CHALLENGES AND TRENDS ENCOUNTERED
IN THE IMPLEMENTATIONS OF EU LEGISLATION

Challenges in IACS for essential operators

Michael Theuerzeit
Senior Consultant
Hudson Cybertec

Cybersecurity and Data Protection Standards in support of European Policy

Brussels

September 19, 2017

Hudson Cybertec

Cyber Security Solution Provider

for the

Operational Technology

- We help companies to improve and maintain cyber security for their primary processes
- Focus on Industrial Automation & Control Systems domain
  DCS – PLC – HMI – SCADA – Industrial networks
  Instrumentation – Building bound technical installations

“Where technical installations are essential for the operation”

The world is changing rapidly

- Changes in
  - Technology
  - Functionality
  - Society
  - Threats
- What is saf
  bsolete tomorrow

Security has to change accordingly!

DIRECTIVE (EU) 2016/1148

Directive 2016/1148 (1/2)

- The Network and Information Security (NIS) directive
  - Adopted on July 6, 2016
  - Legislation by member states implemented on November 9, 2018
- Mandatory for essential services

Directive 2016/1148 (2/2)

- Objectives
  - Increase national cyber security capabilities
  - EU level cooperation
  - Risk management and reporting
- Goal
  - Boosting the overall online security in the EU

Obligations of member states

- All member states (MS) have in place:
  - NIS national strategy
  - NIS competent national authority (CA)
  - Computer Security Incident Response Team (CSIRT)
- Identify essential services
- Implement legislation

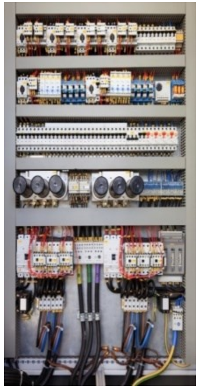
Obligations of essential services

- Obligation to report
- Duty of care
  - Appropriate technical countermeasures
  - Appropriate organizational countermeasures
- Mitigate the risk of network and/or information systems

20
40
60
80
100
120
140
SE
S
NE
N

IEC 62443

- Worldwide standard
- Security of the Industrial Automation & Control Systems in the Operational Technology domain



Using the IEC 62443 to prepare for NIS

Using the IEC 62443 (1/3)

- Prevent risk
  - Organizational measures that are appropriate and proportional to the risk
- IEC 62443-3-2
  - Tolerable risk
- IEC 62443-2-1
  - Organizational countermeasures

Using the IEC 62443 (2/3)

- Ensure NIS
  - The measures should ensure a level of NIS security appropriate to the risk
- IEC 62443-2-1
  - Organizational countermeasures
- IEC 62443-3-3
  - Technical countermeasures

Using the IEC 62443 (3/3)

- Handle incidents
  - The measures should prevent and minimize the impact of incidents on IT systems used to provide the services
  - Incident notification of incidents that have a significant impact

- IEC 62443-2-1
  - Incident planning and response
  - Monitoring and improving

NEN and IEC 62443

- NEN offers IEC 62443 training
  - 3-Day program
  - Apply the standard for practical use
- NEN offers exams to certify knowledge level on IEC 62443
- Looking to cooperate with sister organizations in EU

Get prepared for NIS

- Know your network
- Logging & monitoring is essential
  - If you do not look, you can not see
- Obtain knowledge on managing cyber security

Hudson Cybertec
Laan van ‘s-Gravenmade 74
2495 AJ The Hague
The Netherlands
www.hudsoncybertec.com

+31.70.25.00.717
info@hudsoncybertec.com

NEN
Vlinderweg 6
2623 AX Delft
The Netherlands
www.nen.nl

+31.15.26.90.391
rianne.boek@nen.nl