



**Aktuelle Entwicklungen bei IoT mit  
Fokus auf industrielle IoT-Security**



getragen von

bayern  innovativ  
Innovation leben.



# Wir vernetzen, fördern und beraten bayerische Unternehmen

Geschäftsstelle Forum MedTech Pharma e.V.  
(Europas größtes Netzwerk in der Gesundheitsbranche),  
ZD.B Digitale Gesundheit

Geschäftsstelle Cluster Automotive,  
Kompetenzstelle Elektromobilität,  
ZD.B vernetzte Mobilität

Geschäftsstelle Cluster Neue Werkstoffe, NiM bayern,  
Koordinierungsstelle Additive Fertigung,  
Netzwerk textile Innovation

Geschäftsstelle Cluster Energietechnik,  
ZD.B Digitalisierung im Energiebereich

**ZD.B Zentrum Digitalisierung.Bayern**  
(11 wirtschaftsorientierte Themenplattformen  
darunter Cybersecurity)

**ZD.B**  
CYBER-  
SECURITY

Förderlotse und Projektträger, Anlaufstelle und  
Hotline für die Bayerische Forschungs- und  
Innovationsagentur

Geschäftsstelle Patentzentrum Bayern

Technologie- und Innovationsmanagement,  
Digitale Innovationsplattform

Technologie- und Innovationsvermarktung,  
Messegemeinschaftsstände Bayern,  
Enterprise Europe Network

Geschäftsstelle Bayerisches Zentrum für  
Kultur- und Kreativwirtschaft – bayernkreativ

# Vision der TP Cybersecurity

**Unsere Vision ist ein Bayern mit dem höchsten Grad an Cybersecurity und den wenigsten Schadensfällen, mit den resilientesten Unternehmen und Organisationen. Cybersecurity als Basis für die digitale Wirtschaft.**

# ZD.B-Themenplattform Cybersecurity – auf einen Blick

| Mission                                                                                                                                                                                                                 | Themenschwerpunkte                                                                                                                                                                                                                                         | Aktivitäten                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>IT-Sicherheit in Bayern nachhaltig stärken von</p> <ul style="list-style-type: none"> <li>- der Awareness der Menschen,</li> <li>- den IT-Security-Technologien bis zur</li> <li>- Überwachung im Betrieb</li> </ul> | <ul style="list-style-type: none"> <li>• IoT-Security in der Industrie (Sicherer Betrieb)</li> <li>• IT-Security im Landmanagement</li> <li>• Security &amp; Privacy im Smart Home</li> <li>• IT-Security als Teil von Corporate Responsibility</li> </ul> | <ul style="list-style-type: none"> <li>• Awarenesskampagne forcieren</li> <li>• Online Event-Reihe: IIoT Security Best Practice</li> <li>• It-sa: Virtueller Messeauftritt im Juni und vor Ort im Oktober</li> <li>• Tech Days MUC</li> <li>• Veranstaltungsreihen #DigitalDialog mit HWK, IHK</li> <li>• Förderaufruf Cybersecurity</li> </ul> |

**Ansprechpartner:** Dr. Robert Couronné – [robert.couronne@bayern-innovativ.de](mailto:robert.couronne@bayern-innovativ.de)

**Wissenschaftliche Sprecherin:** Prof. Dr. Claudia Eckert, Institutsleiterin Fraunhofer AISEC

**Wirtschaftlicher Sprecher:** Dr. Thomas Nowey, CISO Syskron GmbH/Krones AG

# Internet of Things

Vom

- Internet der Computer über das
- Internet der Menschen zum
- Internet der Dinge

Bild im Internet verfügbar

<https://medium.com/@thinkwik/why-people-are-talking-so-much-about-iot-is-iot-really-future-74d5008fe2af>

# Internet of Things im Smart Home

Analyse der Smart Home Devices in 2019:

- 26 Milliarden vernetzte Geräte im Einsatz
- jeder Mensch nutzt mehr als 3 IoT-Devices
- erst 0,06 % der Dinge sind mit dem Internet verbunden

➔ enormes Wachstumspotenzial für IoT, bis 2025 zu 75 Milliarden IoT-Devices

(Quelle: Software-Entwicklungsunternehmen Perfectial 3 zitiert nach  
<https://www.ingenieur.de/technik/fachbereiche/ittk/die-3-wichtigsten-iiot-security-trends/>)

# Internet of Things im Smart Home

## Vernetzte Hausgeräte

- Digitale Assistenten
- Audio/Video/TV
- Schließsysteme
- Alarmanlagen
- Life Style Anwendungen

Bild im Internet verfügbar

<https://medium.com/@thinkwik/why-people-are-talking-so-much-about-iot-is-iot-really-future-74d5008fe2af>

# Internet of Things industriellen Umfeld

## Vernetzte

- Maschinen
- Datenbanken
- Unternehmens-IT und -OT
- Infrastrukturkomponenten  
bei Stromnetzen

➔ Neue Angriffsflächen

Bild im Internet verfügbar

<https://www.domino-printing.com/de-de/blog/2020/industrial-internet-of-things-revolutioniert-prozesse>

# Industrial Internet of Things – bietet neue Angriffsmöglichkeiten

- Bevorzugtes Aktionsfeld krimineller Organisationen aber auch Geheimdienste
- Erpressung und Sabotage gegenüber Unternehmen

Erpressung via

- Offenlegung von Geheimnissen
- Verschlüsselung von Datenträgern
- Manipulation an kritischen Infrastrukturen  
→ Versorgungsengpässe

→ IoT braucht Cybersecurity

Bild im Internet verfügbar

<https://iiot-world.com/ics-security/cybersecurity/four-most-hard-to-solve-iiot-security-issues/>

# Sicherheit vernetzter Systeme

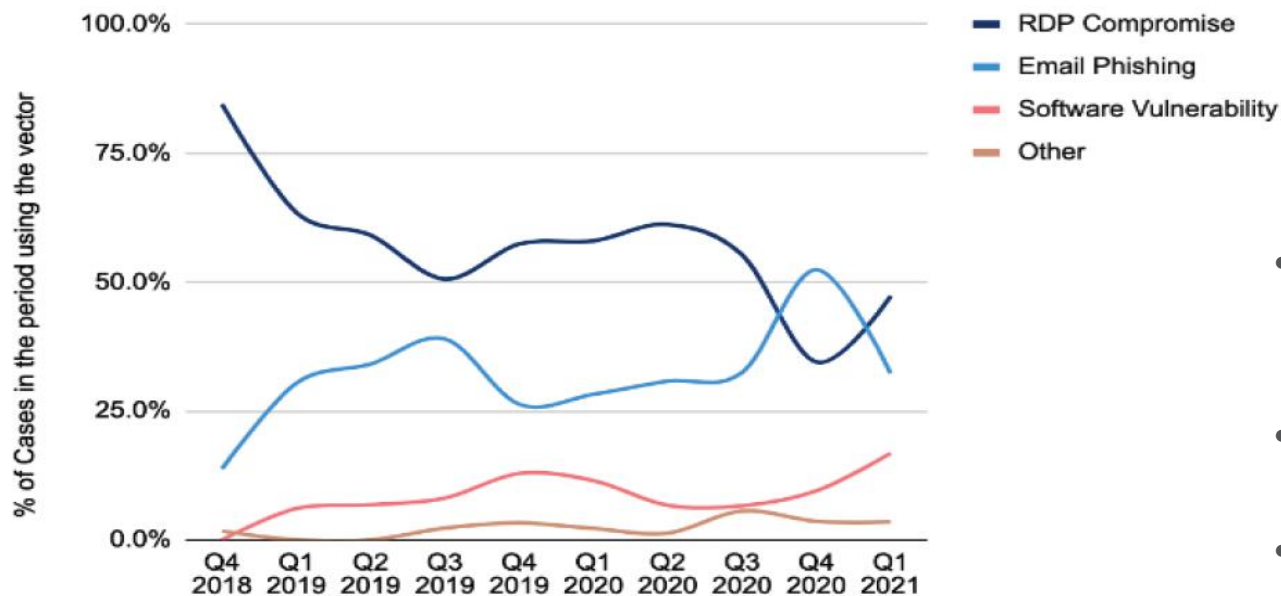
## Best Practice im industriellen Internet of Things (IIoT)

- Secure Remote Services – Voraussetzung digitaler Geschäftsmodelle
- Secure Operations – Anomalieerkennung
- Secure Apps
- Secure Product Development by Governance (IEC )
- Qualifikation schärfen und Awareness wachhalten



# Haupteinfallstor Remote Service

Ransomware Attack Vectors



Quelle: Coveware Ransomware Report Q1/2021

- Umfrage des VDMA (Verband Deutscher Maschinen- und Anlagenbau e. V.): Maschinenbauer sehen Risiko für ein ungewolltes Eindringen dritter Personen über Remotezugänge für unwahrscheinlich.
- Größte Einfallstore für Ransomware-Angriffe sind aber gerade Remote-Desktop- oder andere Remote-Zugänge.
- Wesentlich hierfür: Zugriffsschutz nur mit Benutzernamen und Passwort.
- Sicherheit funktioniert nur in der Zusammenarbeit zwischen Hersteller und Betreiber.

# Herausforderungen Remote Services - aus Sicht eines „Hidden Champion“

## Technisch

- Zunehmende Vernetzung von Systemen, die nicht dafür vorgesehen waren -> Industrie 4.0
- Verwendung von teilweise sehr veralteten Betriebssystemen
- Kein Patchmanagement

## Organisatorisch

- Einstellungen wie „Was soll schon passieren?“
- Systeme mit einfachen Passwörtern ins Internet stellen

## Awareness Inhouse

- IT wird zu spät über Neuinstallation von Maschinen informiert  
Kein Budget für neue Maschinen, wenn die „alte“ noch Lläuft
- Lösungen sollen für alle Menschen funktionieren

Quelle: Grotz-Beckert, 2021

# Remote Services – „mein Haus, meine Regeln“

Vorgaben durch die Entwicklung:

- Keine Remotewartung mehr über USB Ports - USB Ports werden gesperrt

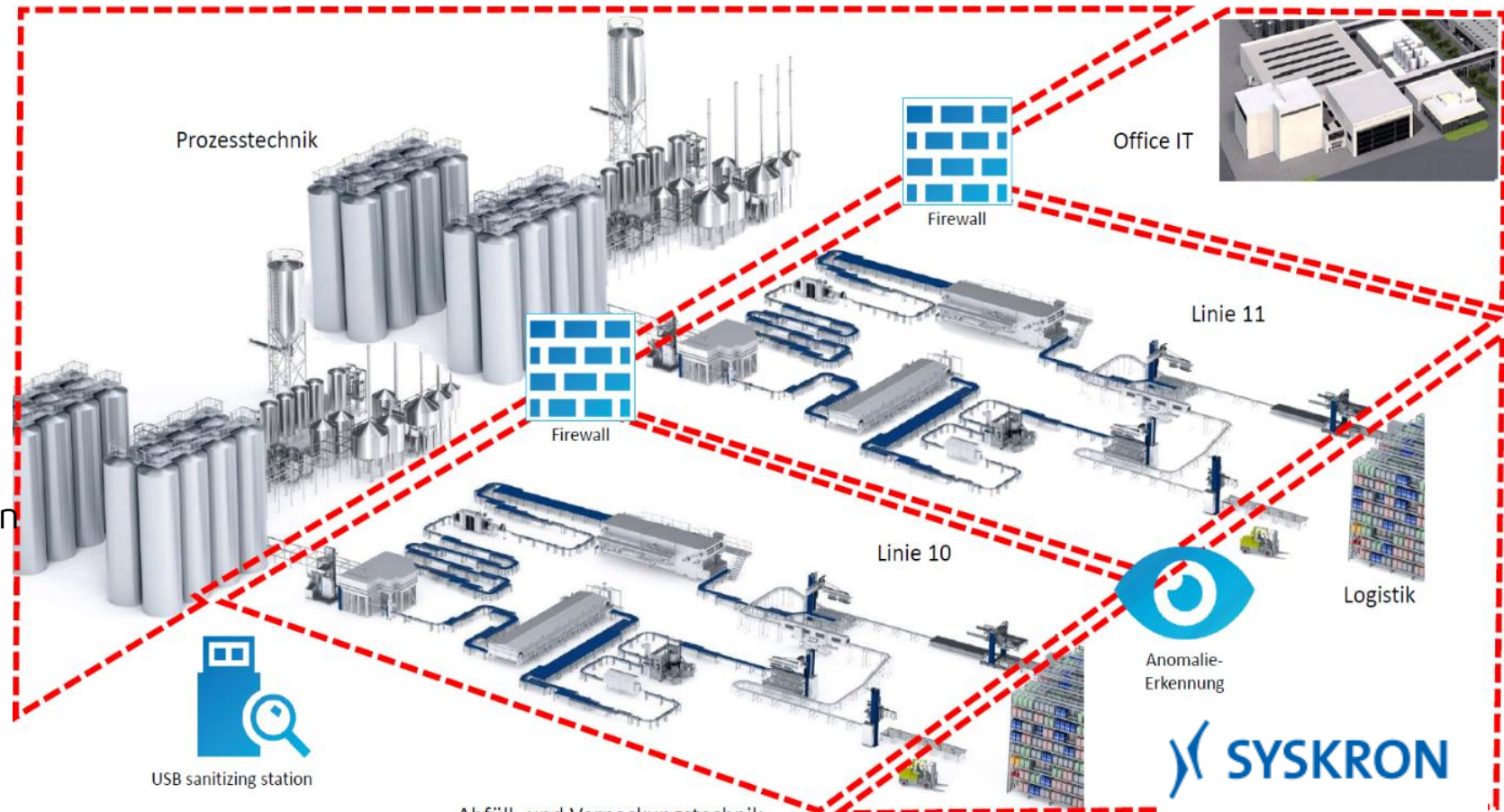
Vorgaben durch den Bereich Informationsmanagement:

- Offline Virenschanning der Maschinen PCs vor Inbetriebnahme und nach Wartungsarbeiten
- Jede Maschine bekommt eine eigene Firewall mit eigenem Regelwerk
- Platzierung der Firewall in separatem Baukasten mit separater Stromversorgung
- Administration der Firewall erfolgt durch die IT nach dem „Least Privilege “ Prinzip
- Mikrosegmentierung statt eigenem Produktionsnetzwerk

# Anomalieerkennung in der Industrie

- Produktionsanlagen häufig schwach geschützt
- Sinnvolle „Zonierung“ des Produktionsnetzes durch Firewalls ist Minimalanforderung
- IT Sicherheit = Aufgabe des täglichen Betriebs der Produktion
- Anomalieerkennung enorm wirkungsvoll aber Alarmer müssen täglich von Personal geprüft werden
- Neben der Technik auch menschliche Schwachstellen berücksichtigen

➔ **Sicherheit ist tägliche Betriebsaufgabe!**



Quelle: Syskron GmbH

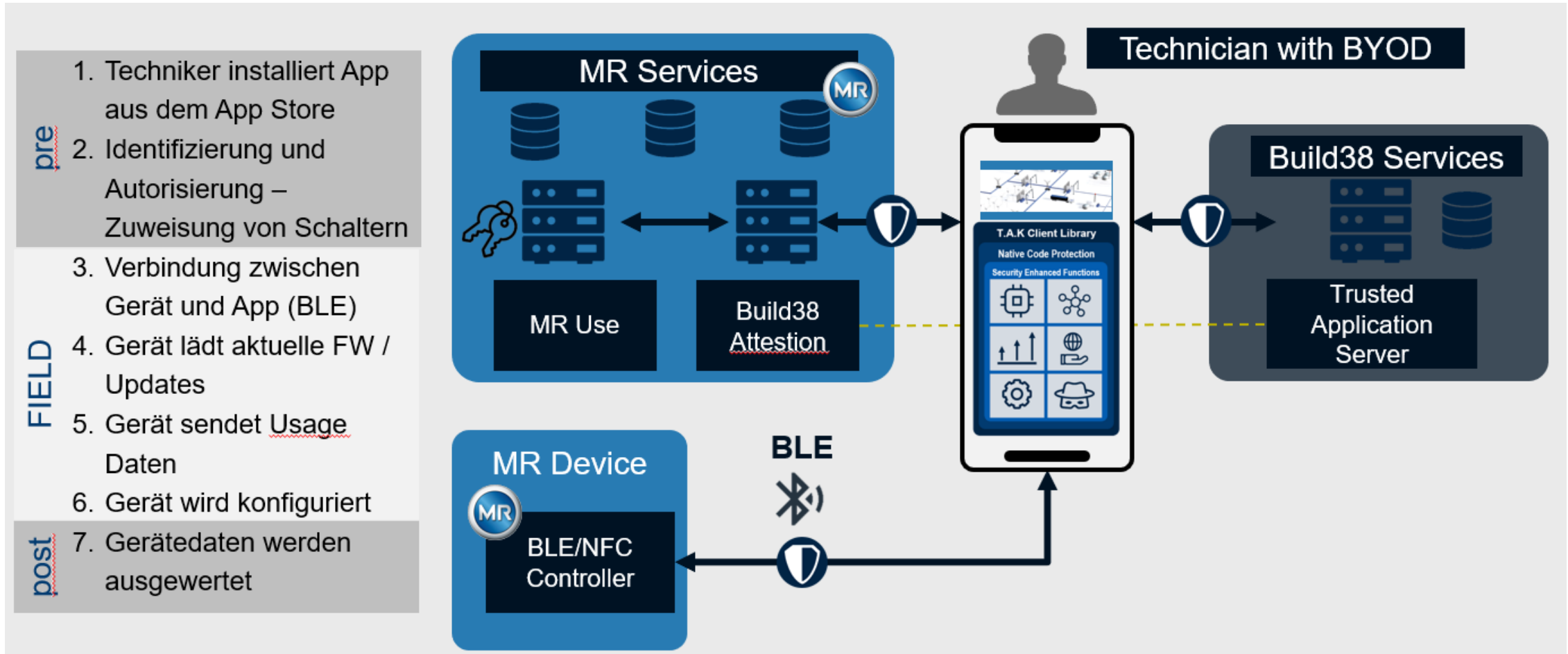
# Sicherer Zugriff auf Steuerungs-(IoT-)komponenten in Verteilnetzen

Elektrische Geräte wie Transformatoren mit Lastschaltern werden im Verteilungsnetz zum IoT-Gerät

- Für eine sichere, zuverlässige und kostengünstige Kommunikation kann das eigene Endgerät (Smartphone, Tablet) genutzt werden
- Sicher Verbindung zum Transformator notwendig
- Zuverlässige und nachverfolgbare Authentifizierung und Autorisierung von Verbindungsanfragen (auch ohne Internetverbindung)
- Berechtigungsmanagement über verschiedene, eindeutig identifizierbare Nutzer und Zeitfenster

Bild im Internet verfügbar

# Lösungsarchitektur als Referenz für die Industrielle IoT



Quelle: build38 GmbH, 2021

## Vielen Dank für Ihre Aufmerksamkeit – Fragen?

- 29. Juni: Best Practice IIoT Teil 5  
„Sichere Produktentwicklung durch Governance & Architecture  
- hilft die IEC 62443?“
- 13. Juli: Best Practice IIoT Teil 6  
„Mitarbeiter effizient & erfolgreich für eine  
sichere Fabrik qualifizieren,“
- 12. - 14. Oktober 2021: it-sa 2021 in Nürnberg
- Kontakt:  
[robert.couronne@bayern-innovativ.de](mailto:robert.couronne@bayern-innovativ.de)  
Mobil +49 162 2093 307

