Working with the EU Directive
„High common level of network and information security“

Martin Apel, SANS ICS Summit, Munich und 18.06.2018
Outline

1. Overview over NIS-Directive
2. Who is an operator of essential services?
3. Protecting essential services
4. Reporting Incidents
5. Conclusion
1. Overview over NIS-Directive
Main aspects of NIS-Directive

- National Strategy for Cybersecurity
- Protection of Digital Services
- Cooperation between Member States
- Protection of Essential Services
Essential Services

- Energy
  - Gas
  - Oil
  - Electricity

- Transport
  - Air
  - Water
  - Rail
  - Road

- Digital Infrastructure
  - DNS-Provider
  - IXPs

- Health sector
  - Healthcare providers

- Financial market infrastructures
  - Supply
  - Distribution

- Banking
Key aspects for the protection of essential services

- Designate competent authority
  - Member states
  - BSI

- Identify Operators of essential services (OES)
  - Member states
  - OES

- Designate CSIRT
  - Member states
  - CERT-Bund

- Assess Compliance of OES
  - BSI
  - Evidence from OES
  - Audits

- Report incidents
  - OES

- Protect network and information systems used for provision of essential services
  - BSI
2. Who is an operator of essential services?
Identify OES

Criteria to consider:
1. provides an essential service
2. provision of service depends on network and information systems
3. incidents would have a disruptive effect
German approach

Sector

Essential Service

Energy

Step

Electricity

Transmission

... Gas

Infrastructure

Erzeugung

Power plant

Transmissiongrid

... Threshold

420 MW

...
Identifying Operators of essential Services - Results

List of essential services extended
>> Wastewater treatment
>> Food

German OES have been identified
>> about 1300 infrastructures

Evaluation planned
>> 2019
>> new sectors?
3. Protecting essential services
Security requirements for Operators of essential services

OES have to:

• protect the network and information systems used for the provision of essential services

• take appropriate and proportionate technical and organizational measures to manage the risks

• take appropriate measures to prevent and minimize the impact of incidents with a view to ensure the continuity of the services
German approach

Problem:
• Smaller companies struggle with determining appropriate measures
• A similar level of security is desirable within a subsector

Solution:
• OES of a subsector may create their own „subsectoral standard“ for the protection of the IT needed for their essential service
• BSI will review these standards and approve or disapprove them
Security requirements for Operators of essential services - Results

**Developing and reviewing standards takes time**

>> usually 1 – 2 years

**OES have developed standards and BSI approved them**

>> Drinking Water and Wastewater treatment

>> Data Center and Hosting

>> Food Distribution/Commerce

**OES are developing more standards**

>> 6 – 8 standards

>> BSI advises OES
4. Reporting incidents

What to report?
What support do I receive?
Reporting Incidents

- significant incidents have to be reported to the competent authority or the CSIRT

- Criteria for significance:
  - number of users affected by disruption of essential service,
  - duration, and
  - geographical spread.
Reporting Incidents – German Approach

Why is reporting incidents important?

Prevent this from happening elsewhere

Information Sharing is crucial!

BSI is obliged to share its information about important IT-Security Issues

... and is doing so happily

Getting help!

Government

OES

CSIRTs
Reporting incidents - Results

>> In 2018: 113
Report Incidents
>> most of them are not attacks but failures

Cyber-Security Warnings from BSI
>> 50 Warnings in 2017

BSI supported
Incident Handling of OES
>> phone support
>> assembled team
supported on site
5. Conclusion
Summary

• NIS-Directive is forcing OES to implement a baseline of cybersecurity
  ... and has been successfully implemented in Germany

• BSI works with OES together to help them
  - fulfill the security requirements from the NIS-Directive
  - handle security incidents successfully

• Contact us!
Any questions?
Feel free to ask!

Contact

Martin Apel
Director of Section Critical Infrastructure Sectors: Energy and Water Supply; Nuclear Facilities

martin.apel@bsi.bund.de
Tel. +49 (0) 228 9582 6035
Fax +49 (0) 228 10 9582 6035

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de