30. Cyber-Sicherheits-Tag
Herausforderung Industrial Security

Stuttgart, 03. Februar 2020
Rainer Wende, BSH Hausgeräte GmbH
30. Cyber-Sicherheits-Tag “Industrial Security”
BSH Markets Home Appliances for Daily Use

2018
42 production sites worldwide,
61,000 employees,
€13.4 billion revenues

Cooking/ Baking
Cooling/ Freezing
Washing/ Drying
Small Home Appliances
Dishwashing
30. Cyber-Sicherheits-Tag “Industrial Security”
The exponential Age – Opportunities and Risks

The exponential age offers us exponential opportunities and risks.

Investments into Cyber Security are often seen as risk mitigation only.

We should see them as a business opportunity.
The innovative Business needs to be kept on or next to the exponential path to be successful

Failure to provide adequate IT solutions, fosters unmanaged ‘Owner IT’ (cf. shadow IT) and increases risks

With digitalization, the security team must push for new security culture in their enterprise to enable digital change
**30. Cyber-Sicherheits-Tag “Industrial Security”**
The right balance is needed between risk and cost – but this remains a challenge

**Cost pressure**
- Reduce manufacturing cycle times
- Improve manufacturing profitability
- Improve equipment/resource efficiency

**“Need to open up”**
- Machine to machine (M2M) / IoT
- 3D printing / additive manufacturing
- Robotics
- AI/machine learning
- AR / VR
- Big Data Analytics e.g. real time asset and performance management
Security strategy needs to address Information, Cyber and Digital Security E2E

Information Security
‘Rules and Regulations’

Cyber Security
‘Cyber Attacks’

Digital Security is key to build Digital Trust
30. Cyber-Sicherheits-Tag “Industrial Security”
Digital Security, Resilience and Digital Trust are key enabler for the Digital Business

Digital Security & Resilience
are the foundation of Digital Trust

Enterprise IT

Industrial IT
- Operational Technology (OT)
- Engineering Technology

Consumer Interaction

Connected Products (Appliance IT)

Organization’s reputation of it’s digital activities

Organization or brand reputation overall

Confidentiality
Integrity
Availability

Privacy
Safety
Reliability

C
I
A
P
S
R
30. Cyber-Sicherheits-Tag “Industrial Security”
OT is special in many ways …

- General focus on functionality, quality and availability
  - Security was often less important

- 24h production line, strong dependencies in complete manufacturing chain, complex boot procedures
  - Little downtime for maintenance or software upgrades

- Limited choice of solution providers for OT
  - Multitude of proprietary solutions
  - Focus on Integration, Security often not in focus

- Industrial IT often 15-20 years „in the field“
  - old insecure protocols, often weak authentication

Sources:
https://pixabay.com/photos/calculating-machine-calculator-370777/
30. Cyber-Sicherheits-Tag “Industrial Security”
… but to enable Industry 4.0, Industrial IT has to be managed as part of digital
### 30. Cyber-Sicherheits-Tag “Industrial Security”

**Recommendations and good practices to foster cyber security in Industrial IT**

<table>
<thead>
<tr>
<th>Reporting</th>
<th>Knowledge exchange</th>
<th>Awareness</th>
<th>Set of Rules</th>
<th>Culture</th>
<th>Cyber Risk</th>
<th>Supply Chain</th>
<th>Security Interoperability</th>
<th>Incentives for security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a meaningful Security Report</td>
<td>Promote cross-functional knowledge on IT and OT security</td>
<td>Establish relaxed awareness</td>
<td>Adjust your regulations to reflect your guiding principles</td>
<td>Review your approach to Cyber Security: ‘Compliance centric with predominant approval culture’? or better be a ‘Trusted Partner’?</td>
<td>Conduct a top down Cyber Risk Assessment</td>
<td>Secure supply chain management processes</td>
<td>Establish Industry 4.0 baselines for security interoperability</td>
<td>Foster economic and administrative incentives for Industry 4.0 security. E.g. incentivize innovation and R&amp;D activities for securing IT and OT environments, components and systems.</td>
</tr>
</tbody>
</table>

### Technical Measures

- Apply technical measures to ensure Industry 4.0 security. As adaption rate for security changes in industrial IT is slow, it may take 2 years or more to introduce the basics only.

### Prioritize

- Prioritize your security initiatives using corporate strategy, cost of delay and risk mitigation.

### Set of Rules

- Adjust your regulations to reflect your guiding principles.
- Define matching controls.

### Liability

- Clarify liability among your Industry 4.0 actors. Large number of stakeholders in supply chain and lifecycle. Security and safety are tightly intertwined.

### Exercise

- Conduct frequent exercises: Cyber Incident Drills, Crisis Mgmt, BCM, Liability

### Supply Chain

- Secure supply chain management processes.

### Source:

Industry 4.0 Cybersecurity challenges & recommendations., ENISA May 2019; BSH
30. Cyber-Sicherheits-Tag “Industrial Security”
Frequently exercise and check the basics …

“We have done all the basics. Now we are working on perfection”

“Our offline backup failed, and our online backups are all encrypted”

20% effort  80% security

We are here!

Identify
Have a look for new ‘Shadow or Owner IT’

Protect
Shop floor & i4.0: Look for new holes in the hull

Detect
Implement more use cases into your SIEM

Response
Exercise using cyber drills, red or purple team attacks

Recover
Check and adjust your BCM to Cyber and challenge backup strategies
30. Cyber-Sicherheits-Tag “Industrial Security”
Push for more flexible and dynamic network and application architectures

Loose coupling of outside systems to inside backend systems is key

Outside-In
Design2Trust

Inside-Out
ZeroTrust

Corporate Networks
30. Cyber-Sicherheits-Tag “Industrial Security”
Key Take Aways

Investments into Industrial Security are more than just risk mitigation
- The risk of cyber business interruption is very real – act now
- Cyber Security can be an competitive advantage
- Digital Security is the foundation of Digital Trust and Resilience. Two imperatives for digital business

Industrial Security is a technical and organizational challenge
- IT, OT and IoT are often separate organizations – for cyber, they need to be manged as one
- Industrial Security is relevant for Safety (Cyber meets Physical)
- A holistic approach to security must address all ITs. Manage Digital.
- Secure your supply chain management – supply chain attacks are popular

Adopt recommendations and good practices to foster cyber security in Industrial IT
- 30. ACS Cyber-Sicherheits-Tag
- Publications and conferences of BSI, Allianz für Cyber-Sicherheit, ENISA and many others
- ‘Industry 4.0 Cybersecurity challenges & recommendations’ issued by ENISA, May 2019
Vielen Dank!