Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
PO Box 20011
2500 EA The Hague

I www.cybersecurityraad.nl
T +31 (0)70 751 5333 (secretariat)
E info@cybersecurityraad.nl

Ministry of Justice and Security
Attn: Prof. F.B.J. Grapperhaus, LLM
PO Box 20301
2500 EH The Hague

Date
22 February 2021

Subject
CSR Recommendation Letter on the accelerated sharing of incident information

Your Excellency,

The Cyber Security Council (hereinafter referred to as the CSR) is issuing this recommendation in response to your Letter to Parliament 'Results of exploratory study on statutory powers, digital resilience and policy response in connection with Research and Documentation Centre reports',[1] dated 3 February 2021, in which you announced your intention to explore whether a legislative amendment to facilitate the establishment of a mature nationwide network of information hubs (*Landelijk Dekkend Stelsel*, LDS) is in order. The nationwide network has been a frequent topic of discussion within the CSR. The CSR published a recommendation[2] concerning the nationwide network in 2017. Since that recommendation, important steps have been taken toward the (further) design and roll-out of the nationwide network, including the establishment of the *Digital Trust Center (DTC)*. As it currently stands, the nationwide network remains a work in progress and has yet to achieve the level of maturity the CSR would prefer. It would be prudent to offer transparency into how the further roll-out of the nationwide network will be arranged, to allow organisations to prepare for their role within the system. The CSR is of the opinion that, in anticipation of the amendment you propose, actions should be taken in the near future to accelerate this process in the interest of an open, free and prosperous society, both digital and otherwise.

One of the most vital instruments for enhancing the digital resilience of organisations and citizens is the ability to quickly inform them when vulnerabilities in their IT systems have been detected or when those systems have been hacked. Our *National Cyber Security Centre (NCSC) has been designated the national central point of contact* as referred to in Section 8(3) of the NIS Directive and, in that capacity, receives thousands of reports each day regarding the Dutch IP addresses at which compromised systems are located. The incident reports arrive at the NCSC via automated data flows from the national CERTs of other countries and via Internet companies, non-profit organisations, security researchers and other parties, both in the Netherlands and abroad.
The primary task of the NCSC is to inform the Dutch government and critical providers in the event that cybersecurity vulnerabilities are detected in their systems. In addition, the NCSC has a duty to forward any incident reports it receives to intermediary organisations (*schakelorganisaties*), who then pass the incident

[1] This inventory has no bearing on the tasks and powers of government services in the context of criminal investigations into cyber-related offences.

[2] CSR Recommendation 2017, No. 2: 'Towards a nationwide network of information hubs, advice on information exchange with regard to cybersecurity and cybercrime'

reports along to the affected parties in their respective constituencies. In order to create a comprehensive information system, the nationwide network of cybersecurity alliances has been established.

An objective set out in the 2018 National Cybersecurity Agenda (NCSA)[3] concerns the construction of this nationwide network in order to strengthen public and private parties' ability to take decisive action to combat digital threats and incidents. The *Network and Information Systems Security Act (Wbni)* and its predecessor, the *Data Processing and Cybersecurity Notification Obligation Act (Wgmc),*[4] include several provisions regarding the sharing of information by NCSC with parties outside its primary target group. In practice, the NCSC is now encountering a number of situations in which – according to the legal advice provided on this matter to date – it **cannot** share incident information with the most relevant intermediary organisations, despite these parties being specifically designated for that purpose in the Wbni and having been subsequently established, organised and certified by the private-market stakeholders. The combined result is that, at this time, the NCSC does not share incident information with the most relevant intermediary organisations – as a result, critical incident information **does not** reach the businesses and citizens[5] affected. That information is potentially valuable to the police and the public prosecutor as well. Sharing incident-related and/or residual information with the police and the public prosecutor can prove beneficial to efforts to secure digital traces, as well as to the investigation and prosecution of offences in general.
All parties involved in the nationwide network (including the NCSC) now concur that this yields an unworkable situation and is preventing the realisation of the nationwide network. As it currently stands, many thousands of businesses and citizens are not being informed in instances where the government possesses information indicating they are vulnerable or have been victims of an incident.
We will first provide a brief description of the legal issues at play. This will be followed by the recommendation of the CSR as to how you should address this problem.

Legal aspects

Pursuant to Section 3(1) of the Wbni, the primary task of the NCSC is to inform, advise and otherwise support the Dutch government and critical providers in the event of threats and incidents involving their network and information systems. The NCSC has an additional duty with regard to information concerning threats and incidents that has been obtained in connection with the stated primary task (also referred to by the NCSC as 'residual information'), namely to provide this information to specific 'intermediary organisations' within the nationwide network, in the event that doing so may serve to prevent a negative societal impact.

Section 3(2) of the Wbni stipulates the third parties with whom the NCSC is permitted to share this residual information:

a. organisations with an objective manifest duty to inform the public or other organisation(s) with regard to such incidents (OKTTs);
b. Computer Security Incident Response Teams (CSIRTs);

[3] National Cyber Security Agenda: A cyber secure Netherlands, National Coordinator for Security and Counterterrorism (NCTV), on behalf of the Dutch government, 2018, page 19
[4] The Wgmc came into force on 1 May 2018 and was superseded by the Wbni on 9 November 2018. The provisions discussed in this letter are virtually identical. Hereinafter, we will refer exclusively to the Wbni, though this should be taken to mean both Acts.
[5] Citizens are notified by their Internet provider in the event that one of their devices has been infected. To supply this notification, Internet providers rely on information shared with them regarding IP addresses in the provider's network at which an infected device has been detected. Many Internet providers receive such information via AbuseHUB, the 'abuse information exchange' established by providers for the purpose of informing and protecting their users.

c. other digital crisis teams, whether appointed directly by Our Minister or belonging to a category designated as such in the legislation;
d. providers of Internet access and Internet communication services, for the purpose of informing the users of those services.

In practice, the NCSC now faces a situation in which – according to the legal advice issued within the Ministry of Justice and Security on this matter to date – it cannot share residual information with the OKTTs alluded to in Section 3(2), despite the fact that the OKTTs have a key role to play with regard to the functioning of the nationwide network. At this time, four such OKTTs exist: AbuseHUB, the Dutch National Internet Providers Management Organisation (NBIP), Cyber Resilience Center Brainport (CRB) and the sector organisation Cyberveilig Nederland. Other organisations, such as the Digital Trust Center (DTC) run by the Ministry of Economic Affairs and Climate Policy, hope to gain OKTT status in the near future.

The main obstacle impeding the NCSC from sharing residual information with the OKTTs is that Section 20(2) of the Wbni states that the NCSC may share *confidential* data that can be traced to a specific provider with a limited number of third parties and may do so solely to the extent to which this serves to facilitate measures aimed at preventing or mitigating the disruption of social and economic life. In all other cases, prior permission must be obtained from the affected provider. The aforementioned category of intermediary organisations with whom confidential information may be shared without consent from the provider in question does not include the OKTTs.
According to legal counsel, in virtually all cases, the residual information pertaining to vulnerable or compromised systems also contains confidential traceable data such as the domain names and IP addresses where compromised systems are located. These data are *traceable*, as the IP addresses can easily be traced back to the provider and from there to the owners of the IP addresses, simply by consulting the RIPE registry. The same applies to the domain names, which can be traced to a provider or owner via SIDN. The data are *confidential* as well, as the residual information includes information indicating that the systems of these providers have been compromised. Failure to process these data in a confidential manner may result in harm to the provider (potential victim). In light of the aforementioned obstacle presented by Section 20(2) of the Wbni, the NCSC does *not* share residual information with the OKTTs. This situation is obviously undesirable and is most certainly contrary to the intention underlying the Wbni; it is in any case contrary to the aims of the nationwide network.
The objective of both the Wbni and the nationwide network is to enable the NCSC to forward incident data to intermediary organisations, so that they in turn can inform victims among their constituencies in order to protect those victims. Achieving this objective requires the use of *traceable* data (without which it is impossible to identify and notify the victim, so that they may – after receiving this information – take actual measures in response). However, because this incident information also concerns *confidential data* belonging to the victim, the legal reasoning applied here says that, in order to protect the confidential data, this victim may not be notified.
In short, it is not possible to inform the victim for the purpose of protecting that victim, due to the confidential nature of the information in question. The confidentiality is, in turn, intended to protect that same victim. To put this in terms of the physical world, the lock on the front door of a private home is broken, meaning anyone can simply walk in off the street, yet we are not allowed to have the neighbourhood watch inform the citizen that their lock is broken, because this is confidential information belonging to the citizen.
Little explanation is needed as to why this cannot be the intent of the Wbni, and any reasonable interpretation of the provisions contained in the Wbni must conclude that sharing such information should, in fact, be possible. The CSR also wishes to remind all parties that, prior to 1 May 2018, when these provisions came into

force, the NCSC did share these incident data with the affected organisations. The Wbni was intended to provide a statutory basis for this sharing, but it now poses an impediment to it.

All parties involved in the nationwide network (including the NCSC) are now in agreement with regard to the undesirability of the aforementioned impediment, and you have informed the House that you intend to explore whether an urgent procedure to realise a specific amendment is in order.

Recommendation

In principle, the CSR supports your proposal for this legislative amendment. That being said, the CSR notes that – realistically speaking – it will most likely be another two years before the amendment actually enters into force. The CSR would ask you to consider exploring whether it might be possible to implement the amendment more quickly via an *emergency repair procedure.* In light of the urgent need to establish a nationwide network, it is the further opinion of the CSR that the sharing of incident information with the OKTTs cannot wait until such time as the entire amendment procedure has been completed. There is every reason to apply the Network and Information Systems Security Act (Wbni) as it was intended.

The CSR therefore recommends that you, in keeping with the spirit of the Wbni and in anticipation of the planned amendment, commence the sharing of incident information with OKTTs at this stage. Doing so will support efforts to protect the interests of the thousands of businesses, organisations and citizens who are currently not being informed in instances where the government possesses information indicating the former parties are either vulnerable or have been victims of an incident.

We look forward to receiving your response prior to our CSR meeting on 25 March 2021.

On behalf of the Cyber Security Council,

Hans de Jong
CSR co-chair