NIS2 & DNS Industry: Overall introduction

ICANN78 Day Zero Workshop, 20 October 2023

Juuso Järviniemi, Policy Officer
Unit H2 – Cybersecurity and Digital Privacy Policy
DG CONNECT, European Commission

NIS2: Overall context

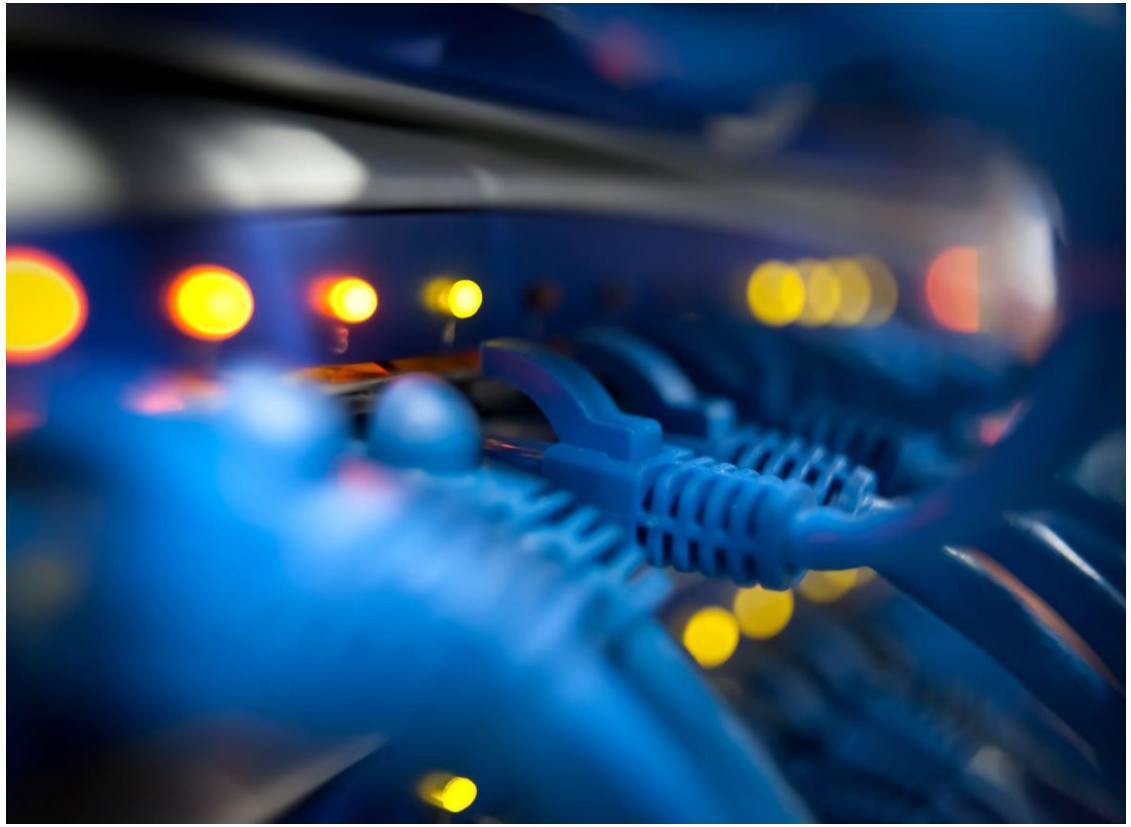
- Directive adopted December 2022 -> transposed into national laws by **October 2024**
- Measures for a high common level of cybersecurity:
  - Cybersecurity frameworks & cooperation at EU level
  - Risk management measures & reporting obligations
- Replaces the first NIS Directive from 2016

NIS2: Entities in scope

- Principle: Entities in scope are
  - **public or private entities**
  - of a **type referred to in Annex I or II**
  - which qualify as **medium-sized enterprises** under Article 2 of the Annex to Recommendation 2003/361/EC, or **exceed the ceilings for medium-sized enterprises** provided for in paragraph 1 of that Article,
  - and which **provide their services or carry out their activities within the Union**.

NIS2: Entities in scope

- TLD name registries and DNS service providers are **essential entities**, regardless of size
    - Excludes operators of root name servers
- Regardless of size, NIS2 applies to entities providing domain name registration services
    - However, not defined as “essential” or “important” entities

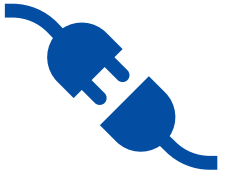


European Commission

Definitions

- **TLD name registry**:
  - Entity which has been delegated a specific TLD, and is responsible for administering the TLD
  - Irrespective of whether any of the operations are carried out by the entity itself or outsourced
  - Excludes situations where TLD names are only used by a registry for its own use
- **DNS service provider**:
  - Provides publicly available recursive domain name resolution services for Internet end-users, or
  - Authoritative domain name resolution services for third-party use – excluding root name servers
- **Provider of domain name registration services:**
  - Registrar, or
  - Agent acting on behalf of registrars (e.g. proxy registration service provider or reseller)

Minimum set of security requirements



- Policies on **risk analysis** and information system security
- **Incident handling**
- **Business continuity**, such as backup management and disaster recovery, and **crisis management**
- **Supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- Security in network and information systems **acquisition, development and maintenance**, including vulnerability handling and disclosure
- Policies and procedures to assess the **effectiveness** of cybersecurity risk-management measures
- Basic **cyber hygiene** practices and cybersecurity **training**
- Policies and procedures regarding the use of **cryptography** and, where appropriate, **encryption**
- **Human resources** security, **access control** policies and **asset management**
- Use of **MFA** or continuous **authentication solutions**, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

More harmonised incident reporting obligations

- Essential & important entities have to report significant incidents to the CSIRT or competent authority
- **Multiple-stage approach**:
  1. Early warning, without undue delay and at the latest within 24 hours of becoming aware of the significant incident,
  2. Incident notification, without undue delay and at the latest within 72 hours
  3. Final report, no later than one month after incident notification.

Implementing acts

- Certain entities should be subject to a high degree of harmonisation at EU level due to their cross-border nature.
- Implementing acts to be adopted by Commission, by **October 2024**:
  - Technical and methodological requirements for risk management measures
  - Specifying cases where a cyber incident is considered significant (reporting obligations)
- DNS service providers & TLD name registries are in scope

Jurisdiction & territoriality

- General rule (Art. 26): Entities fall under the jurisdiction of the Member State (MS) where they are established
- Art. 26(1)(b): Jurisdiction by MS where the entity has its **main establishment**
  - Includes DNS service providers, TLD name registries, entities providing domain name registration services
- Main establishment: MS where decisions on cybersecurity risk management are predominantly taken
  - Fallback: MS where cybersecurity operations are carried out
  - Fallback: MS with the establishment with the most employees in the EU

Jurisdiction & territoriality

- Entity not established in the EU, but offers services in the EU -> obligation to nominate a **representative**
  - Natural or legal person, designated to act on the entity's behalf. May be addressed by competent authority or CSIRT
- Representative in a MS where services are offered
- Jurisdiction by MS where representative is established
- No representative -> any MS where services are provided can take legal actions

Registry of entities

- Art. 27: ENISA to create and maintain a registry of entities, and allow competent authorities to access it
  - DNS service providers, TLD name registries & entities providing domain name registration services are included
- Entities to submit information to the competent authorities by **17 January 2025**:
  - Name, relevant sector
  - Address of main establishment/legal representative; Contact details
  - Member States where the entity provides services
  - IP ranges (not forwarded to ENISA)

Thank you

European Commission