OMV Group

Cyber Security
Emerging threats to Industrial Control Systems require intensified countermeasures

VCSW 2018
History of attacks affecting critical infrastructure

- **Estonia**: Cyber attack took down banks
- **US**: Power Plant malware detected
- **US**: Rye Brook Dam control system hacked
- **Ukraine**: “Crash Override” Power grid down
- **WW**: Ransomware stopping production

**2007**

- **2010**
  - **US**: “Stuxnet” malware in uranium enrichment plant
  - **SAUDI ARABIA**: “Shamoon” malware wiped PCs

**2012**

- **2013**
  - **WW**: “BlackEnergy” Trojan
  - **GERMANY**: Steel mill taken over

**2014**

- **2015**
  - **WW**: SWIFT down
  - **WW**: Ransomware

**2016**

- **US, SUI, TRK**: “Dragonfly” group intrudes energy companies

**2017**

- **Ukraine**: Power grid down
  - **US**: Wolf Creek nuclear Power Plant malware detected

**INFORMATION SECURITY**: Damage, Reconnaissance, ICS
Possible patterns behind attacks

- **Estonia:** Cyber attack took down banks
- **US:** Rye Brook Dam control system hacked
- **Ukraine:** “Crash Override” Power grid down
- **Iran:** “Stuxnet” malware in uranium enrichment plant
- **Saudi Arabia:** “Shamoon” malware wiped PCs
- **US:** “BlackEnergy” Trojan
- **ww:** “Havex” Trojan
- **Ukraine:** Power grid down
- **US, SUI, TRK:** “Dragonfly” group intrudes energy companies

ICS/SCADA Systems provide exploitable vulnerabilities

- ICS/SCADA equipment specifics:
  - designed primarily for operational safety and reliability
  - security not top priority
  - long lifecycle
  - patching possibility not always built in
  - downtime (for patching) not desired

\[
\text{Vulnerabilities} + \text{Lack of Patches} + \text{delayed Patching} = \text{exploitable Vulnerabilities}
\]
Exposure of ICS/SCADA Systems is growing

- Increased exposure of ICS/SCADA systems:
  - Digitalization requires more data exchange
  - Remote service instead of physical access
  - Increasing amount of involved devices
  - New connection technologies (e.g. wireless)
  - Trend to standardization
  - More Windows-based solutions in ICS environments (e.g. HMI)

\[
\text{growing Attack Surface} + \text{Loss of Obscurity} = \text{increased Exposure}
\]
Defense against Cyber Security Threats
Components to be considered

**ARCHITECTURE**
Planning and running systems considering security aspects

- "Security by Obscurity" does not protect anymore
- Multiple layer defense:
  - Perimeter protection
  - Network protection
  - Malware protection

**PASSIVE DEFENSE**
Systems without human interaction

- Perimeter Protection:
  - Firewalls to outside and within ICS
  - Unidirectional gateways: outbound only
- Network segmentation & protection
- VPN between ICS components
- Access Control Lists
- 802.1.x

**ACTIVE DEFENSE**
Analysts monitoring, responding and learning from intrusions

- Log file monitoring of firewalls within the SCADA/ICS environment + to the "outside world"
- Fast reaction / having resources available quickly
- Using trained, aware people for operations and defense

**INTELLIGENCE**
Collecting data, condensing it into information and producing intelligence

- Lessons learned from previous experiences
- Exchange with peers / CERT/ national organizations
- Vulnerability feeds / external warnings + reaction on them
- Good cooperation with "classical IT"

Source of drawing: E-ISAC “The Sliding Scale of Cyber Security”
Further readings

- IEC 62443-2-1
  Industrial communication networks – Network and system security –
  Part 2-1: Establishing an industrial automation and control system security program


- ENISA, Can we learn from SCADA security incidents?

- ENISA, Communication network dependencies for ICS/SCADA Systems

- ISACA SCADA Cybersecurity Framework

- RISI Industrial Security Incidents Database (ISID) – discontinued since 2015
  http://www.risidata.com/Database

- 21 Steps to Improve Cyber Security of SCADA Networks
Thank you for your attention!