„NIS 2“ – VDMA-Position Paper

Evaluation and recommendations on the legislative proposal for a directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 - COM (2020) 823 final

March 2021
1. Evaluation: right approach, but considerable burden for SMEs

The goal of strengthening security capabilities across the board through an EU regulation is right. NIS 2 takes up the criticism towards the NIS 1 and correctly addresses the need for more European harmonisation and an EU-wide uniform approach. The proposal contains suitable and in part appropriate measures to increase cyber resilience in industrial value chains. The VDMA supports the security objectives of the proposal.

However, by extending the scope to a new category of “important entities”, the proposal will lead to a considerable burden on a large number of companies. Based on figures from Eurostat, more than 9,000 companies in the European mechanical engineering sector alone, of which almost 80% are small businesses, will suddenly be affected by measures that were previously only mandatory for a category of critical and “essential entities”.

### Draft NIS 2.0: Machine manufacturers heavily affected

<table>
<thead>
<tr>
<th>(d) Manufacture of machinery and equipment n.e.c.</th>
<th>Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>EU-27 ≥ 50 employees</td>
<td>9,018 manufacturers</td>
</tr>
<tr>
<td>DE ≥ 50 employees</td>
<td>3,081 manufacturers</td>
</tr>
</tbody>
</table>

The question therefore arises whether the proposal is proportionate and feasible if this breadth and depth of intervention is maintained. The compliance costs will be considerable and many companies at the lower end of the size spectrum (number of employees 50 plus) will hardly be able to comply with the requirements. The lack of specialists alone will pose major problems for many companies and NIS 2 will further increase the competition for Cybersecurity experts.

The lack of differentiation between the measures for “essential” and “important” is particularly critical: The same requirements apply to all companies without differentiation, whether “essential” - such as energy suppliers - or “important” - such as a small mechanical engineering company. It remains unclear which criteria and reasons lead to a classification as “important” or “essential”. It can be assumed that NIS 2 will cover many companies that are neither an indispensable part of essential value chains nor represent a relevant security risk for others.

The proposal seeks to compensate for this lack of differentiation by adopting a risk-based approach ("...appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented", Art 18 (1)). Whether this risk-based approach leads to the necessary case-specific differentiation and relief is questionable, however, for the following reasons:
• The measures listed in Art. 17 and 18 (2) are very extensive and, from the perspective of smaller companies, more than just minimum requirements. They disproportionately restrict the scope for case-specific, risk-oriented measures according to Art. 18 (1)

• Cybersecurity threats are "moving targets" and strongly depend on the capabilities of the attackers and the current state of the threat scenarios. The required analysis of the risk ("...shall ensure a level of security of network and information systems appropriate to the risk presented.") is difficult to perform by many SMEs, among other things because the needed specialists, expertise and tools are not available.

• Coordinating whether measures are appropriate to the risk requires close cooperation with the authorities of the member states. It is hardly conceivable that the authorities can offer this coordination and advisory service for such a high number of companies.

• There is a risk that this situation will lead to a lack of guidance and insufficient legal and compliance certainty.

• The notification and reporting obligations described in Art. 20 are far-reaching and represent considerable bureaucratic effort, which is not dependent on a risk assessment but applies in principle. The ability of companies to comply with these obligations varies greatly. For example, the 24-hour reporting deadline is difficult for small businesses to comply with.

The proposal contains a few ambiguities that would make compliance difficult for the companies concerned. These include, among others, the question which criteria trigger the ex post supervisory measures described in Art 30 and which indications are considered sufficient. It is also unclear which criteria apply to the security scans mentioned in Art 30 (2) (c).

2. Recommendations

The VDMA supports the approach of increasing cyber security via a harmonised European approach and in this way strengthening the Digital Single Market. The envisaged measures on coordination and information exchange are purposeful.

In principle, the envisaged obligations are suitable for increasing the level of cyber security in the EU internal market. However, the resulting compliance burden is considerable, especially for small businesses with fewer than 250 employees. It is not appropriate that "important" and "essential" organisations are subject to the same procedures. For example, a medium-sized company classified as "important" must comply with the same reporting requirements as a nuclear power plant. Changes are necessary in order to reduce the burden on companies, to maintain proportionality and to facilitate applicability in the industry. From the VDMA's point of view, this can be achieved - while maintaining the targeted security level - by changes in the following areas:

• Focusing the scope on critical entities

• Easing the burden for "important facilities" and a clear differentiation from "essential facilities".

• Elimination of ambiguities
2.1 Reducing the burden on SMEs by focusing the scope

In the view of the VDMA, it is not proportionate to classify by NACE codes alone, as the risks to the general public are not reflected in these very rough categories. NACE codes are not suitable risk classes, neither in the sense of cybersecurity, nor in the sense of overall economic resilience.

Mandatory cybersecurity measures with this depth of intervention in business processes and burden must focus on those companies that have overarching significance for the functionality and/or cybersecurity of supply chains. An appropriate balance between risk and effort and a reduction in the burden on companies could be achieved through the following changes:

- Sharpening the definition of "important" by focusing on "manufacturing of critical products": This classification cannot be made on the basis of NACE sectors alone, but the role of the respective facilities in the value chain must be added as a criterion: "Important" in the sense of cybersecurity and resilience is a company (or part of a company) if it is important for an essential company or is part of an essential value chain. This differentiation would lead to substantial relief for companies outside the supply chain for critical infrastructure and public authorities.

- The classification of a company as "important" could, for example, be the result of a supply chain assessment as described in Art 19 or recitals 46/47. This would not jeopardise the long-term goal of a horizontal increase in cyber security: In the medium term, regulation and increased cyber security at the most important interfaces would have a "pull effect" on other institutions.

- In the current version of the proposal, companies with a size of 50 (!) employees or more are in scope, which places a considerable compliance burden on a large number of small companies. According to Eurostat figures from 2018, this is 7118 small enterprises with 50-249 employees in the mechanical engineering sector. It is questionable whether companies of this size can comply with these requirements. The "size cap" for "important" entities should be based on the usual EU SME definition of 250 employees or more. According to Eurostat, this is still 1900 companies. This extension of the exemption rule would hardly decrease the targeted security level, as companies with a critical function can be included in the scope by the member states through the criteria listed in Art. 2 (2), regardless of the number of employees.

- A clearer definition of the protection goal would help companies to focus their efforts on essential business processes: The obligations described should not apply to the whole company, but to the parts and services that are essential for the protection of intellectual property, the maintenance of operations and the value chain.

2.2 Less obligations for "important" facilities

The weakness of the proposal is that - in terms of obligations - it makes no distinction between "important facilities" and "essential facilities". The risk-based approach only partially solves this problem, as already the risk assessment mentioned in Art. 18 and the minimum obligations listed will pose considerable problems for many companies and lead to legal uncertainty.

The VDMA therefore proposes on the one hand to facilitate the measures for "important facilities" and on the other hand to provide for corresponding support measures. These could include:
• As an alternative to complying with the measures required in Art. 18 (2), the submission of a simple, officially acknowledged protection concept for minimum resilience should be assumed as sufficient. The initial preparation should be appropriately financially supported.

• Complementary to NIS, the development of EU-wide harmonised methodologies for adequate risk assessments (in the corresponding country language) must be pursued in order to provide guidance to all companies (including those not covered by NIS 2).

• At the same time, it must be ensured that the increase in security obligations for companies is matched by the timely creation of sufficient capacities on the part of authorities and service providers.

• Registration procedures should be facilitated (for example by registering via CSIRTs instead of ENISA (Art. 25)).

• The notification and reporting obligations for "important entities" should be reduced (for example by removing the reporting obligations in the case of "significant threads" (Art 20); the necessary investigations are hardly feasible for SMEs without sufficient (financial) support, especially after a ransomware attack.

• The reporting deadline should be extended to 72 hours for "important" entities. Reports should be able to suffice for transnational companies to only one coordinating reporting authority.

2.3 Reducing ambiguities and increasing legal certainty

The proposal contains ambiguities that may lead to legal uncertainties and compliance failures for the entities concerned. For example:

• It remains vague which are the triggers for "subsequent supervisory measures" mentioned in Art. 30 (1). In particular, it needs to be clarified what is meant by "indications".

• There is a lack of clarity which criteria should apply to the security scans mentioned in Art. 30 (2) c. There should at least be a restriction to passive scans (port scans).

• The restriction on the exchange of confidential information by public authorities mentioned in Art. 2 (5) should be complemented by a fundamental requirement to treat trade secrets confidentially, including within public authorities and their agents (e.g. auditors).

• The possibility of mandating the use of CSA schemes (Art. 21) creates confusion, as schemes declared as voluntary in the CSA are declared to be mandatory. It is also unclear to what extent the rather product-oriented schemes of the CSA can serve the goals of the NIS2 and can be mapped to open source solutions, among other things. Article 21 should be deleted.

3. Summary:

The "NIS2" proposes the right goals and measures, but leads to considerable effort and resource requirements which will overcharge smaller companies. By focusing the scope of application and easing the obligations for "important" entities, the burden for medium-sized companies can be relieved whilst maintaining the desired high level of security across the European Union.
Kontakte VDMA:

Steffen Zimmermann
VDMA Competence Center Industrial Security
+49 69 6603 1978
E-Mail steffen.zimmermann@vdma.org

Thomas Kraus
VDMA Technical, Environmental Affairs and Sustainability
+49 69 6603 1602
E-Mail thomas.kraus@vdma.org

Kai Peters
VDMA European Office
+322 7068219
E-Mail kai.peters@vdma.org