At present, there is no collective basis for helping organizations to increase their resilience. It is up to each individual organization to build up a basis of resilience, using the knowledge and capacity at their disposal.

Due to the asymmetric relationship between manufacturers and customers in the field of software security, users are usually unable to impose safety and security requirements and make the right assessments themselves, when purchasing software. There are possibilities for organizations to consciously deal with the risks of software, but not every organization has the knowledge and capacity to impose and check the appropriate requirements. There are no generally applicable rules concerning the control of software, that require manufacturers to satisfy specific safety and security requirements.

As concerns prevention and preparation for incidents, there are major differences in the level of resilience of organizations. Many measures require a risk assessment. Not all organizations have the expertise and capacity to sufficiently implement the appropriate measures, or fail to recognize the urgency of deploying their capacity for this task. Every organization is independently responsible for its own digital resilience. There is no collective foundation available, to assist organizations in increasing their digital resilience.

4.3 Incident management (response)

The occurrences described in chapter 3 show clearly that the time between the reporting of a software vulnerability and an attack being launched on vulnerable organizations is limited: ranging from a month to just a few days or even zero days. In the previous sections, we discussed the factors that influence the way in which manufacturers prevent and respond to software vulnerabilities, and what organizations that use software do to prevent their digital systems suffering security leaks as a result. In this section, we deal with the factors that influence how the various stakeholders such as manufacturers, organizations and public and private incident managers tackle the incidents in order to limit the consequences.

4.3.1 Information flow

Following the announcement of a vulnerability, it is crucial that the relevant organizations be informed as directly and as quickly as possible. Organizations that use the software need information that is as precise and reliable as possible, in order to determine quickly how to respond in order to manage the risks; organizations unable to independently arrive at such a consideration need advice that they can follow. Manufacturers and incident managers want to know how many and which organizations are vulnerable and how they are being attacked, so they can take the appropriate measures and offer support and/or advice. This information can be collected from a variety of sources such as manufacturers, voluntary and commercial security investigators, CERTS via coordinated vulnerability disclosure-procedures and security and intelligence services. The occurrences investigated in this report show that at present there are barriers that prevent information received from various public and private sources being shared as quickly as possible with all the organizations that need the information in order to tackle the consequences of vulnerabilities in software.

Barriers to the sharing of information

Information provision is of crucial importance to organizations, because in incidents such as those discussed in this investigation, a rapid response is essential in order to prevent attacks.[175] Most countries have a national authority that acts as incident manager. In the Netherlands, the NCSC is the national CERT. One reason why the position of the national CERT is relevant is because other parties such as software manufacturers in each country use the national CERT as the first point of contact, for example for notifying which organizations in a particular country are vulnerable to attack.

Two types of information are central to information sharing: fact-finding information (to achieve perspective for action or security advisories and messages about vulnerabilities) and threat information. Threat information consists of attacker information and victim information. The bottlenecks in incident response relate primarily to threat information: information about which organizations are vulnerable and how to identify attackers.[176] This concerns in particular the victim information that is not used, resulting in parties not being warned.

Much information from a variety of sources comes together at the NCSC: as well as manufacturers, information is provided by security and intelligence services, other government organizations, sectoral partnerships (ISACs), independent security researchers (via the DIVD and otherwise), cybersecurity companies and IT service providers as well as via messages on social media such as Twitter, Reddit and professional media. The organizations we interviewed indicated that at present, they themselves often go in search of information via formal and informal sources, because the information they need is not provided via the NCSC, or at least not on time.

Observed legal impediments

On the basis of its limited legal mandate and other legal impediments like the GDPR, the NCSC states that it is restricted to sharing victim information (like IP addresses of vulnerable servers) with the organizations that need it, namely that NCSC may only share this information with national government and vital operators.[177] During the Citrix crisis, the NCSC decided to deviate from its own legal frameworks and share threat information with a number of collaborative teams and computer crisis teams such as Z-CERT and the IBD. Following this, these frameworks were broadened in 2020 and 2021. Other sectors including almost the whole of the Dutch private sector (1.8 million companies[178]) received no threat information.

[175] This importance was recently underlined in the report of recommendations Integrated approach to cyber resilience by the Cyber Security Council, April 2021.

[176] Definition from report from Dialogic and TU/e, 2020.

[177] The legal mandate of the NCSC is regulated in the Security of Network and Information Systems Act (Wbni), which came into effect on 9 November 2018.

[178] Self-employed, SMEs and businesses. Source: https://www.digitaltrustcenter.nl/over-het-digital-trust-center

A further barrier lies in what information the NCSC shares with the information hubs. The NCSC has adopted a position that according to the Wbni, confidential, traceable data may only be shared with CERTs, CSIRTs and the intelligence services, and not with OKTTs. The Ministry of Justice and Security views IP addresses of vulnerable servers as confidential information that can be traced back to providers, in the framework of the Wbni, and as personal data in the framework of the GDPR.

A study on information sharing commissioned by the WODC acknowledged that the institutional setting and laws and regulations create barriers for the NCSC to share information, but indicated that these barriers are partly the result of how the Ministry of Justice and Security interprets the rules. In other words, it is also possible within the current frameworks of laws and regulations to come to different legal insights and judgments and decide to share the information.

The WODC study does not make a statement about what the correct view is, but it does state that it is important to reach consensus on this point. Therefore, the researchers recommend that follow-up research be conducted into these legal questions. The Minister of Security and Justice has announced a legislative proposal to remove the barrier by expanding the NCSC's authority to share relevant threat information. However, it may take one to several years for this law to be passed and implemented. [179]

Incident response in the Netherlands, under which the collecting and sharing of information, is fragmented and contains gaps. As a consequence, for many organizations, including a large portion of the Dutch private sector, there are no arrangements in place in order for them to receive timely information when they are at risk. This especially concerns victim information, or that an organization is warned that its systems are vulnerable (also unsolicited) and that it is at risk to be attacked. The NCSC, which receives information for the entire Netherlands, from inter alia manufacturers, NCSCs in other countries, intelligence services and other forums, now only shares this victim information with a select group of organizations, not with local governments and with most of the Dutch private sector, and on the basis that an organization consents to being informed in advance.

[179] Dialogic en TU/e, *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity* in opdracht van WODC, 14 October 2020.
https://www.rijksoverheid.nl/actueel/nieuws/2021/06/28/meer-mogelijkheden-ncsc-en-dtc-om-dreigings--en-incidentinformatie-te-delen

Nationwide system of linking organizations

To improve the possibilities for information sharing, the Minister of Security and Justice is working on a nationwide system of linking organizations (in Dutch: Landelijk Dekkend Stelsel)[180], so that the NCSC is authorized to share information with organizations that are identified as authorized to receive and pass on that information. The result will be a system with a large number of organizations each of which provides a counter service to its target organizations, and is capable of sharing information with each other. In a system of this kind there will be delays, because it takes time to determine which particular information is relevant to which information hub. There is also a risk that information will be lost at each stage. As a result, the NCSC as national CERT loses valuable time, preventing it from adequately facilitating their public role within the digital domain. In addition to the Nationwide system of linking organizations, the informal circuit consisting of volunteers is also important to maintain proactive information sharing.

Another obstacle is that not all organizations in the Netherlands are covered by linking organizations within the Nationwide System. This applies in particular to the private sector. This sector includes many companies that fulfil essential functions for vital operators or for other socially important organizations that are not covered by the definition vital, such as the food sector. Against that background, the Minister of Justice and Security has announced a bill that would, inter alia, enable the NCSC to share information via the Digital Trust Center (DTC) with the Dutch private sector ('the rest of the rest').[181] In addition, the ministry of Economic Affairs and Climate Policy has announced a bill to strengthen the legal basis of the DTC. Based on that, DTC will launch a pilot to share threat information with 40 companies that sign up for it in the fall of 2021.[182]

With these efforts the nationwide system would gain coverage, but the sharing of information will remain fragmented across a large number of linking organizations, each of which must deploy capacity and expertise, in order to make meaningful sense of the information.[183] The following figure created by the Anti Abuse Network (AAN) of how threat information is exchanged between organizations highlights how complicated information sharing is.

[180] These are referred to by the NCSC as linking organizations. https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds

[181] https://www.rijksoverheid.nl/actueel/nieuws/2021/06/28/meer-mogelijkheden-ncsc-en-dtc-om-dreigings--en-incidentinformatie-te-delen

[182] https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat/nieuws/2021/09/13/digital-trust-center-start-met-actief-informeren-bedrijven-over-digitale-dreigingen

[183] At present the DTC consists of 20 FTE to serve 1.8 million companies. Moreover, the DTC has no direct relationships with these companies, only via collaborative ventures (even more links in the information sharing chain).

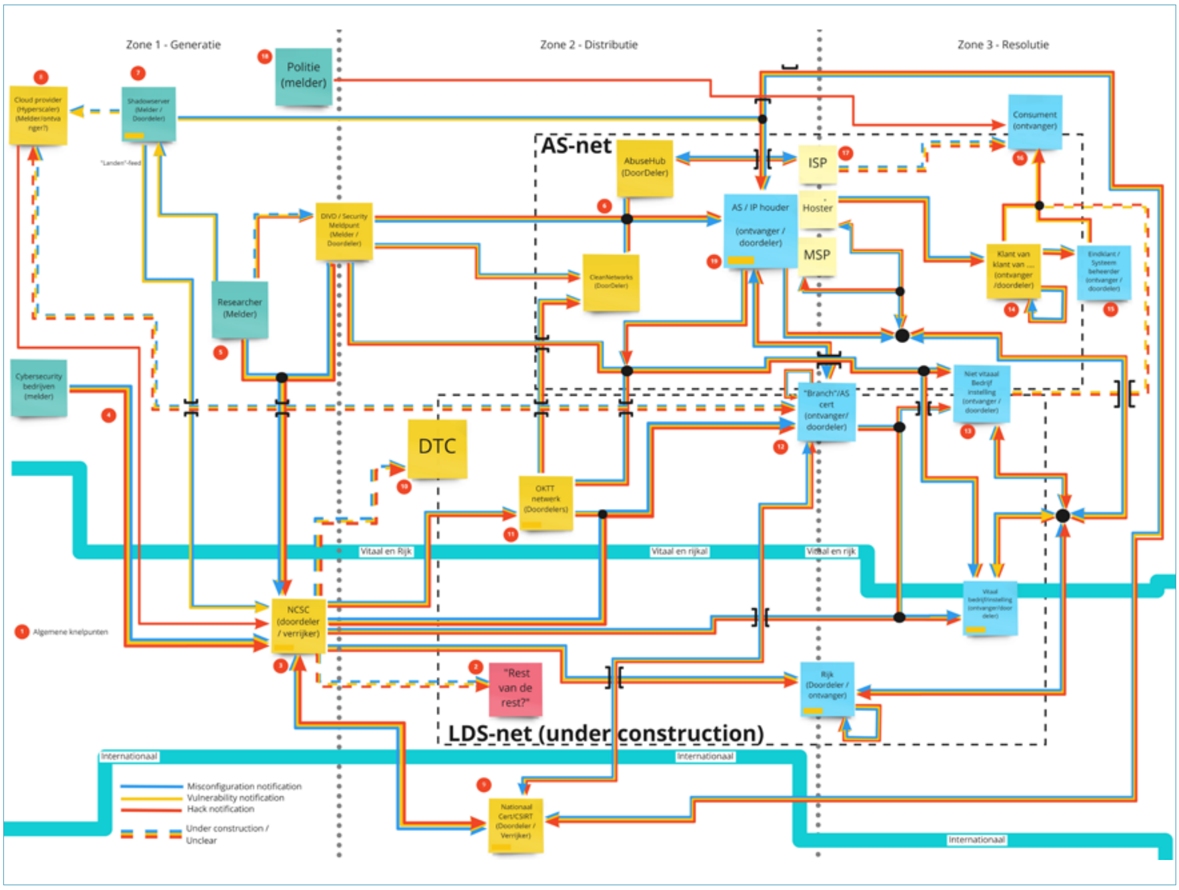
Zone 1 - Generatie
Zone 2 - Distributie
Zone 3 - Resolutie
Politie (melder)
Cloud provider (Hyperscaler) (Melder/ontvanger?)
Shadowserver (Melder / Doordeler)
"Landen"-feed
DIVD / Security Meldpunt (Melder / Doordeler)
Researcher (Melder)
Cybersecurity bedrijven (melder)
AS-net
AbuseHub (DoorDeler)
CleanNetworks (DoorDeler)
AS / IP houder (ontvanger / doordeler)
ISP
Hoster
MSP
Consument (ontvanger)
Klant van klant van .... (ontvanger /doordeler)
Eindklant / Systeem beheerder (ontvanger / doordeler)
Niet vitaal Bedrijf instelling (ontvanger / doordeler)
"Branch"/AS cert (ontvanger/ doordeler)
DTC
OKTT netwerk (Doordelers)
Vitaal en Rijk
Vitaal en rijkal
Vitaal en rijk
Vitaal bedrijf/instelling (ontvanger/door deler)
NCSC (doordeler / verrijker)
Algemene knelpunten
"Rest van de rest?"
Rijk (Doordeler / ontvanger)
LDS-net (under construction)
Internationaal
Nationaal Cert/CSIRT (Doordeler / Verrijker)
Misconfiguration notification
Vulnerability notification
Hack notification
Under construction / Unclear
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

Figure 18: Subway map of the exchange of threat information on organizations. (Source: AAN)[184]

Finally, barriers to information sharing between Member States and between public and private entities have a negative influence on the effectiveness of cybersecurity measures and the picture of the scale and seriousness of the situation.[185]

Barriers to gathering information

A further issue is whether the NCSC or the other information hubs are themselves permitted to gather the information needed to help organizations tackle the consequences. The occurrences analysed in this investigation show that IP addresses of vulnerable servers are crucial in convincing organizations of the urgency of intervening, and also represent important management information in creating a picture of the situation and the extent to which it is under control (see also 4.3.2).

Via certain tools on the Internet, investigators are able to scan the outside of digital systems, and in this way map out which servers make use of specific versions of specific software. This method of scanning does not reveal whether the servers are still vulnerable (or whether the organization has already implemented the mitigating measure or patch). To reveal that information, a scan usually has to be carried out whereby the person carrying out the scan as it were 'rattles the door' to check whether it is locked or can be

[184] https://www.abuse.nl/publicaties/metrokaart-december-2020.html
[185] European Parliament, *The NIS2 Directive – A high common level of cybersecurity in the EU*, 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

opened. Scans of this kind are often carried out in practice, and in certain cases are in fact recommended by manufacturers and national CERTs.[186]

There is a clear need within the NCSC at least to be able to carry out scans to map out which servers make use of specific software, and preferably also whether these servers are still vulnerable, so that more targeted warnings can be issued, and to gain a clearer picture of the scale of the situation. However, legal advisors within the NCSC and NCTV recommend against this, because of the perceived legal risks. Scanning tools are after all also used by attackers, and the legal concern is that 'rattling the door' could result in unauthorized intrusion.[187]

The occurrences described in chapter 3 show that voluntary security investigators, represented, among others, in the DIVD are attempting to fill this gap in information provision and incident management by scanning which organizations have vulnerable systems, and subsequently warning those organizations. The NCSC and other CERTs also use their information. However, this is a vulnerable situation. These security investigators are operating voluntarily, generally alongside a fulltime position elsewhere. Because of the large number of vulnerabilities and attacks in recent times, this has imposed huge demands on these volunteers.[188]

Situation differs between organizations

The fragmentation and blank patches in the landscape of information hubs not only mean that relevant information fails to reach the affected organizations, but also that it is not possible to form a consistent picture of the scale and seriousness of an occurrence. Every (government) organization is required to make its own impact analysis and must determine for itself whether or not to follow the recommendations from the information hubs or cooperative ventures to which it is affiliated, and what actions to take. Both shutting down as a precaution and leaving systems on can have implications for digital safety and security, but these risks and their perception vary from organization to organization. As a consequence, certain organizations take measures immediately after an incident occurs, while others are unable or unwilling to do so (see section 4.2 for a further analysis of the considerations made by organizations). In practice, it turned out most organizations failed to feedback how they responded to the recommendations, such that a diffuse picture emerged within the information hubs about the extent to which the situation in the Netherlands was under control. In addition, if organizations fail to take any measures, this not only represents a risk for the organization itself but also for its supply chain partners (suppliers and customers).

[186] See for example https://www.us-cert.gov/ncas/alerts/aa20-031a. In the case of the Citrix vulnerability, during the scan, a non-existing file is requested on the Citrix server at a location to which the user should not be given access. If the Citrix server replies that the file does not exist, it is clear that the vulnerability is still present on the server.

[187] Non-public source: memorandums and mail exchange.

[188] See for example this podcast in which DIVD volunteers talk about their involvement in the Kaseya occurrence. https://www.cyberhelden.nl/episodes/episode-27/, July 2021.

The national government aims to improve the exchange of information that the NCSC does want to share through the National Coverage System for sharing cybersecurity information, in which sectoral organizations and (groups of) businesses share information crucial for responding to incidents on a voluntary basis. However, if the NCSC as national point of contact receives information but does not share all information, even with a complete coverage system, not all potential victims will be warned. Security researchers try to compensate for this, by scanning the Dutch internet domain for vulnerable servers – on a voluntary basis - and by sharing this information with parties that can warn others. However, this was a vulnerable situation because they were not facilitated in this and their structural commitment is not guaranteed.[189]

4.3.2 Developments in incident management

What the incidents show is that good cooperation between government and organizations is crucial to combat incidents as well as preventing them (see sections 4.1 and 4.2). Mutual trust is crucial here, as is a consistent national approach. [190]

In a number of other countries, the cybersecurity system and incident response are centrally organized; there are also calls in the Netherlands for more central control. In the Netherlands, a decentral approach to incident management has been chosen. It is argued that a decentral approach is appropriate to the Dutch culture. A central approach to cybersecurity and incident management in other countries (see block) often goes hand in hand with supervision by the intelligence services. In the Netherlands, such an approach could lead to opposition.[191]

[189] In the meantime this situation has changed: the end of September 2021 the private sector announced that it would set up its own warning system. Source: *FD*, Bedrijfsleven start eigen alarmsysteem tegen hackers: 'overheid te traag', 28 September 2021.

[190] Atkins, S. and C. Lawson, An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure. *Public Administration Review*, Vol. 81, Iss. 5, pp. 847–861, 2020.

[191] See a.o.: Rand, *Cybersecurity A State-of-the-art Review Phase 2*: Final Report, 2020.
NSOB, *Actuele kwestie, klassieke afweging. Een verkenning naar de governance van het Nederlands digitaliseringsbeleid,* 2021.

Incident response in other countries

Other countries have opted for a central approach to the cybersecurity system. In the United Kingdom, the NCSC is the national organization for cybersecurity. As well as being responsible for tackling incidents, they are also the centre of excellence, and work to improve the cyber resilience of both government and the private sector. The NCSC falls under the auspices of British intelligence gathering organization GCHQ, and as such has access to topflight experts and intelligence. The cybersecurity policy is prepared by the Cabinet Office, at national government level (as opposed to departmental level). In France the GIP ACYMA (comparable to the DTC) has proven successful in reaching small businesses, by linking them to private IT experts. In Germany, incident management is just as splintered as in the Netherlands, because of the federal system of government.[192]

The American Cybersecurity and Infrastructure Security Agency (CISA) just like the British NCSC is equipped both for incident management and improving resilience, for all government organizations and businesses in the US. The CISA works closely together with the private sector and regularly issues recommendations in conjunction with the NSA and the FBI.[193]

Following evaluations and letters to parliament in response to the occurrences, measures have been and are being taken to improve incident management, including the bill from the Minister of Justice and Security that should make it possible to share more information with the private sector. Municipalities are also connected to the National Detection Network, that in the past, in compliance with the Wbni, was reserved to national government and vital operators. These developments show that although national government still maintains the distinction in law, in practice it is slowly relaxing its restrictions.

Nonetheless, the sharing of information will continue to take place within the frameworks of the decentralized approach. The analysis of the occurrences shows that in the event of a vulnerability that is subject to attack worldwide, the time to respond is limited to just a few days or sometimes zero days. A decentralized approach leads to loss of both time and information, as a result of which organizations are not informed in time of the risks they run.

Another development that has emerged from the analysis of the occurrences is that for national government (Justice and Security, Interior and Kingdom Relations) a political and administrative need has emerged for accounting for the fact that all relevant organizations in the Netherlands follow the advice of the NCSC. This not only relates to organizations subject to the mandate of the NCSC but also organizations beyond that mandate such as municipalities, provinces and healthcare institutions. This would seem to suggest that there is a need for a central approach, that does not yet exist. Conversely, the undirected guidance by the NCSC and the sometimes direct contacts from national

[192] Dialogic and TU/e, *Information exchange nationwide cybersecurity network on behalf of WODC*, 14 October 2020.
[193] https://www.cisa.gov/

government led these organizations to feel pressured into following advice, despite the absence of any formal relationship for control or accountability with national government. These organizations have their own forum responsible for governing them and to whom they are accountable.

4.4 Learning from digital incidents

In bringing about any improvement in safety, it is important to investigate what happened, and which factors contributed to the occurrence and consequences of the incident. These insights are key in preventing future incidents, and limiting their consequences, especially in a domain as dynamic as cybersecurity.

In many domains, major incidents and public outcry serve as an incentive to learn, and improve safety. In the Netherlands, investigations have been undertaken for more than one hundred years into accidents and disasters, initially only in the transport sector. Following the firework disaster in Enschede, and the fire in a café in Volendam, the Dutch Safety Board was established in 2005 to meet the need for a permanent investigative body that as well as transport, was also authorized to carry out investigations into occurrences in other domains.[194] In the domain of transport, this research has a long tradition worldwide. For example, an air crash involving a popular football coach in the US in 1931 eventually led to the establishment of the NTSB (the American counterpart to the Dutch Safety Board).[195]

The digital domain is a relatively recent domain, and the tradition of learning from incidents affecting this domain is limited and still under development. In this section we describe:

- how digital incidents are currently reported and investigated;
- which factors influence how lessons are learned from digital incidents. This relates both to choices and assumptions made and held by investigators and the context within which the investigations take place.

4.4.1 Current practice for investigations into digital incidents

There can be several different reasons for investigating an incident. Firstly, based on the individual needs of the organization affected, be it a manufacturer of software or an organization using software, there is an intrinsic need to learn from occurrences so as to prevent recurrences in the future, not only within the organization itself but also for others. There are also a variety of legal obligations that mean that particular occurrences have to be reported to specific bodies (although they are then not always investigated). Parties such as the police and insurers carry out forensic investigations into occurrences. Below, we will discuss our observations on current practice as regards the reporting and investigation of digital occurrences.

[194] https://www.onderzoeksraad.nl/nl/page/12056/geschiedenis
[195] Anderson, R., *Security Engineering*, 2020.