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

eco

Position Paper on the Parliament's decision on the draft Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM (2020) 823 final)

Berlin, 25 November 2021

With the Commission's presentation for the new NIS-2 directive in December 2020, the debate on the future regulation of cybersecurity within the European Union kicked off. eco contributed to both the Inception Impact Assessment preceding the presentation of the new directive and the Commission's draft in February 2021. Almost a year later, the European Parliament concluded its debate in October 2021 and published a report which it will discuss in the upcoming trilogue negotiations.

eco would like to take the opportunity to point out several aspects, which – from the perspective of the Internet industry – need further attention to turn NIS-2 into a regulatory success; increasing the level of cybersecurity throughout the European Union, while avoiding legal uncertainty for companies.

- **Avoiding bureaucracy through NIS-2**

Many provisions of the NIS draft included fixed deadlines for reporting security incidents within a layered system. These include several instances where the reports from infrastructures have to be submitted within fixed timeframes in order to comply with the regulation. The first report following an incident has to be submitted within 24 hours after the incident was noticed (Art. 20). This impractical and inappropriate burdensome bureaucratic system has increased in complexity through the Parliament's decision to add another layer. This requires companies to declare within 72 hours whether any unlawful activities were discovered.

This may be even more complicated when looking into the different national provisions for IT-based cybercrime, which would also require the operator of an infrastructure to determine whether they were the victim of an attack or whether the incident – although problematic – may not have been the result of criminal activity. The issue of rigid and impracticable deadlines has not only increased for central reporting duties but has also been extended to the already problematic establishment of reporting structures for TLD operators.

eco advises that fixed deadlines should be avoided and limited to best effort requirements. This would ensure swift reporting by the operators of affected infrastructures while also allowing for the thorough investigation of any issues and incidents and accurate reporting, which could otherwise be neglected to meet a deadline. The overall objective and main focus for the NIS-2 should be on the identification and elimination of such security incidents instead of establishing an extensive regulatory report system.

Once again, eco also questions the establishment of reporting mechanisms for TLD operators (Art. 23). These rules are very specific and go beyond the requirements for operating a safe Domain Name System. The establishment of the reporting system as intended by the Commission's proposal – and further worsened by the parliamentary committee decision – is not adequate in the light of risks and possible damages arising from cybersecurity incidents related to the DNS or a domain. It is also questionable whether this information is actually helpful in mitigating damage in the case of such an incident. eco considers the establishment of such a reporting mechanism to be a bureaucratic and costly burden, which has to be carried by the domain industry, with a negligible contribution to the improvement of cybersecurity, in the eyes of the Internet industry.

In addition, attention needs to be drawn to the creation of dedicated registrant information through TLD operators. This very opaquely refers to "legitimate access seekers", without further specifying who or what a legitimate access seeker actually is and for what purposes this information can be used. eco views this formulation to be a potential risk to people's privacy and calls upon the trilogue participants to critically review this policy.

Finally, eco reminds the trilogue parties that NIS-2 should aim to be a well-targeted and transparent regulation and should avoid creating uncertainty by establishing new oversight boards. The NIS-1 directive set a clear institutional framework, which has so far proven to be successful. Further complexity should be avoided so as not to make the regulation more complicated for operators of critical and important infrastructures. In this light, the provisions set out by both Parliament and Commission regarding Article 6 should be reviewed in the light of reporting structures and access to information.

- **Assessing competencies for state actors in relation to cybersecurity**

Despite further concretization of the competencies of CSIRTs in Article 10 (2)

and of competent national authorities in Article 29, eco recommends further determining their competencies with special regard to the proactive scanning of networks and systems and other intrusive cybersecurity activities to avoid harmful interaction with companies' technical systems and infrastructures. It must be ensured that these activities do not impair and endanger the functionality of digital infrastructures with possibly massive and unforeseeable effects. The entire economy and society are dependent on the functioning of digital infrastructures. eco considers this to be an essential factor for the overall success of the NIS-2 directive.

- **Clarifying the field of application**

Article 2 of the directive differentiates between essential and important entities. These definitions, while by themselves are understandable, still leave room for interpretation on how to differentiate between the two categories when applying the NIS-2 directive obscuring the differentiation between the two. This would call the differentiation between essential and important entities in question and might add to legal uncertainty for important entities. Clear differentiation between the two categories in both definition and regulation – as far as security requirements and the establishment of an ex-post oversight are concerned – is necessary for the establishment of a functional cybersecurity regime. eco acknowledges the efforts of the Parliament to promote more clarity in this field. However, the Internet industry still sees potential for more transparency for all parties involved. eco considers the further need for clarification and specification to be a primary requirement.

- **Conclusion**

The NIS-2 directive, while generally an appropriate and welcome measure to bolster cybersecurity across the European Union, still needs further refinement and discussion in order to be a regulatory success. The field of application needs further clarity so that companies can properly determine whether they are covered by the directive.

In addition, the draft directive needs greater efforts to avoid NIS-2 becoming a bureaucratic and economic burden for companies and the operators of digital infrastructures. NIS-2 should not become too rigid on deadlines which will prove impracticable, and requirements when establishing its reporting scheme. This will help avoid creating a bureaucratic and expensive system that does not improve cybersecurity but only increases the complexity in

application. The Internet industry advocates for a reporting scheme which contributes to the quick elimination of security threats. This should not imply that the reporting system has to be as complex as it is intended in the current drafts discussed.

The competencies for CSIRTs need further clarification and limitation. Special regard should be paid to intrusive cybersecurity activities, which should be avoided to minimize disruption of services through cybersecurity measures.

Finally, when negotiating the NIS-2 directive, intrusive regulation which might create adverse effects on the Domain Name System or the functioning of digital infrastructures should be avoided. eco hopes that these criteria will be met in further negotiations.
