Directive on security of network and information systems (NIS)

Dr. Florent Frederix
Trust and Security Unit
DG Communications Networks, Content and Technology,
European Commission

CyberSecurity4Rail Conference
October 4, 2017
Hotel Thon, Brussels
In the News

- Wannacry ransomware attack on Deutche Bahn
- Risk? Liability?
- Is it cybersecure?
- Safety threats due to hacking
- Rail speeds up ERTMS roll out
- UK installs digital signalling
- Automatic Train Operation in rail freight sector is the future
- Risk? Liability?

http://www.telegraph.co.uk/news/2017/05/13
http://www.railway-technology.com
23/03/2017
http://www.dailymail.co.uk/sciencetech
25/09/2017
EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace

Digital Agenda for Europe
1. Cyber resilience
   - NIS Directive (capabilities, cooperation, risk management, incident reporting)
   - Raising awareness

Justice and Home Affairs
2. Reduce cybercrime

EU Foreign and Security Policy
3. Cyber defence policy and capabilities
5. International cyberspace policy

4. Industrial and technological resources: NIS platform; H2020

- Fundamental rights apply both in physical and digital world
- Cybersecurity depends on and contributes to protecting fundamental rights
- Access for all
- Democratic and efficient multi-stakeholder governance
- Cybersecurity is a shared responsibility

The umbrella strategy
The NIS Directive: objectives

- Increased national cybersecurity capabilities
- EU level cooperation
- Risk management & reporting

Boosting the overall online security in Europe
Capabilities

All MS to have in place

NIS National strategy

NIS competent national authority

Computer Security Incident Response Team (CSIRT)
Cooperation Group

what: strategic cooperation
who: MSs; EC (secretariat), ENISA

CSIRT network

what: operational cooperation
who: national CSIRTs; CERT-EU; ENISA (secretariat)
Security and notification requirements

Operators of essential services

Energy: electricity, gas and oil
Transport: air, rail, water and road
Banking: credit institutions
Financial market infrastructure
Health: healthcare providers
Water: drinking water supply and distribution
Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registers
Security and notification requirements

Digital Services Providers (DSPs)

- Online market places
- Cloud computing services
- Search engines
Capabilities
National competent authorities

- Cover(s) at least the actors referred in the Directive
- Monitor(s) Directive application
- Its role may be assigned to an existing authority

Automatically becomes a national single point of contact.
Single Point of contact

Liaison function to ensure cross-border cooperation with other Member States and the CSIRTs network

Reports annually to the Cooperation Group on the notifications received within Member State (information received from competent authorities and/or CSIRTs)

Might be an existing authority

If only one competent national authority = automatically single point of contact
Cooperation
Cooperation Group - Overview

**Aims**
- Foster EU-level strategic cooperation
- Build trust & confidence

**Composition**
- Member States
- ENISA
- European Commission (secretariat)

**EC will establish operational rules and procedures via implementing act**

Work to start 6 months after entry into force.
Cooperation Group - Tasks

Information & Best practices on
- Risks
- Incidents
- Awareness raising
- Training
- R&D

Work of the Group
- Establish a work programme by 18 months after entry into force
- Prepare WP every 2 years thereafter

Policy coordination
- guidance for CSIRTs Network
- assist MSs in NIS capacity building
- support MSs in the identification of operators of essential services
- discuss incident notification practices
- Discuss standards
- Engage with relevant EU institutions
- Evaluate NIS national strategies and CSIRTs (voluntary)

On progress
- Every 1.5 yrs provide a report as input to EC's review of the Directive
CSIRTs Network - Overview

**Aims**
- Foster EU-level **operational** cooperation
- Build trust & confidence

**Composition**
- National CSIRTs
- CERT-EU
- ENISA (secretariat)
- European Commission (observer)

CSIRTs Network will establish its own **rules of procedures**
Exchange info on CSIRTs services, operations & capabilities

Exchange info on individual incidents (on request & voluntary)

Identify coordinated response to incidents (on request & voluntary)

Support cross-border incident handling (voluntary)

Explore further forms of operational cooperation

Discuss lessons learnt from NIS exercises

Discuss individual CSIRT issues (on request)

Guidelines on Operational cooperation

Inform Cooperation Group & seek guidance

Report as input to EC review every 1,5 yrs
Identification of operators of essential services

Each MS will identify the entities subject to security and notification obligations by applying these criteria:

1. The entity provides a service which is essential for the maintenance of critical societal/economic activities.

2. The provision of that service depends on network and information systems; and

3. A NIS incident would have significant disruptive effects on the provision of the essential service.
Lex specialis

IF a sector specific Union act provides for either security requirements or notification obligations for operators of essential services or digital service providers.

IF the provisions of the sector specific act are at least equivalent in the effect to the obligations contained in the Directive.

The relevant provisions of the sector specific act apply.
Notification requirements

MSs shall ensure notifications without undue delay to the competent authority or to the CSIRT.

Operators of Essential services

"incidents having a significant impact on the continuity of the essential services they provide. [...]"

Digital Services providers

"any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union"
Member States' different provisions

Operators of essential services

MSs are not prevented from adopting/maintaining provisions with a view of achieving a higher security of networks and information systems.

Digital services providers

Member States are not allowed to impose any further security or notification requirements.
Implementation and Enforcement

Operators of essential services

*Competent national authorities* should have the necessary powers/means to *assess the compliance* with the Directive and issue enforcement measures if necessary.

Digital services providers

The competent national authorities are entitled to carry out solely reactive *ex-post supervisory activities* in line with the light-touch regulatory approach applicable to DSPs.
The NIS Directive: from proposal to transposition

- **EC proposal COM (2013)48**
- **February 2013**
- **6 July 2016**
  - Entry into force 20 days after publication in OJ (19/07/2016)
- **7 Dec 2015**
  - Sixth informal triilogue
- **21 months** after entry into force for transposition into national laws
  - Additional **6 months** to identify Operators of essential services
Cybersecurity contractual Public-Private Partnership (cPPP)

- Stimulate the **competitiveness and innovation** capacities of the digital security and privacy industry in Europe
- Ensure a sustained **supply of innovative cybersecurity products and services** in Europe
Thank you for your attention!