18 JULY 2024 • *Brussels, Belgium*

CENTR Board statement on the Cybersecurity risk management & reporting obligations for digital infrastructure under the Draft implementing regulation of the NIS 2 Directive

CENTR Key recommendations

- In order to provide legal clarity for essential entities, and ensure manageability of handling incident reporting for CSIRTs and competent authorities, CENTR calls for keeping Article 3 as focused as possible. A voluntary reporting mechanism available in NIS 2 Directive will provide necessary leverage for more ambiguous situations and facilitate cooperation between CSIRTs and essential entities.
- CENTR calls for further clarifications in Articles 5 and 6 regarding disruptions of authoritative domain name resolution service that should only include situations under control of the affected entity, within their managed network systems.
- In order to avoid the overlap of competence between authorities, CENTR calls for narrowing down a significant incident criteria in Article 6(c) to cover breaches of the integrity, confidentiality or authenticity of stored, transmitted or processed data in relation to technical operation of the TLD under the definition provided in the NIS 2 Directive.
- CENTR calls for including a reasonable and uniform transition period for compliance with the mandatory cybersecurity risk management measures in Annex.

Introduction

CENTR is the association of European country code top-level domain registries (hereinafter ccTLDs). All EU Member State and EEA country ccTLDs (such as .hu, .eu and .no) are members of CENTR.

CENTR members are at the core of the public internet, safeguarding the stability and security of the internet. The majority of European ccTLDs are non-profit organisations, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (i.e. registrars, end-users, rightsholders but also in cooperation with CSIRTs, law enforcement authorities and national governments).

ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain (TLD). ccTLD registries maintain a domain name registration database that contains technical and administrative data necessary to provide DNS services, as well as identity and contact information of domain name holders. Registration data can be queried by the general public using different protocols like the web, WHOIS and RDAP, each offering their own unique controls to comply with the EU General Data Protection Regulation (GDPR) and national data protection legislation. ccTLD technical operations differ largely depending on the infrastructure and software they use. These differences reduce the risk that a single vulnerability would affect all ccTLD operators.

ccTLDs are considered "essential entities" under the Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (hereinafter 'NIS 2 Directive'). As entities that are directly targeted by the provisions of the European Commission's Draft implementing regulation laying down rules for the application of the NIS 2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant, CENTR members appreciate an opportunity to provide feedback and would like to draw the European Commission's attention to the following areas of concern.

Definition of significant incident

General remarks

The Draft implementing regulation provides concrete definitions of significant incidents relevant for ccTLD registries in Articles 3-6. In general, CENTR would like to point out that the details provided for in Article 3 may be too prescriptive. We understand policymakers' intention to include as many situations as possible that could be considered significant for the relevant entities in scope of the Draft implementing regulation. However, it may result in overreporting of incidents that are outside of control of the affected entity. When reports in the media, as well as the complaints from the end-users are supposed to be taken into account, these are often not based on the factual evidence about the source of the incident, but are rather speculative. In addition, not all criteria in Article 3(2) are equal in their impact on the concerned entity, or helpful for assessing the reputational impact on the affected entity. In case of the foundational internet's infrastructure that is used for the provision of specific services used by other sectoral entities under scope of the NIS 2 Directive, unavailability of a domain name may be caused by a variety of reasons not necessarily under control of a TLD registry. It is, therefore, **advisable to include language that specifies the impact of a significant incident on the networks and systems managed by the affected entity,** rather than base it on arbitrary criteria like media reporting or complaints by customers of other providers.

It is also worth mentioning that all entities under the scope of the NIS 2 Directive are encouraged to voluntarily report incidents and near misses to CSIRTs and/or competent authorities (Article 30 of the NIS 2 Directive), which will most likely cover grey areas not envisaged by the Draft implementing regulation. In order to provide legal clarity for essential entities, and ensure manageability of incident reporting for the CSIRTs and competent authorities, it is advisable to keep Article 3 as focused as possible. A voluntary reporting mechanism will provide

necessary leverage for more ambiguous situations and facilitate cooperation between CSIRTs and essential entities.

Interplay with DNS service providers

CENTR would like to point out an overlap between provision of an authoritative domain name resolution service in Articles 5 (DNS service providers) and Article 6 (TLD registries). While the distinction between two types of operators is welcome and needed, as well as the level of detail and granularity in Article 5, we do see a potential confusion element for TLD registries and DNS service providers.

Due to the distributed nature of the DNS, the DNS queries for a specific domain name are served by several actors. TLD registries hold authoritative data for administration of domain names within their zone, while DNS service providers respond to DNS queries when users browse the internet by requesting data from authoritative databases across the DNS resolution chain (e.g., root name servers, TLD servers, and authoritative nameservers), and/or provide authoritative DNS services that host the DNS records for top, second, and third-level domains. It is not clear from the references to an "authoritative domain resolution service" in both Articles 5 and 6 which type of DNS resolution data is expected to be covered under both Articles and when. As a result, this unclarity may bring unnecessary overreporting or conflicting reporting by both types of entities. It is therefore **advisable to clarify in both Articles 5 and 6 that disruptions of authoritative domain name resolution service should cover situations under control of the affected entity, within their managed network systems**. The control over its managed network systems should also assume that the operator is able to experience and measure the impact of unavailability of its service. Clarifying language in both Articles 5 and 6 are, therefore, merited to exclude situations when operators may be obliged to report incidents outside of their control.

Concerning TLD registries, **we are in full support of including the complete unavailability of "authoritative domain name resolution service" for TLD registries in Article 6(a)**, as in our interpretation, the unavailability of service that is covered by Article 6(a) results in absence of the TLD from the internet. Without any further guidance on the definition of "authoritative domain name resolution service", we expect national authorities to take into account the nature and the role of different actors within the DNS resolution chain and align their reporting expectations accordingly.

The integrity, confidentiality or authenticity of stored data

Article 6(c) includes a reference towards compromising the integrity, confidentiality or authenticity of stored, transmitted or processed data *related to the administration of the TLD*. According to the TLD definition provided in the Article 6(21) of the NIS 2 Directive, administration of the TLD covers "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" (emphasis added).

When it comes to the maintenance of a database of domain name registration data, including domain name holders' personal data, the NIS 2 Directive includes a separate set of obligations in Article 28. Considering the

fact that the database of domain name registration data contains personal data, any reports of the breaches of integrity, confidentiality, and authenticity of that data should be reported to the competent authorities under the EU GDPR, in case these are likely to result in a risk to the rights and freedoms of natural persons. In order to avoid the overlap of competence, it is advisable to specify that a significant incident under the NIS 2 Directive **covers breaches** of the integrity, confidentiality or authenticity of stored, transmitted or processed data **in relation to technical operation of the TLD under the definition provided in the NIS 2 Directive.** However, there might be situations when incidents within technical operation of TLD may involve personal data breaches. In these situations, it may be beneficial to allow for automatic involvement of data protection authorities through the existing cybersecurity incident reporting channels.

Technical and methodological requirements of cybersecurity risk-management measures

Annex of the Draft implementing regulation provides an extensive list of technical and methodological requirements mandatory for all concerned entities to implement in order to be compliant with the NIS 2 Directive.

First, CENTR would like to point out that albeit the list of technical and methodological requirements in Annex is clearly inspired by well-established and adopted industry standards, such as the ISO 27000 family standards for information security and the NIST Cybersecurity Framework, it takes away the risk-based approach by making all requirements in the Annex mandatory. While the established ISO/IEC 27001 is set on a risk-based approach to determine the controls needed to manage the cybersecurity risks depending on the risk profile, having an Annex with mandatory measures assumes a stricter baseline security for all affected entities, without the possibility to reassess whether all measures might or might not be applicable to the targeted industry. There is also an inherent contradiction between Section 2 that asks for identification and justification of chosen cybersecurity measures based on the risk management framework, and the rest of the mandatory measures in the Annex. When making measures mandatory, the link to risk assessment and risk management becomes irrelevant. We still believe that risk assessments are important and can be utilised as an operational tool to determine priorities in vulnerability management, security requirements in development or acquisition, etc[1]. Some flexibility for operators to be able to conduct risk assessments based on their specific role and risk profile is desirable.

This is something that competent authorities would need to keep in mind when supervising compliance of an extensive list of entities covered by the NIS 2 Directive, considering essential entities are subject to stricter ex ante supervisory regime. More clarity on conformity with the measures in Annex for essential entities and their interplay with the well-established international standards is needed. We expect national authorities to provide further guidance, depending on the national context.

[1] See also PCI-DSS 4.0, 6.3 Security vulnerabilities are identified and addressed.

Second, considering an extensive list of mandatory requirements that does not address the specificities and the size of the operators, and takes a rather 'one size fits all' approach when it comes to managing cybersecurity, CENTR would like to draw EU policymakers' attention towards inadvertent impact on small operators within the DNS ecosystem. The all-encompassing approach of the NIS 2 Directive to include entities of all sizes and business models within the DNS ecosystem will have an impact on the ecosystem, and will likely drive towards more centralisation and homogeneity of operators currently active in the field. CENTR calls on the **European Commission and EU Member States to increase support and cybersecurity capacity building for small operators**. This is especially important within the European context, where small and medium sized enterprises (SMEs) are the backbone of Europe's economy[2].

CENTR would also like to point out a potential mismatch with expectations under supply chain management in Section 5 of the Annex, and upcoming legal requirements under the Cyber Resilience Act (CRA), that take into account the special status of Free and Open Source Software (FOSS) development ecosystem. As FOSS is widely used and embedded within the foundational internet's infrastructure, we welcome the attention given to the FOSS ecosystem within the regulatory discussions on CRA, and would like to see that complexity to be reflected in Section 5. CENTR calls for the recognition of the role of FOSS in the development of the internet's infrastructure and further alignment between Section 5 and the CRA.

We also expect further assistance from the European Commission and the EU Member States in assessing cybersecurity risks of critical products necessary for essential entities, as well as a close alignment of the measures in Section 6 of the Annex of the Draft implementing regulation and the essential requirements under Annex I of the CRA. The burden of providing the necessary assurance with cybersecurity requirements under Annex should fall on the manufacturers of commercial products with critical dependencies for the provision of the internet's infrastructure. Conformity assessment procedures under the CRA can alleviate some of the compliance burden for essential entities, especially in situations of contractual imbalances between parties of different size and organisational structure.

Due to the aforementioned reasons, CENTR calls for a reasonable transition period for compliance with the mandatory measures in Annex. Even for organisations that are already certified under the international information security frameworks, existing certifications would not be sufficient to comply with the measures in the Annex of the Draft implementing regulation. A reasonable transitional timeline for all entities in scope, considering the exponential expansion to more operators previously not captured by the NIS Directive, as well as to alleviate compliance burden for SMEs and non-profit organisations, should be a timeframe of 24-36 months after the implementing regulation enters into force. In addition, in order to support a high common level of cybersecurity across the Union the transitional timelines should be consistent across the EU, and be favourable to essential entities and competent authorities alike, as the number of entities in scope is significantly higher than under previous regulatory regime. The uniform transitional timeline will allow both operators and competent authorities to increase their levels of preparedness and increase the overall levels of cybersecurity across essential sectors.

[2] According to the European Commission's data, 99% of European businesses are SMEs.