Stockholm 2023-01-23

European Commission

Your reference: COM(2022)454
Our reference: 23-001

On the 19th of September 2022 the EU Commission opened a feedback period on the commission adoption of the Cyber Resilience Act.

Netnod has the following comments on the content of the suggested regulation:

- There is no recognition that a product can consist of many components.
  Netnod is of the opinion that many products consists of products that might or might not exist on the wholesale market, and although one can build secure solutions with insecure components, the proposed regulation does not discuss what requirements there are on such components one build more complex products with, for example open source libraries used in a car.
- Requirements on the functionality of a product is not properly addressed.
  Netnod is of the opinion that having a description of the functionality is key to attaining cybersecurity (regardless of definition), and in this dimension the suggested regulation falls short.
- Updatability of products is not properly addressed, for example the situations where the manufacturer of the product does not provide support anymore.
  Netnod is of the opinion that all devices with software components need an upgrade route, and those who do not provide upgrade routes must publish specifications for third parties so that all software components can be upgraded.
- Default configurations are not properly addressed, by for example not defining what a *secure* default configuration implies.
  Netnod argues that a proper installation and setup process is key, no product should ever be accessible with default credentials or any other type of secret.
- Adherence to previously agreed on norms and standards is not covered in relevant detail.
  Netnod argues that a key component of security is the possibility to replace devices, therefore all configuration should be exportable and all products should follow relevant networking standards.

Netnod AB
Greta Garbos väg 13
169 40 Solna

At a high level Netnod is positive towards cybersecurity initiatives, but the current formulation risks doing more harm than good. Netnod is of the opinion that the four points above are enough for the first iteration of the directive.

In particular Netnod is of the opinion that certification should never be a requirement, but something market actors do willingly due to market positioning advantages. It is inherently problematic to force certification.

See appendix for detailed comments.

Patrik Fältström
Head of Security

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

Appendix 1 - Detailed commentary

1. Overarching comments

Netnod believes that it is enough if the regulation handles the below mentioned aspects. Many aspects of the regulation are either over-the-top or irrelevant for operational cybersecurity.

In particular all certification should be voluntary, and should be considered a market advantage rather than forced by regulation. A possible exception might be certain classes of consumer products which can be directly harmful to human life if they operate outside of specification, but individual certification of all components of a larger product, which might measure in the hundreds of thousands, is neither effective nor efficient.

The regulation should not address import, export, and similar issues of digital products. Rather the relevant import and export regulation should be improved to properly cover the accountability issues of importing and exporting products with digital components.

In general, the EU should concern itself with accountability of involved legal actors, not the requirements and specifications themselves. For example, the specifications in Annex I of the directive are dangerously naive and some of them are impossible to uphold (nor would upholding them have any measurable effect on cybersecurity).

For example, in Annex I the following is stated:

> *(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;*

This would indicate that unencrypted USB-memories should be forbidden, unencrypted WiFi forbidden, forbid unencrypted storage devices of all kinds, and so forth. It seems that the authors of Annex I do not realise the vast scope of products included in the current formulation of the regulation, and therefore include some quite absurd requirements.

As Netnod has noted in other arenas, for example in our comments on the European Electronic Communications Code and the NIS-directive, it seems that legislation focuses on some “end-user-interface” without any serious consideration for the composition of said product or service, regardless of if the service or product is an USB-memory stick, a rubber ducky with a microchip saying “***quack***”, or the entire Internet.

This is deeply problematic.

This is indicative of a lack of competence in the cybersecurity domain, and a considerable issue if the EU commission choses to continue down the indicated path.

2. Secure systems out of insecure components

The regulation does not take height for complex scenarios, such as those where open source software is used in a highly regulated environment, such as a truck, or when many or redundant components are used.

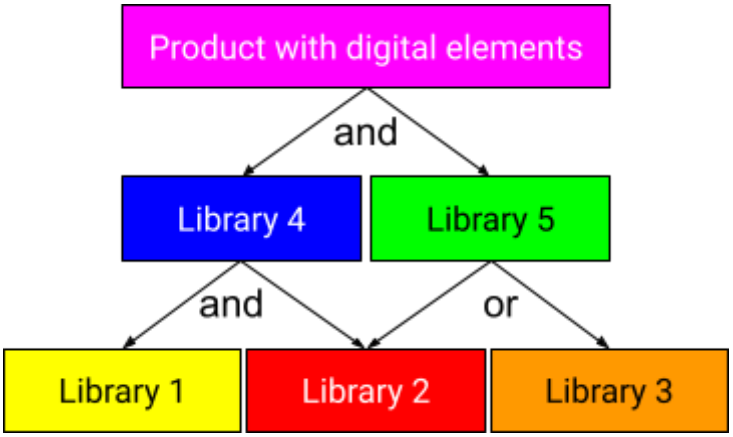

Figure 1: Illustration of dependencies in a complex product

For example, a product with digital elements might at a high level depend on two software components, which in turn depend on three other software components (e.g. libraries), as illustrated in the figure above. Here there is a vast difference between dependence on all of your dependencies, and dependence on a subset of dependencies. If, in the figure above, Library 4 is dependent on both Library 1 and Library 2, that means that if either of those libraries lose function, that Library 4 fails. Library 5, on the other hand, is dependent on either or of Library 2 or Library 3.

This means that if Library 1 or Library 2 fails, that Library 4 will fail and therefore the product will fail, i.e. the failure of a dependency propagates. However, if Library 3 fails, Library 5 will continue to function as it depends on either one of Library 2 and Library 3, i.e. the failure does not propagate.

Now, Figure 1 is illustrative, and meant to convey the problem that the security of individual, or sets of, components is secondary to the functioning of the system if the system is designed with redundancy in mind.

The idea that all components have to be secure for the system as a whole to be secure mostly stems from the aspect of **confidentiality**, which is one tenant of security. However, most digital products deal with **availability**, an aspect of security with other best practices than confidentiality.

Now, as Netnod has argued before[1], redundancy and diversity is a key design principle for availability in the digital age. Therefore it is problematic that the Cyber Resilience Act

[1] See, for example https://www.netnod.se/blog/security-diversity-business-security-through-diversity and https://www.netnod.se/blog/security-diversity-designing-secure-reliable-and-robust-systems

assumes that component failure is critical to the functioning of the product as a whole, instead of providing guidelines, or baselines, for how to assess and evaluate the security of products.

However, Netnod is of the opinion that the regulation should not dictate method or technique for attaining security, rather it should manage the accountability aspects of maintaining security. In such a way that actors are free to choose the methods for attaining security that they believe are the most appropriate for the task at hand, and hold them proportionally accountable if their security approach fails.

3. Functionality of products

The regulation needs to address the functionality of products in a meaningful way. For most intents and purposes, and for an initial regulation, it is enough to ensure proper descriptions of information inputs and outputs, storage of the product, and information regarding the use of the information collected by the product.

In addition, replaceability of products is key, and it should also be a requirement that all products need to include instructions for exporting the information in the product, for example the configuration, so that it is easier to replace the product with a competitor product.

4. Updateability of products

There is no perfect product, nor perfect software, and all products need to have a working update path in terms of all sorts of software (including firmware). The method used to update products should be documented, and available on demand to market surveillance authorities.

If the manufacturer does not provide an update path the market surveillance authority should be able to release the update documentation as provided and used by the manufacturer to ensure that third parties have the ability to update the product. This includes signing keys and other cryptographic information necessary to update the product.

As noted above, the end-of-life of the product is an important aspect to consider to avoid pitfalls related to end-of-life aspects of products and detrimental lock-in effects.

The earlier section describes proper documentation of the current behaviour of a product which should be included with the product, while this section describes proper documentation to alter the product which should be available to market surveillance authorities.

5. Forbid default configurations of connected products

Default credentials should never be exposed to the network. All products should have a setup process requiring personalization of credentials and similar secrets to vulnerabilities stemming from lack of configuration.

The current formulation in the annex is ***secure by default configuration***, which for all intents and purposes is quite fuzzy and does not specify measurable requirements in terms of security.

6. Interaction of products

All products should be required to follow relevant norms and standards related to interactions with other products or connected devices. This should in practice include, but not be limited to, following DHCP(v6), SLAAC, WiFi, IPv6, and similar networking standards.

As noted above, standards are not legal persons in the EU and should not be considered such in the regulation, and this effect should rather be introduced through a voluntary certification scheme. In this light a certified “Internet-of-Things”-product is less likely to mess up home- or corporate networks and should have a market advantage vis-a-vi similar products on the market lacking certification.

7. Summary

In summary, Netnod is positive towards the increased focus on cybersecurity, and that the EU takes cybersecurity seriously. However, the current approach is inherently problematic and the approach needs to be refined and improved to ensure increased cyber resilience, rather than just prioritising resources of firms towards potentially less effective mitigation techniques.

As most organisations have limited resources, enforcement of certification will inevitably reprioritize resources in line with the legal framework, rather than the most efficient allocation of resources for cybersecurity as deemed by the individual organisation for the particular task at hand.

Another important point in terms of cybersecurity is that most secure systems are built out of insecure components. That is, it is the composition of the system which designates the security of a system, not the security of the components on their own. Netnod believes that the Cyber Resilience Act should cover the composition *techniques* of secure systems, not the certification of components of secure systems (which is *one* possible technique).

Netnod argues that the points above; functionality, upgradeability, default configurations, and interaction of products, is a proper focus for an initial piece of legislation on digital products in the EU.