EVERSHEDS SUTHERLAND

Unlocking cybersecurity

Everything you need to know about the NIS2 directive

In partnership with

Contents

Thank you for reading our white paper on the NIS2 directive. In this white paper we will discuss the most important aspects of the NIS2 directive and how it applies to organizations in the EU.

The NIS2 Directive, also known as the new version of the Network and Information Security Directive, is a European directive aimed at strengthening cybersecurity in the European Union (EU). The Directive is designed to help organizations protect themselves against cyber threats and to ensure that the EU's cyber infrastructure is more secure and robust. Now that the directive **has been finally officially published**, member states have 21 months - ie until 17 October 2024 - to integrate the provisions of the directive into local legislation.

In this white paper we will give an overview of the most important provisions of the NIS2 directive and how they apply to organizations in the EU. We will also discuss the obligations that organizations have to comply with the directive and how we, **ESET Netherlands** and **Eversheds Sutherland,** can support this.

We hope this white paper will be useful for organizations looking to learn more about how to protect themselves against cyberthreats and how to comply with the NIS2 directive.

Dave Maasland
CEO, ESET Netherlands

Olaf van Haperen
Partner, Eversheds Sutherland

What is the NIS2 directive?

NIS2

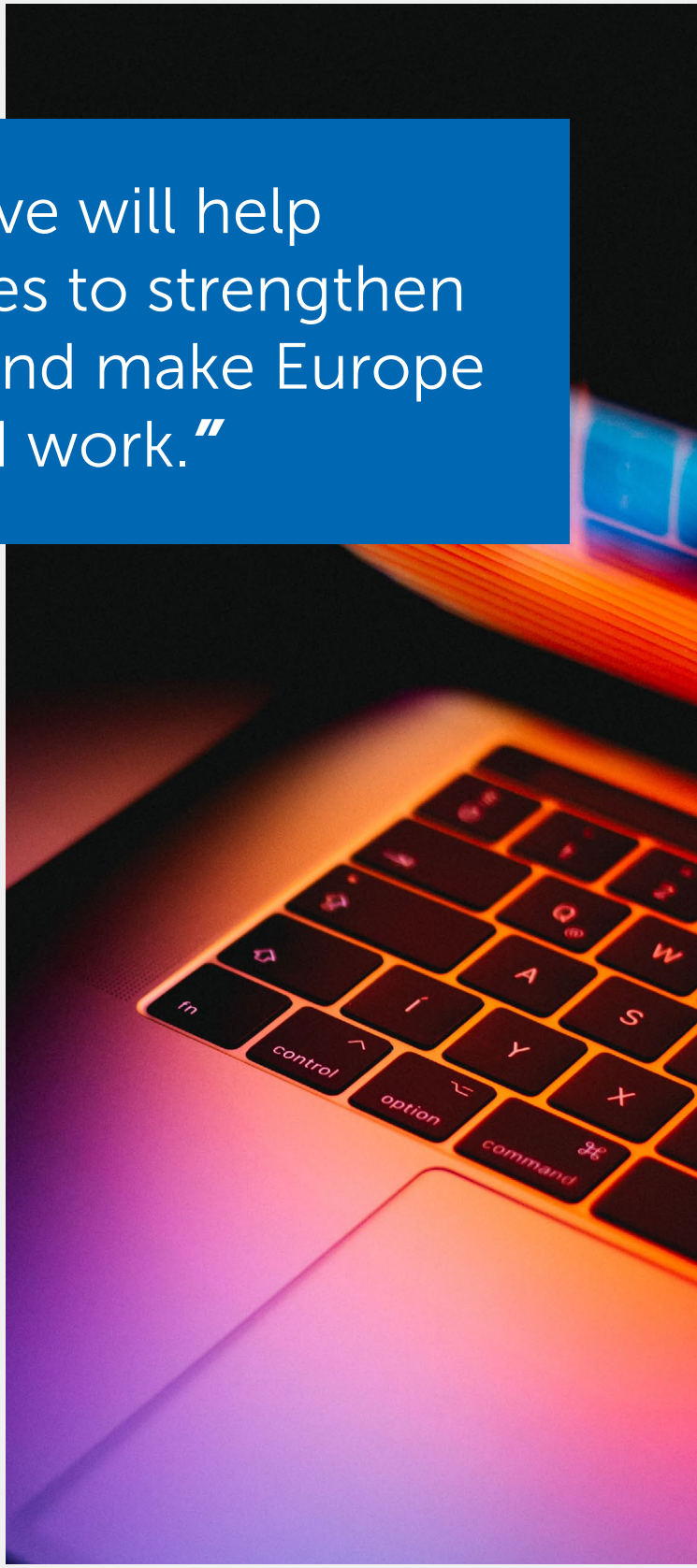
Is your organization medium or large and active in one of the critical sectors such as energy, transport, health and digital infrastructure?

Then new legislation from the EU can have a lot of impact on the requirements for cybersecurity within your organization. "This European directive will help around 160,000 entities to strengthen their grip on security and make Europe a safe place to live and work. The law should also allow for the sharing of information with the private sector and partners around the world.

If we are attacked on an industrial scale, we have to react on an industrial scale," said **Dutch MEP** Bart Groothuis.

Because cybersecurity is extremely important for the protection of our society, the European Union (EU) introduced the first Directive on *Network and Information Security* (NIS Directive) in 2016. Although this European directive has ensured greater coherence within the EU in the field of network and information security, according to the European Parliament, cyber resilience must be increased even further to protect society. With increasing digitization and large numbers of cyberattacks, the NIS Directive now has been revised and improved. The NIS2 Directive will have a wider reach and focus on more sectors, in order to equalize and increase the cyber resilience of organizations domiciled in EU Member States.

> "This European directive will help around **160,000** entities to strengthen their grip on security and make Europe a safe place to live and work."



Risk management and collaboration

But how will this revised directive ensure better cyber resilience? The NIS2 tries to improve the level of cybersecurity within EU member states in various ways. The Directive strengthens imposed security requirements, focuses on addressing supply chain security (the production or supply chain), streamlining reporting obligations, tightening supervisory measures and introducing enforcement requirements with harmonized sanctions in all Member States. The importance of information sharing and (inter)national cooperation in the field of crisis management is also addressed.

Scope of the NIS2

The NIS2 Directive affects many more sectors than the original NIS Directive. The NIS Directive only designated *Healthcare, Transport, Banking and Financial Market Infrastructure, Digital Infrastructure, Water Supply, Energy and Digital Service Providers* with the scope for Member States to define which organizations were considered essential. The NIS2 introduces uniform rules for medium and large bodies operating in critical sectors, such as *energy, transport, health and digital infrastructure.* This now includes *'very critical sectors',* including *energy, transport, banking, financial market infrastructure, healthcare, drinking water, waste water, digital infrastructure, ICT (B2B) management, government and space* and 'critical sectors', such as *postal and courier services, waste management, chemicals, food, manufacturing, digital providers and research*. All medium-sized and large enterprises in these sectors will be covered by the legislation.

Essential or important?

The way in which enforcement will take place depends on the category in which an organization falls. Under the NIS2 there are two categories under which organizations may fall. Organizations can be labeled as **essential** or as **important**. Whether an organization is labeled as essential or important depends on whether the organization falls under a critical or a very critical sector and depends on the size of the company.

Very critical Critical

- Energy
- Transport
- Banking
- Infrastructure for the financial market
- Health care
- Drinking water
- Wastewater
- Digital infrastructure
- Management of ICT services (B2B)
- Government
- Space travel
- Postal and courier servcies
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacture
- Digital providers
- Research

How big is your organization?

*** Large organizations**

*** Medium-sized organizations**

Large organizations

Medium-sized organizations

Essential

Important

* There are some exceptions to the rule, where entities such as, for example, qualified trust service providers, top-level domain name registries as well as DNS service providers, can be designated as essential regardless of the size of their organization. For all exceptions see Article 3(1).

Large:

more than 250 employees and an annual turnover of at least 50 million euros (or a balance sheet total of at least 43 million euros).

Medium-sized:

more than 50 and fewer than 250 employees and an annual turnover not exceeding 50 million euros (or a balance sheet total not exceeding 43 million euros).

Source: https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN

22%

The expected increase in ICT budget of organizations that are not yet covered by the NIS Directive

Medium-sized organizations with fewer than 250 employees and an annual turnover of up to 50 million euros (or balance sheet total of up to 43 million euros) operating in very critical sectors are considered important, along with other large and medium-sized organizations in critical sectors. Only large organizations that exceed the ceilings for medium-sized organizations and fall under very critical sectors are considered **essential**. Some organizations are automatically considered "essential", regardless of their size, if a service outage would have serious consequences to society or they are the exclusive national provider. This includes organizations that provide public communications networks and services, trust service providers, and top-level domain name and domain name registration service providers.

In principle, the NIS2 Directive does not target small and micro-enterprises that have fewer than 50 employees and an annual turnover of less than 7 million euros (or a balance sheet total of less than 5 million euros). But if they have a key role for society, economy, sectors or services, Member States must ensure that they are covered by this directive.

The main difference between essential and important entities is in the monitoring of compliance with the rules. For the essential entities, mainly parties from vital sectors, supervision will be proactive. This means that these organizations will actively be monitored whether the legislation is being complied with. In the case of the important entities, supervision takes place afterwards, if there are indications that there is an incident. If, after an incident, it appears that the organization has not taken the required steps, these organizations may also have to deal with possible consequences of non-compliance with this legislation.

What can we expect from the NIS2?

We will explain this on the basis of two use cases.

BRIGHTENERGIES
ENERGY COMPANY

Energy company BrightEnergies with 500 employees already had to deal with security obligations with the introduction of the first NIS Directive. In the local NIS legislation (in the Netherlands included in the Network and Information Systems Security Act), the sector to which it belonged ('energy') was classified as a vital provider. The current director Lennard was not yet working at BrightEnergies, but there is documentation of which measures and processes were adjusted or renewed at that time. In 2022, he learned that there would be new NIS legislation. In this new legislation, an energy company is an 'essential entity'. With the introduction of the NIS legislation, quite a few changes had already been made. Because hackers in other countries (such as Luxembourg, Italy and Portugal) have already targeted energy companies several times, Lennard wants to do everything he can to ensure that BrightEnergies is not affected. The NIS2 legislation is therefore given high priority.

WASTE2RESOURCE

Waste processor and recycling company Waste2Resource was previously not covered by NIS or other cybersecurity legislation. In recent years, however, it has become clearer that even a waste processor may have to deal with a cyber-attack: a competitor was shut down for days in 2021 due to ransomware, which prevented the garbage trucks from driving. The IT team at Waste2Resource is happy that they fall under the NIS2 directive, but there is a lot of work to be done. The team, led by the newly hired CISO Kayleigh, is currently busy with the preparation such as making a risk analysis. In any case, she and her team already know that they are seen as an important entity under the NIS2 directive and therefore have to deal with a duty of care and a reactive reporting obligation.

Obligations and implications

The NIS2 requires additional industries to adopt more extensive cybersecurity requirements, and important and essential entities to take measures to manage security risks. Among other things, they have to make backups, carry out risk analyses and are obliged to report incidents with a significant impact on the service. In order to keep the administrative burden low, the management of an organization will be responsible for compliance with the provisions of the NIS2 Directive.

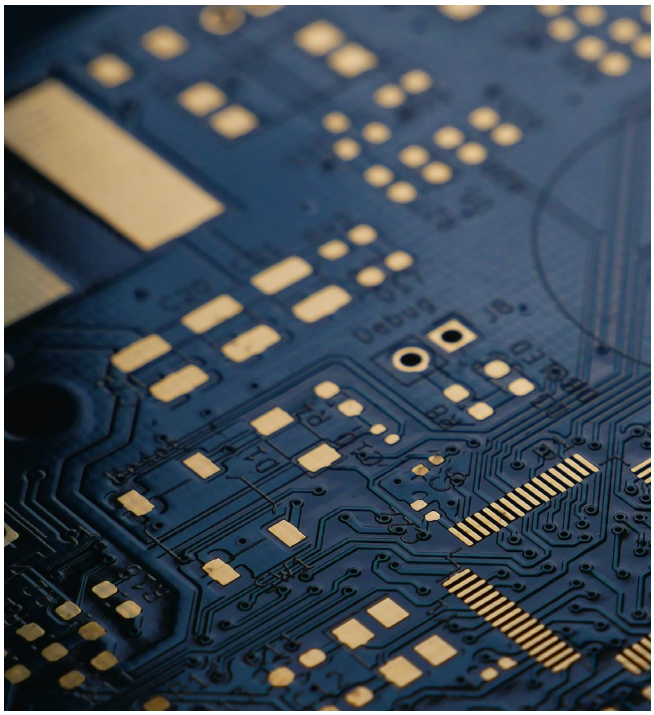
This new policy represents a big step for many organizations, large or small. Both the government and organizations will have to bear more responsibility. This also has financial consequences: the ICT budget of companies that are not yet covered by the directive expects to increase by a maximum of 22% and for companies that are already covered by the directive, up to a maximum of 12%. The administrative burden will also increase. Whether this additional ICT expenditure will be rewarding and give companies competitive advantages due to the higher level of cybersecurity remains to be seen.

The NIS2 Directive is expected to lead not only to stricter enforcement and obligations, but also to a safer digital economy in the European Union and protection against cyberattacks.

What will the NIS2 mean for your organization?

As discussed earlier, the NIS2 directive will distinguish between two categories; essential and important entities, where previously only a distinction was made between vital organizations that were covered by the NIS and non-vital organizations. All sectors and organizations that will fall under NIS2 are of great importance to society. It would cause major problems for society if these organizations could no longer fulfill their role.

Cyberattacks can have a major impact, not only on organizations, but also on society. Some examples of major attacks are the spread of NotPetya ransomware in 2017, in which, among other things, the Port of Rotterdam came to a standstill and the ransomware attacks on De Mandemakers Groep and VDL in which business operations were seriously affected. Another example is the attack on Bakker Logistiek, which left supermarkets without cheese for days. And in an attack on software vendor Kaseya 2021, thousands of companies were hit by cybercriminals gaining access to their systems through the hacked IT management software.



The two categories were created because not all sectors on the same scale would have an impact on society in the event of an incident. Below we explain the difference between the two groups – essential and important – and what the influence of this is on what changes NIS2 will bring about.

Duty of care and reporting

All organizations that fall under NIS2 – essential or important – will have to comply with their duty of care. The Directive contains a list of types of measures that providers must comply with as a minimum.

Examples include:

- policies on risk analysis and information system security
- attention to crisis management and operational continuity in the event of a major cyber incident
- ensuring supply chain security
- duty of care to ensure security of network and information systems
- use of cryptography and encryption
- policies and procedures for assessing the effectiveness of risk management measures

The European Commission reserves the right to further specify measures by means of delegated and implementing decisions and to extend them with additional measures. Member States may then be given the scope to impose specific measures, taking into account national and sectoral circumstances. The reporting obligation will also apply to all organizations that fall under the NIS2. This reporting obligation means that affected organizations must report the incident to the designated authority within 24 hours of becoming aware of the incident, followed by a final report within one month.

Important

As in the case of **Waste2Resource**

Medium organizations active in one of the 11 '*very critical sectors*' or medium and large organizations active in one of the 7 '*critical sectors*'

Essential

As in the case of **BrightEnergies**

Large organisations active in the '*very critical sectors*'

Duty of care

- maintaining a basic level of digital hygiene and implementing cybersecurity education
- risk assessment for security of information systems
- attention to crisis management and operational continuity in the event of a major cyber incident
- ensuring supply chain security
- duty of care to ensure security of network and information systems, including responding and communicating vulnerabilities
- ensuring human resources security, access policies and securing digital assets
- use of cryptography and encryption
- entering or applying multifactor authentication and/or secure internal communication
- policies and procedures for assessing the effectiveness of risk management measures

Reactive monitoring (after incident)

Proactive monitoring (even outside of incidents)

Reporting obligation (in 3 phases)

- early warning within 24 hours
- incident notification within 72 hours
- final report after one month (or progress report in case of ongoing incident)

Administration fine for failure to comply with the duty of care or reporting:

- a maximum fine of at least **7,000,000** euros
- or **at least 1.4%** of global annual revenue in the prior financial year; depending on which amount is higher

Administration fine for failure to comply with the duty of care or reporting:

- a maximum fine of at least **10,000,000** euros
- or **at least 2%** of global annual revenue in the prior financial year; depending on which amount is higher

In addition, permits can be temporarily suspended or a natural person, such as the CEO, can be temporarily suspended.

Monitoring

Where the two categories will differ is the way in which it is monitored whether the organizations comply with the imposed requirements. For sectors and organizations that are labeled as essential, proactively monitoring will be carried out to see if they meet the requirements. There will therefore be active monitoring and the consequences of mismanagement will therefore be able to apply without an incident having taken place.

In the second category, important entities, checking compliance with the law will take place in a reactive manner. This means that these organizations will only be checked for compliance with the legislation and requirements after an incident. If it turns out afterwards that not enough action has been taken and the requirements have not been met, the same sanctions can follow as for essential entities.

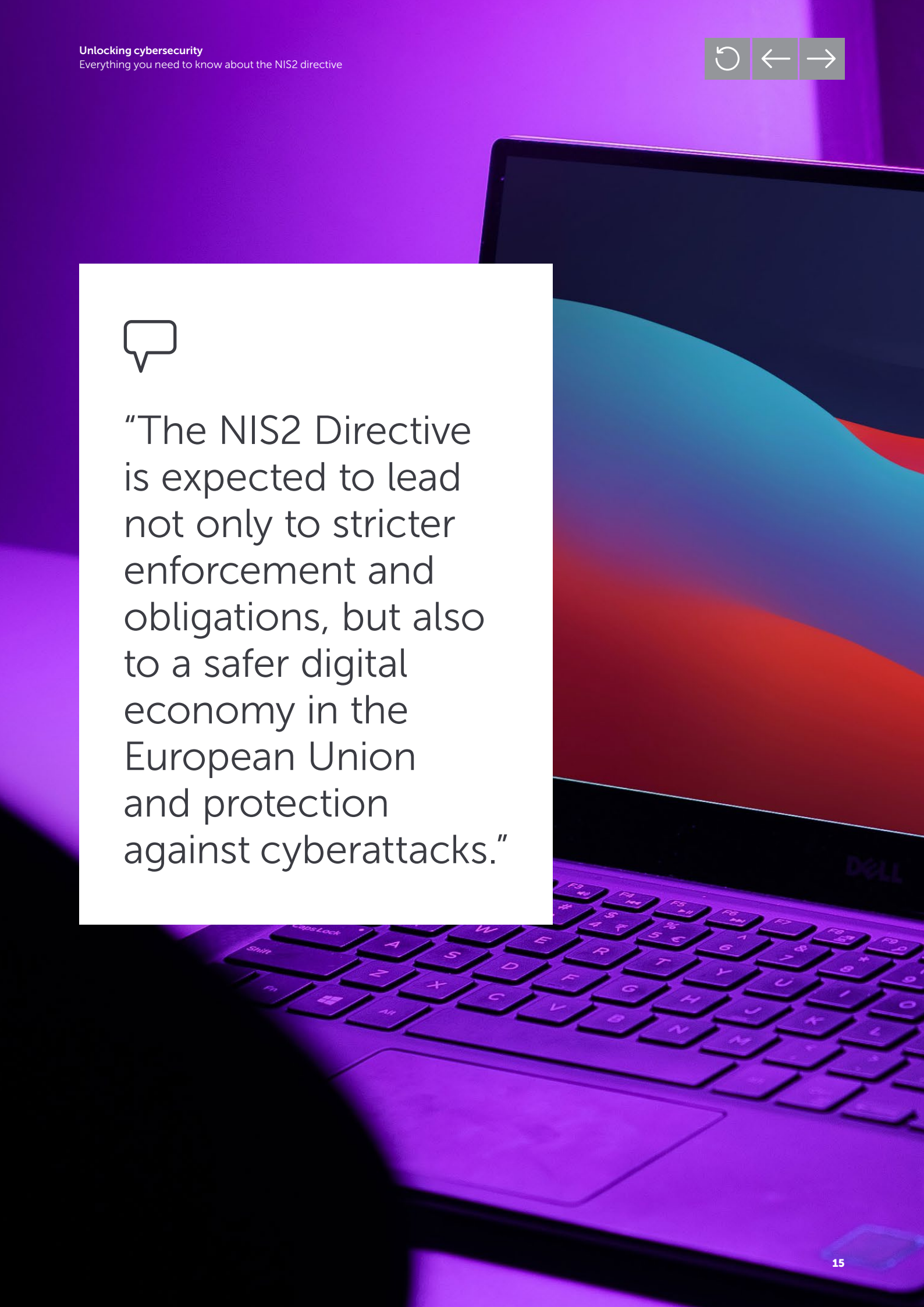
Back to our use cases:

BRIGHTENERGIES
ENERGY COMPANY

Energy company BrightEnergies is therefore actively preparing for the upcoming enforcement, because it is an essential entity. Lennard has called the security and compliance teams together to discuss this topic. Even more than at the time of the first NIS Directive, it is emphasized internally that compliance with the new cybersecurity legislation is of great importance and working groups are set up to steer this in the right direction.

WASTE2RESOURCE

Waste processor and recycling company Waste2Resource has to deal with reactive enforcement, only after an incident will it be checked whether they meet all the requirements of the NIS2. The company wants to arrange everything as well as possible and Kayleigh decides to document everything, proactive or reactive enforcement makes little difference to her: "As long as everything is well arranged at the outset!"



"The NIS2 Directive is expected to lead not only to stricter enforcement and obligations, but also to a safer digital economy in the European Union and protection against cyberattacks."

Reporting

Three-stage reporting

The NIS2 directive provides for a 'three-stage approach' for reporting incidents. The 'early warning' within 24 hours aims to limit the potential spread of incidents and to allow entities to seek support. The 'incident notification' within 72 hours must include an initial assessment of the significant incident, indicating its severity and impact and indicators of compromise. The final report – after one month – must ensure that lessons can be learned from previous incidents. This approach aims to gradually improve the resilience of individual entities and entire sectors to cyber threats. Apart from the obligation to submit the early warning, the focus on the incident notification is in the handling of incidents.

Early warning

Without undue delay and in any case within 24 hours of becoming aware of the significant incident, an early warning to the competent supervisory authority. In this warning, it must be indicated whether the incident was caused by an unlawful or malicious act or could have a cross-border impact. This is the strictly necessary information. Within 24 hours of the submission of this warning, the reporting entity shall receive a response with initial feedback from the competent supervisory authority or the CSIRT. If the entity so requests, guidance on the implementation of possible mitigation measures and possibly additional technical support may be received. In the event of an incident of a criminal nature, the entity shall also receive guidance on how to report the incident to law enforcement authorities.

Incident notification

Without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, must update the information provided with the early warning and indicate an (i) initial assessment of the significant incident, (ii) including its severity and impact, as well as, where available, (iii) the indicators of compromise.

Final report

Finally, within one month of the submission of the incident notification, a final report will be submitted containing (i) a detailed description of the incident, its severity and impact, (ii) the type of threat or root cause likely to have triggered the incident, (iii) applied and ongoing mitigation measures and (iv) cross-border impact of the incident. In justified cases and in consultation with the competent supervisory authority, the 24-hour period for the incident notification and a one-month period of the report may be derogated from.

Case study examples:

BRIGHTENERGIES
ENERGY COMPANY

It's a crisis at BrightEnergies. An attacker has entered the network, no one knows how that was possible and what had to be done at that time. And then the CISO cannot be reached! Everyone is in turmoil and IT specialist Menno is taking the reins as a replacement. He sends an early warning to the RDI within 24 hours. Together with an external party, the company's backups are searched for diligently. These are found and the organization knows how to prevent worse consequences, because they have access to their important data. Nevertheless, the company has been down for a number of days, with all the consequences that entails. A month after the incident, a detailed description, mitigation measures and the root cause will be reported in a final report. The fact that everything was not so well organized in the field of security was a big eye-opener for director Lennard. This crisis has serious consequences for BrightEnergies.

WASTE2RESOURCE

Waste2Resource is facing a ransomware attack, just like its competitor in 2021. Thanks to the processes that CISO Kayleigh wanted to have documented, the IT team can quickly restore a recent backup. Just under 24 hours later, the organization is up and running again. Thanks to the efforts to comply with the requirements of NIS2, the damage is not too bad. Kayleigh has forgotten only one thing, the early warning. Fortunately, one of her teammates just alerted her at the last minute that the early warning must be made within 24 hours. "Don't forget to schedule the updated and final notification!" says Kayleighs's colleague before she goes home.

Significant cyber threats

Tighter rules have been established for reporting incidents with major consequences in the NIS2 directive. Organizations should also report any significant cyber threat they encounter that could lead to a significant incident. With regard to the concept of cybersecurity, NIS2 is in line with the European Union's definition of cybersecurity and certification of IT. An incident is considered significant if it results in significant operational disruption or financial losses for the organization or if it could cause significant material or immaterial damage to individuals or organizations.

Voluntary notifications

Organizations outside the scope of the NIS2 Directive can voluntarily report significant incidents, cyber threats or near-incidents. The supervisory authority follows the reporting procedure. No additional obligations should be imposed in the case of voluntary notifications.

Scope of obligations

The European Commission can provide further guidance on the information, format and reporting process for both high-impact incidents and cyber threats. The scope of the obligations can therefore be extended.

Fines and penalties

The duty of care and the reporting obligation also bring a form of enforcement to ensure effective compliance with the rules. Authorities will have various supervisory measures and resources at their disposal for this purpose.

Cybersecurity and resilience is being made a boardroom issue by NIS2. In addition to common enforcement modalities - including fines, penalties and the public shaming effect - personal liability and suspension of directors is at stake. The days of ignorance and delegating away is over.

Minimum sanctions

The NIS2 Directive contains a mandatory list of sanctions, including on-site inspections, security audits, security scans, requests for information and requests for access to data. Some sanctions are the same for all countries, others are not, such as sanctions for serious violations. In such cases, the countries themselves must ensure effective, proportionate and dissuasive sanctions. The type of sanction (criminal or administrative) is also determined by the country itself. Penalties should be appropriate to the seriousness and nature of the infringement and should take into account factors such as the damage caused, cooperation with the competent authority and other circumstances.

Administrative fines

Instead of, or in addition to the other measures, administrative fines may be imposed, depending on the circumstances of the case. The same elements as the other sanctions should be taken into account when imposing an administrative fine. Infringements can be punished with administrative fines of up to 10 million euros or 2% of the company's annual worldwide turnover, whichever is higher. Local supervisory authorities must develop their own policies for imposing fines.

Our use cases:

BRIGHTENERGIES
ENERGY COMPANY

BrightEnergies faces sanctions after the ransomware attack. As an essential entity, they are obliged to have state of the art security. The CISO is suspended and a hefty fine follows. Director Lennard concludes that security is now top priority for IT teams and wants to implement advanced security solutions to proactively prevent attacks.

WASTE2RESOURCE

Fortunately, Waste2Resource avoids the clean sanctions. The incident has opened Kayleigh's eyes, she goes to the CEO and points out that with a little more budget she thinks she can secure the organization even better. Although the CEO recognizes the seriousness, he is already quite satisfied, "we meet the requirements neatly, don't we?", Kayleigh gets a slightly increased budget to help bolster security further.

Together for a resilient future

Furthermore, the NIS2 will ensure that a European Cyber Crises Liaison Organization Network (EU-CyCLONe) is established to provide support and coordination in the event of a large-scale cyber-attack in the EU. Experts will also insist on working together and learning from each other between member states in order to hand out tips and increase mutual trust.

Need help with the implementation of NIS2?

EVERSHEDS SUTHERLAND

This is what ESET in the Netherlands can do for your organization

As a European supplier in the field of digital security solutions, we are happy to think along with you and help you with the issues you have with regard to the NIS2 or its implementation.

Possibilities we offer in the field of NIS2:

- knowledge sharing through our channels such as the Digital Security Guide or our corporate blog
- interactive sessions such as workshops
- thinking along with regard to compliance and implementing NIS2 measures
- providing security solutions that contribute to compliance
- our specialists are always available to answer your questions

This is what Eversheds Sutherland can do for your organization

As a global top 10 law practice, Eversheds Sutherland provides legal advice and solutions to an international client base which includes some of the world's largest multinationals. Our highly-integrated, interdisciplinary and deeply collaborative privacy team provides comprehensive, business-focused and time sensitive advice in one of the most rapidly evolving areas of the law.

We can help you interpret how NIS2 will impact your business and implement pragmatic strategies for compliance. We find innovative ways to simplify complexity, bring greater administrative ease, and future-proof your business.

Should a cyberattack occur, our team has a long history of supporting global clients with their compliance projects and incident response. Our unique project management system allows us to deliver complex, multinational legal services through clear and simple contact points.

Key contacts

Astrid Oosenbrug
Public Affairs Officer, ESET Netherlands

M: +316 25 129 947
astrid.oosenbrug
@eset.nl

Olaf van Haperen
Partner, Eversheds Sutherland

M: +316 17 456 299
olafvanhaperen
@eversheds-sutherland.com

Robbert Santifort
Principal Associate, Eversheds Sutherland

M: +316 81 880 472
robbertsantifort
@eversheds-sutherland.com

Sources

https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN

https://www.europarl.europa.eu/news/nl/press-room/20221107IPR49608/cyberbeveiliging-parlement-neemt-nieuwe-wet-aan-om-veerkracht-eu-te-versterken

eversheds-sutherland.com

DTUK004603_06/23