REACTIES OP CONCEPTRAPPORT 'KWETSBAAR DOOR SOFTWARE - LESSEN NAAR AANLEIDING VAN BEVEILIGINGSLEKKEN DOOR SOFTWARE VAN CITRIX'

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
1	Citrix	1.2	This investigation was launched in response to the Citrix security breach… This investigation was launched in response to the Citrix security vulnerability...	Factually inaccurate to refer to this as a Citrix "breach".	Partially	The term Citrix security breach implicates an attack on Citrix' company network. This is an inaccurate translation of the Dutch report.
2	Citrix	2.1.2	Safety and security were less relevant and did not initially play a central role in the development and production. Safety and security were less relevant and did not initially play a central role in the development and production. [Include citation].	Citrix does not recognize itself in this comment and has in fact always had safety and security at the heart of its software development cycle. If this comment is based on an observation of the market as a whole, it would benefit from a citation.	No	This sentence concerns a general comment on the relevance put on safety and security in historical perspective and does not refer to a Citrix product or other manufacturers' products.
3	Citrix	2.2	A hacker is someone who breaks into a computer system with positive intentions. A hacker is someone who breaks into a computer system [delete remainder of sentence].	Factually inaccurate. Hackers can have positive or negative intentions.	Yes	Incorrect footnote.
4	Citrix	2.4	One of the motives of attackers to abuse the vulnerability in Citrix software to penetrate systems (unnoticed) is to obtain high-quality technology developed by Dutch companies and knowledge institutions. One of the motives of attackers to abuse vulnerabilities to penetrate systems (unnoticed) is to obtain high-quality technology developed by Dutch companies and knowledge institutions.	This can be a motivation of attackers generally, not just as it relates to the Citrix vulnerability.	Yes	The motives for hackers to attack systems do not just apply to this incident. Therefore, adopted Citrix's suggestion to formulate more broadly.
5	Citrix	3.1.1	5 until 17 December 2019 - Manufacturer examines vulnerability. 5 until 17 December 2019 - Manufacturer examines vulnerability and develops mitigating measure.	Factually inaccurate. During this time the vulnerability was examined and a mitigating measure was developed.	Partially	It is sufficiently clear from the following entry on the timeline that the manufacturer worked on a mitigating measure in the time before publication. For completeness, we have included that the manufacturer examined the vulnerability and worked on a mitigating measure meanwhile.
6	Citrix	3.1.1	From 17 January 2020 Manufacturer warns a part of its customers. Manufacturer contacted customers that could be identified and for whom contact information was available.	This timeline entry suggests that Citrix chose to warn only specific customers, which is factually inaccurate.	No	It is actually correct that Citrix only warned a part of its customers. Citrix is right to note that it contacted customers whose contact information was available. But this is made sufficiently clear in the accompanying text and it is also a general finding that manufacturers do not have contact information of their customers on record at all times.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
7	Citrix	3.1.1	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. On the basis of this 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. [delete beginning of section] The manufacturer also 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.	Citrix's findings regarding the origins of the vulnerability did not drive decision-making. Rather, Citrix's response was driven by the risk of a public exploit and the need to protect customers.	Partially	It is not disputed that the vulnerability had been in the foundation of the software for more than 10 years, but the connection with the risk analysis made is questioned. The information concerning the presence of the vulnerability in the foundation has therefore been moved and disconnected from the risk analysis made by Citrix.
8	Citrix	3.1.1	In response, Citrix decided to deviate from the standard approach for dealing with vulnerabilities. In response, and based upon the risk that a POC might be in circulation, Citrix decided to treat this as a zero-day vulnerability.	This sentences suggests that Citrix's response strategy was not "standard" and was in response to the vulnerability's presence in a large portion of the install base. This is factually inaccurate; Citrix's response was an accepted approach for zero-day vulnerabilities and was in response to the potential for the exploit to become public.	Yes	The text proposal concerns a clarification and has been adopted.
9	Citrix	3.1.1	Instead, the manufacturer developed mitigating measures as a temporary solution in advance of the definitive patches. Instead, the manufacturer developed mitigating measures in advance of the definitive patches, as this was faster achieved and, considering the risk, a safer solution. Even though a mitigation does not take away the cause of the vulnerability, it does take away the effect and therefore the risk. For these reasons it was considered as effective as a patch.	Referring to the mitigation as 'temporary solution' suggests it may have been ineffective, whereas the mitigation was indeed very effective and - more importantly - able to be developed and published much faster than a patch.	Partially	Citrix's reasoning is correct. Text proposal adopted in different wording.
10	Citrix	3.1.1	They published these mitigating measures on 16 December 2019, eleven days after having received the first report from their sources. They published these mitigating measures on 17 December 2019, twelve days after having received the first report from their sources.	Incorrect date. While the webpage creation date was 16 December 2019, the mitigation measure was not published until the 17th.	Yes	Incorrect date in the report. This sentence was removed because the date of publication of the mitigating measures is repeated in the next paragraph.
11	Citrix	3.1.1	One day later, on 17 December, the manufacturer disclosed the vulnerabilities and the mitigating measures by publishing a security bulletin on their website. On 17 December, the manufacturer disclosed the vulnerabilities and the mitigating measures by publishing a security bulletin on their website.	Incorrect date; the CVE and mitigating measures were published on the same date - 17 December 2019.	Yes	This concerns a clarification. In addition, the word "vulnerabilities" was replaced by "information on the vulnerability" to reflect that Citrix did not publish the vulnerability itself.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
12	Citrix	3.1.1	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. In publishing the mitigation steps, the manufacturer took care to include the minimal information necessary for the mitigation to be implemented. While it nonetheless became possible for attackers to derive where in the Citrix software the vulnerability was located and what type of vulnerability it was, this known industry 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 customers from a zero-day situation.	Providing more factual information on the need for the mitigation and Citrix's work to provide the safest mitigation it could.	Partially	This concerns a clarification of Citrix's risk assessment. The essentials of Citrix's efforts are added to the text.
13	Citrix	3.1.1	Citrix, Support article Mitigation Steps for CVE-2019-19781, 16 December 2019 (latest update 15 October 2020). Citrix, Support article Mitigation Steps for CVE-2019-19781, 16 December 2019 (latest update 1 September 2021).	Incorrect "last update" date.	No	Web pages are updated continuously. The version that the Safety Board has on file has a last update date of 17 December 2019). The date of October 2020 was an incorrect reference to the current version of the CVE at the moment of writing.
14	Citrix	3.1.1	On 10 January 2020, via the platform GitHub, a group of security researchers published the code for exploiting the vulnerability in the Citrix software. On 10 January 2020, via the platform GitHub and without consulting the manufacturer, a group of security researchers published the code for exploiting the vulnerability in the Citrix software.	Citrix was unaware of the exploit and GitHub's publication took place outside of Citrix's view or control.	Yes	Factual addition, in slightly different wording.
15	Citrix	3.1.1	On 17 January 2020, Citrix corrected the published notice via a bulletin update and the CISO 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 client had implemented all steps necessary for ensuring the correct functioning of the mitigation. 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 client had implemented all steps necessary for ensuring the correct functioning of the mitigation.	Factual inaccuracy. Citrix's CISO reported about the mitigation steps in a blog post and on Twitter, but Citrix's EVP of Engineering reported in a TV interview.	Yes	This concerns a factual inaccuracy.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
16	Citrix	3.1.1	In addition to placing the alert on the website and in social media reports, the manufacturer attempted to reach as many of its clients as possible. In the period between 17 and 24 January, Citrix sent out more than 124,00 emails to approximately 36,000 different organizations. During this same period, the manufacturer started to establish a database with contact details for its clients, so that in the event of future vulnerabilities it would be possible to trace products and warn clients more effectively. In addition to placing the alert on the website and in social media reports, which is the common response to a vulnerability, the manufacturer also proactively attempted to reach as many of its clients as possible. As Citrix only had contact details for a subset of its installed base, Citrix initiated a vast campaign to obtain as many contact details of customers as possible. This resulted in Citrix sending out more than 124,00 emails to approximately 36,000 different organizations, in the period between 17 and 24 January. During this same period, the manufacturer further built out a database with contact details for its clients (which it had already initiated before the vulnerability), and has since made it a priority to proactively encourage customers to keep their security contact details updated so that in the event of future vulnerabilities it would be possible to trace products and warn clients more effectively.	The representation of the course of events and effort taken by Citrix is incomplete.	No	The original text adequately reflects the steps taken by the manufacturer.
17	Citrix	3.1.1	In the Dutch version, there is an additional sentence: “The manufacturer on 22 January published at the request of the NCSC in the Netherlands a forensic tool to determine whether a vulnerable server was accessed.” (”De fabrikant bracht op verzoek van het NCSC in Nederland op 22 januari een forensische tool uit om vast te kunnen stellen of een kwetsbare server was binnengedrongen”). The manufacturer already 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.	The development of this tool was not a common industry response to vulnerabilities and in fact highlights Citrix’s commitment towards remediating the vulnerability. The tool also was not readily available and was built pursuant to the NCSC request, and was published within a very short time frame with priority. The current reflection of the course of events creates an incomplete picture.	Yes	This concerns a clarification and fixes a unintentionel discrepancy between the English and Dutch version of the report.
18	Citrix	3.1.1	In the Dutch version, the footnote starts with “Depending on the license and the support contract, there could have been costs for the client.” Remove sentence.	This is factually inaccurate. In regards to this vulnerability, cost was not a factor as the mitigation and patches were made generally available.	Yes	Dutch footnote translated and added to English version. Clarification that this footnote does not refer to costs of mitigating and patching, but costs of upgrading.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
19	Citrix	3.1.1	From the start of January 2020, the manufacturer also started to scan the internet for IP addresses of vulnerable servers. If the manufacturer was able to link a located IP address to a client, they attempted to actively approach the client in question. Citrix also shared the IP addresses it had identified in this way, with the national CERTs, including the Dutch NCSC. From the start of January 2020, the manufacturer also started to scan the internet for IP addresses of vulnerable servers. If the manufacturer was able to link a located IP address to a client, they attempted to actively approach the client 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.	The NCSC offered to assist in contacting Dutch entities that had not applied the mitigation or patch so they could better protect themselves.	Yes	Factual addition.
20	Citrix	3.1.2	Some of the organizations that took measures turn out to be compromised. Some of the organizations that took measures following publication of the exploit had been compromised prior to the full application of the mitigation.	Factually inaccurate. Citrix is not aware of any compromises within organizations with mitigations or patches applied. The only way this can happen is if their systems were already compromised before they applied the patch or mitigations.	Partially	There were signals that organizations that patched were compromised. It cannot be established with certainty that the compromise took place before or after application of the mitigation.
21	Citrix	3.2.1	The consequence was that at organizations that had in some way used this Citrix software in their network, unauthorized persons were able to move throughout the entire network, and could alter the settings in such a way that they themselves were able to place software code on the network, and could then execute that code remotely. The consequence was that at organizations that had in some way used this Citrix software in their network, unauthorized persons could have been able to move throughout the entire network, and could alter the settings in such a way that they themselves were able to place software code on the network, and could then execute that code remotely.	Factually inaccurate to suggest this happened at all organizations that used Citrix software.	No	The text merely states that it was a possibility at all organizations that used Citrix, not that it happened at all organizations.
22	Citrix	3.2.1	Using the vulnerability, unauthorized users (including attackers) were able to gain access to all components of the Citrix server. Using the vulnerability, unauthorized users (including attackers) could have been able to gain access to all components of the Citrix server.	Factually inaccurate to suggest this happened at all organizations that used Citrix software.	Yes	This relates to a nuance.
23	Citrix	3.2.1	References to the Citrix “server” or “webserver”. E.g. “to all components of Citrix server”; “managing the Citrix server”; “all parts of the webserver.” Replace “Citrix server” and “web server” with “Citrix appliance”.	NetScaler is a network appliance; which is different from a web server.	Yes	Factual inaccuracy.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
24	Citrix	3.2.1	End of page after "However, path traversal on its own was not sufficient to read out files." However, path traversal on its own was not sufficient to read out files. Citrix was not aware of any such unauthorized access or attack prior to December 2019.	To Citrix's knowledge, there had never been an exploit of this issue prior to December 2019.	No	Path traversal/directory traversal is a commonly known technique used by attackers. See: https://owasp.org/www-community/attacks/Path_Traversal
25	Citrix	3.2.2	As a consequence, the product became a web server with additional functions such as… As a consequence, the product evolved to include additional network functions such as…	NetScaler is a network appliance, which is different from a web server.	Yes	This is a factual inaccuracy.
26	Citrix	3.2.2	Software that operates in a dynamic environment of this kind calls for adaptive risk management from the manufacturer. Software that operates in a dynamic environment of this kind calls for adaptive risk management from the manufacturer. In this case, Citrix employs a Secure Development Lifecyle program, which is a key aspect of its product development framework and provides a holistic approach to product security management.	This representation suggests that Citrix does not have adaptive risk management. To the contrary, Citrix employs its robust SDL program. The SDL begins during product planning and works its way through the process of code design, development and release. This includes comprehensive product security release criteria; extensive code reviews (manual, static and variant analysis); supply chain security testing; vulnerability scanning; product penetration testing (internal Red Team and third-party penetration testing); and extensive product security training of Citrix engineers, as well as tracking/management reporting of training completion.	Partially	Addition that Citrix employs a secure development lifecycle programme. The Dutch Safety Board has not assessed this programme.
27	Citrix	3.2.4	At that point, 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. 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). Delete next sentence.	The assignment to one team was due to the fact that validation of these types of security fixes require deep knowledge of the product and there are a limited number of engineers in any development organization who have the requisite knowledge.	Partially	Explanation why the manufacturer only had one team available is added. The next sentence is not deleted, as this is not factually inaccurate and explains why different versions of patches could not be developed in parallel.
28	Citrix	3.2.4	Because of the resultant long lead time for manufacturing the patches, the manufacturer decided to take advice steps to mitigate the vulnerability as a temporary measure. Because of the time it would take to develop the patches, the manufacturer decided to, as a priority, work on a mitigation measure as this would be much faster achieved and, considering the zero-day risk, would be a more effective measure. Even though a mitigating measure does not completely remedy the cause of the vulnerability, it does remedy the effect and was therefore considered more effective, considering the speed of deployment.	Referring to the mitigation as 'temporary solution' suggests it may have been ineffective, whereas the mitigation was indeed very effective and - more importantly - able to be developed and published much faster than a patch.	Partially	The essentials of Citrix's efforts are added to the text.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
29	Citrix	3.2.5	The mitigation steps advised by Citrix were formulated in such a way that it was clear how the vulnerability could be exploited. The mitigation steps advised by Citrix were formulated with care to include the minimal information necessary for the mitigation to be implemented. While it was possible that the vulnerability could be exploited with this information, this known industry 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 customers from a zero-day situation.	Providing more factual information on the need for the mitigation and Citrix's work to provide the safest mitigation it could.	Partially	This is a clarification. The suggestion has been adopted, but presented more factually.
30	Citrix	3.2.6	In addition to publishing the vulnerability, the manufacturer decided to warn as many of its customers as possible, directly. In addition to publishing the mitigation, the manufacturer decided to warn as many of its customers as possible, directly.	Factual inaccuracy; Citrix did not publish the vulnerability.	Yes	Factual inaccuracy.
31	Citrix	3.2.6	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%). Contact was challenging for the manufacturer as only a subset of the manufacturer's installed base had signed up to receive security alerts. Citrix initiated a vast campaign to obtain as many contact details of customers as possible.	The representation of the course of events and effort taken by Citrix is incomplete.	Partially	Factual addition, the other facts were already in the text.
32	Citrix	3.3.1	The search for vulnerabilities. The search for vulnerabilities: Fortinet, Palo Alto Networks, and Pulse Secure.	This section is unclear and thus suggesting more specificity in the heading.	No	The heading of section 3.3 'Course of events of other illustrative occurences' already indicates that this entire section concerns other occurences.
33	Citrix	4.1.1	Dealing with the underlying cause in the foundation of the product (programming language, components, architecture) requires the complete rebuilding of the product. Dealing with the underlying cause in the foundation of the product (programming language, components, architecture) can require the complete rebuilding of the product.	The statement is too firm as currently worded. A rebuild can be required, but is not always required in order to address issues in the foundation of a product.	Yes	This relates to a nuance.
34	Citrix	4.1.1	For manufacturers, it is unattractive to protect software development against vulnerabilities: it makes the software slow, and during the programming process, the programmers receive so many (sometimes erroneous) error messages that they switch off the security system. According to one researcher, for manufacturers, it is unattractive to protect software development against vulnerabilities: it makes the software slow, and during the programming process, the programmers receive so many (sometimes erroneous) error messages that they switch off the security system.	Citrix does not agree with this statement and it is not factually correct as to Citrix. To the contrary, Citrix is committed to delivering secure software to its customers.	Partially	Citrix is correct in its statement that this is based on a scientific publication. However, this finding does not only relate to the Citrix specific case, it is a general statement that reflects the current state of affairs. Chapter 4 makes general statements about how multiple parties operate based on interviews, literature, and discussions with experts, among other things. These findings are not exclusively applicable to Citrix.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
35	Citrix	4.1.2	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, they consider end-to-end testing to be too time consuming, because older products often consist of large volumes of source codes. 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 codes. Another consideration is that not all vulnerabilities can always be found.	Most scanning tools do not find vulnerabilities in older programming languages, and some vulnerabilities are inherently more difficult to find using scanning tools.	Partially	"can" and "very" are appropriate, given the general nature of the text. The last sentence "Another consideration […]" was not adopted because this is sufficiently made clear in the remainder of the chapter.
36	Citrix	4.1.2	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). Attackers sometimes need just a single leak in order to gain full access to a system. Also, attackers often consist of determined adversaries, meaning that if they are determined to access a system, they will continue to try. This reveals an imbalance between attacker and defender (manufacturer).	Adversaries are often also determined to find vulnerabilities, which adds to the imbalance.	No	The fact that attackers are determined does not take away from the fact that it only takes one vulnerability to gain access. Even an attacker who is not determined can come across a leak and take advantage of it. This illustrates the extent of the imbalance.
37	Citrix	4.1.4	Manufacturers usually have agreements stipulate that they are not liable for the consequences of any vulnerabilities in software. Manufacturers usually have agreements stipulate that they have limited liability for the consequences of any vulnerabilities in software.	Factual inaccuracy. Most enterprise software agreements do not exclude liability for software defects as suggested in the draft report.	Yes	Factual inaccuracy.
38	Citrix	4.1.4	In addition, in the condition 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. In addition, in the condition they impose on the purchase and use of their software, manufacturers prohibit users from reverse engineering the products.	Factual inaccuracy. Contractual limits are typically on reverse engineering to protect intellectual property.	No	"Opening up" the product refers to reverse engineering.
39	Citrix	4.1.4	At the same time, these products have a long history, as they are built on existing components. This makes 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. 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 could require them to rebuild software that is the result of decades of development.	Added nuance as the statement is worded too definitively.	Yes	This relates to a nuance.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
40	Citrix	4.2.2	As discussed in 4.1, at present there are limited possibilities for forcing manufacturers to safeguard cybersecurity in their products. This places an additional burden on customers to test the products for safety and security, when purchasing software. As discussed in 4.1, at present there are limited possibilities for ensuring that manufacturers uniformly and across the board safeguard cybersecurity in their products. This emphasizes the necessity for customers to test the products for safety and security, when purchasing software.	The way the statement is worded suggests that software is by definition unsafe, that manufacturers have no incentive to produce safe and secure software and that vulnerabilities have no cost, damage or consequences for manufacturers. Citrix disagrees with that suggestion.	No	These sentences discuss the general limited legal possibilities to obligate manufacturers to safeguard cybersecurity. This does not mean that all manufacturers do not ensure the cybersecurity of their products, but customers cannot rely on manufacturers for product safety and security and must therefore be able to assess this for themselves.
41	Citrix	4.2.3	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. It is impossible for both end users as well as manufacturers to fully prevent or mitigate these risks, but it is essential that they first have a clear picture of the risks in order to make any assessment.	This is a risk to the market, not just to end users.	No	As this section focuses on the risks for end users when using software, mentioning risks for manufacturers when developing software does not fit in this section. Section 4.1 already discusses risks for manufacturers and how these are dealt with.
42	Citrix	4.2.3	As a rule, software is not a static product but continues to develop following the purchase moment. 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 and evolve.	Updated to account for the fact that the cyber and risk landscape consists of more than just vulnerabilities, and is equally subject to continuous development and evolution.	Yes	Relevant addition to the current paragraph.
43	Citrix	4.4.2	One of the software manufacturers we spoke to, for example, learned lessons from the occurrence, and took measures. However, it did not share those lessons with other manufacturers, parties involved or the public. One of the software manufacturers we spoke to, for example, learned lessons from the occurrence, and took measures. However, it did not share those lessons with other manufacturers, parties involved or the public. Citrix, on the other hand, shared a number of lessons and enhancements on its Trust Center.	Citrix has added a comprehensive discussion of its vulnerability management and disclosure processes to its Trust Center. https://www.citrix.com/about/trust-center/	Partially	Publishing lessons on one's own website is an important first step, but learning as a system of parties involves more than just this.
44	Citrix	5	This research 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. This research 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 third-party software products.	Clarification [backed by chart on 116].	Yes	Clarification.
45	Citrix	5.1	The number of vulnerabilities in software is growing, as are the consequences of attacks. The number of detected vulnerabilities in software is growing, as are the consequences of attacks.	Many have existed for a long time, but hackers are seeking out and exploiting issues increasingly.	Yes	Nuance added, as we can only reflect upon detected vulnerabilities.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
46	Citrix	5.3	Entire section/paragraph.	It appears that certain important observations in section 4.3 of the report are not (fully) reflected in the conclusions of this section 5.3, such as that it is crucial that in the context of vulnerabilities and incidents information is shared by and between stakeholders in the market, or that legal impediments are perceived to stand in the way of information sharing.	Yes	Analysis and conclusions clarified by naming the relevance of sharing information on victims in analysis. To match the conclusion, we have aligned this in the main text as well.
47	Ivanti	Abreviations and Definitions	(part of Ivanti since December 2001) - should be changed to "acquired by Ivanti in December 2020"	Ivanti acquired Pulse in December 2020, not 2001. The change accurately reflects the software/company ownership.	Yes	Factual inaccuracy.
48	Fortinet	3.3.1	Fortinet dealt with its vulnerability after three months and two months later notified its clients.	Time until first fix was 6 weeks with the release of Release of 5.6.8 (28th Jan 2019). The CVE was specified in releases notes at the time. So dealt with and notified timing should be 6 weeks not 3 +2 months. Advanced Notification Bulletin was published January 2019 The Public Advisory gets published after the final required fix which was 23 May.	Yes	When putting together the timeline for this vulnerability, the timeline for a set of multiple CVE's was mistakenly used. The dates have been changed accordingly.
49	Fortinet	3.3.1	500.000 login credentials from Fortinet VPN servers.	This was somewhat exaggerated as there was significant duplication. As oppposed to 81K devices / 500,000 credentials, this was closer to 24K devices and 140,000 credentials; a large number of which were no longer vulnerable as the administrators had taken action to upgrade or the devices had been taken offline.	Yes	Addition added for completeness.
50	Fortinet	A.3	A number of vendors (Fortinet referenced in Footnote) did not respond to requests to answer questions.	Fortinet PSIRT has no record of any request for information from the @onderzoeksraad.nl domain. If you had reached out via our PSIRT process or via Support we would have responded accordingly as we are here. On request onderzoeksraad.nl responded that a notification letter was sent to headquarters by mail, and also by e-mail to FortinetFederal@fortinet.com. I am not able to find any record of a letter delivery and the email alias is a US sales alias not one for communication of security incidents. The correct contact is our Product Security and Incident Response Team (PSIRT) which is documented in our PSIRT Policy https://www.fortiguard.com/psirt_policy and via the industry standard security.txt format https://www.fortinet.com/.well-known/security.txt Fortinet request that this is removed from the footnote as we are happy to support CERT organizations in all communications as needed - assuming the request is correctly routed as it ultimately was in this case.	No	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 Fortinet were unsuccesful in the investigation phase of this investigation.
51	Fortinet	Appendix D	Fortinet diagram.	Similar timeline change required as described in 3.3.1. Patch was available from, release of 5.6.8 (28th Jan 2019).	Yes	Changed to correct timeline for mentioned CVE. See comment 48.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
52	Fortinet	Additional General Comment		As part of our social responsibility program, Fortinet works in collaboration with regional CERT teams and NCSC organzations. Fortinet would be happy to strike up an ongoing relationship with the team in the Netherlands.	No	This is a comment which does not refer to a specific section of the report.
53	F5	Abbreviations and Definitions	BIG IP	Please consistently refer to this product as BIG-IP, this is the approved reference. The document also uses 'Big-IP' in places, please modify these references as well.	Yes	Changed to correct product name.
54	F5	3.3.1	"User interface" should be "management interface".	F5 does not use the phrase "user interface" in any documentation and the phrase implies an interface accessed via the production network or Internet. The vulnerability, however, was present in the management interface which is intended to be accessed via secure, protected networks by administrative users only.	Yes	Changed to correct term.
55	F5	3.3.1	"User interface" should be "management interface".	See above.	Yes	Changed to correct term.
56	F5	3.3.1	"Anyone could implement any random code" could more properly be written "attackers without legitimate credentials could execute arbitrary malicious code".	This more closely aligns with industry standard language and our Security Advisories.	Yes	Wording changed to align with standard language in industry.
57	F5	A.3	F5 would appreciate your consideration of the note "F5 did not respond" now that we have provided a full response.	We acknowledge the difficulty in establishing contact and reiterate that you are always welcome to reach out to f5sirt@f5.com for any security related concerns (see also https://www.f5.com/services/support/report-a-vulnerability).	Yes	Addition: F5 responded to the questionnaire at the review stage of the investigation. See also comment 50.
58	Ministerie J&V	Lijst van afkortingen en begrippen	OKTT…taak.	De uitleg van de afkorting is onvolledig. Een OKTT is een organisatie die objectief tot taak heeft om organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot netwerk- en informatiesystemen.	Ja	Onvolledige omschrijving in huidige tekst.
59	Ministerie J&V	1.1	op…zetten.	Het NCSC gaf dit advies mede op basis van inlichtingeninformatie.	Nee	Later in het rapport wordt verduidelijkt dat het NCSC dit advies gaf op basis van inlichtingeninformatie.
60	Ministerie J&V	1.1	wijze waarop…	suggestie om toe te voegen…en de mate waarin…	Ja	Verduidelijking.
61	Ministerie J&V	2.2	…coordinated of responsible disclosure…	Deze term is onvolledig. Het betreft Coordinated Vulnerability Disclosure (CVD).	Ja	Er wordt hier coordinated vulnerability disclosure bedoeld.
62	Ministerie J&V	2.5	In bepaalde…waterschappen.	Een groot deel van de hier als CERTs genoemde organisaties zijn opgericht door andere organisaties, en dus niet door de rijksoverheid. Ze zijn daarná krachtens artikel 3, lid 2, Wbni aangewezen als computercrisisteam, zodat zij daarmee in ruimere zin informatie ten behoeve van hun doelgroep van het NCSC kunnen ontvangen, maar bestaan dus al vóór die aanwijzing. De tekst suggereert anderszins.	Ja	Verduidelijking.
63	Ministerie J&V	2.5	Daarnaast bestaan.. (OKTT's).	Er ontbreekt in deze tekst nog welke taak zij objectief kenbaar hebben: zie artikel 3, lid 2, aanhef en onderdeel a, Wbni (informeren van… over…). Voor de als OKTT genoemde partijen geldt overigens ook dat zij vaak door andere organisaties dan de rijksoverheid zijn opgericht en daarna krachtens artikel 3, lid 2, Wbni als zodanig worden aangewezen.	Ja	Dit betreft een onvolledige zin, deze is aangevuld met de taak van OKTT's.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
64	Ministerie J&V	2.5	Brainport Eindhoven.	De naam van deze organisatie is Stichting Cyber Weerbaarheidscentrum Brainport.	Ja	Stichting Cyber Weerbaarheidscentrum Brainport is de officiële naam van de OKTT.
65	Ministerie J&V	2.5	Het beleid…zijn benoemd.	Het is een Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (zie NCSA 2018), niet alleen van de schakelorganisaties die krachtens artikel 3, lid 2, Wbni, als computercrisisteam of OKTT zijn aangewezen. Tot het LDS behoren ook andere samenwerkingsverbanden, die bovendien vaak niet door de rijksoverheid zijn benoemd maar initiatieven zijn vanuit bv. het bedrijfsleven. Computercrisisteams en OKTTs worden krachtens de Wbni niet benoemd, maar aangewezen. Computercrisisteams worden aangewezen via een ministeriële regeling. Besluit tot aanmerken als OKTT is een besluit van de minister (al dan niet gemandateerd aan Directeur NCSC en Directeur Cybersecurity en Statelijke Dreigingen van de NCTV).	Ja	Verduidelijking van partijen die deel uitmaken van het Landelijk Dekkend Stelsel en de manier waarop deze worden aangewezen.
66	Ministerie J&V	2.5	DIVD...CSIRT.	De term CSIRT wordt (in elk geval) in de Wbni alleen gebruikt voor de door Nederland als zodanig aangewezen instanties als bedoeld in artikel 9 NIB-richtlijn (NCSC als CSIRT voor aed's, bij EZK belegde CSIRT voor digitale diensten).	Nee	De term CSIRT wordt ook buiten de context van de Wbni gebruikt. Zie bijvoorbeeld deze handleiding van NCSC voor organisaties om zelf een collectieve CSIRT op te richten in aanvulling op het CSIRT per organisatie. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/start-csirt.
67	Ministerie J&V	2.6	Voor het...Klimaat (EZK).	MinEZK is verantwoordelijk voor het informeren van niet-vitale bedrijfsleven, maar niet alle niet-vitale partijen (bv. gemeenten). Bovendien loopt de informatiestroom niet (alleen) via het DTC. Daarnaast mist hier de vermelding dat EZK (los van het DTC) krachtens de Wbni CSIRT is voor enkele categorieën digitaledienstverleners. Los daarvan is EZK ook verantwoordelijk voor toezicht (Wbni, Tcw) en beleid als het gaat om onder EZK vallende vitale sectoren (telecom, etc.).	Ja	Verduidelijking en aanvulling.
68	Ministerie J&V	2.6	De ministeries...digitale domein.	VWS, OCW, I&W en FIN ontbreken in deze opsomming en hebben ook verantwoordelijkheid voor de digitale veiligheid van de onder hun vallende sectoren (toezicht als bedoeld in met name Wbni, beleidsverantwoordelijkheid).	Ja	Aanvulling.
69	Ministerie J&V	2.6	Het NCSC….	Het NCSC was onderdeel van de NCTV binnen één directie, te weten destijds 'Directie Cyber Security'. Op 1 januari 2019 is het NCSC een zelfstandige uitvoerende dienst geworden van MinJenV met de NCTV als opdrachtgever.	Ja	Verduidelijking, in de huidige tekst staat dat het NCSC onder de NCTV viel, maar het was onderdeel van dezelfde organisatie.
70	Ministerie J&V	2.6	Het NCTV	= de NCTV	Ja	Taalfout.
71	Ministerie J&V	2.6	opdrachtgever. …de	Er ontbreekt hier een nadere duiding van de onderscheidenlijke taken van NCTV en NCSC binnen het ministerie. Tekstvoorstel: De NCTV coördineert en ontwikkelt primair het beleid op het gebied van cybersecurity. NCSC is de uitvoeringsorganisatie ten aanzien van de wettelijke taken van de minister van JenV op dat gebied en opereert binnen de daarvoor gestelde wettelijke en beleidskaders.	Ja	Verduidelijking.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
72	Ministerie J&V	2.6	De wettelijke taak...(Wbni).	De Wbni regelt de (hierna genoemde) taken voor de minister van JenV, niet het NCSC. Voor het NCSC geldt het dat die taken in de praktijk namens de minister uitvoert.	Ja	In de Wbni zijn deze taken gegeven aan de minister, dit is verduidelijkt in de tekst.
73	Ministerie J&V	2.6	Op grond...op zijn beurt...netwerk- en informatiesystemen.	De huidige tekst wekt mogelijk de onjuiste indruk dat het NCSC zijn taken ten behoeve van Rijk en vitaal (artikel 3, lid 1, Wbni) alleen uitvoert naar aanleiding van wettelijk verplichte meldingen van incidenten (vgl. artikel 10, lid 1, Wbni). Die taken (informeren, adviseren) worden echter én in hoofdzaak proactief dan wel naar aanleiding van onverplichte meldingen van aanbieders verricht; genoemde bijstand betreft dus ook vaak dreigingen en incidenten, anders dan die bedoeld in artikel 10, lid 1, Wbni. Daarnaast: de meldplicht in artikel 10 Wbni geldt inderdaad voor (de krachtens artikel 2 Bbni aangewezen) aanbieders van essentiële diensten (die overigens ook vitale aanbieder zijn; zie artikel 1 Wbni), maar niet voor ook alle andere vitale aanbieders (nl. alleen de krachtens artikel 3 Bbni aangewezen vitale aanbieders).	Ja	Verduidelijking.
74	Ministerie J&V	2.6	...en de onderdelen van het rijk.	de onderdelen van het rijk = rijksoverheid.	Ja	Rijksoverheid is een meer gangbare term voor de onderdelen van het Rijk.
75	Ministerie J&V	2.6	ten...verstaan	Niet alle aanbieders in deze sectoren zijn vitaal, vitale aanbieders worden aangewezen. Tekstvoorstel: “Ten tijde van het voorval met de Citrix-software werden daaronder de binnen de volgende vitale processen (als ‘vitale aanbieder’) aangewezen aanbieders daaronder verstaan … ” Ook is (en was toen) de opsomming van vitale sectoren c.q. processen niet compleet. Overzichten zijn hiervan in Kamerbrieven vermeld.	Deels	Verduidelijking dat niet alle aanbieders binnen een sector zijn aangewezen als vitale aanbieder. De lijst van vitale sectoren is overgenomen uit Besluit beveiliging netwerk- en informatiesystemen, versie januari 2019.
76	Ministerie J&V	2.6	Daarbij...AIVD	Het NCSC werkt binnen de wettelijke kaders samen met de AIVD. AIVD heeft eigenstandige taak o.b.v. WIV, geen ondersteunende rol t.a.v. het NCSC.	Ja	Verduidelijking, de AIVD heeft geen wettelijke ondersteunende rol ten aanzien van het NCSC, maar werkt samen met het NCSC.
77	Ministerie J&V	2.6	in hun netwerk- en informatiesystemen	NCSC heeft ten opzichte van Rijk en vitaal alleen tot taak te informeren en adviseren over dreigingen en incidenten, voor zover die relevant zijn voor de netwerk- en informatiesystemen van Rijk en vitaal.	Ja	Het NCSC informeert en adviseert Rijk en vitaal over dreigingen in de systemen van deze doelgroep.
78	Ministerie J&V	3.1	In...Nederland.	12 januari moet 11 januari zijn.	Ja	Feitelijke aanpassing die in de tekst is overgenomen.
79	Ministerie J&V	3.1	Diezelfde...software.	16 januari moet 15 januari zijn.	Ja	Feitelijke aanpassing die in de tekst is overgenomen. Verder “Tientallen gehackte servers” gewijzigd in grote piek in aanvallen”.
80	Ministerie J&V	3.1	Op...werken.	Een aanvulling: In het eerste opschalingsteam van het NCSC is op 13 januari besproken dat de mitigerende maatregelen van Citrix mogelijk niet afdoende zijn. Het NCSC ontving vanaf 13 januari verschillende berichten, o.a. over de mitigerende maatregelen, zorgen van partners, gevallen van (mogelijk) misbruik. Dat leidde tot aanpassing van het advies op 16 januari en het aandringen bij de fabrikant om te komen tot een tool om vast te kunnen stellen of een kwetbare server was binnengedrongen.	Nee	Paragraaf 3.1.1 focust op de vondst van de kwetsbaarheid en de reactie van de fabrikant. De gebeurtenissen in de voorgestelde aanvulling worden al beschreven in paragraaf 3.1.2, die focust op de incidentbestrijding in Nederland.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
81	Ministerie J&V	3.1	NCSC…software.	In het schema staat dat het NCSC vanaf 9 januari informatie deelt met doelgroepen. Op 9 januari is inderdaad informatie gedeeld met doelgroeporganisaties. Echter, het NCSC deelt beveiligingsadviezen actief met doelgroeporganisaties en heeft op 24 december bij de opwaardering van het advies ook actief (via doelgroepbericht en telefonisch) contact gezocht met doelgroeporganisaties. Voorstel om dus bij het tweede blokje toe te voegen dat het NCSC waarschuwt én doelgroepen informeert.	Ja	Feitelijke aanvulling die in de tekst is overgenomen.
82	Ministerie J&V	3.1.1	Opschaling…AIVD.	Op 17 januari is ook het aangepaste advies door het NCSC verstrekt om Citrix uit te zetten, waar dat geen ernstige gevolgen heeft. (Zie persbericht)	Ja	Gebeurtenis is toegevoegd.
83	Ministerie J&V	3.1	Het…doelgroeporganisaties.	Het is reguliere operatie voor het Fusion Centre om telefonisch te informeren bij een high/high. Het is dus niet zo dat het Fusion Centre pas op 10 januari startte met bellen. Tekstvoorstel: Het Fusion Centre informeerde op 10 januari 2020 opnieuw telefonisch verschillende doelgroeporganisaties en…	Ja	Feitelijke aanpassing die in de tekst is overgenomen.
84	Ministerie J&V	3.1	Op…high.	Het NCSC verhoogde het beveiligingsadvies naar high/high én informeerde doelgroeporganisaties hier over.	Ja	Feitelijke aanpassing die in de tekst is overgenomen.
85	Ministerie J&V	3.1	De…delen.	Het NCSC is een uitvoeringsorganisatie ten aanzien van de in de Wbni geregelde taken van de minister van JenV en opereert binnen de gestelde beleidskaders en wettelijke kaders. De Directeur van het NCSC besloot in het kader van die taakuitoefening gegevens die beschouwd worden als persoonsgegevens en/of vertrouwelijke tot aanbieders herleidbare informatie in ruimere mate dan wettelijk mogelijk te delen met schakelorganisaties en andere organisaties niet behorende tot de doelgroep van Rijk en Vitaal. Wettelijk gezien kunnen persoonsgegevens alleen met organisaties die (bijvoorbeeld) als OKTT of CERT zijn aangewezen worden gedeeld én kunnen (persoons-en andere) gegevens die (tevens) beschouwd worden als vertrouwelijke tot aanbieders herleidbare informatie te delen (bijvoorbeeld) niet met OKTT's worden gedeeld. Het besluit om in ruimere mate informatie met schakelorganisaties en andere organisaties niet behorende tot de doelgroep van Rijk en Vitaal te delen vond het NCSC nodig omdat het, handelend binnen de gestelde wettelijke en beleidskaders, geen mogelijkheid had om deze informatie met deze organisaties te delen, maar dit op grond van het maatschappelijke belang wel aangewezen werd geacht.	Ja	Feitelijke aanpassing die in de tekst is overgenomen.
86	Ministerie J&V	3.1	van…team.	Dit noemen we geen incident team. Tekstvoorstel: …schaalde het NCSC op van de reguliere operatie naar een event team.	Ja	Feitelijke aanpassing die in de tekst is overgenomen.
87	Ministerie J&V	3.1	en…CERT's.	Argumentatie / onderbouwing van uw reactie.	Nee	Onduidelijk wat hier het inzagecommentaar betreft.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
88	Ministerie J&V	3.1	externe...genomen.	9 januari moet 13 januari zijn.	Nee	Uit de onderzoeksinformatie blijkt dat NCSC 9 januari 2020 hanteerde als steldatum vanaf wanneer verondersteld moet worden dat een organisatie is binnengedrongen als voor die datum geen maatregelen zijn genomen. Overigens publiceerde NCSC op 13 januari een nieuwsbericht waarin staat “mocht u op dit moment nog geen mitigerende maatregelen hebben getroffen...”
89	Ministerie J&V	3.1.2	Op basis...	MP was niet aanwezig. Bij het overleg op het Catshuis op 17 januari waren de volgende personen aanwezig: Minister JenV, minister BZK, NCTV, CIO Rijk en DGAIVD. In het Catshuis was op dat moment nog wel een andere bijeenkomst van bewindspersonen inclusief de MP gaande, dit betrof geen overleg over de problematiek rondom Citrix.	Ja	Omdat dit overleg niet is vastgelegd kan de Raad dit niet valideren. De Raad neemt deze lezing van de gebeurtenissen over.
90	Ministerie J&V	3.1	Daarbij...toe.	Het NCSC paste geen comply or explain toe. CIO Rijk deed dit voor de rijksoverheid.	Ja	Verduidelijking.
91	Ministerie J&V	3.1	Het...gerubriceerd.	Het beveiligingsadvies was Dep-V gerubriceerd.	Nee	Zie inzagereactie 92.
92	Ministerie J&V	3.1	Het...informatie.	Het NCSC heeft het beveiligingsadvies gedeeld met de rijksoverheidsorganisaties. Tekstvoorstel: Het NCSC communiceerde niet met andere organisaties dan rijksoverheidsorganisaties over de inhoud van het beveiligingsadvies vanwege de rubricering van de informatie.	Ja	De Onderzoeksraad heeft naar aanleiding van het inzagecommentaar van de AIVD en het ministerie van JenV aanvullende informatie gekregen van AIVD en NCSC: AIVD verstrekte het beveiligingsadvies op 17 januari gerubriceerd en op 20 januari gederubriceerd aan onder andere het NCSC. Dit is aangepast in de tijdlijn in het rapport.
93	Ministerie J&V	3.1	NCSC…rijksoverheid.	“In de veronderstelling” is suggestief. Het NCSC heeft gehandeld volgens de formele rubricering van het beveiligingsadvies. Tekstvoorstel: NCSC heeft gehandeld conform de rubricering van het beveiligingsadvies en derhalve het advies niet gedeeld met organisaties buiten de rijksoverheid. Conform Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI).	Nee	Zie inzagereactie 92.
94	Ministerie J&V	3.1	Het...constateerde.	Dit impliceert dat het NCSC tot die maandag 18 januari niets heeft gedaan, dat klopt niet. Het NCSC was namelijk ook in het weekend opgeschaald tot calamiteiten team. Dat houdt in dat activiteiten rondom Citrix doorlopend zijn opgepakt.	Ja	Nuancering.
95	Ministerie J&V	3.1	zou ondersteunen.	Deze zin mist nog wat nuance. Het ging erom dat NCSC deze organisaties vanwege capacitaire overwegingen niet ook nog zou kunnen ondersteunen.	Ja	Nuancering.
96	Ministerie J&V	3.2.7	Ook...vertegenwoordigen.	NCSC is een uitvoeringsorganisatie en opereert binnen de gestelde wettelijke en beleidskaders. Zie ook de toelichting bij regel 30. Tekstvoorstel: “Ook bepaalde het gestelde wettelijk kader dat het NCSC de gegevens niet mocht doorgeven aan de organisaties die deze groepen vertegenwoordigen,...”	Deels	Nuancering. Aangepast: het gaat hierbij om de interpretatie van het wettelijk kader.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
97	Ministerie J&V	3.2.7	Voor...organisaties.	Het NCSC heeft tijdens het Citrix voorval juist besloten buiten de wettelijke kaders te treden en schakelorganisaties in ruimere mate dan wettelijk mogelijk te informeren én ook een aantal andere organisaties niet behorende tot de doelgroep van Rijk en vitaal te informeren. Zie ook p. 52 regel 15-16. Daarbij is het zinsdeel “voor zover het lukte” suggestief. Tekstvoorstel: Het NCSC informeerde de organisaties die tot de eigen doelgroep (Rijksoverheid en Vitaal) behoorden die uit deze lijsten afgeleid konden worden. Op grond van een besluit van de directeur NCSC werden ook andere schakelorganisaties (binnen het Landelijk Dekkend Stelsel) die nog niet als CERT of OKTT waren aangewezen en andere organisaties (niet zijnde rijksoverheid of vitaal) geïnformeerd, die daarbij dus ook persoonsgegevens en/of gegevens als bedoeld in artikel 20, lid 2, Wbni hebben ontvangen. Dit werd gedaan op grond van de potentiele maatschappelijke impact of op grond van het maatschappelijk belang.	Ja	Feitelijke aanvulling.
98	Ministerie J&V	3.2.7	Op...maatregelen.	De onduidelijkheid werd niet alleen veroorzaakt door het gepubliceerde bericht van Citrix dat de mitigerende maatregelen niet werkten. Voor het NCSC was het gepubliceerde bericht van Citrix niet de doorslaggevende reden om te twijfelen aan de maatregelen. Citrix heeft in gesprekken met D-NCSC op 17 januari 2020 aangegeven dat de maatregelen niet werkten voor in elk geval één versie. Dit is per mail rechtstreeks aan het NCSC bevestigd. De abusievelijkheid van het publiceren van het bericht door Citrix wordt dan ook niet herkend, omdat deze in gesprekken op het moment van besluitvorming over het advies van het NCSC juist werd bevestigd. Het verlies van vertrouwen bij het NCSC in de maatregelen ontstond daarnaast voornamelijk door de berichten die het NCSC ontving van Citrix gebruikers. Tekstvoorstel: Op een cruciaal moment tijdens de incidentbestrijding, toen de situatie in Nederland maatschappelijk en bestuurlijk escaleerde op 16 januari, ontstond onduidelijkheid over of de mitigerende maatregelen werkten. Dit kwam onder andere doordat Citrix publiceerde dat de mitigerende maatregelen niet werkten. Het NCSC verloor het vertrouwen in de mitigerende maatregelen voornamelijk door ontvangen berichten van gebruikers en door bevestiging van Citrix dat de maatregelen niet werkten voor ten minste één versie.	Deels	Strijdige informatie tussen NCSC en Citrix. Dit wordt vermeld in het rapport.
99	Ministerie J&V	3.2.8	NCSC...geven.	Dit was niet slechts een opvatting van het NCSC, maar had te maken met de rubricering van het advies. Tekstvoorstel: Wegens rubricering (dep-v) van het beveiligingsadvies heeft het NCSC de informatie niet aan organisaties buiten de rijksoverheid gegeven.	Ja	Zie inzagereactie 92.
100	Ministerie J&V	3.2.8	Daarnaast ... JenV	NCSC is een onderdeel van JenV, dat belast is met het namens de minister uitvoeren van de in de Wbni bedoelde taken van de minister. Niet duidelijk is waarom met het oog daarop hier zowel van NCSC als JenV melding wordt gemaakt.	Ja	Feitelijke aanvulling.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
101	Ministerie J&V	3.3.1	het ministerie van Justitie en Veiligheid.	Het ging niet om het ministerie als geheel, maar twee onderdelen daarvan die hebben gepatched binnen de termijn die de BIO stelt voor deze kritische updates. Bovendien hadden deze organisaties vóór dat tijdstip al andere beveiligingsmaatregelen geïmplementeerd die het risico mitigeerden (waaronder twee-factor authenticatie). De gang van zaken binnen het ministerie kent dus meer nuances dan in deze alinea weergegeven. Voor een gang van zaken is de Kamerbrief d.d. 11 februari te raadplegen 'Kamerbrief over resultaten analyse VPN software'.	Ja	Feitelijke aanvulling.
102	Ministerie J&V	3.2.8.	Net…niet.	NCSC is een uitvoeringsorganisatie en opereert binnen de gestelde wettelijke en beleidskaders. Zie eerdere context bij regel 30. Echter, net als bij Citrix, heeft de D-NCSC ook in de genoemde gevallen toch besloten buiten de wettelijke kaders andere organisaties te informeren vanwege het maatschappelijk belang. Tekstvoorstel: Net als bij de citrix-casus kon het NCSC deze gegevens beperkt delen binnen de wettelijke kaders. Op grond van een besluit van de directeur NCSC werden ook andere schakelorganisaties (binnen het Landelijk Dekkend Stelsel) die nog niet als CERT of OKTT waren aangewezen en andere organisaties (niet zijnde rijksoverheid of vitaal) geïnformeerd, die daarbij dus ook persoonsgegevens en/of gegevens als bedoeld in artikel 20, lid 2, Wbni hebben ontvangen. Dit werd gedaan op grond van de potentiele maatschappelijke impact of op grond van het maatschappelijk belang.	Deels	Feitelijke aanvulling, maar de Onderzoeksraad handhaaft de zin dat dit ook een juridische interpretatie is.
103	Ministerie J&V	4.1.4	De Wbni…cybersecurityincidenten.	Voor de zorgplicht ex artikel 7 tot en met 9 Wbni geldt dat die alleen geldt voor aanbieders van essentiële diensten, maar niet voor andere vitale aanbieders (alsook voor enkele in de Wbni benoemde categorieën (op zich niet-vitale) digitale dienstverleners). Daarnaast ligt het, in plaats van "eisen op het vlak van zorgplicht voor cybersecurity, mede gelet op de tekst van genoemde artikelen in de Wbni, op zich meer in de rede te spreken van "verplichtingen tot het nemen van beveiligingsmaatregelen met betrekking tot hun netwerk en informatiesystemen".	Ja	De huidige alinea maakt dit onvoldoende duidelijk. De zin is aangepast zodat deze de inhoud van de Wbni beter reflecteert.
104	Ministerie J&V	4.2.3	Voor vitale…(NDN).	Graag hier, ook in lijn met de laatste volzin van deze alinea, verduidelijken dat de aansluiting op het NDN vitale aanbieders en rijksoverheidsorganisaties betreft. Ook voor de activiteiten in het kader van het NDN geldt dat die, voor zover het het NCSC aangaat, plaatsvinden met inachtneming van artikel 3 Wbni (en dat bv. ten aanzien van individuele gemeenten een grondslag voor verwerking van persoonsgegevens ontbreekt).	Ja	Het NDN is alleen voor vitale en rijksoverheidsorganisaties, niet voor alle overheidsorganisaties. De toevoeging 'rijks' is daarom noodzakelijk.
105	Ministerie J&V	4.2.4	Bovendien…versnipperd.	Hier ontbreekt de analyse stap om tot de conclusie te komen dat hierdoor de inzet van professionals niet doelmatig of te versnipperd is. Dit leidt tot een feitelijke onduideliljkheid in het rapport.	Ja	De onderbouwing volgt na de conclusie. De tekst is aangepast zodat de redeneerlijn duidelijker te volgen is.
106	Ministerie J&V	4.3.1	en…diensten.	Ook CERTs zijn een bron, bijvoorbeeld via coordinated vulnerability disclosure-procedures en het internationale netwerk van CERTs.	Ja	Aanvulling met een relevant voorbeeld.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
107	Ministerie J&V	4.3.1	NCSC…mandaat.	NCSC is een uitvoeringsorganisatie en opereert binnen de gestelde beleidskaders en wettelijke kaders. Het betreft geen mening van het NCSC, maar een wettelijk kader. Dat leidt tot juridische belemmeringen. Zie hier ook eerdere context bij regel 85.	Deels	Feitelijke nuancering.
108	Ministerie J&V	4.3.1	In 2020…te delen.	Voor het door het NCSC verstrekken van dreigingsinformatie aan krachtens de Wbni aangewezen computercrisisteams, zoals Z-CERT, bevat de Wbni, anders dan hier gesuggereerd, vrijwel geen belemmeringen; zie met name ook artikel 3, lid 2, en artikel 20, lid 2, Wbni. Verstrekking van dergelijke informatie aan individuele andere aanbieders, die niet behoren tot de doelgroep van Rijk en vitaal, zoals een zorginstelling, kent in de Wbni geen grondslag, maar om voor hen informatie beschikbaar te maken is juist dus de bevoegdheid tot verstrekking aan schakelorganisaties (bv. computercrisisteams) opgenomen. Voor OKTT's vormt artikel 20, lid 2, Wbni nog wel een belemmering voor verstrekking; hiervoor is een wetsvoorstel tot wijziging van de Wbni in procedure gebracht.	Deels	Zie de tijdlijn. Tijdens Citrix werd eerst de informatie gedeeld daarna werd oa ZCert aangewezen.
109	Ministerie J&V	4.3.1	aantal…delen.	Zorginstellingen zijn geen sectorale cert, Z-CERT is de sectorale cert voor de zorg. Tekstvoorstel: …aantal schakelorganisaties zoals Z- CERT en de IBD wel dreigingsinformatie te delen.	Ja	Onjuist voorbeeld. Het tekstvoorstel is overgenomen.
110	Ministerie J&V	4.3.1	dreigingsinformatie	Het NCSC deelde in beginsel niet rechtstreeks dreigingsinformatie met organisaties in het 'niet-vitale' bedrijfsleven, maar dat wil niet zeggen dat het gehele bedrijfsleven geen informatie ontving zij het indirect. Tekstvoorstel: … Dreigingsinformatie, tenzij aangesloten bij een CERT of OKTT.	Nee	Het NCSC deelde alleen informatie met bedrijven die vitale aanbieders waren. Verreweg het grootste gedeelte van het bedrijfsleven ontving geen informatie. Bovendien was het aantal CERTS dat informatie ontving beperkt.
111	Ministerie J&V	4.3.1	NCSC…Wbni.	NCSC is een uitvoeringsorganisatie en opereert binnen gestelde wettelijke kaders en beleidskaders. Het betreft geen standpunt. Zie wederom ook context bij regel 85.	Nee	Zie inzagereactie 102.
112	Ministerie J&V	4.3.1	Vertrouwelijke herleidbare gegevens (2x)	Specificatie dat dit tot aanbieders herleidbare gegevens betreft ontbreekt nog; zie artikel 20, lid 2, Wbni.	Ja	Verduidelijking.
113	Ministerie J&V	4.3.1	DTC	Het DTC is pas sinds oktober 2021 een aangewezen OKTT.	Ja	Verkeerd voorbeeld. De tekst is aangepast.
114	Ministerie J&V	4.3.1	NCSC	NCSC is een uitvoeringsorganisatie en opereert binnen de gestelde wettelijke kaders en beleidskaders. Zie wederom ook context bij regel 30. Tekstvoorstel: "JenV beschouwt IP-adressen van kwetsbare servers als dergelijke vertrouwelijke herleidbare gegevens". Zie overigens voor de verwoording van het standpunt van JenV pagina 6 van de memorie van toelichting bij het wetsvoorstel tot wijziging van de Wbni: persoonsgegevens, zoals getroffen IP-adressen, blijken, ondanks artikel 3, lid 2, vaak niet aan OKTT's te kunnen worden verstrekt, omdat zij tevens tot aanbieders herleidbare vertrouwelijke gegevens betreffen (en OKTT's niet in artikel 20, lid 2, staan vermeld).	Ja	Aangepast naar de juiste partij.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
115	Ministerie J&V	4.3.1	NCSC	NCSC is een uitvoeringsorganisatie en opereert binnen de gestelde wettelijke kaders en beleidskaders. Zie wederom context bij regel 85.	Ja	Aangepast naar de juiste partij.
116	Ministerie J&V	4.3.1	De minister…uitgevoerd.	Mocht met het hier genoemde wetsvoorstel worden gedoeld op het wetsvoorstel tot wijziging van de Wbni, dat de minister inmiddels in procedure heeft gebracht, dan bevat dit niet zozeer een wijziging van de "institutionele setting", maar een verruiming van de bevoegdheid voor het NCSC om relevante dreigingsinformatie te delen met OKTT's en in bepaalde gevallen (indien er geen schakelorganisatie is, etc.) individuele andere aanbieders (die niet behoren tot Rijk en vitaal). Dit wetsvoorstel is deze zomer in consultatie gebracht door de minister.	Ja	Verduidelijking van het doel van het wetsvoorstel.
117	Ministerie J&V	4.3.1	Zodat NCSC…doorgeven.	Zie ook hierboven: het LDS betreft niet alleen schakelorganisaties die krachtens artikel 3, lid 2, Wbni bv. als computercrisisteam zijn aangewezen, maar ook andere samenwerkingsverbanden. Met alle tot het LDS behorende organisaties wordt door het NCSC zo veel als (wettelijk) mogelijk informatie uitgewisseld; de wettelijke bevoegdheid daartoe is alleen ruimer als het verstrekking betreft aan een organisatie die krachtens artikel 3, lid 2, Wbni is aangewezen. Anders dan wellicht uit deze volzin kan worden afgeleid is het overigens niet zo dat het NCSC de enige partij is die binnen het LDS informatie uitwisselt; dat gebeurt zo veel als mogelijk juist ook door en tussen de andere tot het LDS behorende organisaties. Formeel spreken we overigens over het Landelijk Dekkend stelsel van samenwerkingsverbanden op het gebied van cybersecurity.	Ja	Aangevuld dat het een stelsel van samenwerkingsverbanden op gebied van cybersecurity betreft.
118	Ministerie J&V	4.3.1	Om die…de rest").	Het wetsvoorstel tot wijziging van de Wbni van de minister van JenV houdt een verruiming in van de mogelijkheid van het NCSC om informatie te delen met OKTT's of in bepaalde gevallen (indien er geen schakelorganisatie is, etc.) met individuele aanbieders die geen deel uitmaken van de Rijksoverheid en evenmin vitale aanbieder zijn. Daarnaast heeft EZK een eigen wetsvoorstel in consultatie gebracht over het DTC. Dat wetsvoorstel bevat onder meer de toevoeging van de minister van EZK (ten behoeve van de DTC-taken) in de artikelen 3, lid 2, en 20, lid 2, Wbni. Ook is het DTC recentelijk als OKTT aangewezen, waardoor het bij inwerkingtreding van de Wbni-wijziging meer informatie zal kunnen ontvangen.	Ja	Feitelijke aanvulling.
119	Ministerie J&V	4.3.1	moet…uitgevoerd.	Het is in de meeste gevallen, maar niet altijd nodig om aan de deur te voelen	Ja	Nuancering.
120	Ministerie J&V	4.3.1	Juristen…leidt.	Het onderzoek naar de vraag 'of en in welke gevallen scannen door het NCSC mogelijk is' loopt nog. Juridische risico's doen zich in het bijzonder voor als het gaat om scanning waarbij wordt binnengetreden in netwerk- en informatiesytemen van organisaties, zonder toestemming van die organisaties.	Nee	Dit betreft extra toelichting van de huidige situatie.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
121	Ministerie J&V	4.3.2	Naar aanleiding…het bedrijfsleven.	Het voorstel tot wijziging van de Wbni van de minister van JenV (zie ook hierboven) betreft niet enkel een verruiming van de bevoegdheid om informatie met of ten behoeve van (niet-vitale) bedrijven te delen; die verruiming betreft namelijk ook informatieverstrekking aan andere organisaties die niet tot de doelgroep van Rijk en vitaal behoren (bv. gemeenten). Het wetsvoorstel Wet bevordering digitale weerbaarheid bedrijven (Wbdwb) van EZK betreft wel alleen informatieverstrekking aan (niet-vitale) bedrijven.	Ja	Verduidelijking van de doelgroep van het wetsvoorstel.
122	Ministerie J&V	4.3.1	vertegenwoordigd	Beveiligingsonderzoekers zijn niet alleen vertegenwoordigd in de DIVD, zij kunnen ook in andere samenwerkingsverbanden werken of zelfstandig. Tekstvoorstel:…, o.a. vertegenwoordigd…	Ja	Toevoeging.
123	Ministerie J&V	4.3.2	Ook worden…vitaal.	Zie ook de opmerking hierboven. Voor zover het gaat om activiteiten van het NCSC in het kader van het NDN geldt dat informatieverstrekking ten behoeve van andere aanbieders dan die behorende tot Rijk en vitaal (bv. gemeenten) met inachtneming van (met name) artikel 3, lid 1 en 2, en artikel 20, lid 2, Wbni dient plaats te vinden.	Ja	Verduidelijking.
124	Ministerie J&V	4.4.1	De Europese…gezondheidszorg IGJ.	De NIB-richtlijn van 2016, die is geïmplementeerd in de Wbni, bevat niet voor alle vitale aanbieders (bedoeld in artikel 1 Wbni) verplichtingen (zoals een meldplicht van incidenten), maar alleen voor aanbieders van essentiële diensten (alsook voor digitaledienstverleners). Krachtens de Wbni zijn als aanbieders van essentiële diensten aangewezen: als vitale aanbieder aangemerkte entiteiten die actief zijn in sectoren, genoemd in de bijlage bij de NIB-richtlijn (zie artikel 2 Bbni). Voor enkele categorieën andere vitale aanbieders geldt, los hiervan, ook een meldplicht bij het NCSC voor ernstige incidenten (zie artikel 3 Bbni), maar voor hen gelden niet de andere, uit de NIB-richtlijn voortvloeiende verplichtingen. Daarnaast: aanbieders van essentiële diensten dienen krachtens artikel 10 Wbni ernstige incidenten bij het NCSC en de sectorale toezichthouder te melden, maar niet ook (of in plaats daarvan) bij een “sectorale CSIRT”. Overigens: voor entiteiten binnen de gezondheidszorg is wel al (in artikel 4 Wbni) de toezichthouder bepaald, maar binnen die sector zijn vooralsnog geen aanbieders van essentiële diensten aangewezen (waarop de verplichtingen vanuit de NIB-richtlijn van toepassing zouden zijn).	Ja	Feitelijke aanvulling.
125	Ministerie J&V	4.4.1	Het betreffende … informeren	Drempelwaarden in het kader van de meldplicht van artikel 10 Wbni dienen door de sectorale toezichthouders (EZK, etc.) én JenV te worden bepaald (vanwege de vaak dubbele meldplicht). Zie wat het informeren van het publiek over incidenten betreft naast (het al vermelde) artikel 23 Wbni ook artikel 20, lid 4, onder b, Wbni.	Ja	Feitelijke aanvulling.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
126	Ministerie J&V	4.4.1	Daarnaast wordt forensische onderzoek gedaan door het Team High Tech Crime van de politie en het NFI.	Het klopt dat het Team High Tech Crime forensische onderzoeken doet, maar dat gebeurt op meer plekken binnen de politie. Er zijn namelijk ook cybercrimeteams in de regionale eenheden van de politie die onderzoek doen. Verzoek is daarom “het Team High Tech Crime” te vervangen door “de politie”.	Ja	Feitelijke aanpassing.
127	Ministerie J&V	4.4.1	In juni 2019 informeerde het Team High Tech Crime….	Het informeren van de gemeente Lochem werd gedaan door het cybercrimeteam van de eenheid Rotterdam in samenwerking dat samenwerkte met het Team High Tech Crime. Voorstel is “het Team High Tech Crime” te vervangen door “de politie” of anders het cybercrimeteam van de regionale eenheid Rotterdam op te nemen.	Ja	Feitelijke aanpassing.
128	AIVD	3.1.2	In de tijdlijn van p. 38 mist het feit dat de AIVD en MIVD op 12 en 13 januari verdacht verkeer detecteerden vanaf digitale infrastructuur van een statelijke actor naar twee organisaties binnen de Rijksoverheid.	Verzoek om in de tijdlijn op p. 38 op te nemen: - 12 en 13 januari AIVD en MIVD detecteren verdacht verkeer statelijke actor naar rijksoverheid.	Ja	Feitelijke aanvulling die in de tekst is overgenomen.
129	AIVD	3.1.2	Verzoek om bovenaan p. 40 na regel 19 de volgende alinea toe te voegen.	AIVD en MIVD onderkennen verdacht verkeer van statelijke actor naar rijksoverheid. De inlichtingendiensten konden vaststellen dat er offensieve activiteiten door een statelijke actor werden uitgevoerd, omdat zij door de inzet van bijzondere middelen zicht hebben op de gebruikte digitale infrastructuur van deze statelijke actor en dit kunnen relateren aan digitaal verkeer naar de Rijksoverheid. Dit verdachte digitale verkeer is op 12 en 13 januari onderkend, direct nader onderzocht, geduid en over gerapporteerd aan verschillende beleidsdepartementen in bovengenoemd inlichtingenbericht.	Ja	Feitelijke aanvulling die in de tekst is overgenomen.
130	AIVD	3.1.2	Er staat nu dat op basis van het inlichtingenbericht is opgeschaald, maar de IAO structuur was er al voordat het inlichtingenbericht is uitgebracht.		Deels	In het rapport staat niet dat er is opgeschaald vanwege het beveiligingsadvies. Er staat “Vanwege de ernst van de situatie besloot het NCC deels op te schalen …” Uit oogpunt van chronologie zullen we de volgorde van beide gebeurtenissen in de tekst omdraaien.
131	AIVD	3.1.2	Het was een gezamenlijk inlichtingenbericht van de AIVD en MIVD. Daarom het verzoek de tekst alsvolgt aan te passen.	Opschaling naar nationale crisisstructuur MIVD en AIVD. Op 17 januari 2020 brachten MIVD en AIVD een gezamenlijk inlichtingenbericht uit aan onder andere NCTV en NCSC, waarin stond dat zij een acute dreiging van een statelijke actor richting twee organisaties binnen de Rijksoverheid hadden waargenomen.	Ja	Feitelijke aanvulling die in de tekst is overgenomen.
132	AIVD	3.1.2	We zouden graag toevoegen dat we het belang wilden benadrukken van het niet afdoende werken van de patch. Die was slechts een workaround voor bepaalde versies en niet volledig.	De AIVD wilde dat NCSC organisaties zou adviseren om alle Citrix-servers uit te zetten vanwege de waargenomen dreiging, het beschikbaar zijn van een exploit en het niet volledig werken van de door Citrix voorgestelde maatregelen terwijl NCSC organisaties wilde adviseren om op basis van hun specifieke situatie een eigen afweging te maken.	Ja	Aanvulling onderbouwing advies.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
133	AIVD	3.1.2	Er is op vrijdag een concept beveiligingsadvies gedeeld met rubri DepV. Iom met NCSC is besproken dat hoe meer info ongerubriceerd gestuurd wer, hoe makkelijker gedeeld kon worden. Het definitieve beveiligingsadvies is ongerubriceerd verstuurd. Het beveiligingsadvies is gezamenlijk opgesteld. Het definitieve advies is maandag 20 januari verstuurd naar NCSC en NCTV.	Het NCSC communiceerde niet met andere organisaties over de inhoud van het beveiligingsadvies vanwege de rubricering van de informatie die op het concept beveiligingsadvies zat. Het definitieve beveiligingsadvies was gezamenlijk (AIVD/ NCSC) opgesteld, gericht aan de NCTV en NCSC en was niet gerubriceerd. Het advies was gericht op de Rijksoverheid. NCTV heeft het overgenomen en verder uitgebreid naar Vitaal.	Deels	Zie inzagereactie 92.
134	AIVD	4.3	In paragraaf 4.3 incident bestrijding (response) ligt de nadruk op het delen van informatie tussen met name het Nationale CERT en relevante partijen. Graag zouden we hier een nuancering in willen aanbrengen. Het 'delen van informatie' is te vrijblijvend. De bedoeling is om handelingsperspectief te bieden zodat de getroffen organisaties ook weten wat hen te doen staat. Met het delen van informatie over kwetsbaarheden en dreiging zijn de slachtoffers niet geholpen. Het ontbreekt hen vaak aan de kennis en kunde om op de juiste wijze te acteren op basis van deze informatie in een dergelijke noodsituatie. Daarom is de belangrijkste taak van een Nationaal CERT om handelingsperspectief te bieden. Uiteraard is informatie over kwetsbaarheden en dreiging daar een onderdeel van. Dit valt ook niet onder de term beveiligingsadvies. Een beveiligingsadvies is erop gericht om aanvallers buiten je netwerk te houden. In het geval dat een hacker binnen je netwerk zit, wil je een ander soort advies. Namelijk waar te zoeken, hoe kun je hem herkennen etc.		Ja	In 4.3.1 worden organisaties benoemd die informatie nodig hebben om een eigen afweging te maken hoe te handelen en om de risico's te beheersen. Er is tekst toegevoegd om te benadrukken dat het gaat om het bieden van handelingsperspectief. Zodoende wordt ook duidelijker dat de paragraaf "belemmeringen in het delen van informatie" raakt aan het handelingsperspectief van partijen.
135	AIVD	2.2		Ter overweging: het blokje is gebaseerd op het boek van N. Pelroth. Op basis van haar boek wordt Nederland genoemd als statelijke actor die kwetsbaarheden opkoopt. Nederland wordt in het rapport in dezelfde zin genoemd (en daardoor vergeleken?) met statelijke actoren met een offensief cyberprogramma, zoals China en Rusland.	Deels	Nuancering: duidelijker onderscheid tussen verschillende actoren en toevoeging initiatiefwet Zero Days Afwegingsproces .
136	AIVD	3.1.1	Op de tijdslijn missen nog een aantal onderdelen. Ter overweging om over te nemen?	16 December publiceerde Citrix al mitigerende maatregelen, waardoor mensen al wisten dat er problemen waren, en die bovendien (voor zover wij weten) niet goed werden gecommuniceerd.	Nee	Zie inzagereactie 156. Het artikel werd tegelijk met de kwetsbaarheden gepubliceerd.
137	AIVD	3.1.2	Op deze tijdslijn mist een onderdeel. Ter overweging om over te nemen?	Het opschalen van de kwetsbaarheid door het NCSC op 24 december naar HIGH/HIGH	Ja	Toevoeging aan tijdlijn.
138	Ministerie EZK	2.5	Coordinated vulnerability disclosure (CVE).	Coordinated vulnerability disclosure en CVE (common vulnerabilities and exposures) zijn twee verschillende zaken. Welke van beiden wordt bedoeld? Op basis van de context waarschijnlijk het uitschrijven van CVE.	Ja	De term die in deze tekst wordt bedoeld is Common Vulnerabilities and Exposures (CVE).
139	Ministerie EZK	2.5	Aanvulling op de tekst: het CSIRT DSP voor digitale dienstverleners.	Het CSIRT DSP, computer incident response team voor digital service providers is gecreeerd op basis van de EU NIB-richtlijn en is onderdeel van het ministerie van EZK.	Ja	Aanvulling.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
140	Ministerie EZK	2.5	Aanvulling op de tekst: het Digital Trust Center voor het niet-vitale bedrijfsleven.	Het proces van aanwijzen van OKTTs door de minister van JenV is sinds het voorval met Citrix verder gegaan. Het DTC is sinds september 2021 aangewezen als OKTT. Indien deze passage is bedoeld om een weergave te geven van het stelsel anno publicatiedatum van het rapport dan zou het toevoegen van het DTC passend zijn in het overzicht.	Ja	De passage betreft een weergave van het huidige stelsel, het DTC is daarom een relevante aanvulling.
141	Ministerie EZK	2.6	voetnoot 40	Onduidelijk is bij deze opsomming van vitale sectoren is of wordt aangesloten op de sectoren zoals opgenomen in de Wbni of in het overzicht van de rijksbreed gedefinieerde vitale processen zoals aangegeven op de website van de NCTV: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen	Ja	Dit sluit aan bij de aanwijzing vitale aanbieders (Besluit beveiliging netwerk- en informatiesystemen, versie januari 2019).
142	Ministerie EZK	3.1	Na ophoging van het beveiligingsadvies van het NCSC naar High/High heeft het DTC het niet-vitale Nederlandse bedrijfsleven meermalig geinformeerd over de kwetbsbaarheid inclusief het daarbij horend handelingsperfectief.	Na ophoging van het beveiligingsadvies van het NCSC naar High/High heeft het DTC de niet-vitale doelgroep meermalig geinformeerd over de kwetsbaarheid en handelingsperfectief geboden.	Ja	Feitelijke aanpassing die in de tekst is overgenomen.
143	Ministerie EZK	3.1	Na de scans van het DIVD en andere partijen brengt het CSIRT-DSP alle gecomprimiteerde en mogelijk gecomprimiteerde doelgroeppartijen (digitale dienstverleners) direct op de hoogte.	Na de scans van het DIVD en andere partijen brengt het CSIRT-DSP alle gecomprimiteerde doelgroeppartijen (digitale dienstverleners) direct op de hoogte.	Ja	Feitelijke aanpassing die in de tekst is overgenomen.
144	Ministerie EZK	4.3	Om die reden…rest).	In het persbericht waaraan wordt gerefeerd in de voetnoot worden 2 wetsvoorstellen aangekondigd door respectievelijk JenV (wijziging Wbni) en EZK (wetsvoorstel Wet bevordering digitale weerbaarheide bedrijven, Wbdwb). In de Wbni-wijziging maakt JenV het mogelijk dat NCSC breder informatie kan delen met partijen, waaronder zogenaamde OKTTs. Met de Wbdwb verstevigt EZK de wettelijke basis van het DTC om informatie over dreigingen en kwetsbaarheden te kunnen ontvangen, verwerken en delen met bedrijven. Daarnaast heeft de minister van JenV in september 2021 de OKTT-status toegekend aan het DTC onder de huidige systematiek van de Wbni en het DTC is in september 2021 begonnen met het delen van informatie met bedrijven. Zie hiervoor de Kamerbrief van 2 juni 2021 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z09619&did=2021D21232 en het persbericht van 13 sept 2021 https://www.rijksoverheid.nl/actueel/nieuws/2021/09/13/digital-trust-center-start-met-actief-informeren-bedrijven-over-digitale-dreigingen	Ja	Verduidelijking.
145	Ministerie EZK	4.4	energie en digitaal	De meld- en zorgplicht bij Agentschap Telecom is op basis van de NIB/Wbni van toepassing op de vitale aanbieders/ AEDs in de sectoren energie en digitale infrastructuur. Voor de telecomsector bestaat sinds 2012 een zorg- en meldplicht inclusief toezicht van AT op basis van de Telecommunicatiewet ongeacht of een partij door EZK als vitaal is aangewezen. In de Wbni is aanvullend op deze sectorale wet- en regelgeving een meldplicht bij het NCSC opgenomen alleen voor de vitaal aangewezen telecompartijen.	Ja	Feitelijke aanvulling.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
146	Ministerie EZK	4.4	AT en JenV	Het onderzoek naar de storing van 112 is uitgevoerd door de toezichthouders AT, IJenV en IGJ https://www.agentschaptelecom.nl/documenten/rapporten/2020/06/25/onbereikbaarheid-van-112-op-24-juni-2019	Ja	Feitelijke aanvulling.
147	Ministerie EZK	4.5	Aanvullingen voor de tabel met EU wet- en regelgeving.	Hierbij een aantal andere relevante voorbeelden van EU wet- en regelgeving op cybersecurity om kennis van te nemen ten behoeve van de tabel inclusief de vindplaatsen voor informatie. In de EU cyber security strategie van december 2020: (1) het voornemen om cybersecurityeisen te stellen aan draadloos verbonden apparaten via een gedelegeerde handeling via de Radio Equipment Directive (voorzien eind 2021), (2) voor automotive worden cybersecurityeisen opgenomen in de General Safety Regulation op basis van VN-afspraken, (3) herziening van de General Product Safety Directive (vangnet in de EU-systematiek van EU productregulering) tot een General Product Safety Regulation. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (pagina 9-10 inclusief voetnoten), BNC-fiche voor de GPSR: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z14961&did=2021D31993 (4) In 2017 zijn twee EU verordeningen aangenomen voor medische apparaten inclusief cybersecurity verplichtingen. In een werkgroep van marktpartijen is begin 2020 een guidance opgesteld voor cybersecurity https://ec.europa.eu/docsroom/documents/41863 (5) Ten aanzien van horizontale regulering heeft voorzitter van de EC von der Leyen de cyberscurity resilience act aangekondigd in haar staat van de Unie in sept 2021. Het wetsvoorstel is nog in ontwikkeling. https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701 (6) in 2019 zijn twee EU richtlijnen aangenomen in het consumentrecht, verkoop goederen en digitale inhoud waarbij zaken rondom recht op updates zijn opgenomen. De implementatiewet is in behandeling bij de Tweede Kamer https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2021A01807	Ja	Feitelijke aanvulling. Dit gaat over IoT en niet over software an sich.
148	Ministerie EZK	Bijlagen	Bijlage A naar bijlage B etc	Er is twee keer ‘bijlage A’ opgenomen waardoor de verdere titels van de bijlagen niet meer klopt	Ja	Incorrecte nummering van bijlagen is aangepast.
149	DIVD	2.2	Opsomming	Een kwetsbaarheid is vooral gevaarlijk als hij deze zaken weet te omzeilen, zoals gebeurde bij de Citrix kwetsbaarheid. Maar deze kwetsbaarheden zitten vaak juist op andere plaatsen dan in deze mechanismes. Bij Citrix ging het b.v. om een functie die een “bookmark” aanmaakte voor een VPN verbinding.	Ja	Verduidelijking
150	DIVD	2.2	aanval te voorkomen.	Hierbij horen ook de maatregelen die een organisatie neemt om impact van misbruik te voorkomen. B.v. door een citrix server niet standaard volledige toegang te geven tot het hele netwerk, maar deze toegang te beperken tot alleen die zaken die de server nodig heeft. Dit geheel wordt defense in depth genoemd.	Ja	Maatregelen om de impact van misbruik te voorkomen behoren ook tot preventieve maatregelen die een organisatie kan nemen.
151	DIVD	2.2	creëren	Het lijkt erop dat hier beheren wordt bedoeld.	Ja	Het gaat hier om het opzetten en het onderhouden van veilige digitale systemen.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
152	DIVD	3.1		In de grafiek lijkt het erop dat de gebeurtenissen van 17-12 op verschillende dagen gebeurden.	Nee	In de grafiek is onderscheid gemaakt tussen de gebeurtenissen voor 17 december, op 17 december en na 17 december (twee events) en als zodanig weergegeven.
153	DIVD	3.1		Aanvallen op systemen gebeurden al voor de exploit code op 10-1 openbaar werd.	Ja	Feitelijke aanpassing die in de tekst is overgenomen.
154	DIVD	3.1		Kies voor een andere weergave van de tijdslijn die het mogelijk maakt tijdsvlakken aan te duiden.	Nee	De gekozen weergave geeft de gebeurtenissen in een duidelijke vorm weer zoals die zich hebben afgespeeld.
155	DIVD	3.1.1		Was de publicatie nu op 16 of 17 december. Het rapport spreek zichzelf hier tegen.	Ja	Zie inzagereactie 11.
156	DIVD	3.1.1		De tekst leest nu alsof Citrix enkel en alleen op verzoek van NCSC deze tool heeft gepubliceerd. Ik hoop oprecht dat het NCSC deze mate van indruk maakt op eenAmerikaanse partij, maaarik denk eerder dat het NCSC om deze tool verzocht heeft (en met hen vele anderen) en dat de leverancier de tool toen heeft uitgebracht. Maar niet enkel op verzoek van het NCSC.	Nee	Zie inzagereactie 17.
157	DIVD	3.1.1.		Het lijkt in deze tekst alsof enkel de fabrikant scans uitvoerde, maar andere onderzoekers zoals b.v. het DIVD hebben dit ook gedaan.	Ja	Paragraaf 3.1.1 focust op de vondst van de kwetsbaarheid en de reactie van de fabrikant. De gebeurtenissen in de voorgestelde aanvulling worden al beschreven in paragraaf 3.1.2, die focust op de incidentbestrijding in Nederland. Een kruisverwijzing naar 3.1.2 is toegevoegd.
158	DIVD	3.1.2	OKTTs	Het kan niet waar zijn dat toen de OKTTs zijn gewaarschuwd. Hoewel de wet al bestond waren er naar mijn weten nog geen OKTTs aangewezen.	Ja	Feitelijke aanpassing.
159	DIVD	3.1.2	Zette op	Het SecurityMeldpunt bestond al, maar was nog niet geactiveerd. Het DIVD activeerde dus het security meldpunt.	Ja	Feitelijke aanpassing.
160	DIVD	3.1.2		Het lijkt uit de opsomming alsof het DIVD deze informatie niet met het NCSC heeft gedeeld. Dat is onjuist. Het DIVD heeft deze informatie ook met het NCSC gedeeld.	Ja	Feitelijke aanpassing.
161	DIVD	3.1.2		Ook particuliere bedrijven (zoals b.v. Schuberg Philis) hebben hun Citrix systemen uitgezet obv het advies van het NCSC.	Ja	Feitelijke aanpassing.
162	DIVD	3.1.2		Het NCSC heeft niet alleen niet over de inhoud van het AIVD advies gepubliceerd, maar zelfs (in het openbaar) niet over het bestaan van het advies. Hierdoor was het voor afnemers van de advisories van het NCSC via de website niet duidelijk op welke basis het verzwaarde advies tot stand gekomen was.	Nee	Tekst is duidelijk en de onderbouwing van (de reactie van de DIVD) is al in de tekst verwerkt.
163	DIVD	3.1.2		Nogmaals het gaat zowel om het delen van de inhoud als delen van het feit dat het advies gebaseerd was op een AIVD advies. Dit feit delen had voor afnemers al veel geholpen. Overigens heeft een ander ministerie (ik weet even niet meer welk) dit die dag of de dag erna wel gedeeld in hun publicatie over waaarom ze Citrix hadden uitgezet.	Nee	Tekst is duidelijk en de onderbouwing van (de reactie van de DIVD) is al in de tekst verwerkt.
164	DIVD	3.1.2		DIVD heeft in deze case vooral Nederland gescand. Deze context ontbreekt in deze paragraaf.	Ja	Feitelijke aanvulling.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste...laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
165	DIVD	3.1.2		Dit lijkt in contrast met pagina 39 regel 28 waarin staat dat deze CERTS werden gewaarschuwd.	Nee	Het betreft twee verschillende gebeurtenissen. Op pagina 39 staat dat het NCSC op 10 januari buiten de regels om CERT's had gewaarschuwd, en dat D-NCSC daarvoor toestemming had verleend. Op pagina 46 staat dat de minister op 23 januari vier sectorale CERT's heeft aangewezen waarmee intensiever mag worden samen gewerkt en binnen de kaders van de wet- en regelgeving informatie mag worden uitgewisseld.
166	DIVD	3.2.1		Het was met de path traversal juist mogelijk bestanden te lezen op de Citrix server.	Nee	Path traversal is noodzakelijk maar op zichzelf niet afdoende om bestanden te lezen op de Citrix server. Daarnaast is het nodig om niet alleen lees- maar ook schrijf- en uitvoerrechten te hebben. Die rechten hoeven niet bij dezelfde entiteit te liggen.
167	DIVD	3.2.5		Het ging niet alleen om de /../ maar ook om het "path" waarin dit voorkomen kon worden. Hierdoor was duidelijk dat het om path traversal ging en in welk deel van de software moest worden gezocht.	Ja	Feitelijke aanvulling.
168	DIVD	3.2.8		Niet alleen niet wisten wat er in het AIVD advies zat, maar zelfs niet wisten DAT er een AIVD advies ten grondslag lag aan het NCSC advies.	Ja	Feitelijke aanvulling.
169	DIVD	3.3.1		Het gaat hier niet om de gebruikersinterface (voor eindegebruikers) maar om de beheerdersinterface.	Ja	Aangepast naar de correcte term.
170	DIVD	3.3.2	werd...gebruikt.	De software wordt voornamelijk gebruikt door MSPs, maar soms ook door bedrijven zelf.	Ja	Feitelijke aanvulling.
171	DIVD	3.3.2	In...supermarktketen.	KCoop heeft een deel van zijn 800 winkels moeten sluiten.	Nee	Dit staat al in de tekst. ("In Zweden leidde dit ertoe dat een supermarktketen van bijna al zijn 800 winkels de deuren moest sluiten.")
172	DIVD	4.1.2	Fabrikanten...software.	Deze regels suggereren dat toegang tot de bronkode noodzakelijk is voor het hebben van een bug bountry programma. Dit is niet zo. Het is natuurlijk zo dat fouten makkelijker te vinden zijn met toegang tot de broncode, maar dit is zeker geen voorwaarde voor het hebben van een program. Microsoft heeft b.v. ook een bug bounty program, maar geef voor veel producten niet de broncode vrij.	Nee	In de zin staat "fabrikanten kunnen kwetsbaarheden ook opsporen zonder derden daarbij directe toegang tot de broncode te geven". Daarmee geven we dus aan dat er ook manieren zijn om kwetsbaarheden op te sporen zonder dat daarbij toegang tot de broncode noodzakelijk is. Het bug bounty programma wordt genoemd als voorbeeld hiervan.
173	DIVD	4.1.2		Deze paragraaf geeft een alles of niets beeld van publiceren. Het is mogelijk over het bestaan een kwetsbaarheid te publiceren zonder de details van de kwetsbaarheid prijs te geven. Daarom is de handelswijze van PA schadelijk. Ze houden niet alleen geheim welke kwetsbaarheid er in het product zit (waarvoor alle begrip) maar ook dat het product een kwetsbaarheid bevat die met de patch wordt opgelost, waardoor de ontvanger van de patch de noodzaak van de patch niet voldoende kan inschatten.	Ja	De huidige alinea maakt onvoldoende duidelijk dat er in het genoemde voorbeeld sprake is van het volledig achterhouden van informatie over de aanwezigheid van een kwetsbaarheid in de software. De alinea is aangepast om dit te benadrukken.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
174	DIVD	4.1.3	redundante...omgeschakeld.	Dit wordt te makkelijk als een oplossing gepresenteerd. Neem bijvoorbeeld Exchange. Het is voor veel bedrijven simpel weg ondoenbaar om naar Exchange nog een andere vorm van groupware in stand te houden en up to date te houden waarop “even” kan worden overgeschakeld in geval van een kwetsbaarheid in Exchange. Producten van verschillende leveranciers zijn vaak niet eens op deze manier compatible.	Ja	In 4.2 wordt verder ingegaan op het omgaan met de afhankelijkheid van software. 4.2.3 noemt o.a. dat het niet realistisch is om alle systemen redundant uit te voeren omdat dit extra middelen kost en dat het zo kan zijn dat systemen van verschillende aanbieders niet goed samen kunnen werken. Daarmee wordt compatibiliteit dus impliciet benoemd. Tekst is aangepast om duidelijker te maken het we het over compatibiliteitsproblemen hebben.
175	DIVD	4.1.3			Nee	Onduidelijk wat hier het inzagecommentaar betreft.
176	DIVD	2.2	Coordinate of responsible disclosure -> coordinated vulnerability disclosure of responsible disclosure.	De afkortingen RD en CVD worden in de praktijk door elkaar en als synoniemen gebruikt, maar CD heeft niemand het over.	Ja	Er wordt hier coordinated vulnerability disclosure bedoeld.
177	DIVD	2.2	Publiceren	Het is niet perse zo dat de kwetsbaarheid zelf “gepubliceerd” hoeft te worden in een CVE entry. Er zit een kwetsbaarheid van dit type in deze software is voldoende. Gaat dus eerder om een “registratie” dan een “publicatie”.	Ja	Verduidelijking.
178	DIVD	2.2	Proof of Concept	Op het moment dat POC code wordt gebruik voor een daadwerkelijke aanval, dan spreek je niet meer over POC maar over een daadwerkelijk exploit. Suggestie: aan 17 toevoegen. Op basis van een PoC kan een hiervoor onderlegd persoon ook code maken die het systeem daarwerkelijk misbruikt, dit wordt een exploit genoemd. En aan 30 PoC of exploit code.	Ja	Verduidelijking.
179	DIVD	2.2	kunnen informeren	Een 0-day kwetsbaarheid is strikt genomen niets meer dan een kwetsbaarheid waarvoor nog geen patch beschrikbaar is. Een 0-day exploit exploit code waarvoor nog geen patch beschikbaar is. Als een leverancier over een kwetsbaarheid communiceert zonder dat er een patch beschrikbaar is (zoals hier is gebeurd) dan blijft de kwetsbaarheid een 0-day kwetsbaarheid.	Deels	Verduidelijking.
180	DIVD	2.2	exploits	Er wordt gehandeld in zowel exploits als kwetsbaarheden. Iemand die een kwetsbaarheid vindt verkoopt hem aan iemand die er een exploit voor maakt en zo de waarde verhoogt, die hem weer verkoopt aan .... Suggestie kwetsbaarheden en exploits.	Ja	Tekstvoorstel overgenomen.
181	DIVD	2.2	miljoenen	Hier onstaat een verkeerde indruk van de handel in 0-days. De “miljoenen” worden vrijwel uitsluitend betaalt op de “zwarte markt” en aan bedrijven als zerodium en NSO. In een bug bounty program worden zelden zulke hoge bedragen bestaald, en mag een onderzoeker blij zijn als hij een paar duizend vangt. Als een bedrijf geen bug bounty program heeft, dan mag je als onderzoeker blij zijn met een “lousy t-shirt”. Dit korte kadertje doet een signifikant onderwerp te weinig recht.	Ja	Verduidelijking.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
182	DIVD	2.2	half-day	Hier wordt weer de indruk gewekt dat de days gemeten worden op basis van de communicatie van de leverancier, maar het gaat om beschikbaarheid van een patch. Een half day kwetsbaarheid wordt vaak gemaakt op basis van een patch en richt zich op de tijd die gebruikers nodig hebben om een patch van een leverancier uit te rollen.	Ja	Verduidelijking van het begrip half-day.
183	DIVD	2.5	“Computer Security Incident Response Team” ipv Computer Security Response Team.	Correcte afkorting. Dit is overigens het response team voor getroffenen en niet voor DIVD zelf, zie: csirt.divd.nl	Ja	De genoemde term is incompleet.
184	DIVD	3.1.2	“het DIVD” ipv “de DIVD”.		Ja	Tekstuele wijziging.
185	DIVD	3.3.1		DIVD heeft al in april gemeld aan vertrouwde partijen dat er een kwetsbaarheid zat in KaseyaVSA en is vanaf dat moment ook wereldwijd gaan scannen hierop en vond 2.200 MSPs die KaseyaVSA gebruikten. Direct na de aanval 2 juli, is DIVD telkens gaan scannen en melden. Zie voor het volledige verslag: https://csirt.divd.nl/cases/DIVD-2021-00011/	Ja	Feitelijke aanwulling.
186	DIVD	4.3.1	“het DIVD” ipv “de DIVD”		Ja	Taalfout.
187	DIVD	Lijst van afkortingen en begrippen	ISO 27001 Wereldwijd erkende norm voor informatiebeveiliging -> ISO 27001 Wereldwijd erkende norm voor informatiebeveiligingsmanagement.	De ISO27001 norm beschrijft niet hoe een bedrijf zich moet beveiligen, maar hoe een bedrijf de informatiebeveiliging moet managen.	Ja	Op de website van de NEN staat ‘norm voor informatiebeveiliging’, maar op de website van ISO staat inderdaad ‘Information Security Management’
188	SurfCert	3.1.1		Mij werd niet helemaal helder wat er met de informatie is gedaan die door Citrix met het NCSC is gedeeld. Verderop lijkt het vooral te gaan over de informatie die via DIVD is gekomen.	Nee	De analyse van hoe met dreigingsinformatie zoals scans naar kwetsbare servers is omgegaan (paragraaf 4.3) heeft ook betrekking op informatie van andere bronnen dan DIVD, zoals fabrikanten.
189	SurfCert	3.1.2		Mij werd pas later duidelijk wat er bedoeld werd met “DIVD blijft monitoren en waarschuwen”. Op het moment van presenteren van de figuur komt dat uit de lucht vallen lijkt het wel.	Nee	Dat geldt voor alle gebeurtenissen in de tijdlijn: in de tijdlijn wordt het kort weergegeven en later in de tekst toegelicht.
190	SurfCert	3.1.2		Was zelf nog wel benieuwd naar het verschil in aanpak tussen Citrix en DIVD.	Nee	Dat lag buiten de scope van het onderzoek.
191	SurfCert	3.1.2	Voetnoot toevoegen?	Tussen de voetnoten staat wel wat het NCSC Fusion Center is maar in de tekst doorboven lijkt niet naar de voetnoot te worden verwezen.	Ja	Tekstuele wijziging.
192	SurfCert	3.1.2	SurfCert -> SURFcert	De indruk wordt gewekt dat het fusion center op 10 januari startte. Met dan een verwijzing naar secorale CERT’s (57). Waaronder SURFcert genoemd staat. Volgens onze gegevens zijn wij door het NCSC echter pas op 13 januari om 18:23 geinformeerd. Dat lijkt mij significant later dan de indruk die de huidige tekst wekt.	Ja	Feitelijke aanvulling.
193	SurfCert	3.2.7		Ik weet vrij zeker dat tijdens de crisis een beroep is gedaan op het NRN (Nationaal Response Netwerk). Op zoek naar partijen die dergelijke middelen wel hadden. Binnen onze doelgroep was dat zeker aanwezig maar wij konden geen full-time inzet leveren. Defensie kon dat wel en er is toen gebruik gemaakt van hun expertise/hulp. Goed om te melden/op te nemen?	Ja	Feitelijke aanvulling.

Nummer	Partij	Hoofdstuk	Te corrigeren tekst (eerste…laatste woord)	Argumentatie, onderbouwing van de reactie	Overgenomen	Toelichting Onderzoeksraad voor Veiligheid
194	SurfCert	3.3.1		Ik blijf het jammer vinden dat niet helder wordt of het "NCSC waarschuwde deze organisaties niet" ook wel tijdig terug is gedeeld met de oorspronkelijke melder (DIVD).	Ja	Feitelijke aanvulling.
195	SurfCert	3.3.3		Behalve het scannen lijkt het mij ook cruciaal dat ze die informatie wilden delen.	Ja	In de laatste zin van de alinea wordt genoemd dat ze met de informatie verkregen door het scannen ook organisaties waarschuwden. Hiermee bedoelen we dus het delen van informatie over kwetsbare servers. De eerste zin is aangepast om te expliciteren dat de DIVD een belangrijke rol heeft gespeeld bij informatiedeling.
196	SurfCert	4.2.3	2021en -> 2021 en	(excuses, maar deze viel me op)	Ja	Dit betreft een typefout.
197	SurfCert	4.3.1		Niet helder is wat ze zouden willen gaan scannen. Enkel hun eigen doelgroep? Voor mij zouden ze dit niet hoeven doen. Al helemaal niet zolang ze de resultaten toch niet kunnen/ willen delen.	Nee	De passage geeft aan waarom het NCSC systemen zou willen scannen. Het overige deel van deze reactie betreft een persoonlijke opvatting van de inzagepartij.