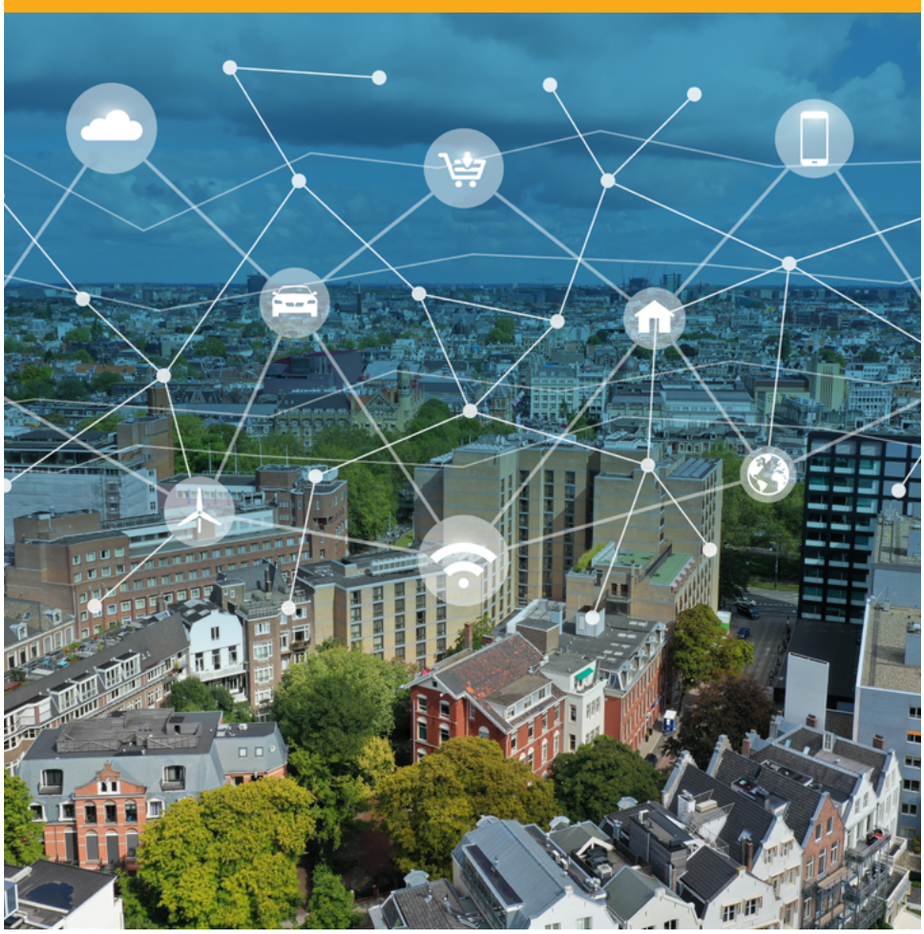
ONDERZOEKSRAAD VOOR VEILIGHEID

Kwetsbaar door software

Lessen naar aanleiding van beveiligingslekken door software van Citrix



Kwetsbaar door software

Lessen naar aanleiding van beveiligingslekken door software van Citrix

Den Haag, december 2021

De rapporten van de Onderzoeksraad voor Veiligheid zijn openbaar en beschikbaar op www.onderzoeksraad.nl

(Bron cover foto: Shutterstock, bewerking door Delta3).

De Onderzoeksraad voor Veiligheid

Als zich een ongeval of ramp voordoet, onderzoekt de Onderzoeksraad voor Veiligheid hoe dat heeft kunnen gebeuren, met als doel daar lessen uit te trekken. Op die manier draagt de Onderzoeksraad bij aan het verbeteren van de veiligheid van Nederland. De Raad is onafhankelijk en besluit zelf welke voorvallen hij onderzoekt. Daarbij richt de Raad zich in het bijzonder op situaties waarin mensen voor hun veiligheid afhankelijk zijn van derden, bijvoorbeeld van de overheid of bedrijven. In een aantal gevallen is de Raad verplicht onderzoek te doen. De onderzoeken gaan niet in op schuld of aansprakelijkheid.

Onderzoeksraad

Voorzitter: ir. J.R.V.A. Dijsselbloem
prof. dr. mr. S. Zouridis
dr. E.A. Bakkum[1]

Secretaris-directeur: mr. C.A.J.F. Verheij

Bezoekadres: Lange Voorhout 9
2514 EA Den Haag

Postadres: Postbus 95404
2509 CK Den Haag

Telefoon: 070 333 7000

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

Dit rapport is in de Nederlandse en Engelse taal gepubliceerd. Bij verschil in interpretatie geldt de Nederlandse tekst.

1 Mevrouw dr. E.A. Bakkum is 1 december 2021, na vaststelling van dit rapport door de Onderzoeksraad voor Veiligheid, tot deze raad toegetreden. Ze heeft geen betrokkenheid gehad bij dit onderzoek.

INHOUD

SAMENVATTING

Op 17 december 2019 deed de Amerikaanse softwarefabrikant Citrix een openbare mededeling op zijn website dat een aantal van hun softwareproducten een kwetsbaarheid bevat. Via deze kwetsbaarheid konden aanvallers binnendringen in de digitale systemen van organisaties die deze producten gebruikten. Citrix gaf aan welke maatregelen organisaties konden nemen om de problemen tijdelijk te verhelpen, maar had nog geen definitieve oplossing. Een maand later, op 17 januari, adviseerde het Nationaal Cyber Security Centrum (NCSC) aan Nederlandse gebruikers hun Citrix-servers uit te zetten. Direct in de weken na de bekendmaking van de softwarekwetsbaarheid drongen aanvallers de digitale systemen van verschillende organisaties binnen. Deze aanvallen gaan door tot aan vandaag de dag.

De Onderzoeksraad onderzocht welke lessen te trekken zijn uit de wijze waarop betrokken partijen zijn omgegaan met de risico's van kwetsbaarheden in Citrix-software en andere voorvallen waarbij kwetsbaarheden in software werden misbruikt door aanvallers. Hierbij is gekeken naar zowel het voorkomen als het bestrijden van dergelijke voorvallen.

Citrix maakt software waarmee onder andere werknemers op afstand kunnen inloggen in de ICT-systemen van hun werkgever. Deze software vormt vaak een belangrijk onderdeel van de digitale infrastructuur, omdat het de koppeling vormt tussen het externe netwerk (internet) en het interne netwerk. Vrijwel alle organisaties in Nederland gebruiken dergelijke software, zowel overheden, bedrijven als andere instellingen. Denk bijvoorbeeld aan de rijksoverheid en decentrale overheden zoals gemeenten, maar ook ziekenhuizen, onderwijsinstellingen, vitale en andersoortige organisaties. Zo werd de Citrix-software uit dit onderzoek gebruikt door 80% van de rijksoverheidsorganisaties en twee-derde van gemeenten en provincies.

Het voorval met Citrix-software en de andere voorvallen die dit rapport analyseert laten zien dat de urgentie en omvang van digitale onveiligheid toeneemt. Nederland is één van de meest gedigitaliseerde landen ter wereld. Software vervult een centrale rol in het functioneren van digitale systemen van organisaties, maar bevat ook kwetsbaarheden. De digitalisering gaat daardoor gepaard met steeds grotere risico's voor organisaties die afhankelijk zijn van software.

Doordat de meeste organisaties niet naar buiten treden als ze zijn aangevallen, is het totale aantal getroffenen van de voorvallen onbekend, maar in potentie groot. Zo waren er toen de aanvallen via Citrix-software in januari 2020 begonnen nog ruim 500 servers van organisaties, waar aanvallers relatief eenvoudig konden binnendringen. Bekend zijn dat een gemeente, ziekenhuis en verschillende overheidsorganisaties getroffen waren.
Daarnaast hebben veel overheidsinstellingen en bedrijven hun servers uitgezet op advies van het NCSC. In juli 2020 bleek dat zeker 25 Nederlandse servers nog steeds waren binnengedrongen.

Ook voor de andere software producten is niet bekend hoe veel aanvallers langs die weg zijn binnengedrongen. Wel hebben aanvallers langs die weg honderdduizenden inloggegevens verzameld en gepubliceerd. De recentere aanvallen via SolarWinds, Kaseya en Microsoft Exchange hebben naar schatting duizenden organisaties wereldwijd getroffen, waaronder een Zweedse supermarktketen en een Nederlandse logistieke dienstverlener voor een supermarktketen.

Sinds 2020 is wereldwijd een toename van cyberaanvallen waarneembaar: van zogenoemde '*ransomware*' tot economische spionage en (voorbereiding op) sabotage. Aanvallers misbruiken nog altijd de kwetsbaarheden die in dit rapport zijn geanalyseerd voor het uitvoeren van aanvallen. Er komen bovendien steeds nieuwe kwetsbaarheden bij. Softwarekwetsbaarheden vormen daarom een steeds urgentere en grotere dreiging voor de digitale en de fysieke veiligheid.

Voorvallen

Door de kwetsbaarheid in Citrix-software konden onbevoegde gebruikers zich toegang verschaffen tot alle onderdelen van de server waarop deze software werkte. Citrix vernam dat de methode om de kwetsbaarheid te misbruiken al werd verspreid. Doordat de kwetsbaarheid in veel versies van de software zat, zou het lang duren voor de fabrikant een definitieve veiligheidsupdate kon uitbrengen. Om die reden besloot hij om eerst tijdelijke mitigerende maatregelen te publiceren. Uit deze tijdelijke maatregelen konden aanvallers afleiden wat de kwetsbaarheid was en hoe zij deze konden misbruiken voor een aanval. Naast het publiceren van de kwetsbaarheid en de mitigerende maatregel op zijn website zette de fabrikant zich in om zoveel mogelijk klanten wereldwijd rechtstreeks te waarschuwen. De fabrikant kon niet alle afnemers bereiken omdat hij niet beschikte over alle contactgegevens.

Zowel fabrikant Citrix als beveiligingsonderzoekers van de vrijwilligersorganisatie *Dutch Institute for Vulnerability Disclosure* (DIVD) verzamelden in de eerste maanden na de ontdekking van de kwetsbaarheid informatie over welke Nederlandse organisaties op hun servers nog kwetsbare software gebruikten, en daardoor risico liepen om aangevallen te worden. Citrix en het DIVD deelden hun informatie met het NCSC, onderdeel van het ministerie van Justitie en Veiligheid (JenV), in de verwachting dat die de kwetsbare organisaties zou waarschuwen. Het NCSC waarschuwde in de praktijk alleen de rijksoverheid en vitale aanbieders; niet de grote groep kwetsbare organisaties daarbuiten. Het NCSC, dat in Nederland functioneert als nationaal aanspreekpunt, beschikt niet over de verantwoordelijkheden en bevoegdheden om dat te kunnen waarmaken.

Halverwege januari 2020 escaleerde de situatie en het risico in Nederland maatschappelijk en bestuurlijk: er werd opgeschaald naar de nationale crisisstructuur, het NCSC adviseerde organisaties aanvankelijk om te overwegen hun Citrix-servers indien mogelijk uit te zetten, en er waren vragen vanuit organisaties over de te nemen maatregelen. Tegelijkertijd ontstond er onduidelijkheid over de effectiviteit van de maatregelen.

Naar aanleiding van een inlichtingenbericht en beveiligingsadvies van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en Algemene Inlichtingen- en Veiligheidsdienst (AIVD) besloten de ministers van JenV, Binnenlandse Zaken en Koninkrijksrelaties (BZK) in samenspraak met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) dat het NCSC het dringende advies moest uitbrengen om Citrix-servers uit te zetten ('*comply or explain*'). Organisaties moesten zelf een afweging maken tussen het risico op een aanval en de mogelijke gevolgen van het uitzetten van hun servers. Ze kregen daarbij niet alle benodigde en beschikbare informatie om deze risicoafweging te kunnen maken: of ze zelf een kwetsbare server hadden en wat de aard van de dreiging was.

Omvang en urgentie nemen toe
Kwetsbaarheden in software zijn nog altijd een veelgebruikte route waarlangs aanvallers binnendringen in de systemen van organisaties. Organisaties hebben steeds minder tijd om kwetsbaarheden te verhelpen voordat servers wereldwijd worden aangevallen. Daarnaast kunnen aanvallers organisaties ook direct of indirect raken door hun ketenpartners aan te vallen (binnen te dringen via de zwakste schakel van omringende klanten en afnemers).

De onderzochte voorvallen vertonen een aantal opvallende overeenkomsten. Zo zijn organisaties, en de mensen die van deze organisaties afhankelijk zijn, blootgesteld aan digitale onveiligheid doordat zij kwetsbare software gebruiken. De wijze waarop fabrikanten, organisaties die de software gebruikten en incidentbestrijders op de voorvallen reageerden laten zien dat de incidentbestrijding nog geen sluitende, vanzelfsprekende, systematisch ingebouwde reflex is. De voorvallen illustreren elk dat waarschuwingen deze organisaties in veel gevallen niet bereiken. Alle door de Onderzoeksraad onderzochte voorvallen laten zien dat (vrijwillige) beveiligings-onderzoekers een cruciale rol spelen in de incidentbestrijding.

Belemmeringen op systeemniveau
Veilige software is het resultaat van een continu verbeterproces in een netwerk van verantwoordelijke partijen die ieder daadwerkelijk hun eigen verantwoordelijkheid nemen, en die in effectieve structuren op basis van onderling vertrouwen met elkaar samenwerken. De analyse van de voorvallen geeft aanleiding om belemmeringen op systeemniveau te adresseren. Daar volgt een aantal lessen uit.

Kwetsbaarheden in software ontstaan tijdens levenscyclus product
De voorvallen die de Onderzoeksraad onderzocht laten zien dat het gebruik van software inherent onveilig is: als een organisatie software gebruikt gaat dit altijd gepaard met risico's. Het is in de praktijk onmogelijk om software te maken die geen kwetsbaarheden bevat. Hoe kan dit, en wie kan op welke wijze bijdragen aan het verminderen van de inherente onveiligheid?

Kwetsbaarheden in software ontstaan bij de ontwikkeling en tijdens de levenscyclus van een product. De softwarefabrikant bouwt voort op een bestaand product door nieuwe functies toe te voegen, waardoor de software complexer wordt. Ook de gebruikte programmeertaal, het hergebruik van reeds bestaande onderdelen en (inconsistente) lagen in de software-architectuur kunnen kwetsbaarheden introduceren.

De risico's van deze kwetsbaarheden nemen toe als het product in de loop van de tijd anders wordt gebruikt en daarbij een meer veiligheidskritische rol krijgt in digitale systemen.

(Veiligheids)problemen die het gevolg zijn van fundamentele keuzes in het product vormen voor de fabrikant een belemmering om kwetsbaarheden bij de wortel aan te pakken. Hiervoor is namelijk een investering nodig in de vorm van geld en capaciteit om het probleem op te lossen. De keuze van de fabrikant om in die situaties alleen de kwetsbaarheid te patchen ('een pleister plakken') met een update lost het achterliggende probleem niet op. Het inherente veiligheidsprobleem blijft.

Er zijn fabrikanten die ethische hackers met beloningen aansporen om te zoeken naar kwetsbaarheden in software. Fabrikanten sporen daarnaast zelf kwetsbaarheden op door verschillende testen uit te voeren. Daardoor worden veel kwetsbaarheden opgespoord, maar het is onwaarschijnlijk dat fabrikanten *alle* kwetsbaarheden vinden.

Kwetsbaarheden in software vormen steeds vaker een route voor aanvallers om digitale systemen van organisaties binnen te dringen. Het bekendmaken van kwetsbaarheden vormt daarmee een dilemma: het kan organisaties helpen zich beter te wapenen tegen mogelijk misbruik van de kwetsbaarheid, het kan aanvallers echter helpen om kwetsbare servers op te sporen en binnen te dringen. Dit onderstreept het belang van het tijdig verwerken van de veiligheidsupdates (patches) van fabrikanten. Maar veelvuldig patchen en mitigeren vormt tegelijkertijd een risico voor organisaties omdat dit kan leiden tot verstoringen in digitale systemen of kan zorgen voor nieuwe kwetsbaarheden. Organisaties moeten het besluit om te patchen daarom goed doordenken vanuit het specifieke ICT-landschap van hun organisatie. In sommige gevallen beginnen de aanvallen binnen enkele dagen na bekendmaking. Daardoor moet de organisatie in korte tijd reageren.

Aanschaf en gebruik van software door organisaties
De ongelijke verhouding tussen fabrikanten en afnemers van softwareproducten dwingt te weinig af dat fabrikanten zich inspannen om de veiligheidsrisico's te beheersen. Op dit moment biedt wet- en regelgeving weinig mogelijkheden voor organisaties om fabrikanten te verplichten cybersecurity in hun producten te borgen. Afnemers weten niet altijd hoe ze zelf eisen moeten stellen en een fabrikant verantwoording moeten laten afleggen. Veel afnemers hebben bovendien niet de kennis en capaciteit om de juiste eisen te stellen en deze te controleren. Daarmee worden kwetsbaarheden in software een probleem van de afnemer. Het aanbieden van software vanuit de *cloud* verplaatst de verantwoordelijkheid om te patchen van de afnemer naar de fabrikant, maar gaat ook gepaard met nadelen voor afnemers zoals minder autonomie en privacy.

Wat betreft preventie en voorbereiding op incidenten is er verschil in de weerbaarheid van organisaties. Maatregelen vergen dat organisaties risicoafwegingen maken. Niet alle organisaties hebben de expertise en capaciteit om maatregelen voldoende uit te voeren, of onderkennen niet de urgentie om hier capaciteit op in te zetten. De overheid biedt geen collectief fundament dat organisaties helpt hun digitale weerbaarheid te vergroten of een (institutionele) infrastructuur dan wel netwerk waarin partijen gezamenlijk de digitale weerbaarheid versterken.

Incidentbestrijding
Bij het gebruik van software in organisaties ontstaan incidenten die zo snel mogelijk moeten worden bestreden. De incidentbestrijding in Nederland wordt momenteel echter belemmerd door het feit dat er geen nationale structuur bestaat die erin voorziet dat alle organisaties tijdig informatie over kwetsbaarheden in software ontvangen. In het bijzonder gaat het daarbij om informatie over welke systemen van welke organisaties kwetsbaar zijn en risico lopen om aangevallen te worden, zogenaamde 'slachtofferinformatie'. Daardoor zou een organisatie, ook ongevraagd, gewaarschuwd kunnen worden wanneer haar systemen kwetsbaar zijn en zij risico loopt om te worden aangevallen.

Het NCSC ontvangt momenteel voor heel Nederland informatie van onder meer fabrikanten, NCSC's in andere landen, inlichtingen- en veiligheidsdiensten en anderen. Het NCSC deelt deze slachtofferinformatie nu echter alleen met een selecte groep organisaties, niet met decentrale overheden en het merendeel van het Nederlandse bedrijfsleven en vanuit het uitgangspunt dat een organisatie vooraf toestemming geeft om te worden geïnformeerd.

Wel streeft de rijksoverheid er naar dat de informatie die NCSC wel wil delen beter wordt uitgewisseld via het zogenoemde Landelijk Dekkend Stelsel, waarin sectorale organisaties en (groepen) bedrijven ook op vrijwillige basis informatie met elkaar delen die cruciaal is voor het bestrijden van incidenten. Als het NCSC als nationaal aanspreekpunt informatie echter wel ontvangt maar niet volledig deelt, worden ook bij een volledig dekkend stelsel niet alle potentiële slachtoffers gewaarschuwd. Beveiligingsonderzoekers proberen dit hiaat op te vangen door – op vrijwillige basis – het Nederlandse internetdomein te scannen op kwetsbare servers en deze informatie te delen met partijen die kunnen waarschuwen. Dat is echter een kwetsbare situatie, omdat zij hierin niet werden gefaciliteerd: noch door de overheid, noch door andere betrokken partijen, waardoor hun structurele inzet niet is geborgd.[2]

Leren van voorvallen
Om de veiligheid te kunnen verbeteren is het belangrijk om te onderzoeken wat er gebeurde en welke factoren bijdroegen aan het ontstaan van voorvallen. Deze inzichten zijn nodig om te kunnen leren en zo de kans te verkleinen dat toekomstige voorvallen gebeuren en de gevolgen te beperken door sneller te reageren. De traditie om van voorvallen te leren is in het digitale domein nog in ontwikkeling. Organisaties moeten voorvallen met vitale aanbieders en datalekken melden. Toezichthouders doen op dit moment incidenteel onderzoek naar digitale voorvallen en geven aan nog niet in staat te zijn om samenhangende uitspraken te kunnen doen over hoe het gesteld is met de digitale veiligheid in vitale sectoren en processen. Een platform voor gezamenlijk leren door fabrikanten, organisaties die software gebruiken en andere relevante publieke en private partijen ontbreekt.

2 Inmiddels is deze situatie veranderd: eind september 2021 kondigde het bedrijfsleven aan om zelf een waarschuwingssysteem op te zetten . Bron: FD, Bedrijfsleven start eigen alarmsysteem tegen hackers: 'overheid te traag', 28 september 2021.

Er zijn verschillende belemmeringen bij het leren van digitale voorvallen. Zo komen veel organisaties er in de huidige praktijk niet voor uit dat ze zijn aangevallen, onder meer vanwege angst voor aansprakelijkheid en reputatieschade. Een andere belemmering om te kunnen leren van voorvallen is dat de onderzoeken niet de verklaringen bieden die nodig zijn om het systeem te verbeteren. Zo is het niet alleen relevant om te weten in hoeverre een organisatie de verwachte basismaatregelen had geïmplementeerd, maar ook om te begrijpen waardoor het komt dat het voor organisaties moeilijk is om weerstand te bieden tegen aanvallen. Tenslotte verspreiden organisaties de lessen uit voorvallen meestal niet buiten de eigen organisatie of gemeenschap.

Beleid en internationale context
Er is Europese regelgeving ontwikkeld gericht op incidentbestrijding, en verantwoording op het gebied van informatiebeveiliging voor de financiële sector. Binnenkort komt er ook regelgeving voor de toepassing van software in producten (*Internet of Things*). Voor software zelf is er behalve regulering voor bepaalde toepassingen nog geen internationaal kader. Een belemmering daarbij is dat kwetsbaarheden niet alleen een probleem zijn voor landen, maar dat landen ze zelf ook inzetten als middel bij hun eigen activiteiten zoals opsporing en inlichtingen. Daarnaast wordt internationale samenwerking belemmerd door ideologische verschillen, zoals hoe de staat zich verhoudt tot het internet en hoe aanvallers af te schrikken.

Digitale afhankelijkheid neemt toe

Onze maatschappij digitaliseert in hoog tempo. De afhankelijkheid van digitale systemen van zowel individuen, organisaties als de gehele maatschappij is de afgelopen tijd toegenomen en zal nog verder toenemen. Dit is in het bijzonder zichtbaar geworden tijdens de coronapandemie: binnen veel organisaties werd vrijwel alleen op afstand gewerkt. Het ligt in lijn der verwachting dat (gedeeltelijk) 'thuiswerken' met digitale hulpmiddelen een vast gegeven blijft in de samenleving.

Organisaties gebruiken digitale systemen om hun werkzaamheden te kunnen uitvoeren. Deze digitale systemen bevatten verschillende soorten software. Software bevat per definitie kwetsbaarheden en deze kwetsbaarheden vormen steeds vaker een route voor aanvallers om systemen aan te vallen. De potentiële gevolgen van deze aanvallen voor individuele organisaties – of zelfs voor de gehele nationale veiligheid – zijn niet altijd te overzien. Dit rapport beschrijft en analyseert deze negatieve effecten.

Dat software per definitie kwetsbaarheden bevat, betekent wat de Onderzoeksraad voor Veiligheid betreft dat het belangrijk is om voortdurend te streven naar het veiliger maken van software en adequaat te reageren als er toch kwetsbaarheden bekend worden. Organisaties hebben bij het gebruik van digitale systemen een verantwoordelijkheid om de veiligheid en de beveiliging te waarborgen. Daarbij zijn ze mede afhankelijk van fabrikanten die op hun beurt verantwoordelijk zijn voor de veiligheid van de software die zij op de markt brengen. Op welke manier vullen fabrikanten deze verantwoordelijkheid in? En hoe gaan organisaties om met hun digitale afhankelijkheid en de gevolgen daarvan voor anderen die weer van hen afhankelijk zijn? Wat vraagt deze situatie van overheden in hun regulerende en toezichthoudende rol en welke rol kunnen niet-gouvernementele organisaties spelen?

Deze vragen zijn juist nu actueel, gelet op alle cyberaanvallen die de afgelopen jaren wereldwijd tal van organisaties raakte. Het ging daarbij onder meer om organisaties met cruciale maatschappelijke functies, zoals overheidsinstellingen, ziekenhuizen, universiteiten, nutsvoorzieningen en distributiecentra. Dergelijke aanvallen benadrukken de actuele relevantie van dit onderzoek naar beveiligingslekken door kwetsbaarheden in Citrix-software, dat de Onderzoeksraad in juli 2020 startte. De wereldwijde cyberaanvallen die als voorbeelden dienen in dit rapport, laten zien dat de problematiek inmiddels ernstiger en urgenter is dan bij aanvang van dit onderzoek.

Kwetsbaar door software

Software is mensenwerk: alle computers bevatten software die wordt gemaakt door mensen. Softwarefabrikanten passen bestaande en nieuwe software steeds aan de wensen van hun klanten aan door nieuwe functies toe te voegen.

Bij deze *updates* gaat het onder andere om het toevoegen van extra functionaliteiten. Daarnaast updaten fabrikanten hun software om veiligheidsproblemen te verhelpen (patchen). Bij patchen gaat het om het verhelpen van kwetsbaarheden in software die ertoe kunnen leiden dat software niet zoals bedoeld functioneert, of kwetsbaarheden die aanvallers kunnen misbruiken om digitale systemen binnen te dringen.

Bij het zo snel mogelijk verhelpen van kwetsbaarheden gaat de aandacht van fabrikanten in eerste instantie uit naar het *symptoom* van de kwetsbaarheid. Het verhelpen van de fundamentele *oorzaken* van het veiligheidsprobleem vraagt om fundamentele ingrepen. Vanwege de levensduur en omvang van softwareproducten kosten dergelijke fundamentele ingrepen veel tijd en geld. Fabrikanten ontvangen op dit moment weinig prikkels om het aantal kwetsbaarheden te reduceren en dat is om ten minste drie redenen zorgelijk.

Ten eerste zijn het maatschappelijk verkeer en de productie van goederen en diensten steeds meer afhankelijk van digitale systemen. Van voedselproductie tot acute zorg, van transport tot chemische industrie, van waterbeheer tot financieel verkeer: zonder software zijn ze onvoorstelbaar. Als digitale systemen door kwetsbaarheden in software niet goed werken, heeft dit ingrijpende gevolgen.

Ten tweede speelt de meeste software een veiligheidskritische rol in deze digitale systemen. De software die de Onderzoeksraad in dit onderzoek behandelt, fungeert als toegangspoort naar het digitale systeem van organisaties. Het regelt het verkeer tussen de systemen in organisaties en de medewerkers en klanten die zich erbuiten bevinden. Kwetsbaarheden in dergelijke software zetten de digitale toegangspoort van een organisatie open voor onbevoegde gebruikers en kunnen in sommige gevallen onbevoegden zelfs toegang geven tot cruciale bedrijfsprocessen, objecten (gebouwen, infrastructuur) en vertrouwelijke gegevens.

Ten derde staat software per definitie centraal in het digitale verkeer binnen organisaties en tussen organisaties onderling. En is software vrijwel altijd verbonden met andere software binnen en buiten de organisatie. Kwetsbaarheden in software kunnen daardoor doorwerken in het hele ICT-landschap van een organisatie en, zoals blijkt uit casussen in dit rapport, zelfs in het ICT-landschap van (delen van) sectoren.

Veilige software is primair de verantwoordelijkheid van de fabrikant die de software op de markt brengt. De ongelijke verhoudingen tussen fabrikanten en afnemers belemmeren de prikkels die fabrikanten krijgen om hun inspanningen te vergroten en daarover verantwoording af te leggen aan hun afnemers. Afnemers weten niet precies hoe de software werkt en wat de risico's zijn. Of hun organisaties zijn te klein om fabrikanten tot hogere veiligheidseisen te bewegen of zelfs te dwingen. Daar waar de overheid afnemer is en er sprake is van veiligheidskritische software kunnen de verhoudingen tussen afnemer en fabrikant echter aanzienlijk anders liggen.

Deze kwesties makken het aanlokkelijk om verantwoordelijkheden voor veilige software te verdelen en af te schuiven. Een voorbeeld hiervan is dat een fabrikant software op de markt heeft die een kwetsbaarheid bevat.

De fabrikant biedt een veiligheidsupdate (patch) aan, maar houdt de afnemer ervoor verantwoordelijk dat hij de update daadwerkelijk uitvoert. Daarmee wentelt de fabrikant het risico van kwetsbaarheden in software af op afnemers, terwijl die waarschijnlijk niet in staat zullen zijn om letterlijk duizenden keren per jaar veiligheidsupdates uit te voeren.

Voor veilige software zijn de inspanningen van fabrikanten en gebruikers niet afdoende. Het is nodig dat verschillende overheidsinstanties en bedrijven samenwerken zodat zij in gezamenlijkheid expertise mobiliseren om de veiligheid van software te beoordelen en daarmee hun positie als afnemers ten opzichte van fabrikanten te versterken. Ook past het bij de rol van de overheid als hoeder van digitale veiligheid om als regulerende en toezichthoudende instantie, maar ook als afnemer die voorop loopt, wettelijke eisen te stellen aan veiligheidskritische software die op de markt is en in de toekomst zal komen, en af te dwingen dat die eisen worden ingewilligd.

Gezien de groeiende digitale afhankelijkheid en de snelle ontwikkelingen ligt het stellen van eisen aan de software zelf niet voor de hand. Wettelijke maatregelen zullen al achterhaald zijn op het moment dat wetgeving in werking treedt. Het afdwingen van procedurele waarborgen in het ontwikkelproces van software is echter wel degelijk denkbaar. Daarbij kan worden gedacht aan verplichte deelname aan zogenoemde *bug bounty*-programma's waarin ethische hackers worden beloond als zij kwetsbaarheden vinden, of aan onafhankelijke software audits die plaatsvinden voordat en nadat de software op de markt wordt aangeboden. Ook is belangrijk dat – vergelijkbaar met voedselveiligheid – traceerbaar is welke componenten softwarefabrikanten gebruiken en waar die vandaan komen en terecht komen (traceerbaarheid via een zogenoemde *chain of trust*). Met dat laatste moet worden voorkomen dat bijvoorbeeld softwareonderdelen die eerder aantoonbaar kwetsbaar zijn gebleken, worden hergebruikt in nieuwe software.

Responscapaciteit

Software is in de praktijk dus kwetsbaar én essentieel voor het waarborgen van veiligheid en het functioneren van de maatschappij. Dit onderzoek laat zien dat het cruciaal is om kwetsbaarheden in software zo veel mogelijk te voorkomen. Het rapport laat ook zien dat dit een kwestie is van lange adem en dat het onmogelijk is om álle kwetsbaarheden te voorkomen. Dit betekent dat, naast inspanningen om software voortdurend veiliger te maken, de responscapaciteit een cruciale verantwoordelijkheid is voor het stelsel van betrokken partijen (fabrikanten, overheden, toezichthouders en afnemers). Ook met oog op respons is veilige software van groot belang – vergelijkbaar met dat een brand beter te bestrijden is als het gebouw brandwerend is. Alleen door samen te werken, zowel nationaal als in internationaal verband, en zo optimaal mogelijk informatie uit te wisselen kunnen zij hun eigen verantwoordelijkheid waarmaken. Dit rapport beschrijft een aantal belemmeringen in de responscapaciteit. Die belemmeringen bestaan tegen de achtergrond dat het Nationaal Cyber Security Centrum (NCSC) in Nederland in de praktijk functioneert als het nationale aanspreekpunt, maar formeel niet de taken en de verantwoordelijkheden heeft om dat te kunnen waarmaken.

Belemmeringen

De onderzochte voorvallen tonen dat verschillende partijen slachtofferinformatie naar het NCSC sturen, maar dat het NCSC vervolgens niet alle slachtoffers waarschuwde. In dit rapport beschrijft de Onderzoeksraad de juridische obstakels die het NCSC en het

ministerie van Justitie en Veiligheid tegenkomen, en die belemmeren dat alle potentiële slachtoffers (gevraagd en ongevraagd) kunnen worden gewaarschuwd. Veel belemmeringen zijn terug te voeren op de juridische interpretatie van het mandaat van het NCSC en andere overheidsonderdelen, evenals de AVG.

Versterking van het stelsel
Ondanks recent aangekondigde beleidsmaatregelen, zoals de versterking van het Landelijk Dekkend Stelsel, blijven fundamentele problemen bestaan. Om de digitale veiligheid van organisaties te kunnen waarborgen is het nodig om belemmeringen weg te nemen en de overstap te maken naar een nieuwe structuur, waarin de ongelijkheid tussen fabrikant en afnemer zo veel mogelijk wordt verminderd en informatie zo snel en doeltreffend mogelijk wordt uitgewisseld. Dit vraagt om een andere toedeling van verantwoordelijkheden (proportioneel naar risico en handelingsperspectief); houding (van 'niet delen tenzij' naar 'openbaar delen mits'); en structuur (laagdrempelig, toegankelijk en eenvoudig).

Daarnaast is het cruciaal voor betrokken partijen om in gezamenlijkheid te leren van voorvallen die plaatsvinden, zowel vóórdat als nádat software op de markt komt. Angst voor aansprakelijkheid en reputatieschade staan de benodigde openheid om in gezamenlijkheid van voorvallen te leren in de weg. Als organisaties en fabrikanten samen op zoek gaan naar verklaringen die nodig zijn om de veiligheid van het systeem te verbeteren en de lessen die ze geleerd hebben transparant uitdragen, zijn zij door de bundeling van hun ervaring en inzichten beter in staat om de veiligheid van digitale systemen te beheersen. Door wet- en regelgeving die de ongelijke verhouding tussen fabrikant en afnemer vermindert enerzijds, en door afnemers die hun krachten bundelen anderzijds, kunnen prikkels worden gegeven die een dergelijke lerende aanpak stimuleren.

Samenwerking maakt ook een doelmatiger inzet van de schaarse capaciteit aan cybersecurity-expertise mogelijk. Dat kan bijvoorbeeld door CERTs en andere sectorale organisaties niet alleen een responstaak te geven, maar ook een auditrol toe te delen richting fabrikanten. Voorwaarde is dat alle betrokken partijen deze aanpak vanaf het moment van de ontwikkeling van software hanteren. Een samenwerkingsverband van partijen dat voortdurend alert blijft, een vrije informatiestroom over software-kwetsbaarheden en een waarschuwingssysteem voor alle potentiële slachtoffers zijn daarbij randvoorwaarden.

De vele cyberaanvallen van de afgelopen jaren hebben laten zien dat een gezamenlijke aanpak van alle betrokken partijen tegen digitale onveiligheid urgent en noodzakelijk is. De kloof groeit tussen digitale afhankelijkheid en de dreigingsomvang aan de ene kant; en de mate waarin de samenleving daartegen weerbaar is aan de andere kant. Snel en fundamenteel ingrijpen is nodig om te voorkomen dat de maatschappij ontwricht raakt. De bestrijding van cybercriminaliteit is daarbij een belangrijk sluitstuk van een effectieve aanpak om tot het veilig gebruik van software te kunnen komen. Dit vraagt om centrale regie vanuit de overheid, vanuit een domein-overstijgende visie en strategie op wat nodig is om de digitale veiligheid van organisaties in Nederland te waarborgen.

AANBEVELINGEN

Dit onderzoek laat zien dat kwetsbaarheden in software leiden tot onveiligheid voor organisaties die software gebruiken, en voor hen die van deze organisaties afhankelijk zijn. De kloof groeit tussen digitale afhankelijkheid en de dreigingsomvang enerzijds, en de weerbaarheid van de samenleving daartegen anderzijds. Snel en fundamenteel ingrijpen is nodig om te voorkomen dat de maatschappij ontwricht raakt. Daarom doet de Onderzoeksraad voor Veiligheid aanbevelingen. De eerste aanbeveling is erop gericht om op korte termijn de responscapaciteit te vergroten. De erna volgende aanbevelingen hebben als doel om op de langere termijn het publieke en private stelsel te versterken en prikkels te introduceren zodat er een systeem ontstaat waarbinnen fabrikanten en afnemers voortdurend werken aan het veiliger maken van software.

Aan het Nederlandse kabinet en aan organisaties in Nederland die software gebruiken:[3]

1. Zorg er op korte termijn voor dat alle potentiële slachtoffers van cyberaanvallen snel en doeltreffend - gevraagd en ongevraagd - worden gewaarschuwd, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid. Breng daartoe private en publieke responscapaciteit samen en zorg daarbij voor voldoende mandaat en wettelijke waarborgen.

Toelichting: Het gaat hierbij in ieder geval om informatie over welke systemen van welke organisaties kwetsbaar zijn en risico lopen om aangevallen te worden (zogenoemde 'slachtofferinformatie'). Momenteel staat de juridische interpretatie van de AVG/GDPR (IP-adressen als persoonsgegeven) en de Wbni (mandaat van het NCSC beperkt tot Rijk en vitaal) het NCSC in de weg om alle slachtoffers waar zij informatie over krijgen te waarschuwen en om zelf proactief deze informatie te verzamelen ('scannen').

Aan de Eurocommissaris voor Interne Markt en de Eurocommissaris voor een Europa dat klaar is voor het digitale tijdperk:

2. Zorg dat uw initiatieven om te komen tot wetgeving voor veiligere software leiden tot een Europese verordening die de verantwoordelijkheid van fabrikanten vastlegt en afnemers inzicht geeft in hoe fabrikanten die verantwoordelijkheid invullen. Leg vast dat fabrikanten aansprakelijk zijn voor de gevolgen van softwarekwetsbaarheden.

Toelichting: Essentiële elementen van deze verordening zijn onder andere – maar niet uitsluitend - verplichte deelname aan *bug bounty* programma's, richtlijnen voor onafhankelijke audits, het melden van kwetsbaarheden, traceerbaarheid, *recalls*, en het delen van lessen uit cyberaanvallen. Ervaringen met wet- en regelgeving als de AVG/GDPR hebben bewezen dat Europese regulering in het digitale domein haalbaar en effectief is.

3 Uit praktische overwegingen schrijft de Onderzoeksraad de overheid in zijn rol als afnemer aan via de staatssecretaris van Binnenlandse Zaken, het Interprovinciaal Overleg, de Vereniging van Nederlandse Gemeenten en de Unie van Waterschappen. De andere organisaties, waaronder zorg, onderwijs, vitale aanbieders en het overige bedrijfsleven schrijft de Raad aan via de bij de SER betrokken ondernemersorganisaties VNO-NCW, MKB-Nederland en LTO Nederland.

Aan fabrikanten van software gezamenlijk:[4]

3. Ontwikkel met andere fabrikanten *good practices* om software veiliger te maken. Neem in de overeenkomsten met uw afnemers op dat u zich hieraan committeert.
4. Waarschuw en help al uw afnemers zo snel en doeltreffend mogelijk wanneer kwetsbaarheden in software gesignaleerd worden. Schep de randvoorwaarden die noodzakelijk zijn om uw afnemers te kunnen waarschuwen.

Toelichting: De verantwoordelijkheid en mogelijkheden om software veiliger te maken en om afnemers te waarschuwen ligt in de eerste plaats bij fabrikanten zelf.

Aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Economische Zaken en Klimaat (ten behoeve van alle organisaties en consumenten in Nederland):[5]

5. Bevorder dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten. Zorg dat de overheid daarbij een voortrekkersrol speelt. Ga uit van het principe: collectieve samenwerking waar mogelijk; branche-specifiek waar noodzakelijk.

Toelichting: Het is noodzakelijk dat afnemers hun krachten bundelen zodat zij hun positie richting fabrikanten versterken en schaarse cybersecurity-expertise gezamenlijk zo doelmatig en effectief mogelijk inzetten, zoals een aantal Nederlandse banken nu al doet.

Aan het Nederlandse kabinet:

6. Creëer naar analogie van de Comptabiliteitswet een wettelijke basis voor de beheersing van digitale veiligheid door de overheid.
7. Verplicht alle organisaties om op eenduidige wijze verantwoording af te leggen over de wijze waarop zij digitale veiligheidsrisico's beheersen.[6]

Toelichting: De wijze waarop overheden en bedrijven de risico's die gepaard gaan met digitalisering beheersen en zich daarover verantwoorden is vooralsnog vrijblijvend. Versnippering van verantwoordelijkheden staat een slagvaardig optreden in de weg.

4 Deze aanbeveling is gericht aan *alle* fabrikanten van software. Uit praktische overwegingen schrijft de Onderzoeksraad de fabrikanten aan die betrokken waren bij de voorvallen die dit onderzoek beschrijft, de gemeenschappen van de betrokken *open source*-projecten en de (leden van de) brancheorganisatie Business Software Alliance.

5 Zie voetnoot 2. Vanwege de relevantie van veilige software voor eindgebruikers (inclusief consumenten) dient ook de Consumentenbond hierbij te worden betrokken. En de Kamer van Koophandel voor ondersteuning aan organisaties.

6 Het ligt in de rede om aan te sluiten bij bestaande structuren en verplichtingen in de Comptabiliteitswet 2016 (van toepassing op overheden), Burgerlijk Wetboek (niet-beursgenoteerde rechtspersonen), nadere voorschriften controle- en overige standaarden (NV COS) vanuit de NBA en geharmoniseerde wetgeving voor naamloze vennootschappen vanuit de EU.

Essentieel is dat er een sluitend stelsel komt dat organisaties helpt om de digitale veiligheid op systematische en doelmatige wijze te beheersen. Mogelijke elementen zijn een eenduidig mandaat voor CISO's bij de overheid, toezicht dat is belegd bij de minister die het aangaat en voor alle organisaties verplichte verantwoording over de beheersing van digitale veiligheidsrisico's, via jaarverslagen en onder controleverklaring van de accountant.

ir. J.R.V.A. Dijsselbloem

Voorzitter van de Onderzoeksraad

mr. C.A.J.F. Verheij

Secretaris-directeur

LIJST VAN AFKORTINGEN EN BEGRIPPEN

AAN	Anti Abuse Netwerk
ABDO	Algemene Beveiligingseisen voor Defensieopdrachten
ADC	Application Delivery Controller
AIVD	Algemene Inlichtingen-en Veiligheidsdienst
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BIG-IP	Productlijn van F5 Networks gericht op onder andere toegangscontrole en security
BIO	Baseline Informatiebeveiliging Overheid
(Ministerie van) BZ	Ministerie van Buitenlandse Zaken
(Ministerie van) BZK	Ministerie van Binnenlandse Zaken en Koningsrijkrelaties
CERT	Computer Emergency Reponse Team
CIO	Chief Information Officier
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
Citrix	Software producent
Citrix NetScaler	Software product van Citrix
CMDB	Configuration Management Database
CSIRT	Computer Security Incident Response Team
CSR	Cyber Security Raad
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DIVD	Dutch Institute for Vulnerability Disclosure
Dreigingsinformatie	Concrete informatie over dreigingen die zeer specifiek worden gericht op bepaalde partijen, of waar bepaalde partijen of systemen kwetsbaar voor zijn, zoals de gegevens van (potentiële) slachtoffers (slachtofferinformatie), daders (daderinformatie) of kwetsbare systemen, bijvoorbeeld in de vorm van IP-adressen[7]
DTC	Digital Trust Center
(Ministerie van) EZK	Ministerie van Economische Zaken en Klimaat
F5	Software producent
Fortigate	Software product van Fortinet
Fortinet	Software producent
GDPR	General Data Protection Regulation

7 Dialogic en TU/e, *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity in opdracht van WODC*, 14 oktober 2020.

IAo	Interdepartementaal Afstemmingsoverleg
ICCb	Interdepartementale Commissie Crisisbeheersing
ICO	Inkoopeisen Cybersecurity Overheid
ICT	Informatie- en communicatietechnologie
IoT	Internet of Things
ISAC	Information Sharing and Analysis Center
ISO 27001	Wereldwijd erkende norm voor informatie beveiligingsmanagement
(Ministerie van) JenV	Ministerie van Justitie en Veiligheid
Kwetsbaarheid	Zwakheid in software die misbruikt kan worden door aanvallers om een netwerk binnen te dringen
LDS	Landelijk Dekkend Stelsel
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MFA	Meerfactorauthenticatie
NCC	Nationaal Crisis Centrum
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDN	Nationaal Detectie Netwerk
NIS directive	Network and Information Security directive
OKTT	Objectief kenbaar tot taak; een organisatie die objectief tot taak heeft om organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot netwerk- en informatiesystemen
Palo Alto	Software producent
PoC	Proof of Concept
PSIRT	Product Security Incident Response Team
Pulse Secure	Software producent (onderdeel van Ivanti sinds december 2020)
SaaS	Software as a Service
SDLC	Secure Development Lifecycle
Slachtofferinformatie	Informatie over (potentiële) slachtoffers[8]
SSL VPN	Secure Socket Layer Virtual Private Network

8 Dialogic en TU/e, *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity in opdracht van WODC*, 14 oktober 2020.

Voorval	Gebeurtenis die de dood of letsel van een persoon dan wel schade aan een zaak of het milieu veroorzaakt, alsmede een gebeurtenis die gevaar voor een dergelijk gevolg in het leven heeft geroepen[9]
VPN	Virtual Private Network
Wbni	Wet Beveiliging Netwerk- en Informatiesystemen
Zaak	Een voor menselijke beheersing vatbaar stoffelijk object. Op grond van rechtspraak worden ook warmte, informatie en elektriciteit als zaken aangemerkt[10]

Bij het samenstellen van deze begrippenlijst is onder meer gebruik gemaakt van het Cybersecurity Woordenboek.[11]

9 Artikel 3 Rijkswet Onderzoeksraad voor veiligheid.
10 Artikel 2 Burgerlijk Wetboek Boek 3.
11 Zie onder andere https://www.digitaltrustcenter.nl/cybersecurity-woordenboek

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 stelselverantwoordelijkheid 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.

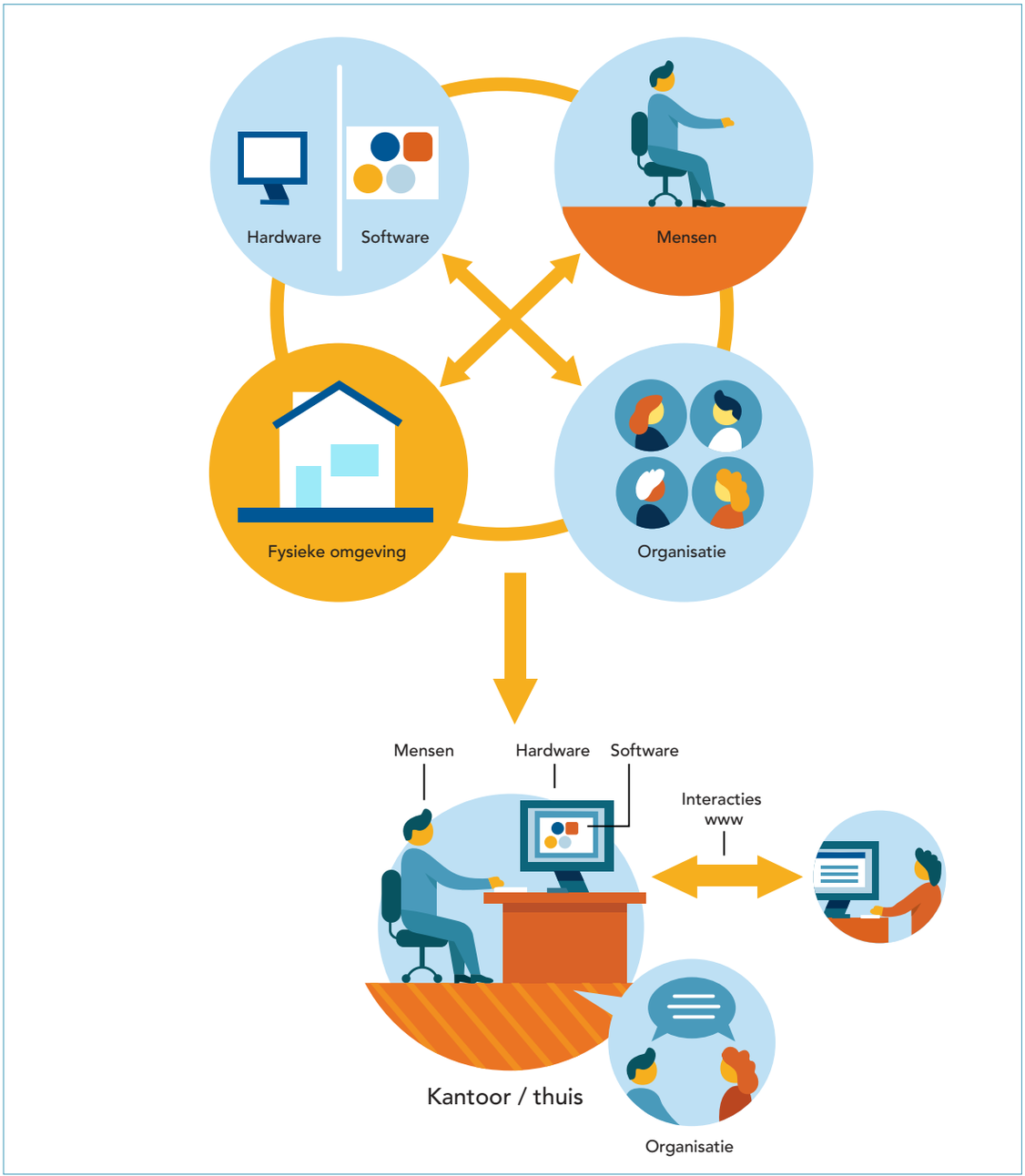
2 RELEVANTE BEGRIPPEN TOEGELICHT

Dit hoofdstuk bevat achtergrondinformatie die van belang is om de beschrijving en analyse van de voorvallen in de hoofdstukken erna te kunnen begrijpen en te kunnen duiden. Het hoofdstuk begint met een uitleg over wat digitale systemen zijn, hoe kwetsbaarheden kunnen ontstaan die de veiligheid aantasten en op welke manier de risico's worden voorkomen en beheerst. We beschrijven een aantal begrippen en mechanismen die centraal staan in dit onderzoek. Sommige begrippen zijn op meerdere manieren uitlegbaar, hier beschrijven we wat we er in dit onderzoek onder verstaan.

2.1 (Digitaal) systeem[21]

Digitaal systeem is een begrip dat een smalle tot brede betekenis kan hebben. In ons onderzoek geven we het een brede betekenis en verstaan we daar de volgende zaken onder. Ten eerste de techniek, bestaande uit hardware (bijvoorbeeld computers, printers, netwerken) enerzijds, en software anderzijds. En de fysieke omgeving, zoals het gebouw, Ten tweede de mensen die de techniek gebruiken om bepaalde activiteiten te kunnen uitvoeren. Ten derde de organisatie waarbinnen de techniek en de mensen zich bevinden. Ten slotte bevindt dit systeem zich in een complexe omgeving. Dat behelst de onderlinge interacties van de genoemde onderdelen met de maatschappij, denk aan regelgeving, prikkels, (re)acties en met het internet. We noemen dit geheel ook wel een socio-technisch systeem. Een aantal afzonderlijke onderdelen van het systeem wordt in figuur 1 nader uitgelegd.

21 In dit onderzoek wordt aangesloten bij definities en concepten uit de domeinen *Security Engineering* en *Systems Engineering*.



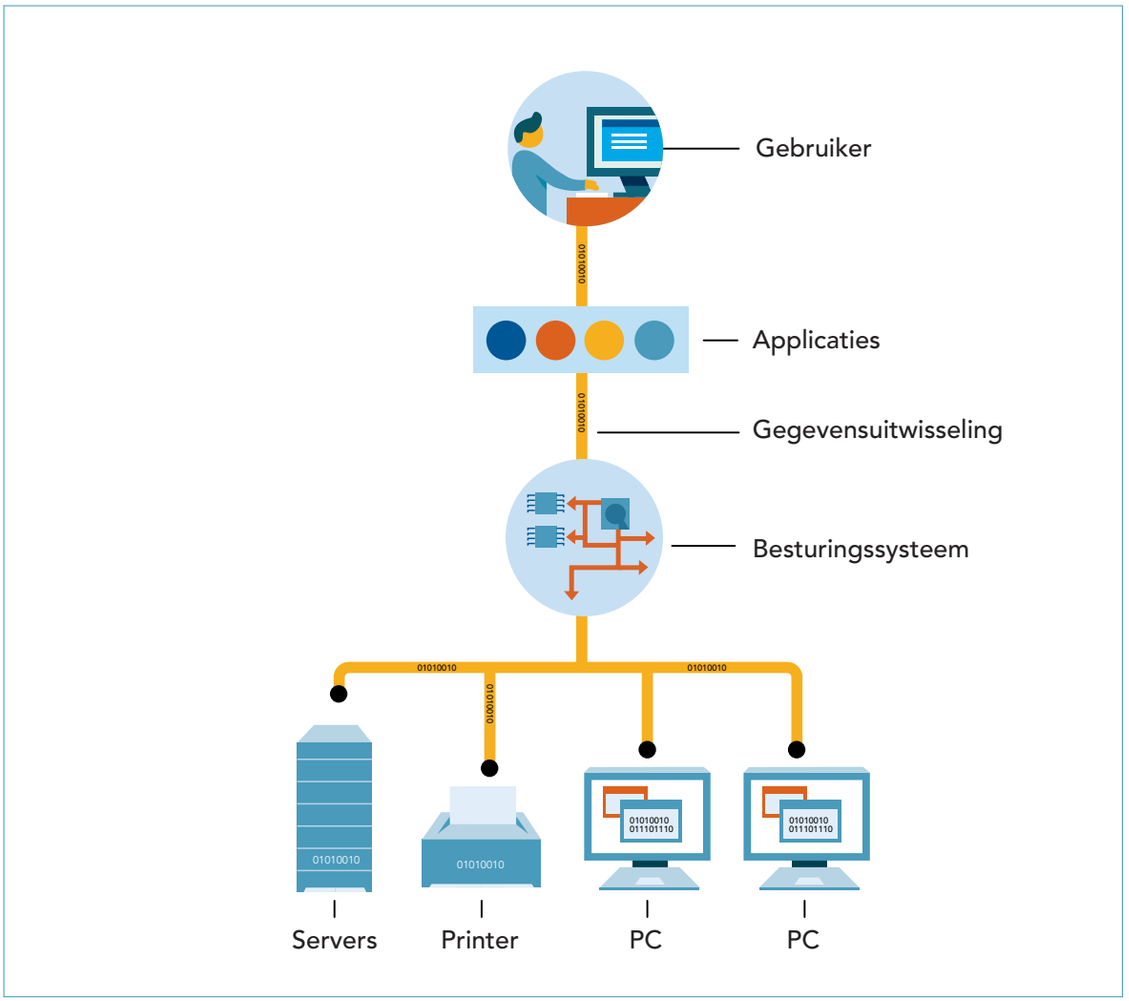
Figuur 1: Socio-technisch systeem.

2.1.1 Techniek: netwerk, hardware, software[22]

Digitalisering vereist het opzetten en onderhouden van een ICT-fundament: het geheel aan ICT-componenten (hardware en software) die het digitale fundament vormen van de organisatie. Hardware zijn de elektronische en mechanische onderdelen van een digitaal systeem, de tastbare onderdelen. Verschillende hardware-onderdelen zoals pc's, printers en servers (netwerkcomputers voor het opslaan en doorgeven van informatie) zijn met elkaar verbonden: zij vormen samen een netwerk. Software is de computercode die het mogelijk maakt dat de hardware-onderdelen onderling informatie uitwisselen. Elk digitaal fundament bestaat uit een aantal universele onderdelen: rekenkracht via de *processing units*, een transportnetwerk om data te kunnen overbrengen van het ene naar

22 Zie onder andere Anderson, R. *Security Engineering*, 2020. Cisco *CCNA 200-301 Official Cert Guide*, 2020.

het andere onderdeel en *storage servers* waar data wordt vastgelegd, opgeslagen en weer kan worden opgehaald. Dit fundament kent een aantal lagen: de besturingslaag die de hardware aanstuurt, de functies het digitale systeem moet vervullen (applicaties) en de interactie met de gebruiker.



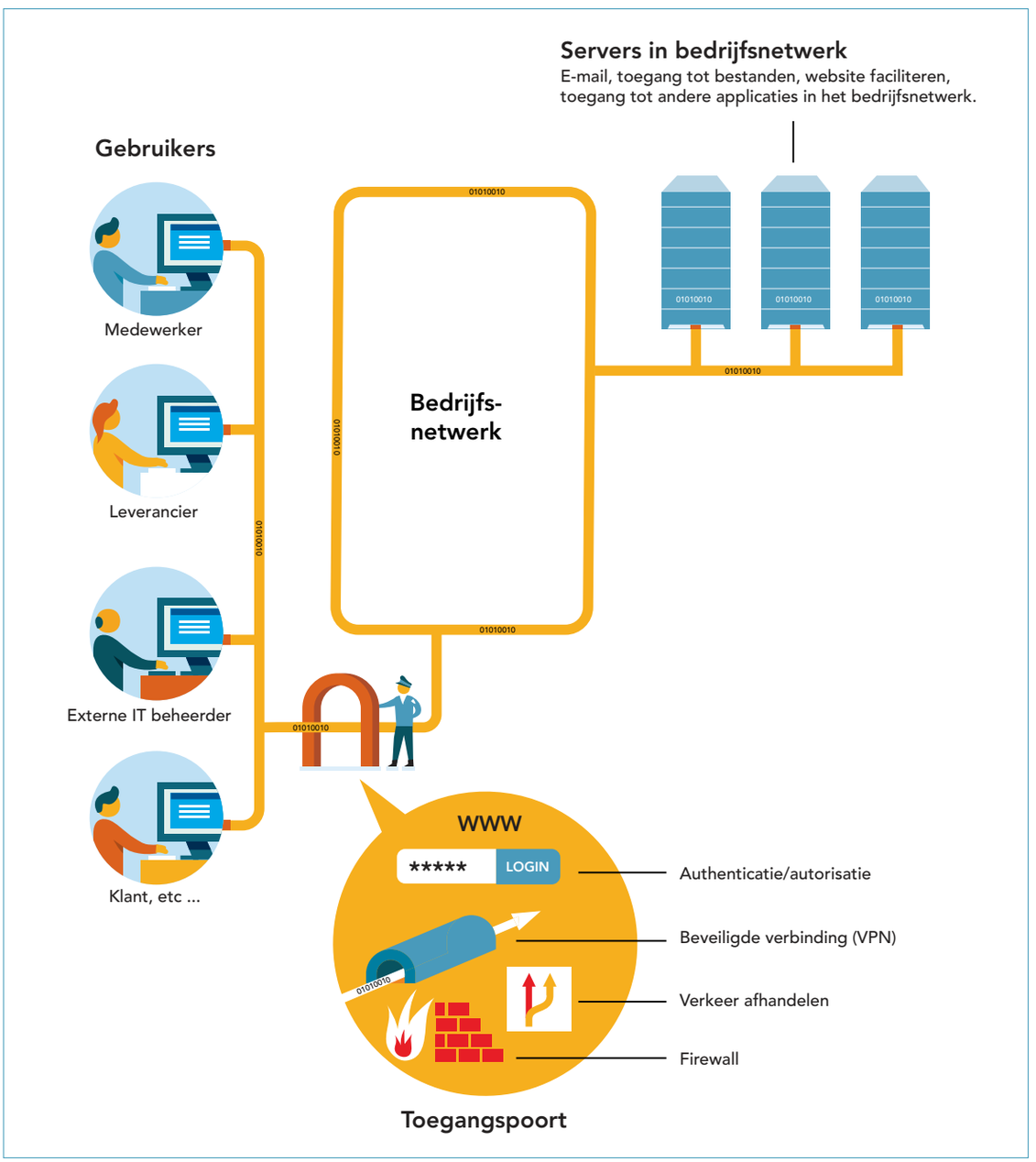
Figuur 2: Schematische weergave van de opbouw van een ICT-fundament.

In de meeste organisaties moet informatie gedeeld worden met anderen buiten de organisatie. Het netwerk van de organisatie is om die reden vaak verbonden met het internet (de digitale buitenwereld). Voor de organisatie is het cruciaal en onontkoombaar dat bevoegden zo goed mogelijk informatie kunnen uitwisselen binnen het netwerk en daarbuiten. Dit maakt digitale systemen wel kwetsbaar. Onbevoegden moeten zo veel mogelijk worden tegengehouden.

Vanuit het perspectief van de gebruiker van een digitaal systeem van een organisatie ziet een systeem er als volgt uit. De gebruiker werkt op een apparaat (zoals PC of laptop) dat via een kabel of draadloos is verbonden met het bedrijfsnetwerk. Het bedrijfsnetwerk speelt zich af buiten het gezichtsveld van de gebruiker en ziet er in essentie meestal als volgt uit. Het netwerk bestaat uit een aantal servers. Dat zijn apparaten die bepaalde functies vervullen, zoals e-mails verzenden en ontvangen, bestanden en databases opslaan, websites of andere toepassingen faciliteren.

De gebruiker van het digitale systeem (dat kan een medewerker zijn of een externe gebruiker, zoals een burger bij de gemeente, of een huisarts bij een ziekenhuis) wil een bepaalde functie van het digitale systeem gebruiken. Als hij of zij niet direct aangesloten is op het digitale systeem, dan gaat dat vanaf afstand. De gebruiker maakt via het internet verbinding met het digitale systeem via een (softwarematige) toegangspoort, vaak is dat een webpagina waarop de gebruiker inlogt en het systeem kan controleren wie het is en welke toegangsrechten deze krijgt.

Tussen het digitale systeem en het internet worden meestal ook één of meerdere *firewalls* geplaatst. Ook kan het netwerk worden opgedeeld in onderdelen, waartussen *firewalls* kunnen worden geplaatst (netwerksegmentatie). Een *firewall* is hardware of software die het verkeer dat via het internet naar het netwerk gaat bekijkt en bepaald verkeer blokkeert. De beheerder van het digitale systeem bepaalt welk verkeer de *firewall* moet blokkeren.



Figuur 3: Toegangspoort naar het digitale systeem.

2.1.2 Mens en organisatie

Een digitaal systeem is niet alleen een kwestie van techniek. Mensen gebruiken namelijk de techniek om hun taken en werkzaamheden uit te voeren binnen de context van de organisatie. Naast de techniek hebben ook de acties van de mensen die de techniek gebruiken en beheren invloed op de prestatie en de veiligheid van de systemen. Verder is het beheer van het digitale systeem verbonden met diverse en soms conflicterende belangen en prioriteiten van de organisatie. Dat is bijvoorbeeld merkbaar wanneer het onderhoud van het digitale systeem ten koste kan gaan van de beschikbaarheid van het systeem. Of bij de keuzes die worden gemaakt om te investeren in uitbreiding of vervanging van software en andere onderdelen van het systeem. Deze organisatorische processen zijn daarom ook onderdeel van het digitale systeem.

Ontwerp en productie

De levenscyclus van een digitaal systeem en de software die daarin wordt gebruikt, begint bij het ontwerp en de productie ervan. Ook dat is een proces dat wordt uitgevoerd door mensen binnen de context van een organisatie, in dit geval de fabrikant van software. Daarbij kan sprake zijn van conflicterende belangen, zoals de keuze hoe veel tijd en middelen kan worden geïnvesteerd in het controleren en testen van de software voor een nieuwe versie op de markt komt. Daarnaast moeten we ons realiseren dat het internet en de software die mensen en organisaties gebruiken zijn ontwikkeld vanuit de wens om verbonden te zijn. Veiligheid en beveiliging waren minder relevant en speelden aanvankelijk geen centrale rol in de ontwikkeling en productie. In paragraaf 4.1 wordt verder ingegaan op het ontwerp en de ontwikkeling van software in relatie tot kwetsbaarheden die daarin voorkomen.

Aanschaf en ingebruikname

Een van de relevante organisatorische processen is de aanschaf van software, hoe de afnemer bepaalt of de software aan zijn eisen voldoet, waaronder veiligheidseisen en wat de gevolgen zijn voor de leverancier als blijkt dat software niet aan de eisen voldoet (aansprakelijkheid voor de gevolgen). Een veel gestelde veiligheidseis van afnemers aan leveranciers is het mogen uitvoeren van penetratietesten.[23] Een organisatie kan een penetratietest (kortweg *pentest*) zelf uitvoeren, laten uitvoeren door een andere partij, of de fabrikant vragen om een rapportage van een penetratietest van een derde partij. Deze pentesten kunnen gericht zijn op het toetsen van een bepaald product of van het totale netwerk, en kunnen zowel extern (van buiten het netwerk) of intern (wanneer de pentester binnen het netwerk toegang tot systemen probeert te krijgen) uitgevoerd worden.[24]

Software met de functie om een koppeling naar buiten te faciliteren (zoals Citrix-software of VPN producten) is vaak doelwit van aanvallers en daarom belangrijk om te testen, maar ook kwetsbaarheden in andere producten die een koppeling naar buiten hebben (om bijvoorbeeld updates binnen te halen) kunnen door aanvallers gebruikt worden om systemen binnen te dringen.

23 Een *pentest* is een beveiligingscontrole waarbij er van buitenaf wordt getoetst op kwetsbaarheden en er vervolgens wordt geprobeerd om via deze kwetsbaarheden in te breken in het systeem.
24 PT Security, *Penetration Testing of corporate information systems*, 2020.

Nadat een organisatie software heeft aangeschaft wordt het in gebruik genomen als onderdeel van het bedrijfssysteem van de organisatie. In deze fase zijn er verschillende maatregelen en processen die afnemers kunnen invoeren om hun bedrijfssystemen te beveiligen en zich voor te bereiden op incidenten.[25] Hieronder worden een aantal maatregelen en overwegingen uitgelegd die van belang zijn bij het mitigeren van risico's op incidenten naar aanleiding van een kwetsbaarheid in software.

Afhankelijkheid reduceren
Een manier om de afhankelijkheid van een bepaald product te verminderen, is om een tweede softwareproduct aan te schaffen. Wanneer het ene product niet meer functioneert, of niet meer veilig gebruikt kan worden, kan overgestapt worden op het andere product zodat organisatieprocessen door blijven gaan. Wanneer een systeem meervoudig is uitgevoerd, spreken we van redundantie.

Een andere manier om de afhankelijkheid van een bepaald softwareproduct te verminderen is door het netwerk op een manier in te richten dat er geen *single point of failure* is. Dat wil zeggen dat wanneer een systeem wegvalt, niet het hele netwerk uitvalt. Bij de selectie van software en het inrichten van een netwerk is het dan van belang om de afhankelijkheden in kaart te brengen en bewust af te wegen welke risico's er zijn bij het gebruik van bepaalde systemen. Dit kan de impact van incidenten verkleinen.

Preventie en detectie
Er zijn verschillende maatregelen mogelijk om aanvallen te kunnen voorkomen en detecteren. Een voorbeeld van een dergelijke maatregel is om toegang van buitenaf tot de systemen van een organisatie te beperken is het instellen van een *firewall*.[26] Een *firewall* is een machine die tussen een netwerk en het internet in staat, verkeer monitort, en mogelijk schadelijk verkeer tegenhoudt.[27]

Naast maatregelen om een aanvaller tegen te houden, zijn er ook maatregelen die organisaties kunnen nemen om de impact van incidenten te beperken wanneer deze toch plaatsvinden. Netwerksegmentatie is een maatregel die genomen kan worden om de gevolgen van eventueel binnendringen te beperken. Een gesegmenteerd netwerk is opgedeeld in meerdere sub-netwerken die ieder beschermd zijn en onnodig verkeer kunnen tegenhouden, bijvoorbeeld met behulp van een *firewall*. Wanneer een netwerk niet gesegmenteerd is, heeft een aanvaller toegang tot het gehele netwerk wanneer deze eenmaal binnen is. Hoe meer een netwerk gesegmenteerd is, hoe meer barrières een aanvaller tegenkomt wanneer deze in het gehele systeem van een organisatie binnen probeert te dringen. De aanvaller blijft op deze manier geïsoleerd in een bepaald segment van het netwerk.[28]

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

Om aanvallen op het bedrijfssysteem te kunnen opmerken, investeren veel organisaties in detectiemogelijkheden. Om aanvallers te kunnen detecteren, is *logging* van systemen cruciaal. Bij *logging* wordt de activiteit op systemen vastgelegd in logbestanden. Hierbij is het mogelijk om bij bepaalde activiteiten en kenmerken (signaturen) een *alertering* in te stellen, bijvoorbeeld bij verdachte inlogpogingen.[29] *Logging* is ook van belang bij het kunnen uitvoeren van onderzoek wanneer er een incident heeft plaatsgevonden. Wanneer er geen loggegevens beschikbaar zijn, of een aanvaller de mogelijkheid heeft deze aan te passen, is het onmogelijk om de bewegingen van een aanvaller in het netwerk na te gaan.

2.2 Kwetsbaarheden en beveiligingslekken[30]

Software die wordt gebruikt in netwerken van organisaties kan kwetsbaarheden bevatten.[31] Aanvallers kunnen die kwetsbaarheden misbruiken om het netwerk binnen te dringen. Ook kunnen kwetsbaarheden andere ongewenste gevolgen hebben, zoals dat een gebruiker onbedoeld schade kan aanrichten.

Kwetsbaarheden kunnen onder meer ontstaan bij het programmeren van de software of bij het samenvoegen van verschillende componenten. Kwetsbaarheden worden soms gevonden door de fabrikant van de software zelf, door organisaties die de software afnemen en gebruiken dan wel door hackers[32] die in opdracht van fabrikanten, afnemers, uit eigen beweging of in opdracht van derden (bijvoorbeeld statelijke actoren) naar kwetsbaarheden zoeken.

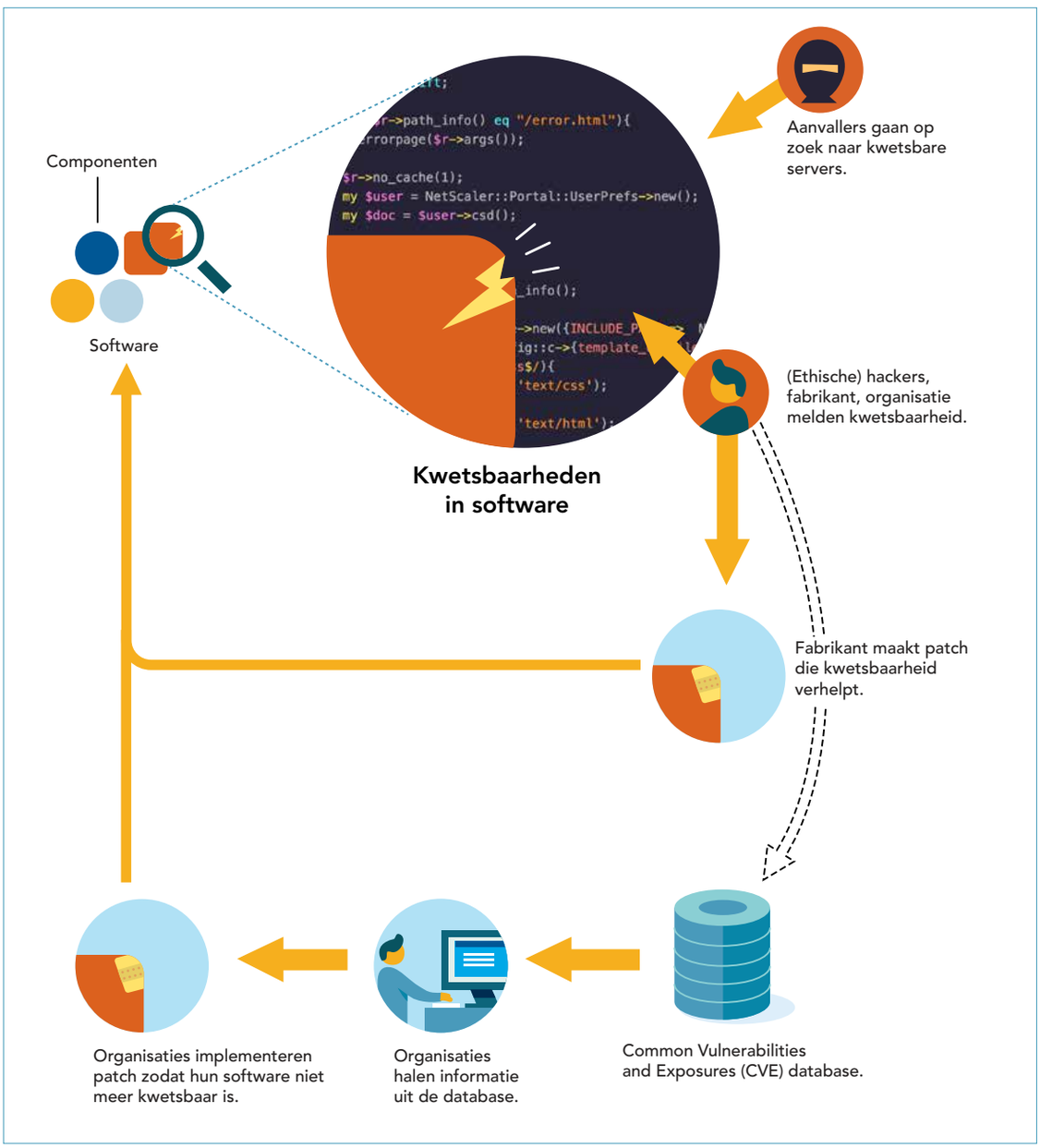
Ethische hackers[33] kunnen gevonden kwetsbaarheden aan de fabrikant en/of aan autoriteiten melden (*coordinated vulnerability disclosure* of *responsible disclosure*). Daarbij laten ze meestal ook zien hoe de kwetsbaarheid kan worden misbruikt om een kwetsbaar systeem binnen te dringen. Deze demonstratiemethode wordt *Proof of Concept code* genoemd.[34]

De fabrikant kan de kwetsbaarheid registreren en laten opnemen in de *Common Vulnerabilities and Exposures* (CVE) database. Dit is een database met kwetsbaarheden die zijn ontdekt en gepubliceerd door organisaties van over de hele wereld. Securityprofessionals kunnen deze database onder andere gebruiken om op eenduidige wijze te communiceren over kwetsbaarheden en de aanpak van verschillende kwetsbaarheden te coördineren en prioriteren.[35] Organisaties kunnen de door hun ontdekte kwetsbaarheid aan de CVE database toevoegen, daarbij wordt door analisten

29 https://www.ncsc.nl/onderwerpen/loginformatie, geraadpleegd op 16 juli 2021.
30 Zie publicaties van Mitre (CVE/CWE), OWASP, Security Engineering Anderson en Google (kader voor veilige software)
31 Hardware, mensen, fysieke omgeving en organisaties kunnen ook kwetsbaarheden bevatten. In dit onderzoek gaat het over kwetsbaarheden in software.
32 Iemand die inbreekt in een computersysteem. Het doel is beveiligingslekken op te sporen.
33 Ethische *hackers* of *whitehat hackers* werken vanuit de positieve intentie om beveiligingslekken op te sporen en zo de veiligheid te verbeteren.
34 Op basis van deze *Proof of Concept* code kan een aanvaller code maken die gebruikt kan worden om het systeem daadwerkelijk te misbruiken. Dit wordt een *exploit* genoemd.
35 https://cve.mitre.org/

een score toegekend aan de CVE die de ernst van de kwetsbaarheid aangeeft. Deze score wordt berekend aan de hand van het *Common Vulnerability Scoring System* (CVSS).

Soms vinden aanvallers de kwetsbaarheid eerder dan de fabrikant of ethische hackers, of wordt de *Proof of Concept code* of andere *exploit code* al bekendgemaakt voordat de fabrikant een patch voor de kwetsbaarheid heeft uitgegeven. In dat geval spreken betrokkenen van een *zero day exploit*. Aanvallers maken dan misbruik van de kwetsbaarheid *voordat* de fabrikant zijn afnemers over de kwetsbaarheid heeft kunnen informeren.



Figuur 4: Kwetsbaarheden en beveiligingslekken.

Wereldwijde handel in kwetsbaarheden en exploits[36]

Met de toegenomen digitalisering is een wereldwijde handel in zero *day exploits* ontstaan. Afhankelijk van hoe krachtig de *zero day* is om organisaties ermee te kunnen aanvallen, worden er duizenden tot (op de zwarte markt) miljoenen dollars voor betaald. In de eerste plaats door fabrikanten zelf, die ethische hackers die een kwetsbaarheid melden inmiddels grote bedragen betalen als beloning (*bug bounty*). Dit doen ze rechtstreeks of via zogenaamde *bug bounty platforms* zoals HackerOne[37].

Er zijn echter ook talrijke handelaren en tussenpersonen actief, die kwetsbaarheden opkopen van hackers om door te verkopen de hoogste bieder. Dit betreft onder meer statelijke actoren (zoals China en Rusland) en hun dienstverleners, en criminele actoren. Maar ook de VS en Nederland maken gebruik van onbekende kwetsbaarheden. Omdat dit een veiligheidsdilemma kan opleveren, heeft de Tweede Kamer een initiatiefwetsvoorstel in behandeling waarin wordt voorgesteld dat inlichtingen- en veiligheidsdiensten, opsporingsdiensten en het Ministerie van Defensie een afwegingskader hanteren voor de omgang met *zero days*.[38]

Er is ook een handel in *half day exploits*, gericht op het misbruiken van kwetsbaarheden waarvan de fabrikant al wel op de hoogte is en een patch beschikbaar heeft gesteld, maar waarvan de meeste gebruikers nog niet op de hoogte zijn. Nadat er verschillende kwetsbaarheden waren gelekt en gestolen, kwam steeds meer kritiek op inlichtingendiensten zoals de Amerikaanse NSA die *zero days* verzamelen en bij zich houden in plaats van dat ze de fabrikant daarover inlichten.[39] Een andere strategie van aanvallers is *living off the land*. Dit houdt in dat ze gebruik maken van bekende kwetsbaarheden, al dan niet via *tooling* (geautomatiseerd zoeken en misbruiken), vanuit de aanname dat een substantieel deel van de gebruikers een kwetsbaarheid na lange tijd of niet verhelpt.

Gevaarlijke en veel voorkomende kwetsbaarheden in software kunnen ertoe leiden dat aanvallers bepaalde veiligheidsbarrières kunnen omzeilen, zoals:[40]

- de toegangscontrole van een gebruiker via de software;
- de controle op de bevoegdheden van een gebruiker (of een gebruiker gegevens mag invoeren die ongewenste activiteiten op het netwerk mogelijk maken, zoals de mogelijkheid om opgeslagen gegevens te veranderen);
- het voorkomen dat een gebruiker zich door het gehele netwerk kan verplaatsen en overal bij kan komen.

36 Perlroth, N., *This is how they tell me the world ends: the Cyberweapons Arms Race*, 2021.
37 HackerOne is opgericht door twee Nederlandse *hackers* om kwetsbaarheden te zoeken in opdracht van grote techbedrijven zoals Facebook, Google, Apple, Microsoft en Twitter. Meerdere ethische *hackers* hebben meer dan 1 miljoen dollar verdiend door kwetsbaarheden te vinden en te melden via dit platform.
38 https://www.eerstekamer.nl/wetsvoorstel/35257_initiatiefvoorstel_verhoeven
39 Schneier, B., *New leaks prove it: the NSA is putting us all at risk to be hacked*, Vox, 2016. Ars Technica, *Cisco confirms NSA-linked zeroday targeted its firewalls for years*, 2016. Greenberg, A., *The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days*, WIRED, 2016.
40 https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

Als een organisatie software gebruikt die één of meer kwetsbaarheden bevat, dan kan dit ertoe leiden dat een *beveiligingslek* ontstaat in diens digitale systeem. De mate waarin een kwetsbaarheid tot een beveiligingslek leidt, is mede afhankelijk van de wijze waarop de organisatie de software gebruikt en welke preventieve maatregelen de organisatie heeft genomen om een aanval te voorkomen dan wel (tijdig) te detecteren, (eventueel) automatisch te reageren en de impact van een aanval te beperken. Aansprakelijkheden van fabrikant en organisaties dienen daarbij in ogenschouw te worden genomen. De wettelijke kaders zijn beperkt. In hoofdstuk 4 gaan we in op de prikkels die daarvan uitgaan naar betrokken partijen.

Het opzetten en onderhouden van veilige digitale systemen behelst meer dan het verhelpen van kwetsbaarheden en beveiligingslekken. Het is ook een kwestie van ontwerp, uitvoering, monitoring (inclusief adequate opvolging daarvan, anders is monitoring nutteloos) en het leren en bijsturen naar aanleiding van hoe dit in de praktijk uitpakt. Paragraaf 1.6 en bijlage C bevatten een referentiekader voor veilige software en digitale systemen vanuit verschillende benaderingen (zoals security engineering en lerende netwerken van gebruikers, fabrikanten en regulatoren). In hoofdstuk 3 komen verschillende kwetsbaarheden en beveiligingslekken aan de orde bij de beschrijving en analyse van de voorvallen. Hoofdstuk 4 bevat een analyse van hoe deze kwetsbaarheden ontstaan en hoe de risico's kunnen worden beheerst, zowel bij de ontwikkeling van software als bij het gebruik van software en tijdens de incidentrespons.

2.3 Aanvallers en hun werkwijzen

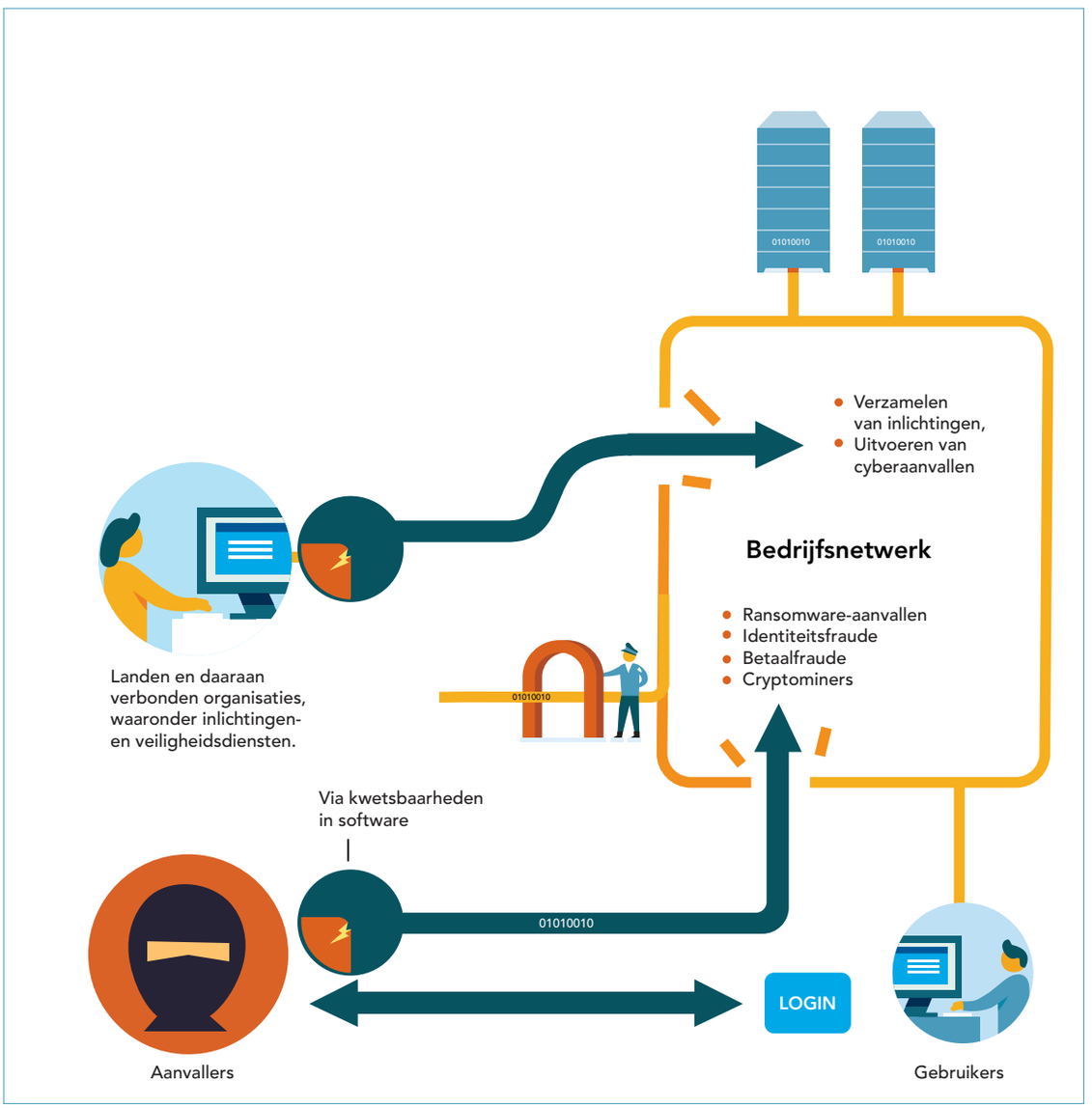
Digitale systemen kunnen door verschillende soorten aanvallers worden aangevallen. Deze aanvallers hebben verschillende motieven, doelwitten, bijpassende werkwijzen (rechtmatig dan wel onrechtmatig). In verband met kwetsbaarheden in software zijn vooral de volgende aanvallers relevant:[41]

- statelijke actoren (oftewel landen en daaraan verbonden organisaties), zoals inlichtingen- en veiligheidsdiensten van staten. Zij dringen digitale systemen binnen om onder meer inlichtingen te verzamelen, cyberaanvallen uit te voeren tegen andere landen of desinformatie verspreiden;
- criminelen die activiteiten uitvoeren zoals *ransomware*-aanvallen, identiteitsfraude en betaalfraude plegen (*phishing* bijvoorbeeld), maar ook cryptominers die gebruik willen maken van de rekenkracht van veel computers om cryptovaluta te valideren (dit wordt ook 'delven' of *mining* genoemd) of zij die het op specifieke personen hebben voorzien.

Het is niet altijd mogelijk om verschillende soorten aanvallers van elkaar te onderscheiden, omdat ze soms samenwerken of omdat criminelen als dekmantel worden gebruikt om zo te kunnen ontkennen als land betrokken te zijn bij een cyberaanval.

41 Anderson, R., *Security Engineering*, 2020. Ethische *hackers* proberen ook om systemen binnen te dringen. Dit is echter niet met het doel om het systeem aan te vallen, maar om de eigenaar/beheerder van het systeem te waarschuwen voor kwetsbaarheden en beveiligingslekken en daarmee de veiligheid te verbeteren.

Naast het misbruiken van een kwetsbaarheid in software zijn er andere technieken om een digitaal systeem gericht of ongericht aan te vallen. Deze technieken worden gebruikt *naast* of *in samenhang* met het misbruiken van kwetsbaarheden in software. Een voorbeeld van een ongerichte aanval is *phishing,* waarbij aanvallers naar een groot aantal mensen e-mails sturen met bijvoorbeeld het verzoek om via een vervalste website de inloggegevens voor hun internetbankieren in te vullen. Een voorbeeld van een gerichte aanval is *spear phishing* middels *social engineering*, waarbij de aanvaller zich verdiept in het slachtoffer en probeert het vertrouwen te wekken, zodat het slachtoffer bijvoorbeeld toegang geeft tot het digitale systeem of geld overmaakt. Een andere tactiek is om de aanval niet te richten op de organisatie zelf, maar op een toeleverancier of klant van de organisatie en bijvoorbeeld via updates van deze leveranciers of de software die deze leveranciers gebruiken de systemen van hun klanten binnen te dringen. Dit wordt ook wel een *supply chain attack* genoemd.



Figuur 5: Aanvallers en hun werkwijzen.

2.4 Veiligheid: safety en security, gevolgen, preventie en respons

Hierboven spraken we een aantal keer over veiligheid (*safety*) en beveiliging (*security*). Dit zijn twee verschillende begrippen die in het digitale domein beide relevant zijn. Ook zijn het veelomvattende containerbegrippen met onduidelijke en soms tegenstrijdige definities. Daarom beschrijven we hier wat we in dit onderzoek verstaan onder veiligheid en beveiliging en hoe beide begrippen verband houden met elkaar.

Veiligheid is een breed begrip dat op verschillende manieren kan worden gedefinieerd. Binnen de context van dit onderzoek verstaan we onder veiligheidsrisico 'de mogelijkheid dat een systeem als gevolg van interne condities of externe omstandigheden zijn omgeving kan schaden. Een voorbeeld hiervan is wanneer een auto door de uitval van de besturing een voetganger aanrijdt. Daarnaast zijn er beveiligingsrisico's, namelijk dat de vertrouwelijkheid, beschikbaarheid en/of integriteit van het digitale systeem kan worden aangetast door zijn omgeving, bijvoorbeeld door aanvallers.[42] In dit onderzoek beschouwen we veiligheids- en beveiligingsrisico's in samenhang.

Veiligheidsgevolgen kunnen op verschillende manieren optreden en zijn niet altijd zichtbaar. Organisaties merken niet altijd dat er in hun systemen is binnengedrongen, en als organisaties daar al inzicht in hebben, zijn ze daar zelden open over. Een aanval kan onzichtbaar blijven doordat aanvallers er – afhankelijk van hun motief – belang bij hebben om onopgemerkt te blijven. Soms duurt het maanden voor zij zich vertonen. In de tussentijd kunnen zij grote schade aanrichten of voorbereidingen treffen voor een latere aanval, zoals een *ransomware* aanval.[43]

De voorvallen in dit onderzoek hebben in sommige gevallen fysieke en sociale gevolgen voor burgers. Als het gaat om alle soorten cybercrime bij elkaar schat het CBS dat in 2018 in Nederland 1,2 miljoen mensen slachtoffer werden van cybercrime en dit aantal stijgt. Slachtoffers van cybercriminaliteit lijden naast financiële schade vaak ook emotionele en psychische schade en verliezen het vertrouwen in technologie, systemen en organisaties. Experts spreken in dit soort gevallen van 'cybertrauma'. Het is achteraf meestal niet meer te achterhalen hoe het komt dat burgers slachtoffers zijn geworden van cybercriminaliteit. Hun gestolen gegevens worden meestal niet direct misbruikt. Ze worden eerst verhandeld en wanneer de aandacht is weggeëbd, gebruiken kwaadwillenden de gegevens om bijvoorbeeld identiteitsfraude te plegen. In verreweg de meeste gevallen wordt daarna niet achterhaald wie de dader is, en wordt ook niet bekend hoe die aan de gegevens is gekomen. Dat kan via een kwetsbaarheid in software zijn geweest, maar ook via andere routes.[44]

42 Anderson, R., *Security Engineering*, 2020.
43 Een positieve uitzondering is de Universiteit Maastricht, die een symposium organiseerde over wat ze hadden geleerd van de *ransomware* aanval waardoor ze waren getroffen. https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt
44 https://www.cbs.nl/nl-nl/nieuws/2019/29/1-2-miljoen-slachtoffers-van-digitale-criminaliteit, https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime. FT, '*Cyber trauma' leaves online victims with psychological scars*, https://www.ft.com/content/1bb6e777-b615-461e-a4f5-3f89927e5ad6

Ook op het niveau van organisaties zijn veiligheidsgevolgen merkbaar. Economische spionage veroorzaakt schade aan de economie. Eén van de motieven van aanvallers om kwetsbaarheden in software te misbruiken om (ongemerkt) binnen te dringen in systemen is om hoogwaardige technologie te bemachtigen die door Nederlandse bedrijven en kennisinstellingen wordt ontwikkeld. Het gevolg van deze economische spionage is dat de concurrentiepositie van belangrijke sectoren verslechtert. Dit brengt aanzienlijke schade toe aan de economie (economische veiligheid). En daarmee komen we op het nationale niveau van de veiligheidsgevolgen. Daarbij is naast economische spionage ook relevant dat inlichtingendiensten in binnen- en buitenland waarnemen dat statelijke actoren op grote schaal misbruik maken van kwetsbaarheden in software (zoals bij de voorvallen die in hoofdstuk 3 zijn beschreven) om systemen van organisaties binnen te dringen.[45] Aanvallers hebben hiervoor verschillende motieven, naast economische spionage zijn dat onder meer spionage op eigen burgers en voorbereidingen voor het op een later moment uitvoeren van ontwrichtende handelingen (aanvallen op vitale infrastructuur, '*preparation of the battle field*').[46]

2.5 Veiligheidsketen en risicobeheersing bij (cyber)voorvallen

Voordat een (cyber)voorval plaatsvindt, zijn er verschillende fasen te onderscheiden waarin het risico van een dergelijk voorval kan worden weggenomen of worden beperkt:[47]

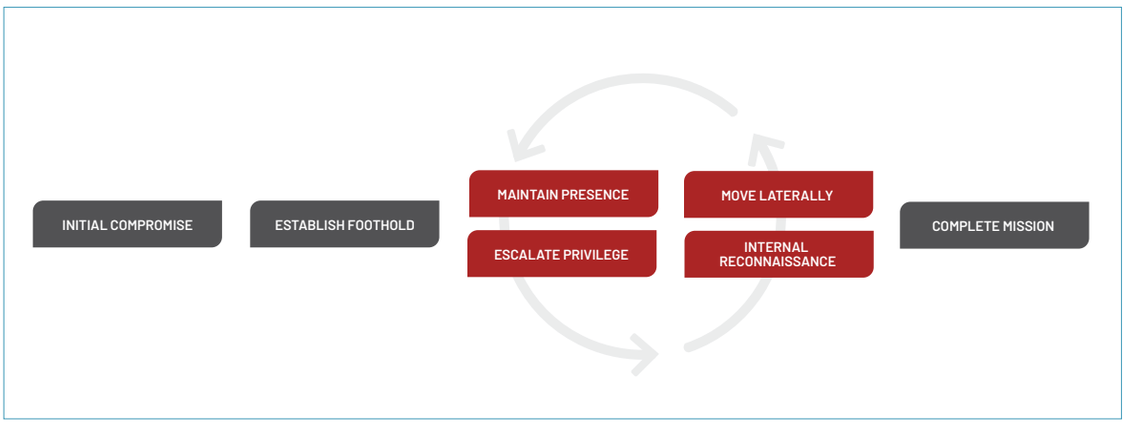
- proactie: maatregelen nemen om structurele oorzaken van onveiligheid en incidenten weg te nemen. In het fysieke veiligheidsdomein gaat het dan onder meer om het niet verlenen van een vergunning aan een bedrijf of activiteit als de risico's voor de omgeving te groot zijn;
- preventie: maatregelen nemen die incidenten voorkomen en/of de gevolgen beperken, zoals het instellen van een firewall of andere beveiligingsmaatregelen;
- preparatie: maatregelen nemen die een goede reactie op een kritieke gebeurtenis mogelijk maken. Een voorbeeld hiervan is het opstellen van een crisisplan en het trainen en oefenen op crisissituaties.
- incidentbestrijding (respons): dit zijn de activiteiten die plaatsvinden als het incident daadwerkelijk is opgetreden;
- nazorg: dat zijn de maatregelen die nodig zijn om de situatie weer te herstellen naar de normale gang van zaken. Zo is bij een *ransomware* aanval het herstel van gegevens een belangrijke voorwaarde voor een organisatie om weer te kunnen functioneren.

Deze fasen in de incidentbestrijding moeten aansluiten bij de verschillende fasen van de cyberaanval, zoals weergegeven in de *Cyber Attack Cycle* in de volgende figuur.

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

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

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



Figuur 6: Cyber Attack Cycle.[48]

Een organisatie zou in alle fasen maatregelen moeten nemen om een aanval te kunnen frustreren. Er zijn wat dat betreft per fase vier soorten reacties mogelijk op het risico (beheersmaatregelen): vermijden of voorkomen (*terminate*), verminderen (*treat*), overdragen of uitbesteden (*transfer*) of accepteren (*take*). Het resterende risico wordt restrisico genoemd (*residual risk*).

In dit onderzoek beschrijven we voorvallen die ontstaan nadat een kwetsbaarheid in software bekend is geworden, waardoor beveiligingslekken in digitale systemen van organisaties ontstaan. Het bekend worden van de kwetsbaarheid zien we als start van de fase van incidentbestrijding. Als de kwetsbaarheid bekend is bij de fabrikant, zal deze in veel gevallen publiceren in de *Common Vulnerabilities and Exposures* (CVE), sommige fabrikanten publiceren de kwetsbaarheden die ze zelf vinden niet (zie paragraaf 3.3). Deze publicatie bevat doorgaans (soms eerst tijdelijke) maatregelen die organisaties waar de software in gebruik is moeten nemen om de kwetsbaarheid en de daaruit volgende onveiligheid weg te kunnen nemen.

Bij een deel van de kwetsbaarheden, die gebruikt worden om grootschalige aanvallen op organisaties uit te voeren ontstaat dan een tweede fase in de incidentbestrijding, waarbij organisaties die de maatregelen niet uitvoerden voordat de aanvallen begonnen, ervan uit kunnen gaan dat zij zijn binnengedrongen.

In bepaalde sectoren hebben overheden en bedrijven organisaties opgericht die hun achterban kunnen bijstaan bij de incidentbestrijding. Dat zijn ten eerste de *Computer Security Incident Response Teams* (CSIRTs) en de *Computer Emergency Response Teams* (CERTs). Het Nationale Cyber Security Centrum (NCSC) is CSIRT voor de rijksoverheid en vitale aanbieders, en het CSIRT DSP voor digitale dienstverleners. Er zijn een aantal sectorale CERTs: Z-CERT voor zorginstellingen, SURFcert voor onderwijsinstellingen, IBD voor gemeenten en WM-CERT voor waterschappen. Daarnaast bestaan er Organisaties die Kenbaar Tot Taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten (OKTT's). Deze zijn opgericht om informatie te delen met hun achterban, zoals Stichting Cyber Weerbaarheidscentrum Brainport, *Abuse Information Exchange*, NBIP voor alle *hosters* in Nederland en het *Digital Trust Center* voor het niet-

48 Bron: Mandiant, Inc., 2021. All rights reserved.

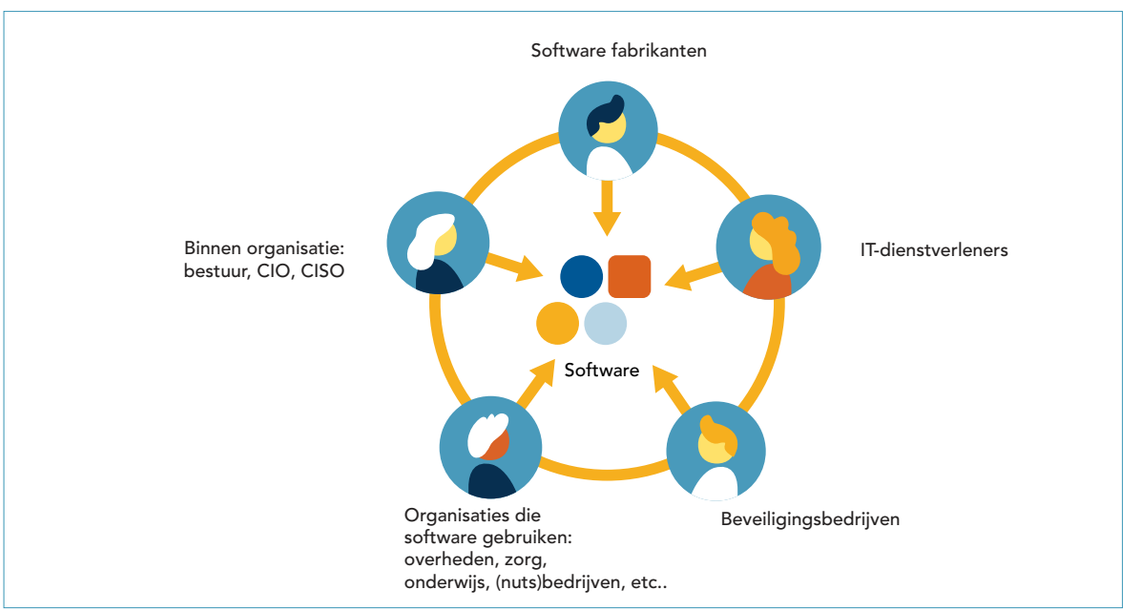
vitale bedrijfsleven.[49] Het beleid van de rijksoverheid is dat uiteindelijk Nederland wordt afgedekt door een zogenaamd Landelijk Dekkend Stelsel van CERTs en OKTT's, die door de rijksoverheid zijn benoemd als partijen waarmee het NCSC relevante informatie mag delen, en andere samenwerkingsverbanden (met name via het DTC).

Verder spelen naast commerciële beveiligingsbedrijven ook vrijwillige beveiligingsonderzoekers een rol bij het bestrijden van cyberincidenten. Onder meer door het scannen van het internet op kwetsbare servers en door organisaties en personen daarover te waarschuwen In Nederland heeft een aantal vrijwillige beveiligingsonderzoekers zich in oktober 2019 verenigd in het *Dutch Insitute for Vulnerability Disclosure* (DIVD). DIVD heeft sinds 2021 een *Computer Security Incident Response Team* (CSIRT), daarvoor heette dit het Security Meldpunt.

2.6 Stelsel

Verschillende soorten organisaties zijn betrokken bij ontwikkeling en gebruik van software, zoals:

- software fabrikanten;
- IT-dienstverleners;
- beveiligingsbedrijven;
- organisaties die software gebruiken, waaronder overheden, zorg, onderwijs, nutsbedrijven, bedrijven;
- binnen organisatie: bestuur, CIO, CISO.



Figuur 7: Organisaties die betrokken zijn bij de ontwikkeling en het gebruik van software.

49 Dit betreft de situatie op het moment van het opstellen van het rapport (oktober 2021). Een deel van de CERTs en OKTTs is na het voorval in december 2019 door de rijksoverheid benoemd als organisatie waarmee informatie mag worden gedeeld.

Het huidige beleid en de uitvoering daarvan ten behoeve van het Nederlandse cybersecurity-systeem is belegd bij verschillende ministeries. Voor het ondersteunen van de Rijksoverheid en de vitale partijen is het Nationaal Cyber Security Centrum (NCSC) ingericht, dit valt onder het ministerie van Justitie en Veiligheid (JenV). Voor het bereiken van het niet-vitale bedrijfsleven loopt de informatiestroom via onder meer het *Digital Trust Center* (DTC), dit valt onder het ministerie van Economische Zaken en Klimaat (EZK). Daarnaast is het ministerie van EZK CSIRT voor enkele categorieën digitale dienstverleners en verantwoordelijk voor het beleid en toezicht op onder meer telecom. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is beleidsverantwoordelijk voor de digitale overheid. De ministeries van Buitenlandse Zaken (BZ) en Defensie zijn op hun gebied verantwoordelijk voor het digitale domein. Verder zijn alle departementen verantwoordelijk voor de digitale veiligheid van de sectoren binnen hun domein.

De minister van JenV is de coördinerend bewindspersoon voor cybersecurity. Het in de vorige paragraaf genoemde NCSC en de NCTV (Nationaal Coördinator Terrorisme-bestrijding en Veiligheid) maken onderdeel uit van dit ministerie. Het NCSC was onderdeel van de NCTV totdat het op 1 januari 2019 een zelfstandig uitvoerende dienst werd van het ministerie van JenV met NCTV als opdrachtgever.[50] De wettelijke taak die het NCSC uitvoert is geregeld in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Op grond van deze wet zijn organisaties in vitale sectoren en aanbieders van essentiële diensten verplicht om ernstige digitale veiligheidsincidenten te melden bij het NCSC. Het NCSC op zijn beurt informeert en adviseert de vitale aanbieders[51] en de Rijksoverheid, zowel proactief als naar aanleiding van meldingen en incidenten, over dreigingen en incidenten in hun netwerk- en informatiesystemen. Daarbij werkt het NCSC onder meer samen met de AIVD. De ministeries en de vitale sectoren zijn primair zelf verantwoordelijk voor de hun eigen ICT, en informatiebeveiliging en digitale weerbaarheid.

50 De NCTV coördineert en ontwikkelt primair het beleid op het gebied van cybersecurity. Het NCSC is de uitvoeringsorganisatie ten aanzien van de wettelijke taken van de minister van JenV op dat gebied.

51 Ten tijde van het voorval met Citrix-software werden daaronder binnen de volgende vitale processen (als 'vitale aanbieder') aangewezen aanbieders verstaan: energie (gas, elektriciteit, aardolie, vervoer (havens en luchthavens). bankwezen, infrastructuur voor de financiële markt, drinkwater, digitale infrastructuur, nucleair, keren en beheren, financiële diensten, elektronische communicatiediensten/ICT; Besluit beveiliging netwerk- en informatiesystemen (aanwijzing vitale aanbieders en nadere regels over beveiliging van aanbieders van een essentiële dienst, versie januari 2019).

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.

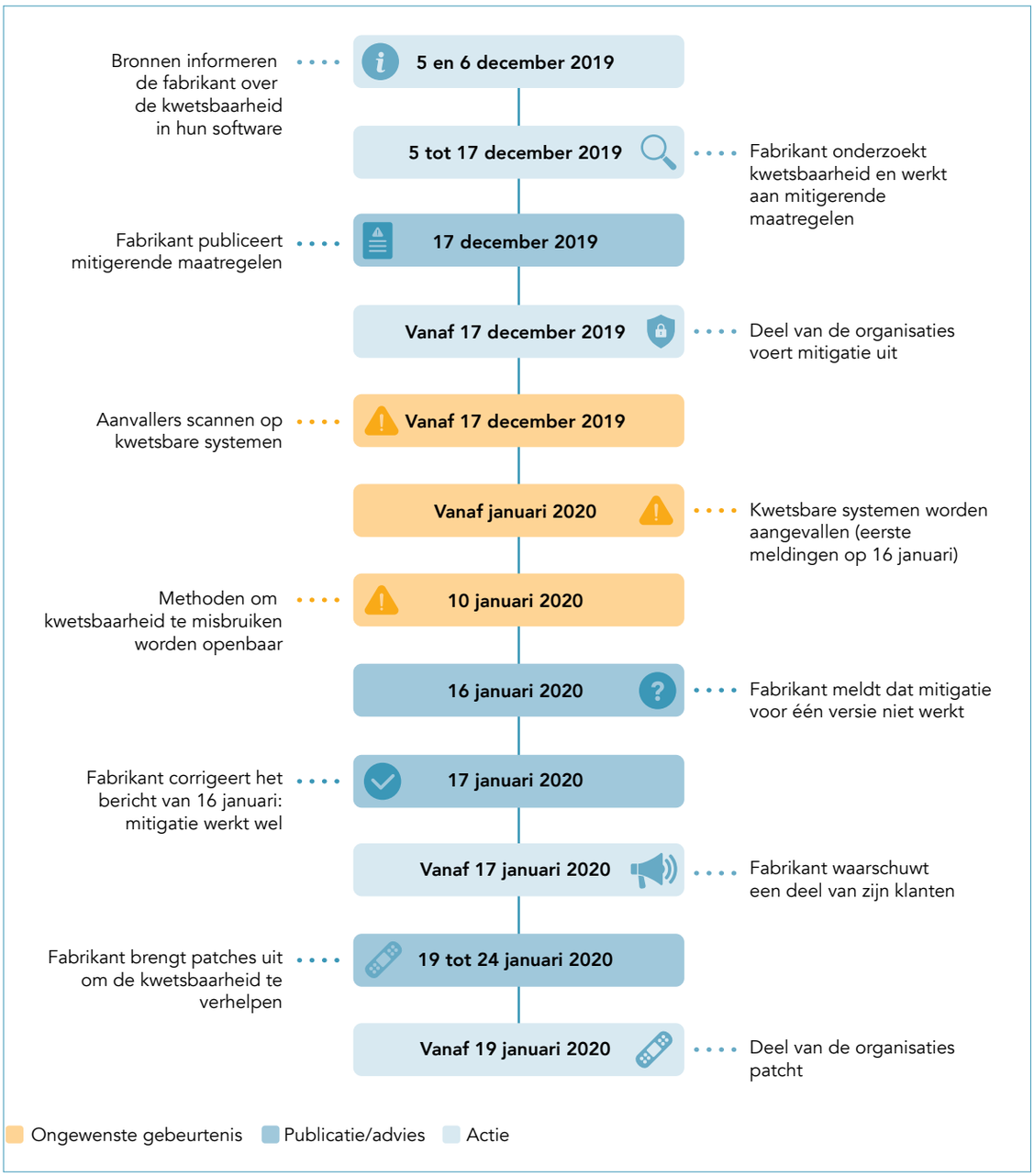
3.1 Toedracht beveiligingslekken door kwetsbaarheid in Citrix-software

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.

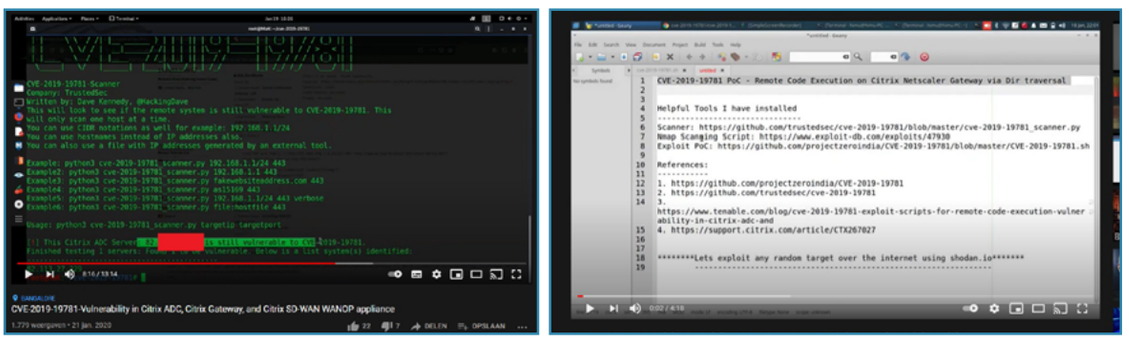
In de week na de bekendmaking publiceerde één van de bronnen die de kwetsbaarheid had gemeld aanvullende details over de kwetsbaarheid. In de periode daarna volgden publicaties van andere beveiligingsonderzoekers, waarin zij op basis van de mitigerende maatregel beschreven wat de aard van de kwetsbaarheid 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/

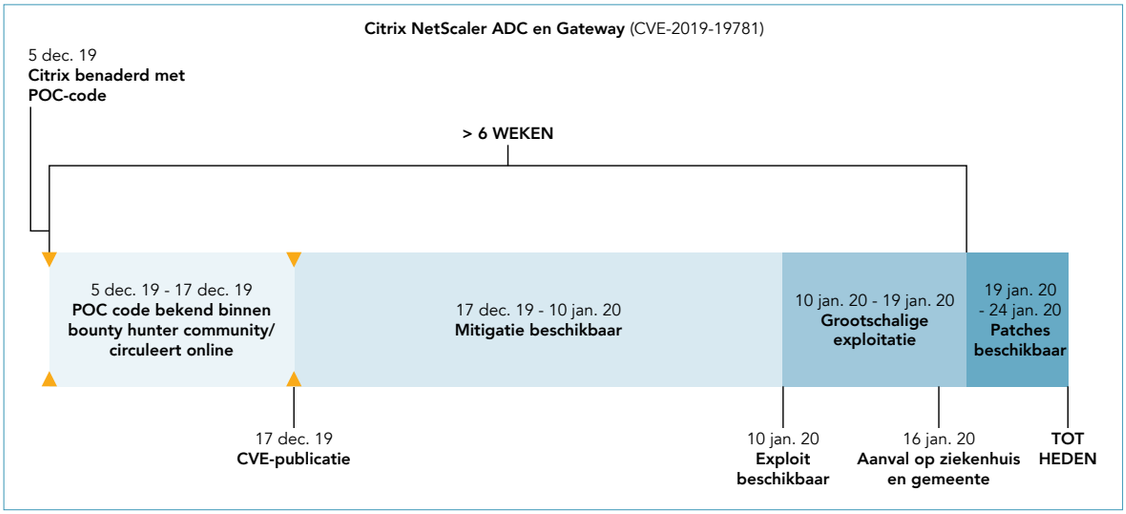
Naast het plaatsen van de alert op de website en in *social media*-berichten deed de fabrikant een poging om zo veel mogelijk van zijn klanten zelf te benaderen. In de periode van 17 tot 24 januari stuurde Citrix ruim 124.000 e-mails naar ongeveer 36.000 verschillende organisaties. In diezelfde periode 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.

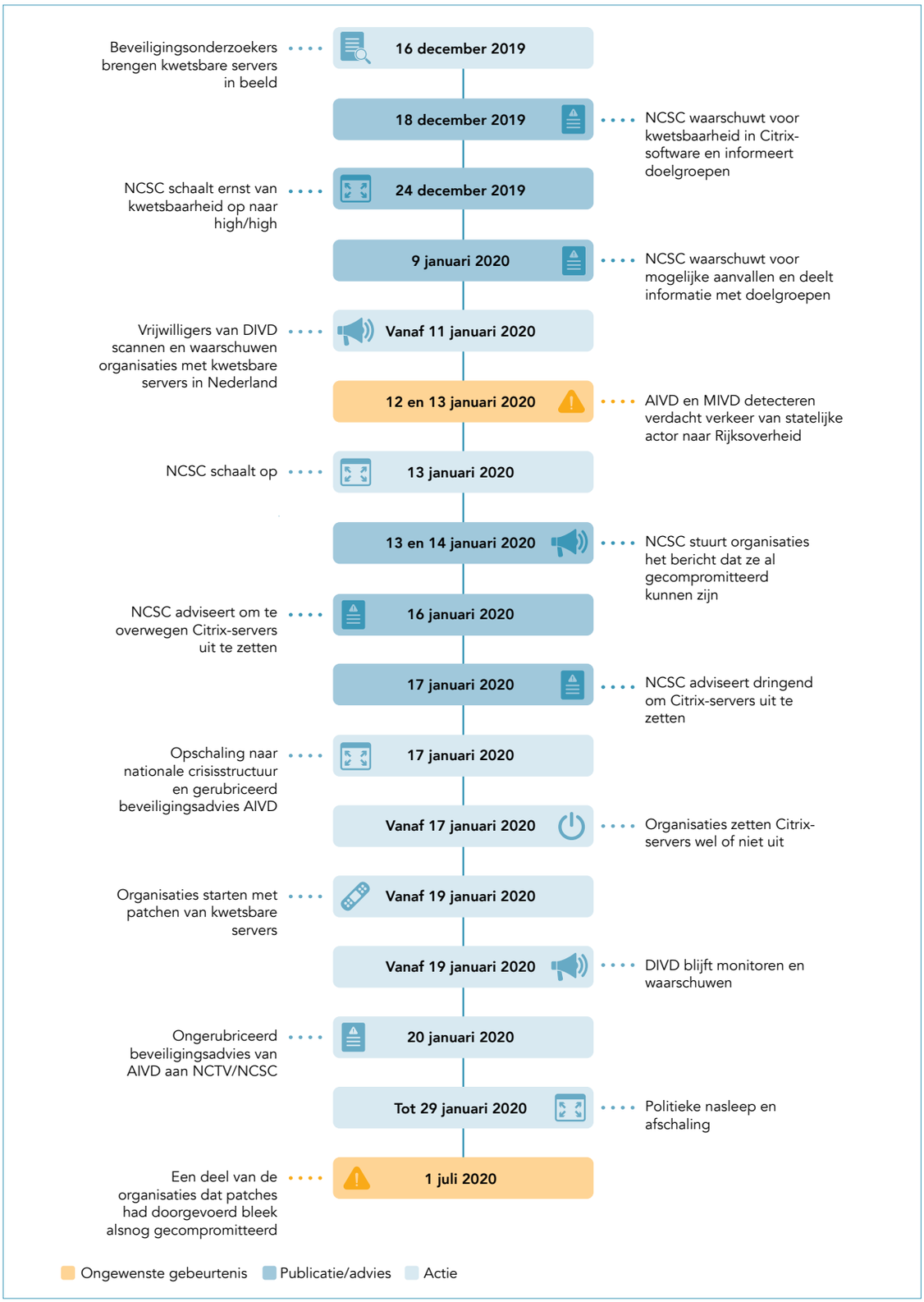
61 *Customer Relationship Management* (CRM).

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.

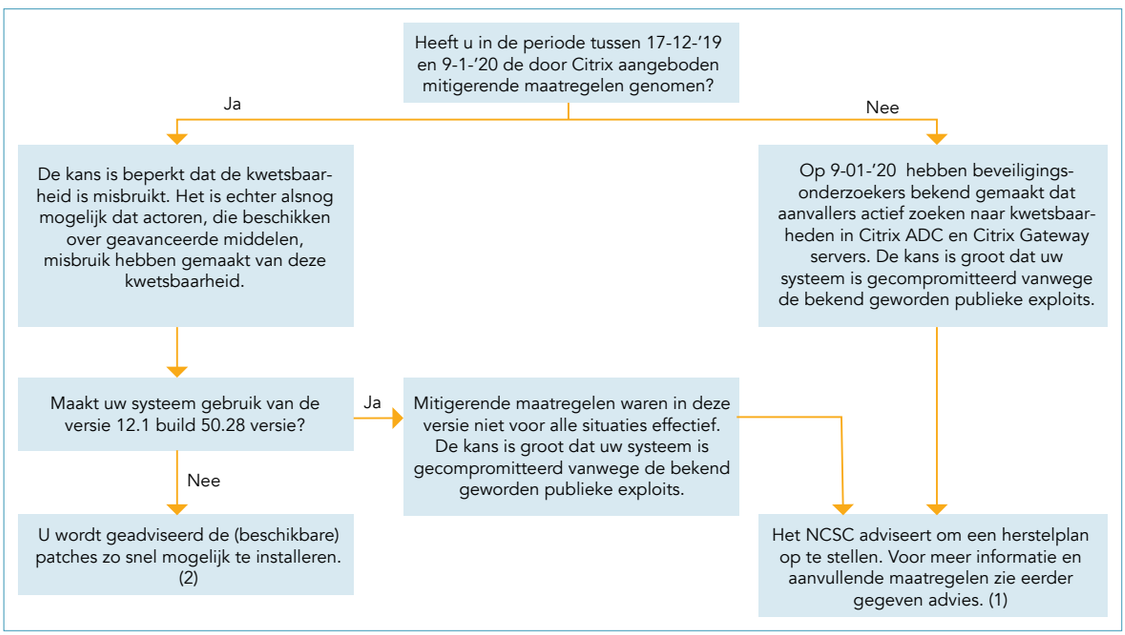
Situatiebeeld Citrix-servers bij de overheid
Vrijwel alle doelgroeporganisaties van het NCSC, zoals de Rijksoverheid en de Tweede kamer, maakten gebruik van Citrix-software:
- 10 van de 12 ministeries;
- 56 van de 69 rijksorganisaties. Daarvan hebben 42 de Citrix-servers uitgeschakeld.

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.

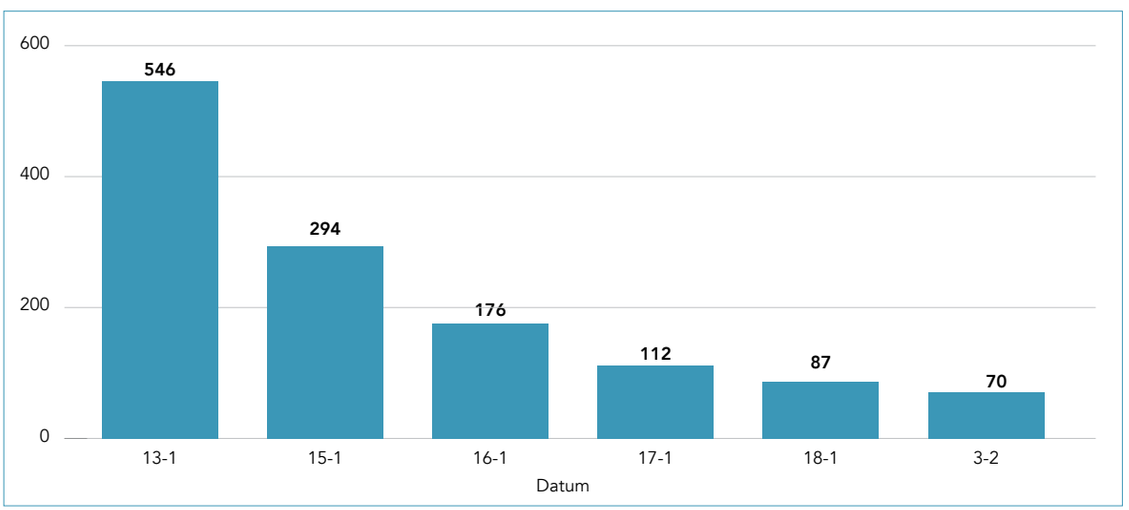
76 https://www.ncsc.nl/documenten/publicaties/2020/januari/20/stroomschema-risicoafweging-citrix.

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:

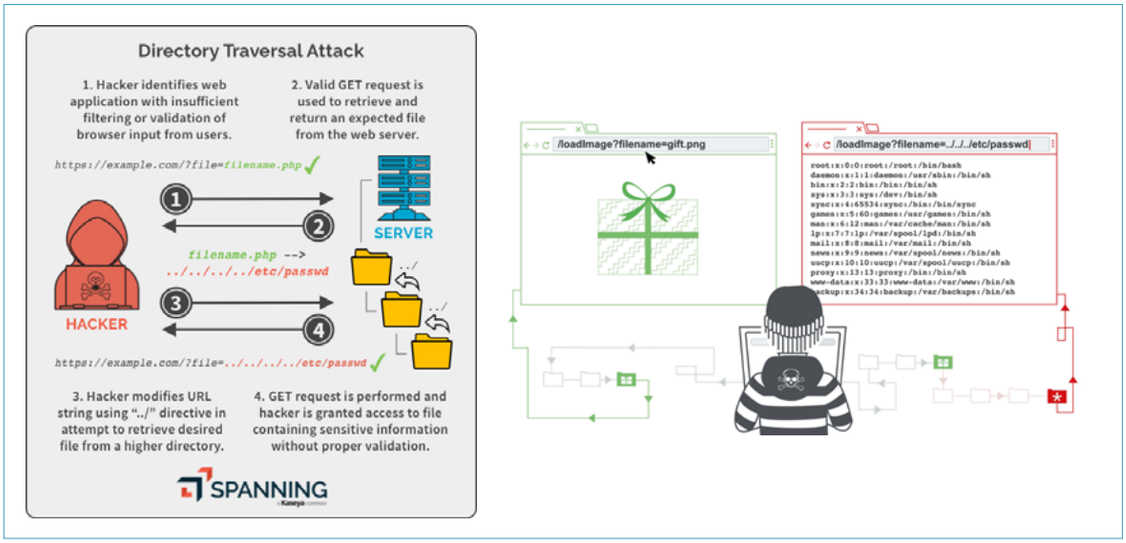
- gebruikers niet de mogelijkheid te geven een commando te geven aan de *appliance* om zich door alle onderdelen van de webserver te verplaatsen en waarmee de gebruiker zich toegang kan verschaffen tot afgeschermde delen van het netwerk en
- gebruikers geen rechten te geven om de complete mappenstructuur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

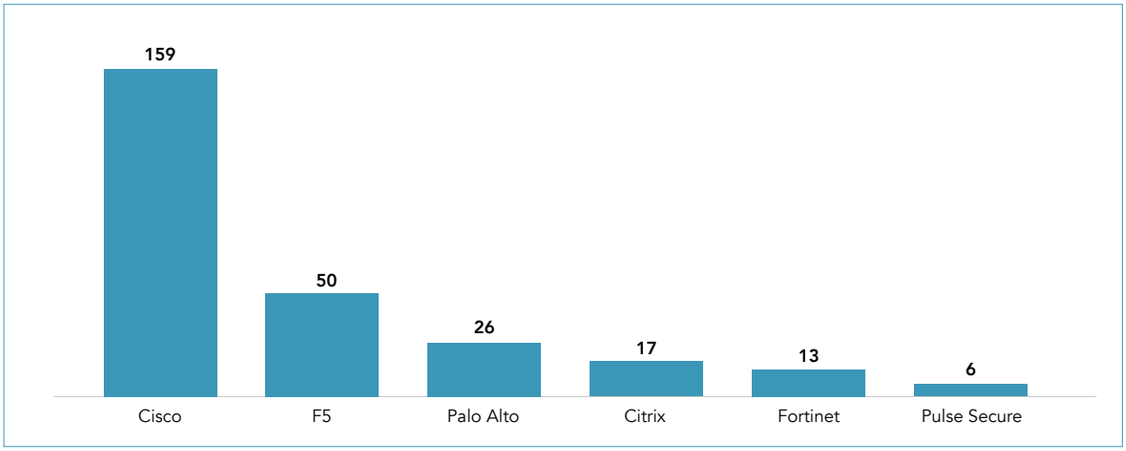
Organisaties gebruiken (zakelijke) VPN-software om hun medewerkers van afstand een veilige verbinding en toegang te geven tot het bedrijfsnetwerk. Net als bij de Gateway van Citrix vervullen deze VPN-producten een centrale rol in de veiligheid van het achterliggende netwerk. Een klein aantal fabrikanten 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

4 ANALYSE SYSTEEM

Hoofdstuk 3 analyseerde het voorval als gevolg van een kwetsbaarheid in Citrix-software. Dit voorval stond niet op zichzelf. Het hoofdstuk analyseerde tevens vergelijkbare voorvallen waarbij kwetsbaarheden in software leidden tot beveiligingslekken bij organisaties. In sommige gevallen had dit directe gevolgen voor de veiligheid van mensen. Dit illustreert dat kwetsbaarheden in software niet op zichzelf staan. Het zijn symptomen van een groter probleem. Deze voorvallen laten namelijk een rode draad zien: organisaties en de mensen die daarvan afhankelijk zijn worden blootgesteld aan digitale onveiligheid. Zij gebruiken namelijk onbewust kwetsbare software. Daarbij bereiken waarschuwingen hen in veel gevallen niet en hebben organisaties niet altijd of hebben organisaties niet de middelen om de kwetsbaarheid te kunnen verhelpen.

Dit hoofdstuk analyseert het vraagstuk op systeemniveau. Daarbij wordt onderscheid gemaakt tussen het proces waarin software tot stand komt; 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 wordt ingegaan op hoe betrokken partijen, zoals fabrikanten, organisaties die software gebruiken en de overheid als beleidsmaker van digitale voorvallen leren. Ook gaan we in op de rol die de internationale context speelt in de beheersing van de onveiligheid als gevolg van kwetsbaarheden in software.

4.1 Software produceren en op de markt brengen

Software vervult een cruciale rol in het functioneren van digitale systemen van organisaties. Software wordt bijvoorbeeld gebruikt voor toegang tot het bedrijfsnetwerk vanuit huis en vormt daarmee ook de koppeling tussen het interne en externe netwerk (internet). Dergelijke producten spelen daardoor ook een essentiële rol bij het waarborgen van de digitale veiligheid.

Softwareproducten dragen altijd inherente kwetsbaarheden met zich mee, waarvan sommige leiden tot grote veiligheidsrisico's. Deze risico's zijn reëel en hebben zich al diverse keren voorgedaan, met ontwrichtende gevolgen voor de publieke dienstverlening. Zo heeft een kwetsbaarheid in een softwareproduct (indirect) geleid tot ernstige verstoringen in de dienstverlening van bijvoorbeeld Nederlandse gemeenten (toeslagen konden niet meer worden uitbetaald aan inwoners) en een ziekenhuis (patiënten konden niet meer bij hun dossiers en er kon geen informatie worden uitgewisseld met andere ziekenhuizen). Hoofdstuk 3 beschreef voorbeelden van kwetsbaarheden in zulke producten en de gevolgen die deze hadden. In deze paragraaf gaan we in op hoe het kan dat software kwetsbaarheden bevat en hoe fabrikanten het risico op deze kwetsbaarheden en de gevolgen ervan inschatten en maatregelen nemen om deze te voorkomen of beperken.

Paragraaf 4.1.1 beschrijft de factoren die verklaren dat kwetsbaarheden in software kunnen ontstaan en de prikkels die daarop van invloed zijn. Vervolgens wordt in 4.1.2 geschetst welke maatregelen fabrikanten treffen om kwetsbaarheden te ontdekken, zowel vóór als nadat software op de markt komt, welke moeilijkheden dat met zich meebrengt en welke dilemma's daarbij ontstaan voor de fabrikant. Tot slot staan we in 4.1.3 stil bij het repareren van kwetsbaarheden en de rol van de fabrikant bij incidentbestrijding.

4.1.1 Voorkomen dat kwetsbaarheden ontstaan in de levenscyclus van software

Kwetsbaarheden kunnen ontstaan gedurende de hele levenscyclus van een softwareproduct. Zo kan een kwetsbaarheid ontstaan tijdens de initiële ontwikkeling van een nieuw product, maar ook bij het vernieuwen of verbeteren van bestaande software, door bijvoorbeeld een *upgrade*, of zelfs als gevolg van het repareren van een andere kwetsbaarheid. Uit interviews met fabrikanten en literatuurstudie blijkt dat een aantal factoren bijdragen aan het ontstaan van kwetsbaarheden tijdens de levenscyclus van een product. We gaan hieronder op een aantal factoren in.

Softwareproducten hebben een geschiedenis

De eerste factor betreft de ontstaansgeschiedenis, die soms lang en ingewikkeld is bij softwareproducten. In het verleden hebben fabrikanten meermaals functionaliteit aan een bestaande softwarepakket toegevoegd en zo doorgebouwd op een bestaand product. In sommige gevallen is de oorspronkelijke code van het softwarepakket (het fundament) zelfs meer dan twintig jaar oud. Door veranderende behoeften en een samenleving die steeds verder en sneller digitaliseert gaat software een andere rol vervullen. Daardoor is een softwareproduct nooit af. Fabrikanten spelen hier steeds weer op in door bestaande platforms te gebruiken en extra functionaliteit toe te voegen of bestaande componenten te hergebruiken.

Doordat fabrikanten herhaaldelijk extra functionaliteit toevoegen groeit het aantal regels code en wordt software complexer.[109] Niet zelden bestaat een softwareproduct bijvoorbeeld uit meer dan één miljoen regels code.[110] Uit interviews en literatuur blijkt dat, zelfs met een uitgebreid raamwerk voor productontwikkeling, het veilig onderhouden van dergelijke hoeveelheden code een significante taak is. Fabrikanten beperken zich daarom meestal tot het verhelpen van de specifieke kwetsbaarheid zoals gepubliceerd in de CVE[111]. Het verhelpen van de achterliggende oorzaak in het fundament van het product (programmeertaal, componenten, architectuur) kan de volledige heropbouw van het product vergen. Fabrikanten vinden dit te kostbaar. Grote softwarebedrijven zijn vaak beursgenoteerde bedrijven en financiële afwegingen spelen een rol. Maar door de ontstaansgeschiedenis van software is een product soms zo gegroeid dat het repareren van een kwetsbaarheid slechts symptoombestrijding is. Dit terwijl een herziening van de basis van het product nodig kan zijn om het echte (veiligheids)probleem op te lossen.

109 https://www.extremetech.com/computing/259977-software-increasingly-complex-thats-dangerous.
110 https://www.informationisbeautiful.net/visualizations/million-lines-of-code/.
111 Common Vulnerabilities and Exposures. Een openbare lijst van bekende en zwakke plekken in software. De lijst staat op https://cve.mitre.org. (Bron: Cybersecurity Alliantie, *Cybersecurity Woordenboek* (2019), https://www.cybersecurityalliantie.nl/binaries/cybersecurityalliantie/documenten/publicaties/2019/09/30/cybersecurity-woordenboek/VCNL-Woordenboek-2eDruk-webversie-Final-2.pdf).

Programmeertaal
De gebruikte programmeertaal kan, als tweede verklarende factor, ook van invloed zijn op het ontstaan van kwetsbaarheden in software. De op dit moment meest gebruikte programmeertaal (C/C++) staat bekend als 'onveilig', omdat het programmeurs veel ruimte laat om fouten te maken.[112]

Er zijn enkele algemene hulpmiddelen die fabrikanten kunnen gebruiken om hele klassen van kwetsbaarheden te elimineren of de werking daarvan te mitigeren. Ongeveer de helft van de beveiligingslekken van de afgelopen jaren betrof bijvoorbeeld kwetsbaarheden in de geheugenveiligheid, die kunnen worden verholpen door code te schrijven in veiligere talen zoals Rust, of door bestaande C/C++ code te onderwerpen aan verificatietools.[113]

Volgens onderzoek is het voor fabrikanten niet aantrekkelijk om de softwareontwikkeling te beveiligen tegen kwetsbaarheden: de software zelf wordt er langzaam van en programmeurs krijgen tijdens het programmeren zo veel foutmeldingen (ook terechte) dat ze de beveiliging uitzetten.[114]

Het is ook niet mogelijk om bij alle programmeertalen tools te gebruiken om kwetsbaarheden op te sporen tijdens het ontwikkelproces.[115] In de Citrix casus speelde bijvoorbeeld een rol dat programmeertaal Perl niet of nauwelijks werd ondersteund door deze *scanning tools*. Zie verder 4.1.2 over wat fabrikanten doen om kwetsbaarheden te ontdekken en welke belemmeringen daarbij spelen.

Gebruik van standaardcomponenten
De derde factor is het gebruik van standaardcomponenten. Fabrikanten maken bij het ontwikkelen van software veelvuldig gebruik van bestaande (open source) software-componenten. Voorbeelden hiervan zijn de Apache en NGINX HTTP server, die vaak dienen als de basis van software met webfunctionaliteit. Ook kan een fabrikant componenten uit reeds bestaande software van henzelf of van overgenomen fabrikanten hergebruiken.

Met het overnemen van andere componenten en de code die daartoe behoort, neemt een fabrikant ook alle (onontdekte) kwetsbaarheden over die de code bevat.[116] Als de

112 De basis voor de SSL VPN (een virtual private network die gebruik maakt van het SSL of TLS protocol) en veel andere software is C/C++. Programmeertalen zoals C stellen programmeurs in staat om code te schrijven op een hoger abstractieniveau. Dit geeft aan hoe dicht een programmeertaal bij de hardware staat. Met een hoger abstractieniveau wordt software ontwikkelen eenvoudiger en begrijpelijker dan op een lager niveau, waarbij specifiekere machine-instructies nodig zijn. Maar dat kan ook leiden tot fouten. C is een programmeertaal die bekend staat als 'onveilig', omdat het werkgeheugenbeheer in deze taal handmatig plaatsvindt (Kroes, T. How to Keep Your Memory Safe and Your Software Fast, 2020; AG Connect, Einde van de oneindige reeks softwarefouten in zicht, 2021). Dit is foutgevoelig en bovendien gebruiken de meeste SSL VPN's eigen toevoegingen aan bestaande programmeertalen. Daardoor kunnen eenvoudig geheugenfouten ontstaan; de meest voorkomende bron van softwarebugs en een belangrijk aanvalsoppervlak voor hackers (zie https://www.zdnet.com/article/microsoft-70-percent-of-all-security-bugs-are-memory-safety-issues/). Desondanks is C nog steeds één van de meest gebruikte programmeertalen.
113 Anderson, R., *Security Engineering*, 2020.
114 Kroes, T., *How to Keep Your Memory Safe and Your Software Fast*, 2020 https://research.vu.nl/en/publications/how-to-keep-your-memory-safe-and-your-software-fast
115 Tjong Tjin Tai, E. en Knoops, B., Zorgplichten tegen cybercrime (*Nederlands Juristenblad* 24-04-2015, afl. 16), 2015.
116 AG Connect, *Veel kritieke lekken door open source in standard apps*, 2021. https://www.agconnect.nl/artikel/veel-kritieke-lekken-door-open-source-standaard-apps

code eenmaal geïntegreerd is in het eigen pakket, kan het veel inspanning kosten om de onderliggende component in het geval van een kwetsbaarheid te updaten. Het softwarepakket is dan immers afhankelijk van een bepaalde versie van het component. Fabrikanten hebben ook niet altijd de juiste kennis in huis om componenten van anderen te kunnen updaten.[117]

Architectuur
De vierde factor die bijdraagt aan de aanwezigheid van kwetsbaarheden betreft het gegeven wanneer verschillende lagen in de architectuur van het product onderling niet consistent zijn. Het is essentieel voor de werking van software dat de verschillende onderdelen waaruit het bestaat op elkaar aansluiten. De aansluiting van verschillende componenten moet op een gecontroleerde manier tot stand zijn gekomen, onder het toeziend oog van een persoon met veel ervaring, voldoende kennis en die een groot belang heeft bij de beveiliging van een product.[118]

Configuratie
Een laatste factor, die niet zozeer bijdraagt aan het ontstaan van kwetsbaarheden, maar wel de gevolgen kan beperken, is de wijze waarop de software wordt geconfigureerd door de fabrikant (de standaard-instellingen). Daarbij gaat het onder meer om welke rechten er aan de verschillende soorten gebruikers kunnen worden toegekend, hoe deze rechten standaard staan ingesteld en of het mogelijk is als afnemer om deze rechten te beperken.

Verschillende factoren dragen bij aan het ontstaan van kwetsbaarheden tijdens de levenscyclus van een product. Vaak wordt doorgebouwd aan een bestaand product, daardoor wordt software steeds complexer. Ook kan de gebruikte programmeertaal bijdragen aan het ontstaan van fouten en het gebruik van bestaande componenten en (inconsistente) lagen in de architectuur kwetsbaarheden introduceren.

Als (veiligheids)problemen gekoppeld zijn aan fundamentele keuzes in het product kan dat een belemmering vormen voor de fabrikant om het probleem bij de wortel aan te pakken. Hiervoor is namelijk een investering nodig in de vorm van geld en/of capaciteit voor het oplossen van het probleem. De keuze van de fabrikant om in plaats daarvan alleen de kwetsbaarheid te repareren is verklaarbaar, maar soms is een herziening van de basis nodig om het echte (veiligheids)probleem op te lossen.

4.1.2 Kwetsbaarheden opsporen tijdens de levenscyclus
Fabrikanten hebben processen ingericht om kwetsbaarheden op te sporen tijdens de ontwikkeling van een product en om kwetsbaarheden op te sporen als het product al in gebruik is. In deze paragraaf gaan wij nader in op welke maatregelen fabrikanten kunnen treffen om kwetsbaarheden op te sporen en welke dilemma's daarbij voor hen ontstaan.

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

Handelingsperspectief van de fabrikant

Fabrikanten sporen kwetsbaarheden op door middel van het doen van verschillende testen, zowel voor, tijdens als na het afronden van het ontwikkelproces. Voor open source software is de broncode voor iedereen inzichtelijk, daarom kunnen fouten in de code worden opgespoord door derde partijen, ook zonder dat daar specifiek naar wordt gevraagd. Voor *closed source code* is dit niet mogelijk, en de fabrikant moet zelf het initiatief nemen tot het uitvoeren van een audit.

Van een fabrikant kan verwacht worden dat deze een constante veiligheidsanalyse maakt van de gehele architectuur van het product (zie referentiekader: de rol van fabrikant en afnemer in hoofdstuk 2). Fabrikanten gebruiken verschillende methodologieën voor het ontwikkelen van software, bijvoorbeeld de *Secure Development Lifecycle* (SDLC).[119] Onderdeel hiervan is dat fabrikanten op verschillende momenten tijdens het ontwikkelproces (tijdens de initiële ontwikkeling maar ook bij het uitbrengen van patches) testen op kwetsbaarheden. Dat testen wordt gedaan op individuele componenten (*unit testing*), samenhang tussen componenten (*integration testing*) en het gehele product (audit[120] of *security code review*).

Door het gebruik van geautomatiseerde tools zijn fabrikanten in staat om meer kwetsbaarheden uit software te halen. Op die manier hopen zij de levensduur van het software te kunnen verlengen. Maar de *security code reviews* van het gehele product herkennen echter niet altijd het type kwetsbaarheden dat we hier behandelen. Kwetsbaarheden zijn niet (altijd) het gevolg van fouten in de broncode, maar ook een gevolg van de samenhang binnen het product. De fabrikant heeft dan ook nog de mogelijkheid om het product uitvoerig te testen op de beoogde werking (*end-to-end testing*). Uit interviews met fabrikanten blijkt dat voor oudere producten *end-to-end testing* zeer tijdrovend kan zijn, omdat oudere producten vaak bestaan uit een grote hoeveelheid broncode.

Fabrikanten kunnen kwetsbaarheden ook opsporen zonder derden daarbij directe toegang tot de broncode te geven. Veel fabrikanten hebben *bug bounty* programma's waarbij ethische hackers in ruil voor een beloning op zoek gaan naar kwetsbaarheden in de software. Deze ethische hackers zoeken handmatig en gaan als eerste op zoek naar eenvoudig vindbare kwetsbaarheden die het gevolg zijn van fundamentele ontwerpkeuzes en problemen in de samenhang of configuratie.

Veel van deze *bug bounty* programma's zijn voor iedereen toegankelijk, maar sommige fabrikanten kiezen ook voor een gesloten variant of hebben geen *bug bounty* programma. Ook krijgen fabrikanten soms informatie over kwetsbaarheden doorgestuurd uit *bug bounty* programma's van andere partijen, zoals toeleveranciers of klanten. Citrix had bijvoorbeeld ten tijde van het voorval alleen een gesloten *bug bounty* programma, het bedrijf is recentelijk gestart met een open programma.

119 Zie bijvoorbeeld https://owasp.org/www-pdf-archive/Jim_Manico_(Hamburg)_-_Securiing_the_SDLC.pdf

120 Onderdeel van de audit die de fabrikant doet is bijvoorbeeld threat modeling (het identificeren van bedreigingen en mitigerende maatregelen) en pentesting (het testen op kwetsbaarheden en hiermee proberen in te breken op het systeem). Pentesten kan deels geautomatiseerd worden gedaan, maar ook deze software kan weer kwetsbaarheden bevatten (zie bijvoorbeeld https://arstechnica.com/gadgets/2021/08/critical-cobalt-strike-bug-leaves-botnet-servers-vulnerable-to-takedown/).

Fabrikanten moeten een overzicht hebben van de afnemers van een softwareproduct (zie referentiekader in hoofdstuk 2). In dat geval kan de fabrikant afnemers snel waarschuwen in het geval van een kwetsbaarheid. Niet alle fabrikanten hebben een *up-to-date* overzicht van wie de afnemers van een product zijn. Dit komt omdat producten niet altijd rechtstreeks worden verkocht aan een afnemer; regelmatig gaat dit via allerlei tussenpartijen. Uit interviews blijkt dat sommige fabrikanten dit hebben opgelost door contactgegevens van afnemers, ook als een product wordt verkocht via een tussenpartij, te koppelen aan hun eigen overzicht. Vanuit het veiligheidskundig perspectief lijkt het logisch dat fabrikanten een overzicht hebben van de afnemers van een product. Het kan echter een dilemma opleveren dat onder andere raakt aan de autonomie van de afnemer. Zo is het niet mogelijk hen te dwingen zich bij een fabrikant te registreren en inzage te geven in hoe het systeem is geïnstalleerd.

Een trend van de laatste jaren is dat fabrikanten producten naar de *cloud* verplaatsen (*Software as a Service*) om beter te kunnen testen en sneller patches toe te passen op systemen van klanten. Het patchen van een product wordt hiermee de verantwoordelijkheid van de fabrikant. Dit brengt echter voor afnemers ook nadelen met zich mee, zie paragraaf 4.2.

Asymmetrie: fabrikant moet alles vinden, hackers hebben maar één lek nodig

De fabrikant moet veel tijd en moeite steken in het opsporen van kwetsbaarheden, voor en na het op de markt brengen van software. Met technieken zoals *end-to-end testing* kunnen veel kwetsbaarheden uit software gehaald worden. Maar het kost veel moeite om een enkele kwetsbaarheid op te sporen. Op het gebied van preventie hebben fabrikanten vaak al uitgebreide procedures opgenomen in het ontwikkelproces. Problemen in software die al langer bestaan (zie ontstaansgeschiedenis in 4.1.1) zijn onoverkomelijk vanwege de omvang en de preventieparadox. Het is niet mogelijk alle kwetsbaarheden op te sporen.

Aanvallers proberen met verschillende methodes, bijvoorbeeld door een *brute-force attack*, een kwetsbaarheid in een systeem te vinden. Soms doen ze dat aan de hand van bepaalde aanwijzingen (bijvoorbeeld met informatie uit een CVE), maar ook regelmatig komen ze per toeval een kwetsbaarheid tegen. Aanvallers hebben soms genoeg aan een enkel lek om volledige toegang tot een systeem te krijgen. Daarmee ontstaan een onbalans tussen aanvaller en verdediger (fabrikant).

Waar het vroeger nodig was zelf op het internet op zoek te gaan naar kwetsbare servers, een tijdrovend proces, is dat tegenwoordig makkelijker gemaakt door het gebruik van diensten die het internet scannen.[121] Aanvallers kunnen hiermee gemakkelijk een lijst van IP-adressen kopen die betrekking hebben op een (net gepubliceerde) CVE. Een aanvaller die een kwetsbaarheid heeft ontdekt heeft dus meteen toegang tot een lijst aan potentieel kwetsbare servers.

121 Bijvoorbeeld Shodan (https://www.shodan.io), een zoekmachine die het internet scant en benaderbare IP-adres en poortcombinaties indexeert. Als een server wordt geïndexeerd dan is de server via het internet te benaderen. Dat betekent niet automatisch dat een server ook kwetsbaar is. Dat is iets wat de hacker moet nagaan.

Relatie fabrikant en ethische hackers / redteams

Ethische hackers leveren een belangrijke bijdrage aan het opsporen van kwetsbaarheden. *Bug bounties* (een beloning ontvangen als men een kwetsbaarheid meldt) zijn daarbij een relevante prikkel. Zo hebben de meeste grote fabrikanten een *bug bounty* programma[122] waarmee ethische hackers geld kunnen verdienen voor het opsporen en rapporteren van kwetsbaarheden. Ook kan opsporen en publiceren over een specifieke kwetsbaarheid bijdragen aan de bekendheid van een hacker of hackersgroep. Dit mechanisme in combinatie met potentieel financieel gewin zorgt ervoor dat er veel wordt gespeurd naar kwetsbaarheden door derde partijen en leidt ertoe dat veel kwetsbaarheden worden gevonden.

Maar kwetsbaarheden vormen steeds vaker een potentiele aanvalsroute (zie 4.1.3) en het kost fabrikanten veel moeite om kwetsbaarheden te voorkomen en te verhelpen (zie 4.1.1). In dat licht zou het fabrikanten helpen en systemen beschermen om kwetsbaarheden geheim te houden. Het is mogelijk te publiceren over kwetsbaarheden zonder daarbij de details van een kwetsbaarheid prijs te geven. Maar sommige fabrikanten kiezen er bewust voor om niet alle (informatie over de aanwezigheid van) kwetsbaarheden openbaar te maken.[123] Deze gedachte staat echter haaks op het tijdig bekend maken van informatie over kwetsbaarheden voor het mitigeren en bestrijden van potentiele risico's. Er is een duidelijke impuls ter voorkoming dat informatie over kwetsbaarheden openbaar wordt. Bekendmaken stelt afnemers in staat de gevolgen te bestrijden maar leidt tegelijkertijd tot een nieuw veiligheidsprobleem: een dilemma.

Degene die de kwetsbaarheid vindt meldt dit niet altijd aan de fabrikant. Kwetsbaarheden in software zijn handelswaar, die niet alleen worden gemeld aan de fabrikant (al dan niet tegen een beloning), maar die ook worden aangeboden aan de hoogste bieder. Zo is het interessant voor statelijke actoren en criminelen om een lijst met onbekende kwetsbaarheden te bezitten zodat zij deze zelf kunnen gebruiken.[124] Ook worden commerciële spywareproducten verkocht, waarbij niet zichtbaar is of dit product gebaseerd is op onbekende kwetsbaarheden en ook niet aan welke partijen en voor welk doeleinde deze producten worden ingezet.[125]

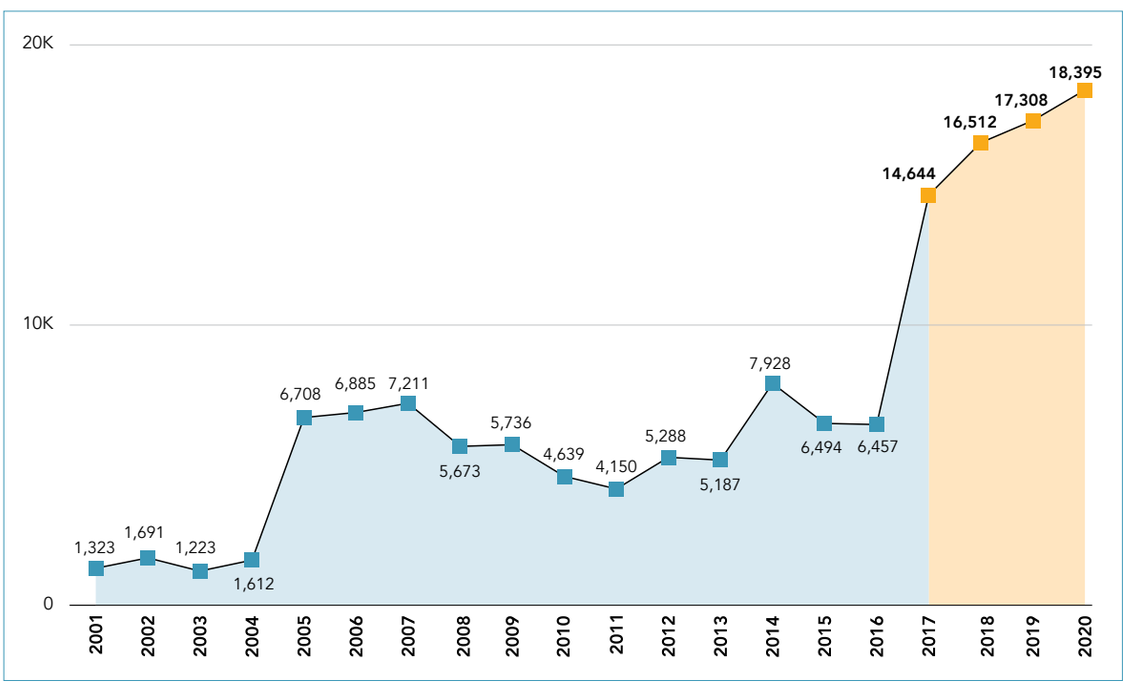
122 Voor een overzicht van bug bountry programma's, zie bijv. https://www.bugcrowd.com/bug-bounty-list/.
123 Bijvoorbeeld Palo Alto, waar volgens de beveiligingsonderzoeker die de kwetsbaarheid vond geen CVE was gepubliceerd over een kwetsbaarheid (die ook al door de fabrikant gerepareerd was) in GlobalProtect. Bron: https://blog.orange.tw/2019/07/attacking-ssl-vpn-part-1-preauth-rce-on-palo-alto.html. Het is onduidelijk of Palo Alto via directe kanalen met hun klanten heeft gecommuniceerd over de kwetsbaarheid. De Onderzoeksraad heeft dit niet kunnen verifiëren omdat Palo Alto niet heeft gereageerd op onze verzoeken om mee te werken aan het onderzoek.
124 Perlroth, N., *This is how they tell me the world ends: the cyberweapons arms race*, 2021.
125 https://www.wired.com/story/nso-group-hacks-ios-android-observability/, https://www.nrc.nl/nieuws/2021/07/26/de-overheid-moet-stoppen-met-gebruik-van-zero-day-software-a4052412

Ethische hackers worden met beloningen aangespoord om te zoeken naar kwetsbaarheden in software. Daardoor worden veel kwetsbaarheden opgespoord. Fabrikanten sporen daarnaast kwetsbaarheden op door het doen van verschillende testen. Maar het is niet mogelijk *alle* kwetsbaarheden op te sporen. Kwetsbaarheden vormen steeds vaker een aanvalsroute. Een kwetsbaarheid bekend maken kan organisaties helpen zich beter te wapenen tegen mogelijk misbruik, het kan aanvallers echter ook in staat stellen de kwetsbaarheid te misbruiken. Temeer omdat hackers soms maar één lek nodig hebben om toegang te krijgen tot een systeem en het voor hen relatief eenvoudig is om kwetsbare servers op te sporen. Daarmee ontstaat een dilemma met onveiligheid tot gevolg.

4.1.3 De rol van kwetsbaarheden bij digitale onveiligheid

Kwetsbaarheden spelen een grotere rol

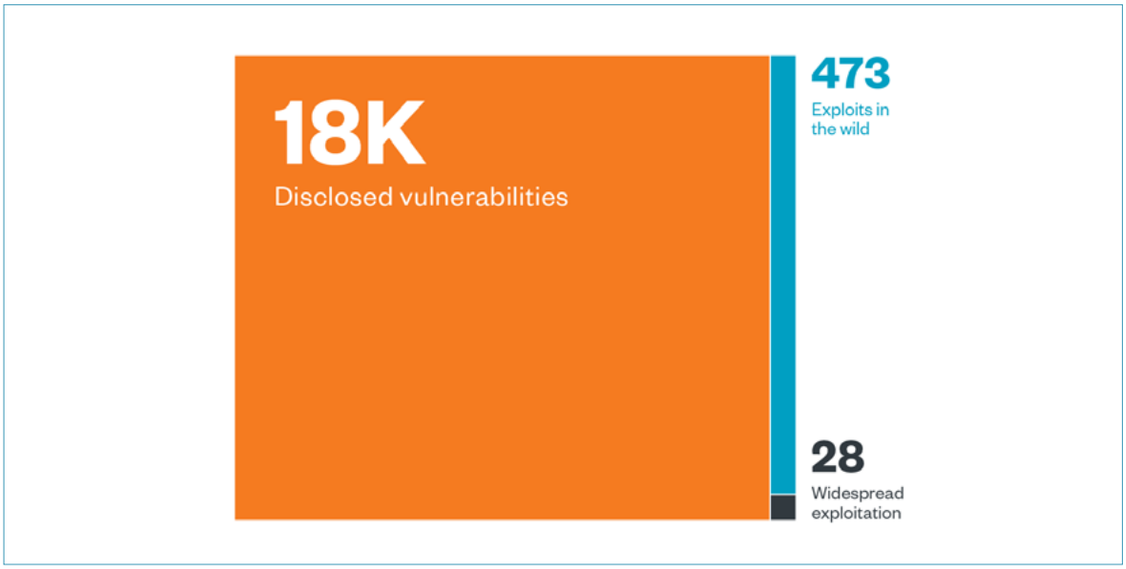
Organisaties worden jaarlijks blootgesteld aan een groot en alsmaar groeiend aantal kwetsbaarheden. In 2020 ging het om ruim 25 duizend kwetsbaarheden. Een deel van deze kwetsbaarheden, 18 duizend, is in 2020 gepubliceerd met een CVE nummer[126] (zie Figuur 16). Slechts een klein deel van het aantal gepubliceerde kwetsbaarheden (circa 3%) wordt gebruikt om organisaties en/of individuen aan te vallen. Een nog kleiner deel (0,5%) is in de praktijk succesvol gebruikt om een wijdverbreide aanval zoals bij de beveiligingslekken beschreven in hoofdstuk 3 tot stand te laten komen (zie Figuur 17). Toch groeit dit aantal en experts waarschuwen dat dit slechts het topje van de ijsberg is.[127]



Figuur 16: Het aantal CVE meldingen per jaar. (Bron: Trend Micro)

126 Er zijn ook veel kwetsbaarheden die door de fabrikant worden verholpen zonder dat deze openbaar worden gemaakt. https://vulndb.cyberriskanalytics.com/#statistics

127 AG Connect, *Einde van de oneindige reeks softwarefouten in zicht*, 2021.



Figuur 17: Het aantal exploits en wijdverbreide aanvallen in relatie tot het totaal aantal gerapporteerde kwetsbaarheden. (Bron: Trend Micro)

Ook de gevolgen van deze aanvallen worden steeds groter. Zo waarschuwde de NCTV in het Cybersecuritybeeld 2020 voor aanvallers die op zoek gaan naar zwakke schakels in de leveranciersketen als opstap naar interessante doelen en de grote gevolgen daarvan.[128] Waar een kwetsbaarheid in een softwarepakket in het verleden niet automatisch tot ernstige gevolgen leidde, kan dit tegenwoordige verregaande gevolgen hebben voor achterliggende, afhankelijke systemen, zoals geïllustreerd door de ketenaanvallen waarbij gebruik werd gemaakt van kwetsbaarheden in SolarWinds en Kaseya (zie paragraaf 3.3 voor een beknopte analyse).

Kwetsbaarheden zoals in de door de Onderzoeksraad onderzochte voorvallen spelen dus een steeds grotere rol bij cyberaanvallen en worden door aanvallers steeds vaker gebruikt als startpunt voor het opzetten van een aanval.[129] Vooral grote organisaties (zoals overheidsorganisaties en vitale bedrijven) lopen risico om aangevallen te worden met behulp van deze aanvalsvector.[130] Het misbruiken van kwetsbaarheden in software om *ransomware*-aanvallen uit te voeren is een economisch aantrekkelijke werkwijze voor *ransomware*-bendes, zo is sinds 2020 duidelijk geworden.

Het steeds vaker voorkomen van wijdverspreide aanvallen waarbij gebruik wordt gemaakt van een kwetsbaarheid toont het belang van tijdig patchen van software en/of mitigeren van een kwetsbaarheid aan. Het gebruik van software brengt risico's met zich mee. Zo is het voor afnemers niet altijd mogelijk om te voorspellen welke van de kwetsbaarheden uiteindelijk een gevaar zullen vormen voor hun organisatie. Dit is bijvoorbeeld afhankelijk van hoe eenvoudig het is om de kwetsbaarheid in de software actief te misbruiken, of er een mitigatie voorhanden is en hoe eenvoudig het is om deze toe te passen, en van de

128 NCTV, *Cybersecuritybeeld Nederland 2020*, 2020. https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
129 Modderkolk H., 'Overheid doet te weinig tegen ransomeware', *De Volkskrant*, 4 augustus 2021; CISA, *Alert (AA21-209A) Top Routinely Exploited Vulnerabilities*, 2021.
130 Coveware, *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound*, 2021. https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

versie en configuratie van een product. Het verhelpen van kwetsbaarheden door een mitigerende maatregel of het toepassen van patches vereist van een investering van de organisatie. In de meeste gevallen krijgen ze daar niet direct meer veiligheid voor terug.

Voor fabrikanten en afnemers is het voorkomen, tijdig mitigeren of patchen van een kwetsbaarheid niet de enige verdedigingslinie. In paragraaf 4.2 wordt verder stilgestaan bij maatregelen die organisaties kunnen nemen om de veiligheidsrisico's van kwetsbaarheden in software te mitigeren. Voorbeelden hiervan zijn het gebruik van een firewall om toegang tot het netwerk in te dammen en het gebruik van redundante hard- en software zodat bij het bekend worden van een kwetsbaarheid snel omgeschakeld kan worden naar een ander product.

De keerzijde van patchen en mitigeren

Als de fabrikant software op de markt heeft gebracht waarvan later blijkt dat deze een kwetsbaarheid bevat, zal de fabrikant doorgaans een patch uitbrengen en afnemers adviseren om de software te patchen. In het geval er nog geen patch beschikbaar is kan een fabrikant ook een mitigatie publiceren om het acute gevaar weg te namen. Maar patchen en mitigeren zijn niet altijd makkelijk te nemen oplossingen.

Patches en mitigaties vormen in zekere zin ook een risico. Het is niet altijd te voorzien wat het effect van een patch of mitigatie zal zijn op reeds geconfigureerde en in gebruik zijnde software. Elke mitigatie en patch kan leiden tot (deels) onvoorziene gevolgen, bijvoorbeeld voor de compatibiliteit van belendende/verbonden systemen. In sommige gevallen kunnen patches zelfs zorgen voor verstoringen of het geheel uitvallen van systemen.[131] Ook kunnen *p*atches en mitigaties weer nieuwe fouten in de software of kwetsbaarheden introduceren, zoals bijvoorbeeld het geval bij de patch van Microsoft om de problemen met de *print-spooler* op te lossen die leidde tot problemen bij het printen.[132]

Kwetsbaarheden in software vormden een escalatiefactor. De voorvallen in dit onderzoek illustreren dat. Nadat de kwetsbaarheden bekend waren gemaakt (bijvoorbeeld door de publicatie van een CVE of een *security bulletin*), zochten aanvallers met geautomatiseerde hulpmiddelen naar alle servers die nog niet waren gepatcht om deze aan te vallen. Een mitigatiemaatregel kan bovendien informatie geven over hoe een kwetsbaarheid misbruikt kan worden. De onderzochte voorvallen laten zien dat dit in een tijdbestek van enkele dagen kan gebeuren (of dat de aanvallen al plaatsvonden, in het geval van een *zero day*). De publicatie van een kwetsbaarheid kan de opmaat vormen naar wijdverbreide aanvallen.

Ook aan de kant van afnemers kunnen problemen ontstaan rondom het patchen. Zo is het vanwege het grote aantal patches dat jaarlijks verschijnt niet altijd mogelijk om alles tijdig te installeren. Afnemers hebben ook niet altijd een up-to-date overzicht van welke software gepatcht moet worden, hebben vaak geen zicht op welke onderliggende (kwetsbare) componenten een softwarepakket bevat en zijn niet altijd overtuigd van de

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

noodzaak tot *p*atchen. Hier wordt verder op ingegaan in paragraaf 4.2. Het uitbrengen van een mitigatiemaatregel voordat een patch verschijnt kan een *good practice* zijn omdat afnemers deze in de regel wel gelijk toepassen na publicatie ervan. Zo zorgt een fabrikant ervoor dat de software van afnemers veilig is. Nadeel is dat sommige afnemers de noodzaak van patchen dan nog minder gaat inzien.

Het aantal kwetsbaarheden in software groeit en de gevolgen van aanvallen worden groter. Kwetsbaarheden spelen een steeds grotere rol bij cyberaanvallen en kunnen door aanvallers worden gebruikt als startpunt voor het opzetten van een aanval. Dit onderstreept het belang van tijdig patchen. Maar patchen en mitigeren vormen tegelijkertijd een risico omdat dit kan leiden tot verstoringen of de introductie van nieuwe kwetsbaarheden. De organisatie moet het besluit om te patchen daarom goed doordenken vanuit het ICT-landschap van de organisatie. De publicatie van een kwetsbaarheid kan de opmaat vormen naar wijdverbreide aanvallen.

4.1.4 Prikkels voor veiligere software

Naast de meer intrinsieke factoren, die direct betrekking hebben op het ontwikkelproces bij de fabrikant, spelen ook factoren ten aanzien van regulering en aansprakelijkheid een rol bij het ontstaan van kwetsbaarheden.

Overheden en organisaties die software gebruiken hebben op dit momenteel weinig mogelijkheden om softwarefabrikanten te verplichten cybersecurity in hun producten te borgen. Daarmee komen problemen die ontstaan als gevolg van kwetsbaarheden grotendeels te liggen bij de afnemer van een product. Afnemers moeten hierop extra bedacht zijn bij het aanschaffen van software. Eenmaal aangeschaft kan een afnemer weinig meer doen om te controleren of een product veilig is.

Positie afnemer ten opzichte van fabrikant

Sommige (grote) afnemers, zoals overheden en vitale bedrijven, zijn in staat om met behulp van geavanceerde software en uitgebreide analyses zelf kwetsbaarheden in software op te sporen. Maar niet alle afnemers bevinden zich in de positie om zelf de software te kunnen testen of ontleden (reverse engineering), of om autonoom een volledige risicobeoordeling te kunnen doen (zie ook paragraaf 4.2 over informatie-asymmetrie en referentiekader transparantie). Uit interviews blijkt bovendien dat niet alle organisaties weten hoe ze eisen moeten stellen en af moeten dwingen om een fabrikant verantwoording af te laten leggen. Fabrikanten laten in overeenkomsten doorgaans vastleggen dat zij beperkt aansprakelijk zijn voor de gevolgen van eventuele kwetsbaarheden in de software. Daarmee wordt een kwetsbaarheid een probleem van de afnemer, en niet van de fabrikant.

Verder verbieden fabrikanten met de voorwaarden die zij verbinden aan de aanschaf en het gebruik van hun software dat afnemers het product 'openmaken' om te kijken hoe het werkt en welke componenten het bevat. Dit doen fabrikanten vanuit het oogpunt van bedrijfsgeheim. Deze afspraken werken belemmerend voor afnemers om het product aan een eigen onderzoek te onderwerpen en om kwetsbaarheden te melden die uit zo'n

onderzoek volgen. Ook bepalen fabrikanten via de voorwaarden dat zij niet aansprakelijk kunnen worden gesteld voor de gevolgen van kwetsbaarheden in de software.[133]

Wettelijke eisen

Los van het stellen van eisen aan een softwareproduct door afnemers worden er ook nauwelijks eisen gesteld door de overheid voor het op de markt brengen van software, het onderhoud tijdens de levenscyclus en de rol van de fabrikant tijdens incidentbestrijding. De Wbni[134] verplicht aanbieders van essentiële diensten tot het nemen van beveiligingsmaatregelen met betrekking tot hun netwerk en informatiesystemen (bijvoorbeeld het melden van cybersecurityincidenten), maar dit geldt niet voor softwarefabrikanten. Bovenstaande toont aan dat in het stelsel van partijen, met name op het gebied van wet- en regelgeving, een lacune zit aan de kant van de fabrikanten.

Nationale initiatieven

Er zijn diverse initiatieven om met wet- en regelgeving te komen voor het op de markt brengen van software. Zo zijn het ministerie van Economische Zaken en Klimaat en het ministerie van Justitie en Veiligheid zijn in de vorm van de *roadmap* digitaal veilige hard- en software (*roadmap* DVHS) gekomen met een initiatief waarin ze een pakket aan meetregelen voorstellen om onveiligheden in hard- en software te voorkomen, kwetsbaarheden te detecteren en de gevolgen daarvan te mitigeren.[135] De maatregelen in de *roadmap* zijn gericht op zowel preventie, detectie als mitigatie en bestaan onder meer uit wettelijke eisen en het aansprakelijk stellen van fabrikanten voor schade als gevolg van digitale onveiligheid. Zorg om aansprakelijkheid moet een prikkel vormen voor fabrikanten om voorzorgsmaatregelen te nemen of schade te beperken. De maatregelen zijn met name gericht op kleinere apparaten (IoT[136]), maar zijn universeel toepasbaar op andere typen software. Die vraag die rijst is in hoeverre deze maatregelen ook toegepast moeten worden op alle veiligheidskritische software en software in de algemene zin.

Internationale initiatieven

Verschillende internationale overheden nemen initiatief om de lacune in wet- en regelgeving aan te pakken. Op 27 juni 2019 is de Europese *Cybersecurity Act* in werking getreden.[137] Met deze nieuwe regels voor cyberbeveiliging worden onder meer het mandaat van ENISA[138] versterkt en een cybersecurity certificeringskader geïntroduceerd. Een ander recent voorbeeld van een initiatief op het gebied van wetgeving is de cyberwetgeving in de VS, waarmee eisen worden gesteld aan software die door de overheid wordt aangekocht.[139] Australië heeft ook plannen om regulering voor

133 Cyber Security Raad (CSR), *Integrale aanpak cyberweerbaarheid*, 2021.; Tjong Tjin Tai, E. en Knoops, B., Zorplichten tegen cybercrime (*Nederlands Juristenblad* 24-04-2015, afl. 16), 2015; Anderson, R., *Security Engineering*, 2020.
134 Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor digitale dienstverleners, zie https://wetten.overheid.nl/BWBR0041515/2021-07-01
135 Ministerie van Economische Zaken en Klimaat en ministerie van Justitie en Veiligheid, *Roadmap digitaal veilige hard- en software*, 2018.
136 *Internet-of-Things*, bijvoorbeeld een smart TV, slimme koelkast, verbonden temperatuursensoren, et cetera.
137 https://ecer.minbuza.nl/-/europese-cyber-security-act-van-kracht; https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
138 Het Europees agentschap voor netwerk- en informatiebeveiliging.
139 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, https://www.nytimes.com/2021/05/12/us/politics/biden-cybersecurity-executive-order.html

cybersecurity te verbeteren.[140] De nadruk bij dit voorstel ligt op IoT en organisaties die persoonlijke informatie verwerken. Ten aanzien van softwareveiligheid zet Australië in op sterkere afspraken over *responsible disclosure* als prikkel voor fabrikanten om kwetsbaarheden sneller te patchen. In China wordt het misbruiken van kwetsbaarheden strafbaar en komen er sancties voor fabrikanten die nalaten patches uit te brengen voor gemelde kwetsbaarheden.[141]

De Cyber Security Raad (CSR) concludeert in zijn laatste adviesrapport dat er ondanks een aantal belangrijke initiatieven, zowel binnen de Europese Unie als Nederland, nog geen sluitend mechanisme is van verantwoordelijkheid voor veilige hard- en software.[142] Volgens de CSR moeten fabrikanten meer verantwoordelijk worden gehouden voor economische schade als gevolg van het verzaken van zorgplicht op het gebied van cybersecurity. Deze zorgplicht moet gaan bijdragen aan het beschermen van burgers en bedrijven tegen cybercrime.

Handhaving
Als handhaving van wettelijke eisen wordt ingevuld middels certificering van software, dan is er een risico op perverse effecten. Zo heeft de certificeringsinstantie een verdienmodel richting degene die gecertificeerd wil worden en kan een softwarefabrikant bij het certificering van software gaan voor de weg van de minste weerstand. Concurrentie tussen verschillende certificeringsinstanties leidt niet altijd tot betere standaarden en kan ook uitmonden in een race naar de bodem (het principe van '*maximum complacency*', de fabrikant kiest ervoor om certificering door één enkele certificeerder te laten bekrachtigen en verzet zich tegen pogingen om hem ertoe te brengen het product te verbeteren).[143]

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

Ervaringen uit het verleden: Common criteria, ISO 27001 en BitSight

Common Criteria
De *Common Criteria for Information Technology* is een internationale standaard voor computerbeveiliging. Deze standaard kent een aantal problemen: zo zijn de certificeringskosten hoog, de standaard generiek beschreven (de techniek is er buiten gelaten, inclusief *usability*, een belangrijke randvoorwaarde voor veiligheid), de standaard kan niet goed omgaan met snelle ontwikkelingen in de praktijk/ toepassing, de standaard wordt heel verschillend toegepast (bijvoorbeeld streng in Duitsland, erg los in Nederland) en vormt aansprakelijkheid geen onderdeel van de standaard.

ISO 27001
ISO 27001[144] werkt voor bedrijven vooral als manier om geld te verdienen. Certificering kost veel geld en is een bron van inkomsten voor de certificeringsinstanties. Bij de aanvraag van een certificaat door een bedrijf is de certificeringsinstantie afhankelijk van informatie die door het bedrijf wordt aangeleverd. Zo is het mogelijk voor de aanvrager om aan te geven dat bepaalde beveiligingsmaatregelen zijn genomen, terwijl die in de praktijk niet zijn geïmplementeerd. Er vind geen daadwerkelijke onafhankelijke toetsing plaats. Bijna alle grote lekken zijn voorgekomen bij bedrijven die met 27001 gecertificeerd zijn.[145]

BitSight
BitSight, anders dan ISO 27001 een initiatief van de private sector, is een bedrijf die het internet afspeurt op zoek naar servers van bedrijven en overheidsinstellingen. Servers die zijn ontdekt worden gescand en krijgen een beveiligingsscore toegekend (bijvoorbeeld op basis van hoeveel servers (niet) zijn gepatcht). Ze zijn daarmee niet afhankelijk van informatie aangeleverd door bedrijven (bij ISO 27001 de aanvrager) en komen op basis van de scans tot een score. Maar dit heeft ook nadelige effecten. Zo zijn bedrijven huiverig voor het opzettelijk verbinden van kwetsbare servers met het internet (bijvoorbeeld voor het trainen van werkgevers, studenten, e.a.). Zodra deze server opgemerkt wordt opgemerkt door BitSight heeft dit negatieve invloed op de beveiligingsscore van het bedrijf.

Handhaving kan alleen als fabrikanten verplicht worden transparant te zijn over hoe de software werkt en zodat derden de veiligheid ervan kunnen beoordelen. De *Executive Order* ter verbetering van de cyberveiligheid in de VS gaat hier op in en noemt dat er dringend behoefte is aan strengere en meer voorspelbare mechanismen om ervoor te zorgen dat producten veiliger en overeenkomstig hun beoogde werking functioneren.[146]

144 Een ISO standaard voor informatiebeveiliging. Zie https://www.iso.org/isoiec-27001-information-security.html.
145 Anderson, R., *Security Engineering*, 2020.
146 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Economische prikkels

De voorbeelden in dit onderzoek laten zien dat softwareproducten dynamisch zijn. Ze worden namelijk regelmatig aangepast voor nieuwe functionaliteit en het verhelpen van kwetsbaarheden. Tegelijkertijd kennen de producten vaak een lange geschiedenis omdat kan worden voortgebouwd op bestaande onderdelen. Dit maakt dat het voor fabrikanten een grote investering kan zijn om de fundamentele oorzaken (*root causes*) van onveiligheid, zoals beschreven in paragraaf 4.1.1, aan te pakken. Dat zou namelijk betekenen dat zij software dat het resultaat is van tientallen jaren van ontwikkeling opnieuw zouden moeten opbouwen.

Tegenover deze investering staan weinig economische prikkels. Verzekeraars verzekeren niet alleen organisaties die software gebruiken, maar ook fabrikanten die software maken. In die laatste rol eisten zij van fabrikanten dat zij de aansprakelijkheid voor de gevolgen van onveilige software afwentelen op de afnemers van de software. De Cyber Security Raad schrijft daarover dat verzekeraars idealiter eisen stellen aan zowel de fabrikant als aan de organisatie die de software gebruikt.[147]

Een fabrikant kan ook een economische prikkel ondervinden door waardedaling als gevolg van onveiligheid (aandeelhouders). Zo hebben aandeelhouders van SolarWinds het bedrijf aangeklaagd: volgens de aandeelhouders hebben de *private equity* bedrijven die eigenaar zijn van het bedrijf gekozen voor korte termijn winst boven cybersecurity ('*goldrush* bij investeerders in SaaS business').[148]

Daarnaast kan de materiële verplichting om de onveiligheid weg te nemen zorgen voor een economische prikkel voor een fabrikant om meer te doen om te voorkomen dat er software met kwetsbaarheden op de markt zijn. Op dit moment ligt deze economische prikkel alleen bij de afnemers van de software.

147 Cyber Security Raad (CSR), *Integrale aanpak cyberweerbaarheid*, 2021.
148 https://www.scmagazine.com/home/solarwinds-hack/solarwinds-lawsuit-claims-private-equity-owners-sacrificed-cybersecurity-to-boost-short-term-profits/

Traceren en terugroepen in de voedselsector[149]

In de voedselsector zijn voedselbedrijven verplicht om te kunnen traceren aan wie ze voedselproducten hebben geleverd. Deze plicht geldt voor de gehele voedselketen, van primaire productie (zoals landbouw, veeteelt en visserij) tot de consument die het voedsel opeet. In elke schakel van deze keten moet een voedselbedrijf kunnen traceren waar hun grondstoffen vandaan komen en aan wie zij hun producten hebben geleverd. Deze verplichting wordt traceerbaarheid genoemd. Als een voedselbedrijf tot de ontdekking komt dat ze onveilig voedsel op de markt hebben gebracht, moet het binnen vier uur een distributielijst met alle afnemers[150] en afgenomen producten moeten samenstellen en desgewenst aanleveren aan de autoriteiten.

Voedselbedrijven zijn ook verplicht om dit voedsel uit eigen initiatief of op last van de autoriteiten terug te roepen (*recall*). In de praktijk vinden autoriteiten het voldoende als een voedselbedrijf zich beperkt tot een publicatie in een dagblad en/of op de eigen website, maar een 'zuivere *recall*' betekent dat het voedselbedrijf zijn afnemers zo direct mogelijk waarschuwt en oproept de producten terug te brengen en eventueel de producten zelf ophaalt bij de afnemer. Dat laatste gebeurt bijvoorbeeld bij *recalls* van personenauto's, wanneer het veiligheidsprobleem zo ernstig is dat de personenauto geen gebruik mag maken van de openbare weg.

Regulering en aansprakelijkheid spelen ook een rol bij het ontstaan van kwetsbaarheden. Op dit moment zijn er weinig mogelijkheden voor overheden en organisaties om fabrikanten te verplichten cybersecurity in hun producten te borgen. Afnemers weten niet altijd hoe ze eisen moeten stellen en een fabrikant verantwoording moeten laten afleggen. Daarmee wordt de kwetsbaarheid een probleem van de afnemer.

Er zijn nu nauwelijks regels voor het op de markt brengen van software. De huidige marktwerking van softwareproducten dwingt te weinig af dat veiligheidsrisico's goed worden beheerst. Kwetsbaarheden opsporen is tijdrovend, kost veel menskracht en is daarmee duur. In sommige gevallen kan het nodig zijn om een product opnieuw op te bouwen om het echte (veiligheids)probleem aan te pakken. De afwezigheid van economische prikkels verklaart dat fabrikanten deze afweging op dit moment niet maken.

149 Vanuit het idee dat er een keten is van producent via een aantal tussenstappen tot de consument, geldt de verplichte traceerbaarheid voor elk voedselbedrijf één stap terug en één stap vooruit in de keten (exclusief de stap naar de eindgebruiker ofwel de consument). Bron: Artikel 18, lid 1 van Verordening (EG) nr. 178/2002 in: Richtsnoeren voor de tenuitvoerlegging van de artikelen 11, 12, 14, 17, 18, 19 en 20 van Verordening (EG) nr. 178/2002 betreffende de algemene levensmiddelenwetgeving (26 januari 2010).

150 Voor de laatste schakel (de eindverbruiker, consument) geldt de verplichting om te traceren niet, maar sommige retailers registreren leveringen aan consumenten (deels) wel (online bestellingen, klantenkaarten et cetera).

4.2 De aanschaf en ingebruikname van software door organisaties

Steeds meer processen in onze maatschappij en binnen organisaties vinden digitaal plaats. Hiermee neemt de afhankelijkheid van digitale systemen, en de software die deze systemen bevatten, toe voor zowel organisaties als voor de gehele samenleving. Omdat software altijd kwetsbaarheden zal bevatten, is het voor organisaties van belang om rekening te houden met de risico's die dit met zich meebrengt bij de aanschaf en het gebruik van software. De vragen die hier worden behandeld zijn: hoe gaan organisaties die software aanschaffen en gebruiken (we noemen dit verder 'afnemers'), zoals gemeenten, ziekenhuizen en bedrijven, om met de risico's bij de aanschaf en ingebruikname van software? Welke dilemma's en belemmeringen spelen hierbij een rol?

4.2.1 De verhoudingen op de softwaremarkt

Een aantal factoren belemmert de mate van risicobeheersing bij het aanschaffen van software met kwetsbaarheden. Dat blijkt uit interviews met organisaties. Eén van deze factoren is de verhouding tussen fabrikanten en afnemers op de softwaremarkt. Op de softwaremarkt is sprake van informatieasymmetrie.[151] Softwarefabrikanten hebben meer informatie over de samenstelling van producten dan afnemers. Voor een afnemer is de samenstelling en kwaliteit van software vaak niet te achterhalen. Dit komt doordat fabrikanten over het algemeen weinig transparant zijn over de opbouw van hun producten. Daarnaast hebben veel organisaties niet de juiste kennis en capaciteit om de informatie te kunnen beoordelen wanneer een fabrikant dit inzicht wel biedt.

Door deze informatieasymmetrie is het voor afnemers moeilijk om de kwaliteit en veiligheid van software te beoordelen. Hierdoor beoordelen afnemers producten voornamelijk op de elementen die zij wel kunnen controleren zoals prijs, functionaliteit en gebruiksgemak. Het gevolg hiervan is dat fabrikanten met elkaar concurreren op deze elementen, en dat het voor fabrikanten niet loont om te investeren in de veiligheid van hun producten. Er zijn geen wettelijke bepalingen die deze informatieasymmetrie compenseren door de aansprakelijkheid te verleggen van afnemer naar fabrikant.

Op de softwaremarkt zijn er enkele grote fabrikanten die de markt beheersen. Door de marktmacht van een aantal fabrikanten zijn er voor bepaalde functionaliteiten maar enkele producten beschikbaar van een selecte groep leveranciers, bijvoorbeeld bij besturingssystemen als Windows en macOS of kantoorsoftwarepakketten als Microsoft Office. Fabrikanten bieden veelal standaard pakketten aan en afnemers hebben weinig mogelijkheden om deze op eigen wensen of eisen af te stemmen. Dit komt doordat de softwaremarkt een wereldwijde markt is, waarbij het voor afnemers in Nederland alleen lastig is om hier invloed op uit te oefenen. Daar is een groter machtsblok voor nodig, bijvoorbeeld op EU of VN niveau of door gezamenlijke inspanning van afnemers.

Wanneer kwetsbaarheden worden ontdekt in softwareproducten, gaat de fabrikant aan de slag met het ontwikkelen van een patch voor de kwetsbaarheden. Dit kost de fabrikant middelen. Veel van de kosten en de risico's bij kwetsbaarheden worden gedragen door de afnemer van de software. De afnemer maakt kosten om systemen te mitigeren en te patchen. Bovendien maakt de afnemer ook kosten bij eventuele stilstand van de

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

bedrijfsvoering bijvoorbeeld bij een aanval. Indien de afnemer verzekerd is voor cyberincidenten, vergoedt de verzekeraar in sommige gevallen een deel van de kosten die een afnemer maakt. Over het algemeen worden de risico's op schade door kwetsbaarheden in software hoofdzakelijk door de afnemer gedragen. Deze factoren samen maken dat de markt voor software door experts wordt gekenmerkt door de asymmetrische relatie tussen fabrikant en afnemer.[152]

4.2.2 De aanschaf van software

Een afnemer schaft software aan vanuit een functionele behoefte om werkzaamheden of processen op een digitale manier te kunnen afhandelen. Na het identificeren van deze functionele behoefte kijkt een afnemer welke mogelijkheden er allemaal in de markt zijn om in zijn behoefte te voorzien. Bij het selecteren van een product spelen verschillende wensen en eisen een rol, zoals de functionaliteiten van de software, gebruikersgemak, prijs en beveiliging.

Veiligheidseisen formuleren en daarop controleren

Zoals in paragraaf 4.1 besproken zijn er momenteel weinig manieren om fabrikanten te verplichten cybersecurity te borgen in hun producten. Dit legt een extra belasting bij de afnemers om bij de aanschaf van software op veiligheid te toetsen. Omdat er sprake is van informatieasymmetrie op de softwaremarkt (zie 4.2.1), schaffen afnemers software veelal aan op basis van een functionele behoefte, en spelen veiligheidsaspecten een kleinere rol.

Om de juiste veiligheidseisen te kunnen formuleren heeft de afnemer kennis nodig van wat relevante eisen zijn voor zijn situatie. Daarnaast heeft de afnemer ook informatie nodig over het product om te kunnen beoordelen in hoeverre het product aan die eisen voldoet en hoe dit te duiden voor zijn situatie. Wanneer een organisatie wel de juiste eisen kan stellen, maar deze niet kan controleren, is het immers niet mogelijk voor de organisatie om te beoordelen of de software daadwerkelijk aan de veiligheidseisen voldoet.

Er zijn veel verschillen te zien in de mate waarin organisaties veiligheidseisen stellen aan de softwareproducten die zij aanschaffen. Sommige, veelal grotere, organisaties hebben de juiste kennis in huis om eisen te stellen en deze ook te controleren. Een veel gestelde veiligheidseis is het mogen uitvoeren van penetratietesten.[153] Andere, meestal kleinere, organisaties lukt het niet om de juiste veiligheidseisen te stellen omdat zij de kennis en middelen hiervoor niet beschikbaar hebben, of het belang hiervan niet inzien. Fabrikanten laten ook niet altijd toe dat hun producten gepentest worden, omdat er ook risico's bij komen kijken. Wanneer penetratietesten bijvoorbeeld worden uitgevoerd op een cloud omgeving, bestaat het risico dat de test schade aanricht en de beschikbaarheid van de omgeving in het geding komt. Daarnaast is het bij het uitvoeren van penetratietesten of *reverse engineering*[154] mogelijk om erachter te komen hoe een softwareproduct opgebouwd is, en bijvoorbeeld details over een bepaald algoritme te achterhalen.

152 Anderson, R., *Security Engineering*, 2020.
153 Een pentest is een beveiligingscontrole waarbij er van buitenaf wordt getoetst op kwetsbaarheden en er vervolgens wordt geprobeerd om via deze kwetsbaarheden in te breken in het systeem. Zie hoofdstuk 2.
154 Reverse engineering is het onderzoeken van een product om de werking en opbouw hiervan af te leiden.

Vanwege de concurrentie op de markt geven fabrikanten deze informatie niet graag prijs. Fabrikanten stellen daarom vaak voorwaarden en beperkingen aan penetratietesten.

Het is dus niet vanzelfsprekend dat afnemers penetratietesten mogen uitvoeren op de software die zij gebruiken. Een manier waarop afnemers zeker kunnen stellen dat ze penetratietesten wel mogen uitvoeren, is door dit expliciet als eis op te nemen in het contract met de leverancier. Enkele organisaties gaven in interviews aan dat ze penetratietesten weliswaar als standaardeis in contracten opnemen, maar dat het soms overtuigingskracht kost in de onderhandelingen met leveranciers van producten. Grotere organisaties met een hogere cybervolwassenheid laten over het algemeen wel penetratietesten uitvoeren op hun systemen. Er zijn ook organisaties die bij het vinden van een kwetsbaarheid in software die in hun branche veel gebruikt wordt, deze kwetsbaarheid doorgeven aan de brancheorganisatie zodat deze de kwetsbaarheid namens alle aangesloten organisaties kan aankaarten bij de fabrikant van het product.

Hoewel het stellen van veiligheidseisen en het controleren hiervan dus niet standaard gebeurt, zijn er wel voorbeelden van bepaalde sectoren waarin afnemers verplichte veiligheidseisen stellen aan softwareproducten en leveranciers. Het ministerie van Defensie stelt bijvoorbeeld strenge veiligheidseisen aan leveranciers die opdrachten voor het ministerie uitvoeren. Deze eisen zijn vastgelegd in de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) regeling. De MIVD controleert of een leverancier voldoet aan deze regeling. Daarnaast stellen financiële instellingen ook strenge veiligheidseisen aan de producten die zij in gebruik nemen. Ook de Rijksoverheid wil door middel van inkoopbeleid digitale veiligheid van software bevorderen. Om overheidsorganisaties te helpen bij het formuleren van veiligheidseisen is de Inkoopeisen Cybersecurity Overheid (ICO) wizard ontwikkeld. De ICO-wizard is een hulpmiddel voor overheidsorganisaties, maar het is niet verplicht om deze te gebruiken en het geeft geen handvatten hoe afnemers de gestelde eisen kunnen controleren. Bovendien geeft de ICO-wizard alleen een groslijst aan eisen waar organisaties uit kunnen putten. Een organisatie moet zelf de juiste selectie maken, daar is expertise voor nodig die niet elke organisatie tot zijn beschikking heeft. Daarnaast moet de organisatie ook zelf het product beoordelen, waar ook kennis voor nodig is en medewerking van de fabrikant.[155]

155 Ministerie van Defensie, *Algemene Beveiligingseisen Defensieopdrachten 2019*, februari 2020. Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid, *Roadmap Digitaal Veilige Hard- en Software*, april 2018. De ICO wizard is een tool ontwikkeld voor overheidsorganisaties op basis van de Baseline Informatiebeveiliging Overheid (BIO), om de vraag naar digitaal veilige software te stimuleren en een prikkel voor fabrikanten te creëren om digitaal veilige producten op de markt te brengen. Organisaties kunnen in de ICO-wizard zelf de eisen selecteren die bij hen van toepassing zijn bij de inkoop van software, zie: https://www.bio-overheid.nl/ico-producten/

Inkoopeisen door overheden in het buitenland: US Executive Order
In de Verenigde Staten is in mei 2021 een *Executive Order*[156] uitgebracht, waarin verschillende maatregelen worden genomen met als doel het verbeteren van de nationale cybersecurity.[157] Naast een aantal maatregelen met betrekking tot informatiedeling, het versterken van capaciteit bij incidentbestrijding en leren van incidenten, is de *Executive Order* ook gericht op het veiliger maken van software.

Een van de maatregelen die in de *Executive Order* is opgenomen is het stellen van standaarden aan software die gebruikt wordt door de federale overheden. In het *Executive Order* worden federale overheden verplicht om veiligheidseisen te stellen aan softwareleveranciers. Indien partijen niet aan deze gestelde eisen voldoen, zullen zij geen software meer mogen leveren aan Amerikaanse federale overheidsorganisaties.

In het algemeen is het stellen van veiligheidseisen en controle hierop door organisaties aan fabrikanten vrijblijvend. Hier is geen regelgeving voor. De mate waarin dit gebeurt is dus afhankelijk van de organisaties zelf. Niet iedere organisatie heeft de expertise om de juiste eisen te stellen aan software, en om vervolgens te controleren of producten aan de eisen voldoen. Er zijn geen waarborgen in het systeem om af te dwingen dat producten aan bepaalde eisen voldoen.

4.2.3 Gebruiks- en onderhoudsfase van software binnen organisaties

Zoals in hoofdstuk 2 is beschreven is er een aantal maatregelen die organisaties kunnen nemen om hun bedrijfssystemen te beveiligen en zich voor te bereiden op incidenten. Het NCSC beveelt een aantal basismaatregelen aan, die organisaties kunnen treffen om cyberaanvallen tegen te gaan. Voorbeelden daarvan zijn het patchen van systemen, het gebruik van *firewalls*, netwerksegmentatie en detectiemogelijkheden. In het Cybersecuritybeeld Nederland 2021 en de tien jaren ervoor concludeert de NCTV dat hoewel de weerbaarheid van organisaties zich ontwikkelt, deze nog niet voldoende is. Niet alle organisaties hebben de basismaatregelen getroffen.[158] Hoe kunnen we begrijpen dat organisaties deze basismaatregelen niet altijd nemen? Dit heeft deels te maken met het vermogen om maatregelen te nemen en deels met *biases* in de manier waarop mensen in organisaties naar het risico van cyberaanvallen kijken.[159] Hieronder gaan we in op de belemmeringen en dilemma's die bij deze maatregelen komen kijken.

Omgaan met de afhankelijkheid van software

Bij het gebruik van software en de afhankelijkheid hiervan komen altijd risico's kijken. Het is voor afnemers onmogelijk om een risico volledig te mitigeren, maar wel van belang om allereerst de risico's in beeld te hebben en af te wegen. Het dubbel uitvoeren van een systeem door twee softwareproducten van verschillende fabrikanten te gebruiken is een manier om de afhankelijkheid van een product te verminderen. Het is echter niet

156 Een *Executive Order* is een decreet uitgegeven door de president, met dezelfde kracht als een wet.
157 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, geraadpleegd op 14 juli 2021.
158 Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2021*, juni 2021. https://www.security.nl/posting/710981/Cybersecuritybeeld+Nederland%3A+al+tien+jaar+lang+de+basis+niet+op+orde
159 Meyer, R. en Kunreuther, H., *The Ostrich Paradox: Why we underprepare for disasters*, 2017.

realistisch voor iedere organisatie om alle systemen redundant uit te voeren omdat dit extra middelen kost. Daarnaast kan het ook zo zijn dat wanneer een afnemer verschillende systemen heeft van verschillende leveranciers, systemen niet goed samen kunnen werken (compatibiliteitsproblemen). In sommige gevallen kiezen afnemers er wel uitdrukkelijk voor om systemen redundant uit te voeren, bijvoorbeeld wanneer het gaat om vitale systemen die cruciale processen mogelijk maken en wanneer er grote gevolgen zijn wanneer de beschikbaarheid wegvalt.[160] Wat betreft de systeemafhankelijkheden van een bepaald product in een netwerk, zijn veel verschillen te zien in hoe organisaties netwerken hebben ingericht. Een organisatie gaf in een interview aan zijn systemen zo ingericht te hebben dat er geen *single point of failure* is, zodat wanneer een systeem wegvalt, andere systemen en processen wel door kunnen gaan. Een andere organisatie gaf aan dat in zijn netwerk een aantal producten zit waar veel processen van afhankelijk zijn. Wanneer een systeem in dat geval wegvalt, kunnen veel processen in die organisatie niet meer doorgaan.

Bij het omgaan met de afhankelijkheid van software is het van belang om inzicht te krijgen in de risico's die komen kijken bij het gebruik van een bepaald product en de systeemafhankelijkheden. Wanneer een organisatie zich bewust is van zijn kritieke systemen en de afhankelijkheid hiervan goed in beeld heeft, is het beter mogelijk om een risicoafweging te maken van de maatregelen die genomen moeten worden bij een incident en in voorbereiding op een incident. In het algemeen is een groot verschil te zien tussen organisaties in de mate waarin zij hun systemen in beeld hebben. Voornamelijk de grote organisaties hebben vaak een (redelijk) goed beeld welke systemen ze hebben, en welke versies er draaien. Dit leggen ze bijvoorbeeld vast in een *Configuration Management Database* (CMDB). Wanneer er een kwetsbaarheid wordt gepubliceerd, kunnen zij in deze database zien of de kwetsbaarheid van toepassing is op de organisatie, en of ze dus moeten patchen. Ook kunnen ze, doordat ze systemen en afhankelijkheden in beeld hebben, makkelijker en accurater een risicoanalyse maken wat er zou gebeuren als het systeem bijvoorbeeld uitgeschakeld moet worden. Bij andere (veelal kleinere) organisaties is te zien dat ze niet altijd een compleet beeld hebben van de systemen die ze hebben. Het risico hierbij is dat wanneer er een belangrijke kwetsbaarheid aan het licht komt, deze organisaties niet (op tijd) actie op ondernemen en gecompromitteerd kunnen worden. Bovendien kunnen deze organisaties ook geen complete risicoanalyse maken wat de impact is wanneer een systeem uitgezet moet worden.

Het in beeld brengen en houden van de systemen en de systeemafhankelijkheden kost capaciteit en het belang van het up-to-date houden van dit overzicht moet door de hele organisatie gezien worden. Voor organisaties met weinig capaciteit kan het hierdoor een uitdaging zijn om een compleet beeld te krijgen van alle systemen en de afhankelijkheid tussen deze systemen. Ook de organisatiestructuur kan het lastiger maken om een compleet beeld te krijgen van alle systemen. De Inspectie van het Onderwijs stipt dit, na de aanval met gijzelsoftware bij de Universiteit Maastricht, aan als een van de bepalende factoren.[161] Universiteiten kennen een gelaagde bestuursstructuur met verschillende bestuursorganen, die ieder hun eigen informatiebeveiliging regelen. Dit maakt het een

160 Jacobs, D., *7 factors to consider in network redundancy design*, https://searchnetworking.techtarget.com/tip/7-factors-to-consider-in-network-redundancy-design, geraadpleegd op 16 juli 2021.
161 Inspectie van het Onderwijs, *Cyberaanval Universiteit Maastricht*, mei 2020.

uitdaging om zicht te hebben op de complete netwerk van ICT-systemen. Daarnaast kunnen ketenafhankelijkheden het lastig maken om een beeld te hebben van het complete systeem en de afhankelijkheden. Veel organisaties werken samen met externe leveranciers of ketenpartners. Processen van een organisatie kunnen hierdoor ook (deels) afhankelijk zijn van de systemen die externe partijen in gebruik hebben, zoals bijvoorbeeld het geval was bij het Kaseya voorval (zie 3.3.5).

Patchen

Software is meestal geen statisch product, maar blijft ook na de aanschaf in ontwikkeling. Ook het dreigingslandschap is niet statisch en continu in beweging. Wanneer kwetsbaarheden in software worden gevonden, ontwikkelen fabrikanten patches om deze te verhelpen (zie paragraaf 4.1). Het is op dit moment voornamelijk aan de afnemer om deze patches door te voeren om de kwetsbaarheden op zijn systemen op te lossen. Patchen brengt echter ook risico's en afwegingen met zich mee. Vanwege het grote aantal patches dat jaarlijks verschijnt (sommige organisaties moeten wel 100 duizend patches per jaar toepassen) is het voor een organisatie niet altijd mogelijk om patches op tijd te installeren. Door de grote hoeveelheid jaarlijkse patches hebben organisaties moeite om een volledig en *up-to-date* overzicht te hebben van kwetsbaarheden in hun systemen. Om dit te vereenvoudigen kunnen bedrijven een scanningdienst afnemen. Deze scanningdiensten scannen op bekende kwetsbaarheden. Maar niet alle kwetsbaarheden zijn te scannen en de lijst waarop wordt gescand is vaak incompleet. Kleinere organisaties hebben daarnaast meestal niet de middelen om dergelijke scanningdiensten af te nemen. Zij baseren zich vaak alleen op adviezen van het NCSC. Organisaties kunnen in deze omstandigheden niet alles tijdig patchen. Het is daarom onvermijdelijk dat bekende kwetsbaarheden, ook kritieke, niet worden gepatcht.

Het grote aantal kwetsbaarheden zorgt voor een grote druk op organisaties om het patchproces op gewenste wijze te organiseren en af te wegen bij welke kwetsbaarheden direct actie moet worden ondernomen. Het onvermogen van organisaties om beveiligingslekken tijdig te patchen maakt het volgens penetratietesters van *Positive Technologies* makkelijker voor aanvallers om bedrijfsnetwerken binnen te dringen. Patchen vergt kennis van systemen en capaciteit van medewerkers in organisaties. ICT medewerkers hebben naast het patchen van systemen nog vele andere werkzaamheden die ook uitgevoerd moeten worden. Voor iedere organisatie is het een afweging tussen het door laten gaan van dagelijkse werkzaamheden of het direct patchen van de systemen. Afnemers zijn soms terughoudend om patches direct uit te voeren omdat het risico bestaat dat na de patch systemen niet meer goed werken of uitvallen, wat gevolgen heeft voor de bedrijfsvoering van een organisatie. Daarnaast kan het zijn dat een patch de kwetsbaarheid niet of maar deels verhelpt.[162] Uit interviews blijkt dat deze afweging voornamelijk voor kleinere organisaties lastig is, omdat zij beperkte middelen hebben om extra capaciteit in te zetten voor het patchen van systemen.

Omdat het zoals hierboven besproken voor organisaties een uitdaging kan zijn om een compleet beeld te hebben van alle systemen die in gebruik zijn, kan het ook zijn dat een

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

afnemer een kwetsbaarheid niet patcht omdat deze geen *up-to-date* overzicht heeft van welke software waar draait, welke versie het betreft en of een patch al dan niet nodig is om de veiligheid van de systemen te kunnen garanderen. Ook is voor afnemers niet altijd duidelijk uit welke componenten de door hen gebruikte software precies bestaat omdat deze veelal *closed source* is. Dat wil zeggen dat de broncode niet inzichtelijk is voor de afnemer en de fabrikant ook weinig loslaat over de architectuur van de software. Daarnaast is veel software gebaseerd op open source componenten die kritieke lekken bevatten, zonder dat dit bekend is bij afnemers.[163] Hierdoor kunnen afnemers zonder dat ze het zelf weten kwetsbaar zijn.

Ook moet de gehele organisatie het belang en de urgentie van patchen onderkennen. Voor organisaties is niet altijd duidelijk dat ze aangevallen kunnen worden zonder dat een aanvaller het specifiek op ze voorzien heeft. Een kwetsbaarheid in software op een server die met het internet verbonden is trekt aanvallers als het ware aan. Deze aanvallers scannen automatisch op alle servers die kwetsbare software bevatten, in de hoop dat daar servers bij zijn waarlangs ze het digitale systeem van organisaties kunnen binnendringen. Uit onderzoek blijkt dat afnemers hun acties vaak baseren op eerdere ervaringen die zij hebben gehad met updates.[164] Veel gepubliceerde kwetsbaarheden worden niet actief misbruikt door aanvallers. Wanneer afnemers wachten met patchen van kwetsbaarheden die niet worden gebruikt voor aanvallen, heeft dat geen gevolgen voor de organisatie. Dit zorgt ervoor dat afnemers het belang van een snelle reactie wellicht minder hoog inschatten bij volgende kwetsbaarheden.

Volgens fabrikanten en experts kan het verplaatsen van software naar de *cloud* een oplossing zijn om ervoor te zorgen dat systemen op tijd gepatcht kunnen worden. Dit wordt een *Software as a Service* (SaaS) oplossing genoemd.[165] Omdat de software dan wordt beheerd door de fabrikant, is het voordeel van SaaS dat patches sneller getest en toegepast kunnen worden. Er zit dan namelijk geen tijd tussen het uitkomen van een patch en het toepassen hiervan, waardoor afnemers altijd snel de laatste patches hebben. Bij SaaS wordt het toepassen van patches de verantwoordelijkheid van de fabrikant in plaats van de afnemer. Het verplaatsen van software naar de *cloud* gaat echter ook gepaard met afwegingen en risico's voor een organisatie. Het nadeel van SaaS oplossingen is dat in het geval van een kwetsbaarheid alle servers kwetsbaar zijn, aangezien deze allemaal op dezelfde versie draaien. Daar kan dan alleen door de fabrikant iets aan gedaan worden, de afnemer speelt daar geen rol in.

Wanneer afnemers systemen in eigen beheer hebben, kunnen ze zelf patchen, mitigeren of de systemen afsluiten. Bovendien hebben organisaties bij het afnemen van een clouddienst geen zicht op wat het product inhoudt. Daarnaast is een organisatie dan ook minder flexibel, het aanpassen van software is nog maar beperkt mogelijk. Ook kunnen automatische updates - bij SaaS oplossingen - de continuïteit van systemen bedreigen of nieuwe kwetsbaarheden introduceren. Afnemers hebben daar dan helemaal geen

163 'Veel kritieke lekken door open source in standaard apps', *AG Connect,* https://www.agconnect.nl/artikel/veel-kritieke-lekken-door-open-source-standaard-apps, 5 augustus 2021.
164 Rajivan et al., Update now or later? Effects of experience, cost, and risk preference on update decisions, *Journal of Cybersecurity*, 2020.
165 Bij SaaS wordt software als een online dienst aangeboden. De afnemer krijgt via internet of via een VPN toegang tot de software die bij de aanbieder beheerd wordt.

controle meer over. Een andere overweging voor een afnemer is dat bij een incident de systemen bij de fabrikant staan. Een fabrikant weet het meeste van het product en is daarmee de aangewezen partij om bij een incident zijn software te kunnen analyseren. De fabrikant kan dan de afnemer helpen om te onderzoeken of deze getroffen is, en het probleem op te lossen. Soms willen afnemers echter geen informatie delen met externe partijen, bijvoorbeeld omdat het niet mag, of omdat ze geen risico willen lopen dat informatie buiten de organisatie belandt. Ook kan het vanwege de aard van het systeem zo zijn dat een afnemer deze niet wil verbinden met het internet. In dat geval is SaaS geen oplossing en moet een afnemer (een deel van) zijn systemen fysiek in beheer hebben.

Het veelvuldig patchen van software introduceert nieuwe problemen. Wanneer een afnemer niet patcht heeft deze mogelijk een beveiligingslek dat van buitenaf automatisch op te sporen is. Vanwege de grote en toenemende hoeveelheid patches is het patchen van alle kwetsbaarheden niet behapbaar voor organisaties. Bovendien is voor afnemers de noodzaak van (snel) patchen niet altijd duidelijk. Het aanbieden van software vanuit de *cloud* verplaatst de verantwoordelijkheid om te patchen naar de fabrikant, maar gaat ook gepaard met risico's voor afnemers.

Preventie en detectie

Naast patchen is er ook nog een aantal andere preventieve en detectiemaatregelen die een organisatie kan nemen om zijn netwerk te beschermen, zoals het instellen van een *firewall*, netwerksegmentatie en de monitoring van systemen. Deze maatregelen gaan ieder gepaard met risico's en afwegingen voor een organisatie.

Een maatregel om toegang van buitenaf tot de systemen van een organisatie te beperken is het instellen van een *firewall*.[166] De uitdaging bij *firewalls* is dat deze zo ingesteld moeten worden dat ongewenste activiteit wordt tegengehouden, maar dat gewenste activiteit niet onterecht ook tegen wordt gehouden. Daarnaast moeten de juiste regels en beleid ingesteld worden, en is het van belang deze periodiek te checken en updaten. Dit vraagt kennis en capaciteit van een organisatie. Een *firewall* brengt ook risico's met zich mee wanneer een organisatie niet de juiste kennis heeft over wat de firewall precies doet. Hierdoor heeft een organisatie geen zicht op of er systemen onnodig openstaan voor verkeer.[167]

Om de impact van een mogelijk incident te beperken kan een organisatie zijn netwerk segmenteren. Het risico bij segmentatie is dat wanneer een netwerk uit veel segmenten bestaat, het erg veel tijd en geld kost om het netwerk te beheren.[168] Het implementeren van segmentatie in een netwerk is een proces dat veel aanpassingen vergt, kostbaar is en verstorend kan zijn voor het primaire proces van een organisatie. Voor organisaties is

166 Een firewall is een machine die tussen een netwerk en het internet in staat, verkeer monitort, en mogelijk schadelijk verkeer tegenhoudt.

167 https://www.insightsforprofessionals.com/it/security/firewall-management-challenges-how-solve-them, geraadpleegd op 22 juli 2021. AlgoSec, *Firewall Management: 5 challenges every company must address – an AlgoSec Whitepaper*, 2015.

168 *'Hazardous Network Segmentation: when more isn't better'*, AlgoSec, https://www.algosec.com/blog/hazardous-network-segmentation-when-more-isnt-better, geraadpleegd op 22 juli 2021.

het daarnaast moeilijk om medewerkers te vinden met de noodzakelijke vaardigheden en expertise.[169]

Naast meer preventieve maatregelen als *firewalls* en segmentatie investeren organisaties ook in detectiemogelijkheden en de monitoring van systemen. Hierbij kan een organisatie verdachte activiteit detecteren wanneer deze plaatsvindt. De uitdaging hierbij voor organisaties is dat het van belang is dat de detectie goed ingesteld is. Wanneer dit niet het geval is kan verdachte activiteit niet opgemerkt worden, of kan activiteit ten onrechte gedetecteerd worden als verdacht (*false positives*). Het hebben van detectiemogelijkheden garandeert dus niet dat alle verdachte activiteit opgemerkt wordt. Daarnaast moeten organisaties de kennis hebben om de activiteiten te kunnen duiden, en weten hoe ze moeten reageren wanneer ze activiteit van een aanvaller detecteren. Dit vraagt capaciteit en expertise van een organisatie. Voor vitale en rijksoverheidsorganisaties is het mogelijk om zich aan te sluiten bij het Nationaal Detectie Netwerk (NDN). Het NCSC geeft indicatoren door aan de deelnemers van het NDN om een potentiële aanval te kunnen herkennen. Voor deelname aan het NDN is het een vereiste dat organisaties zelf hun monitoringproces al ingericht hebben. Alleen de rijksoverheid en vitale organisaties kunnen zich direct aansluiten bij het NDN.[170]

Een tendens die in de cybersecuritywereld opgemerkt wordt is dat er steeds meer wordt geïnvesteerd in detectiemogelijkheden ten opzichte van preventie.[171] In de beveiligingswereld wordt vaak benadrukt dat het niet mogelijk is alle aanvallen te voorkomen, dus dat het loont om vooral te investeren in detectie en respons. Dit was ook zichtbaar bij enkele organisaties die we hebben gesproken, die voornamelijk in detectie en respons hadden geïnvesteerd. Investeren in detectie biedt echter niet altijd garanties, zoals hierboven ook besproken. Bij één van de geïnterviewde organisaties detecteerde het systeem de aanval via de software kwetsbaarheid niet, met als gevolg dat de organisatie alsnog werd gecompromitteerd. Voor een zo veilig mogelijk systeem zijn dus meerdere lagen van veiligheid en beveiliging nodig, zowel preventie als detectie en respons.

4.2.4 Besturen van digitale veiligheid in organisaties

Capaciteit en expertise

Alle hierboven genoemde maatregelen vragen capaciteit en kennis van organisaties. De mate waarin een organisatie deze capaciteit en kennis tot zijn beschikking heeft hangt af van de grootte van een organisatie en de volwassenheid op cybersecuritygebied. Kleinere organisaties hebben weinig capaciteit en kennis op het gebied van informatiebeveiliging. In het algemeen zagen we in dit onderzoek grote verschillen in de mate waarin organisaties maatregelen nemen om incidenten te voorkomen en de mate waarin zij voorbereid zijn op incidenten.

169 Holt, M., Security Think Tank: Benefits and challenges of security segmentation, *Computer Weekly*, https://www.computerweekly.com/opinion/Security-Think-Tank-Security-segmentation-benefits-and-challenges, geraadpleegd op 15 juli 2021.

170 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en ministerie van Veiligheid en Justitie, *Handreiking voor implementatie van detectie-oplossingen*, oktober 2015. Bepaalde organisaties als zorginstellingen, gemeenten, onderwijsinstellingen en waterschappen kunnen zich indirect aansluiten op het NDN via de sectorale CERTs. Zie: https://www.ncsc.nl/actueel/weblog/weblog/2020/het-nationaal-detectie-netwerk-voor-een-private-organisatie.

171 https://www.youtube.com/watch?v=3IDiqYil2lQ, geraadpleegd op 16 juli 2021.

Een gemeente met een beperkt budget heeft bijvoorbeeld weinig capaciteit op het gebied van informatiebeveiliging en ICT in het algemeen. De CISO is daar de enige medewerker die zich bezig houdt met informatiebeveiliging. Door de beperkte capaciteit heeft de ICT afdeling onder andere moeite met het op orde krijgen van de CMDB van de organisatie en het op tijd uitvoeren van alle benodigde patches. Daartegenover staan bijvoorbeeld financiële instellingen die honderden cybersecurityprofessionals in dienst hebben. Zij hebben de capaciteit en expertise om de basis op orde te hebben en te anticiperen en reageren op incidenten.

Er zijn veel verschillen zichtbaar tussen organisaties in de mate waarin zij ICT werkzaamheden zelf uitvoeren of uitbesteden. Organisaties besteden werkzaamheden uit omdat zij niet voldoende expertise en capaciteit in huis hebben om het zelf uit te voeren. Door dit gebrek aan expertise en capaciteit hebben zij echter ook niet altijd de kennis om goed te kunnen beoordelen of de partij waar zij werkzaamheden aan hebben uitbesteed goed werk levert.

In het algemeen is er sprake van een tekort aan expertise in de cybersecurity markt. Dit is een jarenlang probleem dat niet af lijkt te nemen. In de gehele IT-sector is sprake van een krappe arbeidsmarkt, zo was in juli 2021 dertig procent van de vacatures voor IT-programmeurs en IT-ontwikkelaars onvervulbaar. Een van de oorzaken van het tekort aan expertise is dat professionals zich ondergewaardeerd voelen, en het moeilijk is in het cybersecurity domein te starten. Door toenemende hoeveelheid en complexiteit van aanvallen ervaren veel professionals daarnaast stress en burn-out klachten.[172]

Het risico hierbij is dat het capaciteitstekort op de markt alleen maar gaat toenemen. Tijdens het Citrix voorval was ook te zien dat er meer vraag naar cybersecurity professionals was dan aanbod, waardoor beveiligingsbedrijven geen capaciteit hadden om iedere organisatie die expertise nodig had te helpen. De capaciteit op het gebied van incidentbestrijding is gefragmenteerd via sectorale CERTs en voor preventieve maatregelen moet elke organisatie zelf capaciteit en expertise inzetten. Expertise wordt niet of weinig gebundeld en is hierdoor versnipperd.

Urgentie

Ook de mate waarin een organisatie het belang en de urgentie van het nemen van maatregelen inziet, en daar ook middelen voor in kan en wil zetten, speelt een rol bij de weerbaarheid van een organisatie. Bij overheden zoals gemeenten kan het bestuur niet zelf bepalen hoe middelen worden besteed, zoals bij private organisaties. Zij leggen daarvoor verantwoording af aan de gemeenteraad, die naast cybersecurity veel andere belangen heeft die ze moeten meewegen en ook veel gemeentelijke taken erbij hebben gekregen waar middelen voor moeten worden ingezet. Daar komt bij dat ICT vaak als vanzelfsprekend wordt beschouwd door bestuurders of volksvertegenwoordigers, zonder dat zij weten wat daar allemaal bij komt kijken. Het is vaak aantrekkelijker om geld uit te geven aan zaken die een tastbaar resultaat opleveren dan aan het voorkomen van problemen. Wanneer problemen worden voorkomen, is het resultaat namelijk niet zichtbaar.

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

Uit interviews is daarnaast gebleken dat in sommige organisaties de positie van de CISO in de organisatie ten tijde van het voorval zwak was, waardoor deze niet bij kon dragen aan een goed verloop van het incident. Bij een van de gesproken organisaties lukte het de CISO tijdens het voorval niet om het besluit om te mitigeren erdoorheen te krijgen bij de ICT afdeling, waardoor de organisatie gecompromitteerd werd. Naar aanleiding van dit incident is de positie van de CISO in de organisatie veranderd en versterkt, waardoor deze incidenten in de toekomst makkelijker aan kan kaarten bij het bestuur. Bij veel van de gesproken organisaties is te zien dat het gevoel van urgentie om te investeren in digitale veiligheid toeneemt na een dergelijk incident.

Individueel risico

Risico's die komen kijken bij kwetsbaarheden in software worden nu voornamelijk gezien als individuele risico's die iedere organisatie zelf moet beheersen. Het uitgangspunt in het Nederlandse stelsel is namelijk dat elke publieke en private organisatie zelf verantwoordelijk zijn voor zijn digitale weerbaarheid. De meeste organisaties hoeven hier geen verantwoording voor af te leggen. (Middel)grote bedrijven en organisaties moeten jaarlijks een accountantscontrole laten uitvoeren op de jaarrekening, om de getrouwheid hiervan aan te tonen. Een IT-verklaring maakt momenteel geen deel uit van deze accountantsverklaring, terwijl het op orde hebben van IT-beveiliging wel van belang is voor de continuïteit van een organisatie. De beroepsvereniging van IT-auditors heeft onlangs voorgesteld om een IT-verslag een vast onderdeel te maken van de accountantsverklaring.[173]

Wanneer incidenten als gevolg van kwetsbaarheden in software plaatsvinden, hebben deze impact op vele organisaties en burgers. Kwetsbaarheden vormen hierdoor een collectief risico voor de samenleving als geheel. Individuele organisaties hebben maar beperkte mogelijkheden om zelf de risico's te beheersen, afhankelijk van de capaciteit en expertise die ze in huis hebben. De kosten van cyberaanvallen stijgen jaarlijks. Steeds meer organisaties sluiten een cyberverzekering af om zich te verzekeren tegen schade bij incidenten. Toch is nog maar een klein deel van MKB bedrijven verzekerd tegen cyberincidenten.[174] Doordat de kosten van cyberincidenten oplopen, stijgt de premie voor cyberverzekeringen op dit moment ook. Wanneer er een incident plaatsvindt met een kwetsbaarheid in software die door vele organisaties wordt gebruikt, zullen de collectieve kosten van een incident echter dusdanig hoog zijn dat deze ook niet meer te dragen zijn door verzekeraars.

Van verzekeraars wordt verwacht dat ze een positieve rol kunnen spelen in het bevorderen van de cyberhygiëne van organisaties. Dit door eisen te stellen aan de maatregelen die organisaties genomen moeten hebben om gedekt te zijn voor cyberincidenten. Tegelijkertijd is er ook kritiek op de rol van verzekeraars, en staat ter discussie of zij een goede cyberhygiëne stimuleren, omdat verzekeraars *ransomware* betalingen dekken en omdat door organisaties genomen beveiligingsmaatregelen niet worden gecontroleerd.

173 NCTV, *Nederlandse Cybersecurity Agenda*, april 2018. Van Gils en Van Wijnen, 'Nieuwe IT-check kan voorwaarde worden voor krediet', *FD*, 11 augustus 2021.

174 Hiscox, *Hiscox Cyber Readiness Report 2020*, 2020; https://www.trouw.nl/economie/het-aantal-cyberaanvallen-groeit-explosief-maar-echt-ongerust-zijn-bedrijven-niet~b332e73e, geraadpleegd op 29 juli 2021. https://www.rtlnieuws.nl/tech/artikel/5000096/cyberverzekering-hacken-ransomware-gijzelsoftware-ddos-citrix, geraadpleegd op 29 juli 2021. Modderkolk, 'Vooraanstaande ict-beveiligers: 'Ransomware gaat richting nationale crisis, overheid moet meer doen', *De Volkskrant*, augustus 2021.

Recent is hier verandering in gekomen, en worden *ransomware* betalingen niet altijd meer gedekt door verzekeraars.[175]

Er is momenteel geen collectieve basis om organisaties te helpen hun weerbaarheid te vergroten. Elke organisatie moet zelf zijn basis opbouwen met de kennis en capaciteit die ze hebben.

Door de asymmetrische relatie tussen fabrikant en afnemer op het gebied van softwareveiligheid zijn afnemers doorgaans niet in staat zelf veiligheidseisen stellen bij de aanschaf van software en de juiste afwegingen maken. Er zijn wel mogelijkheden voor afnemers om bewust om te gaan met risico's van software, maar niet elke afnemer heeft de kennis en capaciteit om de juiste eisen te stellen en deze te controleren. Er bestaat geen algemene regelgeving omtrent de controle van software die fabrikanten verplicht aan bepaalde veiligheidseisen te voldoen.

Wat betreft preventie en voorbereiding op incidenten is er veel verschil in de weerbaarheid van organisaties. Veel maatregelen vergen een afweging van risico's. Niet alle organisaties hebben de expertise en capaciteit om maatregelen voldoende uit te voeren, of onderkennen de urgentie om hier capaciteit op in te zetten niet. Iedere organisatie is zelf verantwoordelijk voor zijn digitale weerbaarheid. Er is geen collectief fundament dat geboden wordt om organisaties te helpen de digitale weerbaarheid te vergroten.

4.3 Incidentbestrijding (respons)

De voorvallen die we in hoofdstuk 3 beschrijven laten zien dat de tijd tussen dat een kwetsbaarheid in software wordt gemeld en dat organisaties die kwetsbaar zijn worden aangevallen beperkt is: variërend van een maand tot enkele dagen of geen (*zero day*). In de vorige paragrafen beschreven we welke factoren van invloed zijn op de wijze waarop fabrikanten kwetsbaarheden in software voorkomen en reageren op kwetsbaarheden en wat organisaties die software gebruiken doen om te voorkomen dat hun digitale systeem daardoor beveiligingslekken kan hebben. In deze paragraaf gaan we in op de factoren die beïnvloeden hoe betrokken partijen, zoals fabrikant, organisatie en publieke en private incidentbestrijders het incident bestrijden om de gevolgen te beperken.

4.3.1 Informatiestroom

Na het bekend worden van een kwetsbaarheid is van cruciaal belang dat de relevante organisaties zo direct en zo snel mogelijk worden geïnformeerd. Organisaties die de software gebruiken hebben zo betrouwbaar en toegesneden mogelijke informatie nodig om in korte tijd een eigen afweging te maken hoe te handelen om de risico's te kunnen beheersen. Organisaties die niet in staat zijn om een eigen afweging te maken hebben behoefte aan een advies dat ze kunnen volgen. Fabrikanten en incidentbestrijders willen

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

weten hoe veel en welke organisaties kwetsbaar zijn en op welke manier deze worden aangevallen, zodat zij de juiste maatregelen kunnen nemen, faciliteren en/of adviseren. Deze informatie kan via een veelheid aan bronnen worden verzameld, zoals fabrikanten, vrijwillige en commerciële beveiligingsonderzoekers, CERTS via *coordinated vulnerability disclosure-procedures* en inlichtingen- en veiligheidsdiensten. De in dit rapport onderzochte voorvallen laten zien dat er op dit moment belemmeringen zijn om ervoor te zorgen dat informatie die vanuit verschillende publieke en private bronnen binnenkomt, zo snel mogelijk alle organisaties bereikt die deze informatie nodig hebben om de gevolgen van kwetsbaarheden in software te bestrijden.

Belemmeringen in het delen van informatie

Informatievoorziening is van cruciaal belang voor organisaties, omdat snel reageren bij incidenten als in dit onderzoek noodzakelijk is om binnendringen te kunnen voorkomen.[176] De meeste landen hebben een nationale autoriteit die optreedt als incidentbestrijder. In Nederland is NCSC het nationale CERT. De positie van nationale CERT is onder meer relevant, omdat andere partijen zoals softwarefabrikanten per land het nationale CERT gebruiken als aanspreekpunt, bijvoorbeeld om door te geven welke organisaties in een bepaald land kwetsbaar zijn om te worden aangevallen.

Bij het delen van informatie staan twee soorten informatie centraal: voorlichtingsinformatie (om te komen tot een handelingsperspectief of berichten over kwetsbaarheden en beveiligingsadviezen) en dreigingsinformatie. Dreigingsinformatie bestaat uit aanvallers-informatie en slachtofferinformatie. De knelpunten tijdens de incidentbestrijding hebben vooral betrekking op dreigingsinformatie: informatie over welke organisaties kwetsbaar zijn en hoe de aanvallers kunnen worden herkend.[177] Daarbij gaat het met name om de slachtofferinformatie die niet wordt gebruikt, waardoor partijen niet worden gewaarschuwd.

Bij NCSC komt veel informatie samen uit verschillende bronnen: naast fabrikanten gaat het om inlichtingen- en veiligheidsdiensten, andere overheden, sectorale samenwerkingsverbanden (ISAC's), onafhankelijke beveiligingsonderzoekers (al dan niet via DIVD), cybersecurity bedrijven en IT-dienstverleners, evenals berichten op social media zoals Twitter, Reddit en vakmedia. Geïnterviewde organisaties gaven aan momenteel zelf via formele en informele bronnen informatie te zoeken, omdat ze de gewenste informatie via NCSC niet of te laat krijgen.

Waargenomen juridische belemmeringen

NCSC stelt vast dat zij vanuit hun wettelijk gelimiteerde mandaat en andere juridische belemmeringen zoals de AVG beperkt is in het delen van slachtofferinformatie (zoals IP-adressen van kwetsbare servers) met organisaties die deze nodig hebben, namelijk dat zij deze informatie alleen mag delen met rijksoverheid en vitale aanbieders.[178] Tijdens de Citrix-crisis heeft het NCSC besloten om af te wijken van de eigen wettelijke kaders en dreigingsinformatie te delen met een aantal schakelorganisaties zoals Z-CERT en de IBD,

176 Dit belang is onlangs onderstreept in het adviesrapport *Integrale aanpak cyberweerbaarheid* van de Cyber Security Raad (april 2021).
177 Definitie Dialogic en TU/e (2020).
178 Het wettelijk mandaat van NCSC is geregeld in de Wet beveiliging netwerk- en informatiesystemen (Wbni), die sinds 9 november 2018 van kracht is.

in navolging daarvan zijn deze kaders in 2020 en 2021 verbreed. Overige sectoren waaronder vrijwel het gehele Nederlandse bedrijfsleven (1,8 miljoen bedrijven[179]) kregen geen dreigingsinformatie.

Een volgende belemmering is gelegen in *welke* informatie NCSC deelt met de informatieknooppunten. NCSC stelt zich namelijk op het standpunt dat het volgens de Wbni vertrouwelijke, tot aanbieders herleidbare gegevens alleen mag delen met CERTs, CSIRTs en inlichtingendiensten, en niet met OKTT's. Het ministerie van JenV beschouwt IP-adressen van kwetsbare servers als dergelijke vertrouwelijke, tot aanbieders herleidbare gegevens in het kader van de Wbni en als persoonsgegevens in het kader van de AVG.

In een onderzoek naar informatiedeling in opdracht van het WODC wordt erkend dat de institutionele setting en wet- en regelgeving belemmeringen opwerpen voor NCSC om informatie te kunnen delen, maar geeft aan dat deze belemmeringen mede het gevolg zijn van de wijze waarop het ministerie van JenV de regels interpreteert. Met andere woorden, het is binnen de huidige kaders van de wet- en regelgeving ook mogelijk om tot andere juridische inzichten en een ander oordeel te komen en tot het besluit om de informatie wel te delen.

In het onderzoek van WODC wordt geen uitspraak gedaan over wat de juiste visie is, wel dat het belangrijk is dat er consensus komt op dit punt. Daarom bevelen de onderzoekers aan dat er vervolgonderzoek wordt gedaan op deze juridische vragen. De minister van JenV kondigde een voorstel voor wetswijziging aan die de belemmering moet wegnemen door de bevoegdheden van het NCSC om relevante dreigingsinformatie te delen te verruimen. Het kan echter één tot enkele jaren duren voor deze wet is aangenomen en wordt uitgevoerd.[180]

De incidentbestrijding in Nederland, waaronder het verzamelen en delen van informatie, is gefragmenteerd en bevat hiaten. Daardoor is voor veel organisaties, waaronder een groot deel van het Nederlandse bedrijfsleven, niet geregeld dat zij tijdig informatie ontvangen wanneer zij gevaar lopen. Het gaat daarbij in het bijzonder om slachtofferinformatie, oftewel dat een organisatie (ook ongevraagd) wordt gewaarschuwd dat zijn systemen kwetsbaar zijn en hij risico loopt om te worden aangevallen. Het NCSC, dat op dit moment ten behoeve van heel Nederland de informatie ontvangt vanuit onder meer fabrikanten, NCSC's in andere landen, inlichtingen- en veiligheidsdiensten en andere gremia, deelt deze slachtoffer-informatie nu alleen met een selecte groep organisaties, maar niet met decentrale overheden en het merendeel van het Nederlandse bedrijfsleven en vanuit het uitgangspunt dat een organisatie vooraf toestemming geeft om te worden geïnformeerd.

179 ZZP, MKB en bedrijven. Bron: https://www.digitaltrustcenter.nl/over-het-digital-trust-center
180 Dialogic en TU/e, *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity* in opdracht van WODC, 14 oktober 2020. https://www.rijksoverheid.nl/actueel/nieuws/2021/06/28/meer-mogelijkheden-ncsc-en-dtc-om-dreigings--en-incidentinformatie-te-delen

Inrichting middels Landelijk Dekkend Stelsel

Om de mogelijkheden voor informatiedeling te verbeteren werkt de minister van JenV aan een Landelijk Dekkend Stelsel van samenwerkingsverbanden op het gebied van cybersecurity[181], zodat NCSC informatie mag delen met organisaties die aangewezen worden om deze informatie te mogen ontvangen en doorgeven. Dit levert een stelsel op met een groot aantal organisaties die elk een apart loket vormen voor hun achterban en ook onderling informatie aan elkaar doorgeven. In een dergelijk stelsel treedt vertraging op doordat het tijd kost om uit te zoeken voor welk informatieknooppunt bepaalde informatie relevant is. En bij elke tussenstap kan informatie verloren gaan. Het NCSC als nationale CERT verliest daardoor kostbare tijd, waardoor ze niet in staat is adequaat de overheidsrol binnen de digitale sector te faciliteren. Naast het Landelijk Dekkend Stelsel van schakelorganisaties is het informele circuit, bestaande uit vrijwilligers, ook van belang om de snelheid in de informatiedeling te behouden.

Een andere belemmering is dat niet alle organisaties in Nederland in het Landelijk Dekkend Stelsel worden 'afgedekt' door samenwerkingsverbanden op het gebied van cybersecurity, met name het bedrijfsleven vormt een witte vlek. Daar zitten bedrijven bij die een belangrijke functie vervullen voor vitale aanbieders, of voor andere maatschappelijk belangrijke organisaties die niet onder de definitie vitaal vallen, zoals de voedselsector. Om die reden kondigde de minister van JenV een wetsvoorstel aan waarin onder meer zou worden geregeld dat NCSC via DTC informatie kon delen met het Nederlandse bedrijfsleven ('de rest van de rest').[182] Daarnaast heeft het ministerie van EZK een wetsvoorstel aangekondigd om de wettelijke basis van het DTC te versterken. Op basis daarvan start DTC in het najaar van 2021 een proef om met 40 bedrijven die zich daarvoor aanmelden dreigingsinformatie te delen.[183]

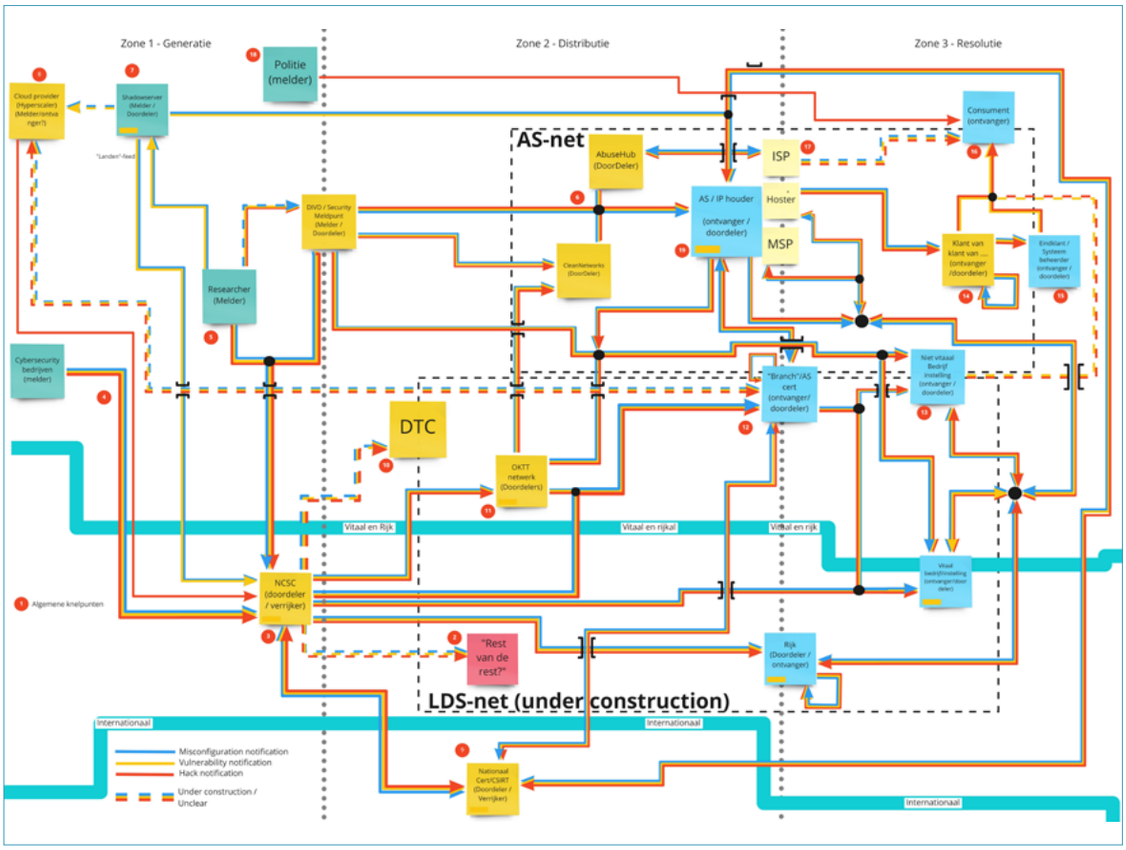
Met deze inspanningen wordt het stelsel meer 'dekkend', maar de informatiedeling blijft versnipperd over een groot aantal schakelorganisaties, die elk capaciteit en expertise moeten inzetten om op een zinvolle manier met de informatie om te kunnen gaan. De volgende figuur die het Anti Abuse Netwerk (AAN) maakte van de wijze waarop dreigingsinformatie tussen organisaties wordt uitgewisseld, maakt duidelijk hoe gecompliceerd de informatiedeling is.[184]

181 NCSC noemt dit schakelorganisaties. https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds

182 https://www.rijksoverheid.nl/actueel/nieuws/2021/06/28/meer-mogelijkheden-ncsc-en-dtc-om-dreigings--en-incidentinformatie-te-delen

183 https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat/nieuws/2021/09/13/digital-trust-center-start-met-actief-informeren-bedrijven-over-digitale-dreigingen

184 Zo bestaat DTC op dit moment uit 20 fte om een achterban van 1,8 miljoen bedrijven te bedienen en heeft DTC geen rechtstreekse relatie met deze bedrijven, alleen via samenwerkingsverbanden (extra schakels in de informatiedeling).



Figuur 18: Metrokaart van de uitwisseling van dreigingsinformatie over organisaties. (Bron: AAN)[185]

Tenslotte hebben belemmeringen om informatie te delen tussen lidstaten en tussen private en publieke entiteiten een negatieve invloed op de effectiviteit van cybersecuritymaatregelen en het beeld van de omvang en ernst van de situatie.[186]

Belemmeringen in het verzamelen van informatie

Een ander vraagstuk is of NCSC en de andere informatieknooppunten zelf informatie mogen vergaren die nodig is om organisaties te helpen de gevolgen te bestrijden. De voorvallen die we in dit onderzoek analyseren tonen dat IP-adressen van kwetsbare servers cruciaal zijn om organisaties te overtuigen van de urgentie om in te grijpen en belangrijke sturingsinformatie is om een beeld te vormen van de situatie en de mate waarin deze onder controle is (zie verder 4.3.2).

Via bepaalde tools op het internet kunnen onderzoekers de buitenkant van digitale systemen scannen en op deze manier in kaart brengen welke servers gebruik maken van een bepaalde versie van bepaalde software. Deze manier van scannen maakt niet zichtbaar of deze servers nog kwetsbaar zijn (of de organisatie de mitigerende maatregel of patch al heeft uitgevoerd). Om dat zichtbaar te maken, wordt doorgaans een scan uitgevoerd, waarmee degene die scant als het ware 'aan de deur voelt' om te kijken of deze op slot zit of geopend kan worden. Dergelijke scans worden in de praktijk veel

185 https://www.abuse.nl/publicaties/metrokaart-december-2020.html
186 European Parliament, *The NIS2 Directive – A high common level of cybersecurity in the EU*, 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

uitgevoerd en in sommige gevallen ook aangeraden door fabrikanten en nationale CERTs.[187]

Binnen NCSC is behoefte om in ieder geval te kunnen scannen om in kaart te brengen op welke servers bepaalde software in gebruik is en bij voorkeur ook of deze servers nog kwetsbaar zijn, om op deze manier gerichter te kunnen waarschuwen en een beter beeld te krijgen van de omvang van de situatie. Juristen binnen NCTV ontraden dit echter vanwege de juridische risico's die ze daarin zien. Zo worden de scantools ook gebruikt door aanvallers en vrezen zij dat het 'aan de deur voelen tot computervredebreuk leidt.[188]

De voorvallen die in hoofdstuk 3 zijn beschreven laten zien dat vrijwillige beveiligingsonderzoekers, onder andere vertegenwoordigd in het DIVD, dit hiaat in de informatievoorziening en incidentbestrijding proberen op te vullen, door te scannen welke organisaties kwetsbare systemen hebben en deze organisaties te waarschuwen. Ook NCSC en andere CERTs maken van hun informatie gebruik. Dit is echter een kwetsbare situatie. Deze beveiligingsonderzoekers doen dit vrijwillig, meestal naast een fulltime baan. Vanwege het grote aantal kwetsbaarheden en aanvallen de laatste tijd heeft dit een enorme belasting opgeleverd voor deze vrijwilligers.[189]

Situatie verschilt per organisatie

De versnippering en witte vlekken in het landschap van informatieknooppunten zorgt er niet alleen voor dat relevante informatie betreffende organisaties niet bereikt, maar ook dat het niet mogelijk is om een consistent beeld te vormen van de omvang en ernst van een voorval. Elke (overheids)organisatie dient zelf een impactanalyse te maken en zelf een afweging te maken of zij adviezen van de informatieknooppunten of samenwerkingsverband waarbij ze zijn aangesloten wel of niet opvolgen en welke acties zij ondernemen. Zowel het uit voorzorg uitzetten als het aan laten staan kan gevolgen hebben voor de digitale veiligheid, maar deze risico's en de perceptie daarvan verschillen per organisatie.

Het gevolg is dat sommige organisaties direct maatregelen nemen bij een incident, en andere dat niet kunnen of niet willen (zie paragraaf 4.2 voor nadere analyse van de afwegingen die organisaties maken). Organisaties bleken in de praktijk meestal niet terug te koppelen hoe ze met de adviezen om zijn gegaan, waardoor bij deze informatieknooppunten een diffuus beeld ontstond van de mate waarin de situatie in Nederland onder controle is. Daar kwam bij dat als een organisatie geen maatregelen neemt, dit niet alleen een risico kan opleveren voor de organisatie zelf, maar ook voor de ketenpartners van deze organisatie (leveranciers en klanten).

187 Zie bijvoorbeeld https://www.us-cert.gov/ncas/alerts/aa20-031a. In het geval van de Citrix-kwetsbaarheid wordt tijdens de scan een niet-bestaand bestand opgevraagd op de Citrix-server op een locatie waar de gebruiker geen toegang toe zou moeten krijgen. Als de Citrix-server antwoordt dat het bestand niet bestaat, is duidelijk dat de kwetsbaarheid nog op de server aanwezig is.

188 Niet-openbare bron: memo's en mailwisseling.

189 Zie bijvoorbeeld deze podcast waarin DIVD-ers vertellen over hun betrokkenheid bij het Kaseya voorval. https://www.cyberhelden.nl/episodes/episode-27/, juli 2021.

De Rijksoverheid streeft er naar dat de informatie die NCSC wel wil delen beter wordt uitgewisseld via het zogenoemde Landelijk Dekkend Stelsel, waarin sectorale organisaties en (groepen) bedrijven ook op vrijwillige basis informatie met elkaar delen die cruciaal is voor het bestrijden van incidenten. Echter als het NCSC als nationaal aanspreekpunt informatie wel ontvangt maar niet volledig deelt, worden ook bij een volledig dekkend stelsel niet alle potentiële slachtoffers gewaarschuwd. Beveiligingsonderzoekers proberen dit hiaat op te vangen, door – op vrijwillige basis – het Nederlandse internetdomein te scannen op kwetsbare servers en deze informatie te delen met partijen die kunnen waarschuwen. Dat is echter een kwetsbare situatie omdat zij hierin niet werden gefaciliteerd: noch door de overheid, noch door andere betrokken partijen, waardoor hun structurele inzet niet is geborgd.[190]

4.3.2 Ontwikkelingen in de incidentbestrijding

Wat de voorvallen tonen is dat goede samenwerking tussen overheid en organisaties is cruciaal is om incidenten te bestrijden. En om ze te voorkomen (zie paragraaf 4.1 en 4.2). Onderling vertrouwen is cruciaal om dit tot stand te brengen, evenals een consistente nationale aanpak.[191]

In een aantal andere landen zijn het cybersecuritystelsel en de incidentbestrijding centraal ingericht, ook in Nederland klinkt de roep om meer centrale aansturing. In Nederland is gekozen voor decentrale aansturing in de incidentbestrijding. Decentrale aansturing zou passen bij de Nederlandse cultuur. Centrale aansturing van cybersecurity en incidentbestrijding in andere landen (zie kader) gaat vaak gepaard met regie vanuit inlichtingendiensten. In Nederland zou centrale aansturing daarom weerstand kunnen oproepen.[192]

190 Inmiddels is deze situatie veranderd: eind september 2021 kondigde het bedrijfsleven aan om zelf een waarschuwingssysteem op te zetten. Bron: *FD*, Bedrijfsleven start eigen alarmsysteem tegen hackers: 'overheid te traag', 28 september 2021.

191 Atkins, S. en C. Lawson, An Improvised Patchwork: Success and Failure in *Cybersecurity Policy for Critical Infrastructure. Public Administration Review*, Vol. 81, Iss. 5, pp. 847–861, 2020.

192 Zie onder andere: Rand, *Cybersecurity A State-of-the-art Review Phase 2: Final Report*, 2020. NSOB, *Actuele kwestie, klassieke afweging. Een verkenning naar de governance van het Nederlands digitaliseringsbeleid*, 2021.

Incidentbestrijding in andere landen

Het Britse NCSC is de centrale organisatie voor cybersecurity in het Verenigd Koninkrijk. Naast het bestrijden van incidenten zijn zij ook een expertisecentrum en helpen zij om de digitale weerbaarheid van zowel overheid als bedrijfsleven te vergroten. Dit NCSC valt onder de Britse inlichtingendienst GCHQ en heeft daardoor toegang tot hoogstaande expertise en inlichtingen. Het cybersecurity beleid wordt gemaakt door de *Cabinet Office*, dus op het niveau van de regering (departement overstijgend). In Frankrijk lijkt het GIP ACYMA (vergelijkbaar met DTC) goed te zijn om kleine bedrijven te bereiken door ze te koppelen aan private IT experts. En in Duitsland is de incidentbestrijding net als in Nederland versplinterd, onder meer vanwege het federale bestuurssysteem.[193]

Het Amerikaanse *Cybersecurity and Infrastructure Security Agency* (CISA) is net als het Britse NCSC zowel gericht op incidentbestrijding als verbetering van de weerbaarheid voor alle overheidsorganisaties en bedrijven in de VS. Ze werken nauw samen met de private sector en brengen regelmatig adviezen uit in samenwerking met de NSA en FBI.[194]

Naar aanleiding van evaluaties en kamerbrieven die over de voorvallen zijn verschenen, zijn en worden maatregelen genomen om de incidentbestrijding te verbeteren, zoals het wetsvoorstel van de minister van JenV dat mogelijk moet maken om meer informatie te delen met partijen die niet tot de doelgroep van Rijk en vitaal behoren. Ook worden gemeenten aangesloten op het Nationale Detectie Netwerk, dat voorheen, met in achtneming van de Wbni, was voorbehouden aan rijk en vitaal. Hieruit blijkt dat de rijksoverheid dit onderscheid weliswaar wettelijk nog handhaaft, maar in de praktijk langzaamaan loslaat. Daarbij blijft de informatiedeling echter plaatsvinden binnen de kaders van de decentrale aansturing. Uit de analyse van de voorvallen blijkt dat als sprake is van een kwetsbaarheid die wereldwijd wordt aangevallen, de tijd om te reageren beperkt is tot enkele dagen of helemaal geen (*zero day*). Decentrale aansturing leidt tot verlies van tijd en informatie, waardoor organisaties niet tijdig worden geïnformeerd dat zij gevaar lopen.

Een andere ontwikkeling die uit de analyse van de voorvallen blijkt, is dat vanuit de Rijksoverheid (JenV, BZK) politiek-bestuurlijk behoefte is gebleken om te kunnen verantwoorden dat alle relevante organisaties in Nederland de adviezen van NCSC opvolgen. Daarbij gaat het niet alleen om organisaties die vallen onder het mandaat van NCSC, maar ook organisaties daarbuiten zoals gemeenten, provincies en zorginstellingen. Hieruit kan worden afgeleid dat er behoefte is aan centrale sturing, die nu niet bestaat. Omgekeerd voelden deze organisaties door het ongerichte advies van NCSC en de soms directe contacten vanuit het rijk druk om adviezen op te volgen, terwijl er formeel geen sturings- en verantwoordingsrelatie bestaat met het Rijk. Deze organisaties hebben eigen gremia die hen aanstuurt en waaraan ze verantwoording afleggen.

193 Dialogic en TU/e, *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity* in opdracht van WODC, 14 oktober 2020.
194 https://www.cisa.gov/

4.4 Leren van digitale voorvallen

Om de veiligheid te kunnen verbeteren is het belangrijk om te onderzoeken wat er gebeurde en welke factoren bijdroegen aan het ontstaan en de gevolgen van het voorval. Deze inzichten zijn belangrijk om toekomstige voorvallen te voorkomen of de gevolgen daarvan te beperken, in het bijzonder in een domein dat zo dynamisch is als digitale veiligheid.

In veel domeinen zijn grote voorvallen en publieke ophef een prikkel om te leren en de veiligheid te verbeteren. In Nederland wordt al meer dan honderd jaar onderzoek gedaan naar ongevallen en rampen, aanvankelijk alleen op transportgebied. Na de vuurwerkramp in Enschede en de cafébrand in Volendam werd in 2005 de Onderzoeksraad voor Veiligheid opgericht, omdat er behoefte was aan een permanent onderzoeksinstituut dat naast transport ook voorvallen in andere domeinen kon onderzoeken.[195] In de transportdomeinen kent dit onderzoek wereldwijd een lange traditie. Zo leidde een vliegtuigcrash met een populaire *football coach* in de VS in 1931 uiteindelijk tot de oprichting van de NTSB (Amerikaanse tegenhanger van de Onderzoeksraad voor Veiligheid).[196]

Het digitale domein is een relatief jong domein en de traditie om van voorvallen te leren is in dit domein beperkt en nog in opbouw. In deze paragraaf beschrijven we:

- hoe digitale voorvallen op dit moment worden gemeld en onderzocht;
- welke factoren beïnvloeden hoe van digitale voorvallen wordt geleerd. Daarbij gaat het zowel om keuzes en veronderstellingen die onderzoekers maken en hebben, als om de context waarbinnen de onderzoeken plaatsvinden.

4.4.1 De huidige praktijk van onderzoek naar digitale voorvallen

Er kunnen verschillende aanleidingen zijn om een voorval te onderzoeken. Allereerst vanuit de eigen behoefte van de betrokken organisatie, of dit nu de fabrikant van de software is of de organisatie die de software gebruikt: vanuit een intrinsieke behoefte om te leren en zo toekomstige voorvallen te voorkomen, niet alleen bij de organisatie zelf maar ook bij anderen. Daarnaast bestaan er verschillende wettelijke verplichtingen, die maken dat bepaalde voorvallen aan bepaalde instanties moeten worden gemeld (alhoewel gerapporteerde voorvallen dan niet altijd worden onderzocht). Partijen zoals politie en verzekeraars doen forensisch onderzoek naar voorvallen. Hierna gaan we in op wat we op dit moment in de praktijk waarnemen voor wat betreft het melden en onderzoeken van digitale voorvallen.

195 https://www.onderzoeksraad.nl/nl/page/12056/geschiedenis
196 Anderson, R., *Security Engineering*, 2020.

Melding en onderzoek op basis van wettelijke verplichting

Incidenten bij vitale aanbieders

De Europese *Network and Information Security* (NIS) *Directive*[197] bevat verplichtingen voor aanbieders van essentiële diensten in vitale sectoren en digitale dienstverleners. Nederland heeft de NIS geïmplementeerd in de Wet beveiliging netwerk- en informatiediensten (Wbni). Op grond van de Wbni moeten aanbieders van essentiële diensten ernstige incidenten melden bij het NCSC/sectorale CSIRT en hun sectorale toezichthouder. Voor energie en digitale infrastructuur is dit Agentschap Telecom, voor banken en betaalinfrastructuur DNB, vervoer en drinkwater ILT en gezondheidszorg IGJ.[198] Voor de telecomsector bestaat sinds 2012 een zorg- en meldplicht inclusief toezicht van AT op basis van de Telecommunicatiewet, ongeacht of een partij door EZK als vitaal is aangewezen. In de Wbni is aanvullend op deze sectorale wet- en regelgeving een meldplicht bij het NCSC opgenomen alleen voor de vitaal aangewezen telecompartijen.

Het betreffende vakdepartement stelt in samenspraak[199] met JenV drempelwaarden waarboven het incident moet worden gemeld. In de Wbni is bepaald dat als publieke bewustwording nodig is om een incident te voorkomen of te beheersen, de betreffende autoriteit het publiek kan informeren over het gemelde incident. Ook kan de autoriteit de vitale aanbieder verzoeken om zelf het publiek te informeren.[200]

Voor het leren is ook van belang dat andere organisaties de voor hen relevante lessen uit de onderzoeken eenvoudig tot zich kunnen nemen en op die manier kunnen leren van wat andere organisaties is overkomen. Incidenteel worden onderzoeken naar aanleiding van meldingen gepubliceerd op de website van de betreffende autoriteit of toezichthouder. Een voorbeeld hiervan zijn de onderzoeken van AT, JenV en IGJ naar de uitval van 112[201] en het onderzoek van ILT naar de cybersecurity bij Waternet naar aanleiding van een signaal in de media dat dit niet op orde zou zijn.[202] We hebben op de websites van NCSC, AT en andere sectorale toezichthouders geen overzicht kunnen vinden welke incidenten zijn onderzocht, of een geaggregeerd overzicht van het aantal incidenten, de factoren die tot de incidenten hebben geleid en de verschillende lessen die daaruit volgden. In theorie is het mogelijk dat de lessen uit incidenten impliciet zijn verwerkt in de adviezen en voorlichting van deze organisaties aan hun doelgroep. In de praktijk zijn toezichthouders op dit moment nog intern bezig met de vraag hoe zij hun

197 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32016L1148&from=EN Krachtens de Wbni zijn als aanbieders van essentiële diensten aangewezen: als vitale aanbieder aangemerkte entiteiten die actief zijn in sectoren, genoemd in de bijlage bij de NIB-richtlijn (zie artikel 2 Bbni). Voor enkele categorieën andere vitale aanbieders geldt, los hiervan, ook een meldplicht bij het NCSC voor ernstige incidenten (zie artikel 3 Bbni), maar voor hen gelden niet de andere, uit de NIB-richtlijn voortvloeiende verplichtingen. Daarnaast: aanbieders van essentiële diensten dienen krachtens artikel 10 Wbni ernstige incidenten bij het NCSC en de sectorale toezichthouder te melden, maar niet ook (of in plaats daarvan) bij een "sectorale CSIRT". Overigens: voor entiteiten binnen de gezondheidszorg is wel al (in artikel 4 Wbni) de toezichthouder bepaald, maar binnen die sector zijn vooralsnog geen aanbieders van essentiële diensten aangewezen (waarop de verplichtingen vanuit de NIB-richtlijn van toepassing zouden zijn).

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

199 Vanwege de vaak dubbele meldplicht aan zowel het vakdepartement als JenV (NCSC)

200 Artikel 23 Wbni artikel 20, lid 4, onder b, Wbni. Zie ook https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/publicaties/2020/januari/20/brochure-meldplicht-voor-aanbieders-van-essentiele-diensten/Brochure+Meldplicht+voor+aanbieders+van+essentiële+diensten.pdf

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

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

eigen verantwoordelijkheid kunnen en moeten invullen. Zo schrijven toezichthouders in hun eerste gezamenlijke inspectiebeeld dat het toezicht nog in een opbouwende fase is en zij nog niet in staat zijn om samenhangende uitspraken te doen (rode draden te trekken) over hoe het op dit moment gaat met cybersecurity in vitale sectoren en processen.[203]

Onderzoek naar datalekken
Organisaties waarvan persoonsgegevens zijn gelekt zijn wettelijk verplicht om dit direct te melden aan de Autoriteit Persoonsgegevens (AP). Bij datalekken gaat het om 'toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie'.[204] De wettelijke plicht om datalekken te melden komt voort uit de Europese Algemene Verordening voor Gegevensbescherming (AVG) in de EU (in het Engels *General Data Protection Regulation* of GDPR). Omdat de AVG een verordening is, is deze Europese rechtsregel rechtstreeks van toepassing in de hele Europese Unie.

AP publiceert onderzoeks- en boeterapporten naar aanleiding van meldingen van datalekken en andere signalen.[205] De onderzoeken van AP zijn gericht op de mate waarin organisaties wettelijke verplichtingen hebben nageleefd, zoals het nemen van technische en organisatorische maatregelen om datalekken te voorkomen en het evalueren van datalekken. Wanneer een organisatie de wettelijke maatregelen niet heeft nageleefd kan AP een boete opleggen. Om deze reden zijn organisaties terughoudend in het melden van mogelijke datalekken. Het niet naleven van de wettelijke meldplicht kan echter ook leiden tot extra boetes, ongeacht de omvang van het oorspronkelijke datalek.

Een andere beperking is dat het bij de meldingen moet gaan om het lekken van persoonsgegevens en dat is slechts bij een deel van de voorvallen aan de orde. Verder gaan de onderzoeken van AP vooral in op het voldoen aan wet- en regelgeving. Om te kunnen leren is vooral de achterliggende vraag van het niet-naleven relevant: welke factoren er mogelijk toe hebben geleid dat organisaties de verplichtingen niet hebben nageleefd en wat kan daarvan worden geleerd?

AP publiceert jaarlijks een jaarverslag. In het jaarverslag over 2020 staat dat meeste van de in 2020 gemelde datalekken het gevolg zijn van het verkeerd versturen of afgeven van persoonsgegevens (66%). AP meldt dat bij 5% van de in 2020 gemelde datalekken een digitaal incident (*hacken, malware, phishing*) de oorzaak was en dat dit aandeel stijgt. In de rapportage gaat AP dieper in op de bijdrage die meerfactorauthenticatie (MFA) had kunnen hebben in het voorkomen en mitigeren van 249 datalekken, waarbij naar schatting minimaal 607.846 en maximaal 2.092.946 personen betrokken waren.[206]

Verdere inzichten biedt het AP op dit moment niet aan organisaties die software gebruiken. Om meer inzichten uit de datalekmeldingen te kunnen halen, en daarmee potentiele lessen voor andere organisaties, diende de Cyber Security Raad (CSR) in 2020 een onderzoeksvoorstel in bij de minister van Justitie en Veiligheid. Doel van dit

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

onderzoek is om te laten zien in hoeverre wetenschappelijk en/of statistisch onderzoek van datalekken het inzicht in de effectiviteit van veiligheidsmaatregelen (of het ontbreken daarvan) kan vergroten.[207]

Forensische onderzoeken

Er zijn verschillende organisaties die achteraf incidenten onderzoeken. Sommige van deze organisaties zijn erkend als digitaal forensisch opsporingsbureau. Deze erkenning betekent dat hun rapporten kunnen worden geaccepteerd als forensische onderbouwing in een rechtszaak. Forensische onderbouwing is primair gericht op het onderbouwen van juridische aansprakelijkheid, niet op het leren van het voorval om herhaling in de toekomst te voorkomen. In de meeste gevallen werken deze digitaal forensische opsporingsbureaus in opdracht van de getroffen organisatie en/of hun verzekeraar. Deze onderzoeken blijven doorgaans vertrouwelijk binnen de eigen organisatie (tenzij de opdrachtgever het uit eigen beweging publiceert, zie volgende paragraaf). Andere organisaties krijgen daardoor geen inzicht in de getrokken lessen en ze dragen niet bij aan een geaggregeerd beeld van factoren en effectiviteit van maatregelen; hooguit binnen een betrokken verzekeraar (silo's tussen verzekeraars).

Daarnaast wordt forensisch onderzoek gedaan door de politie (waaronder het *Team HighTech Crime* en regionale *cybercrimeteams*) en door het NFI. Voor deze organisaties geldt in grote lijnen hetzelfde als voor de opsporingsbureaus voor wat betreft de mogelijkheid om van hun onderzoeken te kunnen leren. Als er een rechtszaak is, kan het zijn dat een deel van deze informatie via media en de gerechtelijke uitspraak openbaar bekend wordt. De informatie is echter niet voor organisaties doorzoekbaar zoals bijvoorbeeld wel het geval is bij verkeersongevallen die worden geregistreerd in een verkeersongevallenregistratie die onder meer wordt gebruikt voor wetenschappelijk onderzoek (onder andere door SWOV) en voor beleidsondersteuning.

Uit eigen beweging onderzoek doen en publiceren

Een aantal organisaties heeft ervoor gekozen om in het publiek belang en ter verantwoording aan zijn eigen achterban (burgers, studenten) de resultaten van forensische of andere onderzoeken, openbaar te maken.

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

Onderzoek naar cyberongevallen in de openbaarheid
In juni 2019 informeerde de politie de gemeente Lochem dat aanvallers het digitale systeem van de gemeente mogelijk was binnengedrongen. Sindsdien ziet de burgemeester van Lochem voor zichzelf een missie om gemeenten en andere overheden te waarschuwen voor dit risico en het belang van digitale weerbaarheid te onderstrepen.[208]

Op 23 december 2019 werd de Universiteit Maastricht getroffen door een cyberaanval. De universiteit liet het voorval onderzoeken en hield medewerkers en studenten op de hoogte van de gebeurtenissen. Tijdens een symposium op 5 februari 2020 presenteerden zij de resultaten en legde de universiteit uit hoe het ongeval kon gebeuren en welke lessen ze eruit trokken.[209] Ook de Onderwijsinspectie onderzocht het ongeval.[210]

In december 2020 werd de gemeente Hof van Twente binnengedrongen. Het gevolg was dat de gemeente zijn dienstverlening aan inwoners een aantal weken (paspoorten, rijbewijzen en uittreksels) tot maanden (gemeentelijke belasting) moest stilleggen, konden facturen niet worden betaald en kon de gemeente niet veilig samenwerken met andere organisaties. Ook moest de gemeente zijn digitale systeem opnieuw opbouwen. Net als de Universiteit Maastricht hield de gemeente Hof van Twente haar inwoners op de hoogte met regelmatige updates. Ook liet zij het voorval onderzoeken en publiceerde de resultaten daarvan aan het publiek.[211]

In februari 2021 werden de Universiteit Amsterdam en de Hogeschool van Amsterdam getroffen door een cyberaanval. Ook zij lieten het voorval onderzoeken en publiceerden daarvan de resultaten.[212]

De traditie om van voorvallen te leren is in het digitale domein nog in ontwikkeling. Voorvallen moeten worden gemeld, maar worden niet systematisch onderzocht. Een "infrastructuur" voor gezamenlijk leren door fabrikanten, organisaties die software gebruiken en andere relevante publieke en private partijen ontbreekt.

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

4.4.2 Belemmeringen om van (onderzoeken naar) digitale voorvallen te leren

In de vorige paragraaf werden de verschillende manieren beschreven waarop op dit moment digitale voorvallen worden gemeld en onderzocht. En op welke manier de resultaten van deze meldingen en onderzoeken worden gebruikt om organisaties meer inzicht te geven in wat zij kunnen doen om toekomstige voorvallen te voorkomen. Over het geheel genomen laat de huidige werkwijze zien dat het leren van digitale ongevallen door een aantal factoren wordt belemmerd.

Melden en in de openbaarheid komen

De gemeenten Lochem en Hof van Twente, evenals onderwijsinstellingen Universiteit Maastricht en Universiteit van Amsterdam/Hogeschool van Amsterdam kunnen worden gezien als uitzonderingen op de regel dat organisaties niet geneigd zijn om in het openbaar te delen dat zij een digitaal voorval hebben meegemaakt en wat zij daarvan hebben geleerd. In de gesprekken die de Onderzoeksraad heeft gevoerd met verschillende organisaties en met partijen die deze organisaties bijstaan, worden meerdere redenen genoemd, waarvan er hier drie worden besproken.

Ten eerste is dat angst voor reputatieschade en afnemend vertrouwen van partijen waar de organisatie mee samenwerkt. Een digitaal voorval zoals een *ransomware* aanval kan in de buitenwereld worden gezien als een teken dat de organisatie de informatiebeveiliging niet op orde heeft. Dit kan ervoor zorgen dat het vertrouwen in de betreffende organisatie afneemt. Dit effect is moeilijk meetbaar. Tot nu toe zijn er geen signalen dat datalekken per definitie leiden tot een waardedaling van het bedrijf. Daarnaast zijn er in andere domeinen zoals de voedselsector aanwijzingen dat organisaties juist het vertrouwen kunnen behouden of versterken als zij vrijwillig naar buiten komen met een veiligheidsprobleem en dit ook daadkrachtig aanpakken.[213] Een ander psychologisch effect is schaamte. Bij cybervoorvallen is dit effect sterker dan bij andere voorvallen zoals een auto-ongeluk. Dat komt onder meer doordat betrokkenen bij een cyberaanval zoals een *ransomware* aanval het gevoel hebben opgelicht te zijn, ergens ingetuind te zijn en gefaald te hebben. Naast verlies van een gevoel van veiligheid leidt dit ook tot een verlies van status.[214]

Een tweede belemmering om met een voorval naar buiten te komen, is dat dit juridische consequenties kan hebben. Als het digitale voorval gepaard is gegaan met het overtreden van wettelijke regels (bijvoorbeeld als er data is gelekt of een zorgplicht niet is nagekomen), dan kunnen toezichthouders handhavend optreden. Andere partijen (consumenten, afnemers, leveranciers, aandeelhouders) kunnen zich aangetast voelen in hun rechten en de organisatie daarvoor aansprakelijk stellen. Zo heeft één van de software fabrikanten die we spraken lessen uit het voorval getrokken, maatregelen genomen en die gedeeld via hun website, maar deze lessen niet actief gedeeld met andere fabrikanten andere betrokken organisaties of het publiek. Als de software industrie onderling en publiekelijk gesloten blijft over hoe fouten ontstaan kan er geen gezamenlijk leerproces plaatsvinden.[215]

213 Zie bijvoorbeeld https://doi.org/10.15728/bbr.2017.14.2.4
214 Goffman, E., On Cooling the Mark Out, 1952, *Psychiatry*, 15:4, 451-463, DOI: 10.1080/00332747.1952.11022896.
215 Zie ook Tjong Tjin Tai, E., en Knoops, B., *Zorplichten tegen cybercrime* (NJb), 2015.

Als derde belemmering wordt genoemd dat de organisatie vreest dat het risico op aanvallen toeneemt zodra bekend wordt dat de organisatie al een keer (succesvol) is aangevallen.

De wijze waarop digitale voorvallen worden onderzocht

Een beletsel voor het leren die samenhangt met de vorige belemmeringen is hoe er in de rapporten wordt geschreven over de factoren die bijdroegen aan het ontstaan van het voorval. Zoals we hiervoor schreven is reputatieschade een reden om voorvallen niet te melden. Schaamte (zelfstigma) speelt daarbij ook een rol. Evaluaties die opsommen welke fouten een organisatie heeft gemaakt, zonder daarbij te onderzoeken hoe het begrijpelijk kan zijn voor een organisatie dat hij zich in deze situatie bevond, kunnen dit (zelf)stigma vergroten en dragen niet bij aan de bereidheid van organisaties om naar buiten te treden met wat ze hebben meegemaakt, zodat anderen ervan kunnen leren.

Veel van de evaluaties zijn gericht op wat de organisatie in kwestie zelf zou moeten doen, en gaan niet in op de systeemvraag die wegkomt achter de vraag hoe het komt dat het voor organisaties moeilijk is om te voorkomen dat ze worden aangevallen en om aanvallen succesvol te kunnen weerstaan. In de evaluaties ligt de focus op *security* (beveiliging) en minder op het inrichten van een veilig digitaal systeem dat weerstand kan bieden tegen allerlei mogelijke bedreigingen.

Willen begrijpen hoe dingen konden gebeuren is cruciaal bij alle onderzoeken naar voorvallen, ook bij het voorliggende onderzoek. Om van ongevallen te leren is dan ook van belang hoe het ongevalsonderzoek is ingericht: dat het ongevalsonderzoek erop is gericht om het ongeval te kunnen verklaren. Daarvoor moet het onderzoek verder gaan dan toetsen aan normen en standaarden (eerste orde leren), het moet ook reflecteren op gehanteerde uitgangspunten (tweede orde leren). Zeker in een domein waar het leren van voorvallen in ontwikkeling is, is belangrijk om ook te reflecteren op de wijze waarop we leren (derde leren of deuteroleren). De meeste evaluaties die de Onderzoeksraad bekeek waren beperkt tot eerste orde leren. De evaluaties bestonden voornamelijk uit constateringen dat de betreffende organisatie niet alle voorgeschreven of verwachte basismaatregelen had geïmplementeerd en dat dit factoren waren die tot het voorval hadden geleid. Of er waren evaluaties die weliswaar de aanpak en het beleid analyseren, maar waaruit niet duidelijk werd welke factoren bijdroegen aan het ontstaan van het voorval.

De evaluatie van de Onderwijsinspectie van de *ransomware* aanval op de Universiteit Maastricht laat zien dat een reflectieve insteek van een voorvalonderzoek mogelijk en zinvol is. Zo is in dat onderzoek gezocht naar een verklaring voor het feit dat de informatiebeveiliging niet aan de beschikbare normen en standaarden voldeed. Eén van deze verklaringen was dat het op universiteiten en hogescholen vanwege de bestuurlijke gelaagdheid moeilijk is voor het bestuur om zicht te hebben op de staat van de informatiebeveiliging. Dit inzicht is van belang, omdat een dergelijke bestuurlijke gelaagdheid bij alle universiteiten en hogescholen aanwezig is en mogelijk bij meer hoger onderwijsinstellingen het zicht van het bestuur op de informatiebeveiliging belemmert.

Het verspreiden van inzichten naar degenen die deze inzichten nodig hebben
In de voorgaande subparagraaf worden verschillende soorten onderzoeken naar voorvallen benoemd. De informatie die deze onderzoeken oplevert wordt in een beperkt aantal gevallen openbaar gemaakt: wanneer de organisatie daar bij uitzondering voor kiest of daartoe wordt bewogen door de toezichthouder. In de vorige subparagraaf worden als voorbeeld de universiteit van Maastricht, Universiteit/Hogeschool van Amsterdam, gemeente Lochem en gemeente Hof van Twente genoemd. Ook wordt beschreven dat de meeste onderzoeken naar voorvallen niet worden gepubliceerd, of alleen in besloten kring. Vaak is de informatie alleen begrijpelijk voor een beperkte kring van experts en lijkt het een abstracte technische gebeurtenis. Daarom is het belangrijk om bij het delen van inzichten uit cyberaanvallen, deze te demystificeren en de menselijke gevolgen ervan te benadrukken.[216]

Ook is er nog geen entiteit die informatie uit onderzoeken en meldingen verzamelt ten behoeve van wetenschappelijk en/of statistisch onderzoek. In het cyberdomein, dat een relatief nieuwe traditie heeft als het gaat om incidentenonderzoek, is behoefte aan een platform waar kennis wordt gedeeld, vastgehouden en waar organisaties op zoek kunnen naar relevante inzichten om hun informatiebeveiligingsbeleid beter te kunnen onderbouwen (*historic capture*). Overigens sluit dit aan bij de missie van het NCSC als Nationaal Cyber Security Centrum: begrijpen en duiden wat er gebeurt, het verbinden van partijen, kennis en ervaring met als doel om herhaling te voorkomen.[217]

In de huidige praktijk komen veel organisaties er niet voor uit dat ze zijn aangevallen. De onderzoeken bieden niet de verklaringen die nodig zijn om het systeem te verbeteren. Betrokken organisaties verspreiden lessen uit voorvallen meestal niet buiten de eigen organisatie of gemeenschap.

4.5 Beleid en internationale context

Op Europees niveau is er verschillende regelgeving op het gebied van cybersecurity, en zijn ook een aantal initiatieven in ontwikkeling. Deze regelgeving en initiatieven hebben ieder een verschillend doel en doelgroep. In de tabel hieronder zijn enkele kenmerken van de regelgeving opgenomen.

216 Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat*. 2020. https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm
217 https://www.ncsc.nl/over-ncsc, geraadpleegd op 13 september 2021.

Naam wetgeving	Soort wetgeving	Status	Inhoud
NIS *directive*/ NIB richtlijn	Richtlijn[218]	Dient vanaf 10 mei 2018 geïmplementeerd te zijn bij lidstaten.[219]	• Doelgroep: digitale dienstverleners en aangewezen aanbieders van essentiële diensten. • Samenwerking tussen lidstaten op het gebied van cybersecurity. • Stelt verplichtingen aan doelgroep om beveiligingseisen te implementeren en incidenten te melden.
NIS 2 *directive*	Richtlijn	Ontwerprichtlijn.	• Doelgroep: uitgebreid ten opzichte van de NIS met o.a. de voedselsector, openbaar bestuur, fabrikanten van kritische producten. • Verscherpte beveiligingseisen voor organisaties en versterking van Europese samenwerking.
Cyber Security Act	Verordening[220]	In werking sinds 27 juni 2019.	• Doelgroep: gehele Europese digitale markt. • Vergroot het mandaat van ENISA. • Introductie van cybersecurity certificeringskader (nog in ontwikkeling).
Digital Operational Resilience Act (DORA)	Verordening	Ontwerpverordening, naar verwachting eind 2022 in werking.	• Doelgroep: financiële sector. • Doel: harmoniseren regels digitale weerbaarheid in de EU. • Basiskader voor financiële organisaties, stelt basiseisen aan financiële organisaties o.a. op het gebied van risicomanagement en digitale incidenten.
Horizontale regulering software	Onbekend	Nog in ontwikkeling.	• Doelgroep: softwarefabrikanten.[221] • Horizontale wetgeving met betrekking tot cybersecurity eisen voor softwareproducten.

Daarnaast is er ook regelgeving (in ontwikkeling) op het gebied van *Internet of Things* (IoT), oftewel software die is opgenomen in producten. Dit betreft onder andere het voornemen om cybersecurityeisen te stellen aan draadloos verbonden apparaten via de *Radio Equipment Directive* en de regulering van apparaten die met elkaar communiceren via internet (*connected devices*) in de *Cybersecurity Resilience Act*. Daarnaast zijn er in 2017 een aantal EU verordeningen aangenomen waarbij cybersecurityeisen worden gesteld aan medische apparaten, en zullen er op VN niveau ook cybersecurityeisen worden opgenomen in regulering voor de auto-industrie. Op het gebied van productveiligheid wordt de algemene EU richtlijn voor productveiligheid herzien. Deze herziene richtlijn regelt onder andere de productveiligheid van producten met digitale

218 Een richtlijn moet door lidstaten geïmplementeerd worden in nationale wetgeving.
219 In Nederland is dit vastgelegd in de WBNI.
220 Een verordening is wetgeving direct van toepassing in alle EU lidstaten.
221 Het is nog niet duidelijk voor welke specifieke doelgroep deze wetgeving ontwikkeld wordt.

componenten. Ook op het gebied van consumentenrecht en IoT zijn er Europese ontwikkelingen waarin onder andere zaken rondom het recht op updates zijn opgenomen. Het tegengaan van kwetsbaarheden in software, evenals het opsporen van strafbare feiten ten behoeve van handhaving en vervolging als ook de afspraken over hoe staten onderling met elkaar omgaan als het gaat om cyberaanvallen, vragen om internationale samenwerking.[222]

De handel in software is een internationale markt in vraag en aanbod. Fabrikanten en afnemers bevinden zich over de hele wereld. Zoals in paragraaf 4.1 is beschreven, wordt software als product en de totstandkoming ervan tijdens de levensduur als proces op dit moment alleen gereguleerd vanuit wet- en regelgeving die van toepassing is op de domeinen waarbinnen software wordt toegepast, zoals software in voertuigen en software in zorginstellingen. Op software zelf is geen product- of procesregulering vanuit de overheid van toepassing. Wel zijn er industrienormen, waartegen een fabrikant zijn software of zijn processen kan certificeren, om daar tegenover afnemers bijvoorbeeld verantwoording over te kunnen afleggen.

Ook de actoren die kwetsbaarheden in software misbruiken om de digitale systemen van organisaties aan te vallen komen overal vandaan. Het gaat daarbij zowel om criminele actoren als om actoren die werken voor natiestaten en combinaties of tussenvormen van beide. Zo worden *ransomware* aanvallen vaak uitgevoerd door criminele organisaties, maar kunnen ze ook een dekmantel zijn voor een actie van een inlichtingendienst of een manier zijn voor een land om inkomsten te verkrijgen. Internationale samenwerking is gecompliceerd mede doordat landen niet alleen slachtoffer zijn van onveiligheid door cyberaanvallen, maar ook baat hebben bij kwetsbaarheden in software voor hun eigen activiteiten.[223] Daarnaast belemmeren ideologische verschillen tussen landen internationale samenwerking, bijvoorbeeld over hoe de staat zich verhoudt tot het internet en welke afschrikwekkende acties tegen aanvallers (*deterrence*) toelaatbaar zijn.[224]

Desondanks hebben de lidstaten van Europese Unie de afgelopen jaren echter laten zien in staat te zijn door samen te werken strenge eisen over gegevensbescherming en buitenlandse investeringen te kunnen afdwingen. Ook roepen landen elkaar vaker (in de openbaarheid) tot verantwoording na grootscheepse cyberaanvallen.

222 Zie onder andere Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat.* 2020. https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm
223 Perlroth, N. *This is how they tell me the world ends: the cyberweapons arms race*, 2021.
224 Henriksen, A. The end of the road for the UN GGE process: The future regulation of cyberspace, *Journal of Cybersecurity*, Volume 5, Issue 1, 2019. Fischerkeller, M.P. en R.J. Harknett, Deterrence is Not a Credible Strategy for Cyberspace. *Orbis,* Volume 61, Issue 3, 2017, Pages 381-393, 2017. Daniel, M., Closing the Gap: Expanding Cyber Deterrence. *Cyberstability Paper Series*, 2021.

Multistakeholder groepen leveren een bijdrage aan het verbeteren van de internationale samenwerking. Zo werkte de *Global Commision on the Stability of Cyberspace* aan voorstellen voor normen en beleid die de internationale cybersecurity en stabiliteit verbeteren. Daarbij gaat het om normen voor verantwoord gedrag van zowel staten als niet-statelijke actoren in *cyberspace*. In deze commissie is een groot aantal stakeholders betrokken uit verschillende landen en vanuit verschillende soorten organisaties, zoals overheden, universiteiten en fabrikanten. Zij kwamen tot acht normen, waaronder de volgende:[225]

- Niet-statelijke actoren mogen geen cyberaanvallen uitvoeren en staten moeten dit voorkomen en erop reageren als dit wel gebeurt;
- Staten moeten kwetsbaarheden waar zij kennis van hebben in principe melden aan de fabrikant en een transparant raamwerk hanteren voor wanneer ze besluiten om dat niet te doen;
- Fabrikanten van producten en diensten moeten cybersecurity en stabiliteit prioriteit geven en alles doen wat redelijkerwijs mogelijk is om er zeker van te zijn dat deze geen kwetsbaarheden bevatten. Ook moeten zij maatregelen nemen om kwetsbaarheden die bekend worden te mitigeren en daar transparant over zijn. Alle actoren hebben een plicht om informatie over kwetsbaarheden te delen om zo cyberaanvallen te voorkomen en de gevolgen ervan te beperken;
- Landen moeten maatregelen nemen, waaronder wet- en regelgeving, zodat de basis cyberhygiëne op orde is.

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

5 CONCLUSIES

Dit onderzoek begon met de vraag welke lessen te trekken zijn 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 en andere, vergelijkbare voorvallen in softwareproducten van andere fabrikanten. De rode draad uit de voorvallen is dat organisaties en de mensen die daarvan afhankelijk zijn, worden blootgesteld aan digitale onveiligheid doordat zij kwetsbare software gebruiken. De voorvallen illustreren stuk voor stuk dat waarschuwingen hen in veel gevallen niet bereiken.

Onze analyse op systeemniveau toont dat de veiligheid van software en de bestrijding van de gevolgen van onveiligheid tot stand komen in een netwerk van partijen die elk hun eigen verantwoordelijkheid hebben. Géén van allen kunnen echter afzonderlijk de veiligheid borgen. Borging van de veiligheid is alleen mogelijk wanneer verantwoordelijke partijen met elkaar samenwerken. Voor deze samenwerking zijn effectieve structuren nodig en dient onderling vertrouwen versterkt. Hierna lichten we toe welke belemmeringen er zijn.

5.1 Kwetsbaarheden in software voorkomen en opsporen tijdens ontwikkeling en gebruik

Verschillende factoren dragen bij aan het ontstaan van kwetsbaarheden tijdens de levenscyclus van een product. Vaak wordt doorgebouwd aan een bestaand product, daardoor wordt software steeds complexer. Ook kan de gebruikte programmeertaal bijdragen aan het ontstaan van fouten en het gebruik van bestaande componenten en (inconsistente) lagen in de architectuur kwetsbaarheden introduceren.

Als (veiligheids)problemen gekoppeld zijn aan fundamentele keuzes in het product kan dat een belemmering vormen voor de fabrikant om het probleem bij de wortel aan te pakken. Hiervoor is namelijk een investering nodig in de vorm van geld en/of capaciteit voor het oplossen van het probleem. De keuze van de fabrikant om in plaats daarvan alleen de kwetsbaarheid te repareren is verklaarbaar, maar soms is een herziening van de basis nodig om het echte (veiligheids)probleem op te lossen.

Ethische *hackers* worden met beloningen aangespoord om te zoeken naar kwetsbaarheden in software. Daardoor worden veel kwetsbaarheden opgespoord. Fabrikanten sporen daarnaast kwetsbaarheden op door het doen van verschillende testen. Maar het is niet mogelijk alle kwetsbaarheden te vinden. Kwetsbaarheden vormen steeds vaker een aanvalsroute. Een kwetsbaarheid bekend maken kan organisaties helpen zich beter te wapenen tegen mogelijk misbruik, het kan aanvallers echter ook in staat stellen de kwetsbaarheid te misbruiken. Temeer omdat hackers soms maar één lek nodig hebben om toegang te krijgen tot een systeem en het voor hen relatief eenvoudig is om

kwetsbare servers op te sporen. Daarmee ontstaat een dilemma met onveiligheid tot gevolg.
Het aantal gedetecteerde kwetsbaarheden in software groeit en de gevolgen van aanvallen worden groter. Kwetsbaarheden spelen een steeds grotere rol bij cyberaanvallen en kunnen door aanvallers worden gebruikt als startpunt voor het opzetten van een aanval. Dit onderstreept het belang van tijdig patchen. Maar patchen en mitigeren vormen tegelijkertijd een risico omdat dit kan leiden tot verstoringen of de introductie van nieuwe kwetsbaarheden. De organisatie moet het besluit om te patchen daarom goed doordenken vanuit het ICT-landschap van de organisatie. De publicatie van een kwetsbaarheid kan de opmaat vormen naar wijdverbreide aanvallen.

Regulering en aansprakelijkheid spelen ook een rol bij het ontstaan van kwetsbaarheden. Op dit moment zijn er weinig mogelijkheden voor overheden en organisaties om fabrikanten te verplichten cybersecurity in hun producten te borgen. Afnemers weten niet altijd hoe ze eisen moeten stellen en een fabrikant verantwoording moeten laten afleggen. Daarmee wordt de kwetsbaarheid een probleem van de afnemer.

Er zijn nu nauwelijks regels voor het op de markt brengen van software. De huidige marktwerking van softwareproducten dwingt te weinig af dat veiligheidsrisico's goed worden beheerst. Kwetsbaarheden opsporen is tijdrovend, kost veel menskracht en is daarmee duur. In sommige gevallen kan het nodig zijn om een product opnieuw op te bouwen om het echte (veiligheids)probleem aan te pakken. De afwezigheid van financieel-economische prikkels verklaart dat fabrikanten deze afweging op dit moment niet maken.

5.2 Aanschaf en gebruik van software door organisaties

Het veelvuldig patchen van software introduceert nieuwe problemen. Wanneer een afnemer niet patcht heeft deze mogelijk een beveiligingslek dat van buitenaf automatisch op te sporen is. Verder is de grote en toenemende hoeveelheid patches niet voor alle organisaties behapbaar. Voor afnemers is de noodzaak van (snel) patchen niet altijd duidelijk. Het aanbieden van software vanuit de *cloud* verplaatst de verantwoordelijkheid om te patchen naar de fabrikant, maar gaat ook gepaard met risico's voor afnemers.

Door de asymmetrische relatie tussen fabrikant en afnemer op het gebied van softwareveiligheid zijn afnemers doorgaans niet in staat zelf veiligheidseisen stellen bij de aanschaf van software en de juiste afwegingen maken. Er zijn wel mogelijkheden voor afnemers om bewust om te gaan met risico's van software, maar niet elke afnemer heeft de kennis en capaciteit om de juiste eisen te stellen en deze te controleren. Er bestaat geen algemene regelgeving omtrent de controle van software die fabrikanten verplicht aan bepaalde veiligheidseisen te voldoen.

Wat betreft preventie en voorbereiding op incidenten is er veel verschil in de weerbaarheid van organisaties. Veel maatregelen vergen een afweging van risico's. Niet alle organisaties hebben de expertise en capaciteit om maatregelen voldoende uit te voeren, of onderkennen de urgentie om hier capaciteit op in te zetten niet. Iedere organisatie is zelf verantwoordelijk voor zijn digitale weerbaarheid. Er is geen collectief

fundament dat geboden wordt om organisaties te helpen de digitale weerbaarheid te vergroten.

5.3 Incidentbestrijding

De incidentbestrijding in Nederland, waaronder het verzamelen en delen van informatie, is gefragmenteerd en bevat hiaten. Daardoor is voor veel organisaties, waaronder een groot deel van het Nederlandse bedrijfsleven, niet geregeld dat zij tijdig informatie ontvangen wanneer zij gevaar lopen. Het gaat daarbij in het bijzonder om slachtofferinformatie, oftewel dat een organisatie (ook ongevraagd) wordt gewaarschuwd dat zijn systemen kwetsbaar zijn en hij risico loopt om te worden aangevallen. Het NCSC, dat op dit moment ten behoeve van heel Nederland de informatie ontvangt vanuit onder meer fabrikanten, NCSC's in andere landen, inlichtingen- en veiligheidsdiensten en andere gremia, deelt deze slachtofferinformatie nu alleen met een selecte groep organisaties, niet met decentrale overheden en het merendeel van het Nederlandse bedrijfsleven en vanuit het uitgangspunt dat een organisatie vooraf toestemming geeft om te worden geïnformeerd.

Wel streeft de rijksoverheid er naar dat de informatie die NCSC wel wil delen beter wordt uitgewisseld via het zogenoemde Landelijk Dekkend Stelsel, waarin sectorale organisaties en (groepen) bedrijven ook op vrijwillige basis informatie met elkaar delen die cruciaal is voor het bestrijden van incidenten. Echter als het NCSC als nationaal aanspreekpunt informatie wel ontvangt maar niet volledig deelt, worden ook bij een volledig dekkend stelsel niet alle potentiële slachtoffers gewaarschuwd. Beveiligingsonderzoekers proberen dit hiaat op te vangen, door – op vrijwillige basis – het Nederlandse internetdomein te scannen op kwetsbare servers en deze informatie te delen met partijen die kunnen waarschuwen. Dat is echter een kwetsbare situatie, omdat zij hierin niet werden gefaciliteerd: noch door de overheid, noch door andere betrokken partijen, waardoor hun structurele inzet niet is geborgd.[226]

5.4 Leren van voorvallen

De traditie om van voorvallen te leren is in het digitale domein nog in ontwikkeling. Voorvallen moeten worden gemeld, maar worden niet systematisch onderzocht. Een 'infrastructuur' voor gezamenlijk leren door fabrikanten, organisaties die software gebruiken en andere relevante publieke en private partijen ontbreekt.

In de huidige praktijk komen veel organisaties er niet voor uit dat ze zijn aangevallen. De onderzoeken bieden niet de verklaringen die nodig zijn om het systeem te verbeteren. Betrokken organisaties verspreiden lessen uit voorvallen meestal niet buiten de eigen organisatie of gemeenschap.

226 Inmiddels is deze situatie veranderd: eind september 2021 kondigde het bedrijfsleven aan om zelf een waarschuwingssysteem op te zetten. Bron: *FD*, Bedrijfsleven start eigen alarmsysteem tegen hackers: 'overheid te traag', 28 september 2021.

6 AANBEVELINGEN

Dit onderzoek laat zien dat kwetsbaarheden in software leiden tot onveiligheid voor organisaties die software gebruiken, en voor hen die van deze organisaties afhankelijk zijn. De kloof groeit tussen digitale afhankelijkheid en de dreigingsomvang enerzijds, en de weerbaarheid van de samenleving daartegen anderzijds. Snel en fundamenteel ingrijpen is nodig om te voorkomen dat de maatschappij ontwricht raakt. Daarom doet de Onderzoeksraad voor Veiligheid aanbevelingen. De eerste aanbeveling is erop gericht om op korte termijn de responscapaciteit te vergroten. De erna volgende aanbevelingen hebben als doel om op de langere termijn het publieke en private stelsel te versterken en prikkels te introduceren zodat er een systeem ontstaat waarbinnen fabrikanten en afnemers voortdurend werken aan het veiliger maken van software.

Aan het Nederlandse kabinet en aan organisaties in Nederland die software gebruiken:[227]

1. Zorg er op korte termijn voor dat alle potentiële slachtoffers van cyberaanvallen snel en doeltreffend - gevraagd en ongevraagd - worden gewaarschuwd, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid . Breng daartoe private en publieke responscapaciteit samen en zorg daarbij voor voldoende mandaat en wettelijke waarborgen.

Toelichting: Het gaat hierbij in ieder geval om informatie over welke systemen van welke organisaties kwetsbaar zijn en risico lopen om aangevallen te worden (zogenoemde 'slachtofferinformatie'). Momenteel staat de juridische interpretatie van de AVG (IP-adressen als persoonsgegeven) en de Wbni (mandaat van het NCSC beperkt tot Rijk en vitaal) het NCSC in de weg om alle slachtoffers waar zij informatie over krijgen te waarschuwen en om zelf proactief deze informatie te verzamelen ('scannen').

Aan de Eurocommissaris voor Interne Markt en de Eurocommissaris voor een Europa dat klaar is voor het digitale tijdperk:

2. Zorg dat uw initiatieven om te komen tot wetgeving voor veiligere software leiden tot een Europese verordening die de verantwoordelijkheid van fabrikanten vastlegt en afnemers inzicht geeft in hoe fabrikanten die verantwoordelijkheid invullen. Leg vast dat fabrikanten aansprakelijk zijn voor de gevolgen van softwarekwetsbaarheden.

Toelichting: Essentiële elementen van deze verordening zijn onder andere – maar niet uitsluitend - verplichte deelname aan *bug bounty* programma's, richtlijnen voor onafhankelijke audits, het melden van kwetsbaarheden, traceerbaarheid, *recalls*, en het delen van lessen uit cyberaanvallen. Ervaringen met wet- en regelgeving als de AVG/GDPR bewezen dat Europese regulering in het digitale domein haalbaar en effectief is.

227 Uit praktische overwegingen schrijft de Onderzoeksraad de overheid in zijn rol als afnemer aan via de staatssecretaris van Binnenlandse Zaken, het Interprovinciaal Overleg, de Vereniging van Nederlandse Gemeenten en de Unie van Waterschappen. De andere organisaties, waaronder zorg, onderwijs, vitale aanbieders en het overige bedrijfsleven schrijft de Raad aan via de bij de SER betrokken ondernemersorganisaties VNO-NCW, MKB-Nederland en LTO Nederland.

Aan fabrikanten van software gezamenlijk:[228]

3. Ontwikkel met andere fabrikanten good practices om software veiliger te maken. Neem in de overeenkomsten met uw afnemers op dat u zich hieraan committeert.
4. Waarschuw en help al uw afnemers zo snel en doeltreffend mogelijk wanneer kwetsbaarheden in software gesignaleerd worden. Schep de randvoorwaarden die noodzakelijk zijn om uw afnemers te kunnen waarschuwen.

Toelichting: De verantwoordelijkheid en mogelijkheden om software veiliger te maken en om afnemers te waarschuwen ligt in de eerste plaats bij fabrikanten zelf.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Economische Zaken en Klimaat (ten behoeve van alle organisaties en consumenten in Nederland): [229]

5. Bevorder dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten. Zorg dat de overheid daarbij een voortrekkersrol speelt. Ga uit van het principe: collectieve samenwerking waar mogelijk; branche-specifiek waar noodzakelijk.

Toelichting: Het is noodzakelijk dat afnemers hun krachten bundelen zodat zij hun positie richting fabrikanten versterken en schaarse cybersecurity-expertise gezamenlijk zo doelmatig en effectief mogelijk inzetten, zoals een aantal Nederlandse banken nu al doet.

Aan het Nederlandse kabinet:

6. Creëer naar analogie van de Comptabiliteitswet een wettelijke basis voor de beheersing van digitale veiligheid door de overheid.
7. Verplicht alle organisaties om op eenduidige wijze verantwoording af te leggen over de wijze waarop zij digitale veiligheidsrisico's beheersen.[230]

Toelichting: De wijze waarop overheden en bedrijven de risico's die gepaard gaan met digitalisering beheersen en zich daarover verantwoorden is vooralsnog vrijblijvend. Versnippering van verantwoordelijkheden staat een slagvaardig optreden in de weg. Essentieel is dat er een sluitend stelsel komt dat organisaties helpt om de digitale veiligheid op systematische en doelmatige wijze te beheersen. Mogelijke elementen zijn een eenduidig mandaat voor CISO's bij de overheid, toezicht dat is belegd bij de minister die het aangaat en voor alle organisaties verplichte verantwoording over de beheersing van digitale veiligheidsrisico's, via jaarverslagen en onder controleverklaring van de accountant.

228 Deze aanbeveling is gericht aan alle fabrikanten van software. Uit praktische overwegingen schrijft de Onderzoeksraad de fabrikanten aan die betrokken waren bij de voorvallen die dit onderzoek beschrijft, de gemeenschappen van de betrokken open source-projecten en de (leden van de) brancheorganisatie Business Software Alliance.

229 Zie voetnoot 224. Vanwege de relevantie van veilige software voor eindgebruikers (inclusief consumenten) dient ook de Consumentenbond hierbij te worden betrokken. En de Kamer van Koophandel voor ondersteuning aan organisaties.

230 Het ligt in de rede om aan te sluiten bij bestaande structuren en verplichtingen in de Comptabiliteitswet 2016 (van toepassing op overheden), Burgerlijk Wetboek (niet-beursgenoteerde rechtspersonen), nadere voorschriften controle- en overige standaarden (NV COS) vanuit de NBA en geharmoniseerde wetgeving voor naamloze vennootschappen vanuit de EU.

ONDERZOEKSVERANTWOORDING

A.1 Doel en onderzoeksvragen van het onderzoek

Het doel van dit onderzoek is lessen te identificeren die verantwoordelijke partijen helpen de beheersing van risico's als gevolg van kwetsbaarheden in software te beheersen. 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 Citrix-voorval in december 2019 vormt de aanleiding voor dit onderzoek, als typisch voorbeeld van een gebeurtenis waarbij deze risico's ontstaan, zoals ook andere cyberaanvallen sinds 2020 demonstreren.

De Onderzoeksraad gaat er vanuit dat de manier waarop fabrikanten, organisaties die software gebruiken, de overheid en andere organisaties digitale veiligheidsrisico's beheersen[231], 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:

8. Hoe konden de beveiligingslekken bij organisaties door een kwetsbaarheid in Citrix software ontstaan en welke gevolgen had dit?
9. 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?
10. Wat er is nodig van betrokken partijen om het systeem van risicobeheersing en -sturing te versterken?

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

A.2 Gegevensverzameling

De Raad heeft de volgende aanpak gehanteerd tijdens het onderzoek.

Om bekend te raken met de materie volgde het team een tweedaagse training van een beveiligingsbedrijf. In dezelfde periode begonnen we met het verzamelen van voornamelijk openbare informatie. Dit betrof onder meer beleidsdocumenten, nieuwsberichten, berichten in vakmedia, gepubliceerde onderzoeken over voorvallen, wetenschappelijke publicaties en documentatie over software, kwetsbaarheden en *exploits*.

Deze informatie vulden we aan door betrokken partijen te benaderen voor interviews en parallel daaraan schriftelijke vragen te stellen over de kwetsbaarheden, de werkwijze van organisaties bij het produceren, updaten, aanschaffen en gebruiken van software en de bestrijding van incidenten (feitenrelazen, interne communicatie, verslagen van overleggen, logboeken). De meeste partijen werkten hieraan mee. De Onderzoeksraad heeft contact gezocht met de in het onderzoek genoemde fabrikanten via de verschillende kanalen die op hun websites worden vermeld, per e-mail en per post. De Raad heeft overwogen contact op te nemen met de betreffende PSIRT's, maar aangezien het onderzoek geen actueel beveiligingsincident betrof en de Raad geen CERT-organisatie of andere doelgroep van PSIRT's is, achtte hij dit geen geschikt kanaal om contact op te nemen. Helaas leidde sommige van onze pogingen om contact te leggen met fabrikanten[232] in de onderzoeksfase van dit onderzoek niet tot contact.

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.

A.3 Analyse

A.3.1 Ongevalsanalyse

We reconstrueerden het verloop van de *gebeurtenissen* met een tijdlijnanalyse. Om de mogelijke *factoren* die van invloed zijn geweest in beeld te krijgen, analyseerden we het voorval met behulp van ongevalsanalysemethode Tripod-Beta. Voor het visualiseren van de bevindingen gebruikten we BowTie. De verschillende analyses hadden vooral een intern doel: het ordenen van de informatie en het controleren of de informatie volledig en consistent is. In het rapport namen we enkele tijdlijnen op hoofdlijnen op, die de lezer helpen bij het lezen van het rapport.[233]

232 Het betreft fabrikanten Fortinet, Palo Alto en F5. Fortinet en F5 hebben wel deelgenomen aan de inzageprocedure en F5 heeft tijdens de inzagefase een vragenlijst ingevuld.

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

A.3.2 Systeemanalyse

Om in beeld te brengen hoe de verschillende actoren de veiligheid borgden, voerden we een omgevings- en stakeholdersanalyse uit en pasten we de CAST/STAMP-methodiek toe. CAST geeft inzicht in de hiërarchische lijnen, rollen en verantwoordelijkheden van de betrokken partijen en de relatie met wet- en regelgeving. We pasten dit toe op:

- kwetsbaarheden in software;
- de wijze waarop organisaties software aanschaffen en gebruiken;
- incidentbestrijding.

Als theoretisch kader sluiten we aan bij de theorie uit publicaties over besturingsarrangementen in de cybersecurity (governance).
Daarbij is op relevante onderdelen een vergelijking gemaakt met andere sectoren waar de Onderzoeksraad onderzoek doet, zoals transport en voedselveiligheid.[234]

A.3.3 Kwaliteitsbeheersing

Om de kwaliteit van het onderzoek te borgen zijn de volgende stappen doorlopen:

- Voor het onderzoek is met het projectteam een kwaliteitsplan opgesteld waarin risico's voor de kwaliteit van het onderzoek en bijhorende beheersmaatregelen zijn geformuleerd.
- Gedurende het onderzoeksproces heeft het projectteam op meerdere momenten sessies gehouden. Tijdens deze sessies werden de onderzoeksbevindingen uit interviews, documenten en analyses gedeeld en geduid en gaven teamleden tegenspraak op elkaars input. De eerste sessies stonden in het teken van het onderzoeksontwerp (onderzoeksvragen, focus en afbakeningen). De sessies daarna waren gewijd aan de ongevalsanalyse en systeemanalyse. Eén van de leden van de begeleidingscommissie reflecteerde tijdens deze sessies expliciet op de confrontatie met de praktijk. In de laatste sessies formuleerden we de conclusies en aanbevelingen van het onderzoek.
- Gedurende het onderzoek is een tegendenksessie georganiseerd en hebben collega's tussen- en eindproducten van het onderzoek tegengelezen. Tegendenken en -lezen houdt in dat onderzoekers die niet in het projectteam zitten tussenproducten van het onderzoek lezen en daar commentaar op geven. Dit is gedaan met de startdocumenten (afwegingskader, focusnotitie, plan van aanpak), de tussentijdse bevindingen en de conceptversie van het rapport. De uitkomsten van de tegen-denksessie en het tegenlezen zijn gebruikt om de analyse en het rapport te verbeteren.
- Het onderzoek werd besproken met een begeleidingscommissie (zie volgende paragraaf.

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

A.4 Begeleidingscommissie

De Onderzoeksraad heeft voor dit onderzoek een begeleidingscommissie samengesteld. Deze commissie bestaat uit externe leden met voor het onderzoek relevante ervaring en deskundigheid onder voorzitterschap van een lid van de Onderzoeksraad. De externe leden hebben op persoonlijke titel zitting in de begeleidingscommissie. Gedurende het onderzoek is de commissie vier keer bijeengekomen om met het raadslid en het projectteam van gedachten te wisselen over de opzet en de resultaten van het onderzoek. De commissie vervult een adviserende rol binnen het onderzoek. De eindverantwoordelijkheid voor het rapport en de aanbevelingen ligt bij de Onderzoeksraad.
De commissie is als volgt samengesteld:

Naam	Functie
prof. dr. mr. S. (Stavros) Zouridis	Voorzitter begeleidingscommissie, Raadslid Onderzoeksraad voor Veiligheid.
schout-bij-nacht b.d. P.J. (Pieter) Bindt	Oud-directeur van de MIVD, tegenwoordig zelfstandig adviseur en buitengewoon raadslid voor de Onderzoeksraad voor Veiligheid.
drs. I. (Inge) Bryan	Managing director NCC Europe/ CEO Fox-IT (hoofdfunctie), Bestuurslid Global Forum on Cyber Expertise, Voorzitter Anti-Abuse Netwerk.[235]
dr. M. (Martijn) Dekker	Chief Information Security Officer (CISO) bij ABN AMRO, lid Security Board IBM en docent TIAS.
prof. dr. M.J.G. (Michel) van Eeten	Hoogleraar governance van cybersecurity aan de TU Delft.
mr. ir. A.P. (Arnoud) Engelfriet	ICT-jurist, partner bij ICTRecht en auteur.
M.R. (Marietje) Schaake MA	Directeur internationaal beleid Stanford University Cyber Policy Center, en President CyberPeace Institute.

235 Overige nevenfuncties: Bestuurslid Koninklijke Hollandsche Maatschappij der Wetenschappen, Lid Raad van Toezicht Instituut Clingendael, Lid Raad van Advies: Nationaal Archief, Politie Academie, Executive Master Legal Technologies Universiteit Leiden en Inspectie Openbare Orde en Veiligheid (ministerie van JenV) (per 1 september 2021).

A.5 Projectorganisatie

Naam	Functie
dr. A. (Arzu) Umar	Onderzoeksmanager
ir. M. (Marjolein) Baart MPS	Projectleider
ir. M.A. (Marlon) van den Hoek	Onderzoeker
N.E. (Nynke) Wierda MSc	Onderzoeker
H.W. (Berthil) Verzijl MSc	Onderzoeker
E.V. (Eliane) de Vilder	Onderzoeker
drs. A.J. (Sander) Bakker	Technisch specialist
drs. E.J. (Elsabé) Willeboordse	Adviseur onderzoek en ontwikkeling
R.T. (Ron) Koppes MSc	Adviseur onderzoek en ontwikkeling
drs. Y.S.A. (Yannick) Balk	Secretaris
drs. R.D. (Reinier) de Wit	Secretaris
J. (Jale) Demir	Projectondersteuning

REACTIES OP CONCEPTRAPPORT

Het conceptrapport (zonder beschouwing en aanbevelingen) is voorgelegd aan de betrokken partijen. Deze partijen is gevraagd het rapport te controleren op feitelijke onjuistheden en onduidelijkheden. De volgende partijen hebben een reactie gegeven op het conceptrapport:

- Citrix
- Ivanti
- Fortinet
- F5
- Minister van JenV, inclusief NCTV en NCSC
- Minister van BZK, inclusief CIO Rijk
- AIVD
- Minister van EZK, inclusief DTC
- DIVD (response team van vrijwilligers)
- SURFCert
- IBD

De volgende partijen hebben afgezien van het geven van een reactie:

- ZCert
- Eurocommissaris voor Interne Markt en de Eurocommissaris voor een Europa dat klaar is voor het digitale tijdperk

Palo Alto kon niet bereikt worden.

De ontvangen reacties, alsook de wijze waarop ze zijn verwerkt, zijn opgenomen in een tabel die te vinden is op de website van de Onderzoeksraad voor Veiligheid (www.onderzoeksraad.nl).

De reacties zijn in twee categorieën te verdelen:

- Correcties van feitelijke onjuistheden, aanvullingen op detailniveau, en redactioneel commentaar heeft de Onderzoeksraad (voor zover juist en relevant) overgenomen. De betreffende tekstdelen zijn in het eindrapport aangepast.
- De reacties die niet zijn overgenomen, zijn in de tabel voorzien van een motivering van de Onderzoeksraad waarom deze niet zijn overgenomen.

REFERENTIEKADER

In al zijn onderzoeken hanteert de Onderzoeksraad een referentiekader. Het maakt expliciet hoe risico's naar de huidige inzichten kunnen worden beheerst en wat de Onderzoeksraad verwacht van partijen bij de beheersing van een voorval, zoals in dit onderzoek kwetsbaarheden in software en de beveiligingslekken die daardoor ontstaan in digitale systemen van organisaties. Het referentiekader beschrijft goede praktijken voor de betrokken actoren en de voorwaarden die idealiter aanwezig zijn om digitale veiligheid te kunnen waarborgen.

C.1 Waarborgen van digitale veiligheid

Net als in andere domeinen, zoals voedsel, transport, zorg en de procesindustrie, komen veilige digitale systemen die gebruik maken van software tot stand in een netwerk van activiteiten en partijen. En net als in andere domeinen is software per definitie een onvolkomen product en brengt het gebruik van digitale systemen inherente veiligheidsrisico's met zich mee.

In Nederland hebben veel partijen een aandeel in het waarborgen van digitale veiligheid. Verschillende soorten organisaties zijn betrokken bij ontwikkeling en gebruik van software.

- software fabrikanten;
- IT-dienstverleners;
- beveiligingsbedrijven;
- organisaties die software gebruiken: overheden, zorg, onderwijs, nutsbedrijven, bedrijven et cetera;
- binnen organisatie: bestuur, CIO, CISO.

In het onderzoek kijken we hoe de rollen en verantwoordelijkheden van deze partijen zijn georganiseerd: de structuren, processen, normen en afspraken voor het beheersen van de risico's van digitale systemen in Nederland. Daarbij gaat het om (semi-) overheidsorganisaties, grote bedrijven en het midden- en kleinbedrijf. Om risico's te kunnen beheersen is het nodig dat partijen duidelijke taken, rollen en verantwoordelijkheden hebben, die samen een sluitend geheel vormen. De onderlinge verhoudingen tussen de partijen zijn helder en er bestaat geen onduidelijkheid over de structuur. Ook is het nodig dat partijen die onderling van elkaar afhankelijk zijn, voldoende op elkaar zijn ingespeeld en routines hebben ontwikkeld om samen tijdig de

noodzakelijke besluiten te nemen en uit te voeren en dat er standaarden zijn die moeten worden gehanteerd om de risico's van het gebruik van digitale systemen te waarborgen.[236]

De Rijksoverheid is verantwoordelijk voor het stelsel waarbinnen al deze partijen opereren en onderling van elkaar afhankelijk zijn voor het borgen van de veiligheid. Het is dan ook nodig dat de rijksoverheid de preventie en bestrijding van digitale voorvallen ziet als collectieve maatschappelijke opgaven, waar de rijksoverheid stelselverantwoordelijk voor is. Net zoals de Rijksoverheid stelselverantwoordelijk is voor hoe we de veiligheid van onze auto's en ons voedsel borgen, zowel preventief als in het bestrijden van incidenten.

C.2 Productveiligheid van software

Software is een dynamisch product: ook nadat het op de markt is gebracht, worden er regelmatig verbeteringen en uitbreidingen aangebracht. Iedere pc- en smartphone-bezitter kent de regelmatig uit te voeren updates en patches. Dit gebeurt ook bij software voor professionele gebruikers (zakelijke markt). Softwareproducten bestaan doorgaans uit een groot aantal componenten. Net als in andere domeinen maakt de uiteindelijke softwarefabrikant (ook wel *vendor* genoemd) deze componenten niet altijd zelf. De fabrikant bouwt voort op componenten die anderen hebben ontwikkeld en ondergebracht zijn in zogenoemde bibliotheken (*libraries*).[237] Voor een deel zijn dit open source componenten en voor een deel worden deze componenten onderling verhandeld.

Tijdens de levenscyclus van software worden kwetsbaarheden ontdekt die moeten worden verholpen. Deze kwetsbaarheden worden ontdekt door of in opdracht van de fabrikant zelf of door ethische *hackers* al dan niet in opdracht van de organisaties die de software gebruiken. Ter indicatie: softwarefabrikanten brengen jaarlijks ongeveer 30.000 software updates (patches) uit om kwetsbaarheden te verhelpen. Hierbij is de vraag wat van fabrikanten en andere betrokken partijen mag worden verwacht als het gaat om het zo veel mogelijk voorkomen van het ontstaan van kwetsbaarheden in software.

Deze verantwoordelijkheden moeten worden bezien vanuit de achtergrond dat veiligheid een emergente eigenschap is die wordt bepaald door de eigenschappen van de software zelf in combinatie met de manier waarop de software deel uitmaakt en wordt gebruikt binnen de context van een digitaal systeem.[238] Het gebruik van een digitaal systeem verbonden met het internet gaat daarbij met extra risico's gepaard, onder meer dat het digitale systeem wordt aangevallen. Om die risico's te beheersen gebruiken organisaties bepaalde software-onderdelen, die bijvoorbeeld regelen wie waartoe toegang tot krijgt in het digitale systeem, of die een verbinding afschermt van de rest van het internet. Dit maakt dat deze software een veiligheidskritische functie heeft voor het digitale systeem: als er in die software een veiligheidsprobleem (kwetsbaarheid) zit, kan dit ten koste gaan van de veiligheid en beveiliging van het digitale systeem als geheel.

236 Zie onder andere Hood C. e.a., *The Government of Risk: Understanding Risk Regulation Schemes*, 2001.
237 Bibliotheken die door meerdere softwaretoepassingen kunnen worden gebruikt wordt dynamic linker genoemd. In Windows heet het dynamic-link library (DLL) en in Linux shared objects (.so).
238 Leveson, N., "Are you sure your software will not kill anyone?", *Communications of the ACM*, 2020.

De rol van fabrikant en afnemer
Zeker bij software die binnen digitale systemen van organisaties een veiligheidskritische functies vervult (zoals de software die aan de orde komt binnen dit onderzoek), verwacht de Raad dat fabrikanten vanaf het begin van de ontwerpfase en gedurende de gehele levenscyclus van software de veiligheid en beveiliging centraal stellen (*safety and security by design*).

De software moet ontworpen zijn om bestand te zijn tegen aanvallen en op de juiste manier te reageren wanneer de techniek faalt (*failsafe*). Daarbij moet de fabrikant bij het ontwerp van het de software rekening houden met ondeskundig gebruik en er voor zorgen dat de software bestand is tegen (onbedoeld) foutief of ondeskundig gebruik (*foolproof*). Denk daarbij bijvoorbeeld aan de standaard configuratie van de software.

Van een fabrikant kan verwacht worden dat deze een constante veiligheidsanalyse maakt van de gehele architectuur van het product, dat is iets wat de gebruiker niet kan. Het is belangrijk dat de fabrikant deze analyses maakt, omdat deze constant bezig is met het door ontwikkelen van de software, onder meer door componenten en andere producten te kopen en te integreren. Daarnaast heeft ook de afnemer een eigen verantwoordelijkheid om af te wegen hoe het product ingezet wordt en hoe het landschap van de organisatie eruit ziet.

Bij het verder ontwikkelen van de software gedurende de gehele levenscyclus moet de fabrikant de veiligheid van de in de software gebruikte componenten continue blijven monitoren. Denk daarbij aan wanneer gebruikte componenten in de software of programmeertalen niet meer aan actuele standaarden voldoen, niet meer worden beschouwd als goede software engineering praktijk of kwetsbaarheden bevatten.

Verder is het belangrijk dat fabrikanten aan organisaties die de software afnemen en gebruiken inzicht geven wat de technologie inhoudt en uit welke componenten de software bevat (transparantie). Dit is belangrijk voor het versterken van de informatiepositie en het handelingsperspectief van de organisatie die de software gebruikt. De organisatie moet de software zo kunnen toepassen in zijn digitale systeem dat de software veilig is binnen de gegeven context van de organisatie, zijn systemen en activiteiten. Ook moeten fabrikanten aan organisaties en autoriteiten demonstreren dat hun software voldoet aan te stellen veiligheidseisen. Zo moeten fabrikanten gelegenheid bieden om de software te laten pentesten en om technisch-inhoudelijke audits zoals code reviews te laten uitvoeren.

De rol van de overheid[239]
De Onderzoeksraad voor Veiligheid ziet digitale veiligheid als een noodzakelijke voorwaarde om op een verantwoorde manier te kunnen digitaliseren. Voor organisaties, of het nu overheden zijn of bedrijven, is digitaliseren geen keuze maar noodzakelijk voor het kunnen functioneren en voortbestaan. Dit geldt in brede zin ook voor personen in hun rol als consument, burgers of werknemer.

239 Zie onder andere ministerie van Economische Zaken en Klimaat & ministerie van Justitie en Veiligheid, *Roadmap Digitaal Veilige Hard- en Software*, april 2018.

Vanuit dit uitgangspunt ziet de Raad een belangrijke rol voor de rijksoverheid als stelselverantwoordelijke. Niet alleen door bij te dragen aan het waarborgen van de digitale veiligheid, maar ook vanuit zijn verantwoordelijkheid voor het beschermen van grondrechten van burgers/consumenten, het opsporen en vervolgen van strafbare feiten, het beschermen van onze economische positie en vitale functies en het bewaken van onze territoriale integriteit.

Voor wat betreft het bestrijden van cybersecurity incidenten ziet de Onderzoeksraad voor de overheid een verantwoordelijkheid vast te stellen en zo nodig te stimuleren dat er een sluitende systematiek van risicobeheersing is, dat de overheid de randvoorwaarden schept die het organisaties mogelijk maakt om hun verantwoordelijkheid voor digitale veiligheid te nemen. Redenerend vanuit andere domeinen waarin de Raad actief is, zoals de transportsectoren en de voedselsector, bestaat een dergelijke systematiek uit een aantal verschillende onderdelen, die elkaar versterken.

Zo is het voor iedereen duidelijk aan welke minimale veiligheidseisen software en processen van fabrikanten en organisaties die software gebruiken (inclusief de overheid zelf) moeten voldoen voor de software op de markt komt (toelatingseisen), gedurende de gehele levenscyclus (permanente eisen) en hoe de organisatie de software toepast in zijn digitale systeem (gebruikseisen). Ook is het voor fabrikanten en voor organisaties die de producten en diensten van fabrikanten afnemen duidelijk en transparant hoe fabrikanten aantonen dat zij aan de veiligheidseisen voldoen. De overheid tenslotte borgt dat organisaties die software gebruiken, beschikken over voldoende informatiepositie en handelingsperspectief, om eigenstandig risico's te kunnen inschatten en afwegingen te maken die verbonden zijn aan de inherent gevaarlijke situatie om verbonden te zijn met het internet en daar veiligheidskritische software bij te gebruiken. En voor klanten, burgers en toezichthouders om vast te stellen of de organisatie de risico's beheerst.

Vanwege het internationale karakter van digitale systemen, zorgt de overheid voor internationale overeenstemming over de eisen, de naleving en de informatie daarover. Een dynamisch product als software vraagt bij uitstek om een lerend systeem, waarin fabrikanten, organisaties en andere betrokken partijen samenwerken om lessen uit ervaringen en incidenten met elkaar te delen, zodat niet elke partij het wiel opnieuw hoeft uit te vinden en processen op elkaar afgestemd blijven. De overheid organiseert daarvoor de randvoorwaarden, zoals de mogelijkheid om veilig te melden en te onderzoeken, zonder dat dezelfde informatie gebruikt wordt in juridische procedures. Een voorbeeld kan worden genomen aan de transportsectoren, waarvoor dit in internationale regelgeving voor zowel fabrikanten als organisaties die de producten gebruiken is vastgelegd. Een ander voorbeeld van een sector met internationale ketens van fabrikanten, tussenhandelaren en afnemers is de voedselsector. In deze sector werken partijen in wereldwijde programma's en platforms samen door eisen en best *practices* op te stellen en risico's gerelateerd aan grondstoffen, producten en leveranciers via platforms met elkaar uitwisselen.

Bijzonder in vergelijking met de andere sectoren is dat kwetsbaarheden in software niet alleen een enkelvoudig productveiligheidsprobleem vormen, maar onderdeel kunnen worden van het cyberarsenaal van diverse wereldwijd opererende actoren, waaronder

criminelen en (zij die werken voor) statelijke actoren. De rijksoverheid heeft vanuit zijn grondwettelijke taak om te streven naar ontwikkeling van de internationale rechtsorde[240] de verantwoordelijkheid om zich op het wereldwijde speelveld in te spannen om te komen tot spelregels en de naleving daarvan. Het gegeven dat kwetsbaarheden in software kunnen worden ingezet als cyberwapen is ook relevant bij de verdeling van rollen, taken en verantwoordelijkheden in de risicobeheersing, incidentbestrijding en het leren van incidenten.

Maatschappelijk verantwoord digitaliseren
Zowel bij de ontwikkeling van nieuwe software als bij de levenscyclus van bestaande software om digitalisering mogelijk te maken, draagt maatschappelijk verantwoord ondernemen bij aan het bereiken van een 'evenwicht tussen inspanningen om de positieve bijdragen van digitalisering te maximaliseren en de negatieve gevolgen ervan te minimaliseren'.[241] Belangrijk hierbij is de gedeelde verantwoordelijkheid voor de maatschappelijke inbedding tussen fabrikanten, overheid en (andere) maatschappelijke actoren (zoals organisaties die de software gebruiken). Daarbij zijn de fabrikanten hoofdverantwoordelijk voor een veilig ontwerp van software. Het is de rol van de overheid om zowel de kansen als de risico's van digitalisering in beeld te krijgen en te houden, en deze te delen met partijen die mitigerende maatregelen kunnen nemen.[242]

C.3 Preventie en voorbereiding op incidenten

Organisaties zijn primair verantwoordelijk voor hun eigen ICT en informatiebeveiliging. Iedere organisatie die gebruik maakt van ICT heeft zogenoemde 'digitale zorgplichten'.[243] Voor verschillende sectoren/typen organisaties bestaan standaarden, normen of wettelijke verplichtingen die organisaties kunnen helpen bij het inrichten van hun informatievoorziening en informatiebeveiliging.[244]

Voorbeelden van deze principes voor informatiebeveiliging bij organisaties zijn de volgende:
- ICT moet een vaste plaats hebben op de agenda bij het management of bestuur van een organisatie, zodat zij deze verantwoordelijkheid voor het ICT-beleid voelt en neemt. Ook zijn duidelijke afspraken omtrent cybersecurity nodig;
- Organisaties dienen voldoende technische en organisatorische expertise en capaciteit in huis te hebben, zodat zij maatregelen kunnen nemen om de veiligheid van de systemen te garanderen. Hier bestaan verschillende standaarden en certificerings-mechanismen voor;
- Het is cruciaal dat een organisatie zijn risico's in beeld heeft en via een kosten-baten analyse vaststelt welke risico's als acceptabel worden gezien en zich bewust is van de

240 Artikel 90 van de Grondwet.
241 Rip, A., The Past and Future of RRI, *Life Sciences, Society and Policy* 10, nummer 1, 2014.
242 Onderzoeksraad voor Veiligheid, *Wie stuurt? Verkeersveiligheid en automatisering in het wegverkeer,* november 2019.
243 Cyber Security Raad, *'Ieder bedrijf heeft digitale zorgplichten', een handreiking voor bedrijven op het gebied van cybersecurity,* februari 2017.
244 Bijvoorbeeld: Baseline Informatiebeveiliging Overheid (BIO, ISO27001 en ISO27002) voor overheidsorganisaties, NEN7510 voor de zorg, AVG betreft de verwerking van persoonsgegevens, WBNI voor digitale dienstverleners, ABDO voor organisaties die werken voor Defensie.

mogelijke gevolgen indien dit niet geborgd is. Een organisatie moet inzicht hebben in vitale onderdelen en proportionele beveiliging hiervan regelen (de beveiligingsmaatregelen hangen af van het risico). Hier hoort ook de afweging bij hoe urgent het is om bepaalde software onderdelen direct te patchen en of onderdelen die cruciaal zijn voor het kunnen functioneren van de organisatie redundant en divers[245] uit te voeren;
- het is van belang om als organisatie bewust te zijn van ketenafhankelijkheden. Organisaties moeten afspraken over cybersecurity maken met hun ketenpartners (een keten is immers zo sterk als de zwakste schakel);
- voordat een organisatie nieuwe software aanschaft, is het van belang na te denken over de veiligheidseisen waar deze software aan moet voldoen.

C.4 Incidentbestrijding (respons)

Hoe kunnen fabrikanten en organisaties die software gebruiken reageren als software die op de markt is en wordt gebruikt toch kwetsbaarheden bevat? Deze activiteiten noemen we incidentbestrijding of respons. Daarbij gaat het zowel om respons door de fabrikant (kwetsbaarheid verhelpen met eventueel een tijdelijke mitigerende maatregel en een definitieve patch, klanten waarschuwen), door organisaties die de software gebruiken, hun branches en de overheid.

Van de fabrikant verwachten we dat deze alles wat redelijkerwijs mogelijk is in het werk stelt om de onveiligheid bij de organisaties die de software gebruiken weg te nemen. En dat de fabrikant onderzoek doet naar waardoor de kwetsbaarheid is veroorzaakt, zodat hij deze factoren zo veel mogelijk kan reduceren en zo toekomstige kwetsbaarheden kan voorkomen. Van de overheid verwachten we dat deze zorgdraagt voor een heldere toedeling van verantwoordelijkheden aan relevante partijen. Daarbij is het belangrijk dat partijen over de juiste middelen en bevoegdheden beschikken om deze verantwoordelijkheden uit te kunnen voeren en dat er duidelijke communicatielijnen en transparante communicatie is die ervoor zorgt informatie terechtkomt bij alle partijen die deze informatie nodig hebben om de veiligheid te kunnen beheersen, en dat deze informatie daarvoor ook voldoende handelingsperspectief biedt.

245 Redundantie houdt in dat wanneer een onderdeel uitvalt, het geheel kan blijven functioneren, bijvoorbeeld door componenten dubbel uit te voeren. Bijvoorbeeld door twee soorten software te gebruiken voor het op afstand toegang gegeven tot het digitale systeem van de organisatie, zodat het andere kan worden uitgezet voor onderhoud of wanneer het onveilig is. Dit hangt samen met software diversiteit, een principe waarbij de beveiliging van een digitaal systeem wordt versterkt door een diversiteit aan producten te gebruiken. Het redundant en divers uitvoeren van functies kan voor een organisatie een dilemma zijn, want het vergroot de complexiteit van het systeem. Zie bijvoorbeeld Q. Zhang, J. -H. Cho, T. J. Moore and I. -R. Chen, 'Vulnerability-Aware Resilient Networks: Software Diversity-based Network Adaptation,' in *IEEE Transactions on Network and Service Management*, doi: 10.1109/TNSM.2020.3047649.

C.5 Leren van voorvallen

Om ongevallen te voorkomen is het van belang om te leren van ongevallen. Daarvoor is een leerproces nodig, waarin de lessen uit ongevallen als feedback terugkomen naar de organisaties die deze feedback nodig hebben om de veiligheid te verbeteren:[246]

1. incidenten en ongevallen worden gerapporteerd binnen de betreffende organisatie en eventueel bij een instantie daarbuiten. In eerste instantie zijn de fabrikant van de software en de verantwoordelijke voor het digitale systeem verantwoordelijk om voorvallen te melden, maar ook andere partijen zoals afnemers en onafhankelijke digitale onderzoekers (ethische hackers) kunnen voorvallen melden. Het is dan belangrijk dat het duidelijk is waar en hoe dergelijke meldingen zorgvuldig en veilig kunnen worden ontvangen en onderzocht.
2. op basis van criteria wordt geselecteerd welk voorval in aanmerking komt voor verder onderzoek, door de betreffende organisatie (de fabrikant van de software, de beheerder van het digitale systeem, etc.) en eventueel door een instantie daarbuiten (bijvoorbeeld een toezichthouder of een onafhankelijke onderzoeksautoriteit). Veel organisaties zijn bereid om te leren van grote en ernstige ongevallen, maar ook uit het onderzoeken van incidenten kunnen inzichten worden opgedaan die kunnen worden gezien als waarschuwingen[247] en grotere ongevallen kunnen voorkomen;[248]
3. het onderzoek wordt uitgevoerd (zie hierna);
4. de betreffende organisatie en/of de onderzoekers delen de resultaten van het onderzoek met die partijen die iets kunnen doen om de veiligheid te verbeteren en zo toekomstige ongevallen te voorkomen;
5. de partijen die het aangaat passen de beheersing van de risico's aan op basis van de inzichten uit het ongevalsonderzoek.

Het is belangrijk dat de factoren die tot het voorval en het ontstaan van de gevolgen hebben geleid, de beheersmaatregelen die daarop van invloed waren en de context waarin dat plaatsvond, zo volledig mogelijk in beeld komen. De inrichting en uitvoering van het onderzoek zijn bepalend voor de mate waarin het onderzoek deze inzichten kan bieden. Uit de literatuur en uit eerdere onderzoeken van de Raad blijkt dat de volgende zaken van belang zijn:

- bewust zijn van en beheersmaatregelen nemen tegen de verschillende vormen van bias bij de onderzoeker (meest bekend is *hindsight bias*) en bij de onderzochte (subjectieve beoordeling, afhankelijkheidspositie);
- zorgen voor kennis en expertise die aansluit bij het type incident of ongeval;
- de onderzoeker moet toegang hebben tot relevante data en middelen voor datacollectie;
- de onderzoekers moeten methoden gebruiken die aansluiten bij het type voorval en zorgen voor een passende wijze van verslaglegging tijdens het onderzoek, zodat de bevindingen herleidbaar zijn;

246 Lindberg, A.K., S.O. Hansson en C. Rollenhagen, Learning from accidents — what more do we need to know? *Safety Science* 2010, nr. 6, p. 714–721.

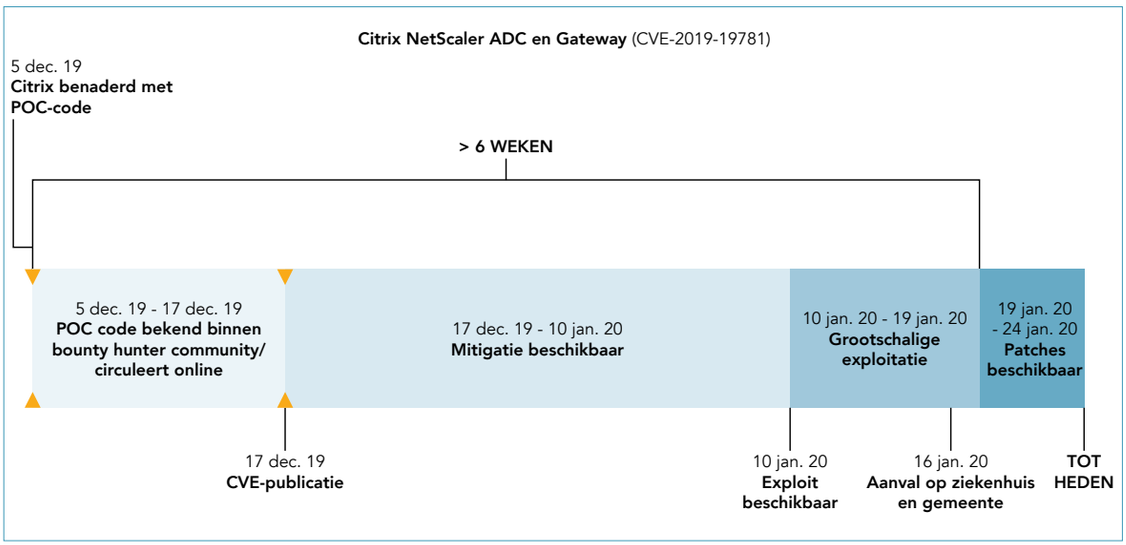
247 Drupsteen, L. en P. Hasle, 'Why do organizations not learn from incidents? Bottlenecks, causes and conditions for a failure to effectively learn', *Accident Analysis & Prevention* 2014, nr. 72, p. 351-358; E. Stemn, C. Bofinger, D. Cliff en M.E. Hassall, 'Failure to learn from safety incidents: Status, challenges and opportunities', *Safety Science* 2018, nr. 101, p. 313-325; Lindberg 2010.

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

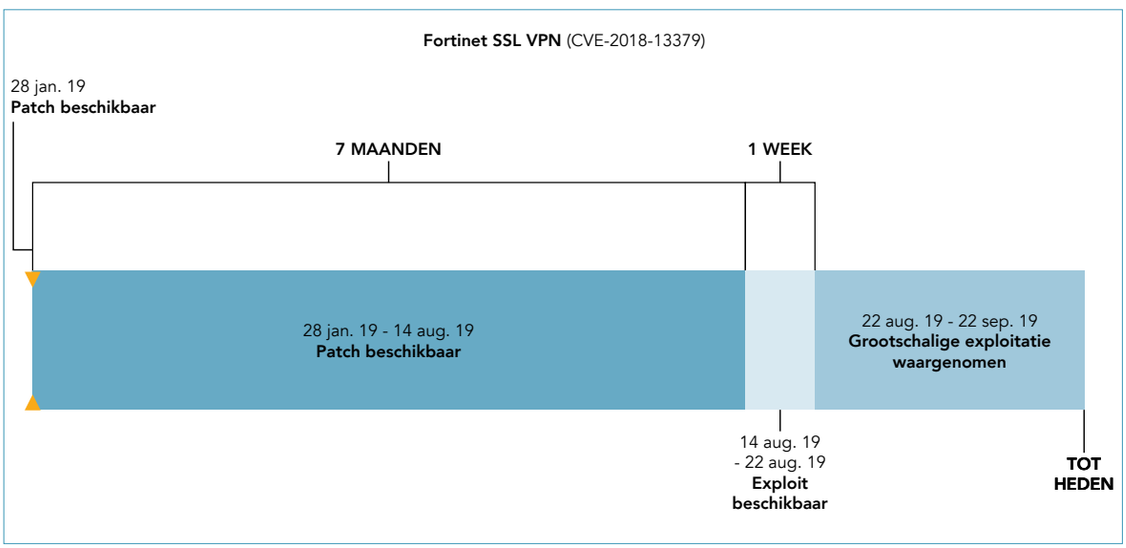
- het onderzoek moet gericht zijn op het verklaren van het ongeval en het reflecteren op gehanteerde uitgangspunten (dubbelslagsleren) en op de mate waarin de organisatie in staat is om te leren (drieslags of deutero-leren), dus verder gaan dan toetsen aan normen en standaarden (enkelslagsleren);[249]
- de scope van het onderzoek moet voldoende breed zijn om de factoren die bijdroegen aan het voorval in beeld te krijgen.

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

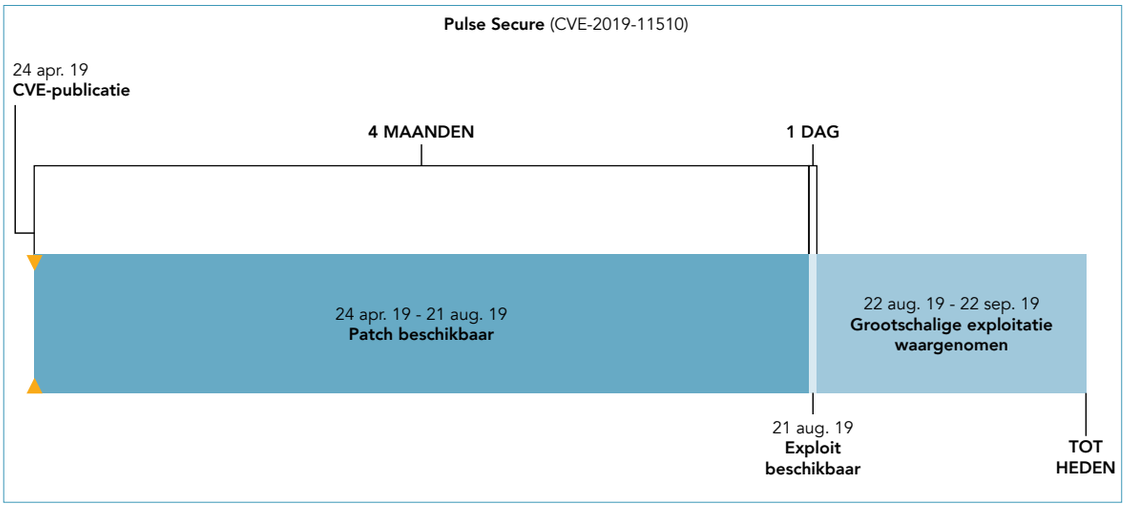
TIJDLIJN PER KWETSBAARHEID



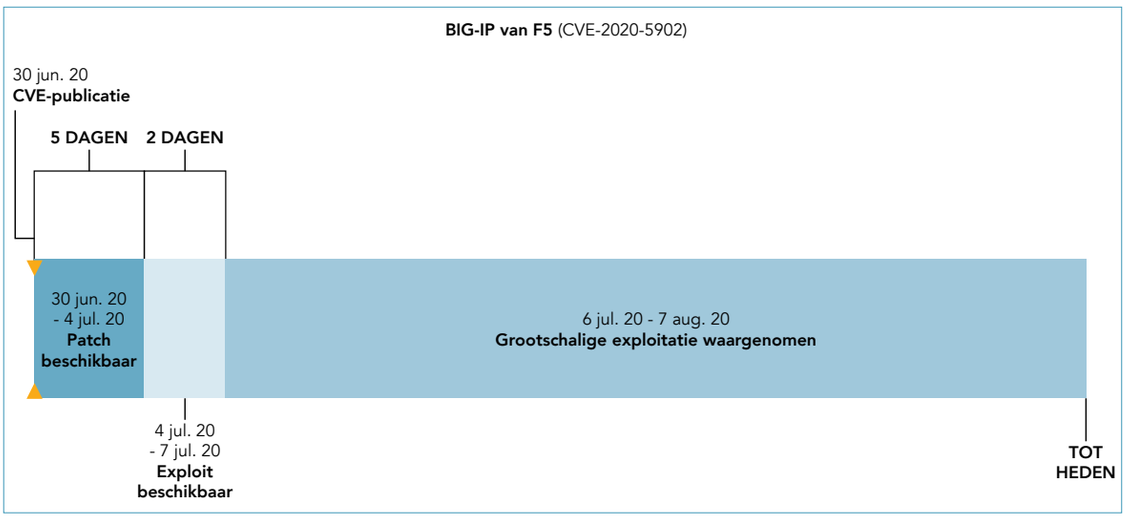
Figuur 19: Tijdlijn Citrix NetScaler ADC en Gateway.



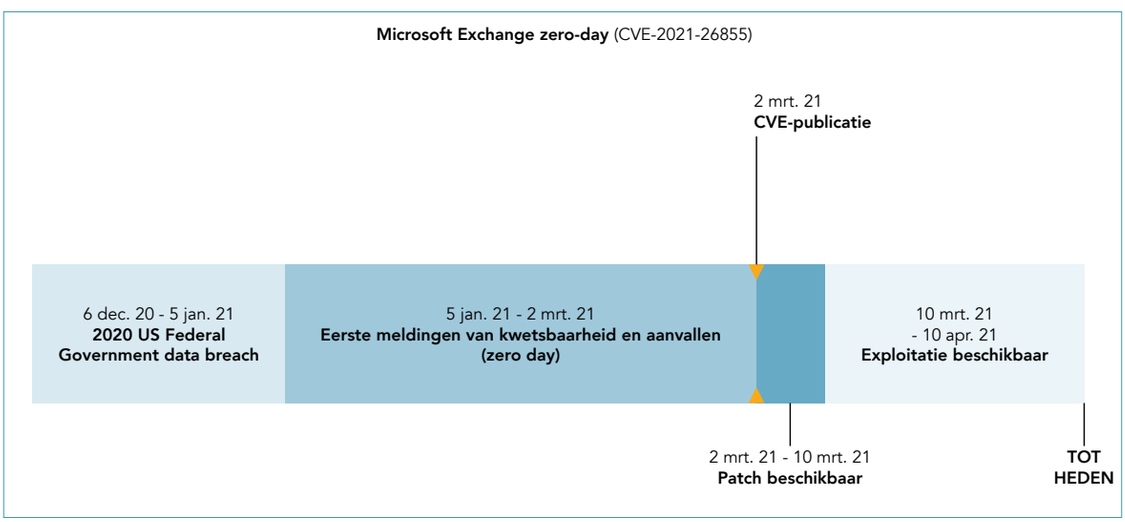
Figuur 20: Tijdlijn Fortinet SSL VPN.



Figuur 21: Tijdlijn Pulse Secure VPN.



Figuur 22: Tijdlijn F5 BIG-IP.



Figuur 23: Tijdlijn Microsoft Exchange.

Over de gebeurtenissen rondom het voorval met de kwetsbaarheid in software van Palo Alto (CVE 2019-1579) was onvoldoende openbare informatie beschikbaar om een tijdlijn te kunnen opstellen.

BERICHTEN NCSC

Doelgroepbericht NCSC (16 januari 2020)
Situatie: Het NCSC heeft eerder gewaarschuwd voor een ernstige kwetsbaarheid in Citrix ADC en Citrix Gateway servers, voorheen bekend als Citrix Netscaler[1,2,3]. Citrix adviseert op zijn website mitigerende maatregelen voor deze kwetsbaarheid. Er heerst momenteel onduidelijkheid over de effectiviteit van de eerder door Citrix geadviseerde mitigerende maatregelen. Dit geldt voor alle versies van Citrix ADC en Citrix Gateway servers. Citrix bevestigt sinds vandaag op zijn website dat deze maatregelen in ieder geval niet werken voor versie 12.1 (builds voor 51.16/51. 19 en 50.31)[4].

Advies: Het NCSC benadrukt dat er op dit moment voor alle versies van Citrix ADC en Citrix Gateway servers geen goede, gegarandeerd betrouwbare oplossing is. Tot het moment dat een patch beschikbaar is[5], adviseert het NCSC om inzichtelijk te maken wat de impact is van het uitzetten van de Citrix ADC en Gateway servers. Afhankelijk van de impact, adviseert het NCSC te overwegen de Citrix ADC en Gateway servers uit te zetten.

Indien de impact van het uitzetten van de Citrix ADC en Gateway servers niet acceptabel is, is het advies om intensief te monitoren op mogelijk misbruik. Als laatste risico-beperkende maatregel kunt u nog kijken naar het whitelisten van specifieke IP-adressen of IP-blokken. Gebruikt u versie 12.1? Dan adviseert het NCSC om in ieder geval de bovenstaande builds van versie 12.1 zo snel mogelijk te upgraden en toch de mitigerende maatregelen toe te passen. Deze upgrade van versie 12.1, biedt ook geen garantie op een betrouwbare oplossing.

Momenteel is er sprake van actief misbruik van de gevonden kwetsbaarheden. Van kwetsbare systemen is de kans dat deze gecompromitteerd zijn hoog. Wanneer u misbruik constateert, dient u te overwegen of deze onderhevig is aan de meldplicht van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni)[6].

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

Nieuwsbericht NCSC op www.ncsc.nl (17 januari 2020)
UPDATE: Schakel Citrix-systemen uit waar dat kan of tref aanvullende maatregelen

Nieuwsbericht | 17-01-2020 | 23:09

Het NCSC raadt u aan Citrix ADC en Citrix Gateway servers uit te schakelen. Tot het moment dat een patch beschikbaar is, adviseert het NCSC om inzichtelijk te maken wat de impact is van het uitzetten van de Citrix ADC en Gateway servers.

Het NCSC raadt u in ieder geval aan Citrix ADC en Citrix Gateway servers uit te schakelen, als uw organisatie niet voor donderdag 9 januari 2020 door Citrix geadviseerde mitigerende maatregelen heeft getroffen. Kan uw organisatie haar primaire proces/taak niet meer uitvoeren wanneer u Citrix ADC en Citrix Gateway servers uitschakelt? Weeg dan het belang van continuïteit van primaire processen af tegen eventuele schade. Indien uw organisatie besluit Citrix ADC en Citrix Gateway servers niet uit te schakelen, adviseert het NCSC met klem dan wel aanvullende maatregelen te treffen (zie hieronder) en intensief te monitoren. Dit ter aanvulling op de maatregelen die Citrix op haar website adviseert.

17 januari 2020, 23:09 uur: Update nieuwsbericht.
17 januari 2020, 10:08 uur: Update nieuwsbericht.
16 januari 2020, 17:22 uur: Publicatiedatum en -tijd eerste versie nieuwsbericht.

Aanvullende mitigerende maatregelen
Mocht het upgraden van uw Citrix-server niet mogelijk zijn en wilt u uw omgeving via internet bereikbaar houden, dan raadt het NCSC aan onderstaande aanvullende maatregelen toe te passen:

IP-whitelisting
Het alleen toestaan van verbindingen van bekende ip-adressen is zeer effectief tegen aanvallers van buitenaf. Dit vereist echter een intensieve beheerinspanning die toeneemt met de omvang van uw organisatie.

Webapplicatiefirewall instellen
Door de Citrix-server achter een webapplicatiefirewall te plaatsen is het mogelijk om filterregels toe te passen die het lastiger kunnen maken voor een kwaadwillende om een aanval uit te voeren.

Clientcertificaten toepassen
Door authenticatie met clientcertificaten te verplichten kan een ongeauthentiseerde kwaadwillende de aanval niet uitvoeren. Het aanmaken en verspreiden van deze certificaten is echter wel een omvangrijke onderneming.

Poort aanpassen
Door het aanpassen van de poort waarop de dienst beschikbaar is, wordt de kans kleiner dat een aanvaller na brede internetscans uw server vindt. Dit betekent dat deze nieuwe poort door alle eindgebruikers ingesteld moet worden.
Dit vereist communicatie en kan een zwaardere last op de helpdesk opleveren. Let op dat het aanpassen van de poort alleen bescherming biedt tegen ontdekking via brede scans, en geen bescherming tegen de aanval als de server toch gevonden wordt. Bovendien zijn er inmiddels waarschijnlijk al diverse scans uitgevoerd en is de kans aanwezig dat uw server al is geïdentificeerd door kwaadwillenden.

ONDERZOEKSRAAD
VOOR VEILIGHEID

Bezoekadres
Lange Voorhout 9
2514 EA Den Haag
T 070 333 70 00
F 070 333 70 77

Postadres
Postbus 95404
2509 CK Den Haag

www.onderzoeksraad.nl