Atos

Trusted partner for your Digital Journey
No Industry 4.0 without Security
Introduction to Atos and Industry 4.0
Who is Atos?
At a glance

Revenue 2016 (M EUR) * | Employees 2016 (Global) | Employees 2016 (Germany) | Countries
---|---|---|---
12,000 | 100,000 | 12,000 | 72

#1 European in Hybrid Cloud
#1 European in Big Data
#1 European in Cybersecurity
#1 European in High-Performance Computing
#1 In terms of hosting and storage of European data

“Our vision for the future: to accelerate progress by uniting people, business and technology.”

| 24-04-2017 | Winfried Holz: “No Industry 4.0 without security“ | © Atos |
Surveys concerning Industry 4.0

Barriers for Industry 4.0
Data security; more than half of the participants expressed fundamental concerns

59% yes 41% no

- Manipulation/espionage: 81%
- Loss of differentiating know-how: 74%
- Protection of personal data: 71%
- Security of systems/machines: 70%
- Hacker attacks: 45%

High investment costs and concerns about data security and data protection are regarded to be problematic

Source: Market study Bosch Software Innovations

Unternehmen fürchten hohe Anforderungen an Datenschutz
Welche Hemmnisse sehen Sie beim Einsatz von Industrie-4.0-Anwendungen in Ihrem Unternehmen?

- Hohe Investitionskosten: 75%
- Anforderungen an den Datenschutz: 55%
- Mangel an Fachkräften: 53%
- Anforderungen an die Datensicherheit: 51%
- Komplexität des Themas: 50%
- Fehlender Rechtsrahmen: 40%
- Störanfälligkeit der Systeme: 38%
- Fehlende Standards: 36%
- Fehlende Akzeptanz in der Belegschaft: 20%
- Nutzen ist unklar: 7%

Source: bitkom Research
The Challenge
IT versus OT security

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Availability</th>
<th>Industrial Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>Availability</td>
<td>Integrity</td>
</tr>
<tr>
<td>Availability</td>
<td></td>
<td>Confidentiality</td>
</tr>
</tbody>
</table>

- **Confidentiality**
  - Integrity
  - Availability

- **Availability**
  - Network disruptions < 300 ms
  - Plant personnel

- **IT Security**
  - Minutes are acceptable
  - Network professionals
  - Frequent audits, penetration tests, monitoring
  - Active protection mechanisms
  - Common practice
  - Every 2-3 years

- **Industrial Security**
  - Audits, pentest and monitoring no common practice
  - Active protection mechanisms can shutdown operation
  - Often not possible
  - Min. 10-20 years

**Investment cycle**
- Min. 10-20 years
Developments and challenges for Industry 4.0

- Dynamic networks
  - value networks
  - further flexibility
  - interaction

- Exchange of confidential data
  - trustworthy relationships

- Autonomous systems
  - components making independent decisions

Challenges

- Globally trusted relationships
  - independent authority
  - standardized secure infrastructure
  - assessment methods for trustworthiness

- Protection of intellectual property and personalized data
  - secure and correct exchange of data

- Allocated security
  - security by design/development
  - holistic security
  - staged security
  - secure and trustworthy components
Hacking ICS devices is terribly easy

Step 1: Identify target

Step 2a: Access system:
No password Set

Step 2a: Access system:
Use default password

---

Source: VNCKeyhole

Source: Defpass
Security Architecture for Industry 4.0
Reference architecture model for Industry 4.0 (RAMI) and security

Layers:
Security concerns all layers. Risks have to be assessed with a holistic approach.

Value stream:
Security has to be assessed throughout the whole life cycle of the objects by the owner.

Hierarchy levels:
All objects and assets are subject to security analysis (risk analysis) and need to have security features matching their tasks and protection.
IT in industrial facilities
from communication islands to complex landscapes
3 Atos – Siemens partnership
Atos and Siemens cooperation
Aligned cybersecurity portfolio to cover both IT and OT needs

<table>
<thead>
<tr>
<th>Assess security</th>
<th>IT assessments by ATOS</th>
<th>OT assessments by SIEMENS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation of the current security status of an ICS environment</td>
<td>ISO/IEC 27001 security assessments</td>
<td>IEC 62443 assessment</td>
</tr>
<tr>
<td></td>
<td>Security maturity assessments</td>
<td>ISO 27001 assessment</td>
</tr>
<tr>
<td></td>
<td>Penetration tests &amp; source code analysis</td>
<td>SIMATIC PCS 7 &amp; WinCC assessment</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Manage security
Comprehensive security through monitoring and proactive protection:
Monitor to detect indicators of compromise
Manage to keep security up-to-date
React fast to security-relevant threats

IT by ATOS
- Security monitoring
- Emergency response
- Network security
- ...

OT by Siemens
- Industrial security monitoring
- Remote incident handling
- Perimeter firewall management
- ...

Implement security
Risk mitigation through implementation of security measures for reactive protection

IT by ATOS
- Information security Management systems
- Security awareness
- Data protection
- ...

OT by Siemens
- Security awareness training
- Security policy and network consulting
- Perimeter firewall installation
- ...

Certify
Certification and preparation of certification

[Diagram showing the relationship between Assess Security, Manage Security, Implement Security, and Certify]
Thanks

For more information please contact:
Winfried Holz