Presentatie NISDUC

Wacht niet op de implementatie van de NIS2 met het nemen van maatregelen, maar kijk wat je nu al kunt doen. Met die boodschap en het benoemen van de toolkits die al voorhanden zijn, opende Hester Somsen, directeur cybersecurity en plaatsvervangend NCTV, de tweede dag van de NISDUC.

Tijdens dit internationale congres over de Europese richtlijn NIS2 kwamen organisaties en bedrijven samen om zich voor te bereiden op de nieuwe wetgeving voor cyberveiligheid. Volgens Hester Somsen is de dreiging inmiddels zo groot dat cyberweerbaarheid niet langer het domein van de IT'ers is, het is *boardroom material* geworden. Haar Engelstalige presentatie is hieronder terug te lezen.

Het gesproken woord geldt | The spoken word applies

[NCTV: Comprehensive approach to national security]

National security is about protecting our country, our democracy and our people. The NCTV serves the Netherlands' national security.

In a complex, changing and ever more digitalised world, the Netherlands is vulnerable to threats. Cyberattacks, foreign interference, terrorism, pandemics – these are all threats to our national security that manifest themselves in many ways, threats the country must be protected from.

National security is a dynamic, multifaceted concept, which demands a robust and flexible approach. Our National Security Strategy sets out the national security interests that must be protected, explains how those interests are currently under threat and specifies what we can do to address these risks and threats. And Cybersecurity is a key element of national security.

The Cyber Security department at the NCTV has the following responsibilities. We boost the Netherlands' resilience to cyber threats and coordinate activities of the government and partners in critical sectors: the National Cybersecurity Strategy and NIS2. We provide the policy and the legal and budgetary framework for the National Cyber Security Centre. And to conclude we are responsible for the system in which parties can work on their own digital resilience - expertise, knowledge and analysis, combined with the public-private network.

[The digital threat for the Netherlands remains as high as ever and changes continuously]

As my minister explained yesterday: We're facing a severe cyberthreat – just look at the most recent edition of the Netherlands' National Cybersecurity Assessment.

This threat comes from a variety of sources. State actors are looking to steal knowledge and technology, and we see pre-position for sabotage as a hight threat. Cyber tools are cheap, easy to conceal and capable of generating large proceeds. As a trend we see that they focus less on primary targets, such as high-tech companies, than on supply chains and the wider ecosystem in which relevant organisations operate. 'Weak links' can serve as a springboard to more interesting targets.

The impact of cyber criminals we can see every day in the media. Recently the Nijmegen chipmaker Nexperia fell victim to an extortion attack: criminals threatened to reveal trade secrets, chip designs and customer data unless a ransom was paid. I wouldn't want to embarrass anyone here, but it's an important point: this isn't a fictional scenario; these kinds of attacks are the order of the day, and preventing them should be your highest priority.

The subsequent damage can be substantial. For the companies affected: damage to their reputation and financial consequences. For those companies' customers: having their data end up in the wrong hands. For national security: in terms of disruptions to vital services. And for the trust of our citizens in our digitalized society.

In short, cybersecurity is no longer the sole domain of the IT crowd; it's boardroom material.

[The Netherlands' Cybersecurity Strategy]

Fortunately, we haven't been letting the grass grow under our feet in the Netherlands. In recent years government has been hard at work, further strengthening the cybersecurity system and boosting the digital resilience of our society, our economy, our vital interests. These measures are guided by the Netherlands' Cybersecurity Strategy. Let me offer a few real-life examples:

- Cyber resilience network
  The current nationwide system is mostly focussed on information sharing. We want to develop that into a network that can reach as many organisations as possible within the Netherlands, with a view to fostering digital resilience.

The network's role is being broadened: from sharing threat information to notifying targets and victims, responding to incidents, sharing knowledge, offering training courses, and staging exercises.
The type of organisation that can participate has been expanded: we are looking at industry organisations, cooperative ventures and suppliers. With more varied partners we can reach a larger target audience by way of public-private partnerships.
Well-established organisations are being given more responsibility within the network, so that bigger entities can help smaller ones.

- Single Cyber Organisation
  Public-private partnership is the core of this cyber resilience network. We do that by merging the NCSC, the Digital Trust Center (DTC) and CSIRT-DSP (for digital service providers) into a single new national cybersecurity organisation: we are creating a one-stop shop where all organisations in the Netherlands can go for cybersecurity advice and assistance following a cyber incident.

- Active Cyber Protection
  Programme Cyclotron is a public-private partnership between government, companies and civil society organisations. This cooperation leads to a platform where public and private parties share information on digital incidents and threats. In this way, programme Cyclotron helps make the Netherlands an unattractive target for digital attacks. Sharing information is needed to improve cyber resilience and reduce the cyber threat.

  The starting point for the design of the Cyclotron platform is the observation that the informational needs that users have are directly proportional to their maturity. The following two needs emerged from the analysis of the landscape. First, high-maturity organisations need to receive unanalysed raw data quickly. Second, all organisations need analysed information. The analyses in question could be carried out jointly. These information needs then translates into four purposes for information sharing: a) to share raw data quickly, b) to request information, c) to analyse information together, d) to distribute these analysis and threat intel in an way so that low and medium mature organisations can act on it.

[Cybersecurity in Europe has been – rightfully so – made a top priority]

Given the severe cyber threat the EU's NIS2 Directive is a pure necessity. The message isn't new, but at this point the interests at stake are so

great that we can no longer depend on organisations to take action voluntarily.

NIS2 doesn't stand on its own. There are additional laws in the pipeline that deal with other aspects of cybersecurity: Cyber Security Act, Cyber Resilience Act, Cyber Solidarity Act, Act on cybersecurity of EU institutions, bodies and agencies.

So cybersecurity in Europe has been – rightfully so – made a top priority. Many policies, directives and acts that strive to strengthen the EU's cyber posture have been introduced.

These efforts are crucial to ensure the cybersecurity of the Union. It is now time to focus on implementation, where Member States, the Commission and the EU agencies work hand-in-hand towards tangible results. And of course the entities that fall under NIS2.

The primary goal of the Commission should be: evolution rather than revolution - fully consolidate ongoing efforts, create necessary preconditions and incentives to support Member States to effectively implement the future-proof cyber legislation, and reduce complexity of and overlap within the EU cyber landscape. Due account should be given to this principal as part of impact assessments. Key is the focus on implementation, harmonisation and innovation.

Government is responsible for the system and for providing information and guidelines so that organisations can take appropriate measures. Obviously, we'd prefer to have everything ready by now: if this is all so important, why are the new laws so slow in coming? At least that holds for the Netherlands.

The answer is as concise as it is frustrating: because it's so complex. Many ministries, implementing organisations, supervisory authorities and organisations will fall under the NIS2 Act. The substance of the law is complex, as are the sheer variety of legal and policy-related choices that have to be made. This will have a major impact on Dutch organisations.

On the one hand we have to move forward with great care. On the other hand it's regrettable that the implementation is delayed. And yet there is already a lot we and you, everyone, can do.

[It is now time to focus on implementation]

Our online consultation for the Dutch legislation is expected to start in mid-May.

The draft bills will be ready by then, and you'll get a chance to see what is expected of you. And to respond and provide us with your comments. The received responses will be carefully studied and assessed, and in some cases incorporated into the final text of the law. We expect that to be ready in October.

As in the whole of the EU the following elements will be present:

- A duty of care – entities will be required to carry out a risk assessment. On that basis they will take appropriate measures to safeguard their services and protect their network and information systems to the greatest possible extent.

- A registration requirement – entities covered by the NIS2 Directive will be required to register themselves. Among other things, this registration requirement is meant to ensure that we have a Europe-wide overview of the number of entities that fall under NIS2. This will be done through the NCSC, which is currently designing a 'My NCSC' portal for this purpose. We will have a minimum viable product ready in autumn.

- A reporting requirement – entities must report incidents to the supervisory authority within 24 hours. Specifically, I'm referring to incidents that could disrupt the provision of essential services. Cyber incidents must also be reported to the CSIRT, which can then provide help and assistance. There are various factors that determine whether an incident should be reported: the number of people affected, its duration and the possible financial losses.

- Supervision – organisations covered by NIS2 will be subject to supervision. This means the authorities have to verify compliance with the obligations set down in the directive, such as the duty of care and the reporting requirement. Currently, in The Netherlands decisions are being made about which sectors fall under which supervisory authorities.

Needless to say, government itself is also obliged to obey the new law.

[Don't wait, act now]

In the Netherlands we're trying to make it as easy as possible for companies and organisations that fall under NIS2. We're doing this in a variety of ways: 1) offering tools, 2) sectoral information-sharing and analysis centres are now looking into who needs what in order to comply with the law, 3) Private-sector initiatives that we welcome. Private parties

that understand what's needed to streamline their cybersecurity, such as ASML's cyber rating tool, which has been embraced by the CISO Circle of Trust. It gives guidelines for mapping out what you should expect from suppliers in order to be resilient to digital risks; an excellent tool which is already available.

This is not the only instrument you can use: there is already a lot available on the websites of the NCSC, the DTC and the Dutch Authority for Digital Infrastructure (RDI). So I'd advise you not to wait for the draft bills before getting started. After all, the risks facing organisations and systems are already very much present.

Organisations that are already taking action are not only protecting themselves from these existing risks; they will also be better prepared when the new law enters into force.

Make use of the tools that are now available.

- Conduct a risk analysis and assessment of the physical and digital risks that could disrupt your organisation's operations. Identify your organisation's 'crown jewels' that require protection. Determine the physical and digital risks that are relevant to your organisation because they could disrupt the continuity of your operations, and what measures have already been taken.

- Take steps to strengthen your organisation's resilience or better protect your organisation from these risks. By drafting business continuity plans and crisis management protocols. Expand staff awareness; the DTC has a lot of tips and material about how to do this on its website. Most cyber incidents are the result of human error. Cyber criminals are skilled at exploiting the gullibility and laziness we'll all guilty of from time to time. So get to work, make this a key part of your operational management, from on-boarding to exit interview and everything in between.

- Ensure that you have procedures in place that enable your organisation to detect, monitor and resolve incidents that can disrupt normal operations. If your organisation is covered by the new law, you're required to report any incidents. Factors that determine whether an incident must be reported include duration and the number of people affected. The measures associated with the reporting requirement must be incorporated into your business process. Drawing up an incident response plan can help in this regard.

- Finally, educate yourself. Under NIS2, senior managers need to take cybersecurity risk-management measures. Your organisation's leadership must exercise the required duty of care, and it bears administrative responsibility for doing so. This is why it's necessary for senior management to have sufficient knowledge and skills to establish a strong culture of cyber resilience. NIS2 requires senior managers to take a training course on this subject. This is another thing you can get a head start on, and by doing so, you set a good example for your staff to get the training they need.

NIS2 aims to boost cyber resilience across Europe in a uniform way. Despite that, not every country is going to implement the directive in exactly the same way.

At some point we'll need to come together and consider the different approaches in order to see whether the directive works and whether we're all more or less on the same page.

It may be necessary to take further steps to ensure that the requirements for cyber resilience are equally clear everywhere and equally robust. But that's a matter for the future, and we have now urgent tasks before us. Nevertheless, I'm curious if we'll get a sense of what awaits us in that regard today.

As you can see, government doesn't know everything. But even if the result isn't yet 100% clear, it shouldn't stop us from doing our best to ensure that the right steps are taken to implement NIS2.

The interests at stake are simply too great.

Thank you.