Towards a nationwide system of information exchanges

Advice on information sharing in the field of cyber security and cybercrime

CSR
Cyber Security Council
Cyber Security Raad

Towards a nationwide system of information exchanges

Advice on information sharing in the field of cyber security and cybercrime

Addressed to:
the Minister of Economic Affairs
the State Secretary for Security and Justice
the Commissioner of the National Police Force
the Board of Procurators General

the chair of VNO-NCW (The Confederation of Netherlands Industry and Employers)
the chair of MKB-Nederland (entrepreneurs' organisation for small and medium-sized businesses in the Netherlands)
the chair of Nederland ICT (the trade association for IT, telecom, internet and office companies in the Netherlands)
the chair of the CIO Platform Nederland (the independent community of persons with overall responsibility for digitalisation and/or ICT for private and public organisations in the Netherlands)
the chair of the Board of Directors of the Chamber of Commerce

CSR
Cyber Security Council
Cyber Security Raad

CSR advisory document 2017, No. 2

Ministers, chairs,

Digitalisation brings great economic and social opportunities. If we are to continue building on these opportunities, we need to be able to trust the digital world and to navigate it safely. Besides opportunities, digitalisation also involves threats, for instance in the realm of espionage and sabotage.[1] In order to combat such threats and ensure that the Netherlands is secure in digital terms, information sharing and collaboration between government bodies and between public and private parties is essential. In her report entitled 'The economic and social need for more cyber security – Keeping "dry feet" in the digital era'[2] Herna Verhagen calls for an effort to improve the sharing of information, for instance by expanding the Information Sharing and Analysis Centres (ISACs) and the National Detection Network (NDN). According to the recent report 'The Netherlands Cyber Readiness at a Glance'[3], information sharing is an important area of attention for this country, which scored lowest on the readiness index. Indeed, the theme is extremely urgent: having the right information at one's disposal in a timely manner is crucial to the digital resilience of organisations in both the public and private sectors. Digital resilience is one of the pillars of prosperity in the Netherlands.

Information position of the business community

The Cyber Security Council has found that the sharing of information about threat intelligence and action perspectives with the parts of the Dutch business community not designated as critical infrastructure is highly deficient. The current sharing of information is aimed chiefly at national government and organisations in the critical infrastructure. Parts of the business community not designated as critical infrastructure suffer, knowingly or unknowingly, from a lack of information because they are not sufficiently connected, if at all, to the structure within which cyber-security-related information is shared. There are a number of public-private partnerships that share information about threat intelligence and action perspectives with the section of the business community not designated as critical infrastructure, but their coverage is limited. Moreover, organisations in the critical infrastructure are highly dependent on suppliers from the section of the business community not designated as part of the critical infrastructure. Hence these parties too have an influence on the digital security of the entire chain. Various parties are now aware that collaboration in digital chains is necessary, but this is far from being realised in practice.

Preconditions not sufficiently met

In order to be able to share up-to-date, reliable and accessible information, certain preconditions need to be met. All parties involved must be aware of the importance of a mutual exchange of information. Companies must also be sufficiently able to process the available information and to quickly follow up on the action perspectives. Currently a section of the business community is still relatively unfamiliar with digital threats and the importance of information sharing for managing these threats. Each company is responsible for its own digital security. Many small and medium-sized enterprises have no budget for this issue, even though this is now a serious management responsibility and an essential element of business management. In her report, Herna Verhagen recommends that companies set aside 10% of their IT budget for this purpose as a benchmark.

The parts of the Dutch business community not designated as critical infrastructure require clear points of contact, but currently they have to rely on public-private partnerships and ICT service

[1] Cyber Security Assessment Netherlands 2017

[2] 'The economic and social need for more cyber security – Keeping "dry feet" in the digital era', Herna Verhagen, September 2016

[3] 'The Netherlands Cyber Readiness at a Glance', Melissa Hathaway & Francesca Spidalieri, Potomac Institute for Policy Studies, May 2017

providers – which do not provide full coverage. It is not only important to share information regarding threats, but also to have the ability to analyse information and to set priorities for approaches based on such information.

Lack of insight into cybercrime

Cybercrime is increasing in scope and presents an ever-increasing threat.[4] The growing threat to cyber security in the Netherlands is chiefly caused by professional criminals and state actors.[5] Due to the inadequate reporting of cybercrime to the police, the picture of cybercrime in the Netherlands is incomplete. To gain an insight into cybercrime is necessary in order to respond to it more effectively. The low number of reports is due to, among other things, the complexity of the procedure for making a report to the police. And once a report has been submitted, the visible follow-up to the report tends to be limited and companies receive very little feedback about what has been done with the report. The chance of damage to the company's image is another important factor that discourages companies from reporting an incident to the police.

It can be concluded that currently the information position of a considerable part of the business community is weak, which means that these companies are easy targets for cyber criminals. There is also a lack of proper insight into the type of cybercrime affecting the country, making it difficult to respond effectively. Information sharing within the Netherlands needs to be improved, which should in the future ensure a significantly higher score for this country on the readiness index.

Advice

Sharing and analysing information allows organisations to increase cyber security and to boost their resilience to cyber incidents and/or to limit the damage they cause. This is important for *all* organisations in the Netherlands. The Cyber Security Council is of the opinion that measures are urgently required to bring information sharing in this country up to the requisite level, thus ensuring that the Netherlands is and remains a safe place to do business, also in digital terms. This requires two things: removing barriers to the sharing of information as well as improving the process of reporting cybercrime to the police and/or pressing charges and boosting the follow-up to these reports.

The goal of this advice is to improve the sharing of information in the Netherlands by (1) the introduction of a nationwide system of information exchanges, (2) the creation of conditions for successful sharing of information through these information exchanges, and (3) increasing to gain an insight into cybercrime by encouraging companies to report incidents to the police and strengthening public-private collaboration in this field.

The Council identifies the following important success factors:

- *A nationwide system of information exchanges[6] for the sharing of information that covers the entire Dutch business community;*
- *The business community is able to quickly respond to threat intelligence and action perspectives;*
- *Suppliers of Internet products and services are pro-active in meeting their duties of care, so that those products and services are intrinsically safe;*
- *Simple procedures for reporting cyber incidents to the police are in place.*

[4] National Threat Assessment 2017, Organised Crime, Netherlands Police, May 2017
[5] Netherlands National Cyber Security Assessment 2017
[6] Information exchanges is taken to mean: existing organisations, intermediate organisations, instruments and initiatives that promote the sharing of information.

The Council identifies the following action perspectives:

- *The Netherlands develops a nationwide system of information exchanges;*
- *The Netherlands ensures that preconditions for a successful sharing of information through the junctions for information exchanges are in place;*
- *The Netherlands ensures that greater insight is gained into cybercrime and strengthens the public-private approach in this area.*

Ad. 1 The Netherlands develops a nationwide system of information exchanges.

Nationwide system

The Cyber Security Council advises the government to collaborate with the private sector to rapidly introduce a nationwide system of information exchanges. The nationwide system must ensure that the sharing of information covers the entire business community in the Netherlands. This is not currently the case and the system needs to be expanded. The development such a nationwide system should make the greatest possible use of existing (intermediate) organisations, instruments and initiatives in this area. The legislative proposal 'data procession and notification obligations regarding cyber security' (WGMC) gives the National Cyber Security Centre (NCSC) a broader mandate for sharing information. The Cyber Security Council views this as a positive development. It is important that the business community, with or without the help of intermediate organisations, be sufficiently able to process threat intelligence and to quickly implement the action perspectives. A survey of the current state of affairs forms the point of departure for the development and expansion of the current system. Furthermore, the Cyber Security Council believes it is important that the various roles, tasks and responsibilities of the participating organisations be properly and mutually coordinated and defined. Fragmentation should be reduced and the missing links in the system should be filled.

The Council recommends that a nationwide system should be developed under the auspices of the Ministry of Security and Justice and the Ministry of Economic Affairs in close collaboration with parties including VNO-NCW (The Confederation of Netherlands Industry and Employers), MKB-Nederland (entrepreneurs' organisation for small and medium-sized businesses in the Netherlands), CIO Platform Nederland (the independent community of persons with overall responsibility for digitalisation and/or ICT for private and public organisations in the Netherlands) and Nederland ICT (the trade association for IT, telecom, internet and office companies in the Netherlands).
Points of attention for the nationwide system are to be found in the following elements: Digital Trust Centre (DTC), National Detection Network (NDN) and Information Sharing and Analysis Centres (ISACs), as well as in regional and sectoral initiatives and suppliers.

DTC

The Cyber Security Council confirms the importance of the motion put forward by the members of parliament Hijink (SP, socialists) and Tellegen (VVD, liberals) and accepted on 13 July 2017 regarding the creation and design of a DTC for the part of the business community not considered as part of the critical infrastructure. The Cyber Security Council warns that a DTC within the framework of the aforementioned nationwide system must be positioned correctly with regard to the existing junctions for information exchanges. A DTC must provide up-to-date, reliable and accessible information to the business community. The business community must in turn endeavour to actively follow such advice and itself be prepared to provide information to a DTC in turn.

NDN

The Cyber Security Council urges an accelerated rollout of the National Detection Network (NDN). Any obstacles to this should be removed. The information from the NDN should also be sent to the part of the business community not considered as part of the critical infrastructure via the Information Sharing and Analysis Centres (ISACs) and a DTC.

ISACs

The Cyber Security Council believes that ISACs play an important role in sharing knowledge and information within sectors. The council does however recommend a stronger focus on a cross-sectoral and chain-oriented approach at the ISACs. The council supports the proposal by the Ministry of Economic Affairs on the creation of ISACs for the top sectors. This will contribute to improved cyber security for companies that belong to the top sectors because these are knowledge-intensive companies vulnerable to cybercrime. This of major importance to the future earning ability of this country.

Regional and sectoral initiatives

The Cyber Security Council considers it important that regional and sectoral initiatives are developed, encompassing the government, the vital sectors and the parts of the business community not designated as vital, ranging from SMEs to multinationals. Large companies have more people and resources at their disposal for investing in cyber security. Due to chain dependencies it is crucial that all chain partners devote attention to cyber security. A range of initiatives have been started, for instance at Amsterdam Airport Schiphol and the Port of Rotterdam, in which chain partners join forces to improve their cyber security. The Cyber Security Council emphasises the importance of such initiatives.

Suppliers

Suppliers of internet products and services play an essential role in making and keeping organisations secure. They must meet their duties of care properly and they must relieve their customers of a burden by supplying relevant and accessible information to keep their digital infrastructure secure.

Ad. 2 The Netherlands ensures that preconditions for a successful sharing of information through the junctions for information exchanges are in place.

Supporting role of the Confederation of Netherlands Industry and Employers (VNO-NCW), branche associations and the Chamber of Commerce (KvK)

All companies, both organisations part of the critical infrastructure and those not considered as a part of the critical infrastructure , from small and medium-sized businesses to multinationals, must be aware of the risks they run and the major role that information sharing can play in identifying the right security measures to be taken. The Cyber Security Council sees an important role for branche associations in the area of cyber security for the business community. This involves informing members of the business community about the information landscape, helping them to navigate through it and disseminating targeted threat information and action perspectives. Branche associations can also encourage their members to report incidents to the police and/or press charges. VNO-NCW can support the industry associations in their role with regard to the business community. The Cyber Security Council also sees an important role for the Chamber of Commerce in raising the business community's cyber-awareness.

Financial incentives

Branche associations vary in maturity level and this is why they can benefit from help in properly fulfilling their desired role in the area of cyber security. The state should enable financial incentives for branche associations so that they can fulfil their role towards the business community in the area of cyber security.

Ad. 3 The Netherlands ensures that greater insight is gained into cybercrime and strengthens the public-private approach in this area.

Reporting incidents

The National Police Force must be able to anticipate developments in the area of cybercrime. If cybercrime is reported this provides a better picture of the current state of affairs in the area of cybercrime. Hence the process of reporting cybercrime to the police and/or pressing charges must become easier and more accessible for citizens and the business community, for instance by making it possible to report cybercrime digitally. The principle to be applied here is 'reporting cybercrime is more important than pressing charges'. An increase in the reporting of incidents can help to identify trends better and to set priorities in the approach to this problem. VNO-NCW, MKB-Nederland, branche associations, the Chamber of Commerce, Nederland ICT and the CIO Platform Nederland can encourage companies to be more active in reporting incidents to the police and pressing charges. The Cyber Security Council stresses the importance of the police providing good feedback to those making the reports so that they remain motivated to continue reporting incidents.

Public-private collaboration on cybercrime

According to the Cyber Security Council it is important that in the context of improving the information position on cybercrime, extra investments must be made in the public-private collaboration. In many cases this collaboration has proved to be of significant value. It means that the police and the Public Prosecution Service work together with, for instance, the banking sector, the ICT sector and other relevant private partners to promote digital resilience and security in the Netherlands.

RECOMMENDATIONS

The recommendations are directed to the government and the business community. They will only work if the improvement of information sharing in the area of cyber security and cybercrime is tackled jointly. The Cyber Security Council advises:

The Minister of Economic Affairs and the State Secretary for Security and Justice jointly:

1. In collaboration with the private sector, to introduce a nationwide system of junctions for information exchanges that is based as far as possible on existing structures. In this context, accelerate the introduction of a Digital Trust Centre for the part of the business community that does not form part of the vital infrastructure.

The Minister of Economic Affairs

2. To provide a financial incentive to industry associations, enabling them to fulfil their role towards the business community in the area of cyber security.

The State Secretary for Security and Justice:

3. To accelerate the rollout of the National Detection Network (NDN) and enable information from the NDN to be shared on a broad basis with the business community.

The Minister of Economic Affairs, the chair of VNO-NCW, the chair of MKB-Nederland the chair of Nederland ICT, the chair of the CIO Platform Nederland, the chair of the Chamber of Commerce and chairs of industry associations jointly:

4. To make the business community cyber-aware and motivate them to play an active role in sharing threat intelligence and to implement action perspectives in the context of the nationwide system.
5. To encourage companies to report cybercrime to the police and/or press charges.
6. To ensure a cross-sectoral approach by ISACs, focusing on the chain philosophy. The initiatives developed by Amsterdam Airport Schiphol and the Port of Rotterdam in conjunction with their chain partners are good examples of this.

The Commissioner of the National Police Force

7. To make it easier for victims to report cybercrime to the police and/or to press charges, and to ensure that they receive high-quality feedback about the follow-up.

The Commissioner of the National Police Force and the Board of Procurators General jointly:

8. To reinforce and structure public-private collaboration in order to strengthen the information position with regard to cybercrime.

The Hague, June 2017

On behalf of the Cyber Security Council,

Eelco Blok Dick Schoof