on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

Ricardo Morla, FEUP/INESC TEC
FEUP, 20 Jun 2022

Key points

- Estimated 7x more organizations covered
- Specific technical and reporting obligations
- Fines up to €4M or 2% worldwide annual turnover

- National and EU-wide coordination mechanisms
  - National cibersecurity strategy and crisis management framework
  - Coordinated vulnerability disclosure
  - Cooperation groups, CSIRT networks
  - Crisis liason network CyCLONe

Which organizations are covered

- All medium and large-sized organizations in specific sectors
  - Energy, transport, banking, financial market infrastructures, health, drinking and waste water, some digital infrastructure
- Some small-sized depending on what they do
- Public administration
  - Covered: central government entities
  - Not covered: defence and national security, public security, law enforcement, judiciary, parliaments, central banks
  - Decision of member state: regional/local level; universities (?)

- Also defines *essential* vs. *important* entities

Technical requirements (Art. 18)

- risk analysis, information system security policies
  - identification major assets, vulnerabilities, and threats
- incident handling
  - prevention, detection, and response to incidents
- business continuity, crisis management
  - recovery plans, PR, interaction with authorities
- supply chain security
  - data storage, processing services, managed security services
- NIS in acquisition, development and maintenance
  - vulnerability handling
- testing and auditing
  - offensive security ??
- use of cryptography and encryption
  - DES ??

Reporting obligations (Art. 20)

- Defines a ‘significant’ incident, potential to cause:
  - substantial operational disruption or financial losses – to the reporting entity
  - considerable material or non-material losses – to other natural or legal persons
- Must submit:
  - within 24 hours: an initial notification
  - upon request: intermediate report, status update
  - not later than one month: final report
    - details, severity, impact
    - type of threat
    - mitigation measures

Supervision

Essential (ex-ante) vs. Important Entities (ex-post)

- on-site inspections, off-site supervision, regular audits, random checks
  - important entities: ex-post inspections/supervision only
- targeted security audits, security scans
  - based on risk assessment
- access data, documents, etc.
  - necessary for supervisory tasks
- evidence of implementation of cybersecurity policies
  - essential only
- check notification to authorities for self-identification
  - ex-post for important entities

Enforcement

- Issue warnings, binding instructions, orders for ceasing non-compliant conduct, for updating risk management measures, etc
- Impose fines
- Make public statement, entity and nature of infringement

- Suspend certification or authorization for part or all services (EE)
- Temporary ban at CEO or legal representative level (EE)

Timeline

- Commission Proposal
  6 December 2020
- Parliament Draft Report
  3 May 2021
- Council Proposal
  26 November 2021
- Provisional agreement Council and Parliament (press release only)
  13 May 2022

21 months to transpose directive after it enters into force

=> mid 2024?

on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

Ricardo Morla, FEUP/INESC TEC
FEUP, 20 Jun 2022