NIS2

EU Directive on measures for a high common level of cybersecurity across the Union

Summarized points of interest from the perspective of Cyber Security solutions

With Inter Engineering proposals for coverage.

Version	2.0
Last Change	17/6/2024

Disclaimer

Everything contained in this document is for informational purposes only and provided as-is.

Inter Engineering and the people related to Inter Engineering do not accept any responsibility whatsoever for what you do with the information you obtain from this document.

By using this document, you agree that Inter Engineering and the people related to Inter Engineering do not have any responsibility whatsoever for any damage whatsoever caused by the use, misuse or inability to use this document or the information or data it contains.

By using this document, you accept and agree with these terms.

If you do not agree with these terms then you should not use this document.

Contents

1. INTRODUCTION

This document aims to help:

- ICT companies including Cyber Security solution providers who want to assist NIS2 affected organizations to become compliant

and

- Affected organizations themselves

It does this by providing the relevant parts of the official EU paper on NIS2 and translations of those into practical conclusions and measures to take.

Thus, the interested person does not need to go through the official paper.

2. IMPORTANT DATES

16-1-2023	NIS2 came into effect
17-10-2024	EU states must have established laws related to NIS2 enforcement
17-4-2025	EU states shall have published lists with essential and important entities

3. THE CONVINCING OF AN AFFECTED ORGANIZATION

1. Your country will have submitted a list with organizations affected to the EU.
   So, if your organization is affected then that will be publicly known.

2. Authorities will do audits from time to time. If in an audit you don't comply you will be fined.

3. If you fall victim of breach, you need to inform CSIRT within 24 hours. If then becomes clear that you did not take measures, you will be fined. If you do not report then by definition you are infringing the regulation and will be fined.

4. Fines are huge.
   For essential entities: At least 2% of annual turnover, or 10M whichever higher.
   For important entities: At least 1,4% of annual turnover, or 7M whichever higher.

5. Natural persons who represent an essential or important entity may also be held liable.

6. By applying the measures to comply your protection against Cyber threats will dramatically increase. This is a very important benefit for your organization.

4. THE FINES

For essential entities: At least 2% of annual turnover, or 10M whichever higher.

For important entities: At least 1,4% of annual turnover, or 7M whichever higher.

Natural persons who represent an essential or important entity may also be held liable.

5. ORGANIZATIONS AFFECTED

Entities of a type referred to in Annex I or II (included in this document as well as for entities identified as critical entities under Directive (EU) 2022/2557

Essential entities

Large organization listed in Annex I of NIS2.
At least 250 employees or annual turnover at least 50 million or annual balance sheet at least 43 million.

Important enterprises

Medium sized from Annex I and medium/large from Annex II
At least 50 employees or annual turnover or annual balance sheet at least 10 million.

Affected regardless of size or turnover

Entities of a type referred to in Annex I or II, where:

(a) services are provided by:

(i) providers of public electronic communications networks or of publicly available electronic communications services;

(ii) trust service providers;

(iii) top-level domain name registries and domain name system service providers;

(b) the entity is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities;

(c) disruption of the service provided by the entity could have a significant impact on public safety, public security or public health;

(d) disruption of the service provided by the entity could induce a significant systemic risk, in particular for sectors where such disruption could have a cross-border impact;

(e) the entity is critical because of its specific importance at national or regional level for the particular sector or type of service, or for other interdependent sectors in the Member State;

(f) the entity is a public administration entity:

(i) of central government as defined by a Member State in accordance with national law; or

(ii) at regional level as defined by a Member State in accordance with national law that, following a risk-based assessment, provides services the disruption of which could have a significant impact on critical societal or economic activities.

3. Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.

4. Regardless of their size, this Directive applies to entities providing domain name registration services.

6. ORGANIZATIONS AFFECTED - ANNEX I (OF NIS2 PAPER)

High Criticality

Energy (production, distribution)

Transport (air, rail, water, road) including companies responsible for the infrastructure

Finance

Health

Drinking water

Waste water

Digital infrastructure (ISPs, DNS, cloud infra & apps, data centers, Cas)

ICT Services (b2b managed services)

Public Administration

Space

7. ORGANIZATIONS AFFECTED - ANNEX II (OF NIS2 PAPER)

Other critical sectors

Postal & Courier services

Waste management

Chemical production, storage, distribution

Food production, processing, distribution

Manufacturing

a. Manufacturing of medical devices
b. Computer, electronic and optical products
c. Electrical equipment
d. Machinery
e. Motor vehicles & trailers
f. Other transport equipment

Digital providers (online marketplace, search engines, social networking)

Research

8. ORGANIZATIONS INDIRECTLY AFFECTED

Indirectly affected are organizations that belong to the supply chain of the affected organizations.

NIS2 considers those mostly to be ICT companies.

NIS2 prescribes that affected organizations should select their supply chain in such a way that compliance will not be jeopardized. That means that the supply chain must have a similar level of Cybersecurity measures as the affected organizations themselves. Otherwise, the affected organizations will not want to work with them anymore.

9. NIS2 IMPOSED REQUIREMENTS IN TITLES

- Risk management measures
- Incident management (prevention, detection and response) and incident reporting
- Business Continuity and Crisis Management
- Supply chain security (with a focus on supplier relationships)
- More transparent disclosure and management of vulnerabilities
- Cooperation between Member States

Or more elaborated from Chapter IV, Article 21

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) **the use of multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

10.SPECIFIC DEMANDS FROM THE ORIGINAL TEXT AND OUR COVERAGE

This section contains the articles which are of interest to "hands on" Cyber Security solution providers and of course the affected organizations. Where applicable, the solutions Inter Engineering can provide are mentioned.

Page 3. Preamble Article (8)

(8) The exclusion of public administration entities from the scope of this Directive should apply to entities whose activities are predominantly carried out in the areas of national security, public security, defense or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences. However, public administration entities whose activities are only marginally related to those areas should not be excluded from the scope of this Directive. For the purposes of this Directive, entities with regulatory competences are not considered to be carrying out activities in the area of law enforcement and are therefore not excluded on that ground from the scope of this Directive.

CONCLUSION:

The public sector must also comply to NIS2. Only police, army, justice system not.

INTER ENGINEERING PROPOSED SOLUTION:

N/A

Page 4. Preamble Article (12)

(12) Postal service providers as defined in Directive 97/67/EC of the European Parliament and of the Council (7), including providers of courier services, should be subject to this Directive if they provide at least one of the steps in the postal delivery chain, in particular clearance, sorting, transport or distribution of postal items, including pick-up services, while taking account of the degree of their dependence on network and information systems. Transport services that are not undertaken in conjunction with one of those steps should be excluded from the scope of postal services.

CONCLUSION

Courier companies must comply with NIS2

INTER ENGINEERING PROPOSED SOLUTION:

N/A

Page 8, Preamble Article 35.

(35) Services offered by data center service providers may not always be provided in the form of a cloud computing service. Accordingly, data centers may not always constitute a part of cloud

computing infrastructure. In order to manage all the risks posed to the security of network and information systems, this Directive should therefore cover providers of data center services that are not cloud computing services. For the purposes of this Directive, the term 'data center service' should cover provision of a service that encompasses structures, or groups of structures, dedicated to the centralized accommodation, interconnection and operation of information technology (IT) and network equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control. The term 'data center service' should not apply to in-house corporate data centers owned and operated by the entity concerned, for its own purposes.

CONCLUSION

Data centers should comply with NIS2.

INTER ENGINEERING PROPOSED SOLUTION:

N/A

PAGE 10, Preamble Article 44

(44) The CSIRTs should have the ability, upon an essential or important entity's request, to monitor the entity's internet facing assets, both on and off premises, in order to identify, understand and manage the entity's overall organizational risks as regards newly identified supply chain compromises or critical vulnerabilities. The entity should be encouraged to communicate to the CSIRT whether it runs a privileged management interface, as this could affect the speed of undertaking mitigating actions.

CONCLUSION

This paragraph at least encourages essential and important entities to have a PAM

INTER ENGINEERING PROPOSED SOLUTION:

Privileged Access Management Solution. PrivX

Page 10, Preamble Article 49

(49) Cyber hygiene policies provide the foundations for protecting network and information system infrastructures, hardware, software and online application security, and business or end-user data upon which entities rely. Cyber hygiene policies comprising a common baseline set of practices, including software and hardware updates, password changes, the management of new installs, the limitation of administrator-level access accounts, and the backing-up of data, enable a proactive framework of preparedness and overall safety and security in the event of incidents or cyber threats. ENISA should monitor and analyze Member States' cyber hygiene policies.

CONCLUSION

Organizations must apply a "baseline set of practices," including

INTER ENGINEERING PROPOSED SOLUTION:

software and hardware updates => Withsecure software updater

Password changes: => PAM

The management of new installs => Limit what can be installed. WithSecure application control

limitation of administrator-level access accounts =>PAM

Backing-up of data => not in our current portfolio

Page 11, Preamble Article 55

(51) Member States should encourage the use of any **innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks**, enabling resources to be diverted towards cyberattacks more effectively. Member States should therefore encourage in their national cybersecurity strategy activities in research and development to facilitate the use of such technologies, in particular those relating to automated or semi-automated tools in cybersecurity, and, where relevant, the sharing of data needed for training users of such technology and for improving it. The use of any innovative technology, including artificial intelligence, should comply with Union data protection law, including the data protection principles of data accuracy, data minimization, fairness and transparency, and data security, such as state-of-the-art encryption. The requirements of data protection by design and by default laid down in Regulation (EU) 2016/679 should be fully exploited.

CONCLUSION

Encourages the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks.

INTER ENGINEERING PROPOSED SOLUTION:

In the IE portfolio several solutions contain AI, with most widely applied WithSecure EDR

Page 11, Preamble Article 56

(56) Member States should, in their national cybersecurity strategies, address the specific cybersecurity needs of small and medium-sized enterprises. Small and medium-sized enterprises represent, across the Union, a large percentage of the industrial and business market and often struggle to adapt to new business practices in a more connected world and to the digital environment, with employees working from home and business increasingly being conducted online. Some small and medium-sized enterprises face specific cybersecurity challenges such as low cyber-awareness, a lack of remote IT security, the high cost of cybersecurity solutions and an increased level of threat, such as ransomware, for which they should receive guidance and assistance. Small and medium-sized enterprises are increasingly becoming the target of supply chain attacks due to their less rigorous cybersecurity risk-management measures and attack management, and the fact that they have limited security resources. Such supply chain attacks not only have an impact on small and medium-sized enterprises and their operations in isolation

but can also have a cascading effect on larger attacks on entities to which they provided supplies. Member States should, through their national cybersecurity strategies, help small and medium-sized enterprises to address the challenges faced in their supply chains. Member States should have a point of contact for small and medium-sized enterprises at national or regional level, which either provides guidance and assistance to small and medium-sized enterprises or directs them to the appropriate bodies for guidance and assistance with regard to cybersecurity related issues. Member States are also encouraged to offer services such as website configuration and logging enabling to microenterprises and small enterprises that lack those capabilities.

CONCLUSION

Under NIS2 Cybersecurity measures at SMBs is considered crucial.
The majority of the market contains of SMBs.
SMBs suffer from Cyberattacks and have difficulties to apply security measures.
SMBs are the supply chain of larger organizations and thus a very prominent target for supply chain attacks.
Member states should support SMBs in their Cybersecurity measures.
Therefore, we can expect supporting plans like state funded subsidies for Cybersecurity in SMBs

INTER ENGINEERING PROPOSED SOLUTION:

Our complete portfolio

Page 12, Preamble Article 57

(57) As part of their national cybersecurity strategies, Member States should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy. Rather than responding reactively, active cyber protection is the prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network. This could include Member States offering free services or tools to certain entities, including self-service checks, detection tools and takedown services. The ability to rapidly and automatically share and understand threat information and analysis, cyber activity alerts, and response action is critical to enable a unity of effort in successfully preventing, detecting, addressing and blocking attacks against network and information systems. Active cyber protection is based on a defensive strategy that excludes offensive measures.

CONCLUSION

So, member states should also encourage Active cyber protection:

Prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner

INTER ENGINEERING PROPOSED SOLUTION:

This translates in using EPP, EDR, Vulnerability Management and preparations for incident handling

Page 17, Preamble Article 85

(85) Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers.

CONCLUSION

Essential and important organizations should protect themselves against possible supply chain attacks, by carefully selecting the partners in their supply chain. This will indirectly affect SMBs who are in the supply chain of essential and important organizations because if those SMBs will not have appropriate Cybersecurity measures, the essential and important organizations will stop working with them.

So essentially this means that all SMBs who are in the supply chain of an essential or important organization, should apply Cybersecurity measures as professional as those applied by the essential and important organizations.

INTER ENGINEERING PROPOSED SOLUTION:

Complete portfolio

Page 17, Preamble Article 89

(89) Essential and important entities should adopt a wide range of **basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness**, organize training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems.

CONCLUSIONS

Essential and important entities must apply wide range of basic cyber hygiene practices:

Zero trust principles: PAM

Software updates: EPP which includes updating

Network segmentation: Firewalling, routing & switching

Identity and access management: PAM

User awareness: Awareness training

AI based measures such as EDR

And of course, the self-explanatory: EPP, Backup

INTER ENGINEERING PROPOSED SOLUTIONS:

Zero trust principles: PAM

Software updates: EPP which includes updating

Network segmentation: Firewalling, routing & switching

Identity and access management: PAM

User awareness: Awareness training

AI based measures such as Endpoint Detection & Response (EDR)

And of course, the self-explanatory: Endpoint Protection (EPP)

Page 18, Preamble Article 90

(90) To further address key supply chain risks and assist essential and important entities operating in sectors covered by this Directive to appropriately manage supply chain and supplier related risks, the Cooperation Group, in cooperation with the Commission and ENISA, and where appropriate after consulting relevant stakeholders including from the industry, should carry out coordinated security risk assessments of critical supply chains, as carried out for 5G networks following Commission Recommendation (EU) 2019/534 (19), with the aim of identifying, per sector, the critical ICT services, ICT systems or ICT products, relevant threats and vulnerabilities. Such coordinated security risk assessments should identify measures, mitigation plans and best practices to counter critical dependencies, potential single points of failure, threats, vulnerabilities and other risks associated with the supply chain and should explore ways to further encourage their wider adoption by essential and important entities. Potential non-technical risk factors, such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance, include concealed vulnerabilities or backdoors and potential systemic supply disruptions, in particular in the case of technological lock-in or provider dependency

CONCLUSION

Security Risk Assessments will be done to find supply chain companies with lacking Cybersecurity.

Meaning that the supply chain companies should apply cybersecurity measures as well.

INTER ENGINEERING PROPOSED SOLUTION:

N/A

Page 18, Preamble Article 91

(91) The coordinated security risk assessments of critical supply chains, in light of the features of the sector concerned, should take into account both technical and, where relevant, non-technical factors including those defined in Recommendation (EU) 2019/534, in the EU coordinated risk assessment of the cybersecurity of 5G networks and in the EU Toolbox on 5G cybersecurity agreed by the Cooperation Group. To identify the supply chains that should be subject to a coordinated security risk assessment, the following criteria should be taken into account:

(i) the extent to which essential and important entities use and rely on specific critical ICT services, ICT systems or ICT products;(ii) the relevance of specific critical ICT services, ICT systems or ICT products for performing critical or sensitive functions, including the processing of personal data;

(iii) the availability of alternative ICT services, ICT systems or ICT products;

(iv) the resilience of the overall supply chain of ICT services, ICT systems or ICT products throughout their lifecycle against disruptive events; and

(v) for emerging ICT services, ICT systems or ICT products, their potential future significance for the entities' activities. Furthermore, particular emphasis should be placed on ICT services, ICT systems or ICT products that are subject to specific requirements stemming from third countries

CONCLUSION

NIS2 considers the supply chain to be (mainly) ICT companies.

INTER ENGINEERING PROPOSED SOLUTION:

N/A

Page 20, Preamble Article 98

(98) In order to safeguard the security of public electronic communications networks and publicly available electronic communications services, the use of encryption technologies, in particular end-to-end encryption as well as datacentric security concepts, such as cartography, segmentation, tagging, access policy and access management, and automated access decisions, should be promoted. Where necessary, the use of encryption, in particular end-to-end encryption should be mandatory for providers of public electronic communications networks or of publicly available electronic communications services in accordance with the principles of security and privacy by default and by design for the purposes of this Directive. The use of end-to-end encryption should be reconciled with the Member States' powers to ensure the protection of their essential security interests and public security, and to allow for the prevention, investigation, detection and prosecution of criminal offences in accordance with Union law. However, this should not weaken end-to-end encryption, which is a critical technology for the effective protection of data and privacy and the security of communications.

CONCLUSION

Communications should be protected by encryption. By default that is so in the usual methods of remote access / administration.

"…access policy and access management, and automated access decisions, should be promoted."

This is covered by PAM

INTER ENGINEERING PROPOSED SOLUTION:

SSH Tectia Server / Client

Privileged Access Management (PAM)

Page 20, Preamble Article (102)

Essential & Important entities are obliged to report incidents. Early warning within 24 hours, report within 72 hours.

CONCLUSION

Hiding an incident means infringement of the NIS2 regulation.

INTER ENGINEERING PROPOSED SOLUTION:

N/A

Page 20, Preamble Article 102 – 107 all about reporting

Page 27, Preamble Article 137

the management bodies of the essential and important entities should approve the cybersecurity risk-management measures and oversee their implementation.

CONCLUSION

The management of the entities is directly responsible for the cybersecurity measures.

Page 31. Chapter I, Article 3, paragraph 3

3. By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years thereafter

CONCLUSION

From 17-4-2025 and on the national and EU authorities will know which organizations need to comply with NIS2. They will have a list.

INTER ENGINEERING PROPOSED SOLUTION:

N/A

Page 48, Chapter IV, Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organizational measures…

… shall include **at least the following**:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) **the use of multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

CONCLUSION

Affected organizations need to develop and apply a number of procedures. They also need to apply practices where Cybersecurity solutions are involved.

INTER ENGINEERING PROPOSED SOLUTION:

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure: Vulnerability handling in network and information systems maintenance means a Vulnerability Management solution.

(g) Basic cyber hygiene practices. This includes essentially the whole portfolio.

(g) Cybersecurity training: Awareness training

(i) Human resources security, access control policies.

This involves access control measures such as Privileged Access Management

(j) The use of Multiple Factor Authentication. Inter Engineering has multiple solutions.

Page 56, Chapter VII, Article 32

Supervisory and enforcement measures in relation to essential entities

Lot of text

CONCLUSION

Summary: Authorities may do random or targeted audits and force organizations to settle their shortcomings in security and set a deadline. If deadline not made then consequences may be: stop activities affected by the lack of security, court cases, legal measures.

In case of targeted auditing the cost of the audit is paid by the organization being audited.

This does not apply to public sector organizations.

INTER ENGINEERING PROPOSED SOLUTION:

N/A

Page 60, Chapter VII, Article (34)

4. Member States shall ensure that where they infringe Article 21 or 23, essential entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.

5. Member States shall ensure that where they infringe Article 21 or 23, important entities are subject, in accordance with paragraphs 2 and 3 of this Article, to administrative fines of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

Sanctions

Violations of risk management measures or incident reports can be penalized:

- For essential entities: with administrative fines of up to €10,000,000 or at least 2% of the total annual worldwide turnover in the previous fiscal year of the company to which the essential entity belongs, whichever amount is higher.
- For important entities: administrative fines of up to €7,000,000 or at least 1.4% of the total annual worldwide turnover in the previous fiscal year of the company to which the important entity belongs, whichever amount is higher.

For the public sector, the transposing legislation may provide that the administrative fines do not apply to public administration entities. However, the other administrative sanctions will apply.

Member States may also provide for the power to impose periodic penalty payments to compel an essential or important entity to cease an infringement of the Directive in accordance with a prior decision of the competent authority.

To motivate compliance with the obligations in this Directive from senior management, natural persons representing essential entities may be held liable for failure to comply.

CONCLUSION

This section sets out the fines.

For essential entities: At least 2% of annual turnover, or 10M whichever higher.

For important entities: At least 1,4% of annual turnover, or 7M whichever higher.

Natural persons who represent an essential or important entity may also be held liable.

"Violations of risk management measures or incident reports can be penalized" so affected organizations must have risk management measures in place.

INTER ENGINEERING PROPOSED SOLUTION:

N/A

The rest of the articles are related to organizational obligations of the authorities, enforcement tasks and procedures of the authorities, penalties and fines, auditing procedures, organization of national CSIRTS and the like.

11.NIS2 SOLUTION TO DEMAND MAPPING MATRIX

Vendor	Solution	Related NIS2 article	Description of coverage
SSH	PrivX Privileged Access Management (PAM)	44,49,89,98 21(i)	44 encourages entities to have a PAM 49 limitation of administrator-level access accounts, Password changes 89 Adopt Zero Trust principle 89 Identity and access management 98 access policy and access management, and automated access decisions 21(i) access control policies
SSH	Tectia SSH Server / Client	98 21(h)	98 end-to-end encryption to safeguard security of electronic communications 21(h) use of cryptography
WithSecure	Endpoint Protection (EPP), includes Software Updater	49,57,89 21(g)	49 Recommends Cybersecurity baseline including: Software updates 57 Prevention, detection of network security breaches in an active manner 89 Basic Cyber Hygiene practices including software updates 21(g) Basic cyber hygiene practices
WithSecure	Endpoint Detection & Response (EDR)	55,57,89	55 encourages use of innovative technology, including artificial intelligence 57 Prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner 89 Pursue integration of technologies such as AI and machine learning
WithSecure	Vulnerability Manager	57 21(e)	57 Prevention of network security breaches in an active manner 21(e) Vulnerability handling in network and information systems maintenance means a Vulnerability Management solution
WithSecure	Collaboration Protection for M365	89	89 Basic cyber hygiene practices. Here augmentation of security in M365

Vendor	Solution	Related NIS2 article	Description of coverage
Censornet	Integrated cloud platform for Email & Web Security, CASB and Awareness Training	55	55 encourages use of innovative technology, including artificial intelligence
Censornet	Email Security	89	89 Basic cyber hygiene practices
Censornet	Web Security	89	89 Basic cyber hygiene practices
Censornet	Security Awareness Training (automated)	89 21(g)	89 Basic cyber hygiene practices including awareness training 21 (g) Basic cyber hygiene practices and awareness training
Censornet	Multiple Factor Authentication	21(i)	21(i) The use of Multiple Factor Authentication
Onespan	Multiple Factor Authentication	21(i)	21(i) The use of Multiple Factor Authentication
Inter Engineering	Secure Email Managed Service	89 21(g)	89 Basic cyber hygiene practices 21(g) Basic cyber hygiene practices
Inter Engineering	Managed Detection & Response service	55,57,89	55 encourages use of innovative technology, including artificial intelligence 57 Prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner 89 Pursue integration of technologies such as AI and machine learning
Inter Engineering	M365 Collaboration protection Managed Service	89	89 Basic cyber hygiene practices. Here augmentation of security in M365
Inter Engineering	Vulnerability Management Managed Service	57 21(e)	57 Prevention of network security breaches in an active manner 21(e) Vulnerability handling in network and information systems maintenance means a Vulnerability Management solution
Inter Engineering	Endpoint Protection Managed Service	49,57,89 21(g)	49 Recommends Cybersecurity baseline including: Software updates 57 Prevention, detection of network security breaches in an active manner 89 Basic Cyber Hygiene practices including software updates 21(g) Basic cyber hygiene practices
Inter Engineering	Entire portfolio	56,85 21(g)	56 Cybersecurity measures for SMBs 85 Protection against supply-chain attacks 21(g) Basic Cyber hygiene practices

12.NIS2 DEMAND TO SOLUTION MAPPING MATRIX

NIS2 Article	NIS2 Description	Inter Engineering Solution covering the requirement
44	encourages entities to have a PAM	PrivX PAM from SSH Communications
48	limitation of administrator-level access accounts, Password changes	PrivX PAM from SSH Communications
49	Recommends Cybersecurity baseline including: Software updates	Endpoint Protection (EPP), includes Software Updater from Withsecure Endpoint Protection Managed Service from Inter Engineering
55	encourages use of innovative technology, including artificial intelligence	Endpoint Detection & Response (EDR) from Withsecure Integrated cloud platform for Email & Web Security, CASB and Awareness Training from Censornet Managed Detection & Response Service from Inter Engineering
56	Cybersecurity measures for SMBs	Entire Portfolio from Inter Engineering
57	Prevention, detection, monitoring, analysis and mitigation of network security breaches in an active manner	Endpoint Protection (EPP) from Withsecure Endpoint Detection & Response (EDR) from Withsecure Vulnerability Manager from Withsecure Managed Detection & Response Service from Inter Engineering Vulnerability Management Managed Service from Inter Engineering Endpoint Protection Managed Service from Inter Engineering
85	Protection against supply-chain attacks	Entire Portfolio from Inter Engineering
89	Adopt Zero Trust principle, Identity and access management	PrivX PAM from SSH Communications

NIS2 Article	NIS2 Description	Inter Engineering Solution covering the requirement
89	Basic Cyber Hygiene practices including software updates	Endpoint Protection (EPP), includes Software Updater from Withsecure
89	Pursue integration of technologies such as AI and machine learning	Endpoint Detection & Response (EDR) from Withsecure Managed Detection & Response Service from Inter Engineering
89	Basic cyber hygiene practices	Collaboration Protection for M365 augmentation of security in M365 from Withsecure Email Security, Web security from Censornet Secure Email Managed Service from Inter Engineering M365 Collaboration protection Managed Service from Inter Engineering Endpoint Protection Managed Service from Inter Engineering
89	Basic cyber hygiene practices including awareness training	Security Awareness Training (automated) from Censornet
98	Access policy and access management, and automated access decisions	PrivX PAM from SSH Communications
98	end-to-end encryption to safeguard security of electronic communications	Tectia SSH Server / Client from SSH Communications