Industrial Security: Manufacturing Facility Learns about Vulnerability and Risk after Assessment (case study)
Feb. 12, 2013: „Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy. That’s why, earlier today, I signed a new executive order that will strengthen our cyber defenses... Now, Congress must act as well, by passing legislation to give our government a greater capacity to secure our networks and deter attacks.“

- U.S. President Barack Obama
December 2014
“...the attackers used a spear phishing campaign aimed at particular individuals in the company to trick people into opening messages that sought and grabbed login names and passwords.”
Chrysler Hack

Spring 2015
Researchers found vulnerabilities in Chrysler automobiles allowing someone to take control of a vehicle remotely.
Why Do this Cyber Security Assessment?

Compelling Event!
Industrial Security
Security Integrated is an essential component of a Defense in Depth concept

**Plant security**
- Access blocked for unauthorized persons
- Physical prevention of access to critical components

**Network security**
- Controlled interfaces with SCALANCE firewalls
- Further segmentation with Advanced CPs

**System integrity**
- Know-how protection
- Copy protection
- Protection against manipulation
- Access protection
- Expanded access protection with CP 1543-1

Siemens products with Security Integrated provide security features such as integrated firewall, VPN communication, access protection, protection against manipulation.
Risk Management methodology

Step 1: Assess
- Information about the security status and development of a security roadmap
- Vulnerability analysis
- Gap analysis
- Threat analysis
- Risk analysis

Step 2: Implement
- Planning, development and implementation of a holistic cyber security program
- Cyber security training
- Development of security strategies and procedures
- Implementation of security technology

Step 3: Manage
- Continuous security through detection and proactive protection
- Continuous operations
- Detection and resolution of incidents
- Fast adaptation to changing threats
Assessment Process

Setup
- Gather Information
- Online meeting to confirm

Action day
- Meeting to discuss process
- Plant Tour
- Active Network Analysis

Analysis
- Siemens write-up
- Face-to-face meeting to summarize results
Plant Tour Found…

- HMIs connected to Internet
- Inconsistent USB policies
- Non-Logical USB policies
- Active malware on plant computers
- Old Operating systems (DOS, NT, 2000, XP)
- Modem connected to PLC (unknown)
- Whitelisting disabled
- Network devices not owned by any group
- Corporate wide flat network (obfuscated by VLANs)
- Inconsistent backup programs (cell by cell)
- No plan B for important applications running on legacy equipment
## Deliverables

<table>
<thead>
<tr>
<th>Customer 1</th>
<th>Initiative 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Initiative 1</td>
</tr>
<tr>
<td>Observation</td>
<td>This is what we found…</td>
</tr>
<tr>
<td>Priority</td>
<td>High</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Implement program</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customer 2</th>
<th>Initiative 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Initiative 3</td>
</tr>
<tr>
<td>Priority</td>
<td>High</td>
</tr>
<tr>
<td>Observation</td>
<td>This is what we found…</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Implement program</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customer 3</th>
<th>Initiative 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Initiative 3</td>
</tr>
<tr>
<td>Observation</td>
<td>What was found</td>
</tr>
<tr>
<td>Priority</td>
<td>Medium</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Implement program</td>
</tr>
</tbody>
</table>

- Long report with appendices
- List of current issues
- Review of each proposed initiative individually
What’s Next

Additional projects, strategy, or thoughts about the future

- Prioritized list of initiatives for this plant
- Investigate ways to securely monitor network activity
- (SIEM = Security information and event management )
Benefits of Assessment

- We were able to review the cyber security footing
- Found some areas that could be improved
- IT in Corporation worked with us
- Better understanding of risks
- Prioritized list of topics (Color coded below)
- Criticality and Cost Review

<table>
<thead>
<tr>
<th>Description of Initiative</th>
<th>Relative Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX</td>
<td>$$</td>
</tr>
<tr>
<td>YYY</td>
<td>$</td>
</tr>
<tr>
<td>ZZZ</td>
<td>$$-$$$$</td>
</tr>
<tr>
<td>AAA</td>
<td>$</td>
</tr>
<tr>
<td>BBB</td>
<td>$</td>
</tr>
<tr>
<td>CCC</td>
<td>$$-$$</td>
</tr>
<tr>
<td>MMM</td>
<td>$$</td>
</tr>
<tr>
<td>NNN</td>
<td>$</td>
</tr>
</tbody>
</table>
State of the Manufacturing environment (IoT)

Enterprise Environment

- Enterprise IT
- Supply Chain
- Plants

Customer Environment

- Connected Services
- Connected Products
- Customers
IT/OT Integration

Business drivers are forcing the connectivity of IT and OT. This establishes new attack avenues to critical OT.

Information Technology (IT)

Internet-connected networks and devices that enable a company to do business, are filled with exposures and face constant attack.

Operational Technology (OT)

Industrial Control Systems (ICS) comprise most of the OT environment. These systems allow operators to monitor and control industrial processes, and are the lifeblood of industrial companies.
What we found in a Manufacturing Site (Versus a Process Site)

Manufacturing
Flat Network
Mix of Legacy and New, NOT isolated

Process
Hierarchical Net
Legacy System Already isolated

Availability
Integrity
Confidentiality

Confidentiality
Integrity
Availability

IT
Flat Network
Confidentiality Updated Hardware
Segmentation (showing real PCS 7 network)
DMZ concept
Conclusion

- Assessment helped plant focus on Cyber Security
- Roadmap to improve our position
- Blueprint for future plants
- Confirmed results of previous assessments
Questions