BDI

INNONATION

POSITION | DIGITAL POLICY | CYBERSECURITY

Draft Implementing Regulation for the Application of Directive (EU) 2022/2555

Harmonisation of risk-management measures and the definition of significant incidents

25 July 2024

Executive Summary

Considering the current implementation of the NIS-2 Directive, German industry appreciates the European Commission's intention to harmonise risk-management measures and the definition of when an incident is deemed significant. Especially for companies operating across EU Member States, common measures and definitions are essential to reduce the implementation costs associated with the NIS 2. While German industry appreciates the possibility to contribute to the European Commission's consultation, we strongly encourage the European Commission to improve stakeholder involvement already at earlier stages of the development of such regulations.

German industry's policy recommendations

German industry would appreciate if the European Commission were to alter the following points before ratifying the implementing regulation:

Article 3 – significant incidents

Each essential or important entity is different. Hence, defining incident thresholds using strictly quantitative metrics is likely to be overtly prescriptive and will not capture the situation within each entity. We therefore urge the European Commission to reevaluate the currently proposed thresholds.

- **Article 3(1)(a) – financial burden:** Article 3(1)(a) determines that incidents with regard to relevant entities that have caused or are capable of causing losses over EUR 100,000 or 5 per cent (which ever is lower) of the relevant entity's annual turnover are to be considered as significant. An entity shall report these significant incidents without delay and at the latest within 24 hours. In most cases, companies will not be able to calculate the damage caused by an incident within the first 24 hours, as companies will do everything they can to minimise the economic implications of such an incident; and will strive to be operational as quick as possible. Henceforth, the information on financial losses caused by the incident may be more suited for the final report one month after the incident, but not as a triggering point to identify whether the incident is or is not significant. Moreover, while a financial damage of EUR 100,000 might have severe implications for a smaller medium-sized entity, it most likely will not have these repercussions for a large multi-national corporate. Therefore, German industry urges the

Bundesverband der Deutschen Industrie e.V. / Federation of German Industries
EU Transparency Register: 1771817758-48 | German Lobbyregister: R000534
Steven Heckler **|** Digitalisation and Innovation **|** T: +49 30 2028-1523 | s.heckler@bdi.eu | www.bdi.eu

European Commission to stick to the financial damage threshold of EUR 1,000,000 currently applicable under NIS 1. This would ensure that especially larger companies do not have to report incidents, which have a comparatively manageable economic impact on the entity. This would also reduce the bureaucratic burden associated with implementing the NIS-2-Directive without reducing the overall cybersecurity level.

- **Article 3(1)(b) – reputational damage:** According to Article 3(1)(b), incidents are considered to be significant if they have caused or are capable of causing considerable reputational damage. However, this is highly subjective and cannot be measured objectively. Therefore, we urge the European Commission to delete this criterion.

- **Article 3(1)(f) – Deleting the criterion "a successful, suspectedly malicious and unauthorized access to network and information systems occurred" in Article 3(1)(f):** German industry notes that the criterion in Article 3(1)(f) does not focus on the impact of an incident like the other criteria in this implementing regulation but rather describes what happens when the incident occurs. We urge the European Commission to solely focus on the end impacts. Therefore, Article 3(1)(f) should be deleted.

- **Article 3(2)(a) and (b) – reputational damage:** To determine a considerable reputational damage caused by an incident, the draft requires relevant entities to take into account whether "the incident has been reported in the media" and "has resulted in complaints from different users or critical business relationships" according to Article 3(2)(a) and 3(2)(b). With regards to media reports, one has to distinguish between (1) the reach of a media outlet and (2) whether the media report is due to a pro-active communication by a company or the result of a research by a media. Especially smaller media outlets, such as certain blogs with a very negligible reach, should not be considered with regard to Article 3(2)(a). Moreover, if a company is actively informing stake- and shareholders about a cyber-incident this can even be beneficial for its reputation or will at least not have negative repercussions. Moreover, the wording "different users or critical business relationships" is unclear as it lacks a clear quantification. We urge the European Commission to specify how many actors must complain to trigger this criterion.

- **Article 3(2)(c) – regulatory requirements:** Article 3(2)(c) should contain a time-specification, such as "exceeding 72 hours", which would be the time to report in more detail on the incident. Since any incident may cause a temporary inability to meet obligations or result in the temporary loss of access to certain documents.

- **Article 3(2)(d) – losing customers:** The criterion of likely losing customers with a material impact on the business in Article 3(2)(d) will be very difficult for the company to evaluate – especially within the first 24 to 72 hours after an incident.

Clear definitions

The implementing regulation contains a significant number of undefined and / or ambiguous legal terms, such as "considerable", "media" or "material". We urge the European Commission to define these terms in order to ensure uniform, harmonised and clearer reporting obligations for entities falling within the scope of the implementing regulation. Otherwise, the intended EU-wide harmonisation of incident reporting will not be successful as competent authorities across Member States will implement the requirements in diverging ways.

- **Defining "user" and "customer" in the regulation's text:** The implementing regulation introduces the concept of the "user" and the "customer". However, the "user" is not defined in

the NIS 2 Directive, and within the implementing regulation only in recital nine. Since the term "user" could refer to both end-users as well as enterprise customers, we urge the European Commission to integrate the definition of “user” in the implementing regulation’s legal text and provide for a concise differentiation from “customers”.

- **Clarifying the term “suspectedly malicious access / action”:** The implementing regulating recurringly refers to the term “suspectedly malicious action” without ever defining its concrete meaning. We urge the European Commission to clarifying this term.

Article 4 – Recurring incidents

Incidents not deemed significant individually will be considered collectively as one significant incident if they occur at least twice within six months and share the same apparent root cause. This shall ensure that repeated issues with a common origin are treated as a major concern. However, these two criteria are too broad. Due to the very broad nature of incidents that have to be reported under NIS 2 – including those due to human error – we urge the European Commission to introduce a materiality qualifier based on the impact and relevance to the critical service to minimize the notification requirements for incidents that would otherwise create an administrative burden for NIS2 cybersecurity regulators. One possible solution to the problem could be to clarify that the recurring incidents are significant only if, collectively, they meet the threshold for significant incidents as described above.

Article 7 – Significant incidents with regard to cloud computing service providers

German industry considers the general specifications qualifying an incident as significant as too detailed. This assessment also applies to the specific provisions for cloud computing service providers. In addition, the indicated thresholds are too low and seem to be arbitrary. In the spirit of a risk-based approach, the scope of reportable incidents should, therefore, be restricted to core, high-volume and high impact services. Furthermore, only major cloud services and primary product groups should be considered, excluding microservices and sub-products. Larger cloud providers typically offer thousands of microservices and sub-products, which individually do not impact critical services.

The threshold for reporting based on service unavailability for more than 10 minutes according to Article 7(a) significantly deviates from the criteria for Data Centre Service Providers in Article 8(b), which is set to one hour. Depending on the cloud service, and hence, the number of users affected, 10 minutes might be negligible or very long. For example, certain kinds of business software are in most of the cases used during certain hours of working days. If those are not available for 10 minutes on a weekend or at nighttime, this cannot be considered a significant incident. Moreover, the service level agreement (SLA) between a cloud service provider and a user regularly specifies the acceptable unavailability of a service, which is also calculated into the costs of the respective service. Furthermore, some SLAs are not calculated on hours or minutes and instead on a monthly or yearly basis. This should be taken into consideration as well. Moreover, Article 7(a) should reference service level agreements.

While we appreciate the reference to “customer service level agreement” in Article 7(b), the given one hour delay is not justified. There seems to be a general lack of coordination between Article 7(a) and Article 7(b) – while the former does not mention customer SLA and focuses on the complete unavailability, the latter mentions SLAs. However, SLAs are exactly related to these unavailability issues and should be considered as a reliable measurement of working service.

Furthermore, a clarification whether the term “cloud computing service users” in Article 7(b) refers to end-users or business customers is paramount. The criteria should be adjusted to reflect B2B/B2C practicalities. This can provide more clarity and avoid ambiguity in the context of SLA breaches.

Article 10 – Significant incidents with regard to managed service providers and managed security service providers

The current definitions of managed service providers and managed security service providers are very broad, and would most likely result in a very high number of incidents that have to be reported even if their implications for customers of managed services are negligible. Therefore, we urge the European Commission to raise the thresholds. Moreover, a more practical approach would be to reference Service Level Agreements, which specify availability commitments, and only consider a security incident significant if these commitments are breached. There is a similar range for managed security service providers as described for cloud computing service providers with regard to Article 7, therefore, Article 10(a) should also reference service level agreements.

Article 16 – Entry into force and application

The timeframe for the entry into force of the implementing regulation following the national implementation of the NIS-2-Directive and the subsequent registration by entities requires clarification and is unrealistically short. A grace period should be introduced to allow for the establishment of relevant processes within entities based on final thresholds. Additionally, dependencies on potential delays in national legislation or the introduction of a unified notification portal must be considered.

Annex

The annex imposes stringent security requirements on affected entities, closely mirroring established standards. Nonetheless, it lacks explicit references of these standards and is overly detailed and prescriptive. This methodology results in significant burdens for companies striving to reconcile these requirements with industry norms. Furthermore, Article 21 (1) of the directive requires that the technical and methodological requirements for cybersecurity risk-management measures consider the state-of-the-art and, where applicable, relevant European and international standards. This aligns with the principles of the New Legislative Framework (NLF), which the EU uses to ensure products meet high safety and performance standards while allowing for flexibility and innovation. Therefore, the detailed requirements prescribed in the Annex of the Implementing Regulation should be removed, as the NIS 2 Directive already adopts principles of the NLF approach, setting out essential requirements in EU legislation that are detailed through the adoption of standards. Consequently, German industry urges the European Commission to reference international norms and standards, such as ISO 27001, ETSI EN 319 401, C5 or SOC2, rather than detailing technical specifications within the Annex itself. This would reduce the implementation costs without reducing the cyber-resilience level attained by the implementation of the NIS-2-Directive.

Imprint

Bundesverband der Deutschen Industrie e.V. (BDI) / Federation of German Industries
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU Transparency Register: 1771817758-48

German Lobbyregister: R000534

Editor
Steven Heckler
Deputy Head of Department Digitalisation and Innovation
T: +49 30 2028-1523
s.heckler@bdi.eu

Document number: D1966