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.