Implementing European Cybersecurity Regulations
NTNU NISlecture
Martin Schallbruch
Gjøvik | Sep 29th, 2017
To introduce myself ...

Interdisciplinary Research on Digital Society
Founded in 2016
Preliminary Focus on
Cyber Security and Privacy

2002-2016

Director General for
Information Technology, Digital Society
and Cyber Security
Deputy Federal Government CIO

Federal Ministry of the Interior
Today’s Agenda

I. The Cybersecurity Challenge

II. EU Cybersecurity Regulations

III. Next Steps
Today’s Agenda

I. The Cybersecurity Challenge

II. EU Cybersecurity Regulations

III. Next Steps
Cybersecurity is a multi-dimensional challenge.

- ICT Complexity
- ICT Quality
- ICT Innovation
- ICT Security Innovation
- User Awareness and Training
- Dependency on Digital Processes
- Threat Development

Cybersecurity
Cybersecurity is a multi-dimensional challenge.

Sustainable Drivers for Improving Cybersecurity?

- Resilient Societies
- ICT Complexity
- ICT Quality
- ICT Innovation
- Secure Systems
- Strong Liability
- Dependency on Digital Processes
- Threat Development
- User Awareness and Training
- ICT Security Innovation
Today’s Agenda

I. The Cybersecurity Challenge

II. EU Cybersecurity Regulations

III. Next Steps
Cybersecurity regulations (narrowly defined)

Legal requirements for the security of

- Systems,
- Services,
- Products

and for those who build,
provide,
use it.
EU cybersecurity law - Overview
**Critical Infrastructures**

**EU NIS Directive of 2016**

- Operators with substantial degree of supply
- Requirement: Technical „state-of-the-art“ measures
- Monitoring: Audits, supply of documents, inspections, fines
- Reporting of incidents
- Enforcement ability

**IT security law 2015 + NIS implementing law 2017**

+ Food, Insurance

1648 operators

Sector-specific standards

BSI/3rd party

BSI/regulator

BSI mobile incident response team

**Sector-specific regulation**

Telecommunications, Energy, Banks, ..
Digital Services

Broad-range basic protection (IT security law 2015)

- all kinds of digital services, such as internet shops, media, platforms
- Requirements: Protection against unauthorised access, data theft, sabotage; appropriate and proportionate "state-of-the-art"-measures
- Oversight: none, ex-post control, fines

Digital Services under NIS Directive

- Online marketplaces, online search engines, cloud services
- Full EU-wide harmonisation, risk-appropriate "state-of-the-art" measures, implementing acts of EU commission, ex-post control (BSI)
- Reporting of incidents (to BSI), no inspections

Trust Services (eIDAS regulation)

Sectors-specific Digital Services (e.g. PSD II; upcoming eHealth, eEnergy)
EU General Data Protection Regulation (EU GDPR)

Security of Processing – Art. 32
Risk-appropriate "state-of-the-art" technical and organizational measures
Considering of BSI technical guidelines and recommendations
Oversight by data protection authorities, high penalties

Other Technology Influencing Provisions
Privacy by Design – Art. 25
Codes of Conduct – Art. 40
Certification – Art. 42
EU Cybersecurity Package 13-Sep 2017

- ENISA shall become the EU Cybersecurity Agency
- NIS directive implementing acts (digital services)
- Blueprint for cybersecurity emergency response and crisis management (recommendation)
- Draft Regulation for EU Cybersecurity Certification Framework
  - All kinds of ICT products and services
  - Voluntary certification, three levels of security
  - Requirements defined by product-specific certification schemes
  - Schemes adopted by EU commission (draft: ENISA)
  - Member states not allowed to pass national schemes for that kind of product

➢ Speed? Cost? Life-time?
Overall trends in cybersecurity regulation

Growing area of regulation
- Sector-specific „digital regulations“
- Digitization of systems that require special approval

Interplay between sector and general law
- Different requirements for the same system
- Cascading compliance obligations
- Varying supervisory authorities

Increasing pressure on manufacturers
- Growing contractual liability in regulated areas
- Increasing need for security confirmation/certification

29-Sep-2017 NTNU NISlecture, Gjøvik
Today’s Agenda

I. The Cybersecurity Challenge

II. EU Cybersecurity Regulations

III. Next steps
Sustainable Drivers for Improving Cybersecurity

- Resilient Societies
- Dependency on Digital Processes
- ICT Complexity
- Strong Liability
- ICT Quality
- ICT Innovation
- Secure Systems
- ICT Security Innovation
- Cybersecurity

Dependency on Digital Processes

Sustainable Drivers for Improving Cybersecurity
Next steps – What issues should EU address?

Secure Systems

• Step up research into high assurance systems
• Redirect public spending into high assurance systems

Strong Liability

• Set up mandatory security requirements
• Define duties of care for manufacturers

Resilient Societies

• Include public service and manufacturing in NIS sectors
• Add online platforms to NIS digital services