Systems and Information Security SEGSI

Topic 9

NIS2

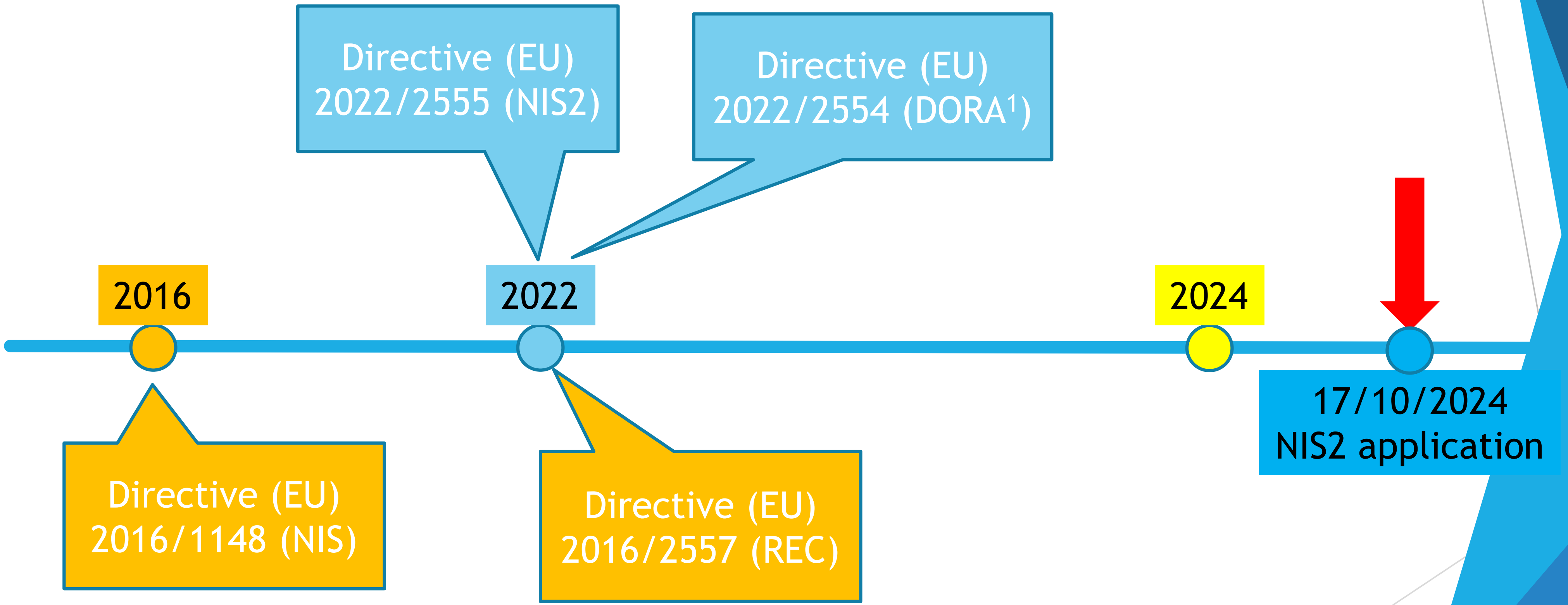
Pinto Leite, Jorge (jpl@isep.ipp.pt)

Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

General view of current state

- Cybersecurity is mandatory since a long time ago due to political, financial and personal reasons
- In 2014 EU produced the Regulation 910/2014 that implemented measures to avoid frauds on electronic transactions
- In 2016, EU published Directive 2016/1148 with the intention to provide an high common level of security on technology usage
  - It is now usually referred as NIS (Network and Information Security) 1
- However, an huge increase of interconnections and technology usage was experienced since than, so a newer version (NIS2) was published on 2022 (Directive 2022/2555)

Normative frame



Directive (EU) 2022/2555 (NIS2)

Directive (EU) 2022/2554 (DORA[1])

2016

2022

2024

17/10/2024 NIS2 application

Directive (EU) 2016/1148 (NIS)

Directive (EU) 2016/2557 (REC)

[1] DORA – Digital Operation Resilience Act, applied to financial institutions

NIS2 aims

- *Preserve a global and open Internet, by using and reinforce all instruments and resources available, with the objective to guarantee and protect European values and the fundamental rights of each citizen*
- It makes some changes to the previous version
  - A common cyber shield to all EU
    - Composed by SOC that makes use of AI and an automatic learning to detect early signs of imminent cyberattacks, allowing for a joining operation before any damage happen
    - A conjunct cyber unit (UE-CyCLONe) that gather all cybersecurity communities, allowing them to share threat perceptions e react collectivity
    - European solutions to improve Internet security worldwide, including an European registration of all DNS service providers, the registered TLD[1] (managed by ENISA)
    - Regulation of IoT
    - A solid EU cyber diplomacy toolbox to prevent, dissuade e give answers to cyberattacks (EU Cyber Diplomacy Toolbox)
    - An enforced cooperation to cybersecurity, mainly thanks to the revision of the European strategic frame for Cyber defense (Cyber Defense Policy Framework)

[1] Top Level Domain

NIS2 – Why was it proposed?

- The digital transformation of society, greatly accelerated during the coronavirus crisis, has multiplied and diversified the threats and is giving rise to new challenges that demand adapted and innovative responses
- In order to be able to analyze the impact and identify the shortcomings of the current NIS Directive, the Commission carried out a wide-ranging stakeholder consultation and identified the following main problems
  1. Insufficient level of cyber resilience of companies operating in the EU;
  2. Large differences in the resilience of different Member States and sectors;
  3. Insufficient common understanding of the main threats and challenges among member states and lack of common crisis response capacity

NIS2 – What are its main elements? (i)

- It removes the distinction between operators of essential services and digital service providers
- Strengthens and simplifies the security and communication requirements imposed on companies
- It covers the security of supply chains and relations with suppliers:
  - At European level, the cybersecurity of supply chains has been strengthened with regard to the main information and communication technologies of information and communication technologies
  - Member States may, in collaboration with the Commission and ENISA (ENISA (europa.eu)), carry out coordinated risk assessments of critical supply chains

NIS2 – What are its main elements? (ii)

- It introduces tougher supervisory measures for national authorities and stricter enforcement requirements in order to harmonize sanctions regimes between member states
- The framework for fines has been significantly increased - to the level of the GDPR
- It also strengthens the role of the cooperation group and intensifies information sharing and cooperation between member state authorities
- NIS2 must now be transposed into national law by national legislators by 17 October 2024 and will apply from 18 October 2024

NIS2 – What sectors and entities are included?

- It splits entities into categories *essential* and *important*, subjected to different requirements
  - **Essential**
    - Energy (electricity, district heating and cooling, oil, gas and hydrogen); transport (air, rail, inland waterways and road); banking; financial market infrastructures; health; manufacture of pharmaceuticals, including vaccines, and essential medical devices; drinking water; waste water; digital infrastructures (internet exchange points; datacenter service providers; top-level domain name registries; cloud computing service providers; datacenter service providers; content distribution networks; trust service providers; public electronic communications networks and electronic communications services; public administration; and Internet space
  - **Important**
    - Postal and courier services; waste management; chemical products; food products; manufacture of other medical devices, computers and electronic products, machinery equipment, motor vehicles and digital service providers (online marketplaces, online search engines online marketplaces, online search engines and social networking service platforms)

NIS2 – Reinforced obligations

- Essential and important entities must implement technical, operational and organizational measures to manage the risks posed to the security of their networks and information systems and to prevent or minimize the impact of incidents
- These measures should cover, among other things, areas such as incident handling, continuity of continuity of operations, the use of encryption and secure authentication and training
- The management bodies of essential and important entities can also be held responsible for non-compliance with the provisions of the NIS Directive2

NIS2 – Article 21

- *2. Measures [...] shall be based on an all-hazards approach to protect network and information systems and their physical environment against incidents and shall cover at least the following network and information systems and their physical environment against incidents, and shall cover at least the following aspects:*
  - a) ***Risk analysis and information systems security policies;***
  - b) ***Incident handling;***
  - c) ***Business continuity, such as backup management and disaster recovery, and crisis management;***
  - d) ***Supply chain security, including security aspects relating to the relationship between each organization and its suppliers or service providers. suppliers or direct service providers;***
  - e) ***Security in the acquisition, development and maintenance of network and information systems, including the treatment and disclosure of vulnerabilities. vulnerabilities;***
  - f) ***Policies and procedures for assessing the effectiveness of cybersecurity risk management measures;***
  - g) ***Basic cyber-hygiene practices and cybersecurity training;***
  - h) ***Policies and procedures regarding the use of cryptography;***
  - i) ***Human resources security, access control and asset management policies;***
  - j) ***Use of multi-factor authentication or continuous authentication solutions, secure voice, video and text communications and secure emergency communications systems within the organization, where appropriate.***

NIS2 – Article 23

- Essential and important entities must notify, without undue delay, the national computer security incident response teams (CSIRT) or, where appropriate, the competent authority, of any incident that has a significant impact on the provision of their services:
  - Has caused or is likely to cause serious operational disruption of services or financial loss to the organization concerned
  - Has affected or is likely to affect other natural or legal persons, causing considerable material or immaterial damage
- Measures to fulfill this requirements
  - A “rapid alert” within a timeline of 24h after being aware of the incident
  - An incident notification within a timeline of 72h that will update the rapid alert
  - If requested, an interim report
  - A final report no later than one month after incident notification
  - In certain situations, notification to the recipients of the service may also be required

NIS2 – Article 32

- Competent authorities will be able to rely on a solid set of enforcement and investigative powers, such as the ability to:
  - On-site inspections and remote supervision, including random checks carried out by professionals qualified professionals
  - Carry out safety audits
  - Requests for access to data, documents and information
  - Requests for evidence of the application of cybersecurity policies

NIS2 – Fines

- Essential entities
  - Maximum of 10.000.000 € or 2% of annual worldwide turnover
- Important entities
  - Maximum of 7.000.000 € or 1,4% of annual worldwide turnover
- In both cases, the maximum fine is the greater of the possibilities
- If due an audit or execution action of a cybersecurity incident the authorities become aware of a personal data breach, they shall without undue delay inform the national privacy authority