secior.

DIGITAL RISK
MANAGEMENT

NIS2 Whitepaper

Food & Beverage Manufacturers -Suppliers & -Distributors

21/07/2023

Reference number 20231204001

Colophon

Editorial Team

T. +31 85 273 6036

E. info@secior.com

W. www.secior.com

Contributors

Sander Nieuwmeijer (Secior)

Fred Streefland (Secior)

Edward Heck RA (Secior)

Poncke Poncin (HvA)

Edition

NIS2 White Paper

May 2023

Disclaimer

The 'NIS2 White Paper' (hereinafter referred to as "report") presents information and data compiled and/or collected by Secior (all information and data referred to herein as "data"). Data in this report may be subject to change without prior notice. While Secior takes all reasonable steps to ensure the accuracy of the data compiled and/or collected in this report, Secior provides the data "as is, as available" and without any warranty, express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement; makes no representations, express or implied, regarding the accuracy of the data in this report or its suitability for any specific purpose; and assumes no liability for any use of the data mentioned herein or reliance thereon, especially regarding any interpretation, decisions, or actions based on the data in this report. Other parties may have proprietary interests in some of the data mentioned in this report. Secior does not declare or warrant in any way that it owns or controls all rights to all data and is not liable to users for claims brought against users by third parties in connection with their use of data. Secior, its employees, do not endorse or warrant products or services of third parties based on data, material, or content referred to or included in this report.

Contents

Introduction

NIS2

Food & beverage manufacturers, suppliers, and distributors play a crucial role in our modern society. They are responsible for storing, managing, and processing large quantities of food and beverages used by governments, businesses, and citizens. Without food producers, our society would not function.

Given the above facts, the food & beverage industry is now classified as critical infrastructure, just like hospitals and utilities. Therefore, it is essential to emphasize that cybersecurity requirements within these organizations must be effectively implemented and enforced.

The vital role the food & beverage industry plays in delivering these goods to users means that these organizations must comply with the NIS2 directive from January 1, 2025. This European Union directive is the successor to the original NIS (Network & Information Security) and is designed to ensure the cyber resilience of organizations that fall under critical infrastructure.

The food & beverage industry will need to take measures to protect itself against cyberattacks. In this document, Secior explains the implications of the NIS2 directive for institutions and provides insights into the steps that can be taken to enhance the cyber resilience of their systems.

NIS2

Cyber resilience is becoming increasingly important as cybercriminals can cause significant harm to business continuity. In addition to the damage, the societal impact must also be considered. Systems are now often interconnected, meaning that a small vulnerability in one system can lead to significant problems in the chain, with potentially severe consequences for society. Therefore, the European Union has chosen to revise the directive.

What is the NIS2 Directive?

The NIS2 directive (Network and Information Systems 2) is European legislation aimed at strengthening the cybersecurity of essential service providers and digital service providers. The directive mandates these organizations to implement appropriate and proportionate measures to secure their network and information systems against cyber threats and report incidents to the relevant authorities. The goal of the NIS2 directive is to enhance Europe's digital resilience and reduce the impact of cyberattacks on critical infrastructure and digital service providers.

To combat the increasing threats of digitization and the wave of cyberattacks, the European Commission proposed a renewal of the NIS directive to tighten security requirements, address supply chain security, clarify reporting requirements, and strengthen supervisory measures with uniform sanctions across the EU.

The expansion of NIS2 requires a significant number of organizations to drastically change their cybersecurity policies. The idea behind this is to elevate the level of cybersecurity in Europe in the long term.

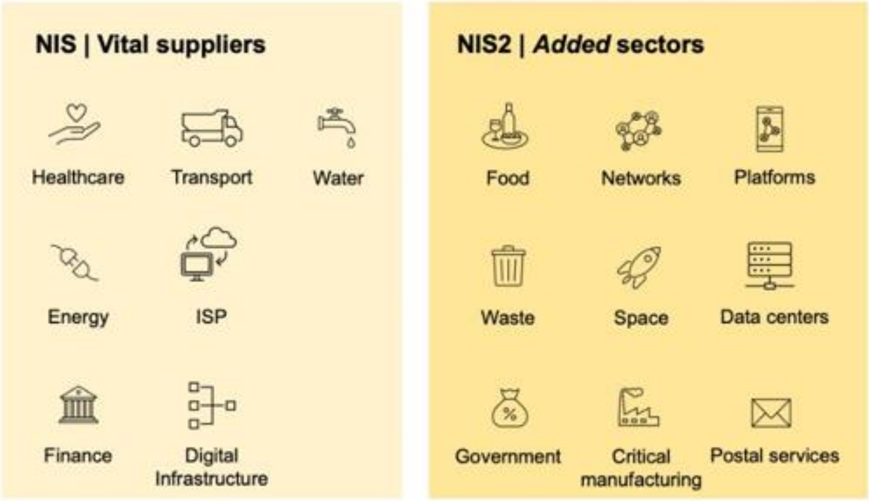
The full name of NIS2 is "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive)."

Why the NIS2 Directive?

The main issue with the NIS1 directive (Network & Information Systems) was that it did not adequately align with the rapidly evolving threat landscape and the fast-changing digital environment. The directive focused on securing critical infrastructure and digital service providers in the EU, but it was limited in the scope of organizations falling under the directive and contained limited measures and requirements for network and information systems' security. Hence, the NIS2 directive was developed to address the shortcomings of NIS1 and offer a more holistic approach to safeguarding Europe's digital infrastructure.

Which sectors are included in NIS2?

Old Sectors	Newly added sectors (2024)
▪ Healthcare	▪ Production, processing, and distribution of food
▪ Transport	▪ Providers of electronic networks, communications, or services
▪ Banking and financial services infrastructure	▪ Digital services like social media platforms, etc.
▪ Digital infrastructure	▪ Wastewater and waste management
▪ Water supply	▪ Space industry
▪ Energy	▪ Datacenters
▪ Digital service providers	▪ Government agencies
	▪ Production of critical products (pharmaceutical, medical, chemical, etc.)
	▪ Mail and courier services



Deciding NIS2 Policy Coverage

The NIS2 directive applies to two main types of organizations: Operators of Essential Services (OES) and Providers of Digital Services (PDS).

OES are organizations that provide essential services in the aforementioned sectors (such as energy, transportation, banking, healthcare, and, of course, the food & beverage industry) and meet certain thresholds concerning the number of users they serve, the impact of a cyber incident on their service, and the interconnectedness with other essential services. The exact thresholds may vary per EU member state, but they are defined in a way that only the most critical organizations fall under the directive.

PDS are organizations that offer online services to the EU market, such as online marketplaces, cloud computing services, or search engines. These organizations fall under the directive if they meet specific criteria related to their size, security risks, and impact on the functioning of the internal market.

In general, the NIS2 directive applies to organizations that provide essential services or online services crucial to the functioning of the EU's internal market and society and, therefore, require a high level of network and information security.

Implications

Similar to the application of GDPR, NIS2 Organizations are subject to a penalty scheme. Thus, these organizations must ensure compliance to avoid penalties. Article 32, paragraph 6, states that every executive of an organization must be authorized to implement cybersecurity measures, and they can be held liable if they fail to demonstrate that they have taken all necessary steps to prevent a cybersecurity incident.

As a consequence of NIS2, thorough checks on governance will be conducted. More inspections and audits will be carried out by regulators than before. If these inspections reveal that organizations do not meet the NIS2 requirements, significant fines can be imposed. Expectations regarding the handling of a cyber incident will also increase. Many organizations will have an obligation to report an incident once it is discovered, similar to the GDPR. This notification must be made within 24 hours, followed by a final report within one month of the incident.

Additionally, NIS2 requires companies to collaborate with their suppliers to discuss the cyber risks that can affect the supply chain. Cybercriminals can target organizations through the networks of (external) parties. The way suppliers and partners handle their security directly impacts your own security. Therefore, chain risks must be identified and agreements made on how to manage these risks. The allocation of liability for the costs of a cyber incident will also need to be stipulated in contracts.

Since cybersecurity is a specialized field, it is advisable to involve a specialized (legal) service provider in making contractual arrangements.

NIS2 Required Elements

Regarding the new cybersecurity risk management framework of NIS2, "appropriate" and "proportionate" measures must be taken, considering the state of technology and existing risks. However, new is the addition of several minimal basic security elements that must be provided.

These measures include:

- Risk analysis ▪ Incident handling
- Business continuity (backups, etc.)
- Supply chain security ▪ Security in the acquisition, development, and maintenance of IT/OT systems; vulnerability management
- Policies and procedures to assess the effectiveness of cybersecurity measures
- Basic cyber hygiene and cybersecurity training
- Cryptography and encryption (where applicable)
- HR, access control, and asset management security
- Multi-factor authentication where possible within the organization

Importantly, the proposed NIS2 directive, unlike the current NIS directive, introduces explicit requirements for managing risks for third parties in supply chains and the potential impact on supplier relationships. This addresses one of the key challenges in cybersecurity at present. The proposal stipulates that the European Commission will establish the technical and methodological specifications of the minimum requirements and determine whether entities can and/or must demonstrate compliance by obtaining a cybersecurity certificate.

Reporting

The reporting obligations are also expanded. Essential and large entities will be required to report incidents that affect the delivery of their services.

Within 24 hours of becoming aware of an incident, the entity must provide an early warning to the national Computer Security Incident Response Team (CSIRT).

In the Netherlands, the criteria for what constitutes a "significant" cyber incident for Operators of Essential Services (OES) are defined in the Dutch Cybersecurity Assessment Framework (CSA). The CSA is a national standard that provides guidelines for assessing the cybersecurity risks of organizations that manage critical infrastructure.

According to the CSA, a cyber incident is considered significant if it meets at least one of the following criteria:

- It causes a significant disruption of the essential service provided by an OED.
- It results in a significant loss or leakage of data or information, such as personal data or confidential business information.
- It leads to significant financial or reputational consequences for the OED.
- It is part of a large-scale cyber campaign targeting multiple OEDs.

The definition of a "significant" cyber incident may vary per European member state, but generally includes incidents with significant impacts on the continuity of essential services or the security of data and information.

Furthermore, these entities must submit an incident report within 72 hours, detailing the severity and impact of the incident. Finally, organizations must submit a final report within one month of the incident, which includes:

- A detailed description of the incident, including its severity and consequences.
- The type of threat or main cause likely to have led to the incident.
- Applied and ongoing risk mitigation measures.
- If applicable, the cross-border implications of the incident.

Heavier Sanctions & Personal Liability

The NIS2 directive includes a framework for sanctions and penalties in case of non-compliance with the regulations. The specific penalties and sanctions may vary per European member state but must be effective, proportionate, and dissuasive.

For Operators of Essential Services, the competent authorities can impose administrative fines of up to €10 million or 2% of the total annual turnover of the OES, whichever is higher, for non-compliance with the NIS2 directive. The competent authorities can also order the OES to take specific corrective measures or, if necessary, suspend or revoke the OES's permit.

In addition to these penalties and sanctions, failure to meet the legal standards of the NIS2 directive can have other consequences. These consequences may include reputational damage, loss of customers, financial losses, and legal liability. A severe cyber incident resulting in the unintentional release of sensitive data or disruption of essential services can have serious and long-lasting consequences for an organization and its stakeholders.

Once NIS2 is in effect, it increases the (minimum) effort organizations must put into cybersecurity. Governments may hold executives personally liable if gross negligence is proven after a cyber incident. However, the security requirements are open norms. Therefore, discussions about personal liability only arise when there are deficiencies that do not fully meet the requirements. Moreover, financial penalties can be imposed on directors.

Timeline

October 28, 2021: The European Commission approves the draft proposal of the EU NIS2 (Network and Information Systems Directive 2) working group.

May 13, 2022: The co-legislators reach a provisional agreement on the NIS2 text.

November 2022: The European Parliament and the Council reach a formal political agreement on NIS2.

January 16, 2023: NIS2 Directive comes into effect, and European member states have until October 17, 2024, to transpose the NIS2 measures into national laws and regulations.

July 17, 2024: Today and every 18 months thereafter, EU-Cyclone submits an evaluation report to the European Parliament and the Council regarding its activities (management of large-scale cybersecurity incidents, coordinating crises, and supporting decision-making at the political level concerning such incidents and crises).

October 17, 2024: By this date, member states must establish and publish the necessary measures to comply with the NIS2 directive (may also be done earlier).

October 18, 2024: Directive (EU) 2022/2055 (the NIS directive) is incorporated into local legislation.

January 1, 2025: All organizations falling under the specified sectors must comply with the NIS2 directive.

January 17, 2025: The cooperation group, with the assistance of the Commission, ENISA, and, if applicable, the CSIRT (Computer Security Incident Response Team) network, establishes the methodology and organizational aspects of peer reviews to learn from shared experiences, enhance mutual trust, achieve a high common level of cybersecurity, and strengthen the cyber capabilities and policies of member states in implementing this directive. Participation in peer reviews is voluntary. Cybersecurity experts designated by at least two other member states other than the one being reviewed conduct the peer reviews.

April 17, 2025: (at the latest): Member states compile a list of essential and important entities and entities offering domain name registration services. The member states evaluate this list regularly and update it at least every two years as needed. Every two years, the competent authorities inform the Commission and the cooperation group of the number of essential and important entities in each sector.

October 17, 2027: Every 36 months, the Commission evaluates the functioning of this directive and reports to the European Parliament and the Council.

Cyber Resilience

In the digital world as we know it now, we do many things more efficiently than 30 years ago, such as administration, banking, and communication. As we strive for increasing efficiency, we have become more dependent on the means that allow us to achieve this.

The food & beverage industry is indispensable and plays a crucial role in modern infrastructure. Partial or complete disruption in this sector can have significant consequences for society, including the delivery of fresh goods or other food products. Therefore, the food & beverage industry is considered part of critical infrastructure.

NIS2 and the Food & Beverage Industry

The NIS2 directive designates the food & beverage industry as critical infrastructure, which means additional requirements are imposed on the sector to enhance cyber resilience. Cyber resilience refers to the extent to which a digital environment is free from danger or damage due to network or system failures. Cybersecurity is as strong as the weakest link, so the overall level of cybersecurity must continually improve for the benefit of all.

IT & OT

The food & beverage industry utilizes various systems, including power supply, climate control, processing machines, access control, etc. These critical systems are necessary for proper daily operations and fall under Operational Technology (OT), also known as process automation, which is often remotely connected to a central management system. While Information Technology (IT) is entirely under the responsibility of the network administrator, it is not always clear which department is responsible for the OT part. This could be the facility department or outsourced to a third party.

Due to this ambiguity, the level of cyber resilience in OT systems is not always transparent. Visibility in OT is crucial as the proper functioning of typical OT systems is essential for business operations. Vulnerabilities in OT, resulting from incorrect patch management, weak password policies, or inadequate logical network segmentation, can enable cybercriminals to disrupt or sabotage operations.

Considering the NIS2 directive, attention must be given not only to IT cybersecurity but also to OT cybersecurity. Cybersecurity practices already known in the IT world can also be applicable to OT environments. The following chapter will describe the steps for cybersecurity in the food & beverage industry to comply with the NIS2 directive.

Incidents

In recent years, the food & beverage industry has become a significant target of cyber-attacks. Cybercriminals are becoming more sophisticated and continuously searching for weak points in systems. Numerous cases have been reported where manufacturers, suppliers, and distributors have been targeted, compromising their security. This has raised concerns about cybersecurity and the need to protect these systems from attacks.

Examples of cyber incidents in the food industry include an attack on a logistics company responsible for distributing cheese products for AH supermarkets in April 2021. The supplier's computer system was hacked through a ransomware attack, leading to 250 trucks from Bakker Logistiek being immobilized. Another example is the cyberattack on Canadian company Maple Leaf in 2022, which temporarily halted production and caused serious operational disruptions.

Physical Infrastructure

Not only virtual attacks but also the cybersecurity of physical infrastructure is becoming a growing problem. The increasing frequency of cyber-attacks highlights the necessity for robust cybersecurity measures. These attacks can result in data loss, financial losses, and reputational damage.

Next Steps

This section discusses the steps that can be taken to become NIS2 compliant:

Step 1: Determine the NIS2 Scope

Identifying which OT/IT systems fall within the scope of NIS2 is the first step towards successful compliance. Key questions to address include:

- What essential services does the organization provide?
- Does the organization fall under the scope of NIS2?
- What new requirements must the organization implement within the scope of NIS2?
- If the organization is not directly subject to NIS2, does it deal with suppliers or customers who are subject to the new rules?
- What obligations must organizations impose on their suppliers or business customers in their contractual arrangements?

For organizations not directly falling under the new law, understanding the legal requirements will be essential. It will also be crucial to determine whether additional local IT/OT security regulations need to be established due to any national regulations.

Step 2: Implement Appropriate Security Measures

The organization must take appropriate security measures to protect its critical systems and infrastructure. These measures can include firewalls, intrusion detection systems, encryption, access controls, and training and awareness programs for staff.

These measures can be divided into different parts:

- Inventory of information systems.
- Conducting a threat analysis.
- Identifying threats affecting operations.
- Prioritizing security risks.
- Developing and implementing a security plan, reviewing and mitigating.
- Update the plan regularly (e.g., quarterly).

When developing measures, organizations can make use of existing measures such as ISO 27001 or other certifications and encryption. Besides building management systems and the buildings, themselves, Operational Technology (OT) and Internet of Things (IoT) applications must be added to the system inventory.

The rise of IoT has made it easier to use sensors instead of physical systems. However, these sensors often lack the same level of security configuration, which can result in cyber incidents.

Step 3: Reporting Cyber Incidents + Documentation.

In case of a significant cyber incident, the organization must report it to the relevant authorities within 24 hours. They must also keep a record of the incident and provide a full report to the authorities within one month.

Compliance requires documentation of organizational measures. For example, the absence of documentation of cybersecurity measures means there is no evidence of compliance.

Auditors may request a wide range of evidence when assessing organizations' compliance with NIS2. This step can be overwhelming, especially for organizations just beginning their compliance journey. A holistic governance system can not only help track progress and improve documentation but also provide a multidisciplinary perspective and a solid framework for businesses to proactively manage cyber threats and work towards countering cyber threats, both now and in the future.

APPENDIX

References:

https://www.security.nl/posting/698665/Ransomware+zorgde+voor+lege+schappen+op+kaasafdelingen+Albert+Heijn

https://www.cybertalk.org/2022/11/10/maple-leaf-foods-confirms-outage-due-to-cyber-security-incident/

https://www.cbsnews.com/miami/news/cyberattack-on-food-giant-dole-temporarily-shuts-down-north-american-production/

Important Organizations:

NCSC - National Cyber Security Centre

https://www.ncsc.nl/

RDI - Rijksinspectie Digitale Infrastructuur (Inspectorate for Digital Infrastructure)

https://www.rdi.nl/

About the Author:

Secior B.V. is a Dutch cybersecurity company with a focus on the cyber resilience of critical infrastructure organizations.

Secior's background lies in the Mission Critical data center industry, which forms the backbone of our digital society.

Their expertise in OT combined with profound cybersecurity experience and proven security compliance methodologies from the demanding financial sector. Secior's specialized knowledge is offered to other vital sectors.

Secior provides (NIS2) Compliance and Cybersecurity Services, including precise OT, IT & IoT detection, enabling a swift response to cyber threats, risks, and anomalies. This helps prevent cyber attacks or significantly reduce the damage of such attacks.

In addition, Secior offers 24/7 monitoring from a Managed Security Operating Center (SOC), NIS2 Gap analyses, Incident Response, Awareness training, and specialized legal support.

secior.

DIGITAL RISK MANAGEMENT

Boeing Avenue 254

1119 PZ Schiphol-Rijk

The Netherlands

T +31 85 273 6036

info@secior.com

www.secior.com