Stockholm 2024-07-25

European Commission

In response to: Ares(2024)4640447
Our ref: 24-006

Netnod welcomes the opportunity to provide feedback on the consultation launched on 27 June on the “Cybersecurity risk management & reporting obligations for digital infrastructure, providers and ICT service managers” implementation act of the larger NIS2-framework. It consists of an implementation act and an annex.

Netnod hereby gives the following commentary on the proposal:

- It defines incidents based on whether explicit metrics have been achieved or not **Netnod suggests that significant incidents are defined as incidents which lead to actual negative impact on for the society essential services**
- In an ex-ante manner, it sets requirements on measures to be implemented **Netnod suggests that the act should define requirements on services in an ex-post manner, and leave the choice of measures entirely up to the covered entity**
- It relies on the ability to for a covered entity to identify its role in a supply chain **Netnod suggests the act needs to explicitly take into account any kind of business relationships and not only contractual agreements, and in that context specifically recognize suppliers of wholesale services**

Please see the appendix for further motivations and elaborations.

Patrik Fältström
Chief Security Officer

Tel: +46-706059051
Email: paf@netnod.se

Netnod AB
Greta Garbos väg 13
169 40 Solna
Sweden

Appendix - Detailed comments

1. Introduction

The issues mentioned stems from the fact that NIS2 takes an all-hazards approach to risk and threats, and that in the form of ex-ante regulation. Netnod strongly believes this is the wrong thing to do. The regulation should not specify the threats and risks organisations have to handle.

Instead NIS2 should set requirements on for the society essential services to be well functioning also under stress, and allow the organisations covered to formulate risk and threats and specifically allow the organisation to decide how to mitigate the identified risks.

There is no scientific evidence that an all-hazards approach is the most productive risk approach for public preparedness.

> The All-Hazards approach presents several arguable advantages; yet, when tested against reality, it often fails to deliver optimal results in terms of public preparedness
>
> (abstract, Bodas et al., 2020)[1]

Instead, evidence points towards the fact that well defined risks and threats which can be appropriately practised and exercised lead to a higher effectiveness of preparedness (see, among others, Adini et al., 2012[2] and Bayntun, 2012[3]).

In short, Netnod argues that the legislation should, through ex-post means and minimal ex-ante means, regulate requirements for which covered entities freely can choose solutions and continuously improve upon those to over time ensure the society is well functioning.

2. Incidents should be defined by their consequences

The implementation act suggests metrics for the decision of whether a significant incident has occurred or not. Some of these metrics can be reached without loss of function, or without damages caused. This implies entities because of this might have to report significant incidents even if the event itself did not lead to negative impact on the essential service.

The NIS2-directive specifies that an incident shall be considered significant if, among other things, “*it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage*” (p. 129, NIS2-directive).

[1] Bodas, M., Kirsch, T. D., & Peleg, K. (2020). Top hazards approach–rethinking the appropriateness of the all-hazards approach in disaster risk management. International journal of disaster risk reduction, 47, 101559.

[2] Adini, B., Goldberg, A., Cohen, R., Laor, D., & Bar-Dayan, Y. (2012). Evidence-based support for the all-hazards approach to emergency preparedness. Israel Journal of Health Policy Research, 1(1), 40.

[3] Bayntun, C. (2012). A health system approach to all-hazards disaster management: A systematic review. PLoS Currents, 4.

As an example, the suggested implementation act allows for an event to be considered a “significant incident” if the event has been reported in the media. This means, conversely, that the media, or rather public opinion, can decide if an event is a significant incident or not, and thus force the release of information by the affected entity.

For the point of argument, here follows some issues with the measurements of Article 5 of the implementation act pertaining to DNS service providers and TLD name registries.

> **Article 5:**
> (b) for a period of more than one hour, the average response time of a recursive or authoritative domain name resolution service to DNS requests is more than 10 seconds,

This criterion is arbitrary, as there is no magic limit at 10 seconds at which the functionality of the DNS system is severely impacted, or for that matter the services that rely on DNS for its functionality.

It is our view that any metric (in this case a time interval) chosen will lead to similar issues. The question whether an event is a significant incident or not has to be defined by the consequences of, in this example, the supposedly long(er) response time (than normal).

Or expressed differently, incidents should be defined by their consequences. Not by metrics.

3. Requirements must apply to the essential service, not describe measures to be implemented

At a general level, Netnod argues that ex-post legislation should be preferred over ex-ante legislation. But in the cases where ex-ante legislation is required, the regulation has to be written in such a way that it still does not prescribe solutions, only effects and requirements on solutions chosen by the covered entity.

This view follows what EU has already expressed, for example:

> (29) This Directive aims to progressively reduce ex ante sector-specific rules as competition in the markets develops and, ultimately, to ensure that electronic communications are governed only by competition law. Considering that the markets for electronic communications have shown strong competitive dynamics in recent years, it is essential that ex ante regulatory obligations are imposed only where there is no effective and sustainable competition on the markets concerned.
>
> (Directive (EU) 2018/1972)[4]

[4] DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code

For example, the current suggested annex discusses “backups”. Backups are a legacy solution to the business continuity problem. Modern services are designed with redundancy and diversity (one type of solution) in mind, so that they do not require backups (a different type of solution). The annex should not specify either type of solution, rather the requirements for the service, so that covered entities are free to choose a solution, and improve that chosen solution over time. And when they themselves decide, change the solution.

The idea of the inner market is seriously undermined when legislation begins to enforce solutions rather than requirements.

The annex is also very specific with mandatory requirements for process standardisation as a tool for solving organisational issues. We must remember that one specific form of organisational standard is optimal only for a subset of organisations.

For example, instead of prescribing specific “processes for crisis management” the annex should, in an ex-ante fashion, list external events which the organisation should be able to handle. That the covered entity does require some kind of processes will that way be implicit.

These could be relatively simple events, such as the main office being inaccessible, two hour electricity blackouts, unstable frequency in the electricity grid, lack of Internet access for four hours, all printers spontaneously combust, and so forth. Having “processes for crisis management” does not guarantee proper preparedness, i.e. that the impact of the event is so small that it is acceptable.

4. Identification of role in a supply chain

The annex, in section 5, specifies requirements for policies for supply chain management, and in particular:

> which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall ***identify their role in the supply chain*** and ***communicate*** it to their direct suppliers and service providers.
>
> (p.9, Annex)

This assumes that all NIS2-entities have explicit relationships with their suppliers, which in turn imply the existence of contractual obligations and communications.

However, in a digital context it is common that services are procured at a wholesale level. This implies that (wholesale) service providers do not know precisely what their services are being used for. This includes but is not limited to DNS services, electronic communications services, compute and storage (“cloud”), (open source) software, and similar services, where services are composed in multiple (wholesale) levels or layers presented together as a coherent unit to the end-user. Often as an aggregation of services provided by a multitude of providers.

As such, it is not without significant cost to “identify their role in the supply chain and communicate it to their direct suppliers and service providers”. In many cases it is simply an impossible task. Rather, it must be up to NIS2-entities to choose their solutions for managing their supply chains, where explicit contracts that delegate tasks (but not responsibility) is one of the possible measures.

For example, one such solution might be to use contracts and explicit communication with single providers, another solution might be choosing technical diversity by using multiple independent providers of wholesale services. Specifically in the latter case, the provider of the wholesale service can not know what their role in the supply chain is.

5. Summary

The increased focus on ex-ante legislation with a focus on processes is worrying. Ex-ante legislation must be kept at a minimum, and in cases where ex-ante legislation is used it must still maximise the possible solution space for covered actors, and specify requirements organisations should be able to handle.

NIS2-entities should be held accountable for production of essential services, not held accountable for whether they follow the by EU stipulated processes or not.