Response to Netherlands NIS2 public consultation

1. General

Cisco is supportive of the overall goals, structure and scope of EU NIS 2. This includes the focus on critical infrastructure sectors and the risk-based approach to security measures and incident reporting, aligned with internationally-recognised standards and frameworks.

We support the broadening of sectors considered important or essential, reflecting developments in our understanding of critical infrastructure. This includes both local public administration and education institutions.

2. Timeline - phased approach

The draft law currently does not contain a specific phase-in for the requirements to take effect once the law is passed. In principle, the draft law suggests the requirements including those related to security measures could take effect immediately. Other EU member countries are phasing the requirements deadlines (e.g., 60 days to register, 1 year to meet security requirements, etc.). It is important that there is a multi-step approach for companies to meet their incident reporting and security measure obligations.

An example of this is the Belgian law transposing the NIS 2 Directive, which effectively gives covered entities 30 months from 18 October 2024 (i.e. until 18 April 2027) to implement the security measures and does so in stages.

Proposal The Dutch NIS2 legislation should adopt a muti-step compliance approach to roll-out security measures and incident reporting, following the Belgium example on how to implement this in practice.

3. Likely/may for incident reporting to customers

Article 23(1) of EU NIS 2 requires service providers to report significant incidents to customers: "*Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are **likely to** adversely affect the provision of those services*." The Dutch implementation law contains very similar language, but unfortunately the word "likely" is not included in the draft corresponding Dutch text, which says, "*Where appropriate, the essential entity or important entity shall without undue delay notify recipients of its services of significant incidents that **may** adversely affect the provision of those services".*

The use of "may" broadens the scope of reportable incidents and adds uncertainty in how to make such a determination. Cisco would propose to use the word "**likely to**" since this is the original intent of the NIS2 article.

Finally, we note that the current draft legislation does not yet set detailed incident reporting thresholds, which we understand will be detailed in further implementing legislation. We urge that the trigger for mandatory reporting obligations be tied to actual or likely impact of incidents to users or infrastructure based within the Netherlands, or in the alternative, within the EU. For example, an incident that impacts a globally-offered public electronic communications service, but is likely to impact only U.S.-based users of that service and U.S. based infrastructure used to provide that service, should not trigger reporting obligations to Dutch regulators. To require otherwise would be to put costly reporting burden on providers of such services with no clear nexus or commensurate benefit to EU cybersecurity.

Proposal

Cisco would propose to use the word "***likely to***" instead of "***may***" in Article 23(1) of EU NIS 2 referring to the requirements for service providers to report significant incidents to customers. We would also propose clarifying in implementing legislation or guidance that incidents must have an actual or likely impact to users or infrastructure based within the Netherlands (or in the alternative, within the EU) to trigger mandatory reporting obligations.

4. Incident reporting to customers

For incident reporting to customers we suggest that companies can satisfy the requirement to notify customers of general service outages meeting NIS 2 reporting thresholds by posting a summary of the outage on its website. Indeed, it is common practice for technology companies to post notifications of outages on websites dedicated to this purpose. Of course, companies will still need to send regulators a notice in writing if they meet the reporting thresholds, this is only about the requirement to notify customers. It is often very burdensome to identify and send written communications to all impacted customers in the midst of an incident, instead of posting news of the outage and related guidance on a website.

The article in scope: NIS 2 Article 23(1): "*EU member states are putting this requirement into their law as required under this sentence in Article 23(1):* "*Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services*."

Belgium has already done this in its NIS 2 guidance on how companies like Cisco should report service outages to customers. Page 8 states that posting on a website is sufficient to notify customers:

1. *"Where the significant incident is likely to affect the provision of the services listed in the annexes to the law, the entity must also inform, without undue delay, the recipients of its services (insofar as they are identifiable). This information obligation may be fulfilled by any available means (**information on the website**, mailing list, message in an application, paper communications, etc)."*

Proposal

For incident reporting to customers we suggest that companies can satisfy the requirement to notify customers of general service outages meeting NIS 2 reporting thresholds by posting a summary of the outage on status outage pages. This is line with the Belgium example on how to implement this in practice.

5. Public electronic communication networks security by design

In the explanatory memorandum, accompanying the draft law, this section can be found: "*More specifically, providers of public electronic communication networks and of public electronic communication services must provide security (and privacy) by default and by design. They should also inform their service recipients of significant cyber threats and the measures they can take to protect the security of their devices and communications, for example by using specific types of software or encryption technologies.*"

The concept of security by design and default is more closely aligned to the scope of product-related security requirements under the Cyber Resilience Act than the organizational approach to security of NIS2 and related standards for demonstrating compliance. To avoid confusion, we advocate deletion of this language or a clarification that a service that meets NIS 2 security controls is presumed to meet the controls.

Proposal

Clarify the language in the explanatory memorandum so that it is clear that a service that meets NIS 2 security controls is presumed to meet the controls. As another option it could be out of scope here and addressed in the Cyber Resilience Act.

6. Security measures - ENISA guidance and mutual recognition of audits/ auditors

Cisco supports that the proposal is referring to the Implementing Regulation, keeping measures high level and using ISO 27001 as an example. Certification against ISO 27001 should explicitly provide presumption of conformity with the cyber risk management measures identified in Article 21 of the NIS2 law and ideally, such presumption of conformity should equally apply on the electronic communications side too. Alongside the Implementing Regulation we would call on future guidance to covered entities to reference the ENISA Implementation Guidance at the next level down: https://www.enisa.europa.eu/news/asking-for-your-feedback-enisa-technical-guidance-for-the-cybersecurity-measures-of-the-nis2-implementing-act

In terms of demonstrating compliance with the security measures, we understand that further rules may be laid down in relation to use of third-party audits. To the extent this comes to fruition, Cisco supports the idea that we should be able to reuse existing audit results from auditors recognised in other countries and not to artificially restrict it to a list of nationally identified auditors. Requiring companies to obtain multiple similar audits from various EU national auditors for the very same product offered across multiple EU jurisdictions (e.g., the

same public electronic communication service offered via the same data centers in the EU) is a large burden on company resources without providing a commensurate security benefit. It can require companies to divert security resources from actually improving security of their products to performing multiple duplicative third party audits with various nationally identified auditors. It would be preferable to be able to scale existing certifications rather than redo them in the Netherlands on the same service in order to derive the same results. Moreover, it would be good to be able to do that on a per product/service basis rather than enterprise-wide.

Proposal

- Cisco propose to go in the direction of the ENISA Implementation Guidance as the next level down ENISA guidance.
- Priorities to include mutual recognition of audits/ auditors in the implementation.

7. **Designated control officer to monitor compliance with security measures and reporting obligations**

In Article 68 it is stated that the Dutch authority may designate a control officer to monitor the compliance with security measures and reporting obligations.

The relevant language is below:

Article 68

1. *"The competent authority may designate a control officer for a specified period in respect of an essential entity.*
2. *The control officer shall be an independent expert being a natural person and shall have the task of:*
    a. *Monitoring compliance by the essential entity concerned with the provisions of or pursuant to Articles 23 [security measures] and 27 to 32 [reporting obligations]; and*
    b. *Informing the competent authority and the management of the essential entity concerned of compliance by the essential entity concerned with the provisions of or pursuant to Articles 23 and 27 to 32.*
3. *The essential entity shall bear the costs of the control officer, unless a case defined by general administrative measure arises in which the entity concerned does not have to bear these costs*
4. *Further rules may be laid down by or pursuant to general administrative measures regarding the provisions of the first and second paragraphs, including the requirements that apply to the designation of the inspection officer."*

Cisco suggests limiting the circumstances in which a control officer is required. This should be based in NIS2 Article 32.2, so that it is only applicable based on a risk assessment and in case of repeated, significant infringement:

"(b) regular and targeted security audits carried out by an independent body or a competent authority;

(c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of this Directive by the essential entity;

[…]

The targeted security audits referred to in the first subparagraph, point (b), shall be based on risk assessments conducted by the competent authority or the audited entity, or on other risk-related available information."

Proposal
Cisco suggests limiting the circumstances in which a control officer is required. This should be based in NIS2 Article 32.2, so that it is only applicable based on a risk assessment and in case of repeated, significant infringement.