M&P
CREATING
ADDED
VALUE

Building Cyber-Security

Relevanz und Herausforderung der OT-Security in Gebäuden

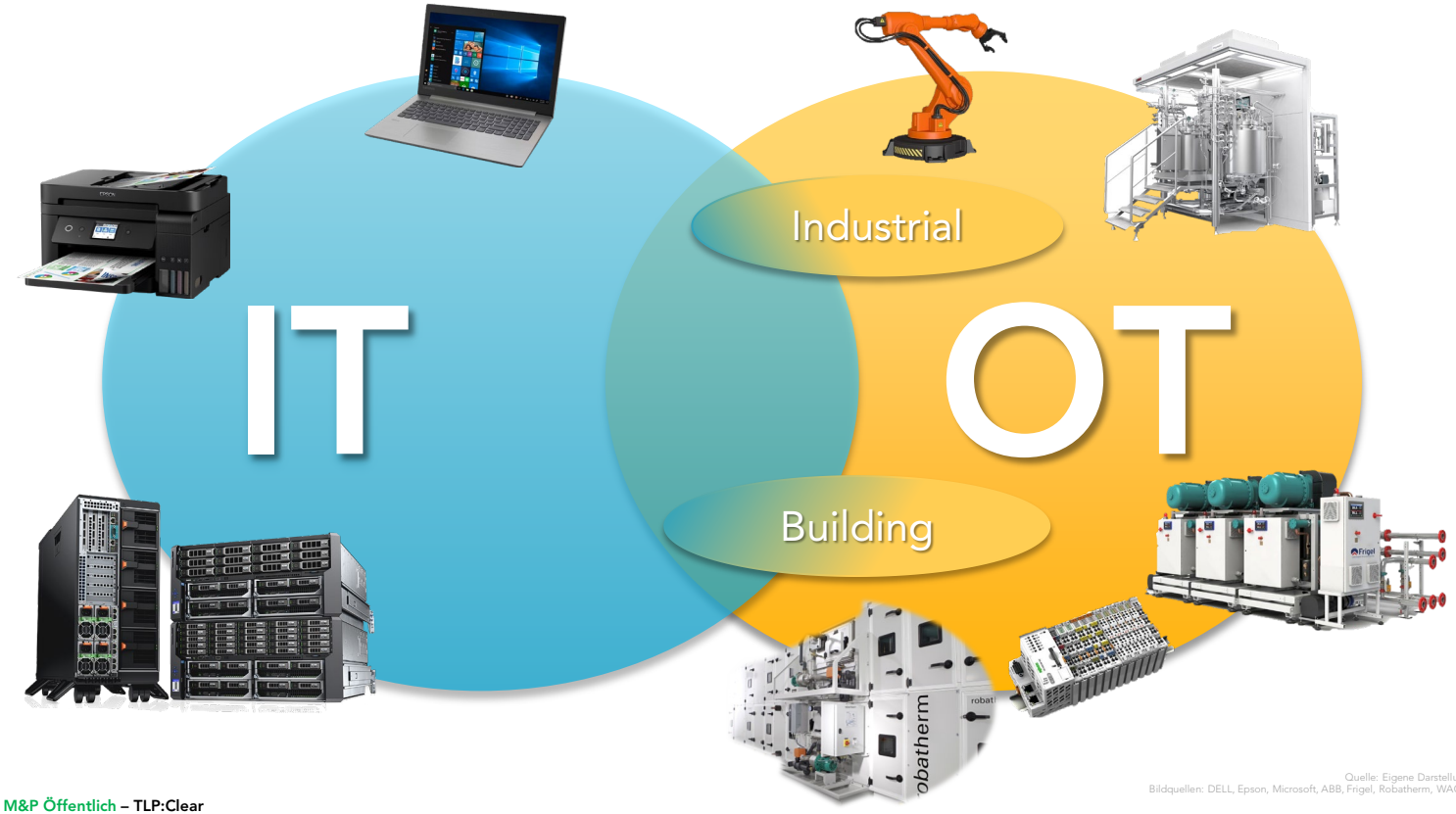
Innovationsgespräche M&P Gruppe Leipzig 2024

Wer sind wir?

M. Sc.
Nicolas Braun
Experte OT-Security Gebäudeautomation
M&P Braunschweig GmbH

B. Eng.
Bastian Helt
Teamleitung Gebäudeautomation Süd
M&P Braunschweig GmbH

Was ist OT – ist das so wie IT?



Quelle: Eigene Darstellung
Bildquellen: DELL, Epson, Microsoft, ABB, Frigel, Robatherm, WAGO

Warum brauche ich OT-Security?

Die Frankfurt University of Applied Sciences ist am 06.07.2024 gegen 20:00 Uhr Ziel eines ernstzunehmenden Hacker-Angriffs geworden. Trotz sehr hoher Sicherheitsvorkehrungen ist es den Kriminellen gelungen, sich Zugriff auf Teile der IT-Infrastruktur der Hochschule zu verschaffen. Als sofortige Sicherheitsmaßnahme wurden der externe Zugang zu unseren IT-Systemen gesperrt und einige Dienste abgeschaltet. Auch die Kommunikationsinfrastruktur wurde eingeschränkt. Darüber hinaus wurden die Polizei und die entsprechenden Behörden eingeschaltet.

Das Ausmaß des Angriffs kann zum jetzigen Zeitpunkt noch nicht abgeschätzt werden. Leider kann daher noch keine Aussage getroffen werden, wann die IT-Systeme und Dienste wieder im gewohnten Umfang zur Verfügung gestellt werden können.

Der Präsenzbetrieb an der Hochschule, einschließlich aller Lehrveranstaltungen, läuft weiter. Bitte beachten Sie, dass die Aufzüge in den Gebäuden aus Sicherheitsgründen nicht nutzbar sind.

Massive Angriffe aus Russland

Schwarz-Gruppe berichtet von 350.000 Hacker-Attacken täglich

07.10.2024, 00:43 Uhr

Ar

ICS/OT

Ransomware Hits Critical Infrastructure Hard, Costs Adding Up

Report finds most organizations have suffered financial impact of $500,000 or more from cyberattacks on cyber-physical systems over past year.

By Ionut Arghire
October 4, 2024

According to a new Claroty survey of 1,100 security professionals involved in OT, IoT, BMS, and IoMT (connected medical devices), about 45% of organizations suffered losses of $500,000 or more over the past year, while 27% disclosed losses of $1 million or more.

More than half of the respondents in the chemical manufacturing, power and energy, and mining and materials sectors have reported losses greater than $500,000 caused by cyber incidents over the past 12 months, Claroty's latest Global State of CPS Security report (PDF) shows.

Regierungsbehörden der Vereinigten Staaten, Kanadas und des Vereinigten Königreichs geben nach einer Reihe von **Angriffen offensichtlich russlandfreundlicher Hacktivisten** auf industrielle Kontrollsysteme (ICS) und **andere Systeme der Betriebstechnologie (OT) Empfehlungen für kritische Infrastrukturen.** (Security-Week, 02.05.2024)

Was kann ohne OT-Security passieren?

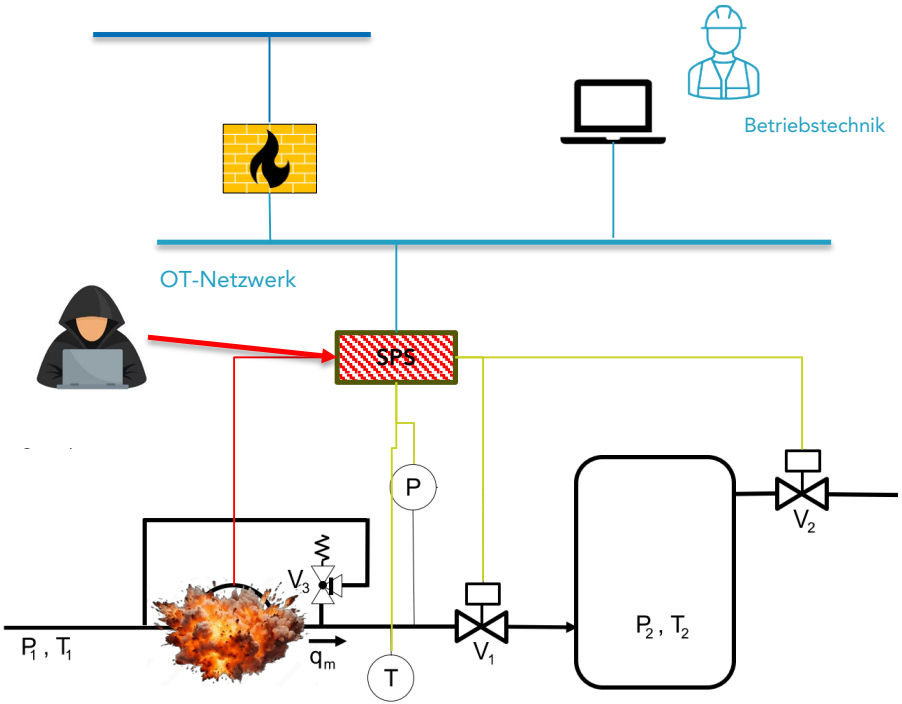
Unkalkulierbares Risiko

Ausfall von Geschäftsprozessen durch manipulierte Unterstützungsprozesse

Finanzieller Schaden

Vertragsstrafen

Abfließen von Geschäftsgeheimnissen



System- oder Produktionsausfälle

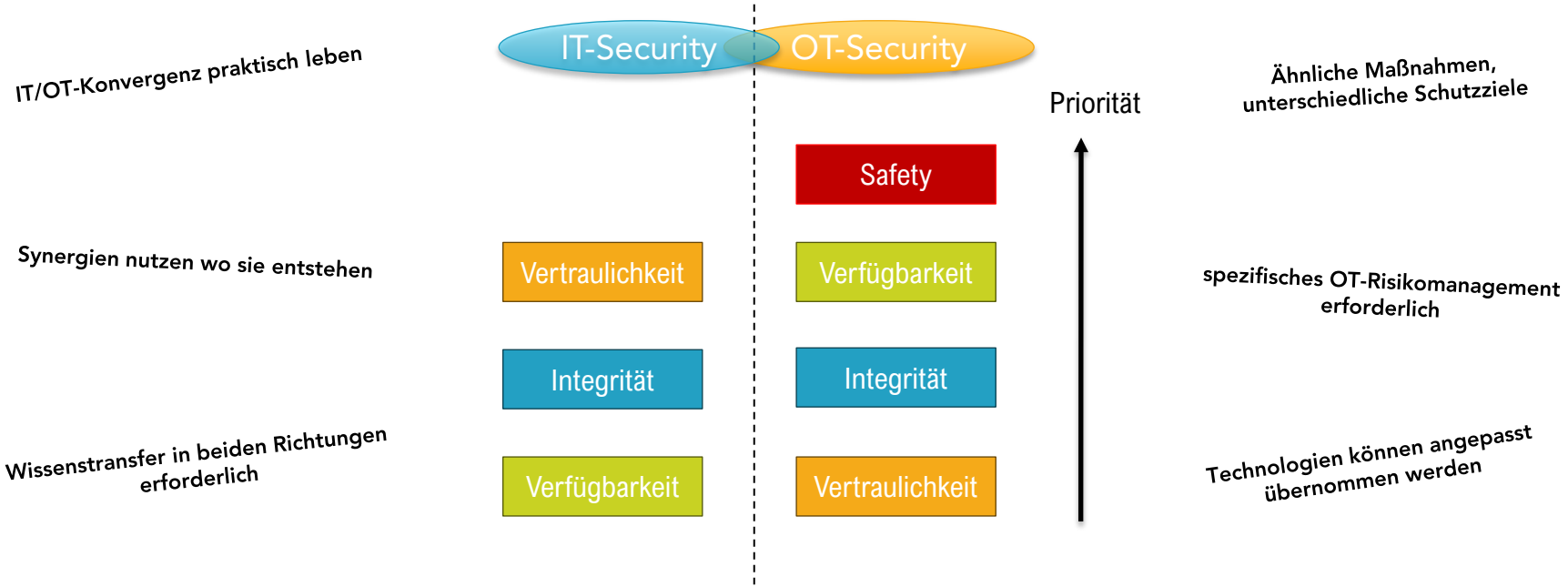
Mechanische Zerstörung von Komponenten und Systemen

Gefährdung von Mitarbeitern oder unbeteiligten Dritten

Reputationsschaden

Quelle: Eigene Darstellung

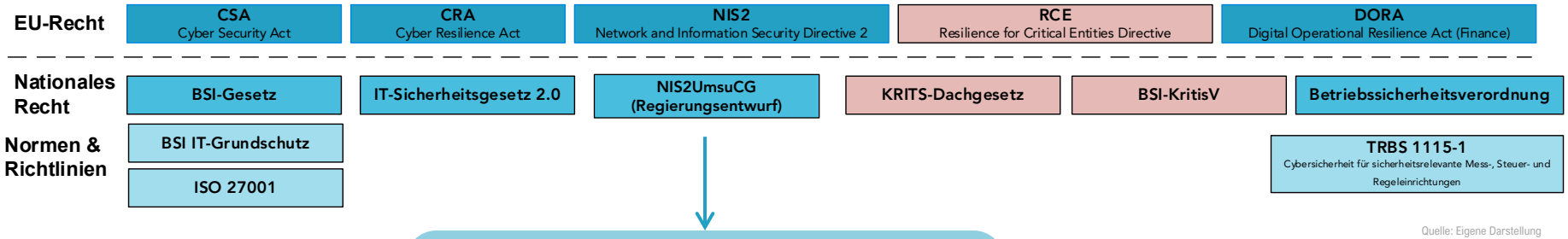
Wenn das in der IT funktioniert, bekommen wir das in der OT auch hin?



Quelle: Eigene Darstellung

Wer braucht OT-Security überhaupt? (Betrifft mich das?)

Jeder ist betroffen, die Frage ist nicht OB man gehackt wird, sondern WANN.



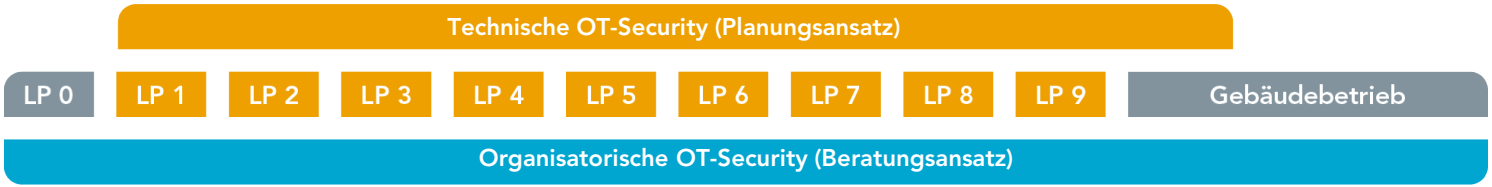
Quelle: Eigene Darstellung

- Betroffenheit: ca. 30.000 Organisationen in D
- **+1600%** mehr als unter IT-SiGe 2.0
- greift ab 50 Mitarbeitern
- Mindeststrafen 7 Mio €
- persönliche Haftung der GF & Prokuristen möglich

Was bieten wir?

» Unser **Planungsansatz** umfasst alle Aspekte der technischen OT-Security:
- Anforderungen: Grundlegende Betrachtungen zu **Sicherheitsanforderungen** der Gebäudeautomation (GA)
- **Technische Lösungen**: Entwicklung von Lösungen für den Aufbau des Gebäudeautomationsnetzwerkes
- Lösungskonzepte: Konzepte für **Netzwerk- und Sicherheitsmanagement**

» **Projektspezifische,** szenariobasierte **Testumgebung** – „Planung praktisch greifbar machen“



Quelle: Eigene Darstellung

» Unser **Beratungsansatz** beinhaltet:
- **Bedarfsermittlung** an die OT-Security (Sicherheitskonzept)
- Projektbegleitender **Risikomanagementprozess**
- **Betreiberkonzepten** für den Betrieb und die Wartung
- Konzepte für **Patch- und Änderungsmanagement**
- Vorgehensweisen bei Systemkomponenten **am Ende von deren Lebenszyklus**

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT.

B. Eng.
Bastian Helt
Teamleitung Gebäudeautomation Süd
M&P Braunschweig GmbH

Kontakt
Fon +49 531 256 02 436
Mobile +49 151 727 00 800
Mail bastian.helt@mp-gruppe.de

M. Sc.
Nicolas Braun
Experte OT-Security
Gebäudeautomation
M&P Braunschweig GmbH

Kontakt
Fon +49 621 72756 44
Mobile +49 173 7378833
Mail nicolas.braun@mp-gruppe.de