1 INLEIDING

1.1 Aanleiding

De directe aanleiding voor dit onderzoek is het voorval waarbij een kwetsbaarheid in software van Citrix gevolgen had voor organisaties die de software gebruiken. Op 17 december 2019 deed Citrix een openbare mededeling dat een aantal van hun softwareproducten een kwetsbaarheid bevatten waardoor aanvallers konden binnendringen in de digitale systemen van organisaties die deze producten gebruiken.[12] Citrix gaf aan welke maatregelen konden worden genomen om de problemen tijdelijk te verhelpen, maar had nog geen definitieve oplossing voor de ontstane kwetsbaarheid. Op 17 januari 2020 adviseerde het Nationaal Cyber Security Centrum (NCSC) aan Nederlandse gebruikers hun Citrix-servers uit te zetten. Aanvallers drongen als gevolg van de kwetsbaarheid in de software digitale systemen van verschillende overheden en bedrijven binnen.[13]

Het Amerikaanse bedrijf Citrix maakt software waarmee onder meer werknemers op afstand kunnen inloggen in de bedrijfs-ICT-systemen van hun werkgever. Deze software vormt vaak een belangrijk onderdeel van de digitale infrastructuur, omdat ze de koppeling vormen tussen het externe netwerk (internet) en het interne netwerk. Een groot deel van de Nederlandse rijksoverheid, maar ook decentrale overheden, ziekenhuizen, onderwijsinstellingen, vitale en overige bedrijven gebruiken deze Citrix-software.

Deze gebeurtenissen (die we kortweg beveiligingslek door Citrix-software noemen) hebben laten zien dat de digitale infrastructuur van de samenleving kwetsbaar is en *security* problemen kunnen leiden tot onveiligheid.[14] Burgers zijn voor hun veiligheid afhankelijk van de wijze waarop en de mate waarin organisaties de veiligheid beheersen. Voor de Onderzoeksraad voor Veiligheid is dit aanleiding om te onderzoeken wat er is gebeurd ten tijde van het voorval en hoe de risico's werden en worden beheerst, zowel bij het voorkomen als het bestrijden van dit voorval en vergelijkbare voorvallen.

12 Citrix, *CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance*, 17 december 2019. https://support.citrix.com/article/CTX267027

13 Dit probleem is tot op de dag van vandaag actueel. Aanvallers zijn nog steeds gedeeltelijk binnengedrongen in sommige systemen.

14 In paragraaf 2.1 worden de begrippen veiligheid en security verder uitgewerkt.

1.2 Doel

Het doel van dit onderzoek is lessen te identificeren die verantwoordelijke partijen helpen de beheersing van risico's als gevolg van kwetsbaarheden in software die veiligheidsgevolgen kunnen hebben te verbeteren. De lessen zijn onder meer gericht op softwarefabrikanten, organisaties die software gebruiken en overheden en andere organisaties die kunnen helpen bij het voorkomen en bestrijden van dergelijke voorvallen.

Het voorval met Citrix vormt de aanleiding voor dit onderzoek, als typisch voorbeeld van een gebeurtenis waarbij deze risico's ontstaan, zoals ook andere cyberaanvallen sinds 2020 demonstreren.

1.3 Onderzoeksvragen

De Onderzoeksraad gaat er vanuit dat de manier waarop fabrikanten, organisaties die software gebruiken, de overheid en andere (deels non-gouvernementele) organisaties digitale veiligheidsrisico's beheersen[15], bepaalt in hoeverre voorvallen als deze kunnen plaatsvinden en de mate waarin deze invloed hebben op de fysieke en sociale veiligheid van burgers. Op basis van dit uitgangspunt formuleerde de Raad de volgende onderzoeksvraag:

> Welke lessen zijn te trekken uit de wijze waarop betrokken partijen zijn omgegaan met de risico's van de kwetsbaarheid in Citrix-software die in december 2019 aan het licht kwam?

Deelvragen:

1. Hoe konden de beveiligingslekken bij organisaties door een kwetsbaarheid in Citrix software ontstaan en welke gevolgen had dit?
2. Op welke manier werden deze risico's ingeschat en maatregelen genomen om ze te voorkomen en de ongewenste gevolgen te bestrijden (risicobeheersing):
   a. door fabrikant en organisaties die de software afnemen en gebruiken;
   b. door het openbaar bestuur/de overheid en niet-overheidspartijen?
3. Wat is er nodig van betrokken partijen om het systeem van risicobeheersing en -sturing te versterken?

15 De manier waarop organisaties de risico's beheersen, wordt ook wel *risk governance* genoemd.

1.4 Afbakening en focus

Kwetsbaarheden in software die leiden tot beveiligingslekken en mogelijke veiligheidsgevolgen
Dit onderzoek is afgebakend tot voorvallen waarbij de digitale systemen van een organisatie een beveiligingslek bevatten en in sommige gevallen werden binnengedrongen als gevolg van een kwetsbaarheid in de gebruikte software, zoals is gebeurd als gevolg van de kwetsbaarheid in de software van Citrix. De focus ligt daarbij op software die een koppeling vormt tussen het internet en het interne netwerk van de organisatie, zoals software om beveiligde verbindingen op te zetten voor thuiswerken en samenwerken op afstand.

Buiten dit onderzoek vallen voorvallen waarbij aanvallers langs andere wegen de digitale systemen van een organisatie binnendringen, zoals bijvoorbeeld via *phishing*, of onbeschikbaar maken zoals via een DDos aanval. Ook voorvallen waarbij de digitale systemen uitvallen[16] zonder dat ze worden aangevallen, vallen buiten de scope van dit onderzoek. Verder richt het onderzoek zich op software voor de zakelijke markt, niet op software voor consumenten. Wel betrekken we de gevolgen voor burgers in het onderzoek.

Gedetailleerde reconstructie Citrix-voorval
De kwetsbaarheden in de software van Citrix en de gevolgen daarvan vormen het startpunt van dit onderzoek. De reconstructie van het voorval met de Citrix-software neemt een centrale plek in binnen het onderzoek. Wat gebeurde er, wie was op welk moment van welke informatie op de hoogte wat deden ze met de informatie en hoe kwam dat? Deze uitgebreide reconstructie is nodig om de directe en achterliggende factoren te kunnen analyseren.

Geen technisch-forensisch onderzoek
De Onderzoeksraad heeft zelf geen technisch-forensisch onderzoek gedaan naar de kwetsbaarheden in de software en de systemen die als gevolg van deze kwetsbaarheden al dan niet zijn binnengedrongen. Wel is waar mogelijk en zinvol gebruik gemaakt van de inzichten uit technisch-forensische onderzoeken van beveiligingsbedrijven en betrokken organisaties.

Generaliseren naar voorvallen als gevolg van kwetsbaarheden in software
Om in bredere zin uitspraken te kunnen doen over hoe betrokken partijen kwetsbaarheden in software (proberen te)voorkomen en de gevolgen daarvan te beperken, heeft de Raad een aantal andere voorvallen onderzocht waarbij kwetsbaarheden in software grote gevolgen hadden voor de digitale veiligheid van organisaties en daarmee ook op de veiligheid van burgers. Het ging daarbij onder andere om software die is bedoeld om een beveiligde verbinding op te zetten (VPN-software).[17] De Onderzoeksraad voegde ook informatie toe over voorvallen die plaatsvonden gedurende de looptijd van het

16 Zie bijvoorbeeld Onderzoeksraad voor Veiligheid, *Patiëntveiligheid bij ICT uitval in ziekenhuizen*, 2020.
17 VPN-software van PulseSecure/Fortinet/Palo Alto, Big IP van F5. Voorvallen die plaatsvonden gedurende de looptijd van het onderzoek: SolarWinds/Sunburst/Supernova en Microsoft Exchange, PrintSpooler, Kaseya. Deze voorvallen worden behandeld in paragraaf 3.3.

onderzoek. De Onderzoeksraad onderzocht deze voorvallen op basis van openbare bronnen.

Raakvlakken tussen openbaar bestuur en andere partijen
In het onderzoek heeft de Raad het accent gelegd op de rol van het openbaar bestuur, dat in verschillende manieren bij dit onderwerp betrokken is: als afnemer/gebruiker van software, als degene die de markt voor software kan reguleren en als de partij die misbruik van software en digitale systemen kan opsporen en handhaven. Tegelijk erkennen we dat, zoals bij de onderzoeksvragen wordt beschreven, ook andere partijen een belangrijke rol moeten spelen bij het borgen van de veiligheid. Het onderzoek is daarom gericht op de raakvlakken en wisselwerking tussen het openbaar bestuur en andere organisaties. Denk bijvoorbeeld aan de wijze waarop het openbaar bestuur stuurt op hoe fabrikanten veilige software maken en hoe organisaties deze gebruiken. Ook speelt het openbaar bestuur een belangrijke rol in de aanpak van de incidentbestrijding, zowel door publieke, private als non-gouvernementele partijen. Bij de analyse van de raakvlakken tussen het openbaar bestuur en andere partijen, heeft de Raad eerder gepubliceerde adviezen van onder meer de Wetenschappelijke Raad voor het Regeringsbeleid en de Cyber Security Raad betrokken.

1.5 Onderzoeksaanpak

De Raad heeft de volgende aanpak gehanteerd tijdens het onderzoek. We begonnen met het verzamelen van voornamelijk openbare informatie. Deze informatie vulden we aan door betrokken partijen schriftelijke vragen te stellen over de kwetsbaarheden, hun werkwijze bij het ontwikkelen van software en de incidentbestrijding en het raadplegen van experts. De meeste partijen werkten hieraan mee, een aantal fabrikanten is echter niet ingegaan op ons verzoek om vragen te beantwoorden. In totaal zijn voor het hele onderzoek ongeveer 1.200 documenten geanalyseerd. In aanvulling daarop namen we ruim 40 interviews af met betrokkenen bij fabrikanten, organisaties die de software gebruiken en die incidenten bestrijden, zowel publiek, privaat als non-gouvernementeel. Bijlage A bevat een verder toelichting op de wijze waarop het onderzoek is uitgevoerd.[18]

Voor het theoretisch kader (concepten, begrippen, mechanismen, en dergelijke) heeft de Raad gebruik gemaakt van verschillende publicaties over technische, bestuurskundige en economische aspecten van digitale veiligheid.[19] Om de onderzoeksvragen te kunnen beantwoorden hebben we een referentiekader opgesteld, waarin we beschrijven wat de Raad verwacht van de verschillende betrokken partijen en hoe deze partijen redelijkerwijs konden bijdragen aan veilige digitale systemen. Aan de hand van dit referentiekader konden we aangeven welke knelpunten er zijn in de wijze waarop de verantwoordelijkheden voor veilige digitale systemen nu zijn belegd.

18 De openbare informatie betrof met name publicaties vanuit de fabrikanten (CVE, berichten op de website), overheden en andere autoriteiten (beleidsdocumenten, berichten van CERTs), ethische hackers (artikelen, presentaties), wetenschappelijke publicaties, (vak/social)media artikelen.

19 Ellis R. en V. Mohan, *Rewired: Cybersecurity Governance*, 2019. Anderson, R., *Security Engineering*, 2020 en andere publicaties over *security engineering*.

Voor de reconstructie van het verloop van de gebeurtenissen gebruikten we een tijdlijnanalyse. Om de mogelijke factoren die van invloed zijn geweest in beeld te krijgen, voerden we een ongevalsanalyse uit. Daarbij pasten we de ongevalsanalysemethode Tripod-Beta toe. Ook analyseerden we het systeem waarbinnen het voorval kon plaatsvinden: we brachten in beeld welke partijen betrokken waren middels een omgevings- en stakeholdersanalyse en de CAST/STAMP-methodiek. Deze methodiek geeft inzicht in de hiërarchische lijnen, rollen en verantwoordelijkheden van de betrokken partijen en de relatie met wet- en regelgeving. We pasten de methodiek toe op de wijze waarop betrokken partijen kwetsbaarheden in software voorkomen en verhelpen, en de manier waarop ze informatiedelen en incidenten bestrijden en hoe van de voorvallen wordt geleerd.[20]

Binnen de analyse van de voorvallen heeft de Onderzoeksraad onderscheid gemaakt tussen de volgende fasen:

- ontstaan en preventie van de kwetsbaarheid en voorbereiding op het aan het licht komen van kwetsbaarheden, zie paragraaf 4.1;
- het afnemen en in gebruik nemen van software en het nemen van preventieve maatregelen door organisaties die software gebruiken, zie paragraaf 4.2;
- incidentbestrijding, met name het delen van informatie, zie paragraaf 4.3;
- de wijze waarop van incidenten wordt geleerd, zie paragraaf 4.4;
- ontwikkelingen in (internationale) regulering, zie paragraaf 4.5.

1.6 Referentiekader

De Raad stelt tijdens zijn onderzoek een referentiekader op. Het referentiekader geeft weer hoe – naar de huidige inzichten – een bepaald veiligheidsrisico kan worden beheerst. De Onderzoeksraad put hierbij zowel uit ervaringen in Nederland en andere landen, als uit zijn eigen ervaring in andere domeinen. Het referentiekader is gebruikt om te reflecteren op de huidige werkwijze rondom beveiligingslekken door kwetsbaarheden in software en de mogelijkheden die er zijn om deze te versterken.

Het volledige referentiekader gericht op de borging van digitale veiligheid is opgenomen in bijlage C. Thema's in dit referentiekader zijn productveiligheid van software, preventie van en voorbereiding op incidenten en het bestrijden van incidenten (respons). Ook de wijze waarop van voorvallen wordt geleerd is een thema binnen dit referentiekader. Belangrijke actoren binnen het domein van digitale veiligheid zijn fabrikanten, organisaties die software aanschaffen en gebruiken, (inter)nationale overheden en andere organisaties die bijdragen aan regelgeving en incidentbestrijding. Het referentiekader beschrijft wat de Raad van de verschillende actoren verwacht.

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

Essentiële elementen in het referentiekader zijn de volgende:

- software kan een veiligheids-kritische rol spelen in de digitale systemen van organisaties: in de ontwikkeling en productie van software moet veiligheid centraal staan (*safety and security by design*);
- fabrikanten zijn verantwoordelijk het zo adequaat mogelijk te voorkomen dat software kwetsbaarheden bevat en organisaties zo veel mogelijk te helpen bij het voorkomen en bestrijden van de gevolgen als een kwetsbaarheid toch is aangetroffen;
- organisaties kunnen via het proces van aanschaf en ingebruikname van software fabrikanten stimuleren om zo veilig mogelijke software te maken. Daarbij is het van belang dat fabrikanten organisaties de informatie en positie verschaffen om deze afweging te kunnen maken. Voor organisaties is het van belang dat zij veilige ICT beschouwen en behandelen als een cruciaal element – maar ook als risico - voor hun organisatie. Organisaties dienen inzicht te hebben in de manier waarop ze zelf risico lopen en hoe ze dat kunnen beheersen.
- partijen zijn onderling van elkaar afhankelijk. Het borgen van digitale veiligheid is daarmee een collectieve maatschappelijke opgave, waar de rijksoverheid stelsel-verantwoordelijkheid voor draagt, de samenwerking en het delen van informatie dient te stimuleren en belemmeringen zo veel als mogelijk weg dient te nemen.

1.7 Leeswijzer

Hoofdstuk 2 geeft een toelichting op de belangrijkste begrippen en concepten die relevant zijn voor dit onderzoek.

Hoofdstuk 3 beantwoordt de vraag hoe dergelijke voorvallen ontstaan, welke gevolgen ze hadden en hoe de risico's werden beheerst. Dit doen we door het voorval dat aanleiding was voor dit onderzoek uitvoerig te beschrijven en te analyseren: de kwetsbaarheid in de software van Citrix en de gevolgen daarvan voor organisaties die deze software gebruikten. Om de bevindingen uit de analyse van dat voorval te kunnen verbreden, beschrijven en analyseren we in hoofdstuk 3 ook vergelijkbare voorvallen.

In hoofdstuk 4 beschrijven we de achterliggende factoren die van invloed waren op het ontstaan en de gevolgen van de voorvallen uit hoofdstuk 3. Daarbij maken we onderscheid tussen het proces waarin software wordt geproduceerd, het proces waarin organisaties bepaalde software selecteren om aan te schaffen en in gebruik te nemen, en de processen die plaatsvinden zodra er een kwetsbaarheid in de software is aangetroffen (incidentbestrijding). In aanvulling daarop gaan we in op hoe op dit moment van digitale voorvallen wordt geleerd en de internationale context die op digitale voorvallen van toepassing is.

Hoofdstuk 5 en 6 bevatten respectievelijk de conclusies en de aanbevelingen die de Raad aan partijen doet om de veiligheid te verbeteren. De bijlagen bevatten achtergronden bij het onderzoek, zoals de onderzoeksverantwoording (bijlage A), de inzagereacties van betrokken partijen op het conceptrapport (bijlage B) en enkele bijlagen met verdiepende informatie over de onderwerpen die in het rapport aan de orde komen.