Directive (EU) 2022/2555 of the European Parliament and of the Council

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Reference:
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1707845859948

M[3]AAWG Comments on the Transposition of NIS2 Directive into EU National Law

M[3]AAWG, the Messaging, Malware and Mobile Anti-Abuse Working group, appreciates this opportunity to comment on the transposition of the Revised Directive on Security of Network and Information Systems (NIS2) into EU national law.

We make these comments in our capacities as cybersecurity professionals and researchers committed to ensuring the security and stability of the internet, including the domain name ecosystem. M[3]AAWG supports the robust transposition of the draft EU national law and notes that many of the obligations included in NIS2 are key to M[3]AAWG members who require access to registration data in order to detect threats, investigate new attack vectors, and to understand trends aimed at protecting users and the internet as a whole.

M[3]AAWG appreciates the opportunity to comment on the current draft text and detail our suggested clarifications below for your consideration.

- **Definition of legitimate access seekers.** Recital 110 of NIS2 defines "legitimate access seeker(s)" of domain name registration data (commonly known as WHOIS) as "any natural or legal person making a request pursuant to Union or national law." EU national law should ensure that "legitimate access seekers" includes any natural or legal person making a request to access WHOIS data to investigate illegality, including for the investigation, establishment, exercise, or defense of cybersecurity, intellectual property,[1] consumer protection, or other legal claims, in addition to governments and law enforcement personnel. It is the experience of M[3]AAWG members that law enforcement agencies often collaborate with and rely upon independent researchers and non-governmental organizations to track and combat illegal online activity. This is consistent with the approach taken by the European Cybercrime Centre, which "aims to engage public and private sector stakeholders whose skills, resources, and reach are needed alongside law enforcement efforts to create a safer digital environment."[2]

[1] Threat actors often abuse their corporate victims' trademarks, designs, logos, etc. to victimize end users.
[2] See: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

- **Shorten the timeline for disclosure.** Article 28(5) of NIS2 states that TLD name registries and the entities providing domain name registration services are required to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Based on our experience and empirical research, this time period represents a significant, often detrimental, delay for investigators, private and law enforcement.For optimal results, immediate access to registration data is often necessary in order to investigate and mitigate cybercrime.
    - **M^{3}AAWG recommends that the text be clarified to read that the disclosure of registrant data must occur within these 72 hours, not just that a response, like a receipt notice, must be sent within 72 hours.** Without this clarification, it is possible that the response would not be actionable information.
    - M^{3}AAWG recommends that **the time period be shortened from 72 to 24 hours.**

- **No cost to requesters.** NIS2 Recital 112 states that "Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge." Although Article 28 does not separately address this issue, it is important to ensure that the EU national law addresses this important point.

- **Disclosures of customer information related to proxy or privacy services.** NIS2 defines "entities providing registration services" to specifically include proxies and similar service providers. Article 28(5) requires entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests.

    - M^{3}AAWG recommends that EU national law clarify that when a proxy or privacy service is involved, the disclosures to legitimate access seekers must include the complete, accurate, and verified data of the **customer or beneficial user** of the domain name. Without this clarification, it is possible that only the contact information of the service provider offering privacy or proxy services would be disclosed.

- **Accuracy and verification of registration data.** Under NIS2 Article 28(1) and (3), TLD name registries and other "entities providing domain name registration services" must verify the accuracy of WHOIS data. Clearly, these obligations should also apply to all privacy and proxy service providers and domain name resellers. In addition, NIS2 Recital 111 requires procedures to prevent and correct inaccurate registration data in accordance with the best practices used within the industry, taking into account developments in the field of electronic identification**.** EU national law should ensure that this important recital be included in its draft law and should reference the best practices conducted by EU-based ccTLDs, which result in far lower rates of abuse and cybercrime.[3]

[3] See Habits of Excellence: Why are European ccTLD abuse rates so low?

- **Mandatory database requirements for registries.**
  M[3]AAWG recommends that national law clarify whether TLD registries must maintain a separate database in addition to the database maintained by a domain name registrar. The M3AAWG membership discussed NIS2 and two main interpretations of Article 28 have emerged, summarized below. It is important that there be no ambiguity, which is why we are asking for clarification if the national transposition of NIS2 requires a "thick registry" approach, or permits a "thin registry approach", and if so, under which circumstances.

  NIS2 Article 28 Sections 1-5 state that "*TLD name registries and the entities providing domain name registration services*" are required:

  > (1) […] *to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence in accordance with Union data protection law as regards data which are personal data.*
  >
  > (2) [the database must contain] *the necessary information to identify and contact the holders of the domain names and the points of contact administering the domain names under the TLDs. Such information shall include: the domain name; the date of registration; the registrant's name, contact email address and telephone number; 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.*
  >
  > (3) […] *to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information.*
  >
  > (4) […] *to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data.*
  >
  > (5) […] *to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law.* […]

  Article 28 Section 6 also states that:

  > (6) *Compliance with the 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.

The following interpretations of the requirements in Article 28 have surfaced during internal discussions by M[3]AAWG members and we would ask member states to clarify the specific requirements for registries:

Interpretation 1:

Some M3AAWG members interpret the language of Section 6, Article 28 of NIS2 above to mean that "*non-duplication of collection*" **applies to the collection from the data subject and registrant only, not changing the obligation for registries to "maintain" a separate database of registrant information** (i.e. requiring a "thick registry" approach). Based on this reading, it would be **necessary for the registry to maintain a separate database** to comply with the verification, accuracy, access, and disclosure requirements described in Article 28.

Having the registry maintain a separate database (including the customer data of any privacy or proxy provider) would require registrant data to be available at the registry in addition to the registrars' databases for cybersecurity investigations and mitigations even if the registrar is located outside of the relevant jurisdiction, or if the registrar is non-responsive. Thus, this approach may promote the swift mitigation and prevention of cybersecurity attacks.

Interpretation 2:

Other M3AAWG members read the language of Section 6, Article 28 of NIS2 to **permit the data to be maintained and stored by the registrar only** (i.e. permitting the "thin registry" model), with the registry and registrar jointly carrying out their obligations under Article 28. Based on this reading, **it would *not* be necessary for the registry to maintain a separate database to comply with NIS2's verification, accuracy, access, and disclosure requirements**, avoiding the duplication of registrant data in multiple places and shared by different controllers/processors.

This reading emphasizes the direct contractual relationship registrars have with registrants, and their need to collect the required registrant information in order to effectuate a domain name registration. Implementing the principle of data minimization per GDPR Article 5(1)(c), TLD name registries would not need to process or store personal data of registrants in order to carry out their registry function, as data are available from registrars. This approach may mitigate risks related to the duplication and processing of personal data by multiple entities.

M[3]AAWG and its members request that transpositions into relevant national laws specifically indicate which of the above interpretations of NIS2's Article 28 is to be followed.

For more information on M[3]AAWG's perspective on these important issues, please kindly refer to our submission during a public consultation on NIS2 in March 2021.

We appreciate your consideration of our input on this important law, and we welcome the opportunity to engage as needed to answer any questions during this process. Please address any inquiries to

Sincerely,
Amy Cadagin, Executive Director
Messaging Malware Mobile Anti-Abuse Working Group
comments@m3aawg.org
P.O. Box 9125
Brea, CA 92822