European Commission

Kapteynstraat 1, SBIC - Building suite 220 / 2201 BB Noordwijk

info@cyberveilignederland.nl
www.cyberveilignederland.nl

KvK 71802525

Noordwijk, 23 July 2024
Ref.: LH/904-0723

Cyberveilig Nederland (hereinafter CVNL), the association of the cybersecurity industry in the Netherlands, welcomes the opportunity to provide feedback on the consultation launched on June 27th, 2024 on the European Commission's draft NIS2 Implementing Act concerning "Cybersecurity risk management & reporting obligations for digital infrastructure, providers and ICT service managers". We are generally positive about the draft but we have some points that require clarification need.

General remarks

- Comment on deadline.
  The draft implementing act covers two substantial pillars of the NIS2 framework: risk management measures and the reporting thresholds. Therefore, stakeholders need more time to prepare appropriate feedback. We recommend extending the feedback period by additional four weeks.

- Postpone the implementation NIS2
  We ask for the postpone of the NIS2 with one year. Entities in scope of the implementing act should be given appropriate time to analyze the final text, review their internal procedures and prepare compliance. It can be estimated that entities will have maximum one month (optimistic scenario) to prepare compliance before the act starts applying – which is clearly insufficient to implement such an ambitious framework. If that's not possible we recommend to include **one year** to allow companies review and prepare their network systems, supply chains and operational procedures before the new rules become binding.

- Importance of encryption
  In the NIS2 and Implementing act is described: "the need of ensuring adequate and

effective use of cryptography to protect the confidentiality, authenticity and integrity of information in line with the relevant entities' information classification and the results of the risk assessment". At this moment the European Commission is taking various initiatives to undermine the importance of the protection of the confidentiality, authenticity and integrity of information by proposing initiatives such as client-side-scanning. In our opinion these initiatives interfere with the measures that entities must take to comply with NIS2

- Leverage existing standards in duty of case obligations
  The regulations in the draft are, not surprisingly, very similar to international adopted standards such as ISO 27001, ISO 20243, SDDF, NIST, etc. These provide meaningful guidance and a strong foundation for effective cybersecurity policies and practices. In our opinion, covered entities within the NIS2 should be able to meet their duty of care obligations by leveraging these commonly accepted global standards for cybersecurity, secure product development, and supply chain integrity. Rather than develop new certification requirements, the NIS2 should leverage existing standards and conformance schemes to facilitate increased transparency and accountability regarding cybersecurity practices. Focusing resources on the consistent application of existing and common standards will result in better cybersecurity overall. Furthermore, CVNL suggest a tabular overview and a comparison that clarifies with EU requirements are already met by an international adopted standard and what the gaps are. This would save redundant work and, for those entities that are already been certified, would reduce the pressure of entities to provide the correct evidence to comply with the NIS2.

- Audits by the regulator
  The regulator has the right to conduct audits of the service provider to determine whether the necessary provisions of the NIS 2 are met.
  1. Service providers will have one or more privately conducted audits per year as part of required certifications and assurance statements. Consider ISO 27001 and SOC 2. It should be sufficient to deploy those certifications and assurance statements so that the regulator does not need to conduct an audit. After all, NIS 2 implementing regulation and ISO 27001 contain a lot of similarities and there would be double auditing. This is an unnecessary burden that will in turn be at the expense of the service provider's IT performance. An undesirable effect.
  2. If the service provider does not have the right certifications, then the regulator will have to take into account the costs the service provider will incur during the audit. After all, the audit will require commitment and effort from service provider employees. This is time that cannot be spent on customers and thus revenue. This loss, or at least the cost, will have to be somewhere. The most obvious is to have the costs borne by the regulator. After

all, the regulator determines that an audit is necessary, the service provider cannot oppose it.

- Customers without adequate services
  The digital sector runs on the delivery of services between companies (B2B). Those services require effort such as training staff, deploying the right tools and implementing a competent service process. The company recovers the costs of setting up and maintaining those services from the customer. The customer must then be included in the service (e.g. implementing required tooling) to enable the performance of the service. For cost reasons, it sometimes happens that customers take only part of the required services, or even no services at all.
  It should then be clear somewhere in the NIS2 that the service provider then only has an ad hoc role in supervising a cyber security incident, with the costs for that handling lying entirely with the customer.

- Reporting to the regulator
  If a cyber security incident occurs that meets the criteria to be reported as a NIS2 cyber security incident to the regulator, the service provider will have to incur costs to create that report, provide expert content and supervise it. So this is the effort towards the regulator, not the mitigation of the incident and coordination with the customer. The costs incurred by the service provider to set up, supervise and complete that reporting to the regulator will have to be recovered from somewhere. It is not clear in the NIS2 implementing regulation how those costs will be reimbursed. It would be good to describe that, with the most obvious party to bear the costs being the regulator.
  Note that if the costs have to be borne by the service provider itself, this puts pressure on the quality of handling. This may lead to a sub-optimal approach and handling of cyber security incidents because time and quality staff deployment obviously will be cut.

- Cascading reports
  An incident may lead to a cascade of reports. An example: At a telecom provider, a main connection fails. The telecom provider will have to report an NIS 2 incident. Because the connections of customers of a service provider using that failed connection also fail, the service provider will have to create an NIS2 incident, as well as all those affected customers as well. One outage can then lead to a veritable cascade of notifications. Not only will the regulator not be able to process them, the actual usefulness and necessity of incident reporting will come under pressure.
  Bear in mind that costs will have to be incurred several times without actually benefiting cyber security. This is not efficient.

A good idea would be to start working with a major incident process, in which a report that is broad and affects the chain is reported only once. This allows attention to be given to that incident and much more focused work on cyber security.
This would require the various regulators to work together and a single incident portal for all sectors.

- NIS2 and DORA
  The DORA is lex specialis, meaning law that takes precedence over other laws, such as NIS 2. However, DORA and NIS2 are very similar and also have a structure with supervisor, duty to report and duty of care. Both DORA and NIS 2 are slightly different in content but with the same goal: improving cyber security.
  Although the full content of the DORA implementation regulation is not yet known and therefore no conclusive document study can be completed, it is certainly already possible to say that there is a challenge. Companies such as a service provider will have to comply with DORA and with NIS2. Since DORA comes before NIS2, it will be a matter of finding gaps in DORA that are filled by NIS2. In practice, this will lead to interpretation differences. A lawyer's paradise. And this is precisely why the quality of a solid cybersecurity framework will be compromised.
  One incident can then lead to a notification to the regulator for DORA, the regulators for NIS2 and from the chain to a veritable cascade of notifications from numerous entities to the various regulators.
  The European Council would do well to form a position on the lex specialis status of DORA. Perhaps the implementing regulation of NIS2, as it currently applies to the digital sector, could be used for companies covered by DORA and DORA abolished. If that cannot be done, then still achieve something of cooperation between NIS2 and DORA, strengthen each other. Get clarity on how the two relate to each other, what the overarching framework for action is. Because in practice, doubt is a prime breeding ground for cyber incidents to occur.

- GDPR
  A subset of cyber incidents are incidents where personal identifiable information (PII) is shared unlawfully. Examples include data leaks. The GDPR, which in the Netherlands has been transposed into local legislation, the AVG, requires that, depending on a set of impact criteria, a notification should be made to the regulator. How does this relate to the NIS2 implementing regulation? Does that obligation to notify then lapse? Or do both apply? In the latter case, doesn't it make sense for the regulator for the GDPR to cooperate with the regulators for NIS2? This could be done by, for example, having one reporting point that would then take care of its own distribution to the appropriate underlying regulators.

- NIS2 sectors
  The NIS2 implementing regulation only applies to the digital sector. For the other sectors, the NIS2 directive and thus the transposition of that directive to local legislation applies. There are considerable substantive differences between the NIS 2 implementing regulation articles and the converted NIS 2 to local law articles. How to deal with implementation if an entity belongs to two or more sectors, one of which is the digital sector? Then two legislations are active that contradict each other on a number of points.

- NIS2 criteria
  The NIS2 directive lists criteria that determine whether or not an entity is directly subject to the NIS2 directive. The NIS 2 implementing regulation lacks that criteria list. Does this mean that all entities in the digital sector fall under the NIS2 implementing regulation, even the small once (less than 50 employees)? Or do the criteria as mentioned in the NIS2 directive apply?

Risk management measures

- Management bodies.
  The draft IA text refers to the tasks and responsibilities of the management bodies. However, some of the obligations do not seem fit for the management bodies (e.g., obligations to update policy or roles and responsibilities or approve risk assessment results in Sections 1.1.2, 1.2.6, 2.1.1 of the Annex). Given the specificity and regularity with which these tasks should be performed, we recommend that they are assigned to teams responsible for the management of granular, day-to-day cybersecurity operations instead.

- Detailed information about components.
  Section 6.1.2.(c) of the Annex implies that ICT suppliers should share information describing the hardware and software components with their customers in critical sectors. This requirement does not contribute to higher security and, on the contrary, creates risks due to dissemination of sensitive information to various third parties. Under the CRA, software and hardware manufacturers should maintain SBOMS and make them available to market surveillance authority upon request – we recommend aligning with this approach and avoid contradicting requirements within NIS2.

- Security in acquisition of ICT services or ICT products.
  (Section 6.1.1 and 6.1.2(a) & (b)) appears to require software manufacturers to provide free software updates, patches and other software support services. The legislation should recognize and distinguish how support is provided in B2C vs B2B software transactions. NIS2 covered entities should be responsible for securing their software.

B2B customers can choose to secure their software by purchasing support services from the ICT software product manufacturer, or they can provide the security support themselves or via other service providers. The Commission should not disrupt the B2B software transactions model by forcing NIS2 covered entities to only use software with security support services from the ICT software product manufacturer. Conversely, ICT software product manufacturers should not be required to provide free security support services to B2B customers.

Reporting requirements

- Reporting criteria
  We recommend that Article 3 of the draft IA refers to "two or more" instead of "one or more" criteria for the selection of an incident as significant. The criteria presented in Article 3 are too numerous, broad and difficult to assess – therefore, selection based on just one would lower the threshold too much.

- Financial loss threshold
  The threshold based on financial loss is too low. Within 24 hours, it is nearly impossible to assess the level of financial loss that an incident may potentially cause. Any incident may potentially meet the threshold of 100 000 of potential financial loss – which will result in overreporting. Due to the variety of companies in scope of NIS2, it will not be easy or even possible to determine the financial loss at the moment an incident occurs. Even if the incident is limited to a small defined scope, direct and indirect damage will still have to be taken into account, making it impossible to determine a hard figure (€ 100,000 or 5% annual turnover). This makes this provision impracticable and unnecessarily obstructive. This criterion can be removed from the regulation and there is no good comparable other criterion.

- Reputational damage
  The criteria proposed in Art 3 are not relevant in the security context and should be removed. Reputational damaged caused by an incident may be relevant under DORA due to specificities of the financial and banking sector. However, even in this context, reputational damage is not a strong threshold to be considered when assessing incident significance as it does not impact the security of the service. CVNL believes that sharing of information is very important to increase the (digital) resilience of Europe. We also believe that victims of, for example, cybercrime are not to be portrayed in the media as the criminals but as victims. To this end, we encourage victims to share their experiences as a victim of cybercrime as much as possible, including in the media. We are afraid that by naming the media as the threshold value of a significant incident, these developments

concerning information sharing in relation with a cybercrime event will have a negative connotation and we therefore ask the EC to reconsider this.

- The number of users impacted.
  Not always will it be possible to determine the number of affected users as intended here. Be aware that customers of service providers often have to offer their management domains in lots. One service provider manages the server parcel, another manages the applications and yet another manages the endpoints and possibly the identities. Depending on which lot is managed by the service provider gives access to the data regarding the number of users.
  In our opinion, clause 3.4 is not conclusive and would be much better replaced by 5% of the number of customers of the service provider. After all, that number can always be determined. With this change, the effect of the impact determination is much more striking and the purpose of incident impact determination is better achieved.

- Recurring incidents
  We recommend raising the threshold proposed in Article 4 to avoid overreporting of incidents, especially when they do not result from a malicious activity. We recommend a threshold of 10 incidents within 6 months.

- Unavailability of service
  The unavailability timeline proposed in several sectors covered by the draft IA is too short. The threshold of 10 minutes is very low and will inevitably draw entities' resources into assessing whether disruptions meet the reporting criteria under the NIS2. It is important to keep balanced thresholds to ensure that dedicated operational and legal teams are triggered only in specific cases where there is reasonable evidence indicating at a potentially significant incident. We recommend extending the reference timeline to 60 minutes.

- Malicious action
  The draft IA suggest a threshold based on a suspectedly malicious action. We recommend removing the word "suspectedly" as it makes the threshold too vague as any incident may be suspected to occur as a result of a malicious action. We recommend that incidents are reported once an entity establishes evidence of malicious activity.

Comments on the "Draft Implementation Regulation"

- Rule 15 page 3
  (15) "The relevant entities should manage the risks stemming from the acquisition of ICT products or ICT services from suppliers or service providers and should obtain assurance

that the ICT products or ICT services achieve certain cybersecurity protection levels, for example by European cybersecurity certificates and EU statements of conformity for ICT products or ICT services issued under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881 of the European Parliament and of the Council."
In order to accomplish a more uniform approach it is recommended to add the next sentence to this rule:
"For ICT Services from suppliers or service providers relevant certification and assurance are accepted means to prove the required cybersecurity protection level, in particular ISO/IEC 27001 combined with SOC 2 type 2 assurance."

- Rule 33 page 6
  The EC introduces the phrase 'Completely unavailability of a service'.
  This term ads confusion. The word 'completely' should be removed.

- Article 10
  "(c) the availability of one or more of the managed or managed security services of a that has no customer service level agreement in place is impacted by the incident;"
  If there is no customer service level agreement in place there is no obligation for the managed or managed security services provider to deliver effort. Most probably there will be no monitoring system implemented and no administration tooling in place to detect and mitigate an incident. Therefor this article cannot be effective and should be withdrawn from the final implementing regulation.

Comments on the "Annex"

- Annex 6.6. Security patch management
  "6.6.1. The relevant entities shall specify and apply procedures for ensuring that:
  (a) security patches are applied within a reasonable time after they become available;
  (b) security patches are tested before being applied in production systems;
  (c) security patches come from trusted sources and are checked for integrity;
  (d) additional measures are implemented and residual risks are accepted in cases where a patch is not available or not applied pursuant to point 6.6.2.
  6.6.2. By way of derogation from point 1(a), the relevant entities may choose not to apply security patches when the disadvantages of applying the security patches outweigh the cybersecurity benefits. The relevant entities shall duly document and substantiate the reasons for any such decision."
  Since accepting exceptions means accepting risks the normal rules for risk re-assessment should apply to this article. Therefor this addition to 6.6.2:

"The relevant entities shall review and, where appropriate, update these exceptions at planned intervals and when significant incidents or significant changes to operations or risks occur."

- Annex article 6.9.1
  This article talks about unauthorized software. What exactly is meant by this? How can it be demonstrated that certain software is authorized? Should a list be drawn up of all authorized software? Securing against unauthorized software means that it should not be technically possible to install software from unknown sources. Mo unauthorized software installations should be possible on systems that are on the network and connected to the information system. If that is so then no software updates can be performed either. This makes the system increasingly insecure over time, increasing the likelihood of a cyber incident occurring. There is a need for clarity on the concept of unauthorized.

- Annex 6.7.2.h :
  "(h) allow connections of service providers only after an authorisation request and for a set time period, such as the duration of a maintenance operation;"
  Asking authorization would delay pro-active interventions when needed, where the time to react and mitigate is crucial.
  Therefore this addition:
  ", unless pro-active actions are needed, stated in a Service Level Agreement and by the use of a secure trusted connection."

- Typo Annex 6.9.2.
  "For that purpose, the relevant entities shall in particular ensure that their network and information systems are equipped with malware detection and repair software, which is updated regularly in accordance with the **with the** risk assessment and the contractual agreements with the providers."

- Annex 10.2.1.
  "The relevant entities shall perform background checks for their employees, direct suppliers and service providers, if required for their role, responsibilities and authorizations.
  It is an infringement to GDPR if personal identification information (PII) of personnel of the supplier or service provider is disclosed or used outside the organization. Therefor this addition:

> “If the direct supplier of service provider has relevant certification, in which the auditing of the background check procedure is included, that audit report will suffice to comply with this article.”

Best regards,

Liesbeth Holterman
Strategic advisor CVNL

About Cyberveilig Nederland

Cyberveilig Nederland is the interest group of the cybersecurity sector in the Netherlands. In this capacity, we are committed to creating more transparency and quality in the market. For example, we are involved in various quality mark developments, we are the initiator of the Cybersecurity Dictionary and we create buyers guides to help customers of cybersecurity service providers choose the right services. We also represent the interests of the cybersecurity sector towards stakeholders such as government, science and politics. Our mission is to increase the digital resilience of the Netherlands. One of the requirements to achieve this is the active sharing of information. At CVNL we encourage this by working together with relevant government parties and other stakeholders. In this capacity, we were designated by the Ministry of Justice and Security in 2020 as a linking organization under the Network Information Systems Security Act (Wbni). In addition, we play an active role in the creation and further development of the 'nationwide system of information nodes', we have been involved in the Anti Abuse Network (AAN) from the start, we are an active participant in the Cyclotron Program and we are co-initiators of project Melissa, where we combat (the consequences of) ransomware.