ANSSI .lu

Agence nationale de la sécurité des systèmes d'information Luxembourg

FEDIL-ICT - EY study

"Hygiene security practices for providers of essential services in Luxembourg"

Feedback & Impact of 'NIS Directive' on OESs/DSPs

7th April 2017

Léon Treff

ANSSI missions(*) :

- **define policies and guidelines** related to information security (for classified and unclassified information) and to **monitor** its **effectiveness**
- **supervise the implementation of safeguards** and check that their application are guaranteed

- certify information and communication technologies (ICT) handling non-classified information (systems, services, infrastructures, or premises)
- act as the national and governmental CERT (operated by GOVCERT)
- coordinate training on security of classified and unclassified information
- ensure adequate user awareness on specific risks related to ICT; more specifically related to cyberattacks
- act as national TEMPEST Authority (TA)
- act as national Crypto Approval Authority (CAA)

(*) Arrêté grand-ducal du 10 février 2015 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information

FEDIL-EY study

- Promote cyber security and raise awareness

- Benchmarking is particularly important
  - Compare to peers/best practices/industry standards
  - Identify weaknesses & key areas for improvement
  - Focus on the right matters
  - Essential for continual improvement
  - Monitor progress

- Outcomes of FEDIL-ICT - EY study are globally encouraging

however

“Hackers only need to get it right once. We need to get it right every time”

'NIS Directive'

Directive on Security of Network and Information Systems

The 'NIS Directive' represents the first EU-wide rules on cybersecurity

Objective : achieve a high common level of security of network and information systems within the EU

- Improved cybersecurity capabilities at national level
- Increased EU-level cooperation
- Risk management and incident reporting obligations for operators of essential services and digital service providers

'NIS Directive'

Improved cybersecurity capabilities at national level

National strategy defining the strategic objectives and appropriate policy and regulatory measures

- Strategic objectives, priorities and governance framework
- Identification of measures on preparedness, response and recovery
- Cooperation methods between the public and private sectors
- Awareness raising, training and education
- Research & development plans
- List of actors involved in the strategy implementation

'NIS Directive'

Member States have to designate :

- National competent authorities (one or more)
  - monitor the application of the Directive at national level
- Single point of contact
  - liaison function to ensure cross–border cooperation
- Computer Security Incident Response Teams (CSIRTs) participating in the CSIRTs network
  - monitoring incidents at a national level
  - providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents
  - responding to incidents
  - providing dynamic risk and incident analysis and situational awareness

'NIS Directive'

Increased EU-level cooperation

NIS Cooperation Group

- Planning
- Steering
- Sharing best practices
- Reporting

Network of the national CSIRTs

- Exchange of incident information
- Coordinated, cross-border response to incidents
- Exercises

'NIS Directive'

Risk management and incident reporting obligations

Operators of essential services (OESs)

Private businesses or public entities

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 security incident would have **significant disruptive effects** on the provision of the essential service.

'NIS Directive'

ANSSI .lu

Covered Sectors :

- **Energy**: electricity, oil and gas
- **Transport**: air, rail, water and road
- **Banking**: credit institutions
- **Financial market infrastructures**: trading venues, central counterparties
- **Health**: healthcare settings
- **Water**: drinking water supply and distribution
- **Digital infrastructure**: internet exchange points, domain name system service providers, top level domain name registries

'NIS Directive'

OESs should :

- **Take appropriate security measures**
  - to manage the risks
  - to ensure a level of security appropriate to the risk
  - to prevent and minimise the impact of incidents and ensure the continuity of the services

- **Notify incidents with significant impact on the continuity of the essential services to the relevant national authority**
  - without undue delay
  - providing information enabling determination of any cross-border impact

'NIS Directive'

Digital Service Providers (DSPs)

Important digital businesses (*)

DSPs in NIS scope

- Online marketplaces
- Cloud computing services
- Search engines

“light touch” regulatory approach

- light-touch and reactive ex post supervision
- minimise compliance burden
- ensure proper functioning of the Digital Single Market

(*) does not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC (1).

'NIS Directive'

DSPs should :

- **Take appropriate security measures**
  - Preventing risks
  - Ensuring security of network and information systems
  - Handling incidents

  Note : DSPs are free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems.

- **Notify substantial incidents to the relevant national authority**

'NIS Directive'

Implementation

- Essential services have first to be identified, criteria and thresholds defined & OESs designated
- OES security requirements will only apply to IS that are critical for the provisioning of essential services
- Baseline security requirements will be based on international standards (e.g. ISO 2700x) - Contribution of OESs will be highly appreciated
- Hygiene rules as defined in FEDIL-EY study 2016 may be considered as a fair starting point
- Sector specific security requirements may be developed with/by the sectors

- Bill of law is scheduled to be submitted to the parliament Q3 2017

info@anssi.etat.lu

Tél. 247-88935

Thank you for your attention