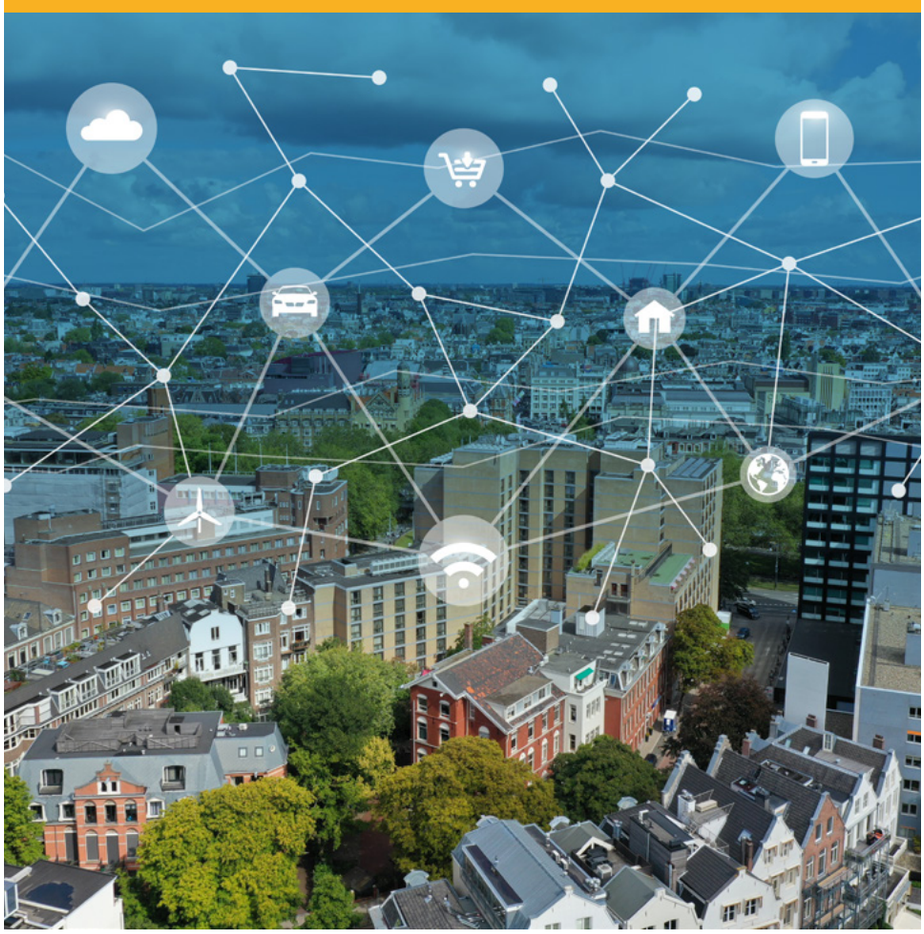
DUTCH
SAFETY BOARD

Vulnerable through software

Lessons resulting from security breaches relating to Citrix software



Vulnerable through software

Lessons resulting from security breaches relating to Citrix software

The Hague, December 2021

The reports issued by the Dutch Safety Board are publicly available on www.safetyboard.nl.

(Source cover photo: Shutterstock, edited by Delta3)

The Dutch Safety Board

When accidents or disasters happen, the Dutch Safety Board investigates how it was possible for these to occur, with the aim of learning lessons for the future and, ultimately, improving safety in the Netherlands. The Safety Board is independent and is free to decide which incidents to investigate. In particular, it focuses on situations in which people's personal safety is dependent on third parties, such as the government or companies. In certain cases the Board is under an obligation to carry out an investigation. Its investigations do not address issues of blame or liability.

Dutch Safety Board

Chairman: J.R.V.A. Dijsselbloem
S. Zouridis
E.A. Bakkum[1]

Secretary Director: C.A.J.F. Verheij

Visiting address: Lange Voorhout 9
2514 EA The Hague
The Netherlands

Postal address: PO Box 95404
2509 CK The Hague
The Netherlands

Telephone: +31 (0)70 333 7000

Website: safetyboard.nl
E-mail: info@safetyboard.nl

N.B:
This report is published in the Dutch and English languages. If there is a difference in interpretation between the Dutch and English versions, the Dutch text will prevail.

1 Ms. dr. E.A. Bakkum joined the Dutch Safety Board on December 1, 2021, following the approval of this report by the Safety Board. She has not been involved in this investigation.

CONTENTS

SUMMARY

On the 17th of December 2019, the American software manufacturer Citrix made a public announcement on its website that some of its software products contained a vulnerability. This vulnerability allowed attackers to penetrate the digital systems of organizations using these products. Citrix indicated which measures organizations could take to temporarily fix the problems, but it did not yet have a definitive solution. One month later, on the 17th of January, the National Cyber Security Centre (NCSC) advised Dutch users to shut down their Citrix servers. Immediately in the weeks following the disclosure of the software vulnerability, attackers penetrated the digital systems of several organizations. These attacks continue to this day.

The Dutch Safety Board investigated what lessons can be learned from the way in which the parties involved dealt with the risks of vulnerabilities in Citrix software and other incidents where vulnerabilities in software were exploited by attackers. Both the prevention and response to such incidents were examined.

Citrix produces software that, among other things, allows employees to remotely log into their employer's ICT systems. This software is often an important part of the digital infrastructure because it forms the link between the external network (the internet) and the internal network. Virtually all organizations in the Netherlands use such software, whether they are governments, companies or other institutions. Examples include the national government and decentralized governments such as municipalities, but also hospitals, educational institutions, vital operators and other types of organizations. For example, the Citrix software in this investigation was used by 80% of the national government organizations and two-thirds of municipalities and provinces.

The incident with Citrix software and the other incidents analyzed in this report show that the urgency and scope of digital insecurity is increasing. The Netherlands is one of the most digitized countries in the world. Software plays a central role in the functioning of digital systems of organizations, but also contains vulnerabilities. Digitalization is therefore accompanied by ever-increasing risks for organizations that depend on software.

Because most organizations do not go public when they have been attacked, the total number of people affected by the incidents is unknown, but potentially large. For example, when the attacks through Citrix software began in January 2020, there were still over 500 servers of organizations where attackers could penetrate with relative ease. It is known that a municipality, hospital and several government organizations were affected. In addition, many government organizations and companies shut down their servers following the NCSC's advice. In July 2020, it appeared that at least 25 Dutch servers were still compromised.

Also for the other software products, it is not known how many attackers penetrated through that way. However, attackers have collected and published hundreds of thousands of login credentials through that route. The more recent attacks through SolarWinds, Kaseya and Microsoft Exchange are estimated to have affected thousands of organizations worldwide, including a Swedish supermarket chain and a Dutch logistics provider for a supermarket chain.

Since 2020, an increase in cyber attacks can be observed worldwide: from so-called 'ransomware' to economic espionage and (preparation for) sabotage. Attackers are still exploiting the vulnerabilities analyzed in this report to carry out attacks. Moreover, new vulnerabilities are constantly emerging. Software vulnerabilities are therefore an increasingly urgent and serious threat to digital and physical safety and security.

Incidents

The vulnerability in Citrix software allowed unauthorized users to gain access to all parts of the server on which it was running. Citrix learned that the method of exploiting the vulnerability had already been circulating publicly. Because the vulnerability was present in many versions of the software, it would take a long time for the manufacturer to release a final security update. For this reason the manufacturer decided to publish temporary mitigating measures first. From these temporary measures, attackers could easily deduce the nature of the vulnerability and how it could be exploited in an attack. In addition to the publication of the vulnerability and the mitigating measure on its website, the manufacturer was committed to directly warning as many customers as possible worldwide. The manufacturer could not reach all customers because it did not have all contact information.

In the first few months after the vulnerability was discovered, both Citrix and security researchers from the volunteer organization Dutch Institute for Vulnerability Disclosure (DIVD) gathered information about which Dutch organizations were still using vulnerable software on their servers, and were therefore at risk of an attack. Citrix and the DIVD shared their information with the NCSC, part of the Ministry of Justice and Security (JenV), in the expectation that it would warn the vulnerable organizations. In practice, the NCSC only warned the national government and vital operators; not the large group of vulnerable organizations that were not part of the national government and vital operators. The NCSC, which functions as the national point of contact in the Netherlands, does not have the responsibilities nor authority to live up to that.

In mid-January 2020, the situation and risks in the Netherlands escalated socially and administratively: the national crisis structure was scaled up, the NCSC initially advised organizations to consider shutting down their Citrix servers if possible, and there were questions from organizations about the measures to be taken. At the same time, there was uncertainty about the effectiveness of the measures. In response to an intelligence report from the Military Intelligence and Security Service (MIVD) and General Intelligence and Security Service (AIVD), and security advice from the AIVD, the Minister of JenV, and the Minister of Interior and Kingdom Relations (BZK) decided, in consultation with the National Coordinator for Counterterrorism and Security (NCTV), that the NCSC should issue the urgent advice to shut down servers ('comply or explain'). Organizations had to make their own trade-offs between the risk of an attack and the possible consequences

of shutting down their servers. They were not given all necessary and available information to make this risk assessment: whether they themselves had a vulnerable server and what the nature of the threat was.

Magnitude and urgency are increasing

Vulnerabilities in software are still a common route through which attackers penetrate into digital systems of organizations. Manufacturers of software also have less and less time to fix vulnerabilities before servers are attacked on a world-wide basis. In addition, attackers can also hit organizations directly or indirectly by attacking their chain partners (penetrating through the weakest link of customers and clients).

The incidents that were investigated show some notable similarities. Organizations, and the people who depend on these organizations, are exposed to digital insecurity because they use vulnerable software. The way in which manufacturers, organizations that use the software, and incident responders responded to the incidents shows that incident response is not yet a natural, self-evident, systematically built-in reflex. Each of the incidents illustrate that in many cases warnings do not reach these organizations. All incidents investigated by the Safety Board show that (voluntary) security researchers play a crucial role in incident response.

Barriers on a system level

Safe and secure software is the result of a continuous improvement process in a network of responsible parties, each of whom genuinely assumes their own responsibility, working together in effective structures based on mutual trust. The analysis of the incidents gives cause to address obstacles at the system level. A number of lessons follow from this.

Vulnerabilities in software arise during product's lifecycle

The incidents investigated by the Safety Board show that the use of software is inherently unsafe: when an organization uses software, this is always accompanied by risks. In practice, it is impossible to make a software product that does not contain vulnerabilities. What causes this, and who can contribute in what way to reducing the inherent insecurity?

Vulnerabilities in software arise during the development and the lifecycle of a product. The software manufacturer builds on an existing product by adding new features, which makes the software more complex. The programming language used, the reuse of existing components and (inconsistent) layers in the software architecture can also introduce vulnerabilities. The risks of these vulnerabilities increase if the product is used differently over time, taking on a more safety-critical role in digital systems.

For the manufacturer, safety and security issues that are the result of fundamental decisions in the product are an obstacle to tackle vulnerabilities at the root. This requires an investment in the form of money and capacity to solve the problem. The decision of the manufacturer in these situations to only patch the vulnerability ("apply a band-aid") with an update does not solve the underlying problem. The inherent safety and security problem remains.

There are manufacturers who encourage ethical hackers with rewards to search for vulnerabilities in software. Manufacturers also identify vulnerabilities themselves by conducting various tests. As a result, many vulnerabilities are identified, but it is unlikely that manufacturers will find *all* vulnerabilities.

Vulnerabilities in software increasingly provide a vector for attackers to penetrate into organizations' digital systems. Disclosing vulnerabilities thus poses a dilemma: it can help organizations better guard themselves against potential exploitation of the vulnerability, but it can also help attackers to detect and penetrate vulnerable servers. This underscores the importance of applying security updates (patches) released by manufacturers in a timely manner. But frequent patching and mitigation simultaneously poses a risk to organizations because it can lead to disruptions in digital systems or create new vulnerabilities. Organizations must therefore carefully think through the decision to patch, keeping in mind their specific IT landscape. In some cases, attacks begin within a few days of disclosure. As a result, organizations must respond in a short period of time.

The purchase and use of software by organizations
The unequal relationship between manufacturers and users of software products does not sufficiently enforce manufacturers to make efforts to manage safety and security risks. Currently, laws and regulations offer few options for governments and organizations to require manufacturers to safeguard cybersecurity in their products. Users don't always know how to draft requirements and hold a manufacturer accountable. Moreover, many users do not have the knowledge and manpower to set the right requirements and monitor them. Thus, vulnerabilities in software become a problem of the organization using the software. Offering software from the cloud shifts the responsibility to patch from the user to the manufacturer, but also introduces drawbacks for user such as less autonomy and privacy.

In terms of prevention and preparation for incidents, there are major differences in the level of resilience of organizations. Measures require that organizations make risk assessments. Not all organizations have the expertise and the capacity to sufficiently implement measures, or do not recognize the urgency of doing so. The government does not provide a collective foundation that helps organizations increase their digital resilience or an (institutional) infrastructure or network in which parties can collectively strengthen digital resilience.

Incident response
When software is used in organizations, incidents occur that need to be addressed as quickly as possible. However, incident response in the Netherlands is currently impaired by the fact that there is no national structure that ensures for all organizations to receive information about vulnerabilities in software in a timely manner. In particular, this involves information about which systems belonging to which organizations are vulnerable and at risk of being attacked, so-called 'victim information'. Using this information, an organization could be warned, even unsolicited, if its systems are vulnerable and at risk of being attacked.

The NCSC currently receives information for the entire Netherlands from inter alia manufacturers, NCSCs in other countries, intelligence and security agencies and others. However, the NCSC only shares this victim information with a select group of organizations, not with decentralized governments and also not with the majority of the Dutch private sector, and on the premise that an organization gives prior consent to be informed.

However, the national government is striving to improve the effective exchange of information that the NCSC is willing to share through the so-called *Landelijk Dekkend Stelsel (national coverage system), in which sectoral* organizations and (groups of) companies voluntarily share information crucial for responding to incidents. However, if the NCSC, as the national point of contact, receives information but does not share it fully, even with a national coverage system, not all potential victims will be warned. Security researchers are trying to fill this gap by - on a voluntary basis - scanning the Dutch Internet domain for vulnerable servers and sharing this information with parties who are in the position to issue security warnings. However, this was a fragile situation because they were not facilitated in this regard: neither by the government nor by other parties involved, which meant that their structural commitment was not secured.[2]

Learning from incidents
To improve safety and security, it is important to investigate what happened and what factors contributed to the occurrence of incidents. These insights are needed to learn in order to reduce the likelihood of future incidents and to limit the consequences by responding more quickly. The tradition of learning from incidents is still evolving in the digital domain. Organizations must report incidents involving vital operators and data breaches. Regulators currently conduct occasional investigations into digital incidents and indicate that they are not yet able to make coherent statements about the state of digital safety and security in vital sectors and processes. A platform for collaborative learning by manufacturers, organizations that use software, and other relevant public and private parties is lacking.

There are several barriers which impede learning from digital occurrences. For example, in current practice, many organizations do not come forward to announce that they have been attacked, in part because of fear of liability and reputational damage. Another barrier to learning from incidents is that investigations do not provide the explanations needed to improve the system. For example, it is not only relevant to know the extent to which an organization had implemented the expected basic measures, but also to understand why it is difficult for organizations to respond to attacks. Finally, organizations usually do not share the lessons from incidents outside their own organization or community.

2 In the meantime, this situation has changed: at the end of September 2021, the business community announced to set up its own alert system. Source: *FD*, Industry starts own alert system against attackers: 'government too slow', September 28, 2021.

Policy and international context

European regulations have been developed focused on incident response, and information security accountability for the financial sector. Soon there will also be regulation for the application of software in products (Internet of Things). For software itself, apart from regulation for certain applications, there is no international framework yet. An obstacle with this is that vulnerabilities are not only a problem for countries, but that countries also use vulnerabilities as a tool in their own activities, such as detection and intelligence activities. In addition, international cooperation is hampered by ideological differences, such as how the state relates to the Internet and how to deter attackers.

Digital dependency is increasing

Our society is digitizing at a rapid pace. The dependency on digital systems of individuals, organizations as well as society as a whole, has increased significantly in recent times. This became particularly visible during the corona pandemic: many organizations worked almost exclusively remotely. It is to be expected that (partially) working from home using digital devices will remain a constant factor in society.

Organizations use digital systems to be able to carry out their operations. These digital systems contain various kinds of software. By definition, software contains vulnerabilities, and these vulnerabilities are increasingly used by attackers as a vector to attack systems. The potential consequences of these attacks for individual organizations – or even national security as a whole – are not always foreseeable. This investigation describes and analyzes these negative effects.

As far as the Dutch Safety Board is concerned, the fact that software by definition contains vulnerabilities means that it is important to continuously pursue making software safer and more secure, and to respond adequately if vulnerabilities do become known. When using digital systems, organizations have a responsibility to safeguard safety and security. In doing so, they are also dependent on manufacturers who, in turn, are responsible for the safety and security of software they place on the market. In which way do manufacturers fulfil these responsibilities? And how do organizations manage their digital dependency and its consequences for other who in turn depend on them? What does this situation require from governments in their regulatory and supervisory roles, and which role can non-governmental organizations play?

These questions are particularly relevant now, considering the large number of cyber-attacks that have hit numerous organizations globally in the past years. These included organizations with crucial societal functions, such as governments, hospitals, universities, utility companies and distribution centers. Such attacks underline the current relevance of this investigation into security breaches as a result of vulnerabilities in Citrix software, which the Dutch Safety Board started in July 2020. The global cyber-attacks that serve as case studies in this report, demonstrate that these issues are now more serious and urgent than at the beginning of this investigation.

Vulnerable through software

Software is people's work: the computers that we use contain software that is made by people. Software manufacturers continually adapt existing and new software to the needs of their customers by adding new functionalities. Moreover, manufacturers update their software to fix safety and security issues (patching). Patching involves fixing vulnerabilities in software that can lead to software not functioning as intended, or that attackers can exploit to penetrate digital systems.

When fixing vulnerabilities as quickly as possible, the manufacturer's focus is initially on the *symptom* of the vulnerability. Fixing the fundamental *causes* of the safety or security problem demands fundamental changes. Due to the life span and size of software products, such fundamental changes cost a lot of time and money. Manufacturers currently receive little incentive to reduce the number of vulnerabilities, which is worrying for at least three reasons.

Firstly, societal interaction and the production of goods and services are increasingly dependent on digital systems. From food production to acute care, from transport to chemical industry, from water management to financial transactions: without software they are unimaginable. When digital systems do not function correctly due to vulnerabilities in software, the consequences are profound.

Secondly, most software plays a safety-critical role in these digital systems. The software the Board addresses in this investigation, acts as a gateway to an organization's digital system. It controls traffic between the systems within an organization and the employees and customers outside of the organization. Vulnerabilities in such software open the organization's digital gateway to unauthorized users and, in some cases, can even give unauthorized persons access to crucial processes, physical objects (buildings, infrastructure) and confidential information.

Thirdly, software is by definition central to digital traffic within and between organizations. Software is also practically always connected to other software in and outside organizations. Vulnerabilities in software can therefore affect the entire IT landscape of an organization and, as cases in this report show, even in the entire IT landscape of (parts of) sectors.

Secure software is primarily the responsibility of the manufacturer who places the software on the market. The unequal relationship between manufacturers and customers impairs the incentives for manufacturers to increase their efforts and be accountable to their customers. Buyers of software do not exactly know how the software works and which risks are involved. Or their organizations are too small to push or even force manufacturers to meet higher safety and security requirements. However, where the government is a customer and safety-critical software is involved, the relationship between customer and manufacturer can be considerably different.

These issues provoke the sharing and shifting of responsibilities for safe and secure software. An example would be where a manufacturer has software on the market that contains a vulnerability. The manufacturer offers a security update (patch), but the customer is responsible for actually implementing the update. In doing so, the manufacturer passes the risk of vulnerabilities onto customers, even though it is unlikely they are able to perform security updates literally thousands of times per year.

For secure software the efforts of manufacturers and buyers of software are not sufficient. It is necessary that different government agencies and companies work together to mobilize their expertise to assess the safety and security of software and strengthen their position as customers towards manufacturers. Moreover, it is fitting that the government, as guardian of digital safety and security, sets and enforces legal requirements for safety-

critical software in its role as regulating and supervisory body, but also as a customer that leads the way.

Considering the increasing digital dependency and rapid developments, setting requirements for software itself is not obvious. Legal measures will be outdated by the time legislation comes into force. However, enforcing procedural safeguards in the development process of software is certainly feasible. This could include compulsory participation in bug bounty programmes in which ethical hackers are rewarded if they find vulnerabilities, or independent software audits that take place before and after the software has been placed on the market. It is also important that, as with food safety, it is traceable which components software manufacturers use and where they come from and end up (traceability through a *chain of trust*). The latter is to prevent, for example, software components which have previously proven to be vulnerable from being reused in new software.

Response capacity

In practice, software is simultaneously vulnerable and essential for safeguarding safety and security and the functioning of society. This investigation demonstrates it is crucial to prevent vulnerabilities in software as much as possible. The investigation also shows that this is a matter of long haul, and that it is impossible to prevent *all* vulnerabilities. This means that, in addition to efforts to make software as safe and secure as possible, the response capacity is a crucial responsibility for the system of parties involved (manufacturers, governments, regulators and software buyers). Regarding safe and secure software it is also of great significance – similar to a fire being easier to fight when the building is fire resistant. Only by working together, both in a national and international context, and by exchanging information as optimally as possible they can fulfil their own responsibilities. This report describes a number of obstacles in the response capacity. These obstacles exist against the background that the National Cyber Security Centre (NCSC) in the Netherlands in practice functions as the national point of contact, but does not formally have the tasks nor responsibilities to live up to that.

Barriers

The investigated incidents show that different parties send victim information to the NCSC, but that not all victims are subsequently warned. In this report, the Dutch Safety Board describes the legal impediments that the NCSC and the Ministry of Justice and Security face, which are preventing all potential victims (solicited and unsolicited) from being warned. Many barriers can be traced back to the legal interpretation of the mandate of the NCSC and other government bodies, as well as the GDPR.

Strengthening the system

Despite recently announced policy measures, such as the strengthening of the Landelijk Dekkend Stelsel (national coverage system, or LDS) for sharing cybersecurity information, fundamental problems persist. To be able to safeguard digital safety and security of organizations, it is necessary to take away barriers and to transform to a new structure in which the imbalance between manufacturer and software user is eliminated, and in which information is exchanged as quickly and efficiently as possible. This calls for a different allocation of responsibilities (proportional to risk and action perspective); attitude (towards a principle of sharing by default) and structure (low-threshold, accessible and simple).

In addition, it is crucial for parties involved to learn from incidents collectively, both before and after software is placed on the market. Fear of liability and reputational damage stand in the way of necessary openness to learn collectively from incidents. If organizations and manufacturers work together to find explanations that are needed to improve the safety and security of the system and transparently share the lessons they have learned, they will be better able to manage the safety and security of digital systems through the pooling of experience and insights. Moreover, it stimulates that manufacturers work to continuously improve the safety and security of software. Through legislation and regulation that decreases the unequal relationship between manufacturer and user of software on the one hand, and through buyers of software who join forces on the other, incentives can be given to stimulate such a learning approach.

Cooperation will also make a more efficient use of the scarce capacity of cybersecurity expertise possible. For example, by giving CERTs and other sectoral organizations an auditory role towards manufacturers in addition to a response role. All parties involved should adopt this approach right from the software development phase. The preconditions for this are a partnership of parties that remains constantly alert, a free flow of information about software vulnerabilities, and a warning system for all potential victims.

The many cyber-attacks in recent years have demonstrated that a joint approach against digital insecurity of all parties involved is urgent and necessary. The gap between digital dependency and the threat level on the one hand; and the extent to which society is resilient to it on the other hand, is growing. Fast and fundamental intervention is necessary to prevent society from being disrupted. In this respect, combating cybercrime is an important final element for an effective approach to achieve safe and secure use of software. This requires central coordination from the government, based on a cross-domain vision and strategy on what is necessary to safeguard digital safety and security of organizations in the Netherlands.

RECOMMENDATIONS

This investigation shows that vulnerabilities in software lead to insecurities for organizations that use software, and for those who depend on these organizations. The gap between digital dependency and the threat level on the one hand; and the extent to which society is resilient to it on the other hand, is growing. Fast and fundamental interventions are needed to prevent society from being disrupted. That is why the Dutch Safety Board issues recommendations. The first recommendation aims to increase response capacity in the short term. The recommendations that follow aim, in the longer term, to strengthen the public and private system and introduce incentives to create a system in which manufacturers and buyers of software work continuously to make software safer and more secure.

To the Dutch Cabinet and to organizations in the Netherlands that use software:[3]

1. Ensure in the near future that all potential victims of cyber attacks are alerted quickly and effectively – solicited and unsolicited - so they can take measures for their digital safety and security. To this end, bring together public and private response capacity and ensure sufficient mandate and legal safeguards.

Note: In any case, this concerns information about which systems of which organizations are vulnerable and at risk of being attacked (so-called 'victim information'). Currently, the legal interpretation of the GDPR (IP addresses as personal data) and the Dutch Security of Network and Information Systems Act (Wbni) (mandate of the NCSC limited to national government and vital operators) prevents the National Cyber Security Centre (NCSC) from warning all victims they receive information about, and from proactively collecting this information (scanning).

To the European Commissioner for Internal Market and the European Commissioner for A Europe Fit for the Digital Age:

2. Ensure that your initiatives to legislate for safer and more secure software lead to a European regulation that establishes the responsibility of manufacturers and provides insight to buyers of software in how manufacturers assume this responsibility. Establish that manufacturers are liable for the consequences of software vulnerabilities.

Note: Essential elements of this regulation include – but are not limited to – mandatory participation in bug bounty programmes, guidelines for independent audits, vulnerability

3 For practical reasons, the Dutch Safety Board addresses the government in its role as user of software through the State Secretary of the Interior, the Interprovincial Consultative Council, the *Vereniging van Nederlandse Gemeenten* (Association of Netherlands Municipalities), and the *Unie van Waterschappen* (Union of Water Boards). The other organizations, including health care, education, vital operators and other businesses, are addressed by the Dutch Safety Board through employers' organizations involved in the SER, such as: VNO-NCW, MKB-Nederland and LTO Nederland.

reporting, traceability, recalls, and the sharing of lessons learnt from cyber-attacks. Legislation such as the GDPR has proven that European regulations in the digital domain are feasible and effective.

To software manufacturers collectively:[4]

3. Develop good practices with other manufacturers to make software safer and more secure. Include a commitment to these practices in contracts with your customers.
4. Warn and help all your customers as quickly and effectively as possible when vulnerabilities in software are identified. Create the preconditions necessary to be able to warn your customers.

Note: The responsibility and possibilities for making software safer and more secure, and for warning customers primary lies with the manufacturers themselves.

To the State Secretary of the Interior and Kingdom Relations and the Minister of Economic Affairs and Climate Policy (for the benefit of all organizations and consumers in the Netherlands):[5]

5. Encourage that Dutch organizations and consumers jointly formulate and enforce safety and security requirements for software manufacturers. Ensure that the government plays a leading role in this. Proceed on the basis of the principle: collective cooperation where possible, sector-specific where necessary.

Note: It is necessary for buyers of software to join forces in order to strengthen their position towards manufacturers and jointly deploy the scarce cybersecurity expertise as efficiently and effectively as possible. A number of Dutch banks is already cooperating in this matter.

To the Dutch Cabinet:

6. Create a legal basis for the management of digital safety and security by the government, by analogy of the Dutch Government Accounts Act (*Comptabiliteitswet*).
7. Require all organizations to uniformly account for the way in which they manage digital safety and security risks.[6]

Note: The way in which governments and companies manage and account for the risks that are associated with digitization is as yet noncommittal. Fragmentation of responsibilities impairs decisive action. It is essential that a comprehensive system is put in place to help organizations to manage digital safety and security in a systematic and

4 This recommendation is addressed to all software manufacturers. For practical reasons, the Dutch Safety Board addresses the manufacturers involved in the incidents described in this investigation, the communities of the open source projects involved and the (members of the) Business Software Alliance trade association.

5 See footnote 2. Because of the relevance of safe and secure software to end users (including consumers), the *Consumentenbond* (Consumers' Association) will also be addressed. And the Chamber of Commerce for support to organizations.

6 It is within reason to align with existing structures and obligations in the 2016 *Comptabiliteitswet* (applicable to governments), Civil Code (non-listed legal entities), further regulations on auditing and other standards (NV COS) from the NBA and harmonized legislation for public limited companies from the European Union.

effective manner. Possible elements include an unambiguous mandate for government CISOs, supervision that is entrusted to the minister responsible, and mandatory accountability for all organizations regarding the management of digital safety and security risks, through annual reports and as part of the auditor's report.

ir. J.R.V.A. Dijsselbloem
Chairman Dutch Safety Board

mr. C.A.J.F. Verheij
Secretary Director

ABBREVIATIONS AND DEFINITIONS

AAN	Anti Abuse Network
ABDO	General Security Requirements relating to Defence Orders
ADC	Application Delivery Controller
AIVD	General Intelligence and Security Service
AP	Dutch Data Protection Authority (Dutch DPA)
BIG-IP	A line of products for access control, security etc. by F5 Networks.
BIO	Government Information Security Baseline
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
Citrix	Software manufacturer, vendor
Citrix NetScaler	Software product for access control and security from Citrix
CMDB	Configuration Management Database
CSIRT	Computer Security Incident Response Team
CSR	Cyber Security Council
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DIVD	Dutch Institute for Vulnerability Disclosure
DTC	Digital Trust Center
F5	Software manufacturer, vendor
Fortigate	An access control and security product from Fortinet
Fortinet	Software manufacturer, vendor
(Fungible) thing	A tangible object that can be controlled by humans. Based on case history, heat information and electricity are also recognized as things[7]
GDPR	General Data Protection Regulation
IAo	Interdepartmental Coordination Consultation
ICCb	Interdepartmental Crisis Management Committee
ICO	Government Cybersecurity Procurement Requirements
IoT	Internet of Things
ISAC	Information Sharing and Analysis Center

7 Article 2 Dutch Civil Code Book 3.

ISO 27001 standard	Worldwide recognized standard for information security management
IT	Information Technology
LDS	National Coverage System for sharing cybersecurity information
MFA	multi factor authentication
(Ministry of) BZ	Ministry of Foreign Affairs
(Ministry of) BZK	Ministry of the Interior and Kingdom Relations
(Ministry of) EZK	Ministry of Economic Affairs and Climate Policy
(Ministry of) JenV	Ministry of Justice and Security
MIVD	Military Intelligence and Security Service
NCC	National Crisis Centre
NCSC	National Cyber Security Centre
NCTV	National Coordinator for Security and Counterterrorism
NDN	National Detection Network
NIS directive	Network and Information Security directive
Occurrence	An occurrence resulting in death or personal injury or material damage or damage to the environment, and an occurrence that led to a risk of such a consequence[8]
OKTT	'Objectief Kenbaar Tot Taak', an organization that objectively has the task to provide other organizations or the public with threat information involving network and information systems
Palo Alto	Software manufacturer, vendor
PoC	Proof of Concept
PSIRT	Product Security Incident Response Team
Pulse Secure	Software manufacturer, vendor (part of Ivanti since December 2020)
SaaS	Software as a Service
SDLC	Secure Development Lifecycle
SSL VPN	Secure Socket Layer Virtual Private Network
Threat information	Specific information about threats that are specifically aimed at certain parties or in respect of which certain parties or systems are vulnerable, for example data regarding (potential) victims (victim information), perpetrators (perpetrator information) or vulnerable systems, for example in the form of IP addresses.[9]

8 Article 3 Dutch Safety Board Act.
9 Dialogic and TU/e, *Information exchange nationwide cybersecurity network* on behalf of WODC Research and Documentation Centre, 14 October 2020.

VPN	Virtual Private Network
Vulnerability	A weakness in software that can be exploited by attackers to penetrate a network
Wbni	Security of Network and Information Systems Act

The Cybersecurity Glossary was used for making this list of abbreviations and definitions.[10]

10 https://www.digitaltrustcenter.nl/cybersecurity-woordenboek (in Dutch).

1 INTRODUCTION

1.1 Background

The immediate background to this investigation is a vulnerability in software from Citrix, which had consequences for organizations that used that software. On 17 December 2019, Citrix issued a public notice that a number of their software products contained a vulnerability which meant that attackers could penetrate the digital systems of organizations that use these products.[11] Citrix then identified the measures that could be taken to temporarily fix (mitigate) the problems, but was unable to offer a definitive solution (patch) for the vulnerability that had arisen. On 17 January 2020, The National Cyber Security Centre (NCSC) advised Dutch organizations to shut down their Citrix servers. As a consequence of this software vulnerability, attackers were able to penetrate the systems of various government organizations and companies.[12]

The American company Citrix manufactures software that among others allows employees to remotely log into the corporate IT systems of their employer. This software often forms a critical component of the digital infrastructure, as it represents the link between the external network (Internet) and the internal network. Much of the national government of the Netherlands, as well as local government authorities, hospitals, educational institutions, vital operators and other corporate entities use Citrix software.

These occurrences (in short security breaches related to Citrix software vulnerability) demonstrate that society's digital infrastructure is vulnerable and security problems can lead to unsafety.[13] For their safety, citizens depend on the way in which and the extent to which organizations manage safety. That is why the Dutch Safety Board decided to investigate what happened at the time of the occurrences and how the risks were and are being managed, both in preventing and combating this incident and similar ones.

11 Citrix, *CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance*, 17 December 2019. https://support.citrix.com/article/CTX267027
12 This problem is still very much current. Attackers have still penetrated parts of some systems.
13 Section 2.1 addresses the concepts of safety and security.

1.2 Objective

The objective of this investigation is to identify safety lessons that will help the responsible parties improve the management of risks caused by vulnerabilities in software. The lessons are among others addressed to software manufacturers, organizations that use software, as well as governmental and other organizations that contribute to the prevention and tackling of these kind of software vulnerabilities and security breaches.

This investigation was launched in response to the Citrix software vulnerability as a typical example of an occurrence resulting in risks of this kind, as further demonstrated by other cyberattacks since 2020.

1.3 Investigation questions

The Dutch Safety Board assumes that the way in which software manufacturers, organizations that use software, the government and other (partially non-governmental) organizations manage cybersecurity risks,[14] determines the extent to which these occurrences can take place and the extent to which these occurrences affect the physical and social safety of citizens Based on this assumption, the Safety Board formulated the following investigation question:

> What lessons can be learned from the way in which the stakeholders dealt with the risks resulting from the Citrix software vulnerability that was discovered in December 2019?

Sub questions:

1. How could the security breaches occur within the organizations as a result of the vulnerability in Citrix software, and what were the consequences?
2. How were these risks assessed and what measures were taken to prevent the occurrences undesirable consequences (risk governance):
   a. by the software manufacturer and organizations that purchase and use the software;
   b. by the public administration / the government and non-government parties?
3. What is needed from parties involved in order to reinforce the system of risk governance and risk management?

14 The way in which organizations manage their risks is also known as risk governance.

1.4 Scope and focus of the investigation

Software vulnerabilities that result in security breaches within organizations with possible safety consequences

This investigation is restricted to occurrences in which the digital systems of an organization contain a security breach and in certain cases are penetrated as a result of the vulnerability in the software used, as occurred with the vulnerability in the Citrix software. The focus of the investigation is on software that forms a link between the Internet and the internal network of the organization, such as software used for establishing secure links for homeworking and remote (online) cooperation. Occurrences in which attackers penetrate the digital systems of an organization in some other way, for example via phishing, or rendering the system inaccessible for example via a DDoS attack are beyond the scope of this investigation. Also beyond the scope of the investigation are occurrences where there is an IT outage[15] without an attack taking place. The investigation also focuses on enterprise software, not consumer software. We do, however, include the consequences for citizens in the research.

Detailed reconstruction of the Citrix occurrence

The vulnerabilities in the Citrix software and its consequences form the starting point for the investigation. The reconstruction of the occurrence involving Citrix software occupies a central position within the investigation. What happened, and who was aware of what information at what time? This detailed reconstruction was essential in order to be able to analyse the direct and underlying factors.

No technical-forensic investigation

The Dutch Safety Board itself undertook no technical-forensic investigation into the vulnerabilities in the software and the systems that as a result of these vulnerabilities were or were not penetrated. Nonetheless, wherever possible and meaningful, use was made of the outcomes of technical forensic investigations by security companies and other organizations involved.

Generalization to occurrences caused by software vulnerabilities

In order to be able to put the findings in a broader context on how the stakeholders (attempt to) prevent vulnerabilities in software and to mitigate their consequences, the Safety Board investigated a number of other occurrences in which vulnerabilities in software had major consequences for the cybersecurity of organizations and also the safety of citizens. These included occurrences with software intended for establishing a secure link (VPN software).[16] The Safety Board also included information on occurrences that took place during the course of the investigation. It investigated these occurrences based on public sources.

15 See for example Dutch Safety Board, *Patient safety during IT outages in hospitals*, 2020.

16 VPN software from PulseSecure/Fortinet/Palo Alto, BIG-IP from F5. Occurrence that took place during the course of the investigation: SolarWinds/Sunburst/Supernova and Microsoft Exchange, PrintSpooler, Kaseya. These occurrences are discussed in section 3.3.

Interaction between public administration and other parties

In this investigation, the Safety Board focused specifically on the role of the public administration that is affected by this subject in several different ways: as an organization that buys and uses software, as the party able to regulate the market for software and as the party able to trace and subsequently enforce the exploitation of software and digital systems. At the same time, as described in the investigation questions, we also recognize that other parties have an essential role in safeguarding safety. For that reason, the investigation is focused on the interfaces and interaction between public administration and other organizations. This relates, for example, to the way in which the public administration works to direct the way that manufacturers produce safe software, and how organizations use that software. Public administration also plays an important role in the approach to incident management, both by public, private and non-governmental parties. In analysing the interfaces between the public administration and other parties, the Safety Board took previously published recommendations by e.g. The Netherlands Scientific Council for Government Policy and the Cyber Security Council into account.

1.5 Investigation approach

The Safety Board took the following approach to this investigation. We started by collecting primarily public information.[17] We supplemented this information by addressing written questions to the parties involved regarding the vulnerabilities, their working methods in software development and incident management, and by consulting experts. The majority of parties cooperated, but a number of manufacturers failed to respond to our request to answer questions. In total, around 1.200 documents were analysed for the entire investigation. In addition, we held more than 40 interviews with persons involved at the manufacturers, and at public, private and non-governmental organizations that use the software, or are responsible for incident management. Appendix A contains a more detailed explanation of the way in which the investigation was carried out.

For the theoretical framework (concepts, definitions, mechanisms, etc.), the Safety Board made use of various publications on technical, administrative and economic aspects of cybersecurity.[18] To be able to answer the investigation questions, we drew up a reference framework, in which we describe what the Safety Board expects from the various stakeholders, and how these parties could be able to make a reasonable contribution to secure digital systems. Based on this reference framework, we were able to identify the bottlenecks present, and the way in which the responsibilities for secure digital systems are currently fulfilled.

17 In particular publications from the manufacturers (CVE, notifications on the website), governments and other authorities (policy documents, notifications from CERTs), ethical hackers (articles, presentations), scientific publications (specialist/social) media articles.

18 Ellis R. and V. Mohan, *Rewired: Cybersecurity Governance,* 2019 a.o.. Anderson, R., *Security Engineering,* 2020. and other publications on security engineering.

To reconstruct the course of events, we made use of a timeline analysis. To obtain a clear picture of the factors that potentially had an influence, we analyzed the accident using the Tripod-Beta accident analysis method. We also analysed the system within which the occurrences took place: we mapped out which parties were involved according to an environment and stakeholder analysis and the CAST/STAMP method. This method generates insights into the hierarchical lines, roles and responsibilities of the parties involved and the relationship with legislation and regulations. We applied this method to the way in which the parties involved managed the risks of software vulnerabilities, how they shared information and managed the incident.[19]

Within the analysis of the occurrences, the Dutch Safety Board made a distinction between the following phases:

- occurrence and prevention of the vulnerability and preparation for the discovery of vulnerabilities (see section 4.1);
- the purchase and use of software and preventive measures by organizations using software, see section 4.2;
- incident management, in particular information sharing, see section 4.3;
- the way in which lessons are learned from incidents, see section 4.4;
- developments in (international) regulations, see section 4.5.

1.6 Reference framework

During its investigation, the Board draws up a reference framework. The frame of reference shows how – according to current insights – a certain safety risk can be controlled. In doing so, the Dutch Safety Board draws on experiences in the Netherlands and other countries, as well as on its own experience in other domains. The frame of reference was used to reflect on the current working method regarding security vulnerabilities in software vulnerabilities and the options available to strengthen them.

The complete frame of reference aimed at safeguarding digital security is included in Appendix C. Themes in this frame of reference are product safety of software, prevention of and preparation for incidents and incident response (response). The way in which lessons are learned from incidents is also a theme within this frame of reference. Important actors in the field of digital security are manufacturers, organizations that purchase and use software, national and international governments and other organizations that contribute to regulations and incident response. The frame of reference describes what the Board expects from the various actors.

19 Hendrick, K. & J. Benner, . *Investigating accidents with STEP. Dekker*, New York, 1987. Stichting Tripod Foundation. *Tripod-Beta User Guide*. Stichting Tripod Foundation, Vlaardingen, 2008. Leveson, N., M. Daouk, N. Dulac & K. Marais, 2003. *Applying STAMP in Accident Analysis*. MIT, Cambridge, MA; Leveson, N., 2004. 'A New Accident Model for Engineering Safer Systems'. In: *Safety Science*, Vol. 42, No. 4, 2004.

Essential elements in the frame of reference are the following:

- Software plays a safety-critical role in the digital systems of organizations: safety must be central in the development and production of software (safety and security by design);
- Manufacturers are responsible for preventing software containing vulnerabilities as effectively as possible and for helping organizations as much as possible to prevent and combat the consequences if a vulnerability is found;
- Organizations can encourage manufacturers to make software as safe as possible through the process of purchasing and deploying software. It is important that manufacturers provide organizations with the information and position to be able to make this assessment. It is important for organizations that they regard and treat secure ICT as a crucial element - but also as a risk - to their organization. Organizations must have insight into the way in which they themselves run risk and how they can manage it;
- Parties are mutually dependent on each other. Ensuring digital security is therefore a collective social task for which the national government bears system responsibility, should encourage collaboration and the sharing of information and remove barriers as much as possible.

1.7 Contents and reading guide

Chapter 2 provides an explanation of the most important terms and concepts relevant to this investigation.

Chapter 3 answers the question how such incidents occur, their consequences and how the risks were managed. This was done by describing and analysing in detail the occurrence that led to this investigation being carried out: the vulnerability in the software from Citrix and its consequences for the organizations using this software. To be able to broaden the scope of the findings from the analysis of that occurrence, we also describe and analyse a number of other comparable occurrences, in chapter 3.

In chapter 4 we describe the underlying factors that influence the origin and consequences of the occurrences described in chapter 3. In that description, we make a distinction between the process in which software is manufactured, the process in which organizations select specific software for purchase and the processes that take place once a vulnerability in the software is identified (incident management). In addition, we consider how lessons are currently learned from digital occurrences, and the (international) policy context applicable to digital occurrences.

Chapters 5 and 6 respectively contain the conclusions and recommendations issued by the Safety Board to the various parties so they can improve digital safety and security. The appendices contain the background to the investigation, such as the accounting for the investigation (appendix A), the reactions of the parties involved following examination of the draft report (appendix B) and a number of appendices with more in-depth information about the subjects discussed in the report.

2 RELEVANT CONCEPTS EXPLAINED

This chapter contains background information essential to understanding and interpreting the description and analysis of the occurrences in the subsequent chapters. The chapter starts with an explanation of what digital systems are, how vulnerabilities can arise that threaten safety and security, and how risks can be prevented and managed. A number of definitions and mechanisms central to this investigation are described. Some of these definitions can be interpreted in several different ways. Here we describe our interpretation in this investigation.

2.1 (Digital) system[20]

A digital system is a term that can have a narrow or a broad meaning. In our investigation, we allocate a broad meaning to the term, such that it has the following definition. Firstly *the technology*, consisting of hardware (for example computers, printers and networks) on the one hand and software on the other, in combination with the physical environment, such as the building. Secondly, *the people* who use the technology to enable them to undertake specific activities. Thirdly *the organization* within which the technology and people are found. Finally, the system is located in a *complex environment*. The term complex environment refers to the mutual interaction between the components already referred to with society, for example regulations, incentives, (re)actions and the Internet. This combination of elements is also referred to as a socio-technical system. We explain a number of the separate elements of this system in greater detail, below. The system is reproduced in the figure below.

20 This investigation employs the definitions and concepts from the Security Engineering and Systems Engineering domains.

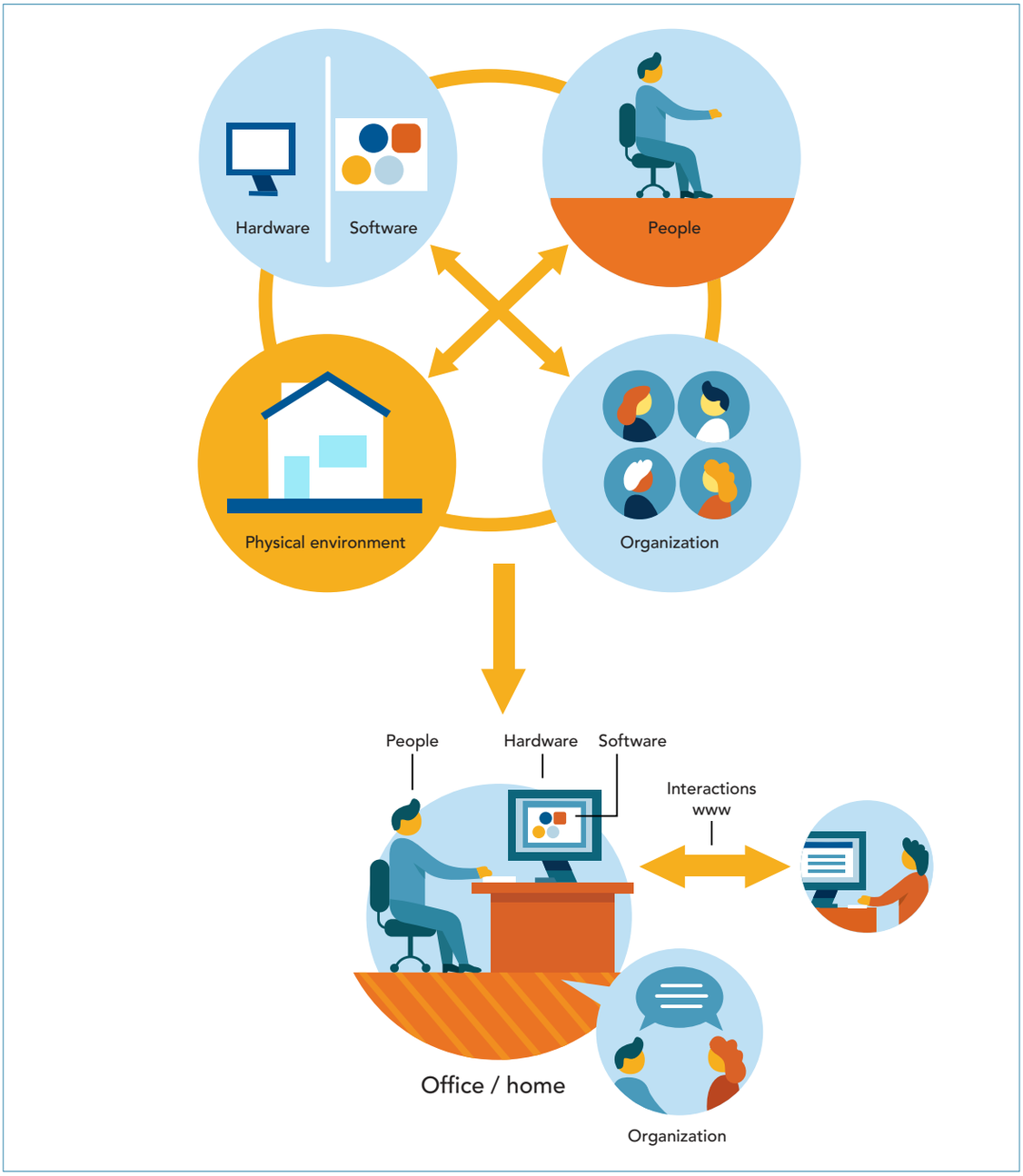


Figure 1: Socio-technical system.

2.1.1 Technology: network, hardware, software[21]

Digitalization requires the establishment and maintenance of an IT foundation: the combination of IT components (hardware and software) that form the digital foundation for the organization. Hardware refers to the electronic and mechanical components of a digital system; the tangible elements. Various hardware components such as PCs, printers and servers (network computers for the storage and transmission of information) are linked together: together they form a network. Software is the computer code that makes it possible for the hardware components to exchange information. Each digital foundation consists of a number of universal components: computing power via the *processing*

21 Anderson, R. *Security Engineering*, 2020; *Cisco CCNA 200-301 Official Cert Guide*, 2020.

units, a transport network to be able to transfer data from one component to another, and *storage servers* where data is recorded, stored and can be retrieved. This foundation comprises a series of layers: the operating layer that controls the hardware, the functions that the digital system must fulfil (applications) and the interaction with the user.

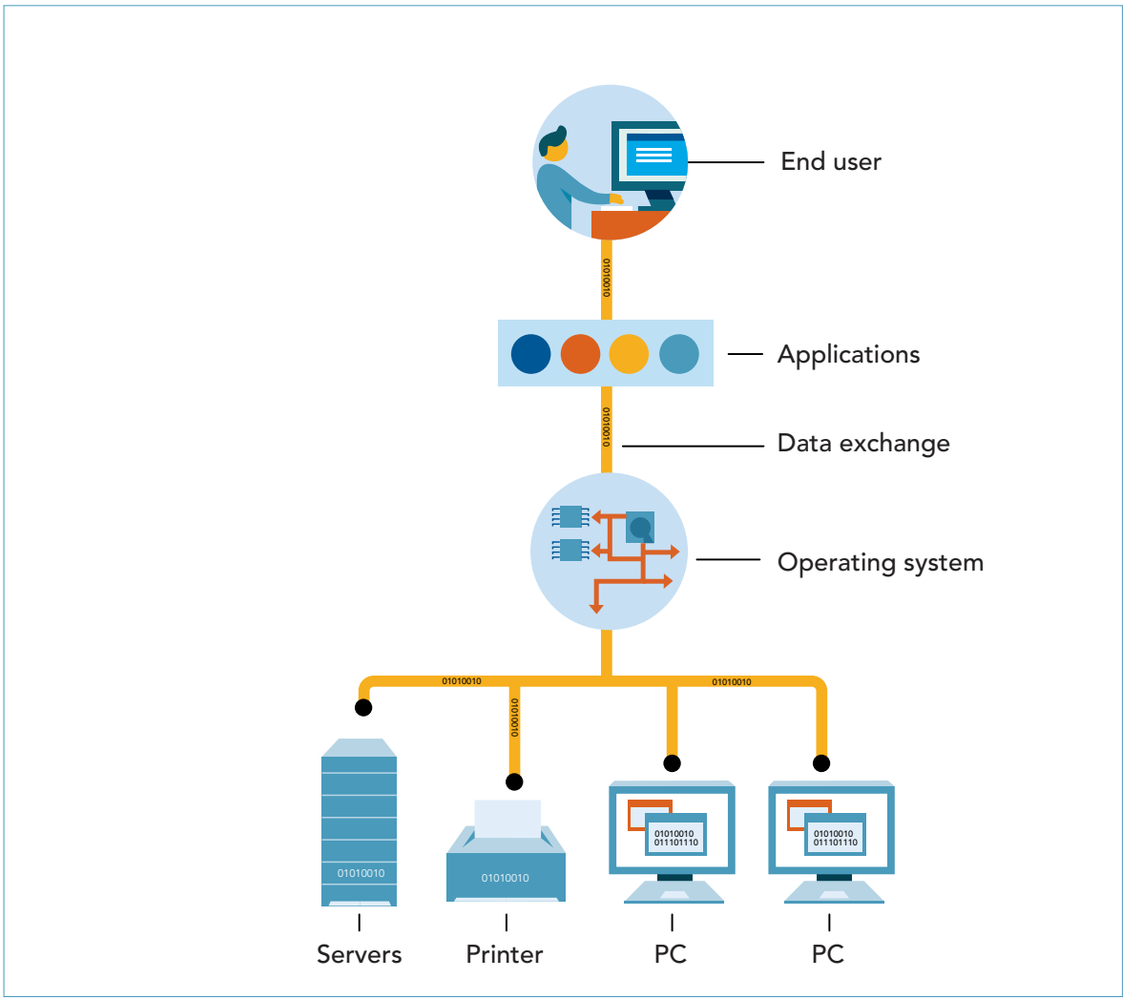


Figure 2: Diagrammatic representation of the structure of an IT foundation.

In the majority of organizations, information has to be shared with others outside the organization. For that reason, the organization's network is often linked to the Internet (the digital outside world). For the organization, it is crucial / unavoidable that authorized individuals be able to exchange information with one another, both inside the network and beyond, as effectively as possible. This fact however also makes digital systems vulnerable. As far as possible, unauthorized persons must be kept out.

From the perspective of the user of a digital system within an organization, the system appears as follows. The user works on a device (such as a PC or laptop) that is connected to the company network via a cable, or via a wireless connection. The company network operates beyond the vision of the user and in essence generally has the following appearance. The network consists of a number of servers. These are devices that fulfil specific functions, such as sending and receiving emails, storing files and databases, and facilitating websites or other applications.

The user of the digital system (who may be an employee or an external user, such as a citizen in the case of a municipality system, or a GP at a hospital) wishes to make use of a specific function of the digital system. If he or she is not directly connected to the digital system, the access will take place remotely. Via the Internet, the user makes a connection with the digital system via a (software-based) access gateway, in many cases a webpage onto which the user logs in, whereby the system can check who the user is and determines which access rights will be awarded.

One or more firewalls are generally installed between the digital system and the Internet. The network can also be divided up into segments, between which firewalls can be installed (network segmentation). A firewall can be hardware or software that observes the traffic to the network via the Internet, and that blocks certain types of traffic. The manager of the digital system determines which traffic the firewall should block.

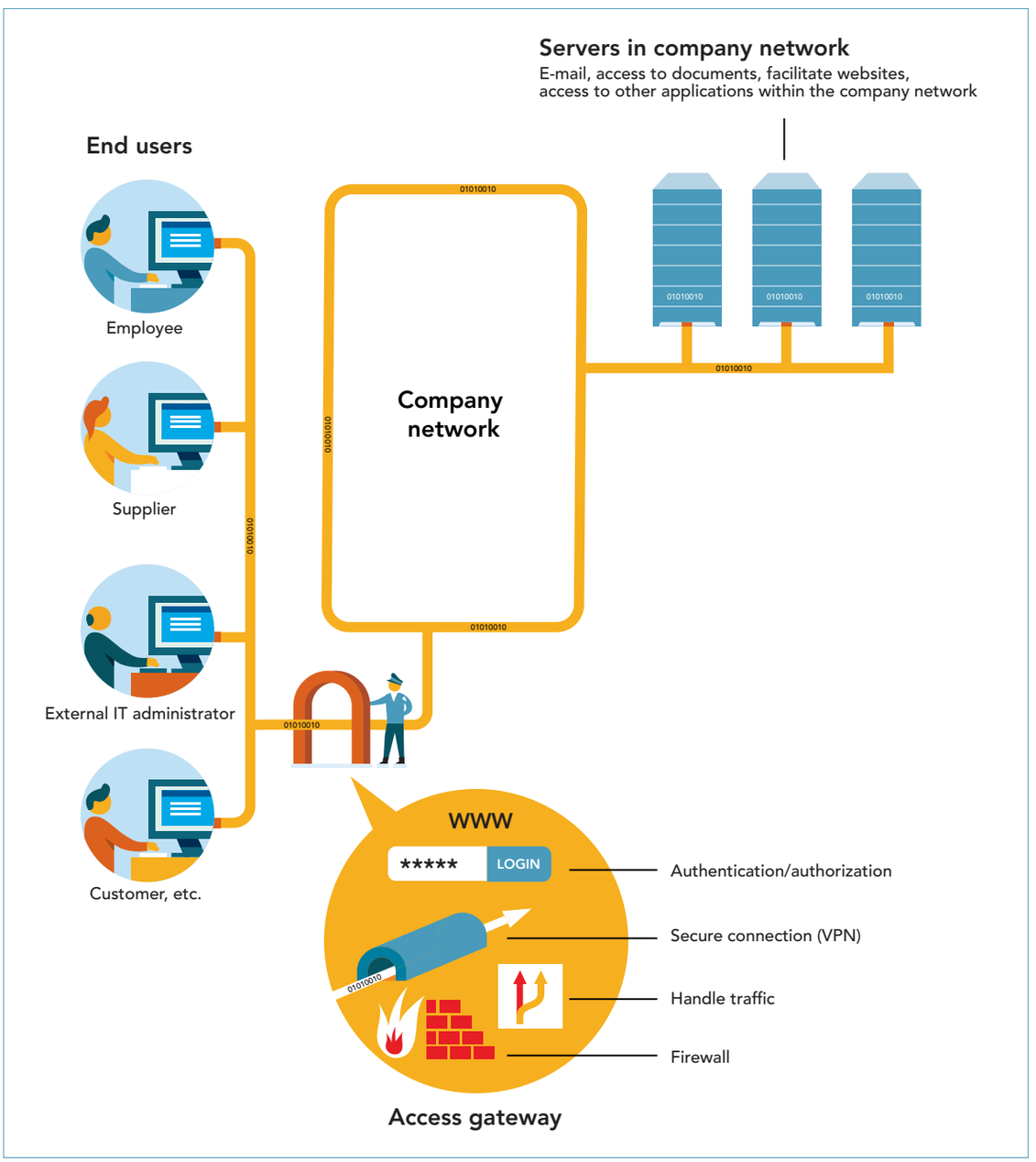


Figure 3: Access gateway to the digital system.

2.1.2 People and organization

A digital system is not exclusively a question of technology. The reason for this is that people use the technology to perform their tasks and activities within the context of the organization. In addition to the technology, the actions of people using and managing the technology influence the performance and security of the systems. Management of the digital system is also linked to various, sometimes conflicting interests and priorities within the organization. This for example emerges when the maintenance of the digital system takes place at the expense of the availability of the system. Or when choices are made to invest in expansion or replacement of software and other system components. These organizational processes are therefore also part of the digital system.

Design and production

The life cycle of a digital system and the software that is used starts with its design and production. That is a process that is carried out by people within the context of an organization as well, in this case the software manufacturer. There may be conflicting interests, such as the choice of how much time and resources can be invested in checking and testing the software before a new version is released. In addition, we must realize that the internet and the software that people and organizations use have been developed from the desire to be connected. Safety and security were less relevant and did not initially play a central role in the development and production. In section 4.1 we discuss the design and development of software in relation to vulnerabilities within the software.

Purchase and use

One of the relevant organizational processes is the purchase of software, how the user determines whether the software meets its requirements, including safety and security requirements, and the consequences for the vendor if it turns out software does not meet the requirements (liability for the consequences). One security requirement often imposed by end users on suppliers is the authority to carry out penetration tests.[22] An organization is able to carry out its own penetration test (abbreviated to pen test), have a pen test carried out by a second party or can request the manufacturer to provide a report of a penetration test via a third party. These pen tests can be focused on testing a specific product or the entire network, and can be undertaken both externally (from outside the network) or internally (whereby the pen tester attempts to gain access to systems from inside the network).[23]

Software that fulfils the function of facilitating a link to the outside world (such as Citrix software or VPN products) is often the target of attackers; this makes testing important. At the same time, vulnerabilities in other products that have an external link (for example for retrieving updates) can also be used by attackers to penetrate systems.

22 A pentest is a security check whereby an external test for vulnerabilities is carried out, followed by an attempt to hack the system via these vulnerabilities.

23 PT Security, *Penetration Testing of corporate information systems*, 2020.

After an organization has purchased software, it is subsequently commissioned as part of the organization's operating system. In this phase, organizations can introduce a series of measures and processes to secure their operating systems, and to prepare for incidents.[24] Below a number of these measures and considerations are explained that can be important in mitigating the risks of incidents following a software vulnerability.

Reducing dependency

One way of reducing the dependency on a particular product is to purchase a second software product. If one product no longer functions, or can no longer be used securely, it is possible to then switch to the other product, so that organization's processes can continue. This kind is known as a redundant system.

Another way of reducing dependency on a particular software product is to structure the network in such a way that there is no *single point of failure*. In other words, if one system fails, this does not mean that the entire network fails. When selecting software and designing a network, it is therefore important to chart out the dependencies, and to make a deliberate assessment of the potential risks, when using particular systems. This can help reduce the impact of incidents.

Prevention and detection

Different measures can be taken to prevent and detect attacks. An example of such a measure is to restrict external access to the systems of an organization by installing a firewall.[25] A firewall is a machine installed between a network and the Internet, which monitors traffic, and prevents potentially harmful traffic.[26]

As well as measures aimed at preventing attackers, there are also measures that organizations can take to mitigate the impact of incidents if they do occur. Network segmentation is one measure that can be taken to mitigate the consequences of possible system penetration. A segmented network is divided into multiple subnetworks, each of which are protected and are able to halt unnecessary traffic, for example on the basis of a firewall. If a network is not segmented, an attacker will have access to the entire network, once it has made its way inside. The more highly segmented a network is, the more barriers an attacker will have to overcome in attempting to penetrate the organization's entire system. In this way, any attacker remains isolated in a particular segment of the network.[27]

24 https://www.ncsc.nl/onderwerpen/basismaatregelen, consulted on 16 July 2021.
25 https://www.ncsc.nl/onderwerpen/basismaatregelen, consulted on 17 July 2021.
26 Anderson, R., *Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition,* December 2020.
27 Kambic and Fricke, *'Network segmentation: concepts and practices'*, Software Engineering Institute, https://insights.sei.cmu.edu/blog/network-segmentation-concepts-and-practices/, consulted on 16 July 2021.
Holt, *'Security Think Tank: Benefits and challenges of security segmentation'*, Computer Weekly, https://www.computerweekly.com/opinion/Security-Think-Tank-Security-segmentation-benefits-and-challenges, consulted on 15 July 2021.

In order to identify attacks on the operating system, many organizations invest in detection capabilities. *Logging* of systems is of crucial importance in detecting attackers. Logging is the process of recording activity on systems in log files. In this process, it is possible to establish alerts for certain activities and characteristics (signatures), for example suspicious login attempts.[28] Logging is also essential in allowing investigations to be carried out following an incident. If no log data are available, or if an attacker is able to alter this information, it is impossible to trace the movements of an attacker in the network.

2.2 Vulnerabilities and security breaches[29]

Software used in organizations' networks can contain *vulnerabilities*.[30] Attackers can exploit these vulnerabilities to penetrate the network. Vulnerabilities can also have other unwanted consequences, such as unintended damage caused by a user.

Vulnerabilities can among others be created during the programming of the software, or when different components are combined. Vulnerabilities are sometimes discovered by the manufacturers of the software themselves, by organizations who purchase and use the software or by hackers[31] who search for vulnerabilities on behalf of manufacturers, organizations, for their own reasons or on behalf of third parties (for example state actors).

Ethical hackers[32] can inform the manufacturer and/or authorities of the vulnerabilities identified (coordinated vulnerability disclosure or responsible disclosure). They generally also show how the vulnerability can be exploited in order to penetrate a vulnerable system. This demonstration method is also known as Proof of Concept code.[33]

The manufacturer can subsequently register the vulnerability and have it recorded in the Common Vulnerabilities and Exposures (CVE) database. This is a database listing vulnerabilities that have been discovered and published by organizations all over the world. Security professionals can among others use this database for uniform communication about vulnerabilities and coordinating and prioritizing the ways to tackle different vulnerabilities.[34] Organizations can also add vulnerabilities they discover to the CVE database. Analysts then allocate a score to the CVE that indicates the seriousness of the vulnerability. This score is calculated according to the Common Vulnerability Scoring System (CVSS).

28 https://www.ncsc.nl/onderwerpen/loginformatie, accessed on 16 July 2021.
29 See publications of Mitre (CVE/CWE), OWASP, Security Engineering Anderson and Google (framework for secure software).
30 Hardware, people, physical environment and organizations can also contain vulnerabilities. This investigation relates to vulnerabilities in software.
31 A hacker is someone who breaks into a computer system. The aim is to identify security vulnerabilities.
32 Ethical hackers or whitehat hackers work with the positive intention of identifying security vulnerabilities and thereby improving safety.
33 Based on this Proof of Concept code, an attacker can write code that can be used to actually exploit the system. This is called an exploit.
34 https://cve.mitre.org/

Attackers sometimes find the vulnerability before the manufacturer or ethical hackers, and in some cases the Proof of Concept code or other exploit code is already announced before the manufacturer has been able to publish a patch for the vulnerability. Attacks of this kind are referred to as *zero day exploits*. In that case, attackers exploit the vulnerability before the manufacturer has been able to inform those who bought the software of the vulnerability.

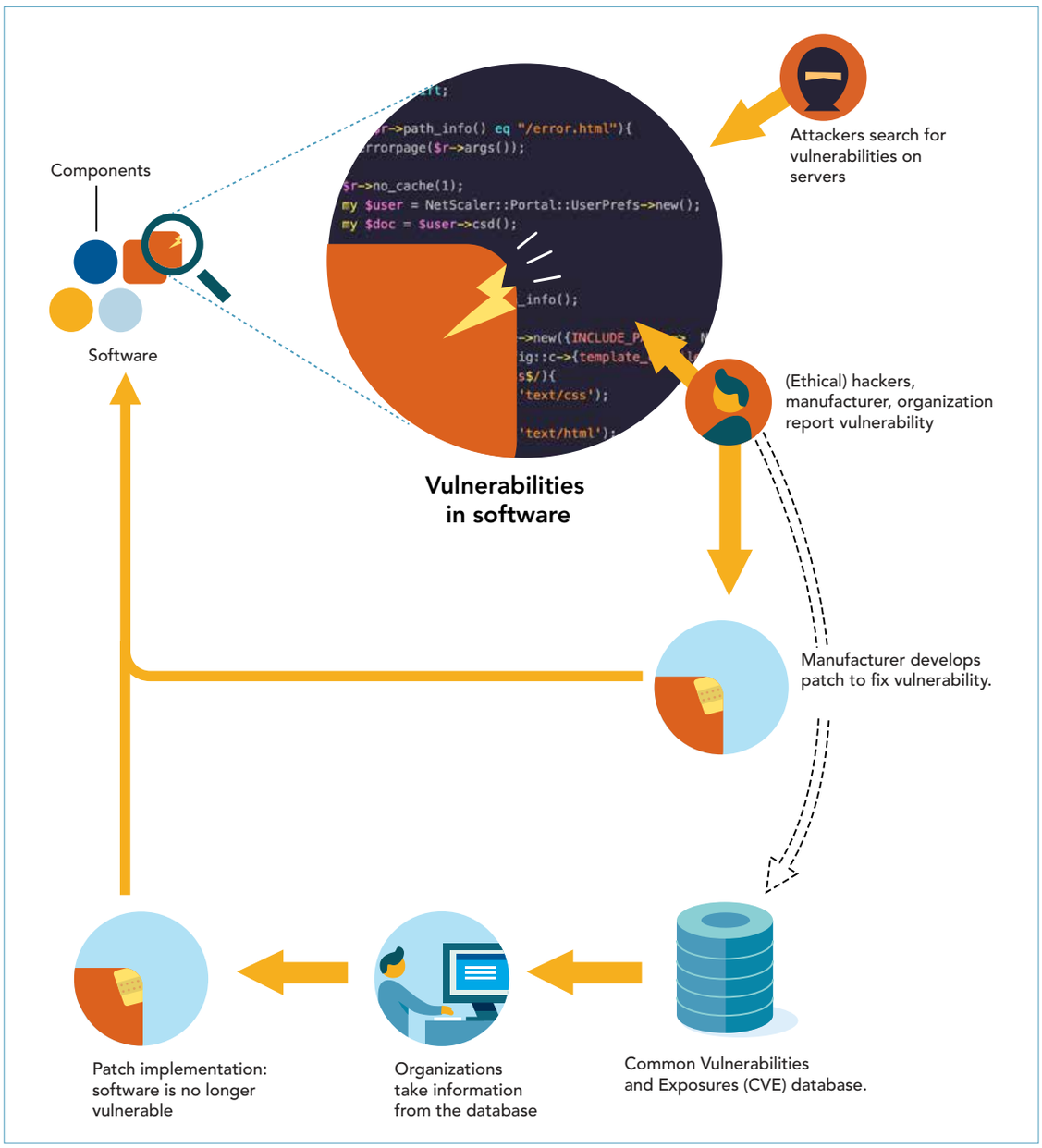


Figure 4: Vulnerabilities in software.

Global trade in vulnerabilities and exploits[35]

The expansion of digitalization has led to a worldwide trade in zero day exploits. Depending on the potential of the zero day to attack organizations, thousands or (on the black market) millions of dollars may be paid for it. In the first place by manufacturers themselves, who pay ethical hackers large amounts as a reward for reporting a vulnerability (known as a *bug bounty*). These payments are made either directly or via so-called *bug bounty platforms* such as HackerOne[36].

There are also numerous traders and brokers who purchase vulnerabilities from hackers, and then sell them on to the highest bidder. These include state actors (such as China and Russia) and their service providers, and criminal actors. But the US and the Netherlands are also using unknown vulnerabilities. This leads to safety and security dilemmas. That is why the House of Representatives has an initiative bill under consideration that proposes that intelligence agencies, investigative agencies, and the Ministry of Defense apply a consideration framework for dealing with zero days.[37]

There is also a trade in *half day exploits*, aimed at the exploitation of vulnerabilities of which the manufacturer is already aware and has made a patch available, but of which the majority of users is not yet aware. Following the leaking and theft of various vulnerabilities, intelligence services such as the American NSA came under serious criticism, for collecting and storing zero days, rather than reporting them to the manufacturer.[38] Another strategy used by attackers is *living off the land*. This means that they use known vulnerabilities, whether or not via *tooling* (automated searching and exploiting), based on the assumption that a substantial part of the users will patch a vulnerability after a long time, or not at all.

Dangerous and common vulnerabilities in software can allow attackers to bypass certain security barriers, such as:[39]

- user access check via the software;
- user authorization checks (whether a user is authorized to enter data that facilitate undesirable activities on the network, such as the possibility of changing stored data);
- preventing users from moving throughout the entire network and accessing all areas.

35 Perlroth, N. *This is how they tell me the world ends: the Cyberweapons Arms Race*, 2021.
36 HackerOne was established by two Dutch hackers to search for vulnerabilities on behalf of major tech companies such as Facebook, Google, Apple, Microsoft and Twitter. Various ethical hackers have earned more than a million dollars by identifying and reporting vulnerabilities via this platform.
37 https://www.eerstekamer.nl/wetsvoorstel/35257_initiatiefvoorstel_verhoeven
38 Schneier, B., *New leaks prove it: the NSA is putting us all at risk to be hacked*. Vox. 2016.
Ars Technica, *Cisco confirms NSA-linked zeroday targeted its firewalls for years*, 2016.
Greenberg, A., *The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days*. WIRED. 2016.
39 https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

If an organization makes use of software that contains one or more vulnerabilities, this can lead to a security breach in the user's digital system. The extent to which a vulnerability leads to a security breach in part depends on the way in which the organization uses the software, and what preventive measures the organization has taken to prevent an attack, timely detect it, (possibly) react automatically, and to limit the impact of an attack. Liability of manufacturers and organizations should be considered in this regard. Chapter 4 discusses the incentives for parties involved.

Setting up and maintaining secure digital systems involves more than patching vulnerabilities and security breaches. It is also a question of design, implementation, monitoring (including adequate follow up on this, otherwise monitoring is useless) and learning and fine-tuning, in response to how systems operate in practice. Section 1.6 and appendix C contain a reference framework for secure software and digital systems viewed from different approaches (such as security engineering and learning networks of software buyers, manufacturers and regulators). Chapter 3 contains various vulnerabilities and security breaches, in the description and analysis of the occurrences. Chapter 4 contains an analysis of how these vulnerabilities occur, and how the risks can be controlled, both during the development of software and during the use of software and during the incident response.

2.3 Attackers and their methods

Digital systems can be attacked by different types of attackers. These attackers have different motives and targets, and different methods (both lawful and unlawful). In connection with vulnerabilities in software, above all the following attackers are relevant:[40]

- state actors (or countries and their associated organizations) such as state intelligence and security services. They hack into digital systems in order to collect further intelligence, to carry out cyberattacks against other countries or to spread disinformation;
- criminals who undertake activities such as ransomware attacks, identity fraud and payment fraud (for example phishing), as well as crypto miners who want to make use of the computing power of large numbers of computers in order to validate crypto currency (this is also referred to as mining) or criminals who target specific individuals.

It is not always possible to distinguish between the different types of attackers, because they sometimes work together, or because criminals are used as a cover to increase the deniability of a country's involvement in a cyberattack.

40 Anderson, R. *Security Engineering,* 2020. Ethical hackers also try to compromise systems. However, this is not for the purpose of attacking the system, but to warn system owners of vulnerabilities, aiming to improve security.

As well as exploiting a vulnerability in software, there are other techniques for carrying out a specific or generic attack on a digital system. These techniques are used *alongside* or *in combination* with the exploitation of vulnerabilities in software. An example of a generic attack is *phishing*, whereby attackers send emails to a large number of people, for example containing a request for them to enter their login details for Internet banking, via a fake website. An example of a specific attack is *spear phishing* through *social engineering*, whereby the attacker studies the victim and attempts to gain his or her confidence, until he or she for example grants access to the digital system or transfers a sum of money. Another tactic is not to target the attack at the organization itself, but at a supplier or customer of the organization, and for example via updates from these suppliers or the software used by these suppliers to hack into the systems of their customers. This is known as a *supply chain attack*.

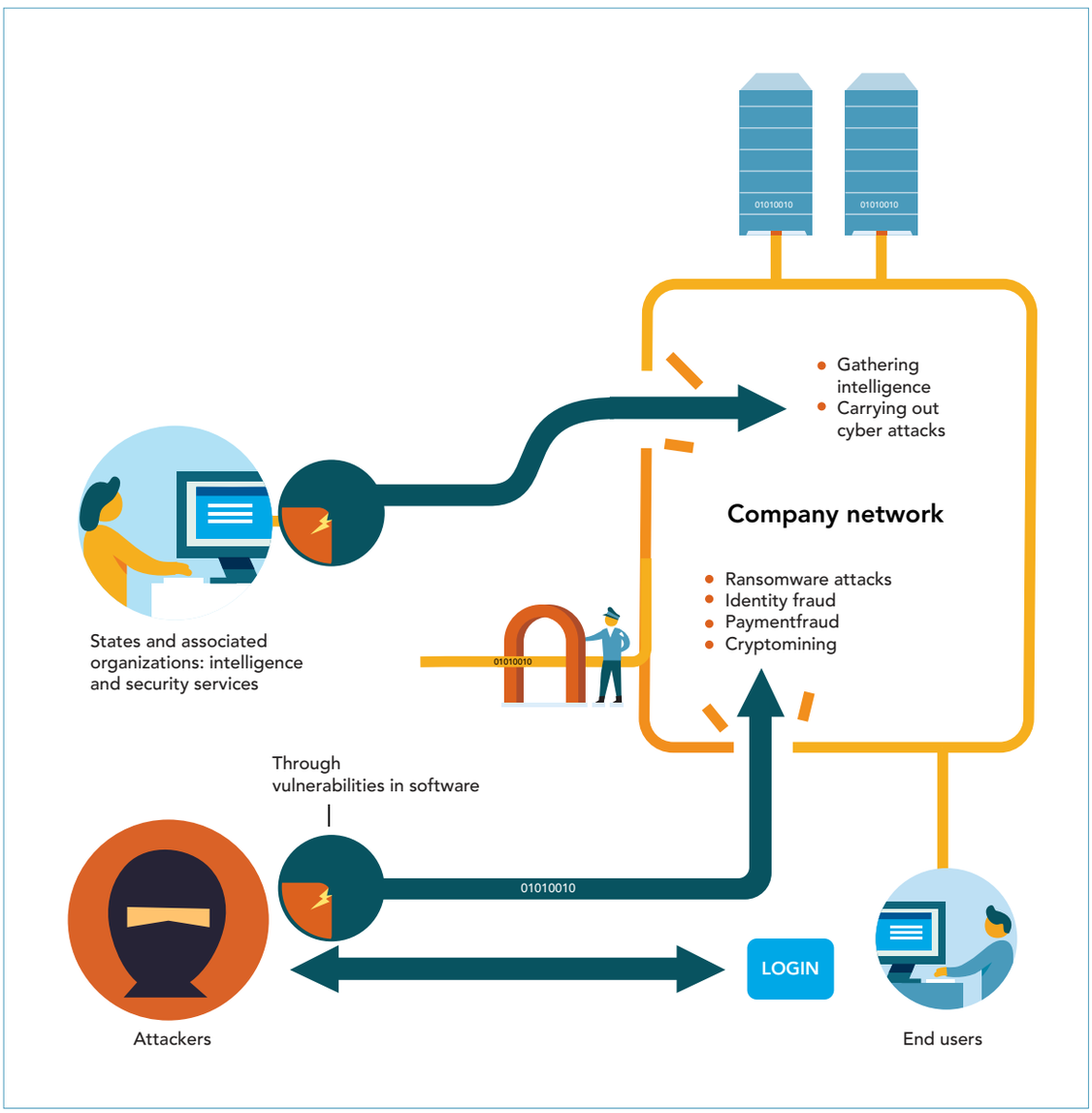


Figure 5: Attackers and their methods.

2.4 Safety and security, consequences, prevention and response

We have already on a number of occasions referred to safety and security. These are two different terms both of which are relevant in the digital domain. They are also all-encompassing container terms with unclear and sometimes contradictory definitions. For that reason, we describe here our definition of the terms safety and security in this investigation, and how the two definitions relate to one another.

Safety is a broad term that can be defined in several different ways. Within the context of this investigation, we define the term safety risks as 'the possibility as a result of internal conditions or external circumstances, that a system could damage its environment'. For example when a car collides with a pedestrian, as a result of a steering failure. There are also security risks, namely that the confidentiality, availability and/or integrity of the digital system can be harmed by the system's environment, for example by attackers.[41] In this investigation, we consider safety and security risks in combination.

Consequences to safety and security can occur in different ways and are not always visible. Organization do not always notice their systems have been compromised, and if organizations do know of this, they are rarely transparent about it. An attack can remain invisible because attackers – depending on their motive – have an interest in remaining undetected. Sometimes it takes months before they show themselves. In the meantime, they can wreak havoc or prepare for another attack, such as a ransomware attack.[42]

In some cases, the incidents in this investigation have physical and social consequences for citizens. When it comes to all types of cybercrime combined, Statistics Netherlands (CBS) estimates that 1.2 million people in the Netherlands (about 7% of the total population) were victims of cybercrime in 2018 and this number is increasing. In addition to financial damage, victims of cybercrime often suffer emotional and psychological damage and lose confidence in technology, systems and organizations. In such cases, experts speak of 'cyber trauma'. It is usually impossible to find out why citizens have become victims of cybercrime after it has occurred. Their stolen data is usually not directly misused. They are first traded, and when the attention has faded, malicious parties use the data to commit identity theft, for example. In the vast majority of cases, it is not subsequently determined who the perpetrator is, nor is it known how this perpetrator obtained the data. This could have been through a vulnerability in software, but also through other vectors.[43]

41 Anderson, R. *Security Engineering*, 2020.
42 A positive exception is Maastricht University, which organized a symposium on the lessons learned after the ransomware attack that affected them. https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt.
43 https://www.cbs.nl/nl-nl/nieuws/2019/29/1-2-miljoen-slachtoffers-van-digitale-criminaliteit; https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime; *FT*, 'Cyber trauma' leaves online victims with psychological scars https://www.ft.com/content/1bb6e777-b615-461e-a4f5-3f89927e5ad6.

Consequences to safety and security are also noticeable at the organizational level. Economic espionage damages the economy. One of the motives of attackers to abuse vulnerabilities in software to penetrate systems (unnoticed) is to obtain high-quality technology developed by Dutch companies and knowledge institutions. The consequence of this economic espionage is that the competitive position of important sectors deteriorates. This causes considerable damage to the economy (economic security). And that brings us to the safety and security implications on the national level. In addition to economic espionage, it is also relevant that intelligence services both in the Netherlands and abroad observe that state actors abuse vulnerabilities in software on a large scale (such as in the incidents described in chapter 3) to penetrate organizations' systems.[44] Attackers have various motives for this, in addition to economic espionage this includes espionage on their own citizens and preparations to carry out disruptive actions at a later date (attacks on vital infrastructure, 'preparation of the battle field').[45]

2.5 Safety chain and risk management in the (cyber) incidents

Before a (cyber) incident occurs, various phases can be identified in which the risk of such an incident can be removed or mitigated:[46]

- proaction: taking measures to remove structural causes of unsafety and incidents. In the physical safety domain, this includes not issuing a permit to a company or activity if the risks for the environment are too great;
- prevention: taking measures that prevent incidents and/or mitigating the consequences, such as installing a firewall or other security measures;
- preparation: taking measures that facilitate a good response to a critical occurrence. One example is drawing up a crisis plan and training and practising crisis situations;
- incident management: these are activities that are undertaken when an incident has actually occurred;
- aftercare: these are measures necessary to recover the situation to normality. Following a ransomware attack, the recovery of data is an essential precondition for an organization to continue functioning.

These phases in incident management have to match the various phases of a cyberattack, as shown in the Cyber Attack Cycle in the following figure.

44 https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020; https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren; https://us-cert.cisa.gov/ncas/alerts/aa20-258a (China), https://us-cert.cisa.gov/ncas/alerts/aa20-259a (Iran), https://us-cert.cisa.gov/ncas/alerts/aa20-296a (Russia).

45 Schulze, M., Cyber in War: *Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations*, NATO CCDCOE publications, 2020.

46 https://www.raadsledenenveiligheid.nl/crisisbeheersing/de-veiligheidsketen.

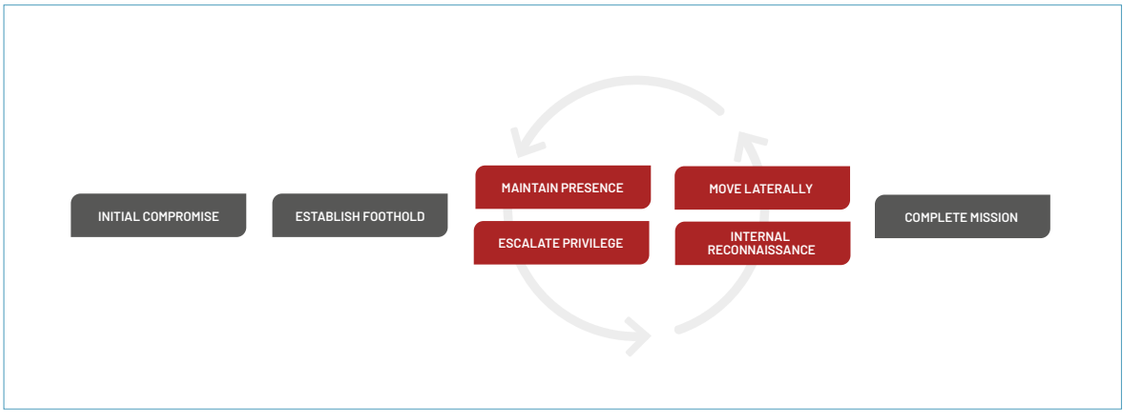


Figure 6: Cyber Attack Cycle.[47]

An organization should take measures within every phase to frustrate an attack. Within each phase, there are four possible types of reaction to the risk (control measures): avoid or prevent (terminate), mitigate (treat), transfer or outsource (transfer) or accept (take). The remainder of the risk is known as residual risk.

In this investigation, we describe incidents that occur following the discovery of a software vulnerability, that led to security breaches in the digital systems of organizations. We consider discovery of the vulnerability as the starting point of the phase of incident management. If the manufacturer becomes aware of a vulnerability, in many cases it is published in the Common Vulnerabilities and Exposures (CVE); some manufacturers do not publish the vulnerabilities they find themselves (see section 3.3). As a rule, this publication contains (sometimes first temporary) measures that organizations which use the software must take in order to remove the vulnerability, and the resultant unsafety.

With regard to a proportion of the vulnerabilities that are used to carry out large-scale attacks on organizations, a second phase in incident management follows, whereby the organizations that failed to carry out the measures before the attacks started, assume that they have been compromised.

For certain sectors, government organizations and businesses have established organizations to offer their grassroots support in incident management. The first line comprises the Computer Security Incident Reponse Teams (CSIRTs) and the Computer Emergency Response Teams (CERTs). The National Cyber Security Centre (NCSC) is CSIRT for national government and vital operators, and CSIRT DSP for digital service providers. There are several sectoral CERTs: Z-CERT for care institutions, SURFcert for educational institutions, IBD for municipalities and WM-CERT for water authorities. There are also organizations that objectively have the task to provide other organizations or the public with threat information (OKTTs). These organizations were established and have been tasked with sharing information with their sector players such as the Cyber Resilience Center Brainport, Abuse Information Exchange, the NBIP for all hosters in the Netherlands, and the Digital Trust Center for non-vital businesses.[48] The policy of national

47 Image presented courtesy Mandiant, Inc., 2021. All rights reserved.
48 This is the situation at the time of writing of the report (October 2021). Several of the mentioned CERTs and OKTTs were appointed by the national government as organizations information may be shared with after the incident in December 2019.

government is that eventually the Netherlands will be covered by what is known as a Nationwide System of CERTS and OKTTs, all appointed by national government as parties the NCSC can share relevant information with, and other relations of cooperation (mainly via the DTC).

In addition to commercial security companies, voluntary security investigators also play a role in tackling cyber incidents. Their work involves scanning the Internet for vulnerable servers and subsequently warning organizations and individuals. In the Netherlands, a number of these voluntary security investigators joined forces in October 2019 in the Dutch Institute for Vulnerability Disclosure (DIVD). Since 2021, the DIVD has operated a Computer Security Incident Response Team (CSIRT), previously known as the Security Reporting Point.

2.6 System

Various types of organization are involved in the development and use of software:

- software manufacturers;
- IT service providers;
- security companies ;
- organizations that use software: government, healthcare, education, public utilities, private companies, et cetera ;
- within the organization: executive board, CIO, CISO.

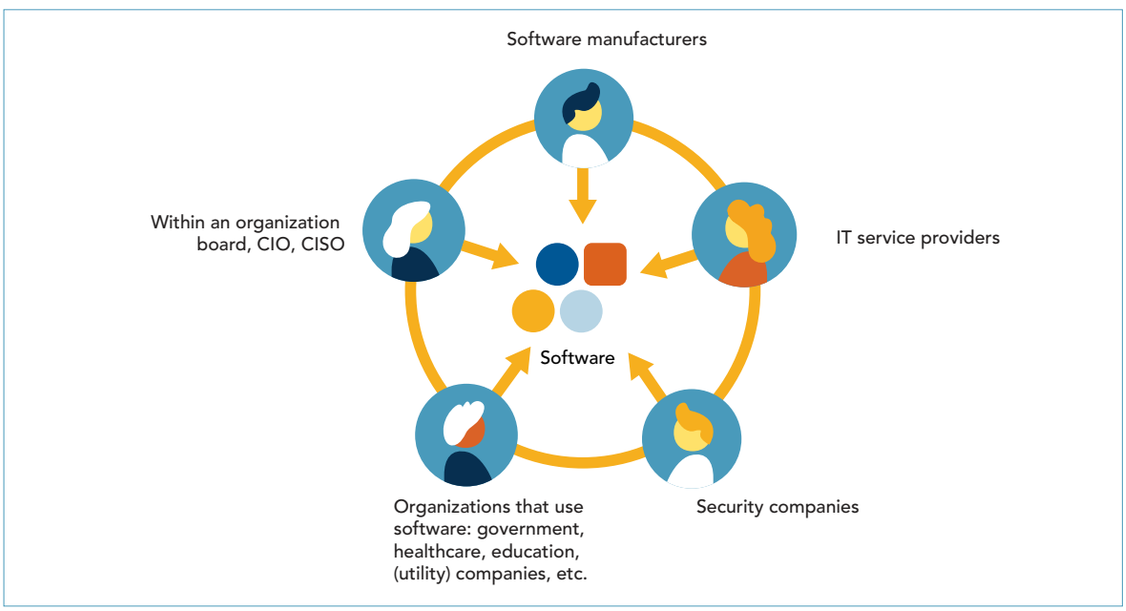


Figure 7: Organizations involved in the development and use of software.

The current policy and its implementation for the Dutch cybersecurity system lies with a number of Ministries. To provide support to national government and vital operators, the National Cyber Security Centre (NCSC) was established, under the auspices of the ministry of Justice and Security (JenV). To reach non-vital businesses, the information flow travels inter alia via the Digital Trust Center (DTC) that reports to the ministry of Economic Affairs and Climate Policy (EZK). The ministry of EZK is also CSIRT for several categories of digital service providers and responsible for policy and for supervising telecommunications. The ministry of the Interior and Kingdom Relations (BZK) bears policy responsibility for digital government. The ministries of Foreign Affairs (BZ) and Defence are responsible for the digital domain in their departments. Furthermore all departments are responsible for digital safety and security of the sectors within their domain.

The minister of Justice and Security is the coordinating government authority for cybersecurity. The NCSC referred to in the previous subsection and the NCTV (National Coordinator for Security and Counterterrorism) are part of this Ministry. The NCSC used to be part of the NCTV, until it became an independently operating department of the Ministry of Justice and Security, on 1 January 2019, with the NCTV as its principal.[49] The statutory task carried out by the NCSC is laid down in the Security of Network and Information Systems Act (Wbni). Pursuant to this Act, organizations in vital sectors and providers of essential services are required to report serious cybersecurity incidents to the NCSC. For its part, the NCSC informs and advises the vital operators[50] and national government on threats and incidents in their network and information systems, both proactively and in response to reports and incidents. The NCSC works together with the AIVD in this, among others. The Ministries and vital sectors primarily bear responsibility for their own IT and information security, and digital resilience.

49 The NCTV primarily coordinates and develops the cybersecurity policy. The NCSC is the executive organization with regard to the statutory tasks of the Minister of Justice and Security in that area.

50 At the time of the incident with Citrix software, this meant providers within the following vital processes (appointed as 'vital provider'): energy (gas, electricity, petroleum), transportation (ports and airports), banking, financial market infrastructure, drinking water, digital infrastructure, nuclear, water management, financial services, electronic communication/ICT; Decision Security of Network and Information Systems (designation of vital providers and further rules on security for essential service providers, version January 2019)

3 SOFTWARE VULNERABILITIES AND THEIR CONSEQUENCES: COURSE OF EVENTS AND ANALYSIS

This chapter provides an answer to the first investigation question, namely how occurrences such as the security breaches caused by the vulnerability in Citrix software happened, what consequences they had and how those risks were managed. Section 3.1 describes what Citrix did after being informed of the vulnerability. Section 3.2 deals with the incident management and the consequences for the organizations using the software. To be able to extend the scope of the findings from the analysis of that occurrence, we then provide a description of other similar occurrences in section 3.3. To support the reader, the texts are provided with timelines.

3.1 Vulnerability in Citrix software and security breaches

This section describes the events that occurred following a vulnerability in Citrix software:[51] the discovery of the vulnerability, the response from the manufacturer and the incident management measures taken in the Netherlands from the moment that the manufacturer announced the vulnerability.

3.1.1 Discovery of vulnerability in Citrix software and response from the manufacturer

This subsection deals with the discovery of the vulnerability in the Citrix software and the response to the discovery by the manufacturer. The most important events are visualised in the following timeline.

51 Manufacturer Citrix published the vulnerability on 17 December 2019 (CVE-2019-19781).

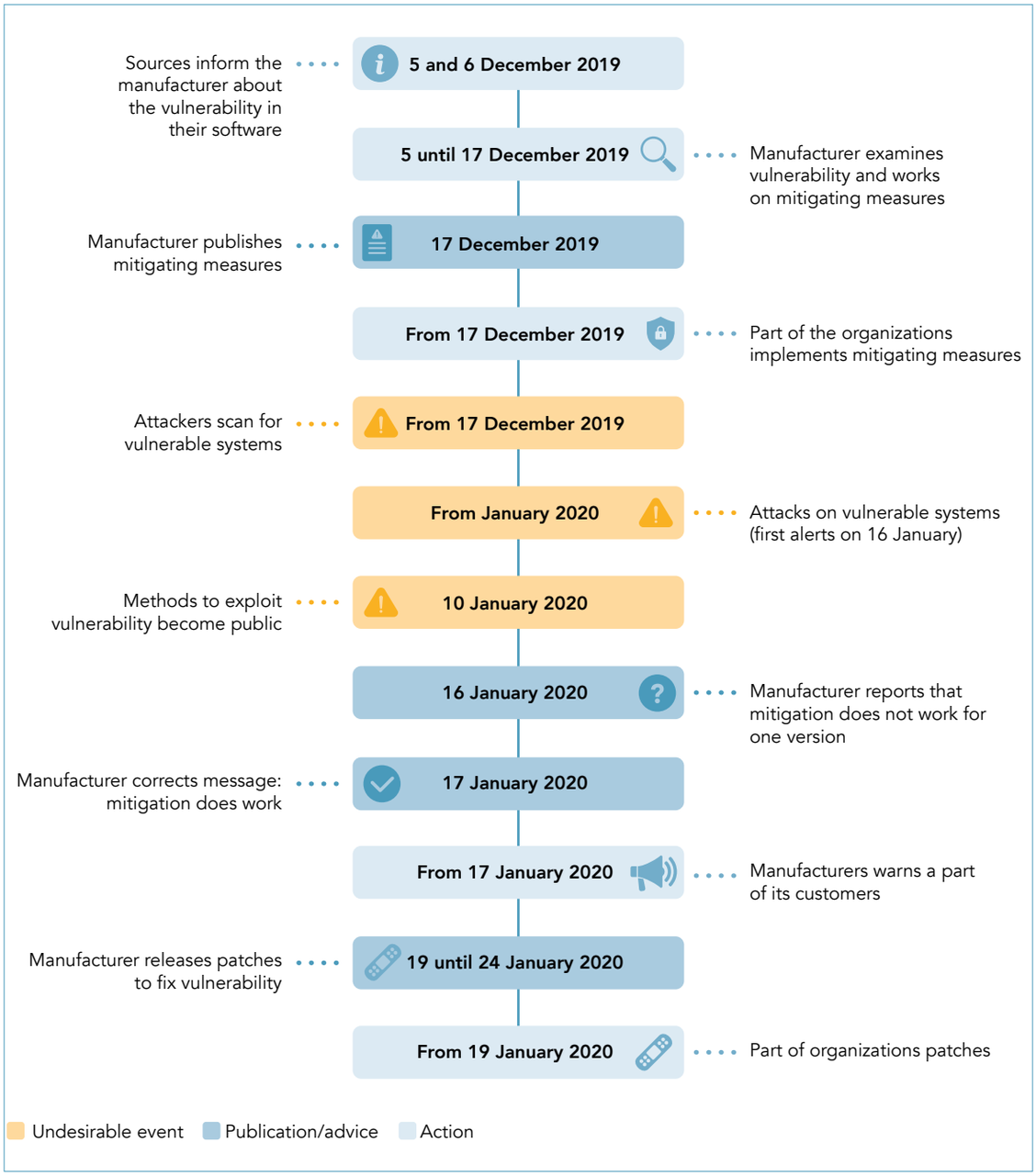


Figure 8: Timeline manufacturer.

Sources inform manufacturer about vulnerability in software

On 5 and 6 December 2019, three different sources approached Citrix. They informed the manufacturer independently of one another about the same vulnerability in the software. One of the sources indicated that the vulnerability was already more widely known. All three used the same method to demonstrate the vulnerability.[52]

52 Two of the sources indicated that they were not the original finder of the vulnerability, but that they had obtained the information from a bug bounty programme operated by one of Citrix's customers. According to this source, the vulnerability had been shared with other so-called bug bounty hunters, via online channels. Bug bounty hunters are individuals (or organizations) that in exchange for recognition or a reward go in search of vulnerabilities in digital systems. Interview CISO Citrix with Techzine, 23 January 2020. Available via: https://www.techzine.eu/blogs/security/44687/exclusive-interview-citrix-ciso-fermin-serna-where-did-it-go-wrong/

Manufacturer investigates vulnerability
Following these notices, Citrix investigated whether the vulnerability was known internally. This was not the case. A number of the manufacturer's departments then investigated the vulnerability. The manufacturer's analysis also revealed that this vulnerability had been present in the foundations of the software for more than ten years, in components that had been part of the product, since the start of its development.

Based on the fact that the PoC code would already be in circulation, the manufacturer estimated that vulnerable systems ran a high risk of being attacked. On the basis of this risk analysis, the manufacturer realized that this meant that the vulnerability was present in a large proportion of all versions (*installed base*) of the Citrix software in use, and that producing patches for all these versions would take a great deal of time and energy.

In response, and based upon the risk that a POC might be in circulation, Citrix decided to treat this as a zero-day vulnerability. The usual method is to first develop a patch aimed at repairing the vulnerability, and then publishing the vulnerability. Instead, the manufacturer developed mitigating measures as a temporary solution in advance of the definitive patches. A mitigating measure could be achieved faster than a patch. Even though a mitigating measure does not take away the cause of the vulnerability, it takes away the effect and reduces the risk. For this reason Citrix considered it to be as effective as a patch.

Manufacturer publishes mitigation steps
On 17 December, the manufacturer disclosed mitigating measures and the information on the vulnerabilities by publishing a support article and security bulletin on their website. In this bulletin, they warned of the vulnerability in various products and versions of the Citrix software. The manufacturer itself classified the vulnerability as very serious (9.8 on a scale of one to ten).[53]

Attackers scan for vulnerable systems
By publishing the mitigation steps, it became possible for attackers to derive where in the Citrix software the vulnerability was located and what type of vulnerability it was (*reverse engineering*) According to Citrix, the risk that a mitigation or patch might be reverse engineered to create an exploit, was outweighed by the importance of communicating the mitigation and the need to protect its customers from a zero-day situation.

In the week following the announcement, one of the sources that had reported the vulnerability published further details about the vulnerability. In the subsequent period, publications from other security researchers followed: based on the mitigation steps, they described the nature of the vulnerability, and how it could be abused to penetrate a vulnerable server. A worldwide scan on 8 January 2020 revealed that worldwide around 60,000 servers were using this product, and that of those around 40,000 still appeared to be vulnerable. For the time being, no one had published a working attack method, so

53 Citrix, *Support article Mitigation Steps for CVE-2019-19781*, created 16 December 2019, published 17 December 2019. Current version available via: https://support.citrix.com/article/CTX267679
Citrix, CVE-2019-19871 – *Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance*, 17 December 2019. Current version available via: https://support.citrix.com/article/CTX267027

it did not appear likely that at that moment attackers were in a position to exploit the vulnerability on a large scale, to attack vulnerable servers. Nonetheless, the manufacturer knew from the sources that had reported the vulnerability to it that the vulnerability and possibly the demonstration method were already circulating in particular groups.[54]

Methods for exploiting the vulnerability are made public

On 10 January 2020, via the platform GitHub and without consulting or notifying the manufacturer, a group of security researchers published the code for exploiting the vulnerability in the Citrix software. On 11 January, a security company also published its version of the exploit. Following the publication of the methods for exploiting the vulnerability, it became known both to the manufacturer and other stakeholders, such as the NCSC in the Netherlands, that an attack on vulnerable Citrix servers was very accessible even to non-expert attackers. The code was available on GitHub and on YouTube videos were published, demonstrating the method for exploiting the vulnerability. [55]

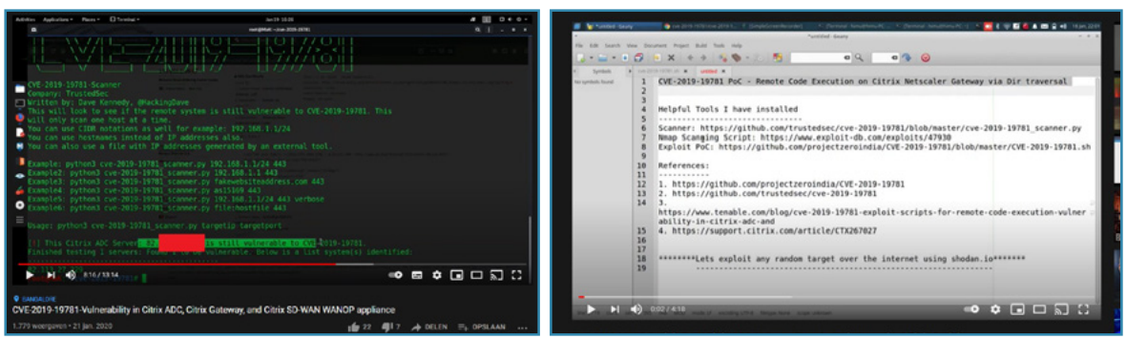


Figure 9: Videos (l) explaining how vulnerable servers can be found and (r) demonstrating how the vulnerability can be attacked.[56]

Vulnerable systems are attacked

In the days that followed, numerous reports were released about vulnerable and attacked servers. On 12 January 2020, for example, one security company published information about 25,000 vulnerable servers in the world, of which 713 in the Netherlands. The NCSC received a list of vulnerable servers from this security company on 11 January 2020. These were servers on which the organizations in question had not yet implemented the mitigation steps published by Citrix before they became under attack. This made the systems of which the servers were part of vulnerable to external attacks. Another security company issued a report on 15 January of a major spike in attacks. On that same day, a

54 Further details were published on: https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of-80000-companies/ The term security investigator in this investigation refers to persons who on an individual basis or as part of a (security) company investigate vulnerabilities in software and systems. For example https://www.tripwire.com/state-of-security/vert/citrix-netscaler-cve-2019-19781-what-you-need-to-know/

55 GitHub is an online platform on which users can place source code, so that other users can make use of it.
Published exploit code 10 January 2020: https://github.com/projectzeroindia/CVE-2019-19781
Published exploit code 11 January 2020: https://github.com/trustedsec/cve-2019-19781

56 (l) https://www.youtube.com/watch?v=cALcgyq42kI (r) https://www.youtube.com/watch?v=c9-V68L5qUwI

hospital and a municipality announced that attackers had penetrated their systems making use of the vulnerability in the Citrix software.[57]

Mitigation received no priority

One government institution with limited IT capacity saw no possibility of implementing the mitigation steps for the Citrix systems, after it had been made available. The decision to not mitigate in this case was made by the IT department. This department was struggling with capacity problems and because they had already planned to replace the Citrix environment in the near future, they did not see immediate mitigation of the Citrix systems as a priority. The CISO[58] at this government institution was not able to communicate the urgency of the situation so that the IT department would implement the mitigation. As a consequence, the organization was attacked, and the Citrix systems had to be shut down. At this organization, this meant that employees could no longer work from home.

Doubts about the effectiveness of the mitigation steps

On 16 January 2020, one month following the publication of the mitigation measures, various sources reported that the mitigation steps as recommended by Citrix apparently were not effective for all versions of the Citrix ADC and Gateway. The manufacturer published a notice stating that for certain older versions of the software, the mitigation was not fully effective, but soon afterwards realized that this conclusion had been drawn erroneously. On 17 January 2020, Citrix corrected the published notice via a bulletin update and executives of the manufacturer reported explicitly in a TV interview, blogpost and on Twitter that the mitigation steps were effective for all releases and patches, on condition the customer had implemented all steps necessary for ensuring the correct functioning of the mitigation. The alternative was to upgrade to a new version, and to implement partial migration.[59]

Manufacturer warns group of customers

One day earlier, on 15 January 2020, Citrix took additional measures beyond the previously published mitigation measures, as an interim solution until the patch for the vulnerability became available. The manufacturer launched a tool on 15 January to test whether machines were vulnerable and whether the mitigation was correctly executed. The NCSC requested Citrix on 17 January to also develop a forensic tool to determine whether a vulnerable server was accessed. As such tool was not yet available, Citrix built it pursuant to the NCSC request and made it available on 22 January.

57 Publication 12 January 2020:
https://badpackets.net/over-25000-citrix-netscaler-endpoints-vulnerable-to-cve-2019-19781/
https://www.security.nl/posting/639015/Honderden+Nederlandse+Citrix-servers+kwetsbaar+voor+aanvallen.
https://www.fireeye.com/blog/threat-research/2020/01/vigilante-deploying-mitigation-for-citrix-netscaler-vulnerability-while-maintaining-backdoor.html
https://nos.nl/nieuwsuur/artikel/2318812-hack-poging-in-ziekenhuis-en-gemeente-urgentie-lek-leek-niet-duidelijk.html and https://www.ad.nl/tech/ziekenhuis-leeuwarden-legt-dataverkeer-met-buitenwereld-stil-na-cyberaanval~a45daf1e/

58 Chief Information Security Officer responsible for information security within an organization.

59 Depending on the license and support contract, there could be a cost to the customer for the upgrade.
Notice that mitigation for one version didn't work https://support.citrix.com/article/CTX269189
Correction of previous notice: https://www.citrix.com/blogs/2020/01/17/citrix-updates-on-citrix-adc-citrix-gateway-vulnerability/

In addition to placing the alert on the website and in social media reports, the manufacturer attempted to reach as many of its customers as possible. In the period between 17 and 24 January, Citrix sent out more than 124,000 emails to approximately 36,000 different organizations. During this same period, the manufacturer started to establish a database with contact details for its customers[60], so that in the event of future vulnerabilities it would be possible to trace products and warn customers more effectively.

From the start of January 2020, the manufacturer (and others like the security researchers of DIVD, see section 3.1.2) also started to scan the internet for IP addresses of vulnerable servers.[61] If the manufacturer was able to link a located IP address to a customer, they attempted to actively approach the customer in question. In consultation with the NCSC, Citrix also shared the IP addresses it had identified in this way, with the national CERTs, including the Dutch NCSC.

Manufacturer publishes patches to definitively repair the vulnerability

On 17 January, Citrix published a timeline showing when the patches that would definitively repair the vulnerability were due to be published. Citrix initially expected that it would need until 31 January to produce patches for all versions of the various products in circulation. Citrix eventually published the patches in the period 19 to 24 January.[62]

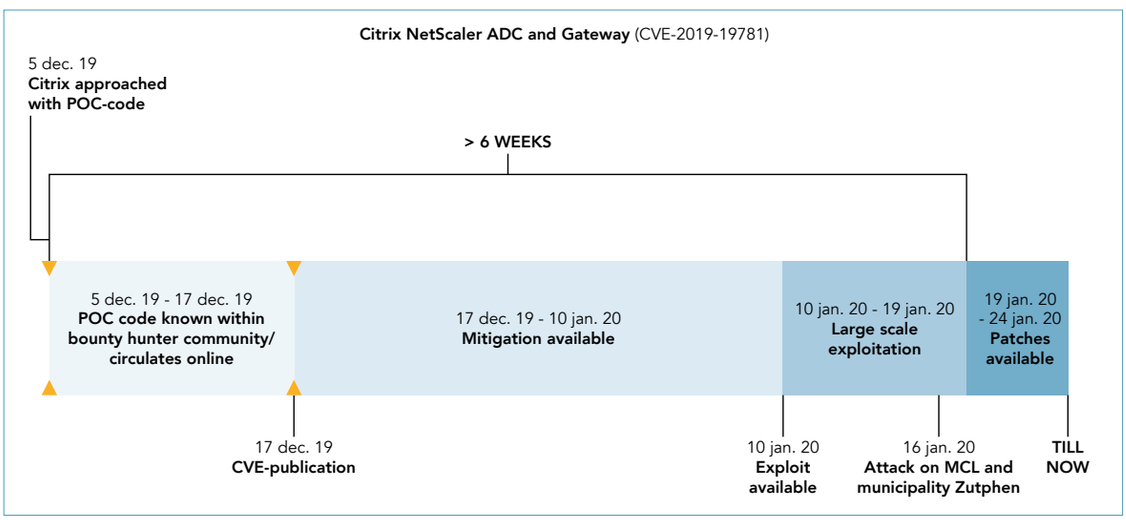


Figure 10: Timeline from discovery of vulnerability through to publication, operation and patches.

60 Customer Relationship Management (CRM).

61 In that process, Citrix made use of a tool produced in-house, in combination with such services as BinaryEdge and Shodan. These services scan the internet to classify devices linked to the Internet (approachable from a specific IP address and gateway combination).

62 A patch is a new version of the software that no longer contains the vulnerability (source: *Woordenboek Cyberveilig Nederland 2019*). First timeline of patches: https://www.citrix.com/blogs/2020/01/11/citrix-provides-update-on-citrix-adc-citrix-gateway-vulnerability/ Publication of patches: https://www.citrix.com/blogs/2020/01/22/update-on-cve-2019-19781-fixes-now-available-for-citrix-sd-wan-wanop/

3.1.2 Consequences and incident management in the Netherlands

This subsection deals with incident management in the Netherlands from the moment that the manufacturer announced the vulnerability.

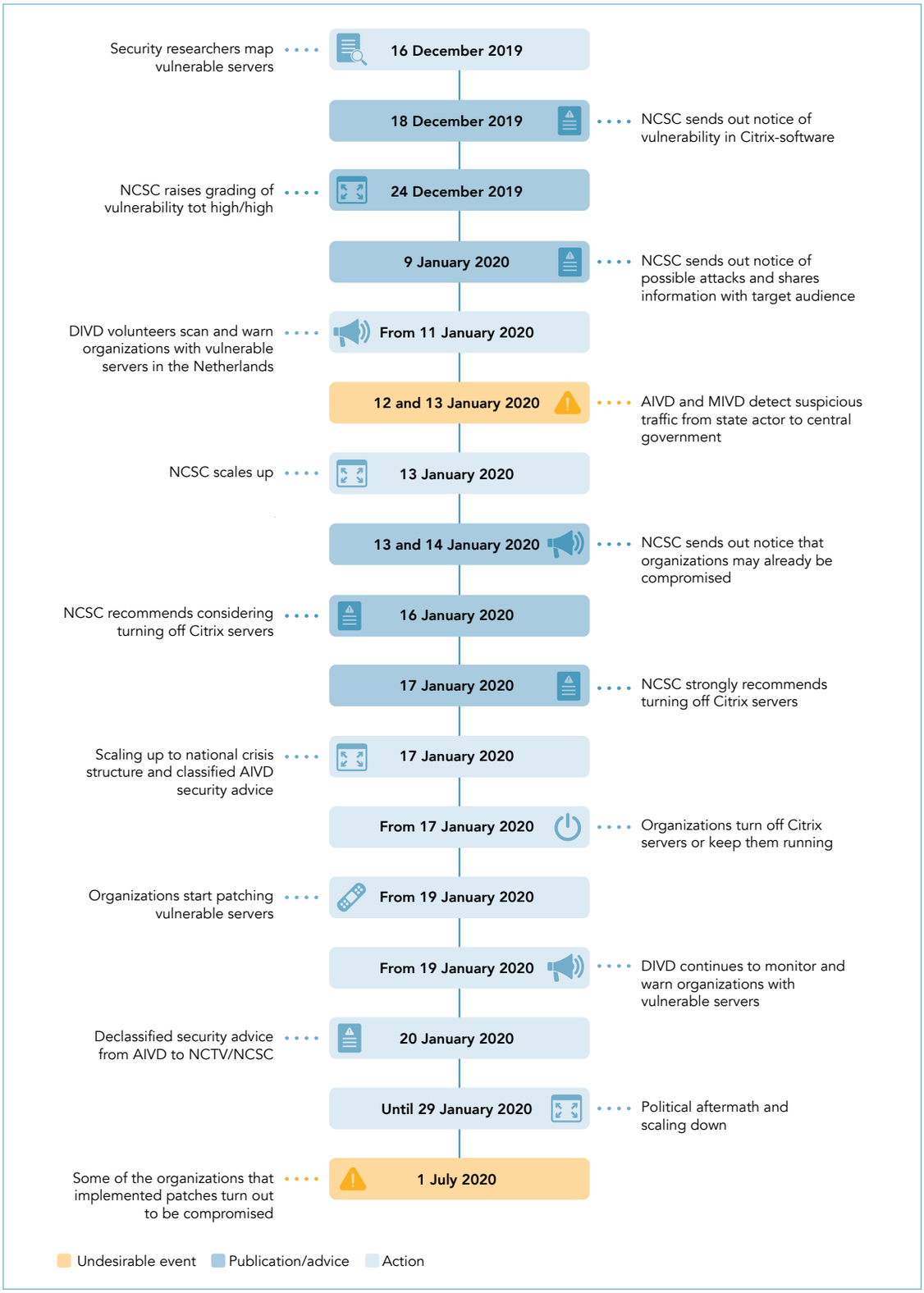


Figure 11: Timeline incident response[63].

63 It is not possible anymore to determine whether these organizations had mitigated in advance, and whether this was done correctly and timely.

Security researcher scan the internet for vulnerable servers

Various security researchers including from DIVD[64] scanned the internet to map out how many servers were using the vulnerable Citrix software. A first scan on 16 December 2019 revealed more than 125,000 vulnerable servers worldwide; on 23 December (one week after publication of the vulnerability), there were still 80,000 vulnerable servers, of which 3,700 in the Netherlands. On 7/8 January 2020, there were still 700 vulnerable servers in the Netherlands.

NCSC warns of vulnerability in Citrix software

On 18 December, the Dutch NCSC published an initial security recommendation about this vulnerability on its website. It also shared the recommendation with its own target groups: national government and vital operators: 'NCSC security recommendation 18 December 2019: Citrix reports that a vulnerability has been discovered in Citrix ADC, Citrix Gateway, Citrix NetScaler and Citrix NetScaler ADC. The vulnerability has also been found in the Citrix SD-WAN WANOP software.' The NCSC identified the seriousness of the vulnerability as medium/high. Based on further information from security investigators, on 24 December, NCSC raised the grading of its earlier security recommendation to high/high and informed its target organization about this.[65]

NCSC warns of possible attacks and shares information with target groups

On 9 January, the NCSC warned its target organizations, and published a bulletin on its website that attackers were actively seeking out vulnerable Citrix servers. This warning was based on notices issued among others by the Internet Storm Center of SANS. The Fusion Center[66] of the NCSC received multiple signals from their target groups that they could observe attackers were seeking out vulnerable severs. The Fusion Center also received lists of IP addresses from security investigators listing more than 700 vulnerable servers. They included this information in an update of their security advice on the website.[67] After the NCSC's security advisory was raised to High/High, the DTC informed the non-vital target group about the vulnerability on several occasions and offered them action perspective.

On 10 January 2020, the Fusion Center again informed various target group organizations by telephone. In the days following NCSC alsoshared information with the affiliated sectoral CERTs[68]. On grounds of societal interest, the director of the NCSC granted permission to also share data they consider to be personal data and/or confidential

64 The Dutch Institute for Vulnerability Disclosure (DIVD) is a Dutch organization consisting of security investigators who voluntarily offer their services, in their own words 'to make the digital world a safer place by tracing and reporting vulnerabilities to the people who can solve the problem'.
Report DIVD: https://www.divd.nl/reports/2020-00001-Citrix/
Message on vulnerable Citrix servers: https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of- 80000-companies/

65 Notice from NCSC: https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 18 December 2019.
Grading matrix of the NCSC:
medium/high: average risk of abuse and high impact in the event of abuse.
High/high: high risk of abuse and high impact in the event of abuse.

66 Operational core of the NCSC where (inter)national information flows are processed 24/7.

67 Message from the Internet Storm Center of SANS: https://isc.sans.edu/forums/diary/A+Quick+Update+on+Scanning+for+CVE201919781+Citrix+ADC+Gateway+Vulnerability/25686/ 7 January 2020.
Among others the Water-ISAC and IWWN network.
https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 9 January 2020.

68 IBD, SurfCert, Cert WM, ZCert. For example, SurfCERT indicated that it was briefed by NCSC in the evening of January 13.

traceable information.[69] This permission was necessary according to NCSC because it finds it has no legal authority to share this information with these organizations. Section 4.3 addresses these considerations. The NCSC also requested the CIO Rijk to inform the CIOs, CTOs and CISOs of the various government departments. The CIO Rijk asked the departments whether they had taken the necessary measures, and asked them to do so if necessary. According to the NCSC, at that time organizations that had not yet applied the mitigation steps to their Citrix systems should assume that their systems had been compromised.

NCSC scales up

On 11 January, the NCSC noticed that exploit codes had been published on 10 January. Those exploit codes could be used to exploit vulnerable systems. In response, the NCSC once again updated its security advice for its target organizations and the general public. In response to signals that large numbers of vulnerable servers in the Netherlands could be penetrated, NCSC deployed its event team on 13 January.[70]

At that time, the event team assessed that the Citrix software was in use by a great number of Dutch organizations, but there was no complete picture of which Citrix users were still vulnerable. Within the NCSC there were doubts about the effectiveness of the mitigating steps published by the manufacturer Citrix. In addition, various organizations had not yet implemented these mitigation steps. The event team focused on informing as many organizations as possible on the vulnerabilities.

AIVD and MIVD recognize suspicious traffic

The intelligence services were able to determine that offensive activities were being carried out by a state actor because, through the deployment of special resources, they have insight into the digital infrastructure used by this state actor and can relate this to digital traffic to the national government. This suspicious digital traffic was recognized on January 12 and 13, immediately investigated further, explained and reported on to various policy departments in the intelligence report mentioned above.

DIVD scans and warns organizations with vulnerable servers in the Netherlands

On 11 January, the DIVD deployed a Security Hotline (currently named DIVD CSIRT). From this Hotline, they initially approached organizations with vulnerable Citrix servers themselves by sending an automatic email with a warning and recommendations to the suspected mail addresses of the organizations related to the vulnerable IP addresses. The DIVD (currently named DIVD-CSIRT) also passed on the list of vulnerable IP addresses

69 The NCSC is an implementing organization with respect to the tasks of the Minister of JenV regulated in the Wbni and operates within the established policy and legal frameworks. These frameworks indicate that personal data or information that can be traced back to it can only be shared with organizations that have been designated as OKTT or CERT.

70 Update security advice: https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 11 January 2020. The NCSC operates various upscaling or escalation levels. In principle, incidents are dealt with by incident handlers who tackle minor problems at organizations. If incidents become too large to be able to be implemented within the regular tasks, upscaling takes place. The first step is the event team, a specific team that is deployed during office hours to relieve the regular operation. If the situation becomes more urgent, or if the problem is larger, the next level of upscaling is the disaster team, whereby it is also possible to continue working outside office hours. In 2020, the NCSC scaled up on two occasions to the highest level: during the Citrix occurrence and during the SolarWinds occurrence. It is possible to further upscale to crisis level, at which point the NCTV takes over coordination.

to internet providers (network owners), in particular KPN and NBIP (National Internet Providers Management Organization) and to sectoral CERTs such as the CERT for the healthcare sector (Z-CERT) and NCSC.[71] Following the scans of the DIVD and other parties, the CSIRT-DSP immediately notified the compressed parties from its own target group (digital service providers).

NCSC publishes notice to organizations that they could already be compromised

On 13 January, the NCSC once again sent a bulletin to its target groups, and on 14 January they published a notice on their website.[72] In that bulletin the NCSC advised urgently to mitigate the vulnerability as soon as possible, as recommended by Citrix. Even if these mitigation measures had recently been taken, the NCSC once again warned of the possibility that attackers may already have access to their systems. From various organizations, the NCSC received requests for more information following this notice.

Dutch organizations report being compromised

On 14 January, the CERT for the municipalities, IBD, informed the NCSC that a municipality had reported abuse of its system. The Citrix servers had been attacked, and the decision had been taken to shut down the systems. On 15 January, the NCSC received a report from a hospital that it too had been attacked, and that it had consequently shut down all data traffic with the outside world. Employees were unable to work from home, and patients were no longer able to access their patient file. The vulnerability in Citrix software received much media attention. External experts reported to the NCSC that organizations were definitely compromised, if they had not taken measures before 9 January. More reports were received from organizations where attackers had penetrated their systems: the rail sector, the police central control room, municipalities and a hospital. The NCSC received a list of vulnerable IP addresses from Citrix, and shifted its focus to advising and informing the target groups. The media attention grew, and with it the pressure on NCSC, for example with the growing number of questions for the NCSC from organizations that use Citrix software.

NCSC publishes Security Advice: consider shutting down Citrix servers

As described in 3.1.1, on 16 January, manufacturer Citrix issued a notice that said the mitigating steps were not effective for one version of the software. One day later, the manufacturer corrected this report in the form of a bulletin update.

On 16 January, the NCSC published a security advice in which it recommended to to consider shutting down the Citrix servers, depending on the impact this would have on the organization involved.[73] This advice was in part provoked by the uncertainty on the effectiveness of the mitigation steps caused by Citrix' erroneous message, and the assumption that many organizations had not yet or not yet fully implemented the mitigating measures. On the basis of NCSC' security advice, the Dutch House of

71 Using an automated script that sent mails to info@, abuse@ and security@ mail addresses belonging to the relevant IP address and the connected domain.
NBIP was established by Internet service providers as a collective means of dealing with tap requests. Since that time, they have also developed a system for countering DDoS attacks. https://www.nbip.nl/en/about-the-nbip

72 Notice from NCSC: https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen

73 This notice is no longer available on the NCSC website. The title is 'mitigating measures recommended by Citrix not always effective', and was sent on 16 January 2020. The notice appears in Appendix C.

Representatives, Amsterdam Airport Schiphol, various Ministries, Municipalities, other (government) organizations and private companies shut down their Citrix systems. The NCSC received numerous questions both from target group organizations and organizations outside its target group, seeking further information as a result of the NCSC security advice. There was considerable unrest among these organizations about the reliability of the mitigating measures recommended by Citrix.

Deploying the national crisis structure and AIVD security advice
Given the seriousness of the situation, the National Crisis Centre (NCC) decided to partially deploy the national crisis structure, by summoning the IAO (Interdepartmental Coordination Consultation). The NCTV coordinated this interdepartmental coordination. Within the NCSC, the team scaled up to the level 'emergency' and assembled the emergency team.

On 17 January, the MIVD and AIVD issued an information notice to the NCTV and NCSC stating that it had identified an acute state actor threat aimed at two organizations within national government. The Cabinet mandated the Minister of the Interior and Kingdom Relations and the Minister of Justice and Security to deal with the crisis.

In the afternoon, it became clear that there was a difference of understanding between the AIVD and the NCSC concerning the Security Advice to be issued to national government. This resulted in two different Safety Advices being laid on the table: the AIVD wanted NCSC to strongly advise organizations to shut down all Citrix servers, because, according to them, the patch did not fully work for all versions of the Citrix software, while the NCSC wanted to advise organizations to reach their own decision to shut down based on their own specific situation.

NCSC publishes urgent Security Advice: shut down Citrix servers
On the basis of the two different security advices, the Minister of Justice and Security, the Minister of the Interior and Kingdom Relations, in consultation with the NCTV, decided on 17 January that NCSC should aggravate their security advice from the NCSC and line up with the AIVD security advice. The NCSC was ordered to issue an urgent security advice to national government and the vital operators to shut down Citrix servers, based on uncertainty about the effectiveness of the mitigation steps recommended by Citrix, and the recognized threat. Starting point of NCSC's advice was the 'comply or explain' principle. CIO Rijk applied this principle in the national government. The security advice remained valid until an effective solution was available. NCSC broadcast the security advice via a target group notice, a press release on rijksoverheid.nl, the NCSC website and via other cybersecurity organizations in the Netherlands.

Each individual organization was required to make its own assessment of the impact and bore primary responsibility for its own measures and its own 'explanation if it chose to not shut down its Citrix servers. National government parties were required to present their 'explanation' to CIO Rijk, for assessment. With regard to the vital operators, the NCSC was able to offer advice and assistance where possible. The NCSC was also in consultation with Citrix on the situation. If the parties opted for 'comply', the impact of

shutting down Citrix servers on the work varied between organizations. In many cases, homeworking was no longer possible, which would lead to a rise in the number of employees travelling to the offices, which in turn would lead to increased traffic congestion during peak hours, while for other organizations, shutting would have more drastic consequences.

The urgent security advice from the NCSC was based on the security advice from the AIVD. The underlying intelligence notice contained information that was classified as state secret, and therefore not allowed to be published. The security advice itself was not classified. The NCSC did not communicate with other organizations about the content of the security advice, because of the classification of the information. Among organizations that received the NCSC security advice, there was confusion about the nature of the advice of 17 January, because it differed from the previous advice issued by the NCSC on 16 January, in particular the less urgent advice to consider shutting down Citrix servers. The recommendation from the NCSC was also more urgent than the advice from Citrix itself, from security companies advising the organizations, such as Fox-IT, and from national CERTs and security companies in other countries. Organizations indicated that they were unable to determine whether the more urgent advice also applied to them, and whether they needed to take action in response. NCSC could not initially share the content of AIVD's security advisory with the organizations outside the national government because of its classification. AIVD declassified the message on January 20. This did not give rise to NCSC to share the security advice at that moment.

Organizations decide whether or not to shut down Citrix servers

Shutting down the Citrix servers had different consequences for different organizations. For certain organizations, such as government departments, the consequences were limited to not being able to work at home.[74] At a number of municipalities, shutting down the Citrix servers meant it was no longer possible to pay social security supplementary benefits to residents of the municipality. The Ministry of Economic Affairs and Climate Policy chose to leave its Citrix servers switched on, because they were convinced they applied the mitigating steps in time, and because shutting down would have meant that the Netherlands Food and Consumer Product Safety Authority (NVWA) would have been unable to carry out any further inspections and customs checks. Without these checks the meat production and trade would have to be halted. In hospitals, patients were no longer able to access their electronic patient file, and in certain cases communication with other hospitals became impossible. There were also organizations that experienced little to no negative impact from the occurrence: their Citrix servers played a minor role in their digital system or they had access to an alternative.

74 It should be noted in this respect that the occurrence took place several months before most employees were required to work from home due to the COVID-19 pandemic, starting in March 2020. The consequences of such an occurrence in that period would have been far more far-reaching than they were in January 2020.

Dependency on Citrix software greater than assessed

Many businesses and Ministries use Citrix servers for the operation of their internal applications, or work with service providers and suppliers who use Citrix software. In many organizations Citrix servers function as a hub for a whole range of applications deep within the organizations' IT. Citrix software is above all known for working from home. However, it is also used as a point of access for example for email and office applications or for primary processes.

One of the government organizations performed a risk analysis to decide whether the systems should be shut down. After shutting down it became clear that more processes were dependent on Citrix software than previously estimated: in their risk analyses they had only identified between 60 and 70 percent of its dependencies on Citrix software. After shutting the Citrix-servers down, the dependency turned out to be so extensive that eventually not a single digital operating process could be continued.

From 9 January onwards, the CIO Rijk had called the CIOs, CISOs and CTOs of national government to follow the security advice of the NCSC, and had asked them to notify the CIO Rijk of the status of their compliance: had the organization shut down its Citrix servers, and if not, what was their reasoning.

Following the security advice of 17 January, CIO Rijk started drawing up a situation report on the compliance of government organizations, for the IAO. The majority of national government organizations (61%) that had responded had shut down their Citrix servers; a small proportion (20%) had left the Citrix servers switched on, reasoning that it would be a threat to national security to switch them off, that their department was protected by multilayer security, or because shutting down could result in too great an impact on critical processes or could cause social or economic damage. 19% of the organizations within national government did not use Citrix software at all. The Minister of Justice and Security and the Minster of the Interior and Kingdom Relations reached out to sectoral CERTs to obtain a clear picture of the extent to which their target organizations had complied with the recommendation from the NCSC to shut down the Citrix servers.

Situation sketch Citrix servers in government

Almost all the target group organizations of the NCSC, such as national government and the House of Representatives used Citrix:

- of the 12 Ministries, 10 used Citrix software;
- of the 69 national government organizations, 56 used Citrix software; of those, 42 shut down parts of the system.

Other public authorities:

- 150-200 of the 352 municipalities used Citrix software, and 80% of them shut the system down;
- 9 of the 12 provinces used and shut down Citrix software;
- all 22 water authorities used Citrix software. The majority shut down Citrix servers; a number remained operational for compelling reasons;
- 16 of the 25 security regions used Citrix software.

Organizations start patching vulnerable servers

After spending the weekend conducting continuous activities around Citrix, the disaster team of the NCSC gathered again on 18 January 2020 and noted the growing media attention.

On 19 January, Citrix released the first patches and the NCSC advised the organizations to urgently implement these. These patches were only suitable for a proportion of the versions of the Citrix software; around 50% of the vulnerable Citrix systems in the Netherlands. NCSC maintained its advice: shut down Citrix servers or explain why not (comply or explain). In addition, the NCSC issued advice on the announced patches and how to re-establish safe working environments. The NCSC indicated that organizations should assume that they had been compromised, if they had not taken the appropriate mitigation steps on time (see subsection 3.1.1: on time meant before the method for exploiting the system became public knowledge). See also the flowchart below, that NCSC published on 20 January so organizations could carry out their own risk analysis with regard to the Citrix vulnerability.

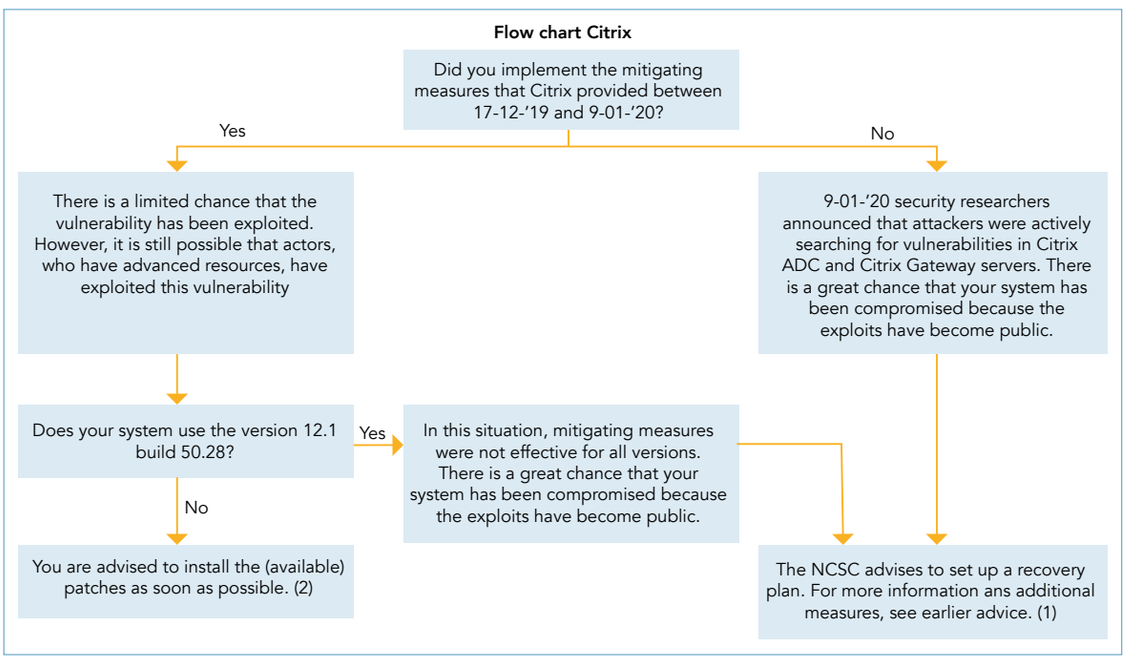


Figure 12: Flowchart Citrix. (Source: NCSC)[75]

A mail was then sent to all national government organizations with work instructions, addressed to civil servants with regard to the impact and potential for response. Within the NCSC, there was discussion as to whether they could scan for vulnerable servers themselves. Given the technical risks and legal restrictions, the NCSC decided not to do this (section 4.3 addresses these restrictions). This decision was also influenced by the presumption in the cybersecurity strategy that organizations themselves are responsible for monitoring their Citrix environment and the underlying systems. When on 21 January a number of organizations using Citrix software reported to the NCSC that they had identified malware on their systems and requested support for a forensic investigation,

75 https://www.ncsc.nl/documenten/publicaties/2020/januari/20/stroomschema-risicoafweging-citrix

the NCSC decided that it should restrict itself to its statutory task due to capacity considerations, and would not provide the requested support. Organizations should turn to security companies with forensic expertise. However, all of those companies were fully occupied at the time, assisting their existing customers: some organizations could not immediately receive the support they needed.

In collaboration with a number of operational partners, the NCSC also started testing the patches provided by Citrix, and the previously recommended mitigation measures. On 24 January, the NCSC sent a notice to all its target organizations that it had verified that the new patches were effective. In the target group notice and on the website, the NCSC issued recommendation security advice to have a forensic investigation carried out. National government organizations were obliged to report to CIO Rijk and the NCSC if the organization decided to switch on its Citrix servers again.

DIVD continues to monitor and issue warnings

On 15 January, the Security Hotline of the DIVD had also issued a advice to organizations within The Netherlands on how to check whether a system in which the mitigation measures had been implemented after 11 January had already been taken over. Depending on the seriousness of the attack organizations should determine whether or not it was necessary for them to carry out a forensic investigation or even to opt to fully reinstall the system. In the months following the release of the patches, the DIVD continued to scan the non-mitigated (vulnerable) servers. The number of vulnerable servers started to fall. On 3 February 2020, 70 vulnerable servers remained; by the start of March 2020 only five. New DIVD volunteers called these organizations once again and reissued the warning to the relevant managers, or left requests along the same lines with the receptionist.[76]

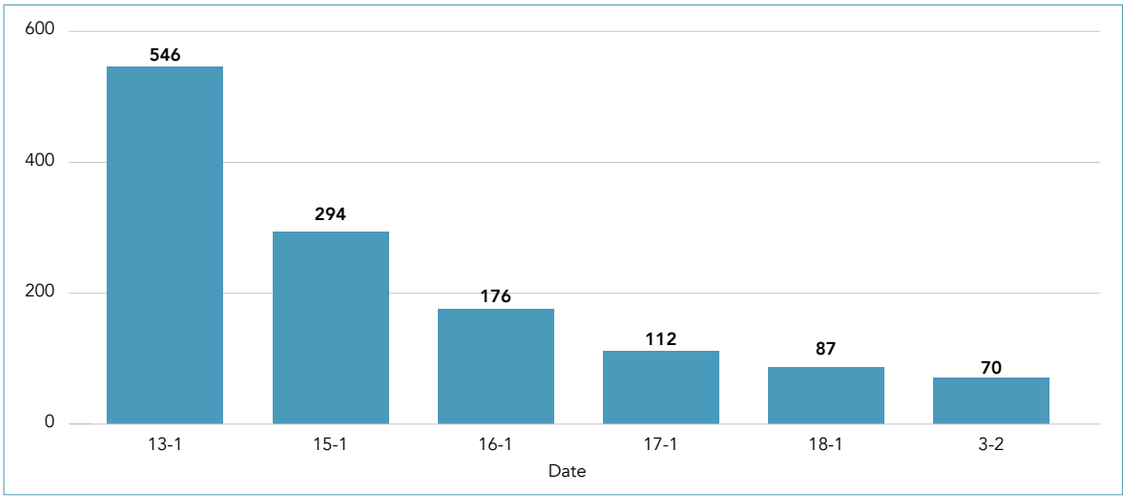


Figure 13: Non-mitigated Citrix systems found by DIVD CSIRT. (Source: divd.nl)

76 Advice from Security Hotline of the DIVD: https://csirt.divd.nl/2020/01/15/How-to-check-your-Citrix-gateway/ In practice, it appeared that these organizations were not yet aware of the DIVD Security Hotline. As a result, the security researchers were not always passed on to the relevant IT manager.

Terminating crisis structures and political aftermath
On 20 January, the Interdepartmental Crisis Management Committee (ICCb) met. The problems surrounding Citrix were discussed in the ICCb. By means of a Letter to Parliament entitled 'Vulnerability in Citrix products', the Minister Justice and Security and the Minister of the Interior and Kingdom Relations informed the Dutch House of Representatives on the identified vulnerability in Citrix products, the warning and the security advice from the NCSC.

In response to the Question Time in the House of Representatives on 21 January, on 23 January, the Minister of Justice and Security sent a report of the facts relating to the vulnerability in Citrix software to the Dutch House of Representatives, and provided a technical briefing. On 24 January, via a ministerial decree, the Minister of Justice and Security identified four sectoral CERTs[77] with whom the NCSC was allowed to exchange information more intensively.

On 29 January, the seventh and final Interdepartmental Coordination Consultation session was held. From that moment onwards the crisis structure was terminated: the activities regarding the vulnerability in the Citrix software were undertaken via the regular reporting lines, both within the NCSC and the whole of national government.
On 31 January 2020, the majority of departments had switched all their systems back on. A number of government organizations required a recovery plan before they could return to their normal working situation. The NCSC and the CIO Rijk did form a task group, that took further control of winding up the activities relating to the vulnerability in the Citrix software.

Some organizations that took measures still turned out to have been hacked.
On 1 July 2020, security firm Fox-IT published information that it had determined that 25 Dutch servers had still been hacked via the vulnerability in the Citrix software. The organizations in question had implemented the patch, but had been penetrated before they took this action. Criminal attackers and/or state actors then had access to the internal network of these organizations. According to Dutch national newspaper de *Volkskrant*, these included a company producing watermarks for banknotes and a pharmaceutical company.[78]

3.2 Analysis of the occurrence involving Citrix software

In the analysis of the occurrence, we answer the following investigation questions:
- How could the security breaches due to vulnerabilities in Citrix software occur and what were the consequences?
- How were these risks managed by the manufacturer and organizations that used the software?
- What was the role of the government and non-government parties?

77 The computer crisis teams for the healthcare sector (Z-CERT), municipalities (Information Security Service for municipalities IBD), water authorities (CERT Water management) and education and research (SURFcert).
78 https://blog.fox-it.com/2020/07/01/a-second-look-at-cve-2019-19781-citrix-netscaler-adc/
https://www.volkskrant.nl/nieuws-achtergrond/half-jaar-na-citrix-crisis-zijn-25-nederlandse-organizaties-gehackt-en-ze-weten-zelf-van-niets

We first describe the nature of the vulnerability in the software, how it remained in the software without being discovered, and how this in turn led to a security breach in a digital system. In the subsequent sections, we analyse the factors that give meaning to the Citrix software containing this vulnerability, how the manufacturer responded to the incident, and how the incident was tackled.

3.2.1 Security breach as a consequence of the vulnerability in Citrix software

The vulnerability in the Citrix software resulted from a combination of multiple minor vulnerabilities.[79] The consequence was that at organizations that had in some way used this Citrix software in their network, *unauthorized* persons cloud have been able to move throughout the entire network, and could alter the settings in such a way that they themselves were able place software code on the network, and could then execute that code remotely. The vulnerabilities in the software made it possible for attackers to bypass security measures and to remotely execute malicious code on the network of the organization in question.

Using the vulnerability, unauthorized users (including attackers) could have been able to gain access to all components of the Citrix appliance.[80] On appliances accessible from the internet, it is common practice to configure the appliance to prevent this: the remainder of the network is then protected and is not accessible to users from outside. This can be achieved in either of two ways:

- by withholding users the possibility of giving a command to the webserver that enables them to move through all components of the appliance and thus gaining access to the protected parts of the network; and/or
- not giving users rights to view the complete directory structure.

These measures can be initiated by the organization managing the Citrix appliance, or they can be enforced by the manufacturer, through the configuration of the Citrix software. The extent to which the vulnerability could lead to a security breach depended on the standard settings in the software and how the organization using the software had restricted the rights of the users on the Citrix appliance. If the organization had not taken these measures, it was possible for an attacker to access all parts of the webserver. An unauthenticated user thereby acquired the same rights as a manager, namely access to all directories on the webserver (see figure 14 below). Not only access to view, but also to execute programmes on the network. The vulnerability that allows an attacker to operate in this way is known as *path traversal*.[81] By using the possibility of path traversal, attackers were able to bypass certain access measures and make their way into otherwise inaccessible paths and to implement programmes without authentication. However, path traversal on its own was not sufficient to read out files.

79 Fox-IT, *A Second Look at CVE-2019-19781* (Citrix NetScaler / ADC), 2020. Available via: https://blog.fox-it.com/2020/07/01/a-second-look-at-cve-2019-19781-citrix-netscaler-adc/

80 A network appliance is a type of computing appliance that aids in the flow of information to other network-connected computing devices.

81 The attacker was able to implement path traversal by entering the code '/../' in the path of the webserver.

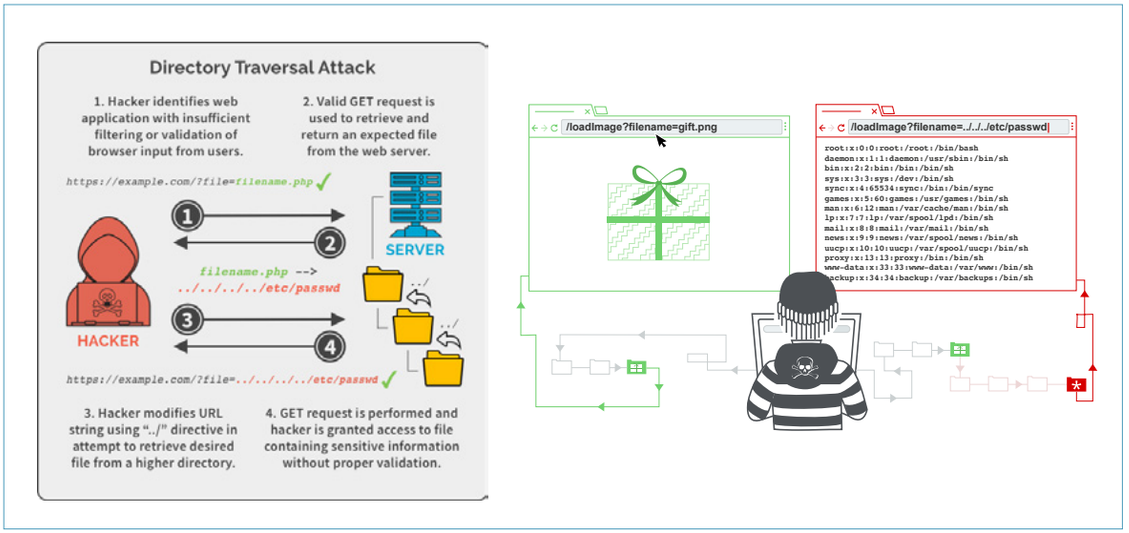


Figure 14: Directory/path traversal attack. (Source: (l) https://spanning.com/blog/directory-traversal-web-based-application-security-part-8/[82] and (r) https://portswigger.net/web-security/file-path-traversal)

3.2.2 The Citrix software had acquired a safety-critical function, over the course of time

The security breaches within organizations were partly due to the vulnerabilities in a series of software products from Citrix, namely the Citrix Application Delivery Controller (ADC). This product series has a long history. ADC is a product developed in 1997 by NetScaler, to assist companies like Google and Amazon to manage their hardware more efficiently, so that as the internet grew, the amount of hardware required remained limited. The product was based on a number of open source components. In 2005, the company NetScaler was purchased by Citrix, to fill a gap in their production line. As time went by, the manufacturer added functionalities to the product, and organizations started to implement the product in a different way. As a consequence, the product evolved to include additional functions, such as the transmission of traffic to applications and distribution across servers in the underlying network, a firewall, establishing VPN links and the authentication of users who were authorized to make use of the underlying network. Over time, the product gradually became the access gateway to the network of the organization.[83] Software that operates in a dynamic environment of this kind calls for adaptive risk management from the manufacturer. In this case, Citrix states it employs a Secure Development Lifecycle program as a key aspect of its product development framework. This issue is discussed in further detail in section 4.1.

3.2.3 Third parties discovered the vulnerability before it was found by the manufacturer

The PoC code that the security investigators shared with Citrix in December 2019 revealed a vulnerability in the ADC and Gateway. Due to the shared origin of both products, the same vulnerability was present in both products. The vulnerability in the ADC and Gateway was not yet known to the manufacturer. Security investigators do not always report a vulnerability to the manufacturer itself. A vulnerability is sometimes discovered by individual investigators or by investigators working on behalf of an

82 Spanning Cloud Apps homepage: https://spanning.com/
83 Citrix, video *The Citrix ADC story*, https://www.youtube.com/watch?v=HEWmy9-te2I, 29 November 2018.

organization using the software. Just like many other software manufacturers, Citrix encourages security investigators to immediately report vulnerabilities to them, to prevent those same vulnerabilities being sold or made available to third parties. The trade in vulnerabilities is both lucrative and non-transparent. As a result, it is possible that third parties may be aware of and exploit vulnerabilities in a software product, without the manufacturer itself having been informed. Also in this case, it was reported that the vulnerability was already circulating without Citrix' knowledge

3.2.4 Mitigating measure prior to definitive patches

As described in section 3.1, Citrix had learned from various sources that the method of exploiting the vulnerability was already circulating on certain online channels. The manufacturer therefore recognized the importance of fixing the vulnerability as quickly as possible. The Citrix response team, the first party to examine and assess reports of this kind, first contacted the *product security incident response team (PSIRT)*. This team specializes in dealing with security incidents for the various products in the Citrix portfolio. The *product R&D team* at Citrix, responsible for developing new software and patches, was then also called in. Discussions between these departments and further analysis by the R&D team revealed that a quick, permanent fix would not be achievable. Because the vulnerability was present in multiple products and multiple versions, a series of different patches had to be developed. The estimate by Citrix at that time was that several months would be needed to prepare all the patches and to work through the relevant test cycles. The manufacturer estimated that this would take so much time because the validation of security fixes of this kind demands in-depth knowledge of the product, and that a limited number of engineers with the required knowledge was available within the company.

Patches have to pass through a test cycle before they can be released to customers by the manufacturer. To repair the vulnerability, the manufacturer decided to produce a new version (*build*) of the software. This activity was expected to take several days. At that point, given the complexity of the issues and the required fixes, the manufacturer had only one team available that would be able to carry out all the automatic tests and manual validations of all patches for the different versions of the product (and because the vulnerability had been in the product line for more than ten years, there were many different versions involved). The manufacturer did not have enough engineers to be able to divide the development, testing and validation of the patches for the different versions among different teams, in such a way that all the different versions could be developed in parallel. As a result the patches for the various product versions could only be developed sequentially. Because of the time it would take to develop the patches, the manufacturer decided to take steps to mitigate the vulnerability as a measure to remedy the effect of the vulnerability.

3.2.5 Publication of mitigating measure made it simple to make an exploit

The mitigation steps advised by Citrix included information necessary for the mitigation to be implemented. Publishing information on how to implement a mitigation measure is standard practice, but may also make clear, as in this case, how the vulnerability can be exploited. The mitigating steps specified how the configuration of the webserver should be adjusted in order to prevent exploitation: make sure that the /../ command is prevented. Also, the mitigation measure disclosed where the 'path' was located so that it is clear which part of the software to look for. Publication of the mitigating steps made it clear to potential attackers that the vulnerability was related to the use of path traversal in the handling of requests (by the server).[84]

3.2.6 Manufacturer did not reach all organizations that used Citrix software

In addition to publishing the mitigation steps, the manufacturer decided to warn as many of its customers as possible, directly. At that time, the manufacturer did not yet have a possibility for contacting large groups of customers. Contact was only possible for customers who had already signed up to receive security warnings. The manufacturer only had access to the contact details of a small proportion of the organizations using its software (10%). in addition, Citrix informed us that they initiated a vast campaign to obtain as many contact details of customers as possible. For those customers whose contact details were known, the manufacturer was not sure whether the contact details were still up to date. Software manufacturers do not always know who is using their software, because the majority of sales take place via partners.

The contact details of customers to which the manufacturer did have access often proved not to be for the person responsible for security but for example the receptionist or the procurement department. The manufacturer realized that it is important to have the contact details of the person responsible for security, because otherwise there is a risk that the information about the vulnerability could end up in the wrong hands or not reach those within the organization with the responsibility and in the position to take action. Another obstacle was that certain partners do not want Citrix to contact their customers directly, and that other customers also do not want direct contact with Citrix, for example to avoid liability, in the event that an organization is contacted by the manufacturer, but doesn't take action.

3.2.7 The NCSC was unable to make inventory of the number of Dutch organizations using Citrix software and of the effectiveness of the mitigation steps

During the occurrence, organizations could be warned using information gathered by security investigators scanning the internet for servers that were still vulnerable. NCSC received most scan information from third parties like the DIVD and Bad Packets (NCSC described the scan information as 'telephone directories' because of the size of these lists). The NCSC did not scan themselves, not even the systems of its own target group organizations (national government and vital operators) because legal objections to such actions had been expressed within the organization. Also, the interpretation of the legal framework resulted into the NCSC not passing on the data to the organizations representing these groups. The NCSC informed the organizations that belonged to its own target group (national government and vital) that could be derived from these lists.

84 See for example https://northwave-security.com/threat-response-citrix-gateway-adc-rce-cve-2019-19781/

Based on a decision by the director of the NCSC, other switching organizations within the National Covering System that had not yet been designated as CERTs or OKTTs and other organizations not being national government or vital were also informed (footnote: These are therefore also personal data and/or data as referred to in Section 20(2) of the Wbni).

At a crucial moment during the incident management process, when the social and administrative situation in the Netherlands escalated on 16 January, more uncertainty emerged because Citrix wrongly announced that the mitigation steps were not always effective. As a result, the NCSC lost confidence in the mitigation steps[85] and in addition to the information from the AIVD, this played a role in formulating the far-reaching security advice to shut down the Citrix servers. Organizations reported to NCSC that the mitigation was not effective, but the NCSC was unable to independently confirm whether the organization had implemented the mitigation steps incorrectly. The NCSC had no resources to determine the reliability of the mitigating measures itself; instead it was dependent on information from third parties. The resources did exist at the department of Defense, and they were used. Security companies including Fox-IT continued to argue (also in public) that there was no reason to assume that the mitigation steps would not be effective in all cases, based on the nature of the mitigation steps that would completely eliminate the possibility of abuse and based on its own experience with customers.[86] When the patches came out, NCSC did organize to get information that would allow it to make statements about the effectiveness of the patches.

The evaluations and interviews held by the Safety Board led the Board to conclude that at a crucial moment in the incident management process (namely at the moment of issuing the security advice to shut down the Citrix servers) the NCSC failed to note that Citrix had withdrawn its earlier notice that the mitigating steps were not effective for every version of the software.

3.2.8 Organizations did not receive all the available information for their independent risk assessment

As described in section 3.1.2 after receiving the advice from the AIVD, politicians and policy makers decided that the NCSC would urgently advise Citrix servers to be shut down. The NCSC operated on the basis of the principle that organizations were first and foremost responsible for making their own risk assessment, because they could determine whether or not implementing security measures had an impact on the security or the continuity of operations. The organizations wanted to know what additional information the urgent security advice from the NCSC was based on, as compared with the previous advice. They needed this information to make a risk assessment based on their own specific circumstances. It was relevant for them whether the new information was related to a specific threat against a particular organization, or whether it was a precautionary measure.

85 The NCSC indicated it had lost confidence in the mitigation measures due to messages received from users and confirmation from Citrix that the measures did not work for at least one version. Citrix states that they immediately retracted the message and that they know of no cases where the measures did not work.

86 Fox-IT, *Advisory on Citrix vulnerability*, 17 January 2020. "Based on all the current rumors and speculations about the Citrix vulnerability, we decided to list all the current known facts in an advisory."

All government organizations were required to inform CIO Rijk whether they had taken measures. The NCSC, the Minister of the Interior and Kingdom Relations and the policy departments of the Minister of Justice and Security also approached organizations that were not part of national government, and were not considered vital operators such as large municipalities and care institutions, with the request to comply with the urgent security advice from the NCSC. Organizations subject to multiple legal regimes (large telecom providers for example) were approached by multiple parties, causing them additional burden, while at the same time they had to fight the crisis. On 23 January 2020, the Minister of Justice and Security and the Minister of the Interior and Kingdom Relations organized a technical briefing for the Dutch House of Representatives, together with the NCTV deputy and the director of the NCSC.[87]

Different organizations consulted by the Safety Board indicated that despite believing that they had correctly implemented all the recommended mitigation steps, they still felt they had to shut down their systems as a precaution. The reason was that they were experiencing administrative pressure, and did not know what information the MIVD and AIVD had issued to the NCSC, nor what the purport of the advice was. The organizations were dependent on the NCSC and the AIVD for this information; they had no possibility of obtaining the information by themselves. The NCSC believed that it was not in a position to pass on this information to organizations outside national government.

3.3 Course of events of other illustrative occurrences

The occurrence where vulnerabilities in Citrix software led to security breaches in organizations is not an isolated event. In this section, we describe other occurrences involving software that fulfils a comparable function as the Citrix software (granting remote access to a digital system at an organization) and whereby vulnerabilities in this software had consequences for the cybersecurity of those organizations. The vulnerabilities that are addressed in this investigation are at present still among the vulnerabilities that are most commonly used in attacks.[88]

87 The Dutch House of Representatives was also one of the organizations that used Citrix and that had shut down its systems.

88 CISA, *Top Routinely Exploited Vulnerabilities* (thus far in 2021), 28 July 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-209a

Outages, accidents and attacks

In this section, we describe occurrences whereby vulnerabilities lead to attacks on organizations. Vulnerabilities in software can however also threaten the security of digital systems in other ways, thereby causing damage and injuries. In June and July 2021, for example, a large number of websites worldwide became inaccessible for a short period of time: newspapers, media, online stores, banks, cloud services and government services, such as the 911 emergency number in parts of the United States and the government domain in the United Kingdom. In both cases, the outage was caused by an error in the software of an Internet service provider used by multiple organizations to improve the speed and stability of Internet traffic to their websites. Software is not only used in digital systems but is also embedded, for example in vehicles, aircraft and chemical installations. Vulnerabilities in software, in combination with other factors, can in such situations lead to an accident.[89] In these cases, coincidence plays a greater role than in the event of attackers exploiting vulnerabilities and thereby using automated systems to identify all servers containing the vulnerability.

3.3.1 VPN software for the enterprise market[90]

Organizations use (enterprise) VPN software to give their employees a remote secure link and access to the company network. As with the Gateway software from Citrix, these VPN products fulfil a central role in the security of the underlying network. A small number of manufacturers dominate the market for these professional VPN products. Pulse Secure, for example, is used in more than 50,000 servers connected to the internet worldwide, in particular for large companies and governments; Fortinet is used by more than 480,000 internet-faced servers worldwide, especially by medium-sized organizations.[91] The number of servers using Palo Alto software is unknown to the Dutch Safety Board.

The search for vulnerabilities

In 2018 security investigators had noticed that until that time, relatively few vulnerabilities in certain enterprise VPN products had been published as compared with other comparable products. They wondered whether this was because the products contained so few vulnerabilities, or because despite their crucial role for the security of digital systems, these products represented a blind spot (in that little action was taken to search for vulnerabilities in these products). For that reason, in 2019 they went in search of vulnerabilities in VPN products from Fortinet, Palo Alto and Pulse Secure.

89 Outage internet service providers: https://www.fastly.com/blog/summary-of-june-8-outage and https://www.reuters.com/technology/websites-airlines-banks-tech-companies-down-widespread-outage-2021-07-22/
See for example a recall by Fiat Chrysler, due to a software vulnerability that meant that airbags were not activated in certain accidents. https://www.reuters.com/article/us-fiatchrysler-recall-idUSKBN1881I6

90 VPN stands for Virtual Private Network.
CVE 2019-11507/10 multiple vulnerabilities in Pulse Secure software (seriousness varying from 6 to 9 on a scale of 1 to 10).
CVE 2018-13379 vulnerability in Fortinet software (seriousness 9.8 on a scale of 1 to 10).
CVE 2019-1579 vulnerability in Palo Alto software (seriousness 8.1 on a scale of 1 to 10).

91 https://techcrunch.com/2019/07/23/corporate-vpn-flaws-risk/

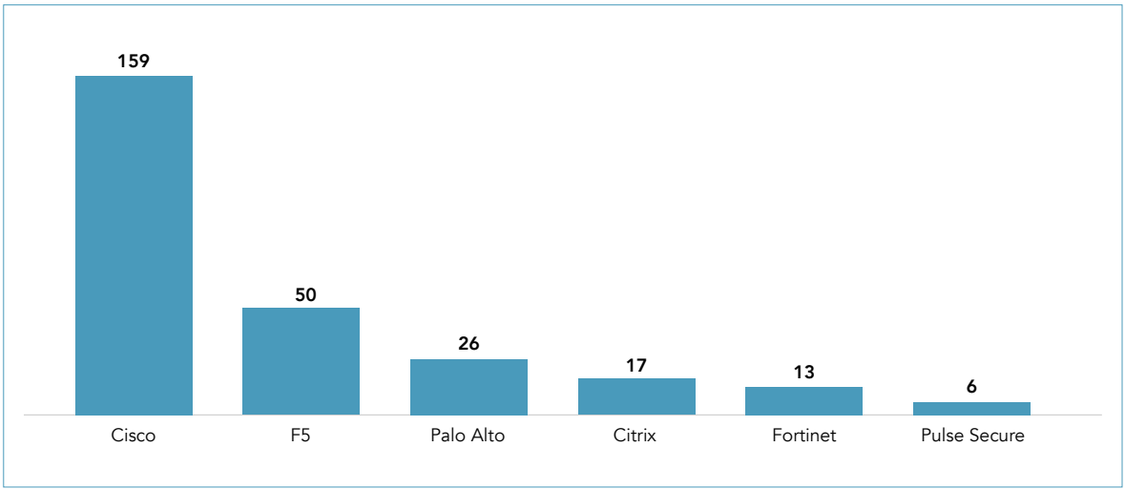


Figure 15: Analysis by security researchers of vulnerabilities in VPN products by the security investigators (no indication is given of the period to which this analysis relates). (Source: Blog of the security researchers)[92]

One obstacle for the security investigators was that the products are closed source. After breaking open the software (a process known as a jailbreak), they found a number of vulnerabilities. The most important vulnerability within the Pulse Secure product occurred after a new functionality had been added to the product in 2016 in version 8.2.

The security investigators reported the vulnerabilities first to the manufacturers and to the owners of the compromised company networks. They then shared their findings in technical journals, at conferences and on their own blog.[93] The incident response by the affected manufacturers varied: Pulse Secure published the vulnerability and a patch one month following the report by the security investigators. A month following the warning, the security investigators used the vulnerability to successfully penetrate Twitter. Fortinet dealt with its vulnerability after 7 weeks, and states to have published a warning at the same time. Palo Alto initially announced that it would not be publishing a warning, because it was already aware of and had repaired the vulnerability. After the security investigators had successfully penetrated Uber via the vulnerability in Palo Alto and had published about their activities, the manufacturer went on to publish a warning.

Between one day and one month after the security investigators had demonstrated how they could exploit the vulnerabilities in the software, it became apparent that attackers were actively scanning the internet for servers on which this vulnerability in the software had not yet been repaired with a patch. At that moment, many dozens of Dutch organizations had not yet implemented the update, including KLM, Shell, Boskalis, various defence-related companies, the Ministry of Justice and Security and Air Traffic

92 https://blog.orange.tw/2019/08/attacking-ssl-vpn-part-2-breaking-the-fortigate-ssl-vpn.html
93 https://www.defcon.org/html/defcon-27/dc-27-speakers.html#Tsai
https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf
https://devco.re/blog/2019/07/17/attacking-ssl-vpn-part-1-PreAuth-RCE-on-Palo-Alto-GlobalProtect-with-Uber-as-case-study/,
https://devco.re/blog/2019/08/09/attacking-ssl-vpn-part-2-breaking-the-Fortigate-ssl-vpn/
https://devco.re/blog/2019/09/02/attacking-ssl-vpn-part-3-the-golden-Pulse-Secure-ssl-vpn-rce-chain-with-Twitter-as-case-study/ Message Pulse Secure
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101

Control the Netherlands (LVNL). Most of these organizations implemented the update after August 2019.[94]

In August 2020, it was announced that attackers had compiled a list of stolen user names, passwords and IP addresses from around 900 vulnerable Pulse Secure VPN servers. The data appeared to have been collected between 24 June and 8 July 2020. The list was published on a forum commonly visited by ransomware gangs. In the summer of 2021, something similar happened: on an newly launched hacker forum, attackers published - possibly as a publicity stunt - a list of 500,000 login credentials for Fortinet VPN servers. These credentials were allegedly collected from servers still vulnerable to the vulnerability described in this section.[95] According to Fortinet of these numbers ultimately 140,000 credentials and 24,000 devices turned out to be exploitable.

In the months and years after publishing the vulnerabilities various national CERTs, including the American national cybersecurity agency CISA, and also the Dutch intelligence and security services, issued repeated warnings that various attackers, including state actors were exploiting vulnerabilities in the software to launch attacks on the digital systems of organizations.[96] The vulnerabilities in the software, just like the vulnerabilities in the Citrix software, had thereby become part of the international arsenal of cyberweapons.

94 Modderkolk, H., Intern netwerk honderden bedrijven en ministerie lang maandenlang wagenwijd open (title translates: Internal network hundreds of companies and ministry wide open for months), *Volkskrant* newspaper of 28 September 2019. Parliamentary Papers II 2019-2020, 26 643, no. 666 'Analysis of risks run due to the vulnerabilities in the virtual private network (VPN) software from the company Pulse Secure'. NCTV, Cybersecurity picture 2020, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z02670&did=2020D05619, https://blog.cyberwar.nl/2019/09/dutch-kwetsbare-pulse-connect-secure-ssl-vpn-in-nederlandse-ip-adresruimte-bevindingen-en-gedachten/ Koot, M., *Field Note on CVE-2019-11510: Pulse Connect Secure SSL-VPN in the Netherlands*.In: Digit. Threat.: Res.Pract.1, 2, Article 13, May 2020. https://dl.acm.org/doi/10.1145/3382765

95 https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/ (August 2020). https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/ (September 2021).

96 https://us-cert.cisa.gov/ncas/alerts/aa20-258a *Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity.* https://us-cert.cisa.gov/ncas/alerts/aa20-259a *Iran-Based Threat Actor Exploits VPN Vulnerabilities*, https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/, https://www.security.nl/posting/697797/FBI+waarschuwt+voor+misbruik+van+Fortinet+FortiOS-kwetsbaarheden

From vulnerability to cyberweapon in less than a week

In the summer of 2020, it became known that the BIG-IP software from the company F5 contained a vulnerability. This product fulfils a similar function to the previously described Citrix software. The product consists of various modules such as Local Traffic Management, DNS, access policy, firewall. On 30 June 2020, F5 announced that the management interface of the Traffic Management module in BIG-IP contained a vulnerability. On servers on which the management interface was connected to the internet, attackers without legitimate credentials could execute arbitrary malicious code on the server, thereby penetrating the digital system behind this module. The vulnerability was so serious that it was given a score of 10 on a scale of 1 to 10. This vulnerability caused considerable unrest, since it was announced just before the weekend of the 4th of July, a period in which many Americans have time off work. This hindered the timely patching of the vulnerability. Five days after F5 published the vulnerability, a security investigator had also published a method for exploiting the vulnerability. The method was so simple that the necessary code fitted in a single Tweet. Two days later, organizations using BIG-IP worldwide suffered attacks.[97]

Incident management

At the time of the vulnerabilities in Pulse Secure, Fortinet and Palo Alto, the DIVD had not yet been established. On his own initiative, one Dutch security investigator scanned the internet for servers containing the vulnerable Pulse Secure and Fortinet software, and passed this information on to the NCSC. The security researchers had also found vulnerable servers outside this target group. NCSC did not warn these organizations, without informing the security researchers. As with the Citrix incident, the legal frameworks were interpreted to allow NCSC to share this data in a limited way. Based on a decision by the director of the NCSC, other switching organizations were also informed, namely: organizations within the National Covering System that had not yet been designated as CERT or OKTT and other organizations not being national government or vital. These received personal data and/or information as referred to in Article 20, paragraph 2, Wbni. This was done on the basis of the potential social impact or on the grounds of social importance.

Months later, the vulnerabilities still continued to have consequences for the organizations using the software, even if in the meantime they patched the vulnerabilities. On 4 August 2020, for example, attackers of Pulse Secure servers published details they had obtained during attacks on more than 900 Pulse Secure servers. The information included login data of server managers (admin account details) and all user names and passwords of the local users.[98] In the meantime the DIVD had been established. On 5 August, the DIVD sent out warnings to the organization connected to the Dutch IP addresses appearing on this list.

97 Notice from F5: https://support.f5.com/csp/article/K52145254
https://www.bleepingcomputer.com/news/security/poc-exploits-released-for-f5-big-ip-vulnerabilities-patch-now/
and https://www.bleepingcomputer.com/news/security/us-govt-confirms-active-exploitation-of-f5-big-ip-rce-flaw/

98 https://csirt.divd.nl/cases/DIVD-2020-00009/

On 19 November 2020, a security investigator came across a list of 49,577 vulnerable Fortinet servers on the Internet, and the magazine Bleeping Computer published an article on this finding, on 22 November. On 25 November 2020, the DIVD started examining the list for Dutch organizations. Starting on 3 December 2020, The DIVD sent out the first warnings to these organizations.[99]

3.3.2 Wave of cyber-attacks via software vulnerabilities and supply chain attacks

The events described in the previous subsection were the precursor to a worldwide wave of cyber-attacks and data breaches via software vulnerabilities, whereby attackers also made use of security breaches at service providers to attack other organizations. This is a phenomenon known as *supply chain attacks*.

SolarWinds/SUNBURST

The escalation of cyberattacks started with the discovery of the SolarWinds/SUNBURST attack in December 2020. The Washington Post wrote on 13 December 2020 that various American governments had been hacked via the Orion software from the company SolarWinds. The attack was attributed to the Russian government. One security company had discovered that attackers had added malicious code to the software updates from SolarWinds, allowing attackers to gain access to all customers that had implemented the software update. Among the SolarWinds customers were American government organizations, major companies (including the security company that discovered the attack), NATO, the European Parliament, AstraZeneca and government organizations in the United Kingdom.[100]

Microsoft Exchange

Following the SolarWinds/SUNBURST attacks, four zero-day vulnerabilities were discovered in local installations of Microsoft Exchange server. Servers with these vulnerabilities suffered attacks, worldwide. These attacks were reported to Microsoft by security investigators. A link was suspected with the previous SolarWinds attack (it was alleged that the attackers had gained access to the source code for the software at Microsoft) but this has not been confirmed. Microsoft attributed the attack to an attack group backed by the Chinese government that targets infectious disease researchers, law firms, educational institutions and defense contractors. On 2 March 2021, patches were published, to fix the vulnerability. However, these patches were not able to rectify the damage or to remove the backdoors the attackers had already installed.[101]

99 https://csirt.divd.nl/cases/DIVD-2020-00012/

100 "Russian government spies are behind a broad hacking campaign that has breached U.S. agencies and a top cyber firm". *The Washington Post.* December 13, 2020. Gallanger, Ryan, Donaldson, Kitty, et al. (15 December 2020). "U.K. Government, NATO Join U.S. in Monitoring Risk From Hack". *Bloomberg News website.* Sanger, David E.; Perlroth, Nicole; Schmitt, Eric (December 15, 2020). "Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit". *New York Times.*

101 https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach#cite_note-Microsoft-CVE-3

'Cheese hack'
One of the companies attacked via the vulnerability in Microsoft Exchange was a Dutch logistic service provider. The attack shut down part of the dairy distribution chain, including the supply of cheese to supermarkets. As a result, this attack campaign in the Netherlands was given the nickname 'the cheese hack'.[102]

It is estimated that on 9 March 2021, 250,000 servers worldwide had become victims of these attacks, both in the US and in Europe. In the US, the attack was judged as being 1,000 times more harmful than the SolarWinds attack in December 2020, in terms of economic damage. This was because the Exchange attack affected large numbers of small and medium-sized enterprises, a driving force for the economy. In the US, at least 30,000 organizations had been hacked as a result of the vulnerability, by the start of March 2021. On 22 March 2021, Microsoft announced that 92% of the servers had been patched or mitigated.[103]

On 3 March 2021, the DIVD in the Netherlands started scanning for vulnerable servers in the Netherlands and the rest of the world. On 4 March, the DIVD sent a list of Dutch IP addresses to the NBIP, for notification. In total, the DIVD sent out more than 42,000 warnings. Later in March, they once again scanned for and warned Dutch organizations. By that time, around 15,000 servers were still vulnerable; in May there were still 7,000 vulnerable servers, in addition to a further 5,500 servers that contained vulnerabilities that were published in April.[104]

Tension between Microsoft and security investigators
Reports were published on 15 March 2021 that the exploit code submitted to Microsoft on 5 January 2021 may have been leaked and used by attackers. The media reported that this had led Microsoft to investigate the partner companies that had received early information about the vulnerabilities and patches. On that same day, reports suggested that there was unrest among security investigators because at the request of Microsoft (owners of GitHub), GitHub had deleted the code of an exploit. GitHub subsequently changed its terms and conditions, allowing GitHub to intervene to prevent the platform being exploited for the exchange of attack methods used in attack campaigns.[105]

102 https://nos.nl/artikel/2376492-oproep-na-kaas-hack-bestempel-voedselvoorziening-als-vitale-infrastructuur, Marc Hijink, "De les van het lege kaasschap" (The lesson learned from the empty cheese shelf), *NRC*, 2021. "Duizenden extra Exchange-servers kwetsbaar" (Thousands of additional Exchange servers vulnerable), *AG Connect*, 2021, consulted on 17 March 2021, https://www.agconnect.nl/artikel/duizenden-extra-exchange-servers-kwetsbaar.
103 https://www.techrepublic.com/article/how-the-microsoft-exchange-hack-could-impact-your-organization/
104 https://csirt.divd.nl/2021/05/14/Closing-ProxyLogon-case/
105 https://www.agconnect.nl/artikel/exchange-exploit-lijkt-uitgelekt-bij-melding-aan-microsoft, https://www.agconnect.nl/artikel/rel-na-wissen-exchange-exploit-door-github and https://www.theregister.com/2021/03/12/github_disappears_exploit/, https://thehackernews.com/2021/06/github-updates-policy-to-remove-exploit.html

Kaseya VSA software

July 2021 saw a new wave of cyber-attacks. Once again in the 4th of July weekend, hundreds of companies were attacked, worldwide. On this occasion, the attack was attributed to a Russian ransomware gang. In April 2021 Dutch security investigators affiliated to the DIVD had informed the company Kaseya that they had discovered vulnerabilities in Kaseya's VSA software. This software was used by IT service providers (also known as managed service providers or MSPs) for the remote management of their customers' digital systems and sometimes also by the companies themselves.. Before Kaseya was able to patch these vulnerabilities, the ransomware gang had launched its worldwide attack campaign. In Sweden, the attack led to a supermarket chain with 800 stores being forced to close its doors. Not because the supermarket itself had been affected via the Kaseya software, but because the company responsible for payment systems in the supermarkets had been attacked.[106]

3.3.3 Urgency and scale of unsafety constantly growing

The occurrences we describe in this chapter show that vulnerabilities continue to be widely exploited to carry out attacks and that new vulnerabilities constantly emerge. Vulnerabilities in software are therefore an increasingly urgent and serious threat to the digital security and safety of organizations.[107]

When a vulnerability in software is identified, organizations have ever less time to mitigate or patch the vulnerability before vulnerable servers suffer attacks, worldwide (see Annex D). This threat has further escalated over the past twelve months, because both criminal attackers and state actors are increasingly opting to launch their attacks via supply chain partners. Via supply chain attacks of this kind, attackers can hack into an organization's supply chain, literally via its weakest link. As a result, attacks can escalate in scale, while the potential for response of individual organizations to protect themselves against attacks via a supply chain partner is diminishing.

What the occurrences also demonstrate is that volunteer security researchers, such as through DIVD, played a crucial role in the response to the incident and information sharing. Indeed, they scanned the entire Dutch (and global) domain, which provided them with the necessary information to identify which organizations had not yet fixed the vulnerability and to warn these organizations...

106 After talks between President Biden and Putin, this ransomware gang disappeared from view for a time. Some see this as proof that it is effective to take (diplomatic) action internationally after cyberattacks from another country. https://nos.nl/artikel/2387973-nederlandse-ethische-hackers-probeerden-ransomware-aanval-te-voorkomen; "Swedish Coop supermarkets shut due to US ransomware cyber-attack," *BBC*, 2021, consulted on 4 July 2021, https://www.bbc.com/news/technology-57707530

107 CISA, Top Routinely Exploited Vulnerabilities, 28 July 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-209a

4 SYSTEM ANALYSIS

Chapter 3 analyzed the occurrence due to a vulnerability in Citrix software. This occurrence was not an isolated one. The chapter also analyzed similar incidents where vulnerabilities in software led to security breaches at organizations. In some cases, this directly impacted people's security and safety. This illustrates that vulnerabilities in software are not isolated incidents. They are symptoms of a larger problem. The occurrences reveal a common thread: organizations and the people who depend on them are exposed to digital unsafety. Unknowingly they use software that is vulnerable. In many cases, warnings do not reach them and organizations do not always have the resources to remedy the vulnerability.

Chapter 4 analyzes the problem at the system level. In so doing, we distinguish between the process in which software is developed; the process in which organizations select certain software to purchase and put into use; and the processes that take place after a vulnerability in the software is found (incident response). In addition, we address how stakeholders, such as manufacturers, organizations that use software, and the government as policymaker, learn from digital incidents. We also address the role that the international context plays in managing insecurity and unsafety due to vulnerabilities in software.

4.1 Producing and releasing software on the market

Software fulfils a crucial role in the functioning of digital systems within organizations. Software is for example used to gain access to the company network from home, and as such forms the link between the internal and external network (Internet). Products of this kind therefore play an essential role in safeguarding cybersecurity.

Vulnerabilities are always inherent in software products, some of which lead to major safety risks. These risks are real and there have already been several examples, with disruptive consequences for public services. A vulnerability in a software product for example (indirectly) led to serious disruptions in service provision by Dutch municipalities (it was no longer possible to pay supplementary benefits to local residents) and a hospital (patients were no longer able to access their personal files and no information could be exchanged with other hospitals). Chapter 3 described examples of vulnerabilities in such products and their consequences. In this section we discuss how it is possible that software contains vulnerabilities and how manufacturers estimate the risk of these vulnerabilities and their consequences, and take measures to prevent or limit those consequences.

In 4.1.1 we describe the factors that explain why vulnerabilities can emerge in software and we describe the incentives that affect those factors. In 4.1.2 we then outline the measures taken by manufacturers to discover vulnerabilities, both before and after the software is released, the difficulties this process involves, and the dilemmas the

manufacturers face. Finally, in 4.1.3 we consider the patching of vulnerabilities and the manufacturer's role in incident response.

4.1.1 Preventing vulnerabilities in the lifecycle of software

Vulnerabilities can arise at any point in the lifecycle of a software product. For example, a vulnerability can emerge during the initial development of a new product, but equally during the renewal or improvement of existing software, in the form of an upgrade, or sometimes even as a consequence of fixing another vulnerability. Interviews with manufacturers and literature studies show that a number of factors contribute to the emergence of vulnerabilities during the lifecycle of a product. Below we discuss a number of factors.

Software products have a history

The first factor relates to the history of the development of software products, which is sometimes long and complex. Over time, manufacturers add new functionalities to existing software packages on multiple occasions, therefore building on an existing product. In certain cases, the original code of the software package (the foundation) is more than twenty years old. Changing needs and increasing digitization in society mean that software is taking on a different role. As a result, a software product is never finished. Manufacturers respond to this time and again by using existing platforms and adding extra functionalities, or reusing existing components.

Because manufacturers repeatedly add additional functionalities, the number of lines of code increases, and the software becomes more complex.[108] It is not uncommon for a software product to consist of more than one million lines of code.[109] Interviews and literature studies show that even with an extended framework for product development, safely maintaining such huge quantities of code is a significant task. Manufacturers therefore oftentimes restrict themselves to fixing the specific vulnerability as published in the CVE.[110] Dealing with the underlying cause in the foundation of the product (programming language, components, architecture) can require the complete rebuilding of the product. Manufacturers consider this to be too costly. Large software companies are often stock exchange-quoted companies and financial considerations play a role. However, the development history of software sometimes means that a product has grown in such a way that fixing a vulnerability is nothing more than tackling symptoms. In reality, a complete revision of the basis of the product may be needed to truly solve the (safety) problem.

108 https://www.extremetech.com/computing/259977-software-increasingly-complex-thats-dangerous.
109 https://www.informationisbeautiful.net/visualizations/million-lines-of-code/.
110 Common Vulnerabilities and Exposures. A public list of known weaknesses in software. The list appears on https://cve.mitre.org. (Source: Cybersecurity Alliantie, *Cybersecurity Woordenboek*, 2019, https://www.cybersecurityalliantie.nl/binaries/cybersecurityalliantie/documenten/publicaties/2019/09/30/cybersecurity-woordenboek/VCNL-Woordenboek-2eDruk-webversie-Final-2.pdf).

Programming language

A second explanatory factor that can also influence the emergence of vulnerabilities is the programming language used. The programming language currently most commonly used (C/C++) is recognized as being 'unsafe', because it allows programmers considerable leeway to make mistakes.[111]

Manufacturers have access to a series of general tools for eliminating whole classes of vulnerabilities, or mitigating their effects. Around half of the security breaches over the past few years have been related to vulnerabilities in memory security, that can be rectified by writing code in more secure languages such as Rust, or by subjecting the existing C/C++ code to verification tools.[112]

According to research, it is unattractive for manufacturers to protect software development against vulnerabilities: it makes the software slow, and during the programming process, the programmers receive so many (sometime erroneous) error messages that they switch off the security system.[113]

It is also not possible with all programming languages to use tools to detect vulnerabilities during the development process.[114] In the Citrix case, for example, the fact that the programming language Perl was barely supported if at all by these scanning tools played a clear role. See also 4.1.2 on what manufacturers do to discover vulnerabilities, and the obstacles they come across.

Use of standard components

The third factor is the use of standard components. When developing software, manufacturers make regular use of existing (open source) software components. Examples are the Apache and NGINX HTTP server, that are often used as the basis for software with web functionality. A manufacturer can also reuse components from their own existing software or from software that was previously made by an acquired company..

By reusing other components and the associated code, the manufacturer also incorporates all (undiscovered) vulnerabilities contained in that code.[115] Once the code has been integrated in the developer's own package, it takes a great deal of effort to

111 The basis for the SSL VPN (a virtual private network that uses the SSL or TLS protocol) and much other software is C/C++. Programming languages like C enable programmers to write code at a higher level of abstraction. This refers to the proximity of the programming language to the hardware. At a higher level of abstraction, developing software becomes simpler and more understandable than at a lower level, whereby more specific machine instructions are needed. However, that too can lead to errors. C is a programming language which is recognized as being 'unsafe', because in this language, working memory management is carried out manually (Kroes, T., *How to Keep Your Memory Safe and Your Software Fast,* 2020; AG Connect, *Einde van de oneindige reeks softwarefouten in zicht,* 2021). This is error sensitive and the majority of SSL VPNs use their own additions to existing programming languages. This can lead to simple memory errors; the most common source of software bugs and an important area of attack for attackers (see https://www.zdnet.com/article/microsoft-70-percent-of-all-security-bugs-are-memory-safety-issues). Nonetheless, C remains one of the most widely used programming languages.

112 Anderson, R., *Security Engineering*, 2020.

113 Kroes, T., *How to Keep Your Memory Safe and Your Software Fast,* 2020 https://research.vu.nl/en/publications/how-to-keep-your-memory-safe-and-your-software-fast

114 Tjong Tjin Tai, E. and Knoops, B., Duties of care and diligence against cybercrime *(Nederlands Juristenblad 24-04-2015*, volume 16), 2015.

115 AG Connect, *Veel kritieke lekken door open source in standard apps, (numerous critical leaks caused by open source in standards apps),* 2021. https://www.agconnect.nl/artikel/veel-kritieke-lekken-door-open-source-standaard-apps

update the underlying component in the event of a vulnerability. By that stage, the software package is after all dependent on a particular version of the component. In addition, manufacturers do not always have access to the relevant knowledge to be able to update components produced by others.[116]

Architecture

The fourth factor that contributes to the presence of vulnerabilities relates to the situation when the different layers that make up the architecture of the product are mutually inconsistent. For the functioning of the software, it is essential that the various components that make up the software match successfully. The matching of the various components must have been achieved in a controlled manner, under the supervision of a person with considerable experience, and sufficient knowledge and who has a major stake in the security of the product.[117]

Configuration

A last factor, which does not necessarily contribute to the emergence of vulnerabilities, but can limit their impact, is the way in which the software is configured by the manufacturer (the default settings). This includes which rights are granted to different types of users, how these rights are set by default, and whether it is possible as a customer to restrict these rights.

A range of factors contribute to the emergence of vulnerabilities during the lifecycle of a product. In many cases, existing products undergo further development, making the software increasingly complex. The programming language used can also contribute to the occurrence of errors, and the use of existing components and (inconsistent) layers in the architecture may introduce vulnerabilities.

Whenever (safety) problems are linked to fundamental choices in the product, this can represent an obstacle for the manufacturer in tackling the root of the problem. Such an approach after all requires an investment in the form of money and/or capacity for problem solving. The decision by the manufacturer to instead opt to only fix the vulnerability is explainable, but to truly solve a (safety) problem, it is sometimes necessary to fully revise a product from the base up.

4.1.2 Identifying vulnerabilities during the lifecycle

Manufacturers have established processes for detecting vulnerabilities during the development and use of a product. In this section, we discuss in more detail the measures that manufacturers can take in order to find vulnerabilities, together with the dilemmas they can face.

116 Tsai, O., *Infiltrating Corporate Intranet Like NSA*, 2020. https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf
117 Anderson, R., *Security Engineering*, 2020.

Action perspective of the manufacturer

Manufacturers detect vulnerabilities by carrying out a series of different tests both before, during and following completion of the development process. For open source software, the source code is openly available to anyone. This means that errors in the code can be unveiled by third parties, even if they are not specifically requested to do so. This is not possible for closed source code, and it is up to manufacturers to take the initiative to carry out an audit.

Manufacturers can be expected to carry out constant security analyses of the entire architecture of the product (see reference framework: the role of the manufacturer and user in chapter 2). Manufacturers use a variety of methods for developing software, for example the Secure Development Lifecycle (SDLC).[118] Part of this involves the manufacturers testing for vulnerabilities at various moments during the development process (during initial development and when releasing patches). These tests are carried out on individual components (unit testing), the integration between components (integration testing) and on the entire product (audit[119] or security code review).

By using automated tools, manufacturers are able to remove more vulnerabilities from software. In this way, they hope to extend the lifecycle of the software. However, the security code reviews of the entire product do not always recognize the type of vulnerabilities relevant in this case. Vulnerabilities are not (always) the consequence of errors in the source code, but may also be the result of integration problems within the product. To detect vulnerabilities of this kind, the manufacturer can also opt to have the product extensively tested for its intended functioning (end-to-end testing). Interviews with manufacturers reveal that for older products, end-to-end testing can be very time consuming, because older products often consist of large volumes of source code.

Manufacturers can also search for vulnerabilities without directly giving third parties access to the source code. Many manufacturers operate bug bounty programmes, according to which in exchange for a reward, ethical hackers search for vulnerabilities in the software. These ethical hackers use manual search methods, firstly aiming their search at easily identifiable vulnerabilities that are the result of fundamental design choices and problems in the integration or configuration.

Many of these bug bounty programmes are open to anyone, but certain manufacturers also opt for a closed variant or decide not to operate any form of bug bounty programme. Manufacturers are sometimes also sent information about vulnerabilities from the bug bounty programmes of other parties, such as suppliers or customers. For example, at the time of the incident Citrix operated only a closed bug bounty programme; the company has however recently launched an open programme.

118 See for example https://owasp.org/www-pdf-archive/Jim_Manico_(Hamburg)_-_Securiing_the_SDLC.pdf

119 Part of the audit performed by the manufacturer is for example threat modelling (identifying threats and mitigating measures) and pen testing (testing for vulnerabilities and attempting to hack into the system). Pen tests can in part be automated, but this test software can also contain vulnerabilities (see for example https://arstechnica.com/gadgets/2021/08/critical-cobalt-strike-bug-leaves-botnet-servers-vulnerable-to-takedown/).

Manufacturers are required to maintain an overview of their customers, those who bought a software product (see reference framework in chapter 2). This enables the manufacturer to warn its customers quickly, in the event of a vulnerability. Not all manufacturers have an up-to-date overview of the customers of their products. This is because products are not always sold directly to the customer; there are often a whole raft of intermediaries. Interviews revealed that certain manufacturers have solved this problem by linking contact details of the customers to their own overview, even if the product is sold via an intermediary. From the safety perspective, it seems obvious that manufacturers have an overview of the customers of a product. However, it may present a dilemma that affects, among other things, the autonomy of the customer. For instance, it is not possible to force customers to register themselves with a manufacturer and to provide transparency on how the system is installed.

A trend that has emerged over the past few years is for manufacturers to migrate their products to the cloud (Software as a Service) in order to improve test capability and to install patches on their customers' systems more quickly. This makes the patching of a product the responsibility of the manufacturer. However, it does involve certain disadvantages for the customer, see section 4.2.

Asymmetry: manufacturer needs to find everything; hackers need just one leak

Manufacturers have to put a lot of time and effort into detecting vulnerabilities, both before and after the software is released. Using such techniques as end-to-end testing, it is possible to remove many vulnerabilities from the software. However, searching for just a single vulnerability takes a great deal of effort. In terms of prevention, manufacturers are already doing everything they can. Problems in software that has been in use for a longer period of time (see the development history in subsection 4.1.1) are unavoidable given the extent of the product and the prevention paradox. It is after all not possible to detect all vulnerabilities.

For their part, attackers attempt to find a vulnerability in a system with different methods, for example a brute-force attack. They sometimes launch their attacks in response to specific clues (for example using information from a CVE), but they regularly also come across a vulnerability by coincidence. Attackers sometimes need just a single leak in order to gain full access to a system. This reveals an imbalance between attacker and defender (manufacturer).

Whereas in the past attackers themselves needed to search the Internet for vulnerable servers (a time-consuming process), the use of services that scan the Internet have made this process far easier.[120] Using scan services of this kind, attackers can easily purchase a list of IP addresses relating to a (just published) CVE. This means that after discovery of a vulnerability attackers have immediate access to a list of potentially vulnerable servers.

120 For example Shodan (https://www.shodan.io), a search engine that scans the Internet and indexes accessible IP address and port combinations. If a server is indexed, then it can be approached over the Internet. This does not automatically mean that the server is also vulnerable. That is something the hacker has to determine.

Relationship between manufacturers and ethical hackers / red teams

Ethical hackers make an important contribution to the identification of vulnerabilities. Bug bounties (earning a reward for reporting a vulnerability) are relevant incentives in this regard. The majority of major manufacturers operate a bug bounty programme[121] that offers ethical hackers an opportunity to earn money by identifying and reporting vulnerabilities. Finding and publishing about a specific vulnerability can also increase the name awareness of a hacker or group of hackers. This mechanism, in combination with the potential financial gain, means that third parties regularly go in search of and subsequently find many vulnerabilities.

At the same time, vulnerabilities increasingly represent a potential attack route (see subsection 4.1.3) and preventing and fixing these vulnerabilities requires tremendous effort on the part of manufacturers (see subsection 4.1.1). In that sense, it would help the manufacturers, and help protect systems if the vulnerabilities were kept secret. It is possible to publish about vulnerabilities without revealing the specifics of a vulnerability. But some manufacturers deliberately choose not to disclose all (information about the presence of) vulnerabilities.[122] This approach, however, is diametrically opposed to the timely disclosure of information about vulnerabilities for mitigating and responding to potential risks. There is a clear incentive for preventing information about vulnerabilities becoming public. Disclosure makes it possible for customers to countermeasure the consequences but at the same time leads to a new security problem: a dilemma.

Parties that discover a vulnerability do not always report their discovery to the manufacturer. Vulnerabilities in software are a tradeable commodity, that is not only reported to the manufacturer (sometimes in return for a reward), but that can also be offered to the highest bidder. For state actors and criminals, obtaining a list of unknown vulnerabilities which they themselves can subsequently exploit can prove attractive.[123] Commercial spyware products are also available for sale. It is unclear whether these products are based on unknown vulnerabilities, and it is also uncertain which parties are offered these products, and for what purpose they are used.[124]

121 For a list of bug bounty programmes, see for example https://www.bugcrowd.com/bug-bounty-list

122 For example Palo Alto, where according to the security researcher that found the vulnerability, no CVE was published about a vulnerability (which had in fact already been repaired by the manufacturer) in GlobalProtect. Source: https://blog.orange.tw/2019/07/attacking-ssl-vpn-part-1-preauth-rce-on-palo-alto.html. It is unclear whether Palo Alto communicated with their customers about the vulnerability through direct channels. The Safety Board was unable to verify this because Palo Alto did not respond to our requests to cooperate with the investigation.

123 Perlroth, N., *This is how they tell me the world ends: the cyberweapons arms race*, 2021.

124 https://www.wired.com/story/nso-group-hacks-ios-android-observability/
https://www.nrc.nl/nieuws/2021/07/26/de-overheid-moet-stoppen-met-gebruik-van-zero-day-software-a4052412

Ethical hackers are encouraged with rewards to identify and report vulnerabilities in software. As a result, many vulnerabilities are identified. In addition, manufacturers detect vulnerabilities by carrying out a variety of tests. Nonetheless, it is not possible to find *all* vulnerabilities. It is becoming more common for vulnerabilities to form an attack route. Disclosing a vulnerability can help organizations better arm themselves against potential exploitation, but it can also enable attackers to exploit the vulnerability. This is reinforced by the fact that sometimes hackers need just a single leak in order to gain access to a system, also because it is relatively simple for them to find vulnerable servers. This creates a dilemma which in turn reduces overall safety.

4.1.3 The role of vulnerabilities in cyber (in)security

Vulnerabilities are playing an ever growing role

Each year, organizations are exposed to a large and ever growing number of vulnerabilities. In 2020, more than 25,000 vulnerabilities were identified. Of these vulnerabilities, 18,000 were published in 2020 with a CVE number[125] (see Figure 16). Only a small proportion of the number of published vulnerabilities (around 3%) are used to hack organizations and/or individuals. An even smaller proportion (0.5%) are successfully used in practice to launch a widespread attack as described in the security breaches in chapter 3 (see Figure 17). Nonetheless, numbers are growing, and experts warn that we are just seeing the tip of the iceberg.[126]

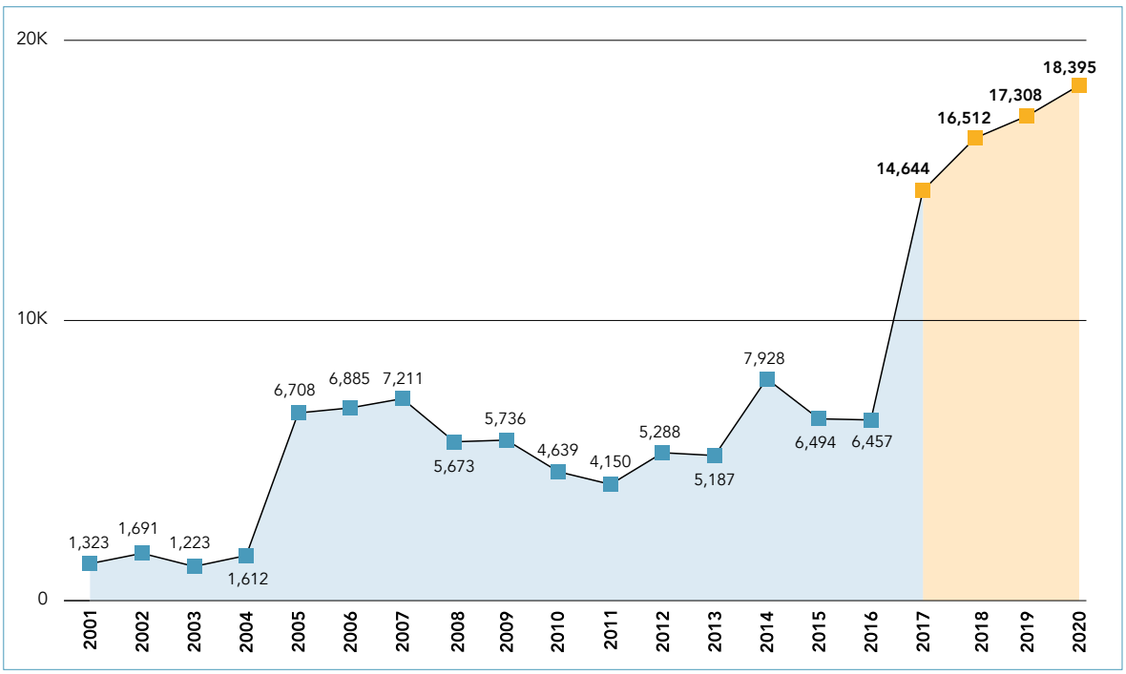


Figure 16: The number of CVE reports per year. (Source: Trend Micro)

125 There are also many vulnerabilities that are fixed by the manufacturer without disclosure. https://vulndb.cyberriskanalytics.com/#statistics

126 AG Connect, *Einde van de oneindige reeks softwarefouten in zicht (End of an infinite series of software errors in sight)*, 2021.

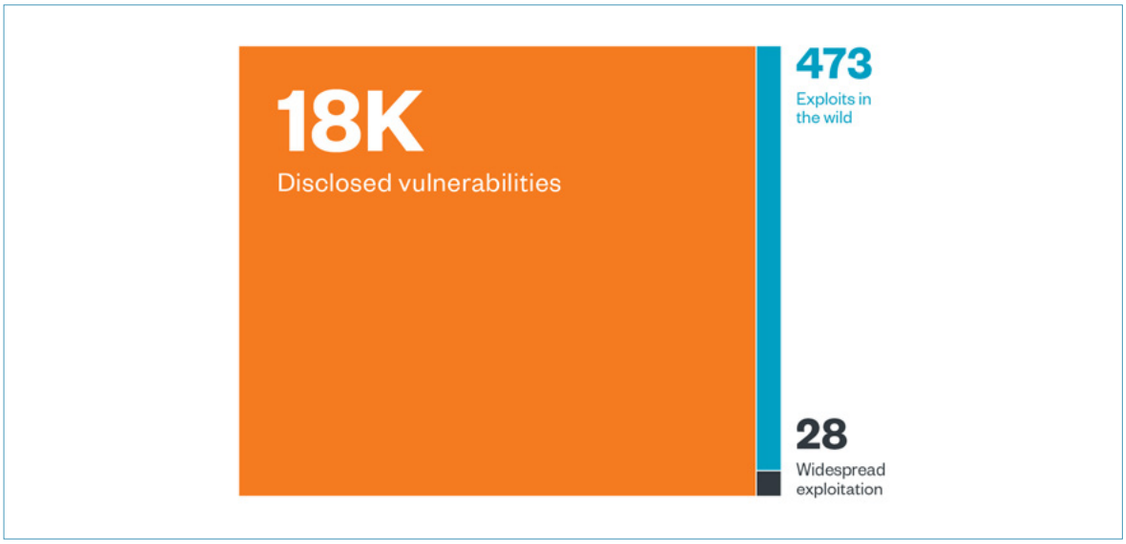


Figure 17: The number of exploits of widespread attacks in relation to the total number of reported vulnerabilities. (Source: Trend Micro)

The consequences of these attacks are also increasing in scale. In its Cyber Security Assessment Netherlands (CSAN) 2020, the Dutch National Coordinator for Security and Counterterrorism (NCTV) warned of attackers searching for weak links in the supply chain, as the next step towards attractive targets and the resultant serious consequences.[127] Whereas in the past a vulnerability in a software package did not automatically result in serious consequences, today they can have far-reaching consequences for the underlying dependent systems, as illustrated by the supply chain attacks using the vulnerabilities in SolarWinds and Kaseya (see section 3.3 for a brief analysis).

In other words, vulnerabilities such as those described in the occurrences investigated by us are playing an ever greater role in cyber-attacks and are increasingly being used by attackers as the starting point to launch an attack.[128] Above all large organizations (such as governments and vital operators) run the risk of being attacked according to this target vector.[129] It has become clear since 2020 that the exploitation of vulnerabilities in software to launch ransomware attacks is an economically attractive method for ransomware gangs.

Growing numbers of widespread attacks using a vulnerability demonstrate the importance of the timely patching of software and/or the mitigation of a vulnerability. The use of software introduces risks. For instance, for organizations it is not always possible to predict which of the vulnerabilities will eventually form a risk for their organization. This depends for example on how easy it is to actively exploit the vulnerability in the software, whether a mitigation is available and how easily it can be

127 NCTV, *Cybersecuritybeeld Nederland 2020*, 2020. https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020

128 Modderkolk, H., 'Overheid doet te weinig tegen ransomware' *(Government failing to take sufficient action against ransomware)* (*De Volkskrant*, 4 August), 2021; CISA, Alert (AA21-209A) Top Routinely Exploited Vulnerabilities, 2021

129 Coveware, *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound*, 2021. https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

implemented, and the version and configuration of a product. Fixing vulnerabilities by implementing a mitigating measure or installing patches requires an investment by the organization. In most cases, they do not immediately get more security, in return.

For manufacturers and organizations that use the software, prevention, timely mitigation or patching of a vulnerability do not represent the only lines of defence. Section 4.2 considers in more detail the measures that organizations can take to mitigate the safety risks of vulnerabilities in software. Examples are the use of a firewall to restrict access to the network, and the use of redundant hardware and software, so that when a vulnerability is made public, it is possible to switch rapidly to another product.

Problems with patching and mitigating

If a manufacturer has placed software on the market that subsequently turns out to contain a vulnerability, as a rule the manufacturer publishes a patch and advises organizations to patch the software. If no patch is yet available, a manufacturer can also publish a mitigation measure to remove the acute danger. However, patching and mitigating are not always easily implemented solutions.

Patches and mitigations represent a certain degree of risk, too. The effect of a patch or mitigation on software that is already configured and in use cannot always be predicted. Every mitigation and patch can result in (partially) unforeseen consequences, for example for the compatibility of adjacent/connected systems. In certain cases, patches can even cause disruptions or the entire failure of systems.[130] Patches and mitigations can also introduce new errors in the software or introduce vulnerabilities, as for example was the case with the Microsoft patch aimed at solving the problems with the print spooler, which led to problems with printing.[131]

Vulnerabilities in software formed an escalation factor. The occurrences in this investigation are clear illustrations. After the vulnerabilities had become known (for example through the publication of a CVE or a security bulletin), attackers used automated tools to search for servers that had not yet been patched, and to subsequently launch attacks. A mitigation measure can also provide information about how a vulnerability can be exploited. The occurrences in this investigation reveal that this can take place in a period of just a few days (or that the attacks had already been carried out, in the event of a zero day). The publication of a vulnerability can be the lead-up to widespread attacks.

Problems with patching can also arise on the side of the user. Because of the large number of patches published each year, it is for example not always possible to install everything in a timely fashion. Organizations are also not always in possession of an up-to-date overview of which software needs to be patched, they often have limited insight into underlying (vulnerable) components contained in a software package, and they are not always convinced of the necessity of patching. This is discussed in more detail in section 4.2.

130 https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond
131 https://www.zdnet.com/article/microsofts-printnightmare-patch-is-now-causing-problems-for-some-printers/

The release of a mitigation measure before a patch is published can be good practice, because following its publication, organizations as a rule implement the measure without delay. In this way, a manufacturer ensures that the end user's software is safe. The disadvantage is that certain organizations then consider patching to be even less necessary.

The number of vulnerabilities in software is growing, as are the consequences of attacks. Vulnerabilities play an increasingly important role in cyberattacks, and can be used by attackers as the starting point for launching an attack. This underpins the importance of timely patching. However, patching and mitigating at the same time pose a risk, because they can lead to disruptions or the introduction of new vulnerabilities. The organization must therefore think through the decision to patch carefully from the perspective of the organization's IT landscape. The publication of a vulnerability can be the precursor to widespread attacks.

4.1.4 Incentives for more secure software

In addition to the more intrinsic factors relating directly to the development process at the manufacturer, other factors relating to regulation and liability also play a role in the emergence of vulnerabilities.

At present, government and other organizations have few possibilities for requiring software manufacturers to safeguard cybersecurity in their products. As a consequence, problems arising from vulnerabilities largely come to lie with the user of a product. Users must therefore be particularly aware of this fact when purchasing software. Once purchased, users can do little more to check whether a product is safe.

Position of end users in relation to the manufacturer

Certain (large) users, such as government organizations and vital operators, are able to use advanced software and extensive analyses to search for vulnerabilities in software, for themselves. However, not all customers are in a position to test or reverse engineer the software for themselves, or to autonomously perform a full risk assessment (see also section 4.2 on information asymmetry and transparency). Interviews also reveal that not all organizations know how to lay down and enforce requirements and hold a manufacturer accountable. Manufacturers usually have agreements stipulate that they have limited liability for the consequences of any vulnerabilities in software. This makes vulnerability a problem for the user and not the manufacturer.

In addition, in the conditions they impose on the purchase and use of their software, manufacturers prohibit users from 'opening up' the product to see how it works, and to identify the components that make it up. This restriction is imposed by manufacturers on the basis of corporate confidentiality. These agreements form obstacles to organizations in subjecting the product to their own examination, and reporting vulnerabilities that are found during such an examination. Finally, via their terms and

conditions, manufacturers specify that they cannot be held liable for the consequences of vulnerabilities in the software.[132]

Statutory requirements

Besides the imposition of requirements on a software product by the users, few other requirements are imposed by government for placing software on the market, maintenance during the lifecycle and the role of the manufacturer during incident management. The Wbni[133] Act requires providers of essential services to take security measures with respect to their network and information systems (e.g. reporting cybersecurity incidents), but this does not apply to software manufacturers. The above observation shows that in this system of parties, in particular with regard to legislation and regulations, there is a clear shortfall on the side of the manufacturers.

National initiatives

There are a series of initiatives aimed at arriving at legislation and regulations for the placing of software on the market. The Dutch ministry of Economic Affairs and Climate Policy and the ministry of Justice and Security, for example, have come up with an initiative in the form of the roadmap for Digital Hard- and Software Security (roadmap DVHS) in which they propose a package of measures aimed at preventing security problems in hardware and software, to detect vulnerabilities and to mitigate their consequences.[134] The measures in this roadmap are aimed both at prevention, detection and mitigation and include statutory requirements and the imposing of liability on manufacturers for damage suffered as a consequence of cyber insecurity. Concern for liability should serve as an incentive for manufacturers to take preventive measures or to limit damage. These measures are aimed specifically at smaller devices (IoT[135]), but are universally applicable to other types of software. The question that emerges is to what extent these measures should also be applied to safety-critical software and software in general.

International initiatives

Various international governments have taken the initiative to tackle the shortcomings in legislation and regulations. On 27 June 2019, the European Cybersecurity Act came into effect.[136] These new rules for cybersecurity among others reinforce the mandate of ENISA[137] and introduce a cybersecurity certification framework. Another recent example of an initiative in the field of legislation is the US cyber legislation, that imposes requirements on software purchased by government.[138] Australia also has plans for

132 Cyber Security Council (CSR), *Integrated approach to cyber resilience*, 2021; Tjong Tjin Tai, E. and Knoops, B., Duties of care and diligence against cybercrime (*Nederlands Juristenblad* 24-04-2015, volume 16), 2015; Anderson, R., *Security Engineering*, 2020.

133 Security of Network and Information Systems Act (Wbni) for digital service providers, see https://wetten.overheid.nl/BWBR0041515/2021-07-01

134 Ministry of Economic Affairs and Climate Policy and ministry of Justice and Security, *Roadmap for Digital Hard- and Software Security*, 2018.

135 Internet of Things, for example a smart TV, a smart refrigerator, connected temperature sensors, etc.

136 https://ecer.minbuza.nl/-/europese-cyber-security-act-van-kracht; https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

137 Originally the European Network and Information Security Agency, currently called the European Union Agency for Cybersecurity

138 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, https://www.nytimes.com/2021/05/12/us/politics/biden-cybersecurity-executive-order.html

improving the regulation of cybersecurity.[139] The focus of this proposal is on IoT and organizations processing personal information. With regard to software safety, Australia is concentrating its efforts on stricter agreements on responsible disclosure as an incentive for manufacturers to accelerate the patching of vulnerabilities. In China, the exploitation of vulnerabilities is punishable by law, and sanctions are to be introduced for manufacturers that fail to release patches for reported vulnerabilities.[140]

In its latest report of recommendations, the Cyber Security Council (CSR) concluded that despite a number of important initiatives, both within the European Union and the Netherlands, there is still no comprehensive mechanism of responsibility for hardware and software security.[141] According to the CSR, manufacturers must be held more responsible for economic damage as a consequence of failing in their duty of care with regard to cybersecurity. This duty of care should help protect citizens and businesses against cybercrime.

Enforcement

If the enforcement of statutory requirements is implemented by means of certification of software, there remains a risk of perverse effects. The certification body after all has a business model in respect of the parties wishing to be certified, while for the certification of its software, a software manufacturer can opt for the route of least resistance. Competition between the different certification bodies does not always bring about improved standards and can in fact result in a race to the bottom (the principle of *maximum complacency,* whereby the manufacturer opts to have certification by a single certifying body confirmed, and objects to any attempt to encourage it to improve its product).[142]

139 Commonwealth of Australia, *Strengthening Australia's cyber security regulations and incentives*, 2021.
140 https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/.
141 CSR, *Integrale aanpak cyberweerbaarheid (Integrated approach to cyber resilience)*, 2021.
142 Anderson, R., *Security Engineering*, 2020.

Past experience: Common criteria, ISO 27001 and BitSight

Common Criteria
The Common Criteria for Information Technology is an international standard for computer security. This standard faces a number of problems: certification costs are high, the standard is described in generic terms (the technology has been left out, including usability, an essential parameter for security), the standard is not capable of responding successfully to rapid developments in practice/application, there is no uniformity in the application of the standard (for example strict in Germany, very loosely defined in the Netherlands) and the standard includes no elements of liability.

ISO 27001 standard
The ISO 27001 standard[143] above all works for businesses as a means of earning money. Certification costs a great deal and is a source of income for the certification bodies. When a company applies for a certificate, the certification body is dependent on the information provided by the company. It is therefore possible for the applicant to indicate that certain security measures have been taken, while they have not actually been implemented in practice. There is no actual independent evaluation. Almost all major leaks have occurred in companies certified according to the 27001 standard.[144]

BitSight
Unlike the ISO 27001 standard, a private sector initiative, BitSight is a company that monitors the Internet in search of servers of companies and government institutions. Any server that is discovered is scanned and awarded a security score (for example on the basis of how many of its servers are (not) patched). As a consequence, BitSight is not dependent on information provided by companies (the applicants in ISO 27001 certification) and arrives at a score, on the basis of its own scans. However, this too has negative effects. For example, companies are cautious in deliberately linking vulnerable servers to the Internet (for example for training employees, students, etc.). As soon as servers of this kind are observed by BitSight, this has a negative influence on the company's security score.

Enforcement is only possible if manufacturers are required to be transparent about how their software works, in such a way that third parties are able to assess its safety. The Executive Order on the improvement of cybersecurity in the US focuses on this point and identifies an urgent need for stricter and more predictable mechanisms for ensuring that products function more safely, in accordance with their intended purpose.[145]

143 An ISO standard for information security. See https://www.iso.org/isoiec-27001-information-security.html
144 Anderson, R., *Security Engineering*, 2020.
145 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Economic incentives

The examples in this investigation reveal that software products are dynamic. This is because they are regularly updated for the addition of new functionalities and for repairing vulnerabilities. At the same time, these products often have a long history, as they can be built on existing components. This can make it a costly investment for manufacturers to tackle the root causes of any insecurity, as described in section 4.1.1. Tackling root causes would require them to rebuild software that is the result of decades of development.

There are few economic incentives to compensate for this investment. Insurers not only insure organizations that use software but also the manufacturers that make the software. In this latter role, the insurers demanded of the manufacturers that they pass on liability for the consequences of unsafe software to the actual organizations that use the software. The Cyber Security Council writes that insurers ideally impose requirements on both the manufacturer and the organization using software.[146]

A manufacturer can also experience an economic incentive if the value of its shares falls as a result of an insecure system (shareholders). Shareholders of SolarWinds, for example, sued the company: according to the shareholders, the private equity companies that own SolarWinds sacrificed cybersecurity in favour of short-term profit ('goldrush among investors in SaaS business').[147]

In addition, the material obligation to remove software insecurity can deliver an economic incentive for a manufacturer to do more to prevent software with vulnerabilities being placed on the market. At present, this economic incentive lies exclusively with the users of the software.

146 CSR, *Integrale aanpak cyberweerbaarheid (Integrated approach to cyber resilience)*, 2021.
147 https://www.scmagazine.com/home/solarwinds-hack/solarwinds-lawsuit-claims-private-equity-owners-sacrificed-cybersecurity-to-boost-short-term-profits/

Tracing and recall in the food sector[148]

In the food sector, food companies are required to be able to trace to whom they have supplied their food products. This obligation applies throughout the food chain, from primary production (such as agriculture, livestock production and fishery) through to the consumer who eventually eats the food. In every link of the chain, a food company must be able to trace where the raw materials came from, and to whom they have supplied their products. This obligation is known as traceability. If a food company discovers that it has placed unsafe food on the market, within four hours it must be able to compile a distribution list with all buyers[149] and purchased products, which on request is submitted to the authorities.

Food companies are also required to recall the unsafe foods on their own initiative, or if so instructed by the authorities. In practice, it is sufficient for the authorities if a food company restricts itself to a publication in a daily newspaper and/or on its own website, but an 'absolute recall' means that the food company must warn its customers as directly as possible, and call for them to return the products, possibly even collecting the products itself, from the end user. This latter action is for example carried out for recalls of passenger cars if the safety problem is so serious that the car may no longer be used on public roads.

Regulation and liability also play a role in the occurrence of vulnerabilities. At present, governments and other organizations have few possibilities for obliging manufacturers to safeguard cybersecurity in their products. Users do not always know how to impose requirements, and force manufacturers to show accountability. This makes vulnerability a problem for the user and not the manufacturer.

There are practically no rules for placing software on the market. The current free market for software products imposes almost no requirements on the sound management of security risks. Identifying vulnerabilities is a time-consuming task, that demands much manpower and as a consequence is costly. In certain cases it can be necessary to completely rebuild a product in order to tackle the underlying (safety) problem. The absence of economic incentives explains why manufacturers at present do not consider this option.

148 Based on the idea that there is a chain from producer to consumer via a number of intermediate steps, the compulsory traceability for every company in the food sector applies one step back and one step forward in the chain (excluding the step to the end user or consumer). Source: Article 18(1) of Regulation (EC) no. 178/2002 in: Guidelines for the enforcement of Articles 11, 12, 14, 17, 18, 19 and 20 of (EC) Regulation no. 178/2002 laying down the general principles and requirements of food law (26 January 2010).

149 For the last link (the end user or consumer), the tracing obligation does not apply, but certain retailers do record (some) deliveries to consumers (online orders, customer loyalty cards, etc.).

4.2 The purchase and use of software by organizations

Growing numbers of processes in our society and within organizations are being undertaken by digital means. As a consequence, dependency on digital systems and the software that these systems contain is growing both for organizations and for society as a whole. Because software will always contain vulnerabilities, it is essential for organizations to take the inherent risks into account when purchasing and using software. The questions discussed here are: how do organizations that purchase and use software, such as municipalities, hospitals and companies, deal with the risks involved in the purchase and use of software? Which dilemmas and obstacles play a role?

4.2.1 Relationships on the software market

The extent to which risks are managed when purchasing software with vulnerabilities is limited by a number of factors. This became clear from interviews with various organizations. One of these factors is the relationship between manufacturers and end users on the software market. The software market is characterized by information asymmetry.[150] Software manufacturers have more information about the composition of the products than customers. It is often not possible for them to identify the composition and quality of software. This is because manufacturers generally demonstrate little transparency as regards the structure of their products. Moreover, many organizations do not have the necessary knowledge or capacity to be able to evaluate the information, even if a manufacturer does offer the necessary insight.

This information asymmetry makes it difficult for customers to assess the quality and safety of software. As a result, they mainly assess products according to the elements they are able to check, such as price, functionality and ease of use. As a consequence, manufacturers compete with one another on these elements as there is no point for them to invest in the safety of the products. There are no legal provisions to compensate this information asymmetry by transferring liability from customer to manufacturer.

The software market is controlled by a small group of large manufacturers. The market power of a number of manufacturers means that for certain functionalities, there are only a few products available from a select group of suppliers, for example for operating systems such as Windows and macOS or office software packages such as Microsoft Office. In many cases, manufacturers offer standard packages and customers have few possibilities for matching these to their own wishes or requirements. This is because the software market is a global market which can hardly be influenced by users in the Netherlands alone. Influencing such a global market requires a larger power block, for example at EU or UN level, or based on joint actions by end users.

When vulnerabilities are discovered in software products, the manufacturer sets to work to develop a patch for those vulnerabilities. Developing this solution requires the manufacturer to spend resources. Many of the costs and risks in the event of vulnerabilities are borne by the user of the software. The user incurs costs in mitigating and patching systems. In addition, the user incurs costs if its operations are shut down, for example following an attack. If the user is insured against cyber incidents, in certain cases, the

150 Anderson, R. and Moore, T., *The Economics of Information Security*, Science 314, October 2006.

insurer will reimburse part of the costs incurred by the organization. Generally speaking, the risks of damage as a result of vulnerabilities in software are mainly borne by the user of the software. These factors together mean that the software market is described by experts as a failing market because of the asymmetric relationship between manufacturer and customer.[151]

4.2.2 The purchase of software

The customer purchases software based on a functional need to manage tasks or processes by digital means. After identifying this functional need, the user looks at the possibilities available on the market to meet its need. When selecting a product, a range of wishes and requirements play a role, such as the functionalities offered by the software, ease of use, price and security.

Formulating safety and security requirements and checking products according to those requirements

As discussed in section 4.1, at present there are limited possibilities to obligate manufacturers to safeguard cybersecurity in their products. This places an additional burden on the customers to test the products for safety and security, when purchasing software. Because of the information asymmetry on the software market (see subsection 4.2.1), customers often purchase software on the basis of a functional need, while safety and security aspects play a more minor role.

To be able to formulate the correct safety and security requirements, the organization that uses the software needs knowledge of the relevant requirements, for its situation. The user also needs information about the product to be able to assess the extent to which the product satisfies those requirements, and how this should be interpreted for its situation. If an organization is able to specify the correct requirements but is unable to check them, it is not possible for the organization to assess whether software actually satisfies the safety and security requirements.

There are broad differences in the extent to which organizations impose safety and security requirements on the software products they purchase. Some, mainly larger organizations do have the appropriate knowledge available to them, to impose requirements and to check them. One commonly imposed security requirement is the authority to carry out penetration tests.[152] Other, generally smaller organizations are unable to impose the correct safety and security requirements because they do not have access to the necessary knowledge and resources, or do not recognize the importance of doing so. In addition, manufacturers do not always allow penetration tests to be carried out on their products, because the process involves certain risks. For example, if penetration tests are carried out in a cloud environment, there is a risk that the test will cause damage or threaten the availability of the environment. In addition, when carrying out penetration tests or reverse engineering[153], it is possible to work out how a software product is built, and for example to ascertain details about a specific algorithm.

151 Anderson R., *Security Engineering*, 2020.
152 A pentest is a security check whereby an external test for vulnerabilities is carried out, followed by an attempt to hack the system via these vulnerabilities. See chapter 2.
153 Reverse engineering is investigating a product to determine its functioning and structure.

Because of the competition on the market, manufacturers are not keen to release this information. As a result, manufacturers often impose conditions and restrictions on penetration testing. It is therefore not common practice that customers be permitted to carry out penetration tests on the software they use. One way in which customers are able to ensure that they are permitted to carry out penetration tests is by including this as an explicit requirement in their contract with the supplier. In interviews, a number of organizations indicated that although they include penetration tests as a standard requirement in contracts, it sometimes takes considerable persuasion to allow this requirement to be included in the negotiations with product suppliers. Larger organizations with greater cyber maturity generally do have penetration tests carried out on their systems. There are also organizations that, if they do discover a vulnerability in software widely used in their sector, pass on this vulnerability to the sector organization. Subsequently the sector organization can raise the question of the vulnerability on behalf of all affiliated organizations, with the product manufacturer.

Although imposing safety and security requirements and checking those requirements is not carried out as standard, there are examples of specific sectors in which organizations impose compulsory safety and security requirements on software products and suppliers. The Dutch Ministry of Defence, for example, imposes strict safety and security requirements on suppliers that carry out work on its behalf. These requirements are laid down in the General Security Requirements for Defence Contracts (ABDO) scheme. The Military intelligence service MIVD also checks whether suppliers comply with this scheme. Financial institutions also impose strict safety and security requirements on the products they commission. By means of its procurement policy, the national government also aims to improve the cybersecurity of software. To assist government organizations in formulating safety and security requirements, the Government Cybersecurity Procurement Requirements wizard (ICO wizard) was developed. The ICO wizard is a tool for government organizations, but its use is not compulsory, and it offers no indicators as to how end users can check the requirements imposed. Moreover, the ICO wizard provides nothing more than a list of requirements, from which organizations can make their own selection. It is up to the organization itself to make the correct selection, and that is something that requires expertise that not every organization can call upon. In addition, the organization itself is required to assess the product, something that also requires knowledge and cooperation from the manufacturer.[154]

154 Ministry of Defence, *General Security Requirements for Defence Contracts 2019*, February 2020; Ministry of Economic Affairs and Climate Policy and ministry of Justice and Security, *Roadmap for Digital Hard- and Software Security*. April 2018;
The ICO wizard is a tool developed for government organizations based on the Government Information Security Baseline (BIO), to encourage demand for digitally safe software, and to create an incentive for manufacturers to place digitally safe products on the market. Within the ICO wizard, organizations can select the requirements they consider applicable to the procurement of software, see: https://www.bio-overheid.nl/ico-producten

Procurement requirements by governments abroad: US Executive Order
In May 2021, an Executive Order[155] was issued in the United States in which a series of measures are specified aimed at improving national cybersecurity.[156] As well as a number of measures relating to information sharing, the reinforcement of capacity in the event of incident management and learning from incidents, the Executive Order also aims to improve the safety of software.

One of the measures taken in the Executive Order is to impose standards on software used by federal governments. Within the Executive Order, federal governments are required to impose safety and security requirements on software suppliers. If the parties fail to satisfy these requirements, they will no longer be able to supply software to American federal government organizations.

As a rule, the imposing and monitoring of safety and security requirements on manufacturers by organizations is non-binding. There are no appropriate regulations. The extent to which it does take place therefore depends on the organizations themselves. Not every organization has the expertise available to impose the appropriate requirements on software, and to subsequently check whether the products satisfy those requirements. There are no safeguards in the system to ensure that products satisfy particular requirements.

4.2.3 Use and maintenance phase of software within organizations

As discussed in chapter 2, organizations are able to take a number of measures to secure their systems and to prepare for incidents. The NCSC recommends several basic measures that organizations can take to counter cyberattacks. Examples include patch management, firewalls, network segmentation and detection capabilities. In the Cyber Security Assessment Netherlands 2021, the NCTV concludes that although the resilience of organizations is improving, it is not yet at a sufficiently high level. Not all organizations have taken the basic measures.[157] How can we better understand the reason why organizations do not always take these basic measures? This is partly due to the ability to take measures, and partly due to biases in the way people in organizations view the risks of cyberattacks.[158] Below we discuss the dilemmas relating to these measures.

Dealing with the dependency on software

Using software and being dependent on that software always entails risks. It is impossible for end users to fully mitigate these risks, but it is essential that they first have a clear picture of the risks in order to make any assessment. One way of reducing the dependency on a product is to implement a redundant system by using software products from different manufacturers. However, it is not realistic for every organization to implement all systems redundantly, because it demands extra resources. If an organization operates

155 An Executive Order is a decree issued by the president, with the same powers as a law
156 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, accessed on 14 July 2021.
157 National Coordinator for Security and Counterterrorism, *Cyber Security Assessment Netherlands 2021*, June 2021. https://www.security.nl/posting/710981/Cybersecuritybeeld+Nederland%3A+al+tien+jaar+lang+de+basis+niet+op+orde
158 Meyer, R. en H. Kunreuther, *The Ostrich Paradox*: *Why we underprepare for disasters*, 2017.

different systems from different suppliers, it is also possible that those systems are unable to work together effectively (compatibility issues). In certain cases, end users deliberately do decide to implement their systems redundantly, for example for vital systems that facilitate crucial processes, or if the consequences of system unavailability are considerable.[159] As regards system dependency on a specific product within a network, there are many differences in how organizations have structured their networks. In an interview, one organization explained that it had structured its systems in such way that there is no single point of failure; as a result, if a system fails, other systems and processes are able to continue. Another organization told us that its network consists of a number of products on which many of its processes depend. In that situation, if a system fails, many of the processes within the organization cannot continue.

In dealing with the dependency on software, it is essential to gain an insight into the risks involved in using a particular product, and the related system dependencies. When an organization is aware of its critical systems, and has a clear understanding of its dependencies, it is in a better position to assess the risks of the measures that need to be taken in an incident, and in preparation for an incident. Generally speaking, there is a big difference between organizations in the extent to which they have an overview of their systems. Above all larger organizations tend to have a (reasonably) clear picture of the systems they operate, and the current versions. They record this information, for example in a Configuration Management Database (CMDB). Whenever a vulnerability is published, they can check the database to see whether the vulnerability applies to their organization and whether they need to implement a patch. Because they understand their systems and dependencies, they are also more easily able to prepare a more precise risk analysis of what would happen if the system were to be shut down. At other (often smaller) organizations, it is clear that they do not always have a complete overview of the systems they use. The risk of this situation is that if a major vulnerability is discovered, these organizations are unable to take the necessary action (in time) and run the risk of becoming compromised. In addition, these organizations are unable to make a complete risk analysis of the impact of a system shutdown.

Mapping out and maintaining a clear picture of the systems and system dependencies requires capacity, and the entire organization must recognize the importance of keeping this overview up to date. For organizations with limited capacity, obtaining a complete picture of all systems and the intersystem dependency can be a challenge. The organization structure can also make it more difficult to obtain a complete picture of all systems in use. The Inspectorate of Education identified this as one of the relevant factors following the ransomware attack at Maastricht University.[160] Universities are characterized by a multi-layered administrative structure with different administrative bodies, each responsible for their own information security. This makes it a challenge to obtain a clear overview of the complete network of IT systems. In addition, chain dependencies can make it difficult to generate a picture of the complete system and the dependencies. Many organizations work together with external suppliers or supply chain partners. As a

159 Jacobs, D., *'7 factors to consider in network redundancy design'*, https://searchnetworking.techtarget.com/tip/7-factors-to-consider-in-network-redundancy-design, accessed on 16 July 2021.
160 Inspectorate of Education, *Cyberattack Maastricht University*, May 2020.

result, processes within an organization can be (partly) dependent on the systems used by external parties, as for example was the case in the Kaseya occurrence (see 3.3.5).

Patching

As a rule, software is not a static product but continues to develop following the purchase moment. In addition, the cyber risk and threat landscape is not static either, and equally continues to develop. When vulnerabilities are discovered in software, manufacturers develop patches to correct them (see section 4.1). At present, it is primarily the responsibility of the organizations that use the software to implement these patches to repair the vulnerabilities on its systems.

However, patching also engenders risks and requires consideration. Because of the large number of patches published each year (some organizations are required to implement up to a 100,000 patches a year), it is not always possible for an organization to install the patches in time. Because of the large number of patches per year, organizations have difficulties to have a complete and up-to-date overview of vulnerabilities in their systems. To simplify this, organizations can purchase scanning services. These scanning services scan for known vulnerabilities. But not all vulnerabilities are able to be scanned, and the list of vulnerabilities that is scanned is often incomplete. In addition, smaller organizations usually do not have the resources to purchase such scanning services. They often rely solely on the NCSC advices. In these circumstances, organizations cannot patch everything in time. It is therefore inevitable that known vulnerabilities, including critical ones, are not patched.

The large amount of vulnerabilities also apply considerable pressure on organizations to implement the patch process in the required manner, and to consider which vulnerabilities require immediate action. The incapacity of organizations to patch vulnerabilities in time, according to penetration testers at Positive Technologies, makes it easier for attackers to hack company networks. Patching requires knowledge of systems and staff capacity within organizations. As well as patching systems, IT staff have numerous other tasks that also have to be carried out. At every organization, it is a question of deciding whether to continue day-to-day operations, or to immediately switch to patching systems. End users are sometimes reticent in immediately implementing patches, because there is a risk that following the patch, systems will no longer function correctly or may even fail, which will have consequences for the organization's normal operations. In addition, it is possible that the patch will not or will only partially repair the vulnerability.[161] Interviews revealed that this consideration is particularly difficult for smaller organizations because they have limited resources to deploy additional capacity for system patching.

As described above, because it can be a challenge for organizations to obtain a complete picture of all the systems in use, it is possible that organizations fail to patch a vulnerability because they lack an up-to-date overview of which software is operated where, which version is affected and whether or not a patch is necessary to be able to guarantee the

161 Nichols, S., *You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that,* The Register, August 2020.
'The Nightmares of Patch Management: the Status Quo and Beyond', Trend Micro, https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond, consulted on 14 July 2021.

security of the systems. Moreover, it is not always clear to organizations precisely which components make up the software they are using, because software is closed source in many cases. In other words, the source code is not accessible to the customer, and the manufacturer is reticent about revealing the software architecture. In addition, much software is based on open source components that contain critical vulnerabilities, without organizations being aware of this situation.[162] As a result, organizations can be vulnerable, without being aware of it themselves.

It is also important for the entire organization to recognize the importance and urgency of patching. It is not always clear to organizations that they can be attacked without an attacker specifically targeting their organization. A vulnerability in software on a server that is connected to the Internet is like honey to a bee, for attackers. These attackers automatically scan all servers containing vulnerable software, in the hope of identifying servers that will enable them to hack into systems of organizations. Research shows that organizations often base their actions on past experiences with updates.[163] Many published vulnerabilities are not actively exploited by attackers. Whenever organizations wait before patching vulnerabilities not used for attacks, it will have no consequences for the organization. As a consequence, organizations may tend to underestimate the importance of a rapid response to future vulnerabilities.

According to manufacturers and experts, transferring software to the cloud can be a solution for ensuring that systems can be patched in time. This is known as a Software as a Service (SaaS) solution.[164] Because the software is then managed by a manufacturer, the advantage of SaaS is that patches can be tested and applied more quickly. This eradicates the time between the release of a patch and its application, so that customers always have the latest patches, quickly. In the case of SaaS, the application of patches becomes the responsibility of the manufacturer rather than the customer.

Transferring software to the cloud, however, also brings with it risks and considerations for an organization. The disadvantage of SaaS solutions is that in the event of a vulnerability all servers will become vulnerable, since they all operate on the same version. Furthermore, the manufacturer is the only party able to do anything about the situation; the organization has no role to play. If organizations manage their own systems, they are in control of patching, mitigation and shutting down systems. In addition, when taking up a cloud service, the organizations have no understanding of the nature of the product. Moreover, an organization becomes less flexible, and the possibilities for software adaptation are restricted. Automatic updates to SaaS solutions can also threaten the continuity of systems, or even introduce new vulnerabilities. Organizations then have no control whatsoever over these risks. Another consideration for an organization is that in the event of an incident, the systems are held by the manufacturer. The manufacturer has the most in-depth knowledge of the product, and is therefore the ideal party to be

162 *'Veel kritieke lekken door open source in standaard apps'* (Numerous critical leaks due to open source in standard apps), AG Connect, https://www.agconnect.nl/artikel/veel-kritieke-lekken-door-open-source-standaard-apps, 5 August 2021.

163 Rajivan et al., *Update now or later? Effects of experience, cost, and risk preference on update decisions, Journal of Cybersecurity,* 2020.

164 In SaaS, software is offered as an online service. Via the Internet or via VPN, the end user is granted access to the software managed by the provider.

able to analyse its software, in the event of an incident. The manufacturer can then assist the organization in investigating whether it has been affected, and solving the problem.

On the other hand, organizations sometimes do not want to share information with external parties, for example because it is not permitted, or because they do not want to risk their information ending up outside the organization. It is also possible that the organization does not want to link a system to the Internet because of the nature of that system. In that case, SaaS is not a solution, and it is up to the organization to physically manage (part of) its own systems.

The regular patching of software introduces new problems. If an organization fails to patch, it may be opening itself up to the risk of a security breach that can be automatically traced by external parties. Due to the large and ever growing number of patches, patching all vulnerabilities is not manageable for all organizations. Moreover, for organizations, the necessity of (rapid) patching is not always clear. Offering software from the cloud shifts the responsibility for patching to the manufacturer, but also entails risks for organizations that use the software.

Prevention and detection

In addition to patching, an organization can also take a series of other prevention and detection measures, to protect its network, for example installing a firewall, introducing network segmentation and monitoring systems. Each of these measures does engender risks and considerations for an organization.

One measure for restricting external access to the systems of an organization is to install a firewall.[165] The challenge with firewalls is that they must be installed in such a way that they prevent undesirable activity but do not inadvertently also prevent desired activity. In addition, the correct rules and policies must be implemented, and it is important that these aspects be checked and updated periodically. This too demands knowledge and capacity from an organization. A firewall can also introduce risks, if an organization does not have the appropriate knowledge about exactly what the firewall does. As a result, the organization may have no understanding of whether its systems are unnecessarily open to traffic.[166]

To limit the impact of a potential incident, organizations can segment their network. The risk of segmentation is that if a network consists of too many segments, it can take a great deal of time and money to manage the network.[167] Implementing segmentation in a network is a process that requires numerous adjustments, that is costly and that can

165 A firewall is a machine located between the network and the Internet, that monitors traffic and filters out possible harmful traffic.

166 https://www.insightsforprofessionals.com/it/security/firewall-management-challenges-how-solve-them, accessed on 22 July 2021; AlgoSec, *Firewall Management: 5 challenges every company must address – an AlgoSec Whitepaper,* 2015.

167 *'Hazardous Network Segmentation: when more isn't better',* AlgoSec, https://www.algosec.com/blog/hazardous-network-segmentation-when-more-isnt-better, accessed on 22 July 2021.

disrupt the primary processes of an organization. It is also difficult for organizations to find staff with the necessary skills and expertise.[168]

As well as more preventive measures like firewalls and segmentation, many organizations also invest in detection capacity and system monitoring. On this basis, organizations are able to detect suspicious activity when it takes place. The challenge for organizations is correctly setting the level of detection. If this is not the case, suspicious activity may go unnoticed, or an activity can be incorrectly detected as suspicious (false positives). In other words, the fact that detection systems are in place does not guarantee that all suspicious activity will be observed. In addition, organizations must have the knowledge to be able to interpret the activity, and to know how to respond when they do detect activity by an attacker. This demands capacity and expertise from the organization. For vital operators and national government organizations, it is possible to sign up to the National Detection Network (NDN). The NCSC passes on indicators to the participants in the NDN, to enable them to recognize a potential attack. To be able to be part of the NDN, organizations must have already implemented their own monitoring process. Direct participation in the NDN is only open to national government and vital operators.[169]

One trend that is emerging in the world of cybersecurity is the growth in investment in detection capabilities, as compared with prevention.[170] It is often emphasized in the security world that it is not possible to prevent all attacks, so it is worthwhile above all to invest in detection and response. This attitude was also clear in a number of the organizations we spoke to, that had invested primarily in detection and response. However, investing in detection does not always offer guarantees, as discussed above. The systems at one of the organizations interviewed, for example, failed to detect the attack via the software vulnerability, as a consequence of which the organization was compromised. To ensure the most secure system possible, multiple layers of security and protection are needed, in terms of both prevention and detection and response.

4.2.4 Managing cybersecurity in organizations

Capacity and expertise

All the measures referred to above require capacity and knowledge from organizations. The extent to which an organization has access to this capacity and knowledge depends on the size of the organization and its cybersecurity maturity level. Smaller organizations have limited capacity and knowledge in the field of information security. Generally speaking, in the course of this investigation, we saw major differences in the extent to which organizations take measures to prevent incidents, and the extent to which they are prepared for incidents. A municipality with a limited budget, for example, has little capacity for information security and IT, in general. Within such organizations, the CISO

168 Holt, M., *Security Think Tank: Benefits and challenges of security segmentation,* Computer Weekly, https://www.computerweekly.com/opinion/Security-Think-Tank-Security-segmentation-benefits-and-challenges, accessed on 15 July 2021.

169 Ministry of the Interior and Kingdom Relations and ministry of Security and Justice, *Handreiking voor implementatie van detectie-oplossingen (Guide for the implementation of detection solutions),* October 2015.
Certain organizations such as healthcare institutions, municipalities, educational institutions and water authorities can sign up to the NDN, indirectly, via the sectoral CERTs. See: https://www.ncsc.nl/actueel/weblog/weblog/2020/het-nationaal-detectie-netwerk-voor-een-private-organisatie.

170 https://www.youtube.com/watch?v=3IDiqYil2lQ, accessed on 16 July 2021.

is the only member of staff actively involved in information security. Due to these capacity limitations, the IT department often finds it difficult, for example, to bring the organization's CMDB up-to-date, and to implement all the necessary patches in time. At the other end of the spectrum, financial institutions have hundreds of cybersecurity professionals on their books. They have the capacity and expertise to thoroughly take the basic measures, and to anticipate and respond to incidents.

We also observed major differences between organizations in terms of the extent to which they implement IT activities themselves, or opt for outsourcing. Organizations outsource tasks because they do not have sufficient expertise and capacity within the organization to carry out those tasks themselves. Due to this lack of expertise and capacity, however, they also do not always have the necessary knowledge to determine whether the party to which they have outsourced the tasks in question in fact delivers good service.

In general, there is a shortage of expertise in the cybersecurity market. This has been a problem for years, and no end is in sight. The entire IT sector is experiencing a tight labour market, for example, in July 2021, thirty percent of the vacancies for IT programmers and IT developers were not able to be filled. One of the causes of this shortage of expertise is that professionals feel undervalued, and that starting a career in the cybersecurity domain is difficult. The growing number and complexity of attacks also means that many professionals suffer stress and burnout problems.[171] The risk of this situation is that the capacity shortfall is only set to grow. During the Citrix incident, it was also apparent that the demand for cybersecurity professionals outgrew the supply, resulting in security companies not being able to help every organization in need of expertise. Incident response capacity is fragmented through sectoral CERTs and each organization needs its own capacity and expertise regarding preventive measures. Expertise is not or rarely bundled and is therefore fragmented.

Urgency

The extent to which an organization recognizes the importance and urgency of taking measures and is able and willing to deploy the necessary resources also plays a role in the resilience of an organization. In government organizations like municipalities, unlike in private organizations, the administrators themselves are unable to determine how resources are spent. Instead, they are accountable to the municipal council, which in addition to cybersecurity, must also take account of any number of interests, as well as having been made responsible for many municipal tasks, that also take up resources. To make matters worse, IT is often taken for granted by public administrators and parliamentarians, despite the fact that they do not understand everything the processes involve. It is often more attractive to spend money on things that deliver a tangible result, than on preventing problems. After all, if a problem is prevented, the result remains out of sight.

It also became clear from interviews that in certain organizations, the position of the CISO in the organization when the Citrix occurrence took place was weak, so that it was

171 ESG & ISSA, *The Life and Times of Cybersecurity Professionals 2021 – Volume V*, July 2021; ABN Amro, Stand van TMT, September 2021; *VMware, Global Incident Response Threat Report*, 2021.

not possible to make a meaningful contribution to the successful management of the incident. At one of the organizations we spoke to, the CISO was not able to convince the IT department to decide to implement mitigation measures, at the time of the occurrence. As a consequence, the organization was compromised. In response to this incident, the position of the CISO within the organization was reviewed and reinforced, so that in the future, it will be easier to notify the management of incidents. At many of the organizations we spoke to, it is clear that the sense of urgency to invest in cybersecurity grows following an incident of this kind.

Individual risk

The risks that emerge in the event of software vulnerabilities are at present mainly seen as individual risks that have to be managed by each organization, operating individually. The operating principle in the Dutch system is that every public and private organization is responsible for its own digital resilience. Most organizations do not have to account for this. Medium-sized and large companies and organizations must have an annual audit of the annual accounts, in order to demonstrate their accuracy. An IT statement is currently not part of this audit report, even though having IT security sorted out is important for the continuity of an organization. The professional association of IT auditors has recently proposed to include an IT statement as a permanent part of the auditor's report.[172]

If incidents occur as a result of vulnerabilities in software, they tend to impact many organizations and individual citizens. As a result, vulnerabilities represent a collective risk to society as a whole. Individual organizations have only limited options to manage these risks, themselves, depending on the capacity and expertise available to them. Every year, the costs of cyberattacks are rising. More and more organizations are taking out cyber insurance to insure themselves against the damage and losses caused by incidents. Nonetheless, only a small portion of SME enterprises are insured against cyber incidents.[173] Because the costs of cyber incidents are continuing to rise, the premiums for cyber insurance are rising, too. Whenever an incident takes place involving a vulnerability in software used by many organizations however, the collective costs for the incident will be so high that they can never be borne by the insurers.

Insurers are expected to play a positive role in promoting cyber hygiene by setting requirements for the measures organizations must have in place to be covered for cyber incidents. At the same time, the role of insurers has also been criticized, and it is questioned whether they promote good cyber hygiene, because insurers cover ransomware payments and because security measures taken by organizations are not checked. Recently, this has changed, ransomware payments are no longer always covered by insurers.[174]

172 NCTV, *National Cybersecurity Agenda*, April 2018; Van Gils en Van Wijnen, 'Nieuwe IT-check kan voorwaarde worden voor krediet', FD, 11 August 2021.

173 Hiscox, *Hiscox Cyber Readiness Report 2020*, 2020; https://www.trouw.nl/economie/het-aantal-cyberaanvallen-groeit-explosief-maar-echt-ongerust-zijn-bedrijven-niet~b332e73e, consulted on 29 July 2021.
https://www.rtlnieuws.nl/tech/artikel/5000096/cyberverzekering-hacken-ransomware-gijzelsoftware-ddos-citrix, consulted on 29 July 2021.
Modderkolk, 'Vooraanstaande ict-beveiligers: 'Ransomware gaat richting nationale crisis, overheid moet meer doen' ('Leading IT security advisors: Ransomware is becoming a national crisis; government needs to do more'), *De Volkskrant*, August 2021.

174 Verzekeraars deinzen terug voor ransomware', *AG Connect*, *https://www.agconnect.nl/artikel/verzekeraars-deinzen-terug-voor-ransomware*, 25 May 2021.

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).

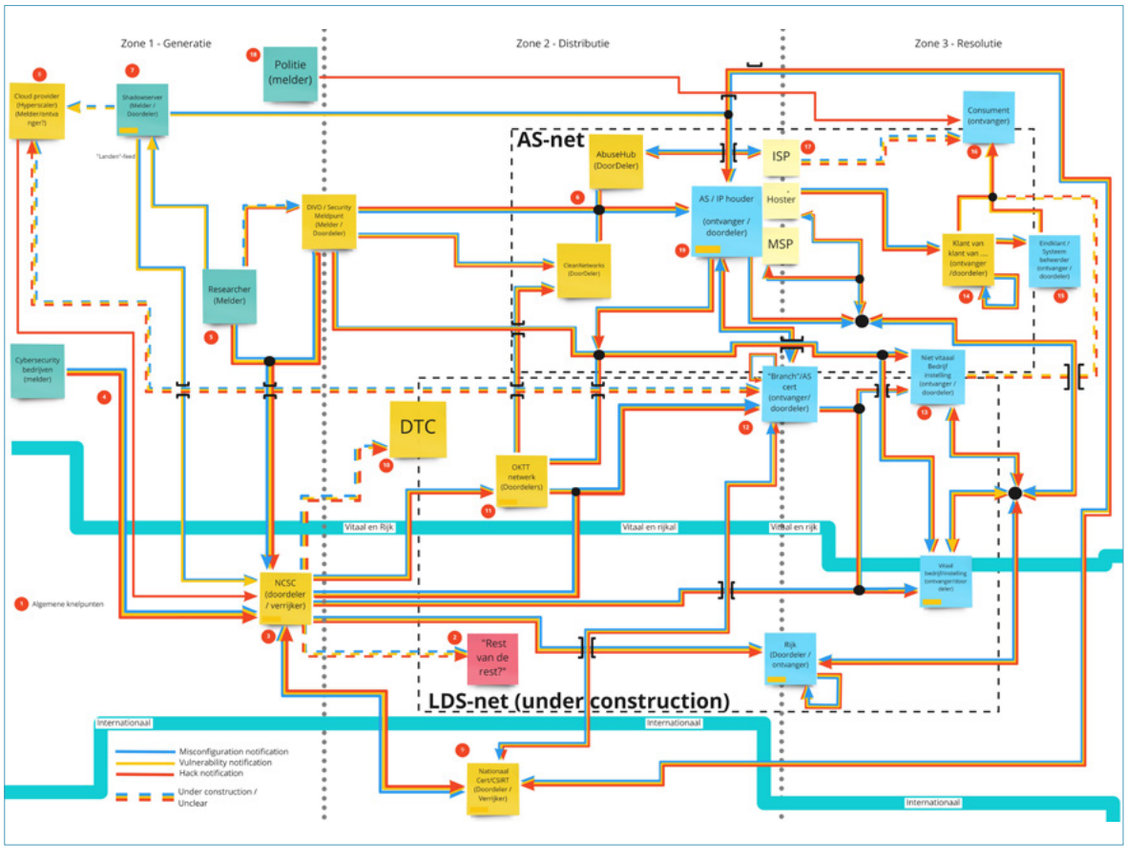


Figure 18: Subway map of the exchange of threat information on organizations. (Source: AAN)[184]

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.

Reporting and investigation on the basis of statutory obligations

Incidents at vital providers

The European Network and Information Security (NIS) Directive[196] contains obligations for providers of essential services in vital sectors and digital service providers.. The Netherlands has implemented the NIS Directive in the Security of Network and Information Systems Act (Wbni). Pursuant to the Wbni, providers of essential services are required to report serious incidents to the NCSC/sectoral CSIRT and their sectoral regulator. For energy and digital infrastructure occurrences, this is the Telecom Agency; for banks and the payment infrastructure the DNB, for transport and drinking water the ILT and for healthcare the IGJ.[197] For the telecom sector there has been a duty of care and notification including supervision by AT since 2012 based on the Telecommunications Act, regardless of whether a party has been designated as vital by the Ministry of Economic Affairs. In addition to this sectoral legislation and regulation, the Wbni includes a duty to report to the NCSC only for the vitally designated telecom parties.

The appropriate specialist department in consultation[198] with JenV then imposes threshold values, above which the incident must be reported. The Wbni specifies that in preventing or managing an incident requiring public awareness, the authority in question is permitted to inform the public about the reported incident. The authority can also call upon the vital provider to inform the public itself.[199]

It is also important for learning that other organizations can easily absorb the lessons from the studies that are relevant to them, and in that way learn from what other organizations have suffered. Occasionally investigations in response to reports are published on the website of the relevant authority or regulator. Examples are the investigations by the Radiocommunications Agency Netherlands (AT), the Inspectorate of Justice and Security (IJenV) and the Health and Youth Care Inspectorate (IGJ) into the failure of the 112 alarm number[200] and the investigation by ILT into cybersecurity at Waternet, in response to signals in the media that there were cybersecurity problems.[201] We were unable to find an overview on the websites of the NCSC, AT or other sectoral regulators of which incidents have been investigated, nor were we able to find an aggregated overview of the number of incidents, the factors that led to those incidents and the various lessons learned from them. On the other hand, it is possible that the lessons from these incidents were implicitly integrated in the recommendations and information provided by these organizations to their target organizations.

196 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32016L1148&from=EN. Under the Wbni, the following are designated as providers of essential services: entities designated as vital providers that operate in sectors listed in the appendix to the NIS Directive (see Article 2 Bbni). For some categories of other vital providers, separately from this, there is also an obligation to report serious incidents to the NCSC (see Article 3 Bbni), but they are not subject to the other obligations arising from the NIS Directive. In addition: providers of essential services are required under Article 10 Wbni to report serious incidents to the NCSC and the sectoral regulator, but not also (or instead) to a "sectoral CSIRT". Incidentally: the regulator for entities within the health care sector has already been determined (in Article 4 of the Wbni), but within that sector no providers of essential services have yet been designated (to whom the obligations from the NIS Directive would apply).

197 https://zoek.officielebekendmakingen.nl/stb-2018-387.html

198 Because of the often dual reporting requirements to both the subject department and JenV (NCSC).

199 Article 20(4)(b) Wbni https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/publicaties/2020/januari/20/brochure-meldplicht-voor-aanbieders-van-essentiele-diensten/Brochure+Meldplicht+voor+aanbieders+van+essentiële+diensten.pdf

200 https://www.agentschaptelecom.nl/actueel/nieuws/2019/06/26/onderzoek-naar-storing-112

201 https://www.ilent.nl/documenten/rapporten/2021/4/2/onderzoeksrapport-stichting-waternet

In practice, inspectorates are currently still working internally on the question of how they can and should interpret their own responsibility. For example, inspectorates write in their first joint inspection report that supervision is still in a constructive phase and that they cannot yet make coherent statements (draw common threads) about how things are going at the moment with regard to cyber security in vital sectors and processes.[202]

Investigation into data leaks

Organizations that have suffered breaches of personal data are legally required to immediately report the occurrence to the Dutch Data Protection Authority (DPA (AP in Dutch)). The term data leaks refers to 'access to or the destruction, rectification or release of personal data from an organization, contrary to the intentions of that organization'.[203] The legal obligation to report data leaks is based on the European General Data Protection Regulation (GDPR) in the EU. Because the GDPR is a Regulation, this European rule of law applies directly across the entire European Union.

The Dutch DPA publishes investigation reports and reports on the imposition of fines in response to reports of data leaks and other signals.[204] The investigations by the Dutch DPA focus on the extent to which organizations have complied with their legal obligations, such as the taking of technical and organizational measures to prevent data leaks and the evaluation of data leaks. If an organization has failed to comply with the statutory measures, the DPA can impose a fine. For this reason, organizations are reluctant to report potential data breaches. However, non-compliance with the legal obligation to report can also lead to additional fines, regardless of the extent of the original data breach. Another limitation is that the reports must involve the leaking of personal data, and that is only the case in some of the incidents. Furthermore, the AP's investigations focus mainly on compliance with legislation and regulations. In order to learn, the underlying question of non-compliance is particularly relevant: what factors may have led to organizations not complying with the obligations and what can be learned from this?

Each year the DPA publishes an annual report. The annual report for 2020 states that the majority of data leaks reported in 2020 were the consequence of the wrong sending or issuing of personal data (66%). The DPA reports that in 5% of the data leaks reported in 2020, a digital incident (hacking, malware, phishing) was the cause of the breach and the proportion is rising. In its report, the DPA discusses in depth the contribution that multi factor authentication (MFA) could have had on preventing and mitigating 249 data leaks, whereby according to estimates, at least 607,846 and at most 2,092,946 people were involved.[205]

At present, the Dutch DPA offers no further insights for organizations that use software. To be able to gain more insights from the reports of data leaks, and in that way to identify potential further lessons for other organizations, in 2020, the Cyber Security Council (CSR) submitted a study proposal to the Minister of Justice and Security. The aim of this study is to show the extent to which the scientific and/or statistic study of data leaks can

202 ANVS, DNB, IGJ, IJenV, ILT, *Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021*, June 2021.
203 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
204 https://autoriteitpersoonsgegevens.nl/nl/onderzoeken
205 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf

increase the understanding of the effectiveness of safety measures (or the absence of such measures).[206]

Forensic investigations

There are a number of organizations that carry out subsequent investigations into incidents. Some of these organizations are recognized as forensic cyber investigation offices. This recognition means that their reports can be accepted as forensic evidence in a court case. Forensic substantiation is primarily focused on substantiating legal liability, not on learning from the incident to prevent future recurrence. In most cases, these digital forensic investigation firms work on behalf of the affected organization and/or their insurer. The investigations generally remain confidential to the commissioning organizations (unless the organization publishes on its own initiative, see the section below). Other organizations gain no insight into the lessons learned and they make no contribution to an overall picture of factors and the effectiveness of measures. At most, they are shared within the offices of the affected insurer (silos between insurers).

The police (HighTech Crime Team and regional cybercrime teams) and the NFI also carry out forensic investigations. For these organizations, the same applies broadly as for investigative agencies in terms of the ability to learn from their investigations. In the event of a court case, some of this information may be made public via the media and by the court judgement. However, the information cannot be examined by other organizations, as for example is the case in the event of road traffic accidents that are registered in a road traffic accident register, that among others can be used for scientific research (for example by the Institute for Road Safety Research, SWOV) and in support of future policy.

Investigations and publication on individual initiative

A number of organizations have decided to publish the results of forensic or other investigations, in the public interest and as a way of accounting for their activities to their grassroots (individual citizens and students).

206 https://www.cybersecurityraad.nl/documenten/adviezen/2020/02/11/csr-advies-beschikbaar-stellen-datalekmeldingen-voor-onderzoeksdoeleinden---csr-advies-2020-nr.-1

Investigation into cyber attacks in public

In June 2019, the police informed the municipality of Lochem that the municipality's digital system had been compromised. Since that time, the Mayor of Lochem has seen it as his personal mission to inform municipalities and other government organizations about this risk and to underline the importance of cyber resilience.[207]

On 23 December 2019, Maastricht University became the victim of a cyberattack. The university commissioned an investigation into the occurrence, and kept its staff and students informed of the events. During a symposium on 5 February 2020, the university presented the reports of the investigation, and explained how the accident occurred and explained the lessons learned.[208] The Inspectorate for Education also investigated the accident.[209]

In December 2020, the Municipality Hof van Twente was hacked. As a consequence, the municipality was forced to shut down its services to local residents for a number of weeks (for passports, driver's licences, central register extracts) and for municipal tax, for several months; the municipality was also unable to pay invoices or cooperate securely with other organizations. The municipality was also forced to fully rebuild its digital system. Just like the Maastricht University, the Municipality of Hof van Twente kept its residents informed, with regular updates. They also commissioned an investigation, and published the results for the general public.[210]

In February 2021, the University of Amsterdam and Amsterdam University of Applied Sciences also suffered a cyber-attack. They too commissioned an investigation, and published the results.[211]

The tradition of learning from occurrences is still developing in the digital domain. Occurrences must be reported, but are not systematically investigated. An 'infrastructure' for shared learning by manufacturers, organizations using software and other relevant public and private parties is lacking.

207 https://ibestuur.nl/magazine/cyberaanval-lochem-gaat-de-hele-overheid-aan
208 https://www.maastrichtuniversity.nl/nl/updates-cyberaanval
209 https://www.onderwijsinspectie.nl/documenten/rapporten/2020/06/12/rapport-cyberaanval-universiteit-maastricht
210 https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2021/03/artikel/hof-van-twente-cyber-hack-stevige-les-voor-ons-1872
211 https://www.uva.nl/content/nieuws/nieuwsberichten/2021/07/evaluatie-cyberaanval.html

4.4.2 Barriers to learning from (investigations into) cyber occurrences

In the previous section, we described the various ways in which cyber occurrences are currently reported and investigated. We also discussed the way in which the results of these reports and investigations are used to give organizations a greater insight into what they can do to prevent future recurrence.

Across the board, the current method shows that learning from cyber accidents is hindered by a number of factors.

Reporting and publication

The Municipalities of Lochem and Hof van Twente and the educational institutions Maastricht University and University of Amsterdam/Amsterdam University of Applied Sciences can be seen as exceptions to the rule that says that organizations are unwilling to share in public the fact that they have been the victim of a cyber-occurrence, and the lessons they have learned as a consequence. In the discussions held by the Safety Board with various organizations and the parties representing them, a number of reasons are mentioned, of which three are discussed below.

Firstly, the fear of harm to reputation and loss of confidence from parties with whom the organization cooperates. A cyber occurrence such as a ransomware attack can be seen by the outside world as a sign that information security at the organization is below par. This can lead to a loss of confidence in the organization in question. This effect is difficult to measure. So far, there are no signs that data breaches necessarily lead to a decline in the value of the company. In addition, in other domains such as the food sector, there is evidence that organizations can actually maintain or strengthen trust if they come forward voluntarily with a security problem and address it decisively.[212] Another psychological effect is shame. This effect is greater in the event of cyber occurrences than other incidents such as a car accident. One of the reasons for this sense of shame is that the persons disadvantaged by a cyberattack, like a ransomware attack, feel that they have been cheated, that they have fallen for some trick and have failed. As well as losing their sense of safety, this also leads to a loss of status.[213]

A second obstacle to announcing an occurrence is the potential for legal consequences. If the cyber occurrence is accompanied by the violation of legal rules (for example if data has leaked or a duty of care has not been complied with), then regulators can take steps to enforce the rules. Other parties (consumers, end users, suppliers, shareholders) may also feel that their rights have been negatively affected, and in response sue the organization. One of the software manufacturers we spoke to, for example, learned lessons from the occurrence, took measures and shared a number of lessons and enhancements via hun website. However, it did not actively share those lessons with other manufacturers, parties involved or the public. If the software industry remains mutually and publicly closed about how errors occur, there can be no shared learning.[214]

212 See for example https://doi.org/10.15728/bbr.2017.14.2.4.
213 Goffman, E., 1952. On Cooling the Mark Out, *Psychiatry,* 15:4, 451-463, DOI: 10.1080/00332747.1952.11022896
214 See also E. Tjong Tjin Tai and B. Duties of care and diligence against cybercrime *(NJb)*, 2015.

The third obstacle mentioned is that the organization is afraid of the increasing risk of attacks, as soon as it becomes known that the organization has already been (successfully) attacked before.

The way in which cyber occurrences are investigated

Another obstacle to learning that relates to the barriers outlined above is how the factors that contributed to the occurrences taking place are described in the reports. As outlined above, reputation damage is one reason for not reporting occurrences. Shame (stigma) also plays a role. Evaluations that summarize the mistakes made by an organization without investigating and explaining how the organization found itself in that situation can increase the sense of stigma and do not contribute to the willingness of organizations to share their experiences with the outside world, so that others have an opportunity to learn.

Many of the evaluations are aimed at what the organization in question itself should do, and do not consider the system question that lies behind the question of why it is so difficult for organizations to prevent being attacked, and to successfully resist attacks. In the evaluations, the focus is more on security and less on establishing a safe digital system that is resistant to all kinds of possible threats.

Willingness to understand how things could happen is crucial in all occurrence investigations, including the ones under scrutiny. Therefore, in order to learn from accidents, it is important how the accident investigation is structured: that the accident investigation is aimed at being able to explain the accident. That in turn requires that the investigation goes beyond an assessment based on standards (single loop learning), and that it also reflects on the principles employed (double loop learning). Especially in a domain where learning from occurrences is evolving, it is important to also reflect on how we learn (third loop learning or deutero learning). Most evaluations examined by the Dutch Safety Board were restricted to single loop learning. Those evaluations consisted primarily of observations that the organization in question had failed to implement all the specified or expected basic measures, and that these were factors that had led to the occurrence. Or there were evaluations that, while analyzing the approach and policies, did not reveal what factors contributed to the occurrence of the incident.

The evaluation by the Inspectorate of Education of the ransomware attack on Maastricht University shows that a reflective approach to an incident investigation is both possible and worthwhile. In that investigation, for example, an explanation was sought for the fact that the information security did not satisfy the available standards. One of the explanations was that because of the multi-layered administration of colleges and universities, it is not possible for the governing board to maintain a clear view of the status of information security. This is an essential insight, because a multi-layered administration of this kind is present at all colleges and universities, and may well prevent the governing boards of other educational institutions from obtaining a clear view of the status of information security.

The dissemination of insights to parties that need those insights

In the subsection above, we refer to different types of investigations into occurrences. The information generated by these investigations is only published in a limited number of cases: when, by way of exception, the organization opts to publish, or is required to do so by the regulator. In the previous subsection, we took as examples Maastricht University, the University of Amsterdam/University of Applied Sciences Amsterdam, the Municipality of Lochem and the Municipality Hof van Twente. We also suggested that the majority of investigations into occurrences are not published, or only within a closed circuit. The information is in fact only comprehensible for a limited group of experts, and that makes it appear an abstract, technical event. For that reason it is important when sharing insights from cyber-attacks to demystify them and to underline their human consequences.[215]

Moreover, at present there is no single entity that collects the information from investigations and reports for the purpose of scientific and/or statistical study. In the cyber domain, which enjoys a relatively new tradition in respect of incident investigation, there is a clear need for a platform where knowledge is shared and retained and where organizations can go in search of relevant insights to further improve their information security policy (historic capture). Incidentally, this aligns with the NCSC's mission as the National Cyber Security Center: to understand and interpret what is happening, to connect parties, knowledge and experience with the goal of preventing recurrence. [216]

> In current practice, many organizations do not come clean about the fact that they have been attacked. The investigations do not provide the explanations needed to improve the system. Involved organizations do not share the lessons learned from occurrences outside their own organizations or communities.

4.5 Policy and the international context

At the European level, there are various regulations in the field of cybersecurity, as well as a number of initiatives under development. These regulations and initiatives each have a different purpose and target group. The table below lists some of the characteristics of the regulations.

215 Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat.* 2020 https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm

216 https://www.ncsc.nl/over-ncsc, accessed on 13 September 2021.

Legislative name	Type of legislation	Status	Content
NIS directive	Directive [217]	Should be implemented by Member States as of 10 May 2018.[218]	• Target audience: digital service providers and designated providers of essential services. • Cooperation among member states on cybersecurity issues. • Imposes obligations on target group to implement security requirements and report incidents.
NIS 2 directive	Directive	Draft directive.	• Target group: expanded from the NIS to include food sector, public administration, manufacturers of critical products, among others. • More stringent security requirements for organizations and strengthening of European cooperation.
Cyber Security Act	Regulation[219]	In operation since 27 juni 2019.	• Target group: entire European digital market • Expand the mandate of ENISA • Introduce cybersecurity certification framework (still under development)
Digital Operational Resilience Act (DORA)	Regulation	Draft regulation, expected to enter info force end 2022.	• Target group: financial sector. • Goal: harmonize rules on digital resilience in the EU. • Basic framework for financial organizations, sets basic requirements for financial organizations including risk management and digital incidents.
Horizontal software regulation	Unknown	Under development.	• Target group: software manufacturers[220]. • Horizontal legislation regarding cybersecurity requirements for software products.

In addition, there are also initiatives (in development) regulating Internet of Things (IoT), i.e. software that is part of other products. This includes the intention to set cybersecurity requirements for wireless devices via the Radio Equipment Directive and the regulation of connected devices in the Cybersecurity Resilience Act. In addition, a number of EU regulations were adopted in 2017 setting cybersecurity requirements for medical devices, and cybersecurity requirements will also be included in regulations for the automotive industry at UN level. Moreover, the general EU directive for product safety is being revised and will also include safety and security of products with digital components. There are also European developments in the field of consumer law for IoT products, which include, among others, matters relating to the right to updates.

217 A directive must be transposed into national law by the member states.
218 In the Netherlands, this is laid down in the Wbni.
219 A regulation is legislation directly applicable in all EU member states.
220 It is not yet clear for which specific target group this legislation is being developed.

Countering vulnerabilities in software, and investigating criminal acts for the purposes of enforcement and prosecution and the agreements on how States interact when it comes to cyberattacks all require international cooperation.[221]

The trade in software is an international market based on supply and demand. Manufacturers and end users are located throughout the world. As described in section 4.1, software as a product and the creation of that product throughout its lifecycle as a process are currently only regulated on the basis of legislation and regulations applicable to the domain in which the software is employed. For example software in vehicles and software in care institutions. Software itself is not subject to any government product or process regulations. There are however industry standards according to which a manufacturer can certify its software or processes, as a means of demonstrating accountability to its end users.

Actors who exploit vulnerabilities in software in order to attack the digital systems of organizations also come from all corners of the globe. They include criminal actors and actors working for nation states and combinations or hybrids of the two. Ransomware attacks, for example, are often carried out by criminal organizations, but often also serve as a cover for an operation by an intelligence service or as a way of generating income for a country. International cooperation is complex, partly because countries are not only the victims of unsafety through cyberattacks, but also benefit from vulnerabilities in software for their own activities.[222] In addition, ideological differences between countries are obstacles to international cooperation, for example disagreements on how States interact with the Internet and what actions against attackers (deterrence) are permissible.[223]

Nonetheless, the Member States of the European Union have shown over the past few years that they are able to enforce strict requirements on data protection and foreign investments, through cooperation. Countries also call each other to account (in public) more often after large-scale cyberattacks.

221 See also: Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat*. 2020 https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm

222 Perlroth, N. *This is how they tell me the world ends: the cyberweapons arms race*, 2021.

223 Henriksen, A., The end of the road for the UN GGE process: The future regulation of cyberspace, *Journal of Cybersecurity*, Volume 5, Issue 1, 2019, tyy009, https://doi.org/10.1093/cybsec/tyy009. Fischerkeller, M.P. en R.J. Harknett, Deterrence is Not a Credible Strategy for Cyberspace. *Orbis*, Volume 61, Issue 3, 2017, Pages 381-393, 2017. Daniel, M., *Closing the Gap: Expanding Cyber Deterrence*. Cyberstability Paper Series, 2021.

Multistakeholder groups also make a contribution to improving international cooperation. The Global Commission on the Stability of Cyberspace has for example developed proposals for standards and policy that have improved international cybersecurity and stability. These are standards for responsible behaviour by both state and non-state actors, in cyberspace. This commission brings together a large number of stakeholders from different countries and from different types of organizations, such as governments, universities and manufacturers. They drew up eight standards, including the following:[224]

- Non-state actors may not carry out cyberattacks and states must prevent this and respond if it does happen.
- States must in principle report vulnerabilities of which they become aware to the manufacturer, and operate a transparent framework for when they decide not to do so.
- Manufacturers of products and services must give priority to cybersecurity and stability and do everything reasonably possible to ensure that they contain no vulnerabilities. They must also take measures to mitigate vulnerabilities of which they become aware, and be transparent about their actions. All actors have a duty to share information about vulnerabilities in order to prevent cyberattacks and to limit their consequences.
- Countries must take measures including legislation and regulations so that basic cyber hygiene is maintained.

224 GCSC, *Advancing Cyberstability*, 2019.https://cyberstability.org/report/

5 CONCLUSIONS

This investigation began by asking what lessons can be learned from how involved parties dealt with the risks of the vulnerability in Citrix software that came to light in December 2019 and other similar occurrences in other manufacturers' software products. The common thread from the occurrences is that organizations and the people who depend on them are exposed to digital insecurity by using vulnerable software. The occurrences investigated in this report all illustrate that in many cases warnings do not reach them.

Our analysis at system level shows that the security of software and combating the consequences of insecurity take place in a network of parties, each of which has its own responsibility. However, none of them can guarantee security individually. Assuring safety is only possible when responsible parties cooperate with each other. For this cooperation, effective structures are needed and mutual trust must be strengthened. Below, we explain what the barriers are.

5.1 Producing and releasing software on the market

A range of factors contribute to the emergence of vulnerabilities during the lifecycle of a product. In many cases, existing products undergo further development, making the software increasingly complex. The programming language used can also contribute to the occurrence of errors, and the use of existing components and (inconsistent) layers in the architecture may introduce vulnerabilities.

Whenever (safety) problems are linked to fundamental choices in the product, this can represent an obstacle for the manufacturer in tackling the root of the problem. Such an approach after all requires an investment in the form of money and/or capacity for problem solving. The decision by the manufacturer to instead opt to only fix the vulnerability is explainable, but to truly solve a (safety) problem, it is sometimes necessary to fully revise a product from the base up.

Ethical hackers are encouraged with rewards to identify and report vulnerabilities in software. As a result, many vulnerabilities are identified. In addition, manufacturers detect vulnerabilities by carrying out a variety of tests. Nonetheless, it is not possible to find all vulnerabilities. It is becoming more common for vulnerabilities to form an attack route. Disclosing a vulnerability can help organizations better arm themselves against potential exploitation, but it can also enable attackers to exploit the vulnerability. This is reinforced by the fact that sometimes hackers need just a single vulnerability in order to gain access to a system, also because it is relatively simple for them to find vulnerable servers. This creates a dilemma which in turn reduces overall safety.

Contents
Summary
Consideration
Recommendations
Abbreviations and definitions
1 Introduction
2 Relevant concepts explained
3 Software vulnerabilities and their consequences: course of events and analysis
4 System analysis
5 Conclusions
6 Recommendations
Appendix

The number of detected vulnerabilities in software is growing, as are the consequences of attacks. Vulnerabilities play an increasingly important role in cyberattacks, and can be used by attackers as the starting point for launching an attack. This underpins the importance of timely patching. However, patching and mitigating at the same time pose a risk, because they can lead to disruptions or the introduction of new vulnerabilities. The organization must therefore think through the decision to patch carefully from the perspective of the organization's IT landscape. The publication of a vulnerability can be the precursor to widespread attacks.

Regulation and liability also play a role in the occurrence of vulnerabilities. At present, governments and other organizations have few possibilities for obliging manufacturers to safeguard cybersecurity in their products. Buyers of software do not always know how to impose requirements, and force manufacturers to show accountability. This makes vulnerability a problem for the user and not the manufacturer.

There are practically no rules for placing software on the market. The current free market for software products imposes almost no requirements on the sound management of security risks. Identifying vulnerabilities is a time-consuming task, that demands much manpower and as a consequence is costly. In certain cases it can be necessary to completely rebuild a product in order to tackle the underlying (safety) problem. The absence of economic incentives explains why manufacturers at present do not consider this option.

5.2 The purchase and use of software by organizations

The regular patching of software introduces new problems. If an organization fails to patch, it may be opening itself up to the risk of a security breach that can be automatically traced by external parties. Due to the large and ever growing number of patches, patching all vulnerabilities is not manageable for all organizations. Moreover, for organizations, the necessity of (rapid) patching is not always clear. Offering software from the cloud shifts the responsibility for patching to the manufacturer, but also entails risks for organizations that use the software.

Due to the asymmetric relationship between manufacturers and customers in the field of software security, buyers of software 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.

5.3 Incident management

Incident response in the Netherlands, including the gathering 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 (also unsolicited) that its systems are vulnerable 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.

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.[225]

5.4 Learning from occurrences

The tradition of learning from occurrences is still developing in the digital domain. Occurrences must be reported, but are not systematically investigated. An 'infrastructure' for shared learning by manufacturers, organizations using software and other relevant public and private parties is lacking.

In current practice, many organizations do not come clean about the fact that they have been attacked. The investigations do not provide the explanations needed to improve the system. Involved organizations do not share the lessons learned from occurrences outside their own organizations or communities.

225 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.

6 RECOMMENDATIONS

This investigation shows that vulnerabilities in software lead to insecurities for organizations that use software, and for those who depend on these organizations. The gap between digital dependency and the threat level on the one hand; and the extent to which society is resilient to it on the other hand, is growing. Fast and fundamental interventions are needed to prevent society from being disrupted. That is why the Dutch Safety Board issues recommendations. The first recommendation aims to increase response capacity in the short term. The recommendations that follow aim, in the longer term, to strengthen the public and private system and introduce incentives to create a system in which manufacturers and buyers of software work continuously to make software safer and more secure.

To the Dutch Cabinet and to organizations in the Netherlands that use software:[226]

1. Ensure in the near future that all potential victims of cyber attacks are alerted quickly and effectively – solicited and unsolicited - so they can take measures for their digital safety and security. To this end, bring together public and private response capacity and ensure sufficient mandate and legal safeguards.

Note: In any case, this concerns information about which systems of which organizations are vulnerable and at risk of being attacked (so-called 'victim information'). Currently, the legal interpretation of the GDPR (IP addresses as personal data) and the Dutch Security of Network and Information Systems Act (Wbni) (mandate of the NCSC limited to national government and vital operators) prevents the National Cyber Security Centre (NCSC) from warning all victims they receive information about, and from proactively collecting this information (scanning).

To the European Commissioner for Internal Market and the European Commissioner for A Europe Fit for the Digital Age:

2. Ensure that your initiatives to legislate for safer and more secure software lead to a European regulation that establishes the responsibility of manufacturers and provides insight to buyers of software in how manufacturers assume this responsibility. Establish that manufacturers are liable for the consequences of software vulnerabilities.

Note: Essential elements of this regulation include – but are not limited to – mandatory participation in bug bounty programmes, guidelines for independent audits, vulnerability reporting, traceability, recalls, and the sharing of lessons learnt from cyber attacks.

226 For practical reasons, the Dutch Safety Board addresses the government in its role as user of software through the State Secretary of the Interior, the Interprovincial Consultative Council, the *Vereniging van Nederlandse Gemeenten* (Association of Netherlands Municipalities), and the *Unie van Waterschappen* (Union of Water Boards). The other organizations, including health care, education, vital operators and other businesses, are addressed by the Dutch Safety Board through employers' organizations involved in the SER, such as: VNO-NCW, MKB-Nederland and LTO Nederland.

Legislation such as the GDPR has proven that European regulations in the digital domain are feasible and effective.

To software manufacturers collectively:[227]

3. Develop good practices with other manufacturers to make software safer and more secure. Include a commitment to these practices in contracts with your customers.
4. Warn and help all your customers as quickly and effectively as possible when vulnerabilities in software are identified. Create the preconditions necessary to be able to warn your customers.

Note: The responsibility and possibilities for making software safer and more secure, and for warning customers primary lies with the manufacturers themselves.

To the State Secretary of the Interior and Kingdom Relations and the Minister of Economic Affairs and Climate Policy (for the benefit of all organizations and consumers in the Netherlands)[228]*:*

5. Encourage that Dutch organizations and consumers jointly formulate and enforce safety and security requirements for software manufacturers. Ensure that the government plays a leading role in this. Proceed on the basis of the principle: collective cooperation where possible, sector-specific where necessary.

Note: It is necessary for buyers of software to join forces in order to strengthen their position towards manufacturers and jointly deploy the scarce cybersecurity expertise as efficiently and effectively as possible. A number of Dutch banks is already cooperating in this matter.

To the Dutch Cabinet:

6. Create a legal basis for the management of digital safety and security by the government, by analogy of the Dutch Government Accounts Act (Comptabiliteitswet).
7. Require all organizations to uniformly account for the way in which they manage digital safety and security risks.[229]

Note: The way in which governments and companies manage and account for the risks that are associated with digitization is as yet noncommittal. Fragmentation of responsibilities impairs decisive action. It is essential that a comprehensive system is put in place to help organizations to manage digital safety and security in a systematic and effective manner. Possible elements include an unambiguous mandate for government CISOs, supervision that is entrusted to the minister responsible, and mandatory accountability for all organizations regarding the management of digital safety and security risks, through annual reports and as part of the auditor's report.

227 This recommendation is addressed to all software manufacturers. For practical reasons, the Dutch Safety Board addresses the manufacturers involved in the incidents described in this investigation, the communities of the open source projects involved and the (members of the) Business Software Alliance trade association.

228 See footnote 2. Because of the relevance of safe and secure software to end users (including consumers), the *Consumentenbond* (Consumers' Association) will also be addressed. And the Chamber of Commerce for support to organizations

229 It is within reason to align with existing structures and obligations in the 2016 *Comptabiliteitswet* (applicable to governments), Civil Code (non-listed legal entities), further regulations on auditing and other standards (NV COS) from the NBA and harmonized legislation for public limited companies from the European Union.

APPENDIX A

JUSTIFICATION OF THE INVESTIGATION

A.1 Objective and investigation questions of the investigation

The aim of this research is to identify lessons that help responsible parties to manage the risks arising from software vulnerabilities. The lessons are aimed at software manufacturers, organizations that use software, and governments and other organizations that can help prevent and manage such incidents.

The Citrix incident in December 2019 was the cause for this investigation, as typical example of an event where these risks arise, as demonstrated by other cyber-attacks since 2020.

The Dutch Safety Board assumes that the way in which manufacturers, organizations that use software, the government and other organizations manage digital security risks[230], determines the extent to which incidents such as these can take place and the extent to which they influence the physical and social safety of citizens. Based on this starting point, the Board formulated the following investigation question:

> What lessons can be learned from the way in which the stakeholders dealt with the risks resulting from the Citrix software vulnerability that was discovered in December 2019?

Sub questions:

1. How could the security breaches occur within the organizations as a result of the vulnerability in Citrix software, and what were the consequences?
2. How were these risks assessed and what measures were taken to prevent the occurrences' undesirable consequences (risk governance):
   a. by the software manufacturer and organizations that purchase and use the software;
   b. by the public administration / the government and non-government parties?
3. What is needed from parties involved in order to reinforce the system of risk governance and risk management?

230 The way in which organizations manage risks is also called risk governance.

A.2 Data gathering

The Board adopted the following approach during the investigation.

To familiarize themselves with the subject matter, the team attended a two day training course organized by a security company. During the same period, we started collecting mainly public information. This included policy documents, news items, media reports, published incident investigations, academic publications and documentation on software, vulnerabilities and exploits.

We supplemented this information by approaching the parties involved for interviews and, in parallel, asking written questions about vulnerabilities, working methods of organizations when producing, updating, purchasing and using software and responding to incidents (statements of facts, internal communication, reports of meetings, logs). Most parties cooperated. The Dutch Safety Board has reached out to vendors mentioned in the investigation through several channels mentioned on their websites, by email and by mail. The Board considered contacting the PSIRT, but since the investigation does not concern a direct security incident and since the Board is not a CERT organization or another target group of Fortinet's PSIRT, did not deem this an appropriate channel to establish contact. Unfortunately our efforts to establish contact with some vendors[231] were unsuccesful in the investigation phase of this investigation.

In total, about 1,200 documents were analyzed in the investigation. In addition, we conducted over 40 interviews with parties involved at manufacturers, organizations that use the software and that respond to incidents, public, private as well as non-governmental.

A.3 Analysis

A.3.1 Accident analysis

We reconstructed the course of events using a timeline analysis. In order to gain insight into the possible factors that may have influenced the incident, we analyzed the incident using the incident analysis method Tripod Beta. We used BowTie to visualize the findings. The various analyzes mainly had an internal purpose: to organize the information and to check whether the information was complete and consistent. In the report we included some general timelines, to help the reader read the report.[232]

A.3.2 System analysis

To visualize how the various actors ensured safety, we did an environmental and stakeholder analysis and applied the CAST/STAMP method. CAST provided insight into

231 Vendors Fortinet, Palo Alto and F5. Fortinet and F5 participated in the review procedure. F5 responded to the questionnaire at the review stage of the investigation.

232 Hendrick, K. & J. Benner, *Investigating accidents with STEP,* 1987. Dekker, New York. Stichting Tripod Foundation, 2008. *Tripod-Beta User Guide*. Stichting Tripod Foundation, Vlaardingen. Hudson, P.T.W., 'Applying the lessons of high risk industries to health care'. In: *Qual. Saf Health Care* 2003, 12 (Suppl.1):17-21, 2003.

the hierarchical lines, roles and responsibilities of the parties involved and the relationship with laws and regulations. We applied this to:

- vulnerabilities in software
- the way in which organizations purchase and use software
- incident response

As a theoretical framework, we align with the theories from publications on cybersecurity governance. Where relevant, a comparison was made with other sectors in which the Dutch Safety Board carries out investigations, such as transport and food safety.[233]

A.3.3 Quality control

The following steps were taken to ensure the quality of the investigation:

- The project team has drawn up a quality plan for the investigation, in which risks to the quality of the research and associated control measures have been formulated.
- During the research process, the project team held several sessions. During these sessions, the research findings from interviews, documents and analyzes were shared and interpreted and team members contradicted each other's input. The first sessions focused on the research design (research questions, focus and boundaries). The sessions that followed were devoted to incident analysis and systems analysis. During these sessions, one of the members of the supervisory committee reflected explicitly on the confrontation of the findings with practice. In the last sessions we formulated the conclusions and recommendations of the research.
- During the research, a counter-thinking session was organized and colleagues counter-read the intermediate and final products of the research. Counter-thinking and counter-reading means that researchers who are not part of the project team read intermediate products of the research and comment on them. This was done with the starting documents (consideration framework, focus memorandum, plan of action), the interim findings and the draft version of the report. The results of the counter-thinking session and the counter reading were used to improve the analysis and the report.
- The research was discussed with a supervisory committee (see next paragraph).

A.4 Guidance committee

The Dutch Safety Board established a guidance committee for the purposes of this investigation, consisting of external experts who can offer experience and expertise relevant to the investigation, chaired by a member of the Safety Board. The external members sit on the guidance committee in a personal capacity. The committee met on four occasions to exchange ideas with the Board member and the project team, regarding the format and findings of the investigation. The committee fulfils an advisory role within the investigation. Final responsibility for the report and the recommendations lies with the Dutch Safety Board.

233 Leveson, N., M. Daouk, N. Dulac & K. Marais. *Applying STAMP in Accident Analysis*. MIT, Cambridge, MA, 2003; Leveson, N. 'A New Accident Model for Engineering Safer Systems'. In: *Safety Science,* Vol. 42, No. 4, 2004. Ellis R. en V. Mohan , *Rewired: Cybersecurity Governance*, 2019, Anderson, R. *Security Engineering*, 2020.

The committee is composed as follows:

Name	Function
Prof Dr S. (Stavros) Zouridis	Chair of the guidance committee, member of the Dutch Safety Board.
Rear Admiral b.d. P.J. (Pieter) Bindt	Former director of the MIVD, currently independent advisor and associate member of the Dutch Safety Board.
I. (Inge) Bryan MA	Managing director NCC Europe/ CEO Fox-IT (main function), Board member Global Forum on Cyber Expertise, Chairman Anti-Abuse Network[234].
Dr M. (Martijn) Dekker	Chief Information Security Officer (CISO) at ABN AMRO, member Security Board IBM and lecturer TIAS.
Prof Dr M.J.G. (Michel) van Eeten	Professor governance of cybersecurity at TU Delft
A.P. (Arnoud) Engelfriet LLM MSc	ICT law expert, partner at ICTRecht, and author.
M.R. (Marietje) Schaake MA	International Policy Director at Stanford University Cyber Policy Center, and President CyberPeace Institute.

A.5 Project organization

Name	Function
Dr A. (Arzu) Umar	Investigation manager
M. (Marjolein) Baart MSc MPS	Project leader
M.A. (Marlon) van den Hoek MSc	Investigator
N.E. (Nynke) Wierda MSc	Investigator
H.W. (Berthil) Verzijl MSc	Investigator
E.V. (Eliane) de Vilder	Investigator
A.J. (Sander) Bakker MSc	Technical specialist
E.J. (Elsabé) Willeboordse MSc	Research and development advisor
R.T. (Ron) Koppes MSc	Research and development advisor
Y.S.A. (Yannick) Balk MA	Secretary – Safety Specialist
R.D. (Reinier) de Wit MSc	Secretary – Safety Specialist
J. (Jale) Demir	Project office assistant

234 Other additional functions: Board member of Royal Holland Society of Sciences and Humanities, Supervisory Board member of Clingendael, Advisory Board member of: National Archives, Police Academy, Executive master Legal technologies Leiden University and Inspectie Openbare Orde en Veiligheid (ministry of JenV) (since 1 September 2021).

APPENDIX B

RESPONSES TO DRAFT REPORT

The draft report (without consideration and recommendations) was submitted to the various stakeholders. These parties were asked to check the report for factual inaccuracies and inconsistencies. The following parties responded to the draft report:

- Citrix
- Ivanti
- Fortinet
- F5
- Minister of JenV, including NCTV and NCSC
- Minister of BZK, including CIO Rijk
- AIVD
- Minister of EZK, including DTC
- DIVD
- SURFcert
- IBD

The following parties refrained from reacting to the draft report:

- Z-CERT
- European Commissioner for Internal Market and European Commissioner for a Europe fit for the Digital Age

Palo Alto could not be reached.

The responses received, as well as the way in which they were processed, are set out in a table that can be found on the Dutch Safety Board's website (www.safetyboard.nl).

The responses received can be divided into the following two categories:

- Corrections and factual inaccuracies; additional details and editorial comments that were taken over by the Dutch Safety Board (insofar correct and relevant). The relevant passages were amended in the final report.
- The responses that have not been adopted are presented in the table with the Dutch Safety Board's reasons for not adopting them.

APPENDIX C

REFERENCE FRAMEWORK

In all its investigations, the Safety Board operates a reference framework. This framework explains how risks can best be managed, based on the latest insights, and outlines what the Safety Board expects from parties in managing an occurrence, such as in this investigation vulnerabilities in software and the resultant security breaches in digital systems of organizations. The reference framework describes best practices for the relevant players, and the ideal conditions that need to be in place to safeguard cybersecurity.

C.1 Safeguarding cybersecurity

As in other domains, such as food, transport, healthcare and the process industry, safe and secure digital systems that use software are developed within a network of activities and parties. And just like in other domains, software is by definition an imperfect product, such that the use of digital systems engenders inherent safety risks.

In the Netherlands, safeguarding cybersecurity is a responsibility shared by many parties.

Various types of organization are involved in the development and use of software.
- Software manufacturers
- IT service providers
- Security companies
- Organizations that use software: government, healthcare, education, public utilities, private companies, et cetera
- Within the organization: executive board, CIO, CISO

In this investigation, we examine how the roles and responsibilities of all these parties are organized: the structures, processes, standards and agreements for managing risks to digital systems in the Netherlands. These organizations are (semi) government organizations, large companies and small and medium-sized enterprises. To be able to control risks, it is essential that all these parties have clear tasks, roles and responsibilities, that in combination form a single unit. The relationships between the parties are clear and there is no uncertainty with regard to structure. It is also necessary that these parties be sufficiently familiar with one another and that they have developed routines that enable them to take and implement necessary decisions in a timely manner, and that

standards be in place that must be enforced in order to secure against the risks of using digital systems.[235]

National government is responsible for the system within which all these parties operate and within which they are mutually dependent for safeguarding safety and security. This makes it necessary for national government to view preventing and responding to digital occurrences as a collective task for society, within which national government bears system responsibility. In the same way that national government bears system responsibility for how we safeguard the safety of our cars and our food, both on a preventive basis and in dealing with incidents.

C.2 Product safety of software

Software is a dynamic product: even after it has been placed on the market, improvements and expansions are regularly added. Every owner of a PC or smartphone is conversant with regular requests to carry out updates and install patches. The same applies to software for professional software buyers (business market). As a rule, software products are made up of a large number of components. As is the case in other domains, the eventual software manufacturer (also known as the vendor) rarely makes these components itself. Instead, the manufacturer builds on components developed by others and housed in libraries[236]. A number of these components are open source, while in respect of other components, there is a system of internal trading.

During the lifecycle of software, vulnerabilities are often discovered that have to be repaired. These vulnerabilities are discovered by or on behalf of the manufacturer itself or by ethical hackers, who may be acting on behalf of the organizations that use the software. By way of indication: every year, software manufacturers release around 30,000 software updates (patches) to repair vulnerabilities. The question remains what manufacturers and other stakeholders can be expected to do, when it comes to preventing the occurrence of vulnerabilities in software wherever possible.

These responsibilities must be seen against the background that security is an emergent property determined by the properties of the software itself combined with the way the software is part of and is used within the context of a digital system.[237] The use of a digital system linked to the Internet then inherently involves additional risks, for example that the digital system could be attacked. To control those risks, organizations use certain software components which for example regulate who is given access to what parts of the digital system, or that protect a link to the rest of the Internet. As a consequence, this software has a security-critical function for the digital system: if there is a security problem (vulnerability) in that software, it can threaten the safety and security of the entire digital system.

235 See among others Hood C. e.a. *The Government of Risk: Understanding Risk Regulation Schemes*, 2001.
236 Libraries that can be used by multiple software applications are known as dynamic linkers. In Windows, this is known as a dynamic link library (DLL) and in Linux it is referred to as shared objects (.so).
237 Leveson, N., 'Are you sure your software will not kill anyone?', *Communications of the ACM*, 2020.

The role of manufacturer and end user

Certainly in respect of software that fulfils a safety-critical function within the digital systems or organizations (such as the software considered in this investigation), the Safety Board expects that manufacturers operate a policy of safety and security by design right from the start of the design phase and throughout the entire lifecycle of the software.

The software must be designed to be resistant to attack and to respond appropriately when the technology fails (failsafe). With that in mind, in designing the software, the manufacturer must take account of inexpert use and must ensure that the software is resistant to (unintended) incorrect or inexpert use (fool proof). This refers for example to the standard configuration of the software.

A manufacturer can therefore be expected to undertake a constant safety and security analysis of the entire architecture of the product, as this is something a user is unable to do. It is important that the manufacturer undertakes these analyses, in the constant process of further developing the software, for example by constantly purchasing and integrating components and other products. At the same time, the end user has an individual responsibility to consider how the product is used, and to understand the nature of the organization's landscape.

In the further development of the software throughout its lifecycle, the manufacturer must continue to monitor the safety and security of the components used in the software. For example when components used in the software or programming languages no longer satisfy the latest standards, are no longer viewed as good software engineering practice or contain vulnerabilities.

It is also important that manufacturers offer those organizations that purchase and use their software an insight into the nature of the technology and the components that make up the software (transparency). This is important for reinforcing the information position and potential for response of the organization using the software. The organization must be able to employ the software in its digital systems in such a way that in the given context of the organization, its systems and activities, the software remains safe. Manufacturers must also be able to demonstrate to organizations and authorities that their software satisfies the safety and security requirements imposed on it. Manufacturers must for example offer the opportunity to have their software pen tested, and subjected to substantial technical audits such as code reviews.

The role of government[238]

The Dutch Safety Board sees cybersecurity as a crucial precondition for a responsible process of digitalization. For organizations, be they governments or businesses, digitalization is no longer a choice but a necessity for performance and continued existence. In a broad sense, this also applies to individuals in their role as consumers, citizens or employees.

238 See for example Ministry of Economic Affairs and Climate Policy & ministry of Justice and Security, *Roadmap for Digital Hard- and Software Security*, April 2018.

Against this background, the Safety Board considers national government as having a crucial role in system responsibility. This applies not only to safeguarding cybersecurity, but is also based on government's responsibility for protecting the fundamental rights of citizens/consumers, investigating and prosecuting criminal actions, protecting our economic position and vital functions and protecting our territorial integrity.

With regard to responding to cybersecurity incidents, the Safety Board considers government responsible for requiring and as necessary stimulating the establishment of an effective system for risk governance, that the government is responsible for establishing the parameters that make it possible for organizations to take their responsibility for cybersecurity. Seen in the light of other domains in which the Safety Board is active, such as the transport sectors and the food sector, a system of this kind must consist of a series of individual but mutually reinforcing components.

This approach means that it is immediately clear to everyone which minimum safety and security requirements the software and processes of manufacturers and organizations that use software (including the government itself) must satisfy before the software is placed on the market (admittance requirements) through the entire lifecycle of the software (permanent requirements) and how the organization uses the software in its digital system (user requirements). It is also clear and transparent for both manufacturers and for organizations that purchase products and services from those manufacturers how the manufacturers can demonstrate their compliance with the safety and security requirements. At the end of the day, it is government that ensures that organizations that use the software occupy an information position and have sufficient potential for response so that they are independently able to assess the risks and reach decisions appropriate to the inherently risky situation that emerges from being connected to the Internet and that they use safety-critical software in that process. It must also be possible for customers and individual citizens to determine that the organization in question controls the risks.

Given the international character of digital systems, government is also responsible for ensuring international agreements on the requirements, compliance and the relevant information. A dynamic product like software is the ultimate example of a product that requires a learning system in which manufacturers, organizations and other stakeholders work together to share with each other lessons from past experiences and incidents, to avoid all parties constantly reinventing the wheel (thereby ensuring that the processes remain adequately harmonized). It is up to government to organize the parameters, such as the possibility of safe reporting and investigation, without the same information being used in legal proceedings. A clear example is set by the transport sectors, for whom these requirements are laid down in international regulations, both for the manufacturers and for the organizations using the products. Another example of a sector with international chains of manufacturers, brokers and buyers is the food sector. Within this sector, various parties collaborate in worldwide programmes by drawing up requirements and best practices, and exchanging information about risks relating to raw materials, products and suppliers, via platforms.

One aspect that is unique in respect of other sectors is that vulnerabilities in software not only represent a product safety problem, but that they can also form part of the cyber arsenal of various globally operating players, including criminals and (those working for) state actors. Based on its constitutional task of striving to develop the international rule of law[239], national government has the responsibility of undertaking to arrive at clear rules of play and ensuring compliance with those rules, on the global playing field. The fact that vulnerabilities in software can be deployed as a cyber-weapon is also relevant in the distribution of roles, tasks and responsibilities in risk governance, incident management and learning from incidents.

Socially responsible digitalization
Both in developing new software and throughout the lifecycle of existing software, to make digitalization possible, corporate social responsibility contributes to achieving a 'balance between the efforts aimed at maximizing the positive contributions of digitalization, and minimizing its negative consequences'.[240] Essential in this respect is the shared responsibility for social integration between manufacturers, government and (other) societal players (such as organizations using software). Naturally, the manufacturers bear primary responsibility for a safe and secure software design. It is then the role of government to map out and to monitor both the opportunities and risks of digitalization and to share these with the parties in a position to take mitigating measures.[241]

C.3 Prevention and preparation for incidents

Organizations bear primary responsibility for their own IT and information security. Any organization that uses IT has what is known as 'digital duty of care'.[242] For various different sectors/types of organizations, there are standards and statutory obligations that can assist organizations in structuring their information provision and information security.[243] Examples of these principles for information security among organizations are as follows:

- IT must occupy a fixed place on the agenda of the management or board of an organization, so that these perceive and take this responsibility for IT policy. Clear agreements on cybersecurity are also essential;
- Organizations must have in-house access to sufficient technical and organizational expertise and capacity, so that they are able to take measures to guarantee the safety of the systems. This is based on a variety of standards and certification mechanisms;
- It is crucial that an organization understands its risks, and based on a cost-benefit analysis identifies which risks are viewed as acceptable and is aware of the possible consequences if these risks are not safeguarded. An organization must have an insight into the vital components and organize proportional and appropriate security (the security measures depend on the risk). This also includes the consideration of how urgent it is to immediately patch certain software components and whether or not to

239 Article 90 of the Dutch Constitution.
240 Rip, *The Past and Future of RRI*, Life Sciences, Society and Policy 10, number 1, 2014.
241 Dutch Safety Board, *Who is in control? Road safety and automation in road traffic*, November 2019.
242 Cyber Security Council, *'Every company has digital duties of care', a guide for businesses in the field of cybersecurity,* February 2017.
243 For example: Government Information Security Baseline (BIO, ISO27001 and ISO27002) for government organizations, NEN7510 for healthcare, GDPR for the processing of personal data, WBNI for digital service providers, ABDO for organizations working for the Defence organization.

produce certain components crucial for the performance of the organization as redundant and diverse[244];
- it is important for an organization to be aware of its chain dependencies. Organizations need to reach agreements on cybersecurity with their chain partners (after all a chain is only as strong as its weakest link);
- before an organization purchases new software, it is important to consider the safety and security requirements the software in question must satisfy.

C.4 Incident management (response)

How can manufacturers and organizations that use software respond if software that is already on the market and in use in fact contains vulnerabilities? These activities are referred to as incident management or response. This relates both to response by the manufacturer (repairing the vulnerability possibly with a temporary mitigating measure and a definitive patch, and warning customers), by organizations using the software, their overarching sectors and government.

A manufacturer can be expected to do everything reasonably within its power to remove unsafety for organizations that use the software. It is also to be expected that manufacturers investigate the causes of the vulnerability, so that as far as possible they can reduce these factors thereby preventing future vulnerabilities. Government can be expected to ensure a clear allocation of responsibilities to the relevant parties. In that connection, it is important that the parties have access to the appropriate means and authorities to be able to exercise these responsibilities and that clear lines of transparent communication be established so that the information quickly reaches all the parties that need it, in order to control safety and security and that this information offers sufficient potential for response.

244 Redundant means that when a component fails, the entire system can continue to function for example by duplicating certain components. For example by using two different types of software for granting remote access to the digital system of the organization, so that one system can be shut down for maintenance or if unsafe. This relates closely to software diversity, a principle whereby the security of a digital system is reinforced by using a diversity of products. The redundant and diverse implementation of functions can be a dilemma for an organization, because it increases the complexity of the system. See for example Q. Zhang, J.-H. Cho, T.J. Moore and I.-R. Chen, "Vulnerability-Aware Resilient Networks: Software Diversity-based Network Adaptation," in *IEEE Transactions on Network and Service Management*, doi: 10.1109/TNSM.2020.3047649

C.5 Learning from incidents

To prevent incidents, it is important to learn from past accidents. This requires a learning process in which the lessons from accidents are returned as feedback to the organizations that need the information in order to improve safety and security:[245]

1. incidents and accidents are reported within the affected organization and possibly to an external body. In the first instance, the manufacturer of the software and the party responsible for the digital system are responsible for reporting incidents, but other parties such as buyers of software and independent digital investigators (ethical hackers) are also able to report occurrences. Another essential aspect is that there must be clarity on where and how reports of this kind can be carefully and safely received and investigated.
2. on the basis of criteria, a selection is made of which occurrences are eligible for further investigation by the appropriate organization (the manufacturer of the software, the manager of the digital system, etc.) and possibly by an external body (for example a regulator or an independent investigating authority). Many organizations are willing to learn from major and serious accidents, but the investigation of incidents can also reveal insights that can be viewed as warnings[246] and thereby prevent larger accidents;[247]
3. the investigation is implemented (see below);
4. the organization and/or investigators in question share the results of the investigation with the parties that are in a position to take action to improve safety and security and prevent accidents in the future.
5. the affected parties adapt the process of risk management on the basis of the insights gained from the accident investigation.

It is important that the factors that led to the occurrence and caused the consequences, the management measures that influenced the occurrence and the context within which the occurrence took place be mapped out in as much detail as possible. The structure and implementation of the investigation are key in determining the extent to which the investigation is able to provide these insights. Literature studies and previous investigations by the Safety Board reveal that the following elements are crucial:

- awareness and the taking of measures to manage the various forms of bias among the investigators (the best-known is the hindsight bias) and among the investigated parties (subjective assessment, dependency position);
- ensuring knowledge and expertise that tie in with the type of incident or accident;
- the investigator must have access to relevant data and the resources needed for data gathering;
- the investigators must use methods that tie in with the type of occurrence and that guarantee an appropriate method of reporting during the investigation, so that the findings remain traceable;

245 Lindberg, A.K., S.O. Hansson and C. Rollenhagen, Learning from accidents – what more do we need to know? *Safety Science* 2010, no. 6, p. 714-721.

246 Drupsteen L. and P. Hasle, 'Why do organizations not learn from incidents? Bottlenecks, causes and conditions for a failure to effectively learn', *Accident Analysis & Prevention 2014,* no. 72, p. 351-358; E. Stemn, C. Bofinger, D. Cliff and M.E. Hassall, 'Failure to learn from safety incidents: Status, challenges and opportunities', *Safety Science,* 2018, no. 101, p. 313-325; Lindberg 2010.

247 Dien Y. and M. Llory, 'Effects of the Columbia Space Shuttle Accident on High Risk Industries or: Can We Learn Lessons from Other Industries?', in: *Proceedings of Hazards* 18 Conference 2004.

- the investigation must be aimed at explaining the accident and reflecting on the principles employed (double loop learning) and the extent to which the organization is capable of learning (triple loop or deutero learning), and therefore go beyond mere assessment according to standards (single loop learning)[248];
- the scope of the investigation must be sufficiently broad to obtain a clear picture of all factors that contributed to the occurrence.

248 Argyris, C. 'Double loop learning in organizations', *Harvard Business Review,* 1977, September, p. 115-124. C. Argyris and Schön 1978; C. Argyris and D.A. Schön, *Organizational learning II: Theory, method and practice*, Reading, MA, United States: Addison-Wesley 1996.

TIMELINES PER VULNERABILITY

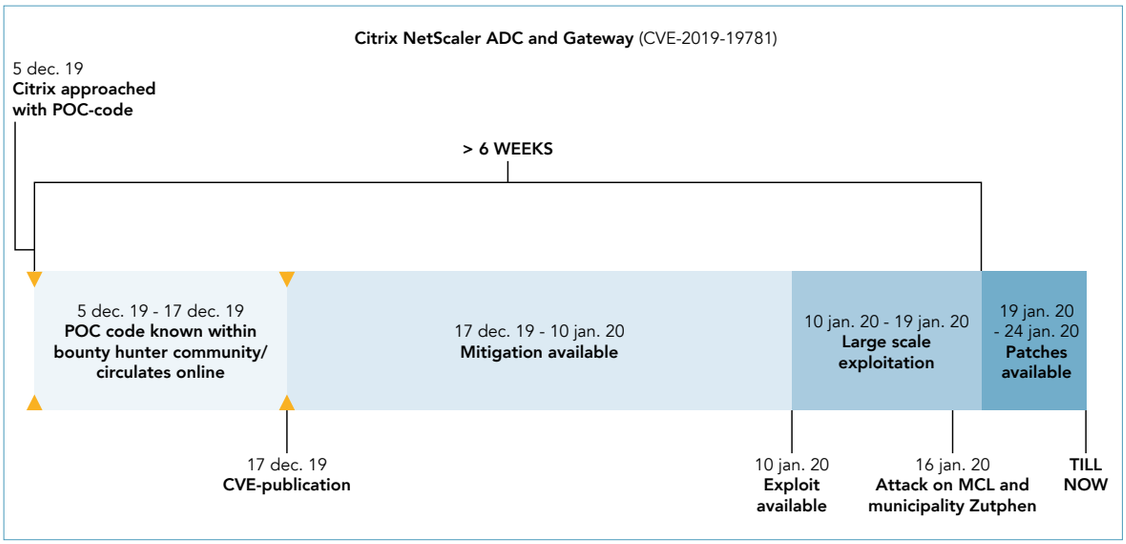


Figure 19: Timeline Citrix NetScaler ADC and Gateway.

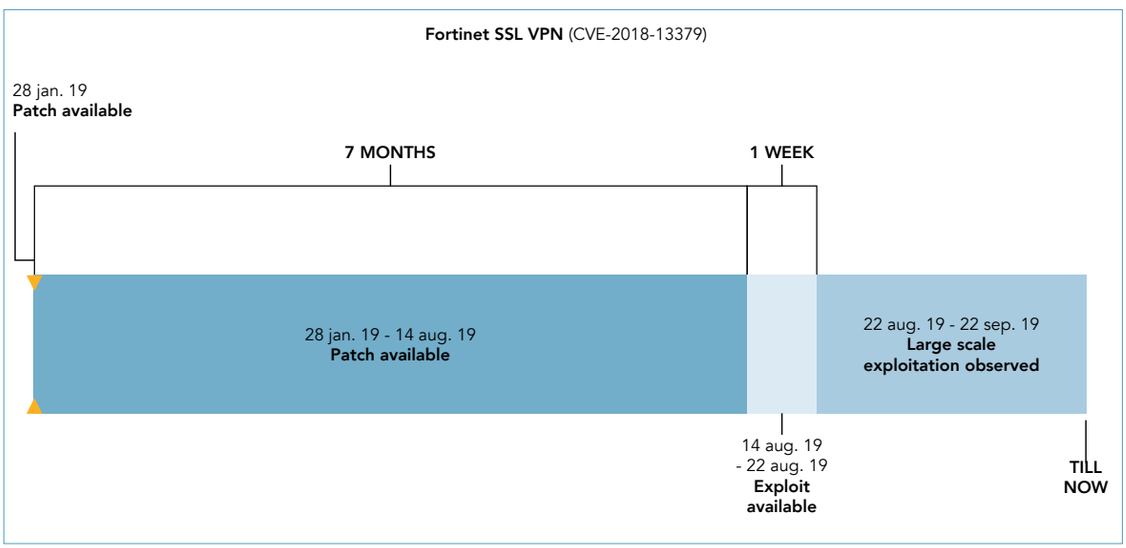


Figure 20: Timeline Fortinet SSL VPN.

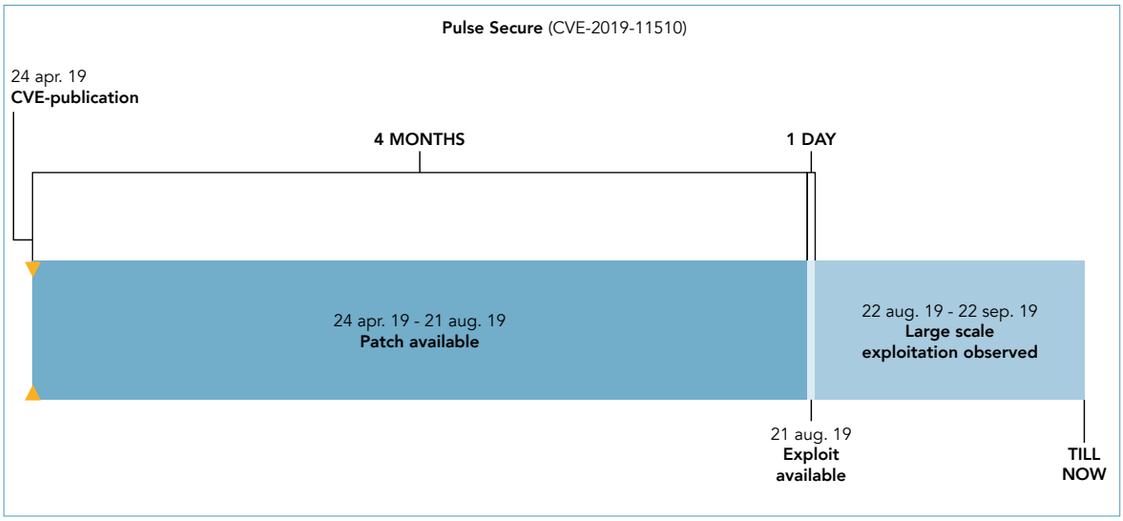


Figure 21: Timeline Pulse Secure VPN.

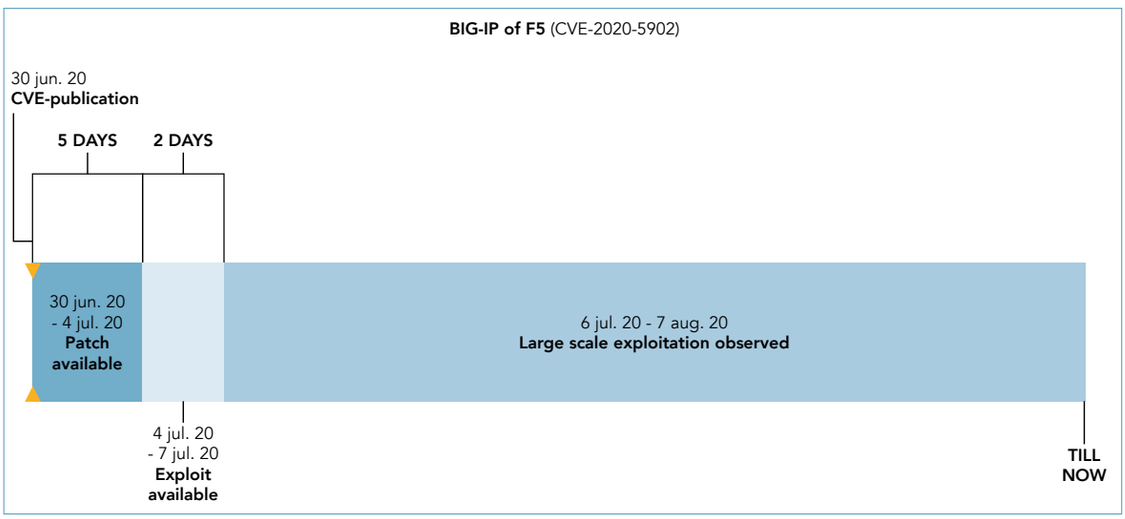


Figure 22: Timeline F5 BIG-IP.

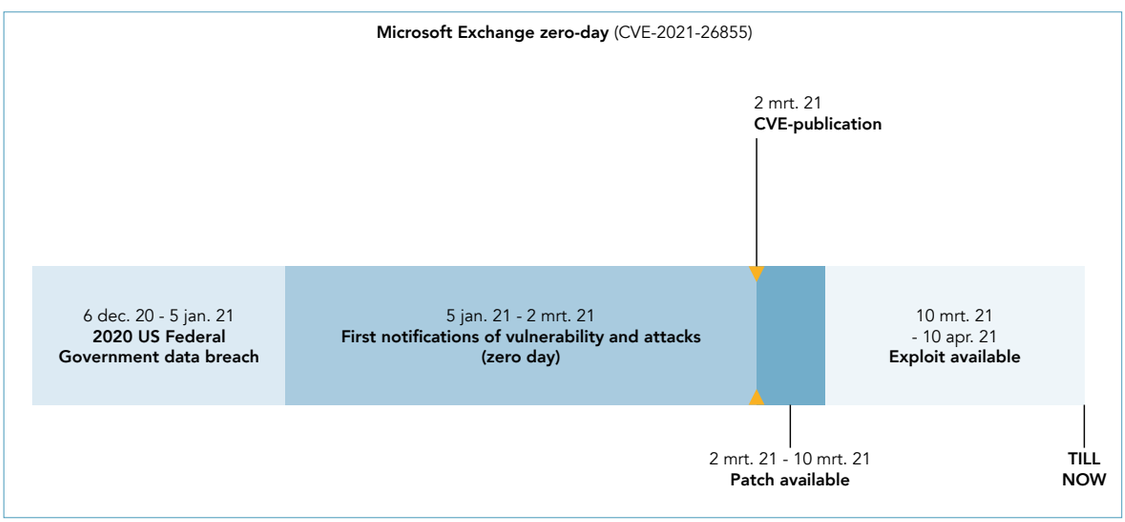


Figure 23: Microsoft Exchange.

The events surrounding the Palo Alto software vulnerability (CVE 2019-1579) were insufficiently publicly available to allow a timeline to be made.

APPENDIX E

NCSC MESSAGES (TRANSLATED FROM DUTCH BY THE DUTCH SAFETY BOARD)

NCSC Target group message (16 January 2020)
Situation: In the past, the NCSC has issued warnings of a serious vulnerability in Citrix ADC and Citrix Gateway servers, formerly known as Citrix NetScaler[1,2,3] On its website, Citrix recommends taking mitigating measures for this vulnerability. There is currently uncertainty about the effectiveness of the mitigating measures previously recommended by Citrix. This applies to all versions of Citrix ADC and Citrix Gateway servers. Since today, Citrix has confirmed on its website that these measures, are not effective at least for version 12.1 (builds for 51.16/51. 19 and 50.31)[4].

Recommendation: The NCSC emphasizes that at present, there is no sound, guaranteed reliable solution for all versions of Citrix ADC and Citrix Gateway servers. Until a patch becomes available[5], the NCSC recommends assessing the impact of shutting down the Citrix ADC and Gateway servers. Depending on the impact, the NCSC recommends considering shutting down Citrix ADC and Gateway servers.

If the impact of shutting down the Citrix ADC and Gateway servers is unacceptable, the recommendation is to monitor intensively for possible exploitation. By way of final risk-mitigating measure, you can also consider viewing the whitelists of specific IP addresses or IP blocks. Do you use version 12.1? In that case, the NCSC recommends at least upgrading the above builds of version 12.1 as quickly as possible, and then implementing the mitigating measures. This upgrade of version 12.1 also offers no guarantee of a reliable solution.

At present, the identified vulnerabilities are being actively exploited. There is a high risk of vulnerable systems being compromised. If you detect the exploitation of vulnerabilities, consider whether the situation is subject to the reporting obligation pursuant to the Security of Network and Information Systems Act (Wbni)[6].

1 https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979
2 https://www.ncsc.nl/actueel/nieuws/2020/januari/9/aanvallers-zoeken-actief-naar-kwetsbare-citrix-servers
3 https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen
4 https://support.citrix.com/article/CTX267027
5 https://www.citrix.com/blogs/2020/01/11/citrix-provides-update-on-citrix-adc-citrix-gateway-vulnerability/
6 https://wetten.overheid.nl/BWBR0041515/2019-01-01#Hoofdstuk4_Paragraaf3

News release by NCSC on www.ncsc.nl (17 January 2020)
UPDATE: Shut down Citrix systems where possible or take additional measures

News release | 17-01-2020 | 23:09

The NCSC recommends shutting down Citrix ADC and Citrix Gateway servers. Until a patch becomes available, the NCSC recommends assessing the impact of shutting down the Citrix ADC and Gateway servers.

Under all circumstances, the NCSC recommends shutting down Citrix ADC and Citrix Gateway servers if your organization failed to take the mitigating measures recommended by Citrix before Thursday 9 January 2020. If your organization is unable to continue its primary process/task after shutting down Citrix ADC and Citrix Gateway servers, carefully consider the importance of the continuity of primary processes against the risks of potential damage. If your organization decides not to shut down its Citrix ADC and Citrix Gateway servers, the NCSC urgently recommends taking additional measures (see below) and urges you to continue intensive monitoring. These recommendations are supplementary to the measures recommended by Citrix on its website.

17 January 2020, 23:09 hours: Update news release.
17 January 2020, 10:08 hours: Update news release.
16 January 2020, 17:22 hours: Publication date and time of first version news release.

Additional mitigating measures
If it is not possible for you to upgrade your Citrix server and you still wish to maintain access to your environment via the Internet, the NCSC recommends implementing the following additional measures:

IP-whitelisting
Only authorizing links to known IP addresses is a very effective countermeasure for external attackers. However, it demands intensive management efforts, that grow proportionally to the size of your organization.

Install a web application firewall
By installing a web application firewall behind the Citrix server, it is possible to implement filter lines that can make it more difficult for malicious actors to carry out an attack.

Apply client certificates
By making authentication with client certificates compulsory, an unauthorized malicious user is unable to carry out an attack. Creating and distributing these certificates is however a complex task.

Alter gateway
By altering the gateway via which the service is available, the risk is reduced that an attacker will find your server following broad Internet scans. This means that the new gateway must be selected by all end users. This requires communication and can impose greater burdens on the helpdesk. Please note that altering the gateway only offers protection against discovery via broad scans and does not offer protection against an attack if your server is discovered. In addition, a number of scans have probably already been carried out, and there is a risk that your server has already been identified by malicious actors.

Visiting address
Lange Voorhout 9
2514 EA The Hague
The Netherlands
T +31 (0)70 333 70 00
F +31 (0)70 333 70 77

Postal address
PO Box 95404
2509 CK The Hague
The Netherlands

www.safetyboard.nl