Industrial Cybersecurity Challenges
Andreas Reiter RC-AT DI FA DH-GRAZ SAS
andreasreiter@siemens.com
IT – OT?

- Dynamic
- Full spectrum of technologies
- Well connected
- Confidentiality, Integrity, Availability

- Data is King
IT – OT?

• Control production floor processes
• Process oriented
• Safety/Availability, Integrity, Confidentiality

• Process is King
IT - OT Challenges

Information Technology

<table>
<thead>
<tr>
<th>3-5 years</th>
<th>Forced migration</th>
<th>Well integrated IAM</th>
<th>High</th>
<th>Low</th>
<th>Heterogeneity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset lifecycle</td>
<td>Software lifecycle</td>
<td>Requirements on Identities</td>
<td>Options to add security SW</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Operational Technology

<table>
<thead>
<tr>
<th>20-40 years</th>
<th>Usage as long as spare parts available</th>
<th>Long living identities (static accounts?)</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
</table>
Observations and pit-falls for IT/OT environments
IT – OT?

• Massive data generation

• Big data analytics capabilities
  • Real-time decisions
  • Predictive maintenance

• Increased efficiency and productivity
  • Create new revenue streams
Concerns

73% are aware that their attack surface increases

55% have no plans invest, or plan to invest in cybersecurity in the next 12 months

91% are aware that OT security can only be tackled together with IT
(Not)Petya (2017)

- Maersk: Petya infected IT infrastructure
- Gates did not open (no data)
- Trucks were locked out
Ransomware is here to stay

Technology

Ransomware attack takes US maritime base offline

BBC

On Monday January 13, 2020, Picanol Group fell victim to a massive ransomware attack. The attack is causing a serious disruption to activities in Ypres, Romania, and China.
Open Industrial Control Systems

TOTAL RESULTS
7,059
Open Industrial Control Systems
Strong Perimeter Security

- Analog to air gapping
- Firewalls
- Traffic analyzers
- Strong access management
Defence in Depth

- Know what’s going on in your network
- Network monitoring
- Log analysis

- “Castle approach”
  - Multiple lines of defense
  - Network segmentation
  - Device security
  - Common cryptographic principles
  - Security-by-design
  - …
Vulnerability Scanning

• Be proactive

• Not only scan IT, but also OT networks and components

• Check against known vulnerabilities
  • Open vulnerability databases
  • Vendor specific databases
Processes

- Security Event Management (SEM)
  - Near real-time security alarms and events

- Security Information Management (SIM)
  - Long-term storage of log data

- Patch management
Siemens DH-Graz

- Founding member of the charter of trust
- Holistic concepts
- Think beyond products and services

- Plant Security Services

- Strong Security competence at DH-Graz
  - Security testing
  - International research projects
    - defense in depth
    - controlled access to production networks
    - certification
Your Takeaways

• IT and OT environments are converging
  • …to make better use of data
  • …to perform data analytics

• More attack vectors

• Be proactive in the definition of your security strategy
Contacts

Andreas Reiter
RC-AT DI FA DH-GRAZ SAS

E-mail:
andreasreiter@siemens.com

https://www.linkedin.com/in/anreiter/

siemens.com/industrialsecurity