3 TOEDRACHT EN ANALYSE VOORVALLEN

Dit hoofdstuk geeft antwoord op de eerste onderzoeksvraag, namelijk hoe voorvallen zoals de beveiligingslekken door de kwetsbaarheid in Citrix-software ontstaan, welke gevolgen ze hadden en hoe de risico's werden beheerst. Paragraaf 3.1 beschrijft wat fabrikant Citrix deed nadat hij over de kwetsbaarheid werd geïnformeerd, paragraaf 3.2 de incidentbestrijding en de gevolgen voor organisaties die de software gebruikten. Om de bevindingen uit de analyse van dat voorval te kunnen verbreden, worden andere vergelijkbare voorvallen in paragraaf 3.3 beschreven. Ter ondersteuning voor de lezer zijn de teksten voorzien van tijdlijnen.

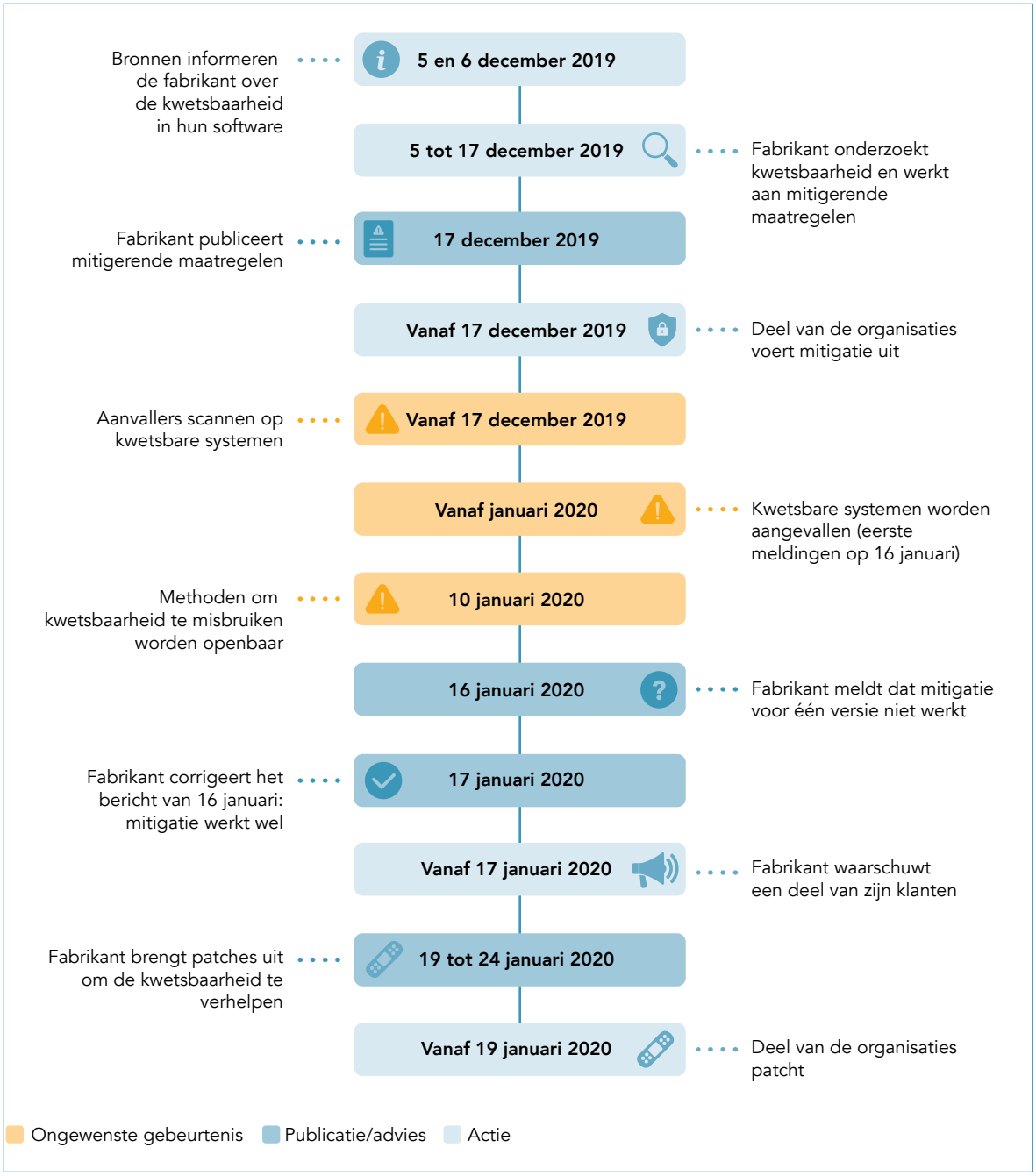
3.1 Toedracht beveiligingslekken door kwetsbaarheid in Citrix-software

Deze paragraaf beschrijft de gebeurtenissen die plaatsvonden naar aanleiding van een kwetsbaarheid in de Citrix-software[52]: de ontdekking van deze kwetsbaarheid, de reactie van de fabrikant en de incidentbestrijding in Nederland vanaf het moment dat de fabrikant de kwetsbaarheid bekendmaakte.

3.1.1 Ontdekking kwetsbaarheid in Citrix-software en reactie van de fabrikant

Deze subparagraaf gaat over de ontdekking van de kwetsbaarheid in de Citrix-software en de reactie van de fabrikant daarop. De belangrijkste gebeurtenissen zijn weergegeven in een tijdlijn.

52 Het betreft de kwetsbaarheid die fabrikant Citrix op 17 december 2019 liet publiceren (CVE-2019-19781).



Figuur 8: Tijdlijn reactie fabrikant.

Bronnen informeren fabrikant over kwetsbaarheid in software

Op 5 en 6 december 2019 benaderden drie verschillende bronnen Citrix. Zij informeerden de fabrikant onafhankelijk van elkaar over dezelfde kwetsbaarheid in de software. Eén van de bronnen gaf aan dat de kwetsbaarheid al breder bekend was. Bij het aantonen daarvan gebruikten zij alle drie dezelfde demonstratiemethode.[53]

53 Twee van de bronnen gaven daarbij aan niet de oorspronkelijke vinder van de kwetsbaarheid te zijn, maar de informatie te hebben gekregen uit een *bug bounty* programma van één van de klanten van Citrix. Volgens één van de bronnen werd de kwetsbaarheid op online kanalen met andere zogenoemde *bug bounty hunters* gedeeld. *Bug bounty hunters* zijn individuen (of organisaties) die in ruil voor erkenning en een beloning op zoek gaan naar kwetsbaarheden in digitale systemen. Zie onder andere publicatie Techzine over interview CISO Citrix met Techzine, 23 januari 2020. Beschikbaar via: https://www.techzine.eu/blogs/security/44687/exclusive-interview-citrix-ciso-fermin-serna-where-did-it-go-wrong/

Fabrikant onderzoekt kwetsbaarheid
Na de meldingen onderzocht Citrix of de kwetsbaarheid intern bekend was. Dit was niet het geval. Daarna onderzochten verschillende afdelingen van de fabrikant de kwetsbaarheid. Bovendien bleek uit de analyse van de fabrikant dat deze kwetsbaarheid al meer dan tien jaar aanwezig was in het fundament van de software, in componenten die al vanaf het begin van de ontwikkeling onderdeel waren van het product.

Gelet op de PoC-code die al in omloop was, schatte de fabrikant in dat kwetsbare systemen een hoog risico liepen om aangevallen te worden. Op basis van deze risico-analyse realiseerde de fabrikant zich dat dit betekende dat de kwetsbaarheid aanwezig was in een groot gedeelte van alle in gebruik zijnde versies (*installed base*) van de Citrix-software en dat het maken van patches voor al deze versies veel tijd en energie zou kosten.

In reactie en op basis van de analyse dat een PoC-code in omloop kon zijn, besloot Citrix daarop om dit te behandelen als een *zero day* kwetsbaarheid. De gebruikelijk werkwijze is dat eerst een patch wordt ontwikkeld die de kwetsbaarheid zou moeten wegnemen en daarna de kwetsbaarheid publiceren. In plaats daarvan ontwikkelde de fabrikant mitigerende maatregelen als tijdelijke oplossing in afwachting van de definitieve patches. Mitigerende maatregelen konden sneller worden uitgebracht dan een patch. En ook al zou de mitigatie de oorzaak van de kwetsbaarheid niet weghalen, het neemt wel het effect van de kwetsbaarheid weg en reduceert zo het risico. Daarom beschouwde Citrix de mitigerende maatregelen als net zo effectief als een patch.

Fabrikant publiceert mitigerende maatregelen
Op 17 december maakte de fabrikant de mitigerende maatregelen en de informatie over de kwetsbaarheden bekend door het publiceren van een *support article* en een *security bulletin* op hun website. Hierin waarschuwde hij voor een kwetsbaarheid in verschillende producten en versies van de Citrix-software. De fabrikant beoordeelde de kwetsbaarheid zelf als zeer ernstig (9,8 op een schaal van één tot tien).[54]

Aanvallers scannen op kwetsbare systemen
Door het publiceren van de mitigatie werd het voor aanvallers mogelijk om af te leiden waar en welke kwetsbaarheid in de software van Citrix zat (*reverse engineering*). Volgens Citrix woog het risico dat een mitigatie of patch zou worden *reverse engineered* in een *exploit* niet op tegen het belang van het communiceren van de mitigatie en de noodzaak om afnemers te beschermen tegen een *zero day* situatie.

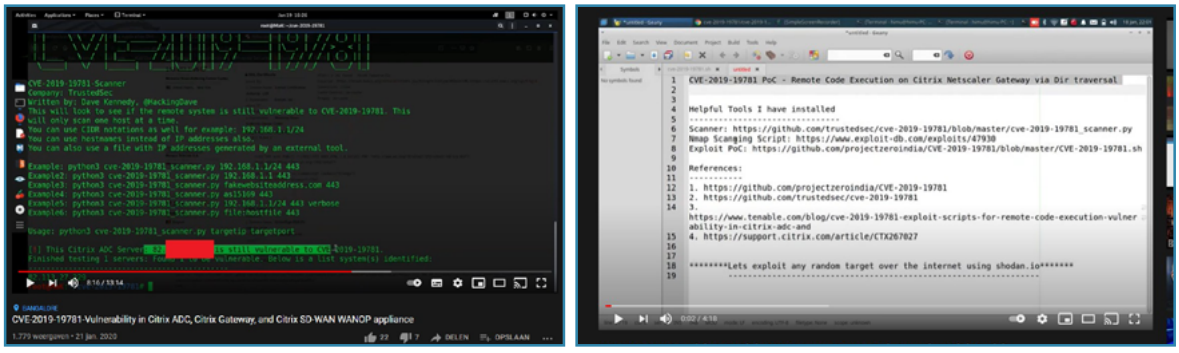
In de week na de bekendmaking publiceerde één van de bronnen die de kwetsbaarheid had gemeld aanvullende details over de kwetsbaarheid. In de periode daarna volgden publicaties van andere beveiligingsonderzoekers, waarin zij op basis van de mitigerende maatregel beschreven wat de aard van de kwetsbaarheid was en hoe deze zou kunnen worden gebruikt. Uit een wereldwijde scan op 8 januari 2020 bleek dat wereldwijd ongeveer 60.000 servers dit product gebruikten en dat daarvan ongeveer 40.000 nog

54 Citrix, Support article mitigation, pagina aangemaakt 16 december 2019, gepubliceerd 17 december 2019. Huidige versie beschikbaar via: https://support.citrix.com/article/CTX267679 Citrix, *CVE-2019-19871 – Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance*, 17 december 2019. Huidige versie beschikbaar via: https://support.citrix.com/article/CTX267027

kwetsbaar leken. Vooralsnog had nog niemand een werkende aanvalsmethode gepubliceerd, waardoor het niet waarschijnlijk leek dat aanvallers op dat moment de kwetsbaarheid al op grote schaal zouden kunnen misbruiken om kwetsbare servers aan te vallen. Wel had de fabrikant van de bronnen die de kwetsbaarheid aan hem meldden vernomen dat de kwetsbaarheid en mogelijk ook de demonstratiemethode al in bepaalde kringen circuleerde.[55]

Methoden om kwetsbaarheid te misbruiken worden openbaar

Op 10 januari 2020 maakte een groep beveiligingsonderzoekers via platform GitHub de *exploit code* openbaar die demonstreerde hoe de kwetsbaarheid in de Citrix-software gebruikt kon worden om een kwetsbare server binnen te dringen. Zij deden dit zonder de fabrikant hierover te raadplegen of informeren. Op 11 januari publiceerde een beveiligingsbedrijf ook zijn versie van de *exploit*. Na het openbaar worden van de methoden om de kwetsbaarheid te misbruiken, was het voor de fabrikant en andere betrokkenen, zoals NCSC in Nederland, bekend dat het voor potentiële aanvallers eenvoudig en laagdrempelig was geworden om kwetsbare Citrix servers te misbruiken. De code was vindbaar op GitHub. Op YouTube verschenen video's waarin de methodiek om de kwetsbaarheid te misbruiken werd gedemonstreerd.[56]



Figuur 9: Video's waarin (l) wordt uitgelegd hoe kwetsbare servers kunnen worden gevonden en (r) wordt gedemonstreerd hoe de kwetsbaarheid kan worden aangevallen.[57]

Kwetsbare systemen worden aangevallen

In de dagen erna kwamen veel berichten over kwetsbare en getroffen servers naar buiten. Zo publiceerde een beveiligingsbedrijf op 12 januari 2020 over 25 duizend kwetsbare servers in de wereld, waarvan 713 in Nederland. Het NCSC ontving op 11 januari een lijst met kwetsbare servers van dit beveiligingsbedrijf. Het ging hier om servers waarop de betreffende organisaties de door Citrix gepubliceerde mitigatie-maatregelen niet hadden toegepast voordat de aanvallen begonnen. Dit maakte dat de systemen waar deze servers deel van uitmaken kwetsbaar waren voor aanvallen van buitenaf. Een ander beveiligingsbedrijf berichtte op 15 januari over een grote piek in

55 Aanvullende details werden gepubliceerd op: https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of-80000-companies/ Met beveiligingsonderzoeker (of *security researcher*) doelen we in dit onderzoek op personen die op individuele basis of vanuit een (beveiligings-)bedrijf onderzoek doen naar kwetsbaarheden in software en systemen. Bijvoorbeeld https://www.tripwire.com/state-of-security/vert/citrix-netscaler-cve-2019-19781-what-you-need-to-know/

56 GitHub is een online platform waar gebruikers broncode kunnen plaatsen, zodat andere gebruikers die kunnen gebruiken. Publicatie exploit code 10 januari 2020: https://github.com/projectzeroindia/CVE-2019-19781 Publicatie exploit code 11 januari 2020: https://github.com/trustedsec/cve-2019-19781

57 (l) https://www.youtube.com/watch?v=cALcgyq42kI (r) https://www.youtube.com/watch?v=c9-V68L5qUw

aanvallen. Diezelfde dag meldden media dat aanvallers de digitale systemen van een ziekenhuis en een gemeente waren binnengedrongen door gebruik te maken van de kwetsbaarheid in de Citrix software.[58]

Mitigeren kreeg geen prioriteit
Een overheidsinstelling met beperkte ICT capaciteit zag geen kans om de mitigatie voor de Citrix systemen uit te voeren toen deze beschikbaar werd gesteld. Het besluit om niet te mitigeren werd in dit geval gemaakt door de ICT-afdeling. Deze afdeling kampte met capaciteitsproblemen, en omdat er al plannen lagen om de Citrix omgeving op korte termijn te vernieuwen, zagen zij het direct mitigeren van de Citrix systemen niet als prioriteit. Het lukte de CISO[59] van deze overheidsinstelling niet om de urgentie over te brengen zodat de ICT afdeling de mitigatie door zou voeren. Het gevolg was dat de organisatie werd aangevallen en de Citrix systemen alsnog moest uitschakelen. Bij deze organisatie had dit tot gevolg dat werknemers niet meer konden thuiswerken.

Twijfel over effectiviteit mitigatie

Op 16 januari 2020, een maand na het publiceren van de mitigatiemaatregelen, rapporteerden verschillende bronnen dat de mitigatie zoals door Citrix geadviseerd niet voor alle versies van de Citrix ADC en Gateway leek te werken. De fabrikant publiceerde een bericht waarin stond dat de mitigatie bij bepaalde oudere versies van de software niet goed werkte, maar kwam kort daarna tot het inzicht dat deze conclusie ten onrechte was getrokken. Op 17 januari 2020 corrigeerde Citrix het uitgebrachte bericht via een bulletin update en directieleden van de fabrikant meldde in een tv-interview, blogpost en op Twitter nadrukkelijk dat de mitigatie wel altijd werkte voor alle releases en patches, mits de klant alle stappen had uitgevoerd die nodig waren om de mitigatie correct te laten werken. Alternatief was om te upgraden naar een nieuwe versie en gedeeltelijke migratie uit te voeren.[60]

Fabrikant waarschuwt deel van zijn klanten

Een dag eerder, op 15 januari 2020, nam Citrix aanvullende maatregelen bovenop de eerder door hen uitgebrachte mitigatiemaatregel als tussenoplossing voor het verhelpen van de kwetsbaarheid.

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

59 *Chief Information Security Officer*, verantwoordelijk voor de informatiebeveiliging binnen een organisatie.

60 Afhankelijk van de licentie en het support contract konden aan de upgrade voor de afnemer kosten aan verbonden zijn. Bericht dat mitigatie voor één versie niet werkte: https://support.citrix.com/article/CTX269189
Correctie van vorig bericht: https://www.citrix.com/blogs/2020/01/17/citrix-updates-on-citrix-adc-citrix-gateway-vulnerability/

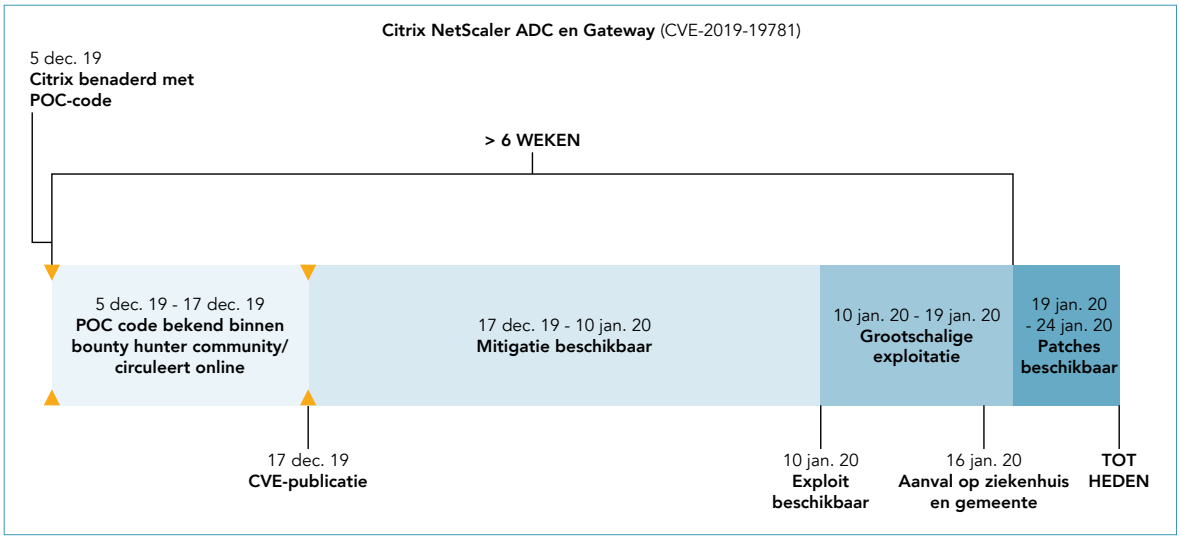
Naast het plaatsen van de alert op de website en in *social media*-berichten deed de fabrikant een poging om zo veel mogelijk van zijn klanten zelf te benaderen. In de periode van 17 tot 24 januari stuurde Citrix ruim 124.000 e-mails naar ongeveer 36.000 verschillende organisaties. In diezelfde periode begon de fabrikant met het aanleggen van een database met contactgegevens van klanten[61], om bij toekomstige kwetsbaarheden effectiever producten te kunnen traceren en klanten te kunnen waarschuwen.

De fabrikant bracht op 15 januari een tool uit om te testen of servers kwetsbaar waren en of de mitigatie correct was uitgevoerd. NCSC in Nederland verzocht Citrix op 17 januari om ook een forensische tool uit te brengen om vast te kunnen stellen of een kwetsbare server was binnengedrongen. Omdat een dergelijke tool niet beschikbaar was, bouwde Citrix deze op verzoek van NCSC en stelde deze op 22 januari beschikbaar.

Ook scande de fabrikant (en andere partijen zoals beveiligingsonderzoekers van het DIVD, zie paragraaf 3.1.2) vanaf begin januari 2020 het internet op IP-adressen van kwetsbare servers.[62] In het geval dat de fabrikant een gevonden IP-adres kon koppelen aan een klant, probeerde ze deze klant actief te benaderen. Ook deelde Citrix de IP-adressen die zij op deze manier vonden met de nationale CERTs, waaronder het Nederlandse NCSC.

Fabrikant brengt patches uit om de kwetsbaarheid definitief te verhelpen

Citrix publiceerde op 17 januari een tijdlijn waarop stond wanneer de patches zouden verschijnen die de kwetsbaarheid definitief zouden moeten verhelpen. In eerste instantie verwachtte Citrix tot 31 januari nodig te hebben om patches te maken voor alle in gebruik zijnde versies van de diverse producten. Uiteindelijk publiceerde Citrix de patches in de periode van 19 tot 24 januari.[63]



Figuur 10: Tijdlijn van bekend worden kwetsbaarheid tot publicatie, exploitatie en patches.

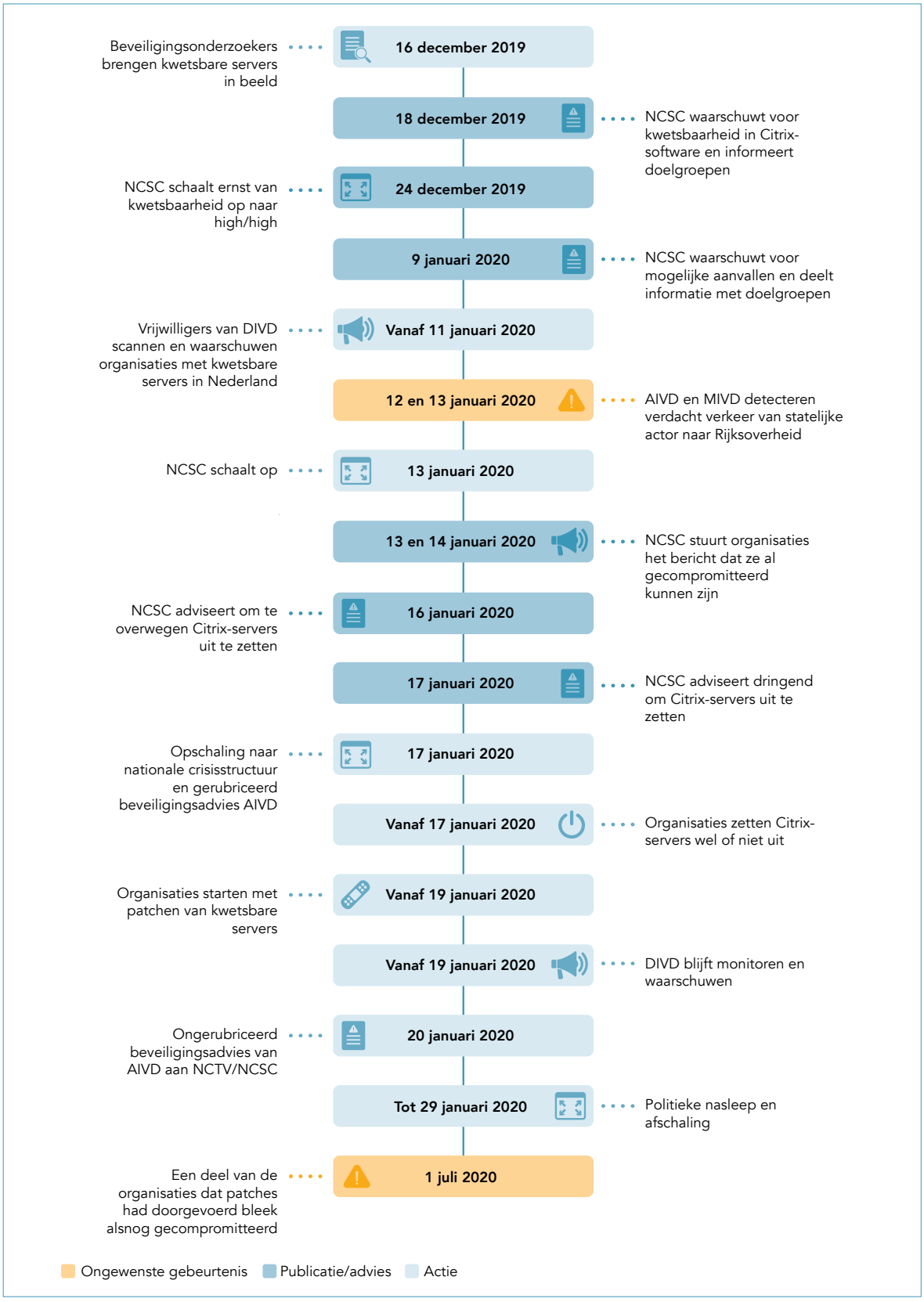
61 *Customer Relationship Management* (CRM).

62 Citrix maakte daarbij gebruik van een zelfgemaakte tool in combinatie met diensten als BinaryEdge en Shodan. Deze diensten scannen het internet om aan internet gekoppelde apparaten (benaderbaar vanaf een bepaalde IP adres en poort combinatie) te classificeren.

63 Een patch is een nieuwe versie van de software die de kwetsbaarheid niet meer bevat (bron: *Woordenboek Cyberveilig Nederland 2019*). Eerste tijdlijn van de patches: https://www.citrix.com/blogs/2020/01/11/citrix-provides-update-on-citrix-adc-citrix-gateway-vulnerability/ Publicatie van de patches: https://www.citrix.com/blogs/2020/01/22/update-on-cve-2019-19781-fixes-now-available-for-citrix-sd-wan-wanop/

3.1.2 Gevolgen en incidentbestrijding in Nederland

Deze subparagraaf gaat over de incidentbestrijding in Nederland vanaf het moment dat de fabrikant de kwetsbaarheid bekendmaakte.



Figuur 11: Tijdlijn incidentbestrijding.[64]

64 Achteraf is niet meer vast te stellen of deze organisaties vooraf hadden gemitigeerd, en of dit correct en op tijd was doorgevoerd.

Beveiligingsonderzoekers brengen kwetsbare servers in kaart
Verschillende beveiligingsonderzoekers, waaronder van de DIVD, scanden het internet om in kaart te brengen hoeveel servers de kwetsbare Citrix-software gebruiken. Een eerste scan op 16 december 2019 toonde wereldwijd ruim 125.000 kwetsbare servers, op 23 december (een week na publicatie van de kwetsbaarheid) waren dat er nog 80.000 waarvan 3.700 in Nederland en op 7/8 januari 2020 waren er nog 700 kwetsbare servers in Nederland.[65]

NCSC waarschuwt voor kwetsbaarheid in Citrix-software
Op 18 december publiceerde NCSC een eerste beveiligingsadvies over deze kwetsbaarheid op zijn website en deelde deze met zijn doelgroepen, de Rijksoverheid en de vitale aanbieders: 'NCSC beveiligingsadvies 18 december 2019: Citrix meldt dat er een kwetsbaarheid is gevonden in Citrix ADC, Citrix Gateway, Citrix Netscaler en Citrix Netscaler ADC. Ook is de kwetsbaarheid gevonden in de Citrix SD-WAN WANOP-software.' NCSC schaalde de ernst van de kwetsbaarheid in als medium/high. Op basis van de informatie van beveiligingsonderzoekers verhoogde NCSC op 24 december de inschaling van het eerdere beveiligingsadvies naar High/High en informeerde doelgroeporganisaties hierover.[66]

NCSC waarschuwt voor mogelijke aanvallen en deelt informatie met doelgroepen
Vanwege berichten vanuit onder meer het *Internet Storm Center* van SANS, waarschuwde NCSC op 9 januari hun doelgroepen en via een bericht op de website dat aanvallers actief naar kwetsbare Citrix-servers zochten. Het *Fusion Center*[67] van het NCSC ontving meerdere signalen vanuit hun doelgroepen dat zij konden zien dat aanvallers naar kwetsbare servers zochten. Ook ontving NCSC van beveiligingsonderzoekers lijsten met IP-adressen van ruim 700 kwetsbare servers. Deze informatie verwerkten zij in een update van hun beveiligingsadvies op de website.[68] Na ophoging van het beveiligingsadvies van het NCSC naar High/High heeft het DTC de niet-vitale doelgroep meermalig geïnformeerd over de kwetsbaarheid en handelingsperspectief geboden.

Het Fusion Center informeerde na 10 januari 2020 opnieuw telefonisch verschillende doelgroeporganisaties. Ook deelde NCSC in de dagen na 10 januari informatie met de aangesloten sectorale CERT's.[69] De directeur van het NCSC gaf, op grond van het maatschappelijk belang, toestemming om daarbij ook gegevens die zij beschouwen als

65 *Dutch Institute for Vulnerability Disclosure* (DIVD) is een Nederlandse organisatie die bestaat uit beveiligingsonderzoekers die zich vrijwillig inzetten om naar eigen zeggen 'de digitale wereld veiliger te maken door kwetsbaarheden op te sporen en te melden bij de mensen die het probleem kunnen oplossen'. https://www.divd.nl/ Rapport DIVD over het Citrix-voorval: https://www.divd.nl/reports/2020-00001-Citrix/ Bericht over kwetsbare Citrix-servers: https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of- 80000-companies/

66 Bericht van NCSC: https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 18 december 2019. Inschalingsmatrix van het NCSC: medium/high: gemiddelde kans op misbruik en hoge impact bij misbruik high/high: hoge kans op misbruik én hoge impact bij misbruik

67 Het *Fusion Center* is de operationele kern van het NCSC waar 24/7 (inter)nationale informatiestromen worden verwerkt.

68 Bericht Internet Storm Center SANS: https://isc.sans.edu/forums/diary/A+Quick+Update+on+Scanning+for+CVE201919781+Citrix+ADC+Gateway+Vulnerability/25686/ 7 januari 2020 Bericht NCSC: https://www.ncsc.nl/actueel/nieuws/2020/januari/9/aanvallers-zoeken-actief-naar-kwetsbare-citrix-servers Update beveiligingsadvies NCSC https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 9 januari 2020.

69 IBD, SurfCert, Cert WM, ZCert. Zo gaf SurfCERT aan in de avond van 13 januari door NCSC te zijn geïnformeerd.

persoonsgegevens en vertrouwelijk herleidbare informatie te delen.[70] Deze toestemming vond NCSC nodig omdat het naar eigen zeggen geen juridische bevoegdheid heeft om deze informatie met deze organisaties te delen. In paragraaf 4.3 gaan we in op deze overwegingen.

Verder vroeg het NCSC aan CIO Rijk om de CIO's, CTO's en CISO's van de departementen te informeren. De CIO Rijk heeft daarbij gevraagd of de departementen de nodige maatregelen hadden getroffen en om deze alsnog te nemen. Organisaties die hun Citrix-systemen op dat moment nog niet hadden aangepast moesten er volgens het NCSC van uitgaan dat hun systemen waren binnengedrongen.

NCSC schaalt op

Het NCSC constateerde op 11 januari dat op 10 januari *exploit codes* waren gepubliceerd waarmee de kwetsbaarheden konden worden misbruikt. Daarop actualiseerde NCSC nogmaals zijn beveiligingsadvies voor zijn doelgroepen en het brede publiek. Vanwege de signalen dat er veel kwetsbare servers in Nederland waren die konden worden binnengedrongen, schaalde NCSC op 13 januari op van de reguliere operatie naar een *event team*.[71]

Op dat moment was het beeld van het event team dat de betreffende Citrix-software door zeer veel organisaties gebruikt werd, maar er was geen volledig beeld van welke organisaties Citrix-software gebruikten en nog kwetsbaar waren. Binnen NCSC heerste twijfel of de mitigerende maatregelen van fabrikant Citrix effectief waren. Daarbij hadden meerdere organisaties deze niet doorgevoerd. Het event team zette in op het breed informeren van organisaties over de kwetsbaarheden.

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 een inlichtingenbericht.

DIVD scant en waarschuwt organisaties met kwetsbare servers in Nederland

DIVD activeerde op 11 januari een Security Meldpunt op (tegenwoordig DIVD CSIRT genaamd). Vanuit dit meldpunt benaderden zij aanvankelijk zelf organisaties met kwetsbare Citrix-servers door automatisch een e-mail met een waarschuwing en een

70 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. Die kaders geven aan dat persoonsgegevens of daartoe herleidbare informatie alleen met organisaties kunnen worden gedeeld, die als OKTT of CERT zijn aangewezen.

71 Update beveiligingsadvies: https://www.ncsc.nl/actueel/advisory?id=NCSC-2019-0979 update 11 januari 2020. NCSC kent verschillende opschalingsniveaus. In de basis worden incidenten afgehandeld door *incident handlers* die kleine problemen bij organisaties oppakken. Als incidenten te groot worden om binnen de reguliere werkzaamheden te kunnen uitvoeren, wordt er opgeschaald. De eerste trede is het *event team*, een specifiek team dat tijdens kantooruren wordt ingezet om de reguliere operatie te ontlasten. Als het urgenter is of er is een groter probleem, wordt er opgeschaald naar een *calamiteitenteam*, waarbij ook buiten kantoortijden kan worden doorgewerkt. In 2020 schaalde NCSC twee keer op naar die hoogste trede: tijdens het Citrix-voorval en tijdens het SolarWinds-voorval. Er kan nog verder opgeschaald worden naar crisis, dan neemt NCTV de coördinatie over.

advies te sturen naar de vermoedelijke mailadressen van de organisaties die horen bij de kwetsbare IP-adressen. Ook stuurde DIVD de lijst met kwetsbare IP-adressen door naar internet providers (netwerkeigenaren), met name KPN en Nationale Beheersorganisatie Internet Providers (NBIP)[72], naar sectorale CERT's, zoals het CERT van de zorg (Z-CERT) en naar het NCSC. Na de scans van het DIVD en andere partijen bracht het CSIRT-DSP de gecomprimiteerde partijen uit zijn eigen doelgroep (digitale dienstverleners) direct op de hoogte.

NCSC stuurt organisaties bericht dat ze al gecompromitteerd kunnen zijn

Op 13 januari stuurde NCSC opnieuw een bericht aan zijn doelgroepen en op 14 januari publiceerden zij een bericht op hun website.[73] In dat nieuwsbericht adviseerde NCSC met klem om zo snel mogelijk de mitigerende maatregelen toe te passen, zoals geadviseerd door Citrix. Ook wanneer deze maatregelen recent al waren toegepast, waarschuwde het NCSC alsnog voor de mogelijkheid dat aanvallers toegang konden hebben tot hun systemen. NCSC kreeg vanuit meerdere organisaties vragen om meer toelichting bij het bericht.

Nederlandse organisaties melden gecompromitteerd te zijn

Op 14 januari meldde het CERT van de gemeenten, IBD, aan NCSC dat er misbruik was geconstateerd bij een gemeente. De Citrix-servers waren aangevallen en daarom was besloten de systemen af te sluiten. NCSC kreeg op 15 januari bericht dat een ziekenhuis eveneens aangevallen was en het daarom al het dataverkeer met de buitenwereld had afgesloten. Medewerkers konden niet thuiswerken en patiënten konden niet bij hun patiëntendossier. In de media was veel aandacht voor het Citrix-lek. Externe experts meldden aan het NCSC dat organisaties zeker binnengedrongen zijn als ze niet voor 9 januari maatregelen hadden genomen. Meer berichten van organisaties waar aanvallers de systemen waren binnengedrongen volgden: railsector, politiemeldkamer, gemeenten en een ziekenhuis. Het NCSC ontving een lijst met kwetsbare IP-adressen van Citrix en richtte de focus op het adviseren en informeren van de doelgroepen. De media-aandacht groeide en daarmee ook de druk op NCSC, hetgeen zich onder meer uitte in veel organisaties die vragen hadden voor NCSC.

NCSC adviseert: overweeg Citrix-servers uit te zetten

Zoals beschreven in 3.1.1 bracht fabrikant Citrix op 16 januari een bericht naar buiten waarin stond dat de mitigerende maatregelen bij één versie van de software niet werkten. Een dag later corrigeerde de fabrikant dat bericht via een bulletin update.

NCSC publiceerde op 16 januari het advies om te overwegen de Citrix-servers uit te zetten, afhankelijk van de impact die dat zou hebben op de organisatie in kwestie.[74] Aanleiding was onder meer de twijfel of de eerder door Citrix geadviseerde mitigerende maatregelen voldoende zekerheid boden en het vermoeden dat veel organisaties de

72 Met behulp van een geautomatiseerd script dat mails stuurde naar info@, abuse@ en security@ mailadressen die hoorden bij het betreffende IP-adres en het daaraan gekoppelde domein. NBIP is opgericht door internet service providers als collectieve manier om met tapverzoeken om te gaan. Sindsdien hebben ze ook een systeem ontwikkeld om DDoS aanvallen af te slaan. https://www.nbip.nl/en/about-the-nbip/

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

74 Dit bericht is niet meer beschikbaar op de website van NCSC. De titel is 'door Citrix geadviseerde mitigerende maatregelen niet altijd effectief', verstuurd op 16 januari 2020. Het bericht is opgenomen in bijlage C.

mitigerende maatregelen nog niet of niet volledig hadden uitgevoerd. Op basis van dit advies schakelden onder andere de Tweede Kamer, Schiphol, verschillende ministeries en andere overheidsinstellingen, een aantal grote gemeenten en particuliere bedrijven hun Citrix systemen uit. Het NCSC kreeg veel vragen van zowel doelgroeporganisaties als organisaties buiten zijn doelgroep die naar aanleiding van het advies nader geïnformeerd wilden worden. Er was bij deze organisaties onrust ontstaan over de betrouwbaarheid van de mitigerende maatregelen die Citrix adviseerde.

Opschaling naar nationale crisisstructuur en advies AIVD
Vanwege de ernst van de situatie besloot het Nationale Crisis Centrum (NCC) deels op te schalen in de nationale crisisstructuur door het Interdepartementaal Afstemmingsoverleg (IAO) bijeen te roepen. De NCTV coördineerde deze interdepartementale afstemming. Het team binnen NCSC schaalde op naar het niveau 'calamiteit' en het calamiteitenteam werd samengesteld.

Op 17 januari brachten MIVD en AIVD een inlichtingenbericht uit aan NCTV en NCSC, waarin stond dat zij acute dreiging van statelijke actoren richting een organisatie binnen de Rijksoverheid hadden waargenomen. Vanuit het kabinet werden de minister van BZK en de minister van JenV gemandateerd om de crisis te bestrijden.

In de middag bleek dat AIVD en NCSC van inzicht verschilden over het uit te brengen veiligheidsadvies aan de Rijksoverheid, waardoor er twee verschillende adviezen voor lagen: de AIVD wilde dat NCSC organisaties zou adviseren om alle Citrix-servers uit te zetten, omdat volgens hen de patch niet voor alle versies van de Citrix- software volledig werkte, terwijl NCSC organisaties wilde adviseren om op basis van hun specifieke situatie een eigen afweging te maken.

NCSC publiceert dringend advies: zet Citrix-servers uit
Op basis van de twee verschillende adviezen besloten de ministers van JenV en van BZK in samenspraak met de NCTV op 17 januari om het eerdere advies van NCSC te verzwaren en de lijn van het AIVD-advies te volgen. NCSC moest het dringende advies uitbrengen aan de Rijksoverheid en de vitale organisaties om Citrix-servers uit te schakelen vanwege de onzekerheid over de door Citrix geadviseerde maatregelen en de waargenomen dreiging. Uitgangspunt van het advies van NCSC was het '*comply or explain*' (Pas toe of Leg uit) principe. CIO Rijk paste dit toe bij de Rijksoverheid. Het advies gold totdat een effectieve oplossing beschikbaar was. NCSC verspreidde het advies breed via een doelgroepbericht, een persbericht op rijksoverheid.nl, de website van het NCSC en via andere cybersecurity-organisaties in Nederland.

Elke afzonderlijke organisatie moest zelf een afweging maken wat de impact was en stond aan de lat voor de eigen maatregelen en een eigen *'explain'* wanneer gekozen werd de Citrix-servers niet werd uit te schakelen. De rijksoverheidspartijen moesten hun *'explain'* voorleggen aan CIO-Rijk ter beoordeling. Voor de vitale aanbieders gold dat het NCSC advies en hulp kon aanbieden waar mogelijk. Het NCSC had eveneens overleg met Citrix over de situatie. Indien gekozen werd voor '*comply*' was de impact vanwege het uitschakelen van Citrix–servers op de werkzaamheden wisselend. In veel gevallen was thuiswerken niet meer mogelijk waardoor er een grote toestroom naar de kantoren

zou ontstaan en moest het verkeer rekening houden met een zeer drukke spits, in sommige organisaties zou het uitschakelen meer ingrijpende gevolgen hebben.

Het dringend advies van NCSC was gebaseerd op een beveiligingsadvies van de AIVD. Het onderliggende inlichtingenbericht bevatte informatie die was gerubriceerd als staatsgeheim en was daarmee niet openbaar. Het beveiligingsadvies zelf was niet gerubriceerd. Het NCSC communiceerde niet met andere organisaties over de inhoud van het beveiligingsadvies vanwege de rubricering van de informatie. Bij organisaties die het NCSC-advies ontvingen, ontstond verwarring over het advies van 17 januari omdat het advies afweek van het eerder uitgebracht advies van de NCSC van 16 januari, namelijk het minder dringende advies om te overwegen Citrix-servers uit te schakelen. Het advies van het NCSC had in die zin een meer dringend karakter dan het advies van Citrix zelf, van beveiligingsbedrijven die de organisaties adviseerden, zoals Fox-IT, en van nationale CERTs en beveiligingsbedrijven in andere landen. Organisaties gaven aan dat zij niet konden inschatten of het verzwaarde advies ook voor hen gold en of zij actie moesten ondernemen. NCSC kon de inhoud van het beveiligingsadvies van de AIVD aanvankelijk niet delen met de organisaties buiten de Rijksoverheid vanwege de rubricering. AIVD derubriceerde het bericht op 20 januari. Dit vormde voor NCSC geen aanleiding om het beveiligingsadvies alsnog te delen.

Organisaties zetten al dan niet Citrix-servers uit

De gevolgen van het uitzetten van de Citrix-servers verschilden per organisatie. Voor sommige organisaties, zoals departementen, was het gevolg beperkt tot niet kunnen thuiswerken.[75] Bij een aantal gemeenten konden als gevolg van het uitzetten van de Citrix-servers geen toelagen binnen het sociaal domein meer worden uitgekeerd aan inwoners. Het ministerie van EZK had de Citrix-servers aan laten staan, omdat ze vonden dat ze tijdig voldoende maatregelen had genomen en omdat uitzetten zou betekenen dat de NVWA dan geen inspecties en douane controles meer kon uitvoeren, waardoor onder meer de vleesproductie en –handel stil zouden komen te liggen. In ziekenhuizen konden patiënten geen toegang meer krijgen tot hun elektronisch patiëntendossier en was in sommige gevallen geen communicatie met andere ziekenhuizen mogelijk. Er waren ook organisaties die weinig tot geen hinder ondervonden van het voorval: de Citrix-servers speelden een beperkte rol in hun digitale systeem of ze hadden een alternatief beschikbaar.

75 Hierbij dient te worden opgemerkt dat het voorval plaatsvond enkele maanden voordat vanaf maart 2020 de meeste medewerkers thuis moesten werken vanwege de COVID-19 pandemie. De gevolgen van een dergelijk voorval zouden daardoor nu veel ingrijpender zijn dan in januari 2020.

Afhankelijkheid van Citrix-software groter dan gedacht
Vele bedrijven en ministeries gebruiken Citrix-servers om daar hun interne programma's en applicaties op te laten draaien of ze hebben leveranciers die met Citrix-software werken. Het is een knooppunt van allerlei applicaties dat diep in de ICT-voorziening van organisaties zit. Citrix-software is vooral bekend als toepassing voor thuiswerken. Maar het wordt ook gebruikt als toegangsvoorziening voor bijvoorbeeld e-mail en kantoorapplicaties of voor primaire processen.

Een overheidsorganisatie maakte na het dringende advies van NCSC een risicoanalyse om te beslissen of de systemen uitgeschakeld moesten worden. Na het uitzetten bleken er meer processen afhankelijk te zijn van Citrix dan vooraf ingeschat: 60 tot 70 procent van de afhankelijkheden van Citrix-software waren bij de risicoanalyse in beeld had gebracht. De afhankelijkheid van de Citrix-servers bleek zo groot, dat na het uitschakelen uiteindelijk geen enkel digitaal bedrijfsproces meer doorgang kon vinden.

Vanaf 9 januari had CIO Rijk de CIO's, CISO's en CTO's van het Rijk opgeroepen de beveiligingsadviezen van NCSC op te volgen en gevraagd om aan CIO Rijk de status van de opvolging door te geven: had de organisatie de Citrix-servers uitgezet en zo nee, wat was daarvoor de onderbouwing.

Na het advies van 17 januari begon CIO Rijk een situatiebeeld van de opvolging op te stellen ten behoeve van het IAO). De meerderheid van de rijksoverheidsorganisaties (61%) die in beeld waren hadden de Citrix-servers uitgezet, een klein deel (20%) had de Citrix-servers aan laten staan met als argumentatie dat de nationale veiligheid in geding kwam, het departement een meerlaagse beveiliging had of er een te grote impact op kritische processen of maatschappelijke of economische schade zou kunnen ontstaan. 19% Van de organisatieonderdelen binnen de rijksoverheid maakte geen gebruik van Citrix. JenV en BZK benaderden sectorale CERTs om een beeld te krijgen van de mate waarin hun achterban het advies van NCSC had opgevolgd om de Citrix-servers uit te zetten.

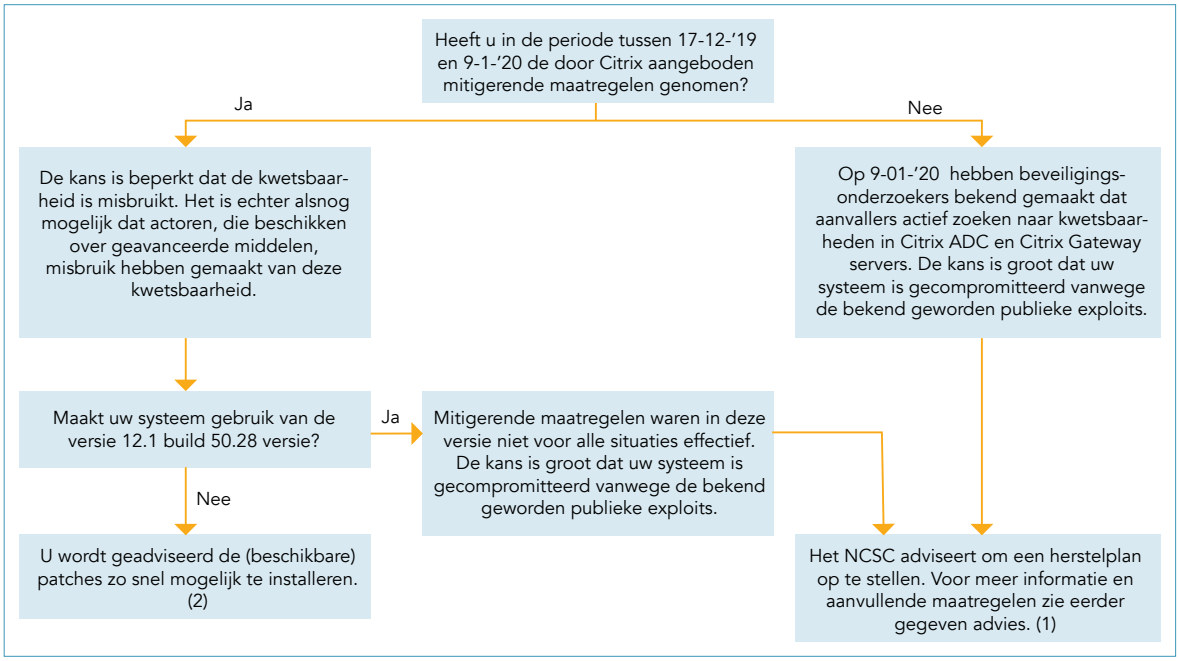
Situatiebeeld Citrix-servers bij de overheid
Vrijwel alle doelgroeporganisaties van het NCSC, zoals de Rijksoverheid en de Tweede kamer, maakten gebruik van Citrix-software:
- 10 van de 12 ministeries;
- 56 van de 69 rijksorganisaties. Daarvan hebben 42 de Citrix-servers uitgeschakeld.

Overige overheden:
- 150-200 van de 352 gemeenten, daarvan heeft 80% de Citrix-servers uitgeschakeld;
- 9 van de 12 provincies gebruikten, alle hebben uitgeschakeld;
- alle 22 waterschappen gebruikten Citrix. Het merendeel heeft Citrix uitgeschakeld, enkele zijn operationeel gebleven, vanwege zwaarwegende redenen;
- 16 van de 25 veiligheidsregio's gebruikten Citrix-software.

Organisaties starten met patchen van kwetsbare servers

Na in het weekend doorlopend activiteiten rondom Citrix te hebben uitgevoerd, kwam het calamiteitenteam van het NCSC op 18 januari 2020 weer bijeen waarbij zij tevens de toenemende media-aandacht constateerde.

Citrix maakte op 19 januari de eerste patches beschikbaar en NCSC adviseerde de organisaties dringend de patches uit te voeren. Deze patches waren voor een deel van de Citrix versies geschikt, ongeveer 50 % van de kwetsbare Citrix-systemen in Nederland. Het advies van het NCSC bleef gehandhaafd: zet de Citrix-servers uit of motiveer waarom niet. Daarnaast gaf NCSC advies in relatie tot aangekondigde patches en hoe weer te komen tot veilige werkomgevingen. NCSC gaf aan dat organisaties ervan uit moesten gaan dat ze waren gecompromitteerd als ze niet tijdig de juiste maatregelen hadden genomen (zie 3.1.1: tijdig is voordat de methode om misbruik te maken openbaar werd). Zie verder onderstaand stroomdiagram die NCSC op 20 januari publiceerde zodat organisaties zelf een risicoanalyse met betrekking tot de Citrix kwetsbaarheid konden uitvoeren.



Figuur 12: Stroomschema Citrix. (Bron: NCSC)[76]

Er volgde een rijksbrede mail met werkinstructie aan rijksambtenaren met betrekking tot de impact en het handelingsperspectief. Binnen NCSC vond discussie plaats of ze zelf zouden mogen scannen om na te gaan welke organisaties nog kwetsbaar waren. Vanwege de technische risico's en juridische beperkingen besloot NCSC dit niet te doen (in paragraaf 4.3 gaan we verder op in op deze beperkingen). Bij dat besluit speelde ook mee dat het centrale uitgangspunt in de cybersecurity strategie is dat organisaties zelf verantwoordelijk zijn voor monitoring van de Citrix-omgeving en de achterliggende systemen.

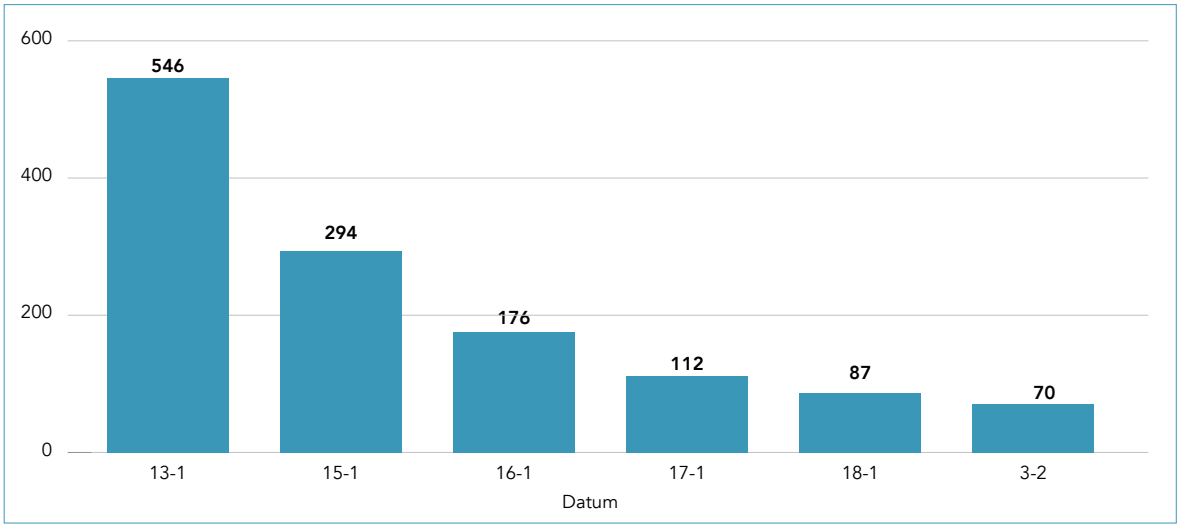
76 https://www.ncsc.nl/documenten/publicaties/2020/januari/20/stroomschema-risicoafweging-citrix.

Toen op 21 januari verschillende organisaties die Citrix-software gebruikten aan NCSC meldden dat zij malware hadden gevonden op hun systemen en om ondersteuning vroegen bij forensisch onderzoek, besloot NCSC dat het zich vanwege capacitaire overwegingen beperkte tot de wettelijke taak en niet andere organisaties niet zou ondersteunen. Organisaties moesten zich wenden tot beveiligingsbedrijven met forensische expertise. Deze waren echter op dat moment al volledig bezet met het helpen van hun bestaande klanten, waardoor een deel van de organisaties niet meteen kon worden ondersteund.

Ook startte NCSC in samenwerking met een aantal operationele partners met het testen van de door Citrix opgeleverde patches en eerder geadviseerde mitigatiemaatregelen. Op 24 januari stuurde NCSC een bericht aan zijn doelgroepen dat het geverifieerd had dat de nieuwe patches werkten. In het doelgroepenbericht en op de website plaatste NCSC het advies om een forensisch onderzoek te laten doen. Daarnaast bleef voor de rijksoverheidsorganisatie de richtlijn van kracht om het aan CIO Rijk en NCSC te melden als de organisatie de Citrix-servers weer ging opstarten.

DIVD blijft monitoren en waarschuwen

Het Security Meldpunt van DIVD had op 15 januari ook advies uitgebracht aan organisaties binnen Nederland over hoe ze konden controleren of een systeem waarbij de mitigatie na 11 januari was toegepast al overgenomen was. Afhankelijk van de ernst van de aanval is het voor een organisatie nodig forensisch onderzoek te doen of zelfs over te gaan tot het volledig opnieuw installeren van het systeem. Ook in de maanden na het uitbrengen van de patches erna bleef DIVD scannen op kwetsbare servers. Het aantal kwetsbare servers nam af. Op 3 februari 2020 waren er nog 70 kwetsbare servers, begin maart 2020 nog vijf. Nieuwe vrijwilligers bij DIVD hebben deze organisaties nogmaals gebeld en de betreffende beheerders alsnog gewaarschuwd of daartoe een verzoek achtergelaten bij de receptioniste.[77]



Figuur 13: Niet-gemitigeerde Citrix-servers, gevonden door DIVD CSIRT. (Bron: divd.nl)

77 Advies Security Meldpunt DIVD: https://csirt.divd.nl/2020/01/15/How-to-check-your-Citrix-gateway/ In de praktijk bleek dat organisaties nog niet bekend waren met het Security Meldpunt van DIVD. Daardoor werden de beveiligingsonderzoekers niet altijd doorverbonden met de betreffende IT-beheerder.

Politieke nasleep en afschalen
Op 20 januari kwam de Interdepartementale Commissie Crisisbeheersing (ICCb) bijeen. In de ICCb werd de problematiek rondom Citrix besproken. Door middel van de kamerbrief 'Kwetsbaarheid in Citrixproducten' informeerde de minister van JenV en minister van BZK de Tweede Kamer over de geconstateerde kwetsbaarheid in Citrix producten, de waarschuwing en het advies van het NCSC.

De minister van JenV stuurde naar aanleiding van het mondeling vragenuur van 21 januari op 23 januari een feitenrelaas over de kwetsbaarheid in Citrix-software naar de Tweede Kamer en verzorgde een technische briefing. Op 24 januari wees de minister van JenV via een ministeriële regeling vier sectorale CERT's[78] aan waarmee NCSC intensiever informatie zou mogen uitwisselen.

Op 29 januari vond het zevende en laatste Interdepartementale Afstemmingsoverleg plaats. Vanaf dat moment werd de crisisorganisatie afgeschaald en werden de activiteiten rondom de kwetsbaarheid in de Citrix-software zowel binnen NCSC als de gehele rijksoverheid weer via de reguliere lijn uitgevoerd. Op 31 januari 2020 hadden de meeste departementen alle systemen weer aangezet. Bij een aantal onderdelen was een herstelplan nodig voordat terug gegaan mocht worden naar de normale werksituatie. NCSC en de CIO Rijk richtten wel een taakgroep in die de activiteiten rondom de kwetsbaarheid in de Citrix-software verder beheerste en afrondde.

Deel organisaties dat maatregelen nam bleek alsnog binnengedrongen
Op 1 juli 2020 publiceerde beveiligingsbedrijf Fox-IT dat zij hadden vastgesteld dat 25 Nederlandse servers nog steeds waren binnengedrongen via de kwetsbaarheid in de Citrix-software. De betreffende organisaties hadden wel de patch uitgevoerd, maar waren daarvoor al binnengedrongen. Criminele aanvallers en/of statelijke actoren hadden bij de betreffende organisaties toegang tot het interne netwerk. Daarbij ging het onder meer om een bedrijf dat watermerken maakt voor bankbiljetten en een farmaceutisch bedrijf, aldus de Volkskrant.[79]

3.2 Analyse voorval met Citrix-software

In de analyse van het voorval beantwoorden we de volgende onderzoeksvragen:
- Hoe konden de beveiligingslekken als gevolg van kwetsbaarheden in Citrix-software ontstaan en welke gevolgen hadden ze?
- Op welke manier werden deze risico's beheerst door fabrikant en gebruikers?
- Wat was daarin de rol van de overheid en niet-overheidspartijen?

Eerst beschrijven we wat de kwetsbaarheid in de software inhield, hoe deze in de software kan bestaan zonder ontdekt te worden en hoe dit kon leiden tot een beveiligingslek in een digitaal systeem. In de volgende subparagrafen worden de

78 De computercrisisteams voor de zorg (Z-CERT), gemeenten (Informatiebeveiligingsdienst IBD), waterschappen (CERT Watermanagement) en onderwijs en onderzoek (SURFcert).
79 https://blog.fox-it.com/2020/07/01/a-second-look-at-cve-2019-19781-citrix-netscaler-adc/ https://www.volkskrant.nl/nieuws-achtergrond/half-jaar-na-citrix-crisis-zijn-25-nederlandse-organisaties-gehackt-en-ze-weten-zelf-van-niets.

factoren geanalyseeerd die het betekenisvol maken dat de Citrix-software deze kwetsbaarheid bevatte, hoe de fabrikant reageerde op dit incident en hoe het incident werd bestreden.

3.2.1 Beveiligingslek als gevolg van kwetsbaarheid in Citrix-software

De kwetsbaarheid in de Citrix-software bestond uit een combinatie van meerdere kleine kwetsbaarheden.[80] De consequentie was dat bij organisaties die deze Citrix-software op een bepaalde manier hadden toegepast in hun netwerk, onbevoegde gebruikers zich mogelijk door het gehele netwerk konden verplaatsen en de instellingen zo konden aanpassen dat zij zelf software code op het netwerk konden zetten en deze code op afstand konden uitvoeren. De kwetsbaarheden maakten het daarmee voor aanvallers mogelijk om beveiligingslagen te omzeilen en op afstand malafide code uit te voeren op het netwerk van de betreffende organisatie.

Met behulp van de kwetsbaarheid konden onbevoegde gebruikers (waaronder aanvallers) zich mogelijk toegang verschaffen tot alle onderdelen van de Citrix-*appliance*. Bij servers die toegankelijk zijn vanaf het internet is het gebruikelijk dat de *appliance* zo wordt geconfigureerd om dat te voorkomen: de rest van het netwerk wordt dan afgeschermd en is niet toegankelijk voor gebruikers van buitenaf. Dit kan op twee manieren:

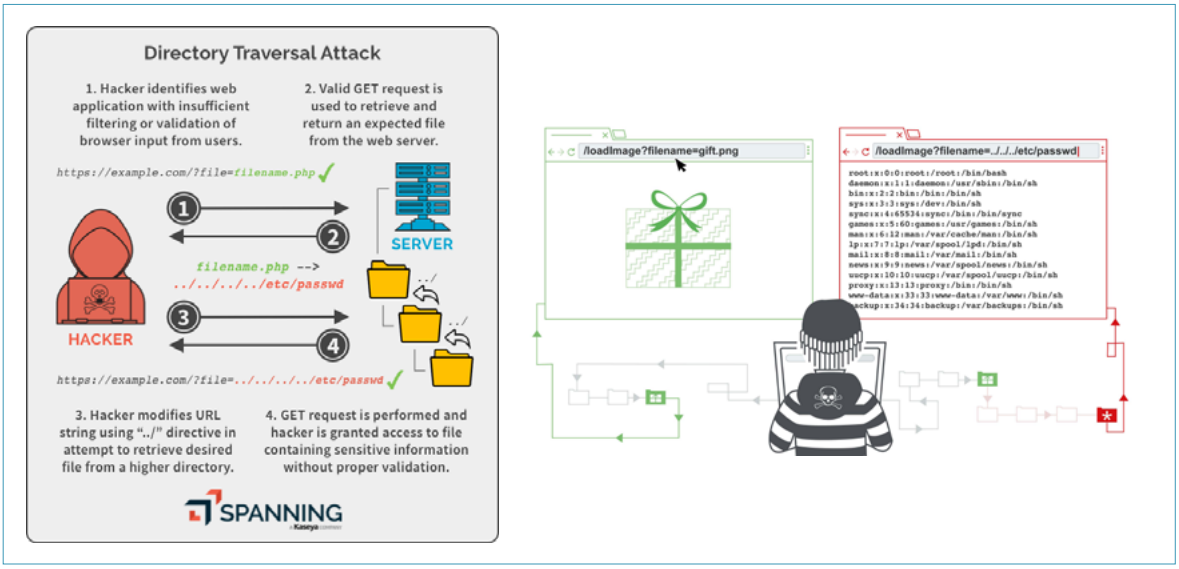
- gebruikers niet de mogelijkheid te geven een commando te geven aan de *appliance* om zich door alle onderdelen van de webserver te verplaatsen en waarmee de gebruiker zich toegang kan verschaffen tot afgeschermde delen van het netwerk en
- gebruikers geen rechten te geven om de complete mappenstructuur te bekijken.

Deze maatregelen kunnen worden ingesteld door de organisatie die de Citrix-*appliance* beheert, en de maatregelen kunnen ook door de fabrikant worden afgedwongen door de configuratie van de Citrix-software.[81] De mate waarin de kwetsbaarheid tot een beveiligingslek kon leiden hing af van de standaardinstellingen en de wijze waarop de organisatie die de software gebruikte de Citrix-*appliance* op deze manier de rechten van de gebruikers had beperkt. Als de organisatie dit niet had gedaan, dan was het voor een aanvaller mogelijk om alle onderdelen van de *appliance* te benaderen. Een niet-geauthentiseerde gebruiker kreeg daarmee dezelfde rechten als een beheerder, namelijk toegang tot alle mappen op de *appliance* (zie figuur 14) Niet alleen toegang om te kijken, maar ook om zelf programma's uit te voeren op het netwerk. De kwetsbaarheid waardoor een aanvaller op deze manier te werk kan gaan staat bekend als *path traversal*.[82] Aanvallers konden door gebruik te maken van de mogelijkheid van *path traversal* bepaalde toegangsmaatregelen omzeilen en niet-geauthentiseerd in anders afgezonderde paden komen en programma's uitvoeren. Met *path traversal* alleen was het niet mogelijk om bestanden uit te lezen.

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

81 Een *network appliance* is een apparaat dat de gegevensuitwisseling ondersteunt tussen apparaten die met elkaar verbonden zijn via een netwerk.

82 De aanvaller kon *path traversal* uitvoeren door de code '/../' in het pad van de webserver in te voeren.



Figuur 14: Directory/path traversal attack.[83]

3.2.2 De Citrix-software had in de loop van de tijd een veiligheidskritische functie gekregen

De beveiligingslekken bij organisaties waren mede het gevolg van kwetsbaarheden in een serie softwareproducten van Citrix, namelijk de *Citrix Application Delivery Controller* (ADC). Deze productserie kent een lange geschiedenis. ADC is een product dat in 1997 werd ontwikkeld door NetScaler om bedrijven als Google en Amazon te helpen hun hardware efficiënter aan te sturen, zodat met de groei van het internet de hoeveelheid benodigde hardware beperkt kon blijven. Het product werd gebaseerd op een aantal open source componenten. In 2005 werd het bedrijf NetScaler gekocht door Citrix, om een gat in de productenlijn te vullen. Gaandeweg voegde de fabrikant functionaliteiten aan het product toe en gingen afnemers het product op een andere manier gebruiken. Het product ontwikkelde zich en kreeg extra functies, zoals het verkeer doorsturen naar applicaties en verdelen over servers in het achterliggende netwerk, een firewall, het opzetten van VPN-verbindingen en authenticatie van gebruikers die van het achterliggende netwerk gebruik mogen maken. Het product is daarmee gaandeweg de toegangspoort tot het netwerk van de organisatie geworden.[84] Software die gepaard gaat met een dergelijke dynamiek vraagt adaptief risicomanagement van de fabrikant.In dit geval gaf Citrix aan dat het werkte met een *Secure Development Lifecycle* programma als sleutelonderdeel van zijn raamwerk voor productontwikkeling. Paragraaf 4.1 gaat verder in op dit onderwerp.

3.2.3 Derden vonden de kwetsbaarheid voordat de fabrikant deze vond

De PoC-code die beveiligingsonderzoekers in december 2019 met Citrix deelden, toonde een kwetsbaarheid aan in de ADC en Gateway. Door een gedeelde oorsprong van deze beide producten was dezelfde kwetsbaarheid in beide producten aanwezig. De kwetsbaarheid in de ADC en Gateway was nog niet bekend bij de fabrikant. Beveiligingsonderzoekers melden een kwetsbaarheid niet altijd bij de fabrikant zelf.

83 Bron afbeeldingen: (l) https://spanning.com/blog/directory-traversal-web-based-application-security-part-8/ (r) https://portswigger.net/web-security/file-path-traversal)

84 Citrix, *video The Citrix ADC story*, https://www.youtube.com/watch?v=HEWmy9-te2I, 29 november 2018.

Soms wordt de kwetsbaarheid gevonden door eigen onderzoek of door onderzoek in opdracht van een organisatie die de software gebruikt. Net als veel andere software fabrikanten stimuleert Citrix dat beveiligingsonderzoekers kwetsbaarheden direct aan hen melden, ook om te voorkomen dat de kwetsbaarheden aan derden worden verkocht of ter beschikking worden gesteld. De handel in kwetsbaarheden is lucratief en ondoorzichtig. Het is daardoor mogelijk dat derden kwetsbaarheden in een software product kennen en misbruiken zonder dat de fabrikant daar zelf van op de hoogte is gebracht. Ook in dit geval werd gemeld dat de kwetsbaarheid al circuleerde zonder dat Citrix daarvan op de hoogte was.

3.2.4 Mitigerende maatregel voorafgaand aan definitieve patches

Zoals in paragraaf 3.1 beschreven had Citrix van de bronnen vernomen dat de methode om de kwetsbaarheid te misbruiken al rondging op bepaalde online kanalen. De fabrikant vond het daarom van belang om de kwetsbaarheid zo snel als mogelijk te verhelpen. Het *response team* van Citrix dat als eerste naar dergelijke meldingen kijkt en deze beoordeelt, nam eerst contact op met het *product security incident response team* (PSIRT). Dit team is gespecialiseerd in het behandelen van veiligheidsincidenten voor de diverse producten in het portfolio van Citrix. Achtereenvolgens werd ook het *product R&D team* van Citrix ingeschakeld, verantwoordelijk voor het ontwikkelen van nieuwe software en patches. Uit overleg tussen deze afdelingen en verdere analyse van het R&D team bleek een snelle, permanente oplossing niet voorhanden. Doordat de kwetsbaarheid in meerdere producten en meerdere versies zat, moesten verschillende patches ontwikkeld worden. De inschatting van Citrix was op dat moment dat meerdere maanden nodig waren voor het gereedmaken van alle patches en het doorlopen van de testcycli. De fabrikant schatte in dat dit veel tijd zou kosten doordat de validatie van dit soort *security fixes* diepe kennis van het product vereist en hiervoor binnen het bedrijf een beperkt aantal engineers beschikbaar is.

Patches moeten een testcyclus doorlopen voordat de fabrikant ze kan verstrekken aan de gebruikers (*release*). Voor het repareren van de kwetsbaarheid maakte de fabrikant een nieuwe versie (*build*) van de software. Deze activiteit zou enkele dagen in beslag nemen. Gegeven de complexiteit van de issues en de te nemen maatregelen, had de fabrikant één team beschikbaar dat de automatische tests en handmatige validaties kon doen van alle patches voor alle verschillende versies van het product (en omdat de kwetsbaarheid al ruim tien jaar in de productlijn zat, ging het om veel verschillende versies). De fabrikant had niet voldoende engineers in huis om de ontwikkeling, tests en validaties van de patches voor verschillende versies over verschillende teams te verdelen, zodat verschillende versies parallel aan elkaar ontwikkeld konden worden. Daardoor konden de patches voor de verschillende productversies alleen na elkaar worden ontwikkeld. Vanwege de tijd die het duurde om de patches te ontwikkelen, besloot de fabrikant tot maatregel om de kwetsbaarheid te mitigeren als maatregel om het effect van de kwetsbaarheid te verhelpen.

3.2.5 Publicatie mitigerende maatregel maakte exploit eenvoudig

De mitigerende maatregel die Citrix voorschreef bevatte informatie die nodig was om de mitigatie uit te voeren. Het publiceren van mitigerende maatregelen is gebruikelijk, maar kan zoals in dit geval duidelijk maken hoe de kwetsbaarheid kan worden geëxploitateerd. In de mitigerende maatregel werd namelijk voorgeschreven hoe de configuratie van de webserver moest worden aangepast om misbruik tegen te gaan: zorg ervoor dat het commando /../ wordt tegengehouden. Ook maakte de mitigerende maatregel bekend waar het *'path'* zich bevond zodat duidelijk is in welk deel van de software moet worden gezocht. Voor potentiële aanvallers werd door publicatie van de mitigerende maatregel duidelijk dat de kwetsbaarheid zat in de afhandeling van verzoeken (door de server) waarbij *path traversal* wordt gebruikt.[85]

3.2.6 Fabrikant bereikte niet alle afnemers

De fabrikant besloot om naast het publiceren van de mitigerende maatregelen te proberen zo veel mogelijk klanten rechtstreeks te waarschuwen. Op dat moment had de fabrikant nog niet de mogelijkheid om grote groepen klanten te contacteren. Dit was alleen mogelijk bij klanten die zich reeds hadden geregistreerd om securitywaarschuwingen te ontvangen. De fabrikant beschikte over de contactgegevens van een klein deel van de organisaties die zijn software gebruikt (10%). Voor de klanten waar wel contactgegevens van waren wist de fabrikant niet of deze gegevens nog actueel waren. Softwarefabrikanten weten niet altijd wie de software gebruikt, omdat het grootste deel van de verkoop verloopt via partners.

Bij klanten waar de fabrikant wel contactgegevens van had, bleek dit vaak niet de persoon die verantwoordelijk was voor de beveiliging, maar bijvoorbeeld de receptionist of de inkoopafdeling. De fabrikant leerde hieruit dat het belangrijk is om de contactgegevens te hebben van de functionarissen die gaan over de beveiliging, omdat anders het risico bestaat dat de informatie over de kwetsbaarheid in verkeerde handen terecht komt of niet de mensen binnen de organisatie bereikt die maatregelen kunnen nemen. Een andere belemmering was dat sommige partners willen dat Citrix hun klanten niet rechtstreeks benadert, en dat andere klanten dat ook niet willen, bijvoorbeeld om aansprakelijkheid te voorkomen doordat de organisatie wel door de fabrikant was gewaarschuwd maar geen maatregel nam.

3.2.7 NCSC kon geen eigen beeld vormen van de gebruikers van Citrix-software in Nederland en van de effectiviteit van de mitigerende maatregelen

Tijdens dit voorval konden organisaties worden gewaarschuwd op basis van informatie die werd verzameld door beveiligingsonderzoekers die het internet scanden op zoek naar servers die nog kwetsbaar waren. Zo kwam veel scan informatie binnen van derden waaronder DIVD en *Bad Packets* (door NCSC aangeduid met 'telefoonboeken' vanwege de omvang van deze lijsten). NCSC scande zelf niet, ook niet de systemen van de eigen doelgroep (rijksoverheid en vitale aanbieders). omdat daar binnen de organisatie juridische bezwaren tegen waren geuit. Ook maakte de interpretatie van het wettelijk kader dat het NCSC de gegevens niet doorgaf aan de organisaties die deze groepen vertegenwoordigen. Het NCSC informeerde de organisaties die tot de eigen doelgroep (Rijksoverheid en Vitaal) behoorden die uit deze lijsten afgeleid konden worden. Op

85 Zie bijvoorbeeld https://northwave-security.com/threat-response-citrix-gateway-adc-rce-cve-2019-19781/.

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. Dit werd gedaan op grond van de potentiele maatschappelijke impact of op grond van het maatschappelijk belang.

Op een cruciaal moment tijdens de incidentbestrijding, toen de situatie in Nederland maatschappelijk en bestuurlijk escaleerde op 16 januari, ontstond onduidelijkheid doordat Citrix per abuis publiceerde dat de mitigerende maatregelen niet altijd werkten. Daardoor verloor NCSC het vertrouwen in de mitigerende maatregelen.[86] Dit speelde naast de informatie van de AIVD een rol bij het formuleren van het verregaande advies om de Citrix-servers uit te zetten. Er kwamen berichten van organisaties dat de mitigatie niet effectief was, echter op afstand kon NCSC niet eigenstandig beoordelen of dat kwam doordat de mitigatie niet goed was uitgevoerd. NCSC had geen middelen om de betrouwbaarheid van de mitigerende maatregelen zelf vast te stellen, ze waren afhankelijk van informatie van derden. De middelen waren wel aanwezig bij Defensie, en daar is ook gebruik van gemaakt. Beveiligingsbedrijven, waaronder Fox-IT, bleven (ook in het openbaar) vasthouden dat er geen reden was om aan te nemen dat de mitigatie niet in alle gevallen zou werken, gebaseerd op de aard van de mitigatie die de mogelijkheid om misbruik te maken volledig zou wegnemen en gebaseerd op de eigen ervaringen met klanten.[87] Toen de patches uitkwamen had NCSC wel georganiseerd dat zij informatie kreeg waarmee ze uitspraken kon doen over de effectiviteit van de patches.

Uit de evaluaties en de gesprekken die de Raad voerde leidt de Raad af dat NCSC op een cruciaal moment in de incidentbestrijding (namelijk ten tijde van het advies om de Citrix-servers uit te schakelen) niet heeft opgemerkt dat Citrix zijn bericht introk dat de mitigerende maatregelen niet effectief waren.

3.2.8 Organisaties kregen niet alle beschikbare informatie voor hun eigenstandige risicoafweging

Zoals beschreven in 3.1.2 nam de politiek na het beveiligingsadvies van AIVD het besluit dat NCSC dringend zou adviseren de Citrix-servers uit te zetten. NCSC hanteerde daarbij het uitgangspunt dat organisaties in de eerste plaats zelf verantwoordelijk zijn voor het maken van de risicoafweging omdat zij konden bepalen of het wel of niet doorvoeren van beveiligingsmaatregelen impact had op de veiligheid en op de continuïteit van de bedrijfsvoering. De organisaties wilden weten op welke aanvullende informatie het dringende advies van NCSC gebaseerd was ten opzichte van het eerdere advies om op basis van de eigen specifieke omstandigheden een risicoafweging te maken. Voor hen was relevant of het een concrete dreiging richting een bepaalde partij betrof of een voorzorgsmaatregel.

86 Het NCSC gaf aan het vertrouwen in de mitigerende maatregelen te hebben verloren door ontvangen berichten van gebruikers en door bevestiging van Citrix dat de maatregelen niet werkten voor ten minste één versie. Citrix geeft aan dat zij het bericht direct hebben ingetrokken en dat zij geen gevallen kennen waarin de maatregelen niet werkten.

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

Alle overheidsorganisaties moesten aan CIO Rijk doorgeven of zij maatregelen hadden genomen. Daarnaast benaderden NCSC, BZK en de beleidsafdelingen van JenV organisaties die geen deel uitmaakten van rijk en vitaal, zoals grote gemeenten en zorginstellingen, met het verzoek het dringende advies van NCSC op te volgen. En er waren organisaties (grote telecomproviders bijvoorbeeld) die onder meerdere wettelijke regimes vallen en door meerdere partijen werden benaderd, wat bij hen zorgde voor een extra belasting terwijl ze tegelijkertijd de crisis moesten bestrijden. Op 23 januari 2020 verzorgden de minister van JenV en minister van BZK met de plaatsvervangend NCTV en de directeur van NCSC een technische briefing aan de Tweede Kamer.[88]

Verschillende organisaties die de Raad sprak gaven aan dat zij - ondanks dat zij meenden alle geadviseerde maatregelen correct hadden uitgevoerd - hun systemen uit voorzorg hadden uitgezet. De reden was dat zij bestuurlijke druk voelden en niet wisten dat MIVD en AIVD informatie en advies aan het NCSC hadden verstrekt, noch wat de strekking van het advies was. De organisaties waren afhankelijk van NCSC en AIVD voor deze informatie, zij hadden geen mogelijkheid om deze informatie zelf te verzamelen. NCSC vond dat hij deze informatie niet aan de organisaties buiten het rijk kon geven.

3.3 Toedracht andere illustratieve voorvallen

Het voorval waarbij door kwetsbaarheden in Citrix-software beveiligingslekken bij organisaties ontstaan, staat niet op zichzelf. In deze paragraaf beschrijven we andere voorvallen met software die een vergelijkbare functie vervult (op afstand toegang verlenen tot een digitaal systeem van een organisatie) en waarbij kwetsbaarheden in deze software die gevolgen had voor de veiligheid digitale systemen van organisaties. De kwetsbaarheden die we in dit onderzoek behandelen behoren ook nog steeds tot de meest bij aanvallen gebruikte kwetsbaarheden van dit moment.[89]

88 De Tweede Kamer was zelf ook een van de organisaties die Citrix gebruikten en hun systemen hadden uitgezet.
89 CISA, *Top Routinely Exploited Vulnerabilities (thus far in 2021)*, 28 juli 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-209a

Uitvallen, ongevallen en aanvallen
In deze paragraaf beschrijven we voorvallen waarbij kwetsbaarheden ertoe leidden dat organisaties werden aangevallen. Kwetsbaarheden in software kunnen echter ook op een andere manier de veiligheid van digitale systemen aantasten en daarbij schade en letsel veroorzaken. Zo was in juni en juli van 2021 een groot aantal websites wereldwijd korte tijd onbereikbaar: kranten, media, webwinkels, banken, clouddiensten en overheidsdiensten, zoals 911 in een deel van de Verenigde Staten en het overheidsdomein in het Verenigd Koninkrijk. In beide gevallen werd de uitval veroorzaakt door een fout in de software van een internetdienstverlener die veel organisaties gebruiken om het internetverkeer naar hun websites sneller en stabieler te laten verlopen. Software wordt niet alleen gebruikt in digitale systemen maar ook ingebouwd, bijvoorbeeld in vervoermiddelen en chemische installaties. Kwetsbaarheden in software kunnen dan in combinatie met andere factoren leiden tot een ongeval.[90] Het toeval speelt bij deze voorvallen dan ook een grotere rol dan bij aanvallers die kwetsbaarheden misbruiken en daarbij geautomatiseerd alle servers kunnen vinden die de kwetsbaarheid bevatten.

3.3.1 VPN-software voor de zakelijke markt[91]

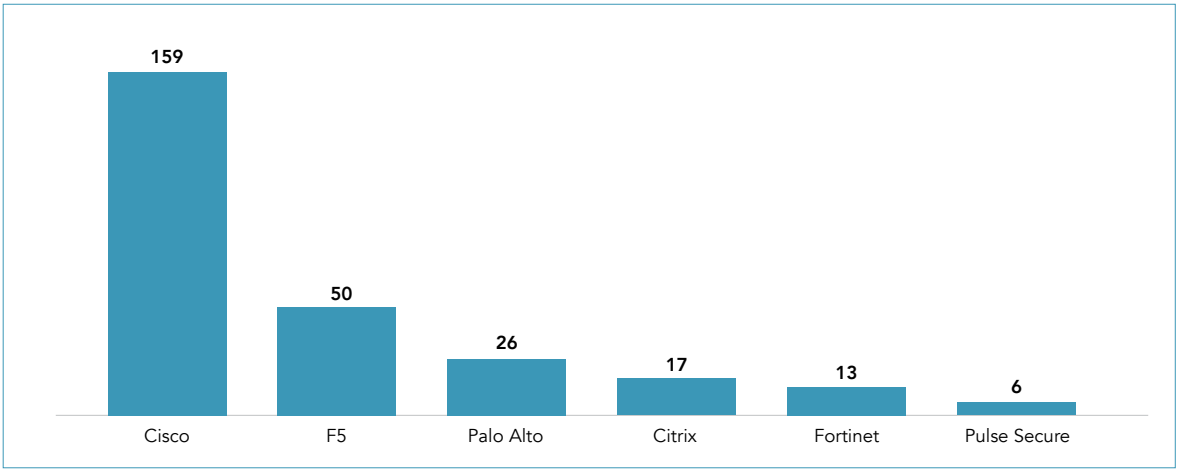
Organisaties gebruiken (zakelijke) VPN-software om hun medewerkers van afstand een veilige verbinding en toegang te geven tot het bedrijfsnetwerk. Net als bij de Gateway van Citrix vervullen deze VPN-producten een centrale rol in de veiligheid van het achterliggende netwerk. Een klein aantal fabrikanten domineert de markt van deze professionele VPN-producten. Zo wordt Pulse Secure gebruikt in ruim 50.000 met internet verbonden servers wereldwijd, met name grote bedrijven en overheden, Fortinet door meer dan 480.000 met internet verbonden servers wereldwijd, vooral middelgrote organisaties.[92] Het aantal servers dat Palo Alto-software gebruikt is niet bekend bij de Onderzoeksraad.

Op zoek naar kwetsbaarheden
In 2018 merkten beveiligingsonderzoekers op dat voor een aantal veelgebruikte VPN-producten voor de zakelijke markt relatief weinig kwetsbaarheden werden gepubliceerd ten opzichte van andere vergelijkbare producten. Zij vroegen zich af of dit kwam doordat de producten zo weinig kwetsbaarheden bevatten, of dat deze producten ondanks hun cruciale rol voor de veiligheid van digitale systemen een blinde vlek vormen (bijvoorbeeld doordat bij deze producten weinig naar kwetsbaarheden wordt gezocht). Daarom gingen zij in 2019 op zoek naar kwetsbaarheden in VPN-producten van Palo Alto, Fortinet en Pulse Secure.

90 Uitval internetdienstverleners: https://www.fastly.com/blog/summary-of-june-8-outage en https://www.reuters.com/technology/websites-airlines-banks-tech-companies-down-widespread-outage-2021-07-22/ Software in voertuigen, zoals de recall van Fiat Chrysler, vanwege een software kwetsbaarheid die maakte dat de airbags niet werden geactiveerd bij bepaalde ongevallen. https://www.reuters.com/article/us-fiatchrysler-recall-idUSKBN1881I6

91 VPN staat voor *Virtual Private Network*. CVE 2019-11507/10 meerdere kwetsbaarheden in PulseSecure-software (ernst varieert van 6 tot 9 op een schaal van 1 tot 10); CVE 2018-13379 kwetsbaarheid in Fortinet-software (ernst 9,8 op een schaal van 1 tot 10); CVE 2019-1579 kwetsbaarheid in Palo Alto-software (ernst 8,1 op een schaal van 1 tot 10).

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



Figuur 15: Analyse door de beveiligingsonderzoekers van het aantal ernstige kwetsbaarheden in VPN-producten (niet vermeld op welke periode deze analyse betrekking heeft). (Bron: Blog beveiligingsonderzoekers) [93]

Een belemmering voor de beveiligingsonderzoekers was dat de producten gesloten zijn (*closed source*). Na het openbreken van de software (*jailbreak*) vonden ze diverse kwetsbaarheden. De belangrijkste kwetsbaarheid binnen het product Pulse Secure ontstond nadat in 2016 in versie 8.2 een nieuwe functionaliteit aan het product werd toegevoegd.

De beveiligingsonderzoekers rapporteerden de kwetsbaarheden eerst aan de fabrikanten en aan de eigenaren van de gecompromitteerde bedrijfsnetwerken. Daarna deelden ze hun bevindingen in vakbladen, op congressen en op hun eigen blog.[94] De *incident response* van de betrokken fabrikanten was wisselend: Pulse Secure publiceerde de kwetsbaarheid en de patch een maand na de melding van de beveiligingsonderzoekers. Een maand na de waarschuwing gebruikten de beveiligingsonderzoekers de kwetsbaarheid om Twitter binnen te dringen, met succes. Fortinet verhielp de kwetsbaarheid na 7 weken, en geeft aan tegelijkertijd een waarschuwing te hebben gepubliceerd. Palo Alto liet aanvankelijk weten geen waarschuwing te zullen publiceren, omdat zij de kwetsbaarheid al kenden en hadden verholpen. Nadat de beveiligingsonderzoekers via de kwetsbaarheid in Palo Alto succesvol Uber waren binnengedrongen en daar zelf over hadden gepubliceerd, publiceerde de fabrikant alsnog een waarschuwing.

Binnen een dag tot een maand nadat de beveiligingsonderzoekers bekend hadden gedemonstreerd hoe de kwetsbaarheden in de software konden worden misbruikt en anderen de *exploit codes* publiceerden op GitHub en andere platforms, werd zichtbaar dat aanvallers het internet afzochten (scanden) op servers waarop deze kwetsbaarheid in de software nog niet was verholpen met een patch. Op dat moment hadden vele tientallen Nederlandse organisaties de update nog niet uitgevoerd, waaronder KLM,

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

Shell, Boskalis, diverse defensiebedrijven, het ministerie van Justitie en Veiligheid en LVNL. De meeste organisaties voerden na augustus 2019 de update uit.[95]

In augustus 2020 werd bekend dat aanvallers een lijst hadden samengesteld met buitgemaakte gebruikersnamen, wachtwoorden en IP-adressen van circa 900 kwetsbare Pulse Secure VPN-servers. De gegevens lijken tussen 24 juni en 8 juli 2020 verzameld te zijn. Deze lijst werd gepubliceerd op een forum dat vaak wordt bezocht door ransomware bendes. En in de zomer van 2021 gebeurde iets vergelijkbaars: aanvallers publiceerden op een nieuw gelanceerd hackersforum – mogelijk als publiciteitsstunt - een lijst met 500.000 inloggegevens voor Fortinet VPN-servers, naar verluid verzameld van servers die nog steeds kwetsbaar waren voor de in deze paragraaf beschreven kwetsbaarheid.[96] Volgens Fortinet waren uiteindelijk 140.000 inloggegevens en 24.000 apparaten exploiteerbaar door dit lek.

Verschillende nationale CERTs, waaronder het Amerikaanse nationale cyber-securitycentrum CISA, maar ook de Nederlandse inlichtingen- en veiligheidsdiensten, waarschuwden in de maanden en jaren die daarop volgden herhaaldelijk dat verschillende aanvallers waaronder statelijke actoren de kwetsbaarheden in de software misbruikten om aanvallen te plegen op digitale systemen van organisaties.[97] De kwetsbaarheden in de software waren net als de kwetsbaarheden in de Citrix-software deel gaan uitmaken van het internationale cyberwapenarsenaal.

95 Modderkolk, H., *Intern netwerk honderden bedrijven en ministerie lang maandenlang wagenwijd open*, De Volkskrant, 28 september 2019. Kamerstukken II 2019-2020, 26 643, nr. 666 Analyse van de gelopen risico's door de kwetsbaarheden in de virtual private network (VPN) software van het bedrijf Pulse Secure, 11 februari 2020. https://blog.cyberwar.nl/2019/09/dutch-kwetsbare-pulse-connect-secure-ssl-vpn-in-nederlandse-ip-adresruimte-bevindingen-en-gedachten/ Koot, M., *Field Note on CVE-2019-11510: Pulse Connect Secure SSL-VPN in the Netherlands*. In: *Digit. Threat.*: Res.Pract.1, 2, Article 13, mei 2020. https://dl.acm.org/doi/10.1145/3382765

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

97 https://us-cert.cisa.gov/ncas/alerts/aa20-258a *Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity* https://us-cert.cisa.gov/ncas/alerts/aa20-259a *Iran-Based Threat Actor Exploits VPN Vulnerabilities* https://ics-cert.kaspersky.com/reports/2021/04/07/vulnerability-in-fortigate-vpn-servers-is-exploited-in-cring-ransomware-attacks/ https://www.security.nl/posting/697797/FBI+waarschuwt+voor+misbruik+van+Fortinet+FortiOS-kwetsbaarheden, NCTV, *Cybersecuritybeeld 2020*.

Binnen een week van kwetsbaarheid tot cyberwapen
In de zomer van 2020 werd bekend dat de BIG-IP-software van het bedrijf F5 een kwetsbaarheid bevatte. Dit product heeft een vergelijkbare functie als de eerder beschreven Citrix-software. Het product bestaat uit verschillende modules zoals *Local Traffic Management*, DNS, toegangsbeleid, *firewall*. Op 30 juni 2020 maakte F5 bekend dat de beheerdersinterface van de *Traffic Management* module in BIG-IP een kwetsbaarheid bevatte. Bij servers waar de beheerdersinterface met internet was verbonden, konden aanvallers zonder autorisatie willekeurig kwaardaardige code op de server uitvoeren en daarmee binnendringen in het digitale systeem achter deze module. De kwetsbaarheid was zo ernstig dat deze een score 10 kreeg in een schaal van 1 tot 10. Deze kwetsbaarheid veroorzaakte onrust, aangezien deze vlak voor het weekend van de '*4th of July*' bekend werd gemaakt, in een periode waarin veel Amerikanen niet werken hetgeen het tijdig patchen zou belemmeren. Vijf dagen nadat F5 de kwetsbaarheid publiceerde, had een beveiligingsonderzoeker een methode gepubliceerd om de kwetsbaarheid te misbruiken.

Deze methode was zo eenvoudig dat de benodigde code in een tweet paste. Twee dagen later werden organisaties die BIG-IP gebruikten wereldwijd aangevallen.[98]

Incidentbestrijding
Ten tijde van de kwetsbaarheden in PulseSecure, Fortinet en Palo Alto bestond DIVD nog niet. Een Nederlandse beveiligingsonderzoeker scande op eigen initiatief het internet op servers die de kwetsbare PulseSecure en Fortinet software bevatte en gaf deze gegevens aan NCSC. De beveiligingsonderzoekers hadden ook kwetsbare servers gevonden buiten deze doelgroep. NCSC waarschuwde deze organisaties niet, zonder de beveiligingsonderzoekers daarover in te lichten. Net als bij het Citrix-voorval werden de wettelijke kaders zodanig geïnterpreteerd dat NCSC deze gegevens beperkt mocht delen. Op grond van een besluit van de directeur NCSC werden ook andere schakelorganisaties geïnformeerd, namelijk: organisaties binnen het Landelijk Dekkend Stelsel die nog niet als CERT of OKTT waren aangewezen en andere organisaties niet zijnde rijksoverheid of vitaal. Deze hebben daarbij 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.

Ook maanden later hadden de kwetsbaarheden nog gevolgen voor de organisaties die de software gebruikten, ook als zij in de tussentijd de kwetsbaarheden hadden verholpen door te patchen. Zo maakten op 4 augustus 2020 aanvallers van Pulse Secure servers gegevens openbaar die ze hadden bemachtigd bij aanvallen op meer dan 900 Pulse Secure servers. Het ging daarbij onder meer om inloggegevens van beheerders van de servers (*admin account details*) en alle gebruikersnamen en wachtwoorden van de lokale gebruikers.[99] In de tussentijd was het DIVD opgericht. Zij stuurden op 5 augustus

98 Bericht van F5 over kwetsbaarheid: https://support.f5.com/csp/article/K52145254 https://www.bleepingcomputer.com/news/security/poc-exploits-released-for-f5-big-ip-vulnerabilities-patch-now/ en https://www.bleepingcomputer.com/news/security/us-govt-confirms-active-exploitation-of-f5-big-ip-rce-flaw/
99 https://csirt.divd.nl/cases/DIVD-2020-00009/

waarschuwingen naar organisaties die zij konden linken aan de Nederlandse IP-adressen die in deze lijst voorkwamen.

Op 19 november 2020 trof een beveiligingsonderzoeker een lijst met 49.577 kwetsbare Fortinet servers aan op internet, op 22 november publiceerde magazine Bleeping Computer daarover. Vanaf 25 november 2020 heeft DIVD de lijst doorzocht op Nederlandse organisaties. Vanaf 3 december 2020 stuurde DIVD de eerste waarschuwingen naar deze organisaties.[100]

3.3.2 Golf van cyberaanvallen via software kwetsbaarheden en ketenaanvallen

De hiervoor beschreven gebeurtenissen vormden de opmaat voor een wereldwijde golf van cyberaanvallen en datalekken via software kwetsbaarheden, waarbij aanvallers ook gebruik maakten van beveiligingslekken van dienstverleners om andere organisaties aan te vallen. Dit fenomeen wordt *supply chain attacks* genoemd.

SolarWinds/SUNBURST

De escalatie van cyberaanvallen begon met de ontdekking van de SolarWinds/SUNBURST aanval in december 2020. De Washington Post schreef op 13 december 2020 dat verschillende Amerikaanse overheden waren binnengedrongen via de Orion software van het bedrijf SolarWinds. De aanval werd toegeschreven aan de Russische overheid. Een beveiligingsbedrijf had ontdekt dat aanvallers kwaadaardige code hadden toegevoegd aan de software updates van SolarWinds, waardoor de aanvallers toegang konden krijgen tot alle klanten die de software update hadden uitgevoerd. Onder de klanten van SolarWinds bevonden zich naast Amerikaanse overheden en grote bedrijven (waaronder het beveiligingsbedrijf dat de aanval ontdekte) ook de NAVO, het Europees Parlement, AstraZeneca en overheden in het Verenigd Koninkrijk.[101]

Microsoft Exchange

Na de SolarWinds/SUNBURST aanvallen werden vier *zero day* kwetsbaarheden ontdekt in lokale installaties van Microsoft Exhange servers. Servers met deze kwetsbaarheden werden wereldwijd aangevallen. Deze aanvallen werden door beveiligingsonderzoekers gemeld aan Microsoft. Er werd een link vermoed met de eerdere SolarWinds aanval (de aanvallers zouden zich toegang hebben verschaft tot de broncode van de software bij Microsoft). Microsoft schreef de aanval toe aan een aanvalsgroep die wordt gesteund door de Chinese overheid en zich richt op onderzoekers van infectieziekten, advocatenkantoren, onderwijsinstellingen en defensie aannemers. Naast deze aanvalsgroep maakten ook andere groepen aanvallers gebruik van de kwetsbaarheden in Exchange. Op 2 maart 2021 kwamen patches beschikbaar om de kwetsbaarheid te verhelpen. Deze patches konden echter niet de schade ongedaan maken of achterdeuren van verwijderen die aanvallers inmiddels hadden aangebracht.[102]

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

101 'Russian government spies are behind a broad hacking campaign that has breached U.S. agencies and a top cyber firm'. *The Washington Post*, 13 december 2020. Gallanger, Ryan, Donaldson, Kitty, et al. 'U.K. Government, NATO Join U.S. in Monitoring Risk From Hack'. *Bloomberg News website*, 15 december 2010. Sanger, David E.; Perlroth, Nicole; Schmitt, Eric. 'Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit'. *New York Times*, 15 december 2010.

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

'Kaas-hack'
Een van de bedrijven die werd aangevallen via de kwetsbaarheid in Microsoft Exchange was een Nederlandse logistieke dienstverlener. Als gevolg daarvan kwam een deel van de zuiveldistributie stil te liggen, waaronder de levering van kaas aan supermarkten. Daardoor werd deze aanvalscampagne in Nederland ook bekend onder de naam 'kaas-hack'.[103]

Geschat werd dat op 9 maart 2021 250.000 servers wereldwijd slachtoffer waren geworden van deze aanvallen, zowel in de VS als in Europa. De aanval wordt in de VS beschouwd als 1.000 keer zo schadelijk als de SolarWinds aanval in december 2020, in termen van economische schade. Dit is omdat door de Exchange aanval veel kleine en middelgrote ondernemingen worden getroffen, die een drijvende kracht zijn voor de economie. In de VS waren begin maart 2021 minstens 30.000 organisaties gehackt als gevolg van deze kwetsbaarheid. Op 22 maart 2021 maakte Microsoft bekend dat 92% van de servers was gepatcht of gemitigeerd.[104]

In Nederland scande DIVD vanaf 3 maart 2021 op kwetsbare servers in Nederland en de rest van de wereld. Op 4 maart stuurde DIVD de lijst met Nederlandse IP-adressen naar NBIP voor notificatie. In totaal stuurde DIVD meer dan 42.000 waarschuwingen. Later in maart scanden en waarschuwden ze opnieuw Nederlandse organisaties, op dat moment waren er nog steeds ongeveer 15.000 servers kwetsbaar, in mei waren het er nog 7.000 en daar kwamen 5.500 servers bij die kwetsbaarheden bevatten die in april 2021 werden gemeld.[105]

Spanningen tussen Microsoft en beveiligingsonderzoekers
Op 15 maart 2021 kwamen berichten dat de op 5 januari 2021 bij Microsoft ingediende *exploit code* mogelijk was gelekt en werd gebruikt door aanvallers. Media melden dat dit voor Microsoft aanleiding is om de partnerbedrijven door te lichten die vroegtijdig geïnformeerd worden over beveiligingslekken en patches. Diezelfde dag werd bericht dat er onder beveilingsonderzoekers onrust was ontstaan omdat GitHub op verzoek van Microsoft (eigenaar van GitHub) de code van een *exploit code* had verwijderd. Daarna paste GitHub zijn voorwaarden aan, zodat GitHub kan ingrijpen om te voorkomen dat het platform wordt misbruikt voor de uitwisseling van aanvalsmethoden die worden toegepast in aanvalscampagnes.[106]

103 https://nos.nl/artikel/2376492-oproep-na-kaas-hack-bestempel-voedselvoorziening-als-vitale-infrastructuur Marc Hijink, 'De les van het lege kaasschap,' *NRC 2021*. 'Duizenden extra Exchange-servers kwetsbaar,' *AG Connect*, 2021, geraadpleegd op 17 maart 2021, https://www.agconnect.nl/artikel/duizenden-extra-exchange-servers-kwetsbaar
104 https://www.techrepublic.com/article/how-the-microsoft-exchange-hack-could-impact-your-organization/
105 https://csirt.divd.nl/2021/05/14/Closing-ProxyLogon-case/
106 https://www.agconnect.nl/artikel/exchange-exploit-lijkt-uitgelekt-bij-melding-aan-microsoft https://www.agconnect.nl/artikel/rel-na-wissen-exchange-exploit-door-github en https://www.theregister.com/2021/03/12/github_disappears_exploit/ https://thehackernews.com/2021/06/github-updates-policy-to-remove-exploit.html

Kaseya VSA-software

Een nieuwe golf van cyberaanvallen diende zich aan in juli 2021. Wederom in het *'4th of July'* weekend werden wereldwijd honderden bedrijven aangevallen. Dit keer werden de aanvallen toegeschreven aan een *ransomware* bende uit Rusland. In april 2021 hadden Nederlandse beveiligingsonderzoekers die aangesloten waren bij DIVD aan bedrijf Kaseya gemeld dat zij kwetsbaarheden hadden gevonden in hun VSA-software. Deze software werd voornamelijk gebruikt door IT-dienstverleners (ook *managed service providers* of MSP genoemd) om vanaf afstand de digitale systemen van hun klanten te beheren, en soms ook door de bedrijven zelf. Voordat Kaseya de kwetsbaarheden had verholpen, was de *ransomware* bende begonnen met zijn wereldwijde aanvalscampagne. In Zweden leidde dit ertoe dat een supermarktketen met 800 winkels zijn deuren moest sluiten. Niet omdat zij zelf getroffen waren via de Kaseya-software, maar wel het bedrijf dat zorgde voor de betaalsystemen in de supermarkten.[107]

3.3.3 Urgentie en omvang onveiligheid neemt toe

De voorvallen die we in deze paragraaf beschrijven laten zien dat kwetsbaarheden die we in dit hoofdstuk beschrijven nog altijd veel worden misbruikt voor het uitvoeren van aanvallen en dat er steeds nieuwe kwetsbaarheden bij komen. Kwetsbaarheden in software vormen daarmee een steeds urgentere en grotere dreiging voor de digitale veiligheid van organisaties.[108]

Wanneer een kwetsbaarheid in software bekend wordt, hebben organisaties steeds minder tijd om de kwetsbaarheid te verhelpen voordat kwetsbare servers wereldwijd worden aangevallen (zie bijlage D). In het afgelopen jaar is deze dreiging verder geëscaleerd, doordat zowel criminele aanvallers als statelijke actoren ervoor kiezen om via ketenpartijen aan te vallen. Via dergelijke *supply chain attacks* kunnen aanvallers via de letterlijk zwakste schakel een keten van organisaties binnendringen. Aanvallen kunnen daardoor escaleren in omvang, terwijl het handelingsperspectief van individuele organisaties om zich te verweren tegen de aanval via een ketenpartner afneemt.

Wat de voorvallen ook laten zien is dat vrijwillige beveiligingsonderzoekers, zoals via DIVD, een cruciale rol speelden bij de incidentbestrijding en informatiedeling. Zij scanden namelijk het hele Nederlandse (en wereldwijde) domein, waardoor zij de noodzakelijke informatie hadden om te constateren welke organisaties de kwetsbaarheid nog niet hadden verholpen en organisaties te waarschuwen.

107 Na gesprekken tussen president Biden en Poetin verdween deze ransomware bende een tijd uit beeld. Sommigen zien dit als bewijs dat het effectief is om in internationaal verband (diplomatieke) actie te ondernemen na cyberaanvallen uit een ander land. https://nos.nl/artikel/2387973-nederlandse-ethische-hackers-probeerden-ransomware-aanval-te-voorkomen; 'Swedish Coop supermarkets shut due to US ransomware cyber-attack,' *BBC*, 2021, geraadpleegd op 4 juli 2021, https://www.bbc.com/news/technology-57707530

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