Solna 2021-03-18

Netnod have reviewed the proposed directive on measures for a high common level of cybersecurity across the Union and have the following comments.

Regarding **CSIRTs** Netnod repeats what we have said in earlier consultations,[1] that it is not only the reporting to a CSIRT that is important, but also what a CSIRT produces with the help of that information. Specifically, we believe the reason why organisations report to a CSIRT should not only be based on penalties for not reporting, but the fact the more data a CSIRT gets, the better reports they can produce. The directive because of this should include requirements for CSIRTs to produce good reports.

Regarding the **domain name system (DNS)** the definitions must be much more clear. Netnod have sent in comments earlier[2] regarding the unclear definitions in the existing NIS directive and its implementation. We can not see the definitions being better in this proposal. For example, we do not see recital 14 match what is specified in Article 4(13)-(15), and specifically we see overlap between recitals 14 and 15.

Regarding **DNS service providers**, we do not believe what is in recital 15 separates enough between the manager of zones, providers of authoritative servers and providers of recursive resolvers. The definition in Annex I is unfortunately making it more unclear. Separation must be done between the providers depending not only on the size of the organisation providing the service but also for example between providers of recursive services and authoritative servers. And further between providers of services for the root, TLDs and other zones further down the domain name hierarchy. Specifically, Netnod do **not** believe the directive *should apply to all providers of DNS services along the DNS resolution chain*[3].

[1] Netnod response (in Swedish) to consultation related to implementation of the NIS directive in Sweden 2017-08-08, https://www.netnod.se/sites/default/files/Pressreleases/Remissvar%20NIS-Direktivet_signed.pdf
[2] Netnod response (in Swedish) to a consultation related to implementation of the NIS directive related to DNS in Sweden 2020-08-17, https://www.netnod.se/sites/default/files/Pressreleases/Remissvar%20NIS-Direktivet_signed.pdf
[3] Recital 15

Patrik Fältström
Technical Director and Head of Security
Netnod

Regarding **cross border provisioning of services** Netnod have sent in comments earlier[4] where we agree with the view that each organisation should only be under regulation in one member state, the one where they have their main establishment in the Union[5].

Regarding the proposed requirement for providers of services outside of the EU that provides services in the EU to **designate a representative within the EU[6]**, we do not see that being possible to implement for DNS. Specifically together with the unclear definitions of providers of DNS service providers.

Regarding **small and medium companies that are excluded** from the directive, we find such entities are excluded based on the meaning of Commission Recommendation 2003/361/EC of 6 May 2003. But at the same time it allows the Commission, in cooperation with the Cooperation Group to issue guidelines on the implementation of the criteria applicable to micro and small enterprises. This uncertainty is by itself an increasing cost for preparation for implementation.

We find **providers of public electronic communications networks or publicly available electronic communications services and domain name system (DNS) service providers** referred to in point 8 of Annex I be covered be covered by the directive regardless of size, which is something that we do not find being acceptable as long as for example domain name system (DNS) service providers are not more well defined as Netnod comments above.

These SME providers include both established entities and startups that will grow larger. The directive is not taking these players into account, neither in the way they are included or excluded (and the uncertainty), nor in the description of the role of CSIRTs in their interactions with SMEs. Specifically the supporting function the CSIRTs can have for SMEs.

Netnod do in general support the initiative the Commission has initiated to refine its **Cybersecurity Strategy for the Digital Decade** and operationalize its contingency plan for dealing with extreme scenarios, including integrity and availability of the global DNS root system. Netnod wants to emphasize that as the Internet is a global network, it requires a single globally unique name space. This is rooted in the one and only root zone managed by processes defined by the multi stakeholder processes hosted and defined by the Internet Corporation for Assigned Names and Numbers (ICANN), where Internet Assigned Numbers Authority (IANA) is the source of the root zone data. This *One Internet* has been, and should continue to be, a core principle guiding all Member State's and Commission's actions and any plan should take care not to fracture the single, authoritative root in any way. This must

[4] Netnod response (in English) to a consultation related to implementation of the NIS directive related to IXPs in Denmark 2017-11-24, https://www.netnod.se/sites/default/files/Pressreleases/Svar%20Forsvarsministeriet%20Sagsnummer%202017.pdf
[5] Recital 64 and Article 24 (1)
[6] Recital 65 and Article 24 (3)

specifically be taken into account when implementing Article 23 of the proposed NIS2 Directive. The root must remain “unbroken” and implemented in a way so that the Internet remains a global interoperable network. Otherwise it could create a precedent for other countries outside of the EU Member States that may seek to regulate DNS and the Internet in such a way that it is fragmented, and global communication ends up being impossible.

Patrik Fältström
Technical Director and Head of Security
Netnod