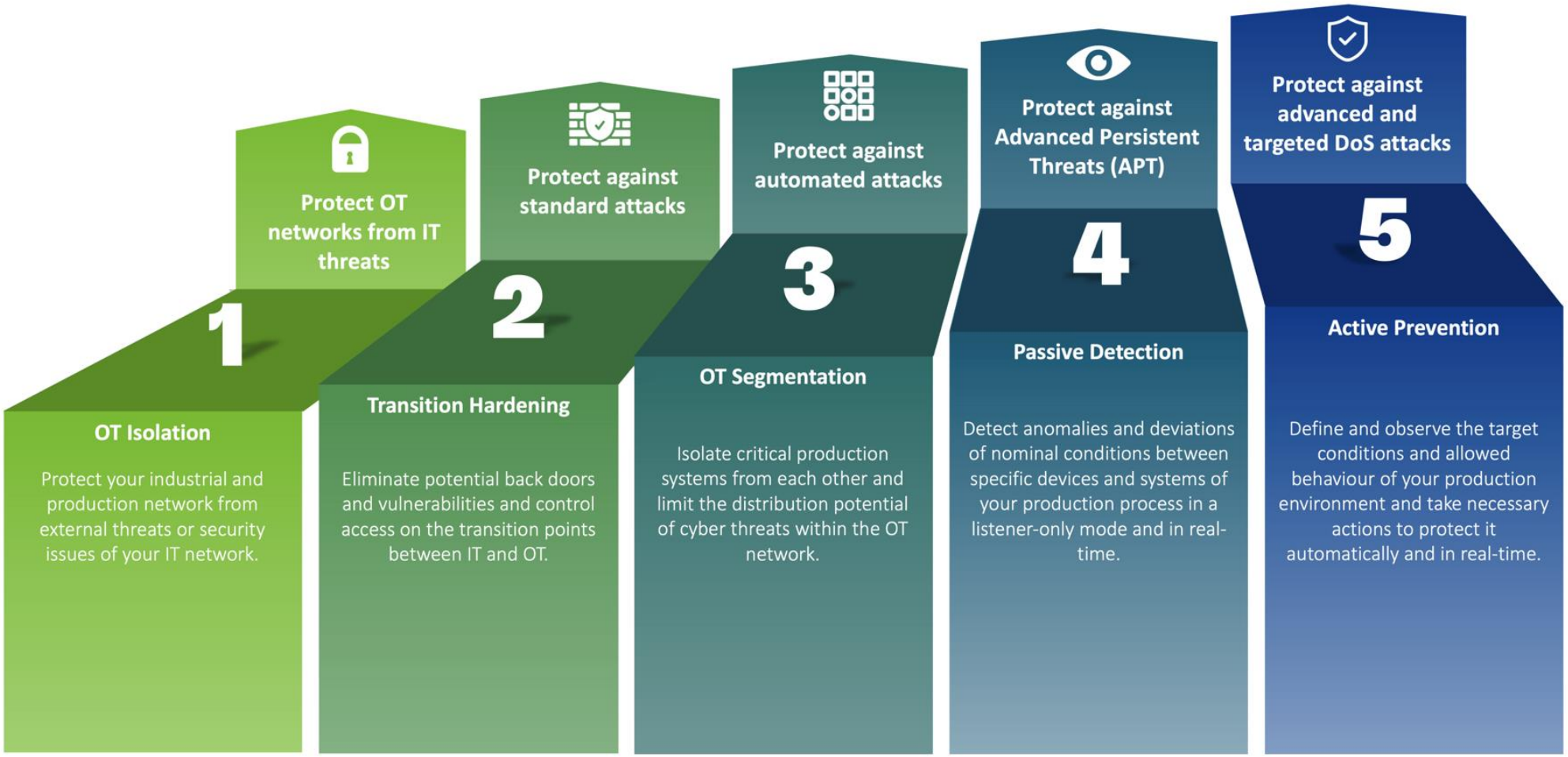
(Einige) technische Herausforderungen in OT Umgebungen

1. Fehlende/schwache Trennung IT/OT
2. Veraltete Systeme / Software (end of life), kein Patching möglich oder verfügbar
3. Unsichere Remote Zugriffe
4. Unreglementierter Datenverkehr
5. Keine/unzureichende Segmentierung
6. Kein Asset/Vulnerability Management
7. Kein Monitoring und Anomalieerkennung



BearingPoint®

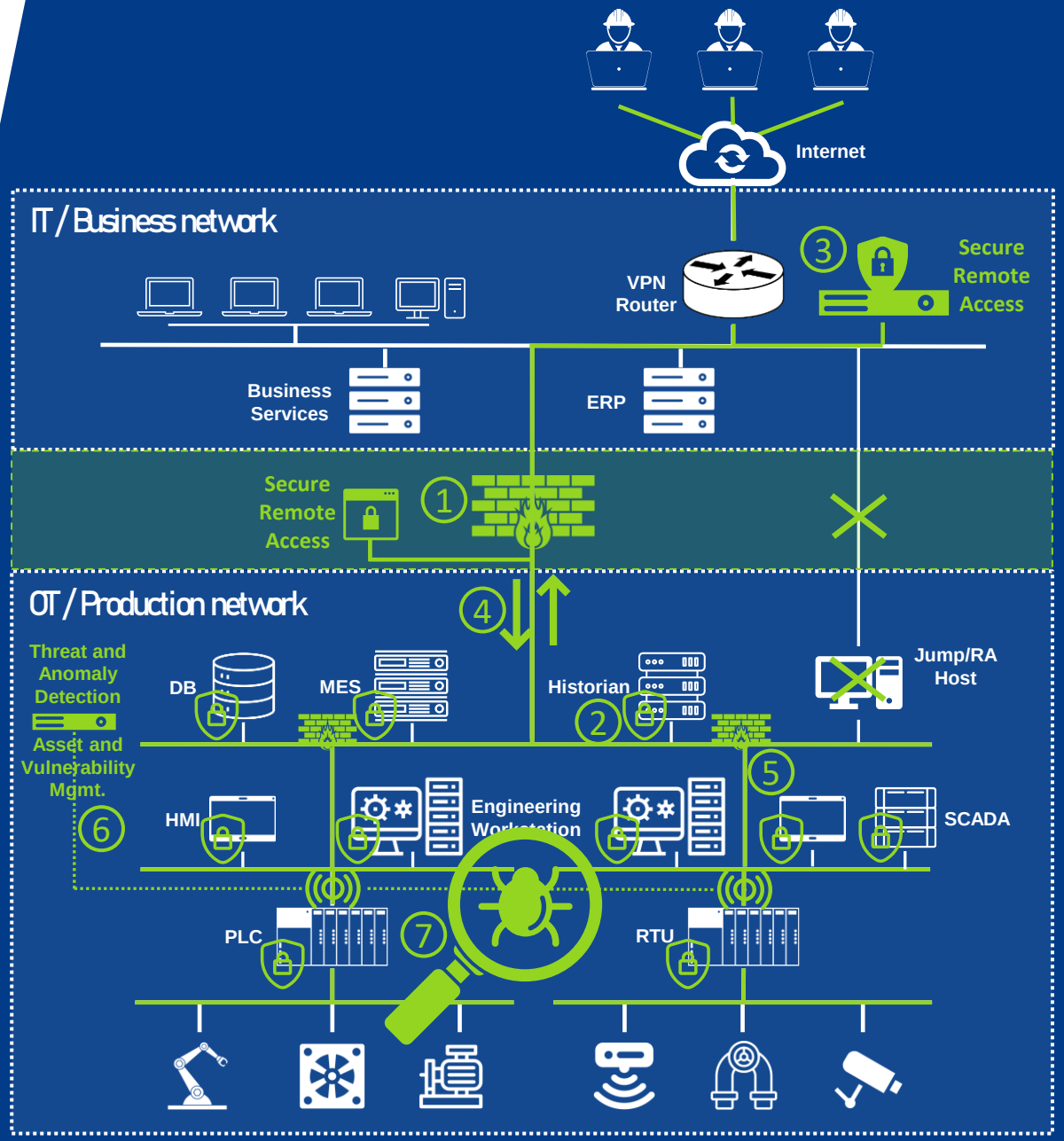
Stufenmodell zur Erhöhung der Security von OT Umgebungen



BearingPoint®

Technische Lösungsmöglichkeiten – ein Auszug

1. Trennung und Absicherung IT/OT
2. Virtual Patching und Intrusion Prevention
3. Secure Remote Access Lösung für OT
4. Absicherung des Datenverkehrs (Anti-Virus, Malware, Botnet, …)
5. Segmentierung der Produktionsebenen zur Eindämmung und Steuerung des Verkehrs
6. Identifikation aller Assets, deren Schwachstellen und Kommunikationswege
7. Monitoring der Prozessabläufe und Erkennung von Anomalien



BearingPoint®

Industrial Cyber Security Handbook

Free Download

https://industrialsecurity.at

BearingPoint®