The Impact of NIS 2.0 on the DNS Ecosystem

Michael D. Palage
mpalage@infonetworks.global

InfoNetworks

419.Consulting

What is NIS 2.0?

- Network and Information Security (NIS 2.0)
- Directive **NOT** a Regulation
- Subject Matter – “lays down measures that aim to achieve a high common level of cybersecurity across the Union” (Article 1)
- Scope – “This Directive applies to public or private entities of a type referred to in Annex I or II” (Article 2)
- Annex 1 (Sector of High Criticality) / Annex 2 (Other Critical Sectors)

Why is it Important to the DNS Community

- Annex I, Paragraph 8 – Digital Infrastructure

8. Digital infrastructure	— Internet Exchange Point providers
	— DNS service providers, excluding operators of root name servers
	— TLD name registries
	— Cloud computing service providers
	— Data centre service providers
	— Content delivery network providers
	— Trust service providers
	— Providers of public electronic communications networks
	— Providers of publicly available electronic communications services

Article 6 - Definitions

(19) 'domain name system' or 'DNS' means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

(20) 'DNS service provider' means an entity that provides:

(a) publicly available recursive domain name resolution services for internet end-users; or

(b) authoritative domain name resolution services for third-party use, with the exception of root name servers;

(21) 'top-level domain name registry' or 'TLD name registry' means an entity which has been delegated a specific TLD and is responsible for administering the TLD including the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where TLD names are used by a registry only for its own use;

(22) 'entity providing domain name registration services' means a registrar or an agent acting on behalf of registrars, such as a privacy or proxy registration service provider or reseller;

Article 28 - Database of Domain Name Registration Data

- Paragraph 1 requires that “TLD name registries and entities providing domain name registration services” **shall** “collect and maintain accurate and complete domain name registration data in a dedicated database.”

- Paragraph 2 sets forth specific data elements that must be collected:
  - domain name
  - registration date
  - registrant’s name, contact email address, and telephone number.

- Paragraph 2 also requires the collection of the “contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.”

Article 28 - Database of Domain Name Registration Data (Continued)

- Paragraph 3 requires that "TLD name registries and the entities providing domain name registration services" **shall have publicly available** "policies and procedures, including verification procedures, in place to ensure that the databases … include accurate and complete information."

- Paragraph 5 requires that "TLD name registries and the entities providing domain name registration services" **shall** "provide access to specific domain name registration data upon lawful and duly substantiated requests by **legitimate access seekers**" … "without undue delay and in any event within 72 hours of receipt of any requests for access."

- Paragraph 6, obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to cooperate with each other.

NIS 2.0 - Recitals

- Recital 110 states “Legitimate access seekers are to be understood as any natural or legal person making a request pursuant to Union or national law. They can include authorities that are competent under this Directive and those that are competent under Union or national law for the prevention, investigation, detection or prosecution of criminal offences, and CERTs or CSIRTs

- Recital 111 states in part “TLD name registries and entities providing domain name registration services should establish policies and procedures to collect and maintain accurate and complete domain name registration data, as well as to prevent and correct inaccurate registration data, in accordance with Union data protection law. **Those policies and procedures should take into account, *to the extent possible*, the standards developed by the multi-stakeholder governance structures at international level.**”

NIS 2.0 – Recitals (Continued)

- Recital 111 additionally states “TLD name registries and the entities providing domain name registration services should adopt and implement proportionate procedures to verify domain name registration data. Those procedures should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification.”

- Recital 112 states “[f]or legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts.”

Article 21 - Cybersecurity Risk-Management Measures

- Paragraph 1 states “Member States shall ensure that **essential** and important **entities** take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.”

- Paragraph 2 states “[t]he measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and **shall include at least** the following:

  (d) **supply chain security**, including security-related aspects concerning the relationships between each entity and its **direct suppliers or service providers;**

Article 34 - General conditions for imposing administrative fines

- Paragraph 4 states that “Member States shall ensure that where they infringe **Article 21** or 23, **essential entities** are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a **maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.”**

Article 27 – Registry of Entities

- Paragraph 1 states that “ENISA shall create and maintain a registry of **DNS service providers, TLD name registries, entities providing domain name registration services**, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms, on the basis of the information received from the single points of contact.”

Article 26 - Jurisdiction and territoriality

- Paragraph 2 states that jurisdiction for “DNS service providers, TLD name registries and entities providing domain name registration services” shall be “the Member State **where the decisions related to the cybersecurity risk-management measures are predominantly taken**.” However, if this determination cannot be made then the “main establishment shall be considered to be in the Member State where the entity concerned has **the establishment with the highest number of employees in the Union**.”

- Paragraph 3 states that DNS service providers, TLD name registries and entities providing domain name registration services” … “not established in the Union, but offer[ing] services within the Union” shall “designate a representative in the Union.”

Article 14 – Cooperation Group

The Cooperation Group tasks include, but are not limited to:

- Providing guidance to competent authorities in relation to the transposition and implementation of this Directive;
- Exchanging best practices and information in relation to the implementation of this Directive;
- Exchanging advice and cooperate with the Commission on emerging cybersecurity policy initiatives;
- Carrying out coordinated security risk assessments of critical supply chains; and
- Organizing regular joint meetings with relevant private stakeholders from across the Union to discuss activities carried out by the Cooperation Group and gather input on emerging policy challenges.

Cooperation Group – Work Streams

- There are two Work Streams (WS) within the Cooperation Group that are directly relevant to the DNS Ecosystem:
  - WS for Digital Infrastructure and Providers
  - WS on WHOIS

- The WS on WHOIS has two Task Forces:
  - Task Force on Verification
  - Task Force on Legitimate Access

Thank You

Questions?