Monitoring The Evolving Threat Landscape

Smart Grid Technical Forum
28th March 2019
The European Network for Cyber Security (ENCS) is a non-profit organization that brings together critical infrastructure stakeholders and security experts to deploy secure European critical energy grids and infrastructure.
Emerging Smart Grids

Selection of 10 Use Cases at the crossroads of digital and energy

<table>
<thead>
<tr>
<th>Digital Themes</th>
<th>Generation</th>
<th>Market operations/trading</th>
<th>Transmission</th>
<th>Distribution</th>
<th>Retail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Customer Engagement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Energy Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart city &amp; Mobility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Grid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital Plant and Field Work</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 1. On-site optimization for C&I and Residential Buildings
- 2. District / multistore buildings' optimization
- 3. Energy aggregator
- 4. Customer data analytics
- 5. Smart EV Charging & Fleet Management
- 6. Urban Data Platforms
- 7. Community energy
- 8. RES origin tracking
- 9. Improved O&M with data analytics & digital services
- 10. Flexibility platform for network services (TSO & DSO)

March 2019
## Emerging Threat Landscape

<table>
<thead>
<tr>
<th>More Standards</th>
<th>More Interconnectivity</th>
<th>More Targeted Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="ISO" />, <img src="image" alt="CENELEC" />, <img src="image" alt="ETSI" /></td>
<td><img src="image" alt="Cloud" />, <img src="image" alt="Smartphone" />, <img src="image" alt="Computer Network" /></td>
<td><img src="image" alt="Phishing" />, <img src="image" alt="Email" />, <img src="image" alt="Social Media" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>More Active Threat Actors</th>
<th>More Automated Attacks/Artificial Intelligence</th>
<th>More Computing Power* and Better Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Hacker" /></td>
<td><img src="image" alt="Robot" /></td>
<td><img src="image" alt="Quantum Computing*" /></td>
</tr>
</tbody>
</table>
Security Experts at Grid Operators Know the Vulnerabilities

SANS Survey:
Control System Components considered risk for compromise?

Source: SANS 2016 State of ICS Security Survey
Attackers Also Know the Vulnerabilities

**CVSS v3 8.6**

ATTENTION: Remotely exploitable/low skill level to exploit.

Vendor: Siemens

Equipment: SIPROTEC 4 and SIPROTEC Compact

Vulnerabilities: Improper Input Validation, Missing Authorization, Improper Authentication

**UPDATE INFORMATION**

This updated advisory is a follow-up to the updated advisory titled ICSA-17-187-03B Siemens SIPROTEC 4 and SIPROTEC Compact that was published July 27, 2017, on the NCCIC/ICS-CERT web site.

**AFFECTED PRODUCTS**

Siemens reports that the vulnerabilities affect the following SIPROTEC 4 and SIPROTEC Compact protection, control, measurement, and automation devices:

-------- Begin Update C Part 1 of 2 --------

- Firmware variants for EN100 Ethernet modules as optional for SIPROTEC 4 and SIPROTEC Compact:
  - Firmware variant PROFINET IO: All versions prior to V1.04.01
  - Firmware variant Modbus TCP: All versions prior to V1.11.00
  - Firmware variant DNP3 TCP: All versions prior to V1.03, and
  - Firmware variant IEC 104: All versions prior to V1.21
- EN100 Ethernet module included in SIPROTEC Merging Unit 6MU80: All firmware versions prior to V1.02.02
Exploits Are In Public Domain

Siemens Warns of Critical Remote-Code Execution ICS Flaw

The affected SICAM 230 process control system is used as an integrated energy system for utility companies, and as a monitoring system for smart-grid applications.

Siemens has released 16 security advisories for various industrial control and utility products, indicating a warranty for a critical flaw in the WinDy digital rights management (DRM) solution.
But Who Would Want to Exploit these Vulnerabilities to Attack the Grid?
Classes of Attackers

Unc targeted / opportunistic attackers

- **Script kiddies**
  - Stereotype teenage hacker
  - Intends no real damage, but may cause it unintentionally

- **Researchers / Journalists**
  - Show what’s possible
  - Like a good story

- **Opportunistic Criminals**
  - Target IT, but may hit OT
  - Just sending spams
  - Ransomware

**Hacktivists**
- Deface websites
- Cause bad publicity

**Disgruntled Employees**
- Taking revenge
- Selling information on the black market

**Terrorists**
- May be interested in causing power outage

**Criminals targeting OT**
- Extortion
- Could work for terrorists of nation states

**Targeted / determined attackers**

- **Nation State Actors**
  - Strategic assets
  - Espionage
  - Sabotage

- **Criminals targeting OT**
  - Extortion
  - Could work for terrorists of nation states
OT Threat Development

Cyber Meter Fraud
Bad Architectures Using Bad Protocols
Ukraine Incidents
PLC Malware
Malware As A Service (MaaS)

Targeted Malware for Energy Sector
ICS Actively Targeted
Malware now knows Industrial Control Systems
Increasing APTs
Are we keeping up?

• Increasing nation state actor activity
• Criminals get business models working
• Fast development and distribution of malware
How To Reduce The Risks
## Countermeasures

### Policies & Procedures
- Implement OT security policies and procedures
- Make employees aware of security risks
- Enable information sharing
- Create an ISMS (ISO 27001)
- Set up a Security Operations Center (SOC)
- Be ready to respond to incidents, and recover normal operations

### System Architecture
- Protect the perimeter of the OT domain
- Validate with penetration tests
- Risk assess crown jewels
- Risk based use cases

### Components
- Procure secure devices with good requirements
- Harden operational devices
- Validate with lab tests
- Active or passive sensors
- Use of honeypots and IDS
- Accurate CMDB
European Regulatory Perspective

- NIS Directive (effective May 2018)
- Cybersecurity act
  - New permanent mandate ENISA
  - European cybersecurity certification framework for ICT products and services
- Network Code Cybersecurity
  - Harmonized Cybersecurity Baseline across the European Union
  - Advanced Cybersecurity Implementation for Operator of Essential Services
  - Supportive Elements for the Network Code on Cybersecurity
ENCS helps its members solve cyber security challenges in the development and operation of smart grids across Europe.

Collaboration projects

Testing

Training

Information & Knowledge sharing

Research
Threat Monitoring Focus

- What do we need to know/what are we looking for?
- Analysis and interpretation of events
- SOC development
- Intrusion detection technology
Collaboration and Resource Sharing

- Collaboration focus on
  - Getting technology in control
  - Closing the skills gap
  - Information & knowledge sharing

- Security Community Building
  - Policy
  - Architecture
  - Operations
Thank you

anjos.nijk@encs.eu