Informatie-uitwisseling landelijk dekkend stelsel cybersecurity

Management Summary

Projectnummer:
2019.151

Publicatienummer
2019.151-2008

Datum:
Utrecht, 4 november 2020

Auteurs:
ir. ing. Reg Brennenraedts, MBA
prof. dr. Rudi Bekkers
Jessica Kats, MSc.
mr. drs. Melvin Hanswijk
Roma Bakhyshov, MSc.
ir. Wazir Sahebali
Roos Jansen, MSc.

© 2020 WODC. Auteursrechten voorbehouden.

Management Summary

Our society is increasingly dependent on information and telecommunication technology (ICT), and is therefore also increasingly vulnerable to threats in the field of cyber security. Dutch intelligence and security services, the National Coordinator for Security and Counter-terrorism (NCTV), the National Cyber Security Centre (NCSC) and the police are signaling a worrying increase in digital threats. Moreover, the capabilities lag behind the development of the threat.

The Netherlands recognizes this vulnerability: the first ambition in the Dutch Cyber Security Agenda (NCSA) is: *'The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats.*[1] One of the objectives in this regard is: *"A nationwide system of cybersecurity partnerships will be created in which information about cybersecurity can be shared between public and private parties more widely, efficiently and effectively. The aim of this nationwide network is to strengthen the capabilities of public and private parties".*[2]

The choice of the Netherlands for a decentralized design comes with the risk that the government has less insight into the scope of information about digital security. This lack of insight mainly affects the non-critical parties. At the Ministry of Justice and Security, the question is therefore currently whether information about cyber security can be shared more widely, more efficiently[3] and more effectively between public and private parties, and what can still be done to achieve a nationwide cyber security network.

In this study we use the following starting point with regard to the nationwide network of cybersecurity partnerships: the ideal of a nationwide network is realized when every party in the Netherlands is 'reached' and has access to the cybersecurity information he needs. Parties are 'reached' by the system if they know where to turn to in case of questions or problems with cybersecurity.

The underlying research aims to provide insights into the problem that has just been posed, and has the following overarching research question: *Which target groups with regard to the non-critical parties are not yet reached, in what way - and via which departments - would this be possible, and what needs to be done concretely to achieve this?*

A number of different research methods were used to answer the overarching question and sub-questions: document and data analysis, interviews with experts and other involved parties, data collection from target groups (interviews, survey), and a country comparison. Subsequently, through an integrated analysis, all the collected information was brought together and the research questions were answered.

How different parties define cybersecurity and its different aspects

Because this is a relatively young and dynamic domain, many different definitions of cyber security are used by the various parties. Not only the term 'cyber security', but also similar concepts or descriptions occur. The main similarities between definitions is the focus on digital resilience, measures and national/digital security. The differences are in the scope of the

[1] National Cyber Security Agenda (NCSA), p. 17.

[2] National Cyber Security Agenda (NCSA), p. 20.

[3] Efficiently in terms of organization, not in financial terms.

term; CBS, for example, maintains the definition of the CSBN, but provides additional context. Many parties do not comment at all on the definition of cyber security; they indicate what you can do (or what they can do for you) to be cyber secure, but they do not specify what this means. A distinction between government, private critical and non-critical parties is not clearly visible.

The definition of cyber security in Cyber Security Assessment Netherlands (CSBN) 2020[4] is adopted by the Dutch government and reads: *"Cyber security is the set of measures to prevent damage caused by disruption, failure or misuse of ICT and, if damage does occur, to repair it. Such damage may consist of compromising the availability, confidentiality or integrity of information systems and information services and the information stored therein."*[5]

The objectives of the Dutch cabinet with regard to cyber security

The objective in the National Cyber Security Agenda (NCSA) is formulated as follows: "*The Netherlands is capable of capitalizing on the economic and social opportunities of digitalisation in a secure way and of protecting national security in the digital domain.*"[6]

The NCSA comprises seven ambitions:[7]

1. The Netherlands has adequate digital capabilities to detect, mitigate and respond decisively to cyber threats.
2. The Netherlands contributes to international peace and security in the digital domain.
3. The Netherlands is at the forefront of digitally secure hardware and software.
4. The Netherlands has resilient digital processes and a robust infrastructure.
5. The Netherlands has successful barriers against cybercrime.
6. The Netherlands leads the way in the field of cybersecurity knowledge development.
7. The Netherlands has an integrated and strong public-private approach to cybersecurity.

These ambitions apply to the Netherlands as a whole, with public-private partnerships as a starting point. Vital sectors fall under the Ministry of Justice and Security and the line ministries, where structural and adaptive risk management are the primary focus. Non-vital sectors fall under the Ministry of Economic Affairs and Climate Policy. Under this Ministry,, the Digital Trust Center (DTC) was established in 2018, an information hub for the non-vital business community.

The current structure of the Dutch cyber security policy

The Dutch system can best be described as a decentralized and dynamic system. It is decentralized because it has different parties for reaching the central government and private, vital parties (including the NCSC) and for reaching non-vital parties (including the DTC), and then makes use of partnerships, which play a major role in the actual dissemination of information. In essence, this is a network approach, visually represented in Figure 5 in paragraph 3.1.1. The Dutch system is also dynamic because the collaborations are constantly evolving: new ones are added regularly or their composition and scope changes.

[4] The Cyber Security Assessment Netherlands (CSBN) provides insight into threats, interests and resilience in the field of cyber security in relation to national security. The CSBN is established annually by the National Coordinator for Security and Counterterrorism (NCTV).

[5] CSBN 2020, p. 48.

[6] National Cyber Security Agenda (NCSA), p. 17.

[7] National Cyber Security Agenda (NCSA), p. 17.

Information exchange in the Dutch cybersecurity system, and possible limitations therein

Two types of information are central to the exchange of information between the parties, namely general educational information and threat information, and due to differences in the nature of these categories, they are subject to different legal regimes. It is this legal component in particular that determines the space for information to be shared. Especially the sharing of threat information with non-vital parties is currently limited, partly due to limitations imposed by the GDPR. The possibilities for data exchange partly depend on the institutional setting, where adjustments can be made if necessary (see below), but it is also partly a matter of legal interpretation (e.g. when it comes to the legal task of the DTC and the possibilities it offers within the GDPR or the question of how to deal with the necessity test required by the GDPR when a partnership cannot provide IP addresses of its members; how broadly the concept of 'confidential information' in the Wbni should be interpreted and what the legislator's intentions were regarding the restrictions on sharing it). It is beyond the scope of this research to judge the different views on the correct legal interpretations. However, as a result of the ongoing discussion, we do expect that in the short or medium term more consensus will emerge about the (im)possibilities of information sharing in the current setting. The same applies to the possibilities that may arise following adjustments in the institutional environment, such as strengthening the legal basis of the DTC within the framework of the GDPR. If necessary, follow-up research could address these legal questions more specifically.

Information needs of target groups of non-vital companies, and the extent to which the current Dutch system reaches these target groups

Based on the data we have gathered, see Figure 1, we conclude that:

- ZZP'ers (self-employed people with no personnel) are a diverse target group in terms of both their knowledge about cybersecurity and their need for (more) such knowledge. There are self-employed people with a very clear need for information about cybersecurity (which they want to receive through multiple channels), such as a basic scan of their cybersecurity, benchmarking (how good is their cybersecurity compared to that of others?), and concrete prospects for action. According to them, this need is currently only met to a very limited extent (and, if so, by parties who have a self-interest and where the neutrality of the information may be in question). Remarkably, the DTC is already able to meet a large part of this need. However, this category of companies is hardly ever reached by the DTC.
- A large part of SMEs do not need more information about cyber security. The 16% who indicated in the telephone survey that they do have a need for this, have wishes that largely correspond with those of the aforementioned self-employed persons. They mainly need general cybersecurity information, preferably by e-mail, a way to test if their security is in order and a reliable source where they can find information.
- Companies that purchase security services from ICT suppliers have a much more limited demand. They trust that these suppliers have taken appropriate measures and that in case of calamities, these suppliers can help them effectively.
- Specialized IT companies, including IT suppliers, network managers, internet service providers (ISPs) and managed service providers (MSPs) also have a clear information need. Although this need is already partly fulfilled by public and private sources (hotlines set up by the market, the American Common Vulnerabilities and Exposures

(CVE) database,[8] etc.), there is still a clear need for (additional) threat information in the Dutch context, as currently available within the NCSC.

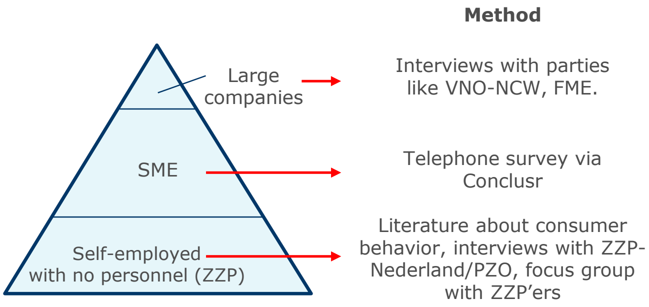
Method
Large companies
SME
Self-employed with no personnel (ZZP)
Interviews with parties like VNO-NCW, FME.
Telephone survey via Conclusr
Literature about consumer behavior, interviews with ZZP-Nederland/PZO, focus group with ZZP'ers

Figure 1. Method of approach per target group.

In addition to the above, our research revealed that there is a very specific theme where knowledge is lacking, namely that of Operational Technology (OT). This concerns the use of hardware and software to control physical processes, devices and infrastructure, and includes industrial Internet of Things (IoT) and critical infrastructures. This is an area in which, for historical reasons, security is often still inadequate, but in which the threat has greatly increased. This results in an as of yet poorly filled demand for knowledge.

Opportunities to better reach target groups and better fulfill information needs

Based on our research, we distinguish a number of different routes that, separately or in combination with each other, could strengthen the Dutch cyber security system and promote information exchange, thus helping to achieve the objectives of the Dutch policy. These routes are as follows:

1. *Towards a (known) central information desk for SMEs and ZZPs*
2. *Distribute residual information from NCSC via DTC to the partnerships;*
3. *Distribute NCSC's residual information through other parties;*
4. *Increase the number of Computer Emergency Response Teams among non-vital cybermature companies;*
5. *Identify more companies as critical, or reconsider the critical/non critical split;*
6. *A single back office for both NCSC and DTC.*

How the routes relate to the Market and Government Act (Wet Markt en Overheid) and the Network and Information Systems Security Act (Wet beveiliging netwerk- en informatiesystemen)

The only route in which distortion of competition could potentially play a role is route 2, in which residual information from the NCSC is passed on via the DTC to the joint ventures and non-vital companies. The Market and Government Act will then become relevant, because parties will be offered information free of charge that is comparable to information that the parties might be able to purchase from commercial parties. The information will, however, consist of data obtained by the DTC in the exercise of its powers under public law (arising from the bill that is discussed as part of route 2). For such data, the Market and Government Act provides for an exception to the code of conduct that the costs of goods and services

[8] The CVE database is maintained by MITRE Corporation and is funded by the National Cyber Security Division of the U.S. Department of Homeland Security.

must be passed on in full. As a result, this solution will not conflict with the Market and Government Act.

The Network and Information Systems Security Act (Wbni) indicates with whom the NCSC may share threat information with personal data, by formulating legal tasks that serve as a basis within the meaning of the GDPR, and indicates with whom the NCSC may share traceable confidential data. A number of times it has been indicated that an amendment to the Wbni would remove certain barriers, but this is not really required for any solution. The main step to be taken from the Wbni is the designation of the DTC as OKTT, within the framework of route 2. An OKTT ("Objectief Kenbaar Tot Taak") is an organization that objectively has the task to provide other organizations or the public with threat information. The NCSC can, in cooperation with the NCTV, designate an organization as OKTT. The designation is an important step needed to enable the sharing of threat information. However, the designation of the DTC can only take place when the DTC has a legal basis to process personal data.

Systems of cybersecurity in other countries, and lessons for the Netherlands

This research looked at the cybersecurity system in England, France and Germany. Given the specific context in which different countries find themselves (e.g. legal framework, size of the economy, administrative classification, etc.) it is difficult to make a hard comparison. Evaluations of the centralist English system are positive, but with a budget (converted) of more than € 2 billion, the effort is not really comparable to that in the Netherlands. We did not always receive consistent input on the equally centralistic French system. Although France, for example, scores high in the Global Cybersecurity Index, the opinion of the interviewees about France is much more critical. The French GIP ACYMA (to a certain extent comparable to the Dutch DTC) does seem to be very successful in reaching small companies, partly by linking these companies to (private) ICT experts. The German cybersecurity system is partly decentralized, but that is mainly prompted by the federal system of governance. Sources indicate that there is fragmentation and unclear division of tasks between the departments involved, and that this situation makes cooperation in Germany more difficult.

Conclusion

Although the goal of a nationwide network is increasingly being achieved, there are still SMEs and self-employed people who are insufficiently aware of where to turn with questions or problems with cyber security. For example, only a small group is aware of the existence of the DTC, while at the same time many companies indicate a need for precisely those things the DTC offers, such as a basic scan. Also in a more general sense, a clear need has been expressed for a central and reliable party that provides companies with information regarding cybersecurity.

Sharing threat information is often problematic because of the legal restrictions on sharing personal data and traceable confidential information. As a result, threat information that is relevant to the non-vital sector remains 'stuck' at the NCSC. Not only are there legal obstacles to the sharing of threat information, practical and organizational problems also play a role. Some collaborations that may be designated as OKTT in the future may not yet be able to use the information they would like to receive, for example because their current systems and capacity do not allow them to send the right data to the right parties in their network, or cannot demonstrate that they can do so safely and GDPR-compliant. Ultimately, the group of non-vital cybermature companies in particular is currently not well served in terms of the desired information provision; this group has limited access to the information they deem necessary to be cyber resilient. For example, the NCSC has relevant threat information that the companies cannot obtain from other sources.

All identified solutions can contribute to the goal of making the Dutch cyber security system a nationwide network. Based on our research, a combination of the first three routes seems to be the most suitable way to achieve both improvement in the short term and the fullest possible coverage in the long term:

1. For the informational aspect of the system, large-scale marketing of the DTC as a central information desk for questions about cyber security can be used to improve the recognizability and findability of the DTC (route 1). In this way, the needs of companies with low cyber maturity, especially self-employed persons and small companies, can be met.

2. It would also make sense to use the DTC for the distribution of threat information (route 2). In time, the DTC can become the primary actor for threat information for the non-critical sector. This route potentially offers the most complete coverage, but it is expected to take some time before the necessary legal basis for the DTC is in place and the exchange of information can really start (early 2021 may be feasible, but a year later is not inconceivable).

3. In the meantime, and also afterwards, the distribution of threat information by existing and new OKTTs could be a solution (route 3). In particular, the idea of having OKTTs inform the NCSC of which organizations among their members have given permission to share traceable confidential information with the OKTT (see section 5.1.3) could improve the situation in a relatively short period of time, because it would make it easier to share information about the vulnerabilities of specific companies. This possibility has since been suggested to the NCSC, which will examine whether this is legally viable.

Recommendations

Based on this research we come to three recommendations:

1. Develop a communication strategy to meet the identified information needs of self-employed persons and SMEs (who do not purchase security services from ICT suppliers). Because this research shows that much of the information desired by these parties is already available through the DTC, but does not reach them, it is important to work on the familiarity and findability of the DTC.

2. Explore the proposed solutions 2 and 3, for better dissemination of threat information through the DTC and through partnerships, and discuss the feasibility with the parties involved. If necessary, further explore the interpretations of certain legal provisions, such as whether permission to share traceable confidential data can be given in advance and through another party, and to what extent data processing can be commenced by the DTC before the forthcoming bill is accepted.

3. Encourage cooperation between the central parties in the system, especially between the NCSC and the DTC. Parties not only need the authority to share information with each other, they also need to understand each other's target groups, goals and practices. To this end, they could engage in more dialogue with each other, possibly through periodic meetings in which problems and ambitions are discussed. Other information hubs, for example computer emergency response teams such as Z-CERT (healthcare) and SURFcert (education and research institutions), could also be involved.

Contact:

Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl