WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

STATEMENT

on the draft Commission Implementing Regulation on laying down rules for the application of Directive (EU) 2022/2555 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 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

Berlin, 25.07.2024

With the NIS2 Regulation entering into force late December 2022, the period devising transposition rules for the EU Member States started along with the deadline for the European Commission, to pass implementing regulations. Both will expire on 17 October 2024.

As per 27 June 2024, the Commission has published its draft Implementing Regulation on the NIS2 Directive and set it up for consultation. eco – Association of the Internet Industry would like to contribute the following aspects to the debate:

1. General Remarks

As a more detailed clarification of the rules already listed in the NIS2 Directive to strengthen cybersecurity, the intention of the Implementing Regulation is to be supported in principle. Unfortunately, the draft does not meet the demand. The scope and attention to detail, as well as the documentation effort resulting from many of the measures, will cause considerable effort for the companies concerned. In particular the implementation will cause problems, particularly for small and very small companies in the covered sectors and areas and will be almost impossible to manage. This is unlikely to be conducive to strengthening cyber security.

The release of the Implementing Regulation leaves member states approximately two more months to complete their own national legislation for the NIS2 transposition. This is unfortunate since member states will either be confronted with the challenge of being noncompliant with the European provisions of the Implementing Regulation or will be required to adjust their already passed national legislation ex post or at last notice possible in a legislative process. From the view of the Internet Industry, this is unfortunate and will without doubt create backlash against European regulation or legislation since companies will in any case have to

readjust their policies or, additionally, run the risk of being subjected to fragmented legislation. eco advocates for an extension of transposition timelines to allow Member States to adjust their legislation if necessary, and companies to adjust their policies and practices in a harmonized regulatory environment.

The Implementing Regulation does not clearly distinguish Trust Services, which are mostly regulated by the European eIDAS regulations and thus subject to uniform European regulation, whereas all other services covered by NIS2 are subject to national jurisdiction. This could pose challenges for the implementation of the Implementing Act throughout the EU. Furthermore, there might be a conflict with the eIDAS Regulation.

2. On the Implementing Regulation in Detail

- **On Article 3 Significant Incidents**

The criteria defined for assuming a significant cybersecurity incident are generally regarded as too broad and lacking actual correlation with operational impact and operational harm. The overbroad criteria occur to Art. 3 (1) a, where incidents are regarded as significant if they are “capable of causing financial loss […]”. It is hard for companies to actually calculate potential losses in advance since the question of economic damage is not necessarily defined by technical means but also by date or time of the day. In addition, the phrase “capable of” is so poorly defined, that it could address essentially any security incident. The Internet Industry requires these definitions and uptake-criteria to be further elaborated, specified and delivered in a precise manner allowing companies to determine whether a reportable significant incident has occurred.

Similar problems can be attributed to Article 3 (2) a, where “media reports” are regarded as a source for assuming significant incidents, which is further impacted by the provisions in Article 3 (2) b, where user complaints are regarded as relevant for the assumption of a significant incident.

It should also be stated that it is practically impossible to take a threshold of 100,000 € or 5% of turnover as the extent of damage for a reporting obligation within 24 hours. Damage cannot be quantified within 24 hours. It is difficult to assess such an estimation during an incident. A damage extent of 100,000 € is reached very quickly especially for larger companies. As an alternative, the Commission could raise the threshold to 500,000 €. This elevated value and the proportionality inherited in the 5% would account for both, larger and smaller entities. The impact on the functioning of society is not considered further here.

Additionally, setting different thresholds for assuming a significant incident and defining one being the lower as the relevant for reporting as this is the case with Article 3 (1) a, will increase the number of reports and significant incidents, which may create a vast amount of bureaucracy, documentation and will divert resources away from the actual reaction to a cyber security incident.

The criteria for assuming a significant incident should also be revised regarding possible redundancies, e.g. in Article 3 (1) f, where the assumption of a "successful, suspectedly malicious and unauthorised" access leads to the assumption of a significant incident. This would most likely overlap with other criteria set up in article 3. eco calls on the legislator to create a clear, comprehensive and applicable set of criteria for determining a significant incident, with the focus of such an incident impacting important functions of state or society along the provisions set up by the NIS2 directive.

Incident reporting requirements including the timelines and reportable metrics should be aligned and harmonized with global requirements, including with multistakeholder model regulatory policies and requirements, particularly given the global nature of cyber threats and their impact.

- **On Article 4 Recurring incidents**

The problem sketched out in the commenting of Article 3 also extends to the definition of recurring incidents according to Article 4. The two criteria listed, are too general and too broad to adequately assess, whether there is a serious cybersecurity incident. In fact, the criteria set up may even trigger a recurring incident although there is no such incident, i.e. an incorrect password entry, which may be labelled as denied access. Criteria should be acceptable and not create an overburden of reporting duties and reports. The case of a recurring incident should be related to the services based on which the relevant entity falls under NIS2, e.g. cloud computing service provisioning. Incidents should only be reported if there is an impact and relevance for the critical service.

- **On Article 5 Serious incidents with regard to DNS service providers**

The criteria defined in Article 5 b is regarded as too strict in the view of the Internet Industry and should also include the possibility to define service-level-agreements (SLA).

Additionally, the aspects set out in Article 5 c are incomprehensible and should be streamlined so that DNS providers will get a clear understanding of the trigger of a serious incident with regard to DNS since the Article 5 c addresses Domain-Names not their resolution.

- **On Article 7: Significant incidents with regard to cloud computing service providers**

The current wording of Article 7 of the Implementing Regulation creates uncertainty among cloud services providers as it does not take into account SLAs and scheduled downtimes. This may lead to respective aspects triggering significant incidents. This should be critically reviewed in the wording of Article 7 in order to

avoid overreporting. It should also be noted that Article 7 d refers to different aspects "related to the provision of cloud computing services" which is in the view of the Internet Industry too broad and inconclusive. The aspect of cloud computing service users, which may be affected, is also not always easy to determine and should be removed from the criteria. In addition to this, the term user regularly leads to confusion as to whether they are corporate customers (B2B) or end users. Even in direct business, there can be ambiguities among end users regarding potential users and current users. Different threshold values should apply to corporate customers than to end users. In B2B business, the number of end users is usually unknown.

Finally, the threshold for reporting based on service unavailability for more than 10 minutes is too short.

- **On Article 8 Significant incidents with regard to data centre service providers**

The criterion arising from Article 8 e should be critically revised. Compromising physical access alone should not lead to assuming a significant incident. It should rather also be clarified that this compromised access led to actual damage.

The assumption of a significant incident in the case of a data centre service not being available for one hour is also problematic, since it does not reflect on certain aspects of scheduled unavailability or downtimes. This will produce reporting for significant incidents which do not qualify for a cybersecurity incident in the eyes of the Internet Industry.

- **On Article 9 Significant incidents with regard to content delivery network providers**

The depiction of the availability of online content delivered through content delivery networks (CDNs) raises questions on the general understanding the Commission sets up towards CDNs. Article 9 a leaves it unclear, whether the provision addresses the CDN as a whole, a data center contributing to a CDN or other aspects of a CDN. It should also be taken into account that it is very difficult for CDN providers to actually determine the number of end-users that are relying on their network to function. This criterion cannot be regarded as helpful.

Furthermore, the criterion referring to several factors being "related to the provision" of a CDN is too broad to actually draw proper conclusions for reporting.

- **On Article 10 Significant incidents with regard to managed service providers and managed security service providers**

Corresponding with criticisms raised above, it is very difficult to actually determine the exact number of users of specific managed security services in the Union, since

this would create questions on data protection. eco advocates for removing this provision.

Additionally, the set timeframe of 10 minutes for assuming a significant incident is regarded as too narrow and a longer duration should be assumed.

- **On Article 14 Significant incidents with regard to trust service providers**

Article 14 introduces the term “customers”, alongside the aforementioned and problematic term of “users”. From the view of the Internet Industry, it would be favourable to clarify the definitions of customers and users and reflect on these terms. The requirement in Article 14 d foresees access to network information systems. eco would like to call this broad approach into question and require the criterion be limited to network information systems of a trust service provider.

- **On Article 16 Entry into force and application**

The timeframe set for the Implementing Regulation to enter into force is regarded as too short and does not reflect aspects of national implementation, especially regarding registration processes for essential and important entities.

Even more so the timeframe to achieve and display compliance is independent from national provisions, which may or may not be in place. The timeframe regarded as too short and unrealistic.

Therefore, a grace period should be introduced to establish relevant processes based on the final thresholds. Dependencies on potential national legislation delays, or the introduction of a unified notification portal need to be taken into account.

- **On the Annex of the Implementing Regulation:**

The annex representing clarifications of rules already listed in the NIS2 Directive is an attempt to strengthen cyber security in the specific digital services areas subject to this implementing act. It is further set out to specify policies and security measures. However, it contains problematic aspects from the view of the Internet industry.

The current definition of the requirements leads to massive efforts for NIS2 affected entities to map these requirements to their existing (standard-based) compliance schemes. These Requirements are too detailed and too prescriptive when it comes to Information Security Management Systems (ISMS). Currently, there is no reference or mapping to internationally recognized industry standards, such as ISO 27001, C5, SOC2 or EUCS. At a minimum, a mapping to ISO 27001: 2022 would be regarded as essential by the Internet Industry.

In addition, the documentation effort that will result from many of the required minimal security standard requirements laid out in the Annex’s thirteen chapters will be even more taxing than the fulfilment of the original NIS2 directive’s article

21 (2) points a-j. As an aside, eco notes that the Annex lacks the courtesy of respecting the same order of technical, operational and organisational measures set down in article 21 (2) points a-j, making it more challenging to follow by comparison.

Especially for those companies categorised as “essential entities” regardless of their size, i.e. recursive resolvers and authoritative DNS services, TLD registries and trust service providers, it will be particularly difficult or even impossible to meet some of the requirements, let alone all of them. The draft implementing act confirms to us that the rules of the directive are being followed without compromise, not ever taking into account the abilities and resources of operators. The requirements placed on them are no different from those for larger companies, which is in direct contradiction of the directive itself that stipulates economically viable measures. If the implementing act fails to address this issue and allow for an acceptable level of security measures for the numerous small companies currently active in this industry, they will have to stop offering domain registration or DNS resolution services altogether.

Another concern raised by parts of the Internet Industry concerns the question in how far developers and providers of Open Source Software are covered as “outsourced developers” according to the draft Implementing Regulation, which may create adversarial impact on Open Source Software development and deployment.

3. Summary and conclusion

The implementation of this regulation will cause problems, particularly for SME companies who will struggle to meet the requirements. It is regrettable that the Implementing Regulation does not address this aspect in concrete terms, as the NIS2 directive allows and allows for economically appropriate measures to be taken. This means that the concerns of the many small and micro-enterprises are not sufficiently taken into account if the implementation of the safety rules overburdens them, as the requirements placed on these companies are no different from those for larger companies. In our opinion, it would be desirable if consideration were given to the size and performance of operators and if this option were also used. This will ultimately improve IT security if manageable and, above all, practicable.

While comprehensive, the Implementing Regulation for the NIS2 Directive falls flat, when it comes to clarity for the Internet Industry. Many criteria are referring to general or unspecified terms, which make application of the Implementing Regulation both bureaucratic and exhaustive for companies and may bear the risk of overreporting, which does not improve cybersecurity. Key definitions and the use of terms should be reviewed and adapted. The term "customers" in particular is not clearly understood. A clear distinction between "customers" and "users" is necessary and would provide companies with more legal certainty. The idea and reference to non-compliance with an SLA for a certain period of time as a basis for

assuming a significant incident, which is also systematically encountered throughout the Implementing Regulation, is problematic. The thresholds for reporting the unavailability of services are unclear. This lack of clarity creates uncertainties, especially in the context of SLA breaches. SLAs are agreed between contracting parties. These assurances become part of the contract and are remunerated separately in monetary terms and subject to penalties in the event of non-compliance. Furthermore, SLAs are usually calculated on a monthly or annual basis, not on an hourly or minute basis. The lack of clarity creates legal uncertainty not only for companies but also for their customers.

The Internet Industry thus would recommend to critically review all criteria of the Implementing Regulation since some of them i.e. “users” are encountered systematically throughout the legal act. Additionally, eco would like to avoid cross- or double regulation and encourages the Commission to double down on redundancies and unclarities within its cybersecurity regulation scheme.

Another problem is the assessment of security incidents that are linked to specific information on the duration or severity of an outage. Specifying such rigid criteria leaves little room for a reliable assessment and will lead to a flood of irrelevant reports in practice. This is counterproductive. In addition, many of the specifications seem arbitrarily chosen and are hardly comprehensible. There is a need for improvement here in order to achieve reasonable and, above all, practicable and manageable provisions.

Finally, there must be a clear distinction between Trust Services and the scope of application of the eIDAS-regulation and the Implementing Regulation. Otherwise, it is already foreseeable that there will be conflicts with eIDAS and implementation. The question of the applicable jurisdiction must be clarified in this specific context as well as in general in order to provide companies with more legal certainty. Otherwise, this could pose challenges for the implementation of the Implementing Act throughout the EU.

eco advocates for an extension of transposition timelines for Member States to adjust their legislation if necessary and for companies to adjust their policies and practices in a harmonized regulatory environment.