Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland

CSBN 2020

Cybersecuritybeeld Nederland

CSBN 2020

Colofon

Het Cybersecuritybeeld Nederland 2020 (CSBN 2020) biedt inzicht in de digitale dreiging en de belangen die daardoor kunnen worden aangetast. Het gaat ook in op de weerbaarheid tegen de digitale dreiging en op de digitale risico's. Het accent ligt daarbij op de nationale veiligheid. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) vastgesteld.

De NCTV beschermt Nederland tegen bedreigingen die de maatschappij kunnen ontwrichten. Samen met zijn partners binnen overheid, wetenschap en bedrijfsleven zorgt de NCTV ervoor dat de Nederlandse vitale infrastructuur veilig is én blijft. De NCTV is binnen de rijksoverheid verantwoordelijk voor terrorismebestrijding, cybersecurity, nationale veiligheid, crisisbeheersing en statelijke dreigingen. Samen met zijn partners uit het veiligheidsdomein maakt de NCTV zich sterk voor een veilig en stabiel Nederland. De focus ligt op het voorkomen en beperken van maatschappelijke ontwrichting.

Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC draagt bij aan het vergroten van de digitale weerbaarheid van de Nederlandse samenleving, specifiek de digitale weerbaarheid van Rijk en vitale aanbieders.

Het CSBN is opgesteld door de NCTV en het NCSC. Daarbij is dankbaar gebruik gemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen.

Inhoud

Digitale risico's staan niet los van andere risico's

Cyberincidenten kunnen maatschappij verlammen

Net als het coronavirus kunnen cyberincidenten onze maatschappij in het hart raken en gedurende korte of langere tijd verlammen. Nederland is sterk afhankelijk van digitale diensten, processen en systemen. Die raken steeds nauwer verweven met fysieke processen, activiteiten en apparaten én ze maken deel uit van een groter geheel, de mondiale digitale ruimte. Naast de vele kansen die de digitale ruimte biedt, maakt die ons ook kwetsbaar voor menselijk en technisch falen én voor kwaadwillenden. Wereldwijd misbruiken allerlei actoren de digitale ruimte voor cyberaanvallen en het is potentieel een terrein voor conflicten tussen staten. Digitale weerbaarheid blijkt nog niet overal op orde. Als landen en organisaties daarin tekort schieten, dan heeft dat ook gevolgen voor anderen. Landen en organisaties die hun digitale weerbaarheid wel op peil hebben, kunnen alsnog in de problemen komen door cyberincidenten bij anderen. Vergroting van de digitale weerbaarheid is het belangrijkste instrument om digitale risico's te beheersen. Dat is zeker niet alleen een vraagstuk voor technische experts. Het is ook, of wellicht vooral, een vraagstuk van governance en/of risicomanagement voor bestuurders.

Digitale risico's onverminderd groot

Een digitaal risico is de kans dat een cyberincident zich voordoet en de impact daarvan op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid. De digitale risico's voor Nederland zijn onverminderd groot en niet fundamenteel veranderd. Vanuit het perspectief van nationale veiligheid gaat het vooral om de risico's van (voorbereidingen voor) sabotage en spionage door statelijke actoren. Ook bestaat het risico van (grootschalige) uitval van digitale diensten, processen of systemen. Verder is er het risico van cyberaanvallen door criminele actoren die het te doen is om economisch gewin. Afpersing door de inzet van ransomware blijkt succesvol. Mogelijk is er onder criminelen sprake van toenemende intenties en capaciteiten om procesbesturingssystemen van vitale processen te raken. Ransomware, maar ook informatiediefstal of digitale manipulatie door criminelen heeft primair impact op de organisatie die daarvan het slachtoffer is. Toch ondervinden ook andere diensten, processen, systemen en organisaties die daarvan afhankelijk zijn of daarmee in verbinding staan de – potentieel dus ook voor de maatschappij cruciale - gevolgen.

Digitale dreiging permanent

Met digitale dreiging wordt een cyberincident bedoeld dat zich kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten. Het kan daarbij gaan om zowel een cyberaanval als uitval door bijvoorbeeld technisch of menselijk falen.

Net als in 2019 kan ook nu worden geconcludeerd dat de digitale dreiging een permanent karakter heeft en dat cyberincidenten kunnen leiden tot maatschappij-ontwrichtende schade. Hoewel maatschappelijke ontwrichting door cyberincidenten zich in Nederland nog niet heeft voorgedaan, valt dat in de toekomst niet uit te sluiten. Vooral de criminele cyberaanvallen op de gemeente Lochem en de Universiteit Maastricht laten zien hoe groot de gevolgen kunnen zijn voor organisaties, hun medewerkers en

burgers. Ook uitval van systemen had maatschappelijke gevolgen. Zo leidde een storing bij KPN tot onbereikbaarheid van 112, waardoor onder andere politie en ambulances enige tijd verminderd bereikbaar waren.

Digitale veiligheid randvoorwaarde voor functioneren maatschappij

Digitale veiligheid gaat om het ongestoord kunnen functioneren van digitale diensten, processen en onderliggende systemen. Dat is onlosmakelijk verbonden met de nationale veiligheid. Dit geldt in het bijzonder voor digitale veiligheid van vitale processen en voor de (mondiale) digitale ruimte[1], hét digitale fundament van onze maatschappij. Het is tegelijkertijd een ruimte die actoren mondiaal misbruiken voor cyberaanvallen en het is potentieel terrein voor conflicten tussen staten. Vitale processen zijn eveneens essentieel voor de maatschappij én doelwit van (vooral) statelijke actoren tijdens of ter voorbereiding op conflicten. De digitale ruimte en vitale processen zijn nauw met elkaar verweven. Zo geven enkele vitale processen de digitale ruimte mede vorm, waaronder 'Internet en datadiensten'. Andere zijn randvoorwaardelijk, zoals 'Landelijk transport en distributie elektriciteit'. Andersom zijn vitale processen vrijwel volledig gedigitaliseerd en daarmee ook afhankelijk van de digitale ruimte. Eveneens van belang is de digitale veiligheid van andere voor de maatschappij cruciale organisaties, diensten en processen. Dat geldt bijvoorbeeld voor kennisintensieve bedrijven die mondiaal toonaangevend zijn, maar zeker ook die van ogenschijnlijk minder belangrijke organisaties of processen: digitale risico's staan niet los van elkaar en kwetsbaarheden bij de een kunnen gevolgen hebben voor de ander.

Digitale weerbaarheid nog niet overal op orde

Digitale weerbaarheid is een complex begrip. Het gaat in essentie over het vermogen om digitale risico's in voldoende mate te kunnen beheersen. Organisaties blijken dagelijks in staat cyberincidenten te voorkomen of de impact daarvan te verkleinen. Partijen werken samen om digitale weerbaarheid te verhogen. Bestuurders voelen zich verantwoordelijk voor beheersing van digitale risico's.

Digitale weerbaarheid is echter nog niet overal op orde. Daardoor zijn partijen extra kwetsbaar voor cyberincidenten. Dat geldt zeker wanneer er onvoldoende basismaatregelen zijn getroffen, om eerste barrières op te werpen tegen cyberaanvallen, schade te beperken en herstel eenvoudiger te maken wanneer incidenten zich toch voordoen. Tegelijkertijd blijft weerbaarheid tegen cyberincidenten een weerbarstige opgave. Digitale diensten en processen zijn onderling verweven. Systemen bestaan uit vele componenten van hard- en software en zijn verbonden met allerlei andere systemen. Er zijn onveilige producten en diensten in de markt. 'Gebruikers' gedragen zich in de digitale ruimte (onbewust) niet veilig. Dit alles introduceert potentiële kwetsbaarheden die niet alleen de gelegenheid bieden voor cyberaanvallen, maar ook kunnen leiden tot uitval.

Een compleet en scherp beeld van de digitale weerbaarheid van vitale processen en bijbehorende systemen ontbreekt (nog). De toezichthouders op aanbieders van vitale processen schetsen een divers beeld. Sommige instellingen zijn voldoende in control, andere niet. Ook blijkt informatiebeveiliging van ministeries en sommige rijksorganisaties nog niet op orde te zijn.

Digitale risico's staan niet los van andere risico's

Digitale risico's van een land, sector of partij zijn met elkaar en met andersoortige risico's verbonden. Digitale diensten, processen en systemen maken onderdeel uit van een groter geheel, de mondiale digitale ruimte. De financiële crisis van 2008 en de COVID-19 pandemie in 2020 (hebben) laten zien dat incidenten snel en op grote schaal wereldwijd kunnen doorwerken naar andere domeinen en de samenleving en economie in het hart kunnen raken. Ook cyberincidenten kunnen dat effect hebben. Dat geldt zeker wanneer incidenten zich op grote schaal gelijktijdig, opeenvolgend of samen met andere incidenten zouden voordoen. Een combinatie van een grootschalig cyberincident en de COVID-19 pandemie zou bijvoorbeeld grote gevolgen hebben. Dankzij digitalisering kunnen commerciële, educatieve en sociale activiteiten die anders volledig stil zouden vallen door de pandemie, deels toch doorgaan. De keerzijde is dat de digitale ruimte zwaarder dan ooit is belast. Grootschalige digitale uitval zou de maatschappij nu nog meer schade berokkenen dan zonder pandemie. Ook geopolitieke ontwikkelingen, zoals een handelsembargo, beïnvloeden digitale risico's.

Als de digitale weerbaarheid van landen of organisaties tekort schiet, dan heeft dat ook gevolgen voor andere landen en organisaties. Als landen of organisaties hun digitale weerbaarheid wel op peil hebben, dan nog kunnen ze in de problemen komen door cyberincidenten bij anderen. De eind 2019 gepubliceerde kwetsbaarheden in Citrix ADC en Gateway servers zijn illustratief. Die kwetsbaarheden creëerden wereldwijd een risico voor misbruik door aanvallers. In Nederland zou het zijn gegaan om honderden, mogelijk meer dan 3700, organisaties, waaronder aanbieders van vitale processen. Als zich een grote stroomstoring of een storing bij een landelijke telecomprovider voordoet, dan komen digitale processen snel tot stilstand. Daar komt bij dat het voor producenten, werknemers en consumenten lang niet eenvoudig is om veilig activiteiten te ontplooien in de digitale ruimte: tal van gevaren, zoals malafide websites, liggen op de loer.

1 De digitale ruimte is de complexe omgeving die het resultaat is van de interactie tussen mensen, software en diensten op het internet, ondersteund door wereldwijd gedistribueerde fysieke informatie- en communicatietechnologie (ICT) -apparaten en verbonden netwerken. De digitale ruimte wordt ook wel omschreven als het 'digitale domein' of 'cyberspace'.

Vergroting weerbaarheid belangrijkste instrument om digitale risico's te beheersen

Vergroting van digitale weerbaarheid blijft het belangrijkste instrument om digitale risico's in voldoende mate te kunnen beheersen. Zowel de kans dat cyberincidenten zich voordoen, als de impact ervan, kunnen zo worden verkleind. Digitale weerbaarheid kan vergroot worden met technische, procedurele of organisatorische maatregelen. Andere manieren zijn bijvoorbeeld wetgeving, subsidieverlening, scholing om gebruikers te bekwamen in veilig gedrag, voorlichtings- en bewustwordingscampagnes, samenwerking tussen partijen en normerende kaders voor digitalisering van diensten en processen en het ontwerp van systemen.

Er zijn diverse redenen waardoor veiligheid van de digitale ruimte niet vanzelf tot stand komt. Mondiaal spelen vele partijen een rol bij het veilig maken en houden daarvan. Digitale risico's, zeker van het grotere geheel, lijken soms te worden onderschat. Individuele partijen hebben lang niet altijd 'prikkels' om bij te dragen aan de veiligheid van het geheel. Zo kunnen kwetsbare plekken ontstaan. De mogelijkheden voor de Nederlandse overheid en Nederlandse partijen om mondiaal digitale veiligheid te bewerkstelligen zijn logischerwijze beperkt. Daar komt bij dat risico's voor de gehele digitale ruimte en de doorwerking daarvan op de maatschappij lastig zijn te doorgronden. Dat maakt de beoordeling van risico's complex evenals de afweging om wel of geen maatregelen te treffen om risico's te beheersen. Ook is niet op voorhand helder welke partijen de prikkels, mogelijkheden en bereidheid hebben om risico's te beperken.

Het vergroten van digitale weerbaarheid is zeker niet alleen een opgave voor technische experts. Het is ook, of wellicht vooral, een vraagstuk van governance en/of risicomanagement voor bestuurders van organisaties en (groepen van) landen.

Dreiging, belang en weerbaarheid bepalen risico

1 Inleiding

Doel en hoofdvragen

Het Cybersecuritybeeld Nederland 2020 (CSBN 2020) biedt inzicht in de digitale dreiging en de belangen die daardoor kunnen worden aangetast. Het gaat ook in op de weerbaarheid tegen de digitale dreiging en op de digitale risico's. Het accent ligt daarbij op de nationale veiligheid.

De hoofdvragen van het CSBN 2020 zijn:

- Wat is in de periode 1 januari 2019 t/m februari 2020 opgevallen over: a) cyberincidenten, b) de weerbaarheid daartegen en c) de belangen die daardoor zijn of kunnen worden aangetast?
- Welke bredere ontwikkelingen hebben naar verwachting de komende jaren invloed op digitale veiligheid?
- Welke digitale dreigingen kunnen de nationale veiligheid aantasten, van wie of wat gaan die uit en waartegen zijn die gericht?
- Welke belangen kunnen worden aangetast wanneer cyberincidenten zich voordoen, wat kan de impact daarvan zijn en in hoeverre houden partijen daar in hun belangenafweging rekening mee?
- Wat is de mate van weerbaarheid van Nederland tegen die digitale dreigingen?

Toelichting begrippen

Aan de analyse in het CSBN liggen primair de invalshoeken dreiging, belang en weerbaarheid ten grondslag (zie hieronder). Deze drie bepalen in samenhang het digitale risico. Wanneer bijvoorbeeld de digitale dreiging toeneemt bij een gelijkblijvend niveau van weerbaarheid, dan neemt per saldo het risico toe: de kans of impact van cyberincidenten wordt groter. Wanneer het belang toeneemt, bijvoorbeeld doordat Nederland nog meer processen digitaliseert, kan per saldo het risico toenemen bij een gelijkblijvend niveau van weerbaarheid en dreiging. De impact van cyberincidenten kan immers toenemen als gevolg van de toegenomen afhankelijkheid. Of partijen de weerbaarheid wel of niet willen verhogen, hangt mede samen met de afweging van het digitale risico en andere belangen. Dit is een vraagstuk van governance en/of risicomanagement.

Sleutelbegrippen

Dreiging: een cyberincident dat zich kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten. In het CSBN gaat het primair om dreigingen die nationale veiligheidsbelangen kunnen aantasten.
Belang: waarden, verworvenheden, materiële en immateriële zaken waaraan schade kan ontstaan als een cyberincident zich voordoet en het gewicht dat de maatschappij of een partij aan de verdediging ervan toekent. In het CSBN ligt het accent op nationale veiligheidsbelangen.
Weerbaarheid: het vermogen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.
Digitale risico('s): de kans dat een cyberincident zich voordoet en de impact daarvan, beide in relatie tot het niveau van de actuele weerbaarheid.
Cyberincident: alle gebeurtenissen of activiteiten die de beschikbaarheid, integriteit of vertrouwelijkheid aantasten van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen. Het kan daarbij gaan om zowel een cyberaanval, een moedwillige activiteit van een cyberactor, als uitval door bijvoorbeeld technisch of menselijk falen.
Digitale ruimte: de digitale ruimte is de complexe omgeving die het resultaat is van de interactie tussen mensen, software en diensten op het internet, ondersteund door wereldwijd gedistribueerde fysieke informatie- en communicatietechnologie (ICT) -apparaten en verbonden netwerken.[II] De digitale ruimte wordt ook wel omschreven als het 'digitale domein' of 'cyberspace'.
Cybersecurity: het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan.

II Betreft (vertaling van) definitie van cyberspace zoals opgenomen in ISO/IEC standard 27032: 2012 (E).

Afbakening

Digitalisering biedt vele kansen en leent zich potentieel voor allerlei vormen van misbruik. Het CSBN richt zich, zoals aangegeven in het doel en de hoofdvragen, níét op de kansen van digitalisering. Het CSBN richt zich evenmin op alle denkbare vormen van misbruik, zoals blijkt uit de hierboven toegelichte sleutelbegrippen. Zo valt propaganda door terroristen buiten de afbakening. Datzelfde geldt voor bepaalde vormen van cybercriminaliteit. Het CSBN richt zich wel op criminaliteit waarbij ICT het doelwit is van aanvallen met behulp van ICT (computer-focused crime). Deze afbakening betekent zeker niet dat andere vormen van misbruik niet belangrijk zijn.

Wijze van totstandkoming

Het CSBN 2020 is tot stand gekomen op basis van de inzichten en expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen. Ook is gebruik gemaakt van open bronnen. Het CSBN 2020 is opgesteld door de NCTV en het NCSC. In opdracht van de NCTV heeft TNO in december 2019 partners van de NCTV en het NCSC gevraagd online input te leveren voor het hoofdstuk Jaarbeeld. TNO heeft verder het hoofdstuk Dreigingsscenario's opgesteld onder hoofdredactionele verantwoordelijkheid van de NCTV. Het monitoren van cyberincidenten, dreigingen, belangen en weerbaarheid is een continu proces, met het CSBN als een van de jaarlijkse resultaten. Zaken die ten opzichte van vorige edities van het CSBN niet of nauwelijks zijn veranderd, zijn niet of slechts beknopt beschreven.

Leeswijzer

Hoofdstuk 2 beschrijft het jaarbeeld: een terugblik wat van januari 2019 t/m februari 2020 is opgevallen. Ook wordt kort stilgestaan bij het inspelen van actoren op de COVID-19 pandemie. Hoofdstuk 3 geeft een vooruitblik op basis van bredere ontwikkelingen die van invloed kunnen zijn op digitale veiligheid. In hoofdstuk 4 wordt de dreiging voor de nationale veiligheid nader beschreven en toegelicht. Hoofdstuk 5 gaat in op belangen die kunnen worden aangetast wanneer cyberincidenten zich voordoen, wat de impact daarvan kan zijn en in hoeverre partijen in hun belangenafweging daarmee rekening houden. De weerbaarheid van Nederland tegen cyberincidenten komt in hoofdstuk 6 aan de orde. Hoofdstuk 7 beschrijft een drietal scenario's die samen een verhaallijn vormen om verder inzicht te geven in specifieke cyberincidenten en de mogelijke gevolgen. U kunt deze scenario's gebruiken om te beoordelen wat bevindingen in dit CSBN voor u of uw organisatie zouden kunnen betekenen vanuit de functie die u bekleedt. Dit hoofdstuk is nieuw ten opzichte van eerdere jaren. De bijlagen geven een toelichting op de gebruikte afkortingen en begrippen en de gebruikte bronnen en referenties.

Cyberincidenten maakten impact en afhankelijkheid duidelijk

2 Jaarbeeld

Maatschappelijke ontwrichting door digitale aanvallen of storingen heeft zich in Nederland niet voorgedaan in 2019 en begin 2020. Wel maakten vooral criminele cyberaanvallen op de gemeente Lochem en de Universiteit Maastricht duidelijk welke impact cyberincidenten kunnen hebben. Naast deze incidenten zijn digitale aanvallen waargenomen van vooral statelijke actoren, als middel voor spionage, sabotage en informatie-operaties, en de inzet van ransomware als middel voor afpersing door criminelen. Uitval van systemen had maatschappelijke gevolgen. Zo leidde een storing bij KPN tot onbereikbaarheid van 112, waardoor onder andere politie en ambulances enige tijd verminderd bereikbaar waren.

De modi operandi en ingezette middelen zijn grotendeels gelijk gebleven. Wel vielen de inzet van ransomware door criminele afpersers en het actieve misbruik van kwetsbaarheden door statelijke en criminele actoren op. Verder bleek dat actoren nog steeds zoeken naar zwakke schakels in de leverancierskete als opstap naar interessante doelwitten. Zeker kwetsbaarheden in Pulse Secure en Fortigate VPN-software en Citrix ADC en Gateway servers maakten duidelijk dat kwetsbaarheden grote gevolgen kunnen hebben.

Cyberaanvallen door vooral statelijke en criminele actoren

Wereldwijd zijn net als eerdere jaren digitale aanvallen waargenomen van statelijke en criminele actoren.

Spanningen tussen mogendheden kregen vervolg in de digitale ruimte

Geopolitieke ontwikkelingen werken door in de digitale ruimte en kunnen direct of indirect impact hebben op Nederland.[1] Conflicten spelen zich voor een steeds groter deel in het grijze gebied tussen oorlog en vrede en op verschillende fronten af. Wedijver over het mondiale of regionale leiderschap voltrekt zich steeds meer in ook niet-militaire domeinen, waaronder het digitale. Een cyberaanval kan grote politieke, militaire en economische schade aanrichten.[2]

AIVD en MIVD: digitale spionage onderkend tegen Nederland

Landen spioneren om hun eigen politieke, militaire, economische en/of ideologische doelen te bereiken. Uit onderzoek van de AIVD blijkt dat steeds meer landen politiek en/of economisch spioneren. Statelijke actoren blijven zeer succesvol in het compromitteren van (overheids)systemen binnen en buiten Nederland. Dit ondanks investeringen in de digitale weerbaarheid van publieke instellingen.[3] Ook de MIVD onderkende in 2019 diverse cyberspionage-activiteiten tegen Nederland, andere westerse landen en bondgenootschappelijke belangen.[4]

De door politieke spionage verkregen inlichtingen dienen als voorkennis voor staten om voorbereid te zijn op politieke of maatschappelijke ontwikkelingen. Deze inlichtingen kunnen ook worden ingezet om besluitvorming en verkiezingen te beïnvloeden of om grip te krijgen op de diaspora. Zo worden inlichtingen verzameld om landen tegen elkaar uit te spelen om de eenheid en de internationale samenwerking binnen de Noord-Atlantische Verdragsorganisatie en Europese Unie te ondermijnen.[5]

Nederland is doelwit van economische spionage. De Nederlandse economie is immers hoogontwikkeld, innovatief en internationaal georiënteerd. Spionageactiviteiten zijn bijvoorbeeld gericht op het verbeteren van de eigen economische ontwikkeling of om kennis te bemachtigen door landen die te maken hebben met sancties.[6]

AIVD en MIVD: digitale sabotage een van de grootste cyberdreigingen

De AIVD en MIVD beschouwen de mogelijke digitale verstoring en sabotage van de vitale infrastructuur als een van de grootste cyberdreigingen voor Nederland en zijn bondgenoten.[7] Meerdere staten hebben bewezen de capaciteiten en de bereidheid te hebben om digitale sabotage in te zetten om hun geopolitieke doelstellingen te bereiken. De AIVD constateert al langere tijd dat sommige van deze staten voorbereidingen treffen om digitale sabotage voor toekomstig gebruik mogelijk te maken. Deze voorbereidingen bestaan uit het zich innestelen in ICT-systemen van onder meer vitale infrastructuur. Ook de MIVD onderkende in 2019 diverse voorbereidende sabotageactiviteiten gericht tegen westerse landen en bondgenootschappelijke belangen.[8] Momenteel ontbreekt het staten aan de intentie om digitale sabotage tegen Nederland in te zetten. Deze intentie is echter veranderlijk en afhankelijk van geopolitieke ontwikkelingen.[9]

Informatie-operaties door statelijke actoren

Enkele landen gebruiken informatie-operaties als instrument in hybride conflicten. Via die operaties proberen ze verdeeldheid te zaaien over onderwerpen die bij de verschillende doellanden of bondgenootschappelijke organisaties gevoelig liggen. Maatschappelijke polarisatie en de versplintering van het politieke landschap in een groot aantal landen vormen een voedingsbodem daarvoor. Onderzoek van de MIVD bracht in 2019 informatie-operaties gericht tegen Nederland, andere westerse landen en bondgenootschappelijke belangen aan het licht.[10]

Cyberaanvallen vormen aantrekkelijk verdienmodel voor criminelen

Cyberaanvallen zijn het afgelopen jaar veelvuldig (succesvol) ingezet door cybercriminelen voor afpersing, informatiediefstal en CEO-fraude[III]. Het is voor hen een aantrekkelijk verdienmodel.[11] Afpersing blijkt succesvol te zijn door de inzet van ransomware (zie Inzet van ransomware als middel voor afpersing).

Mogelijke nieuwe vormen van samenwerking topsegment cybercriminelen

De politie ziet een mogelijk nieuwe vorm van interactie tussen verschillende groepen binnen het topsegment van cybercriminelen. Voorheen opereerden deze groepen redelijk autonoom en voerden ze vele processtappen eigenstandig uit. Nu lijkt er sprake te zijn van samenwerking tussen specifieke groepen. Zowel de politie als een aantal beveiligingsbedrijven vinden het aannemelijk dat sommige criminele actoren binnen het topsegment toegang tot bedrijfsnetwerken onderling verhandelen, nadat ze deze hebben gecompromitteerd en beoordeeld op de waarde.[12]

Statelijke actor combineert spionage en cybercrime

In 2019 bleek een staatsgelieerde hackersgroep zich bezig te houden met zowel spionage als financieel gemotiveerde operaties.[13] Criminelen gebruiken vaak dezelfde (openbare) middelen als statelijke actoren en vice versa. In het verleden hebben staatsgelieerde actoren uit een ander land zich ook met financieel gemotiveerde aanvallen bezig gehouden.

Modi operandi en ingezette middelen grotendeels gelijk gebleven

Inzet van ransomware als middel voor afpersing

Steeds vaker wordt waargenomen dat criminele actoren ransomware zodanig inzetten dat zij het slachtoffer onder druk kunnen zetten om tot betaling van losgeld over te gaan. Het gaat de actoren vooral om organisaties die de mogelijkheid hebben om grotere geldbedragen te betalen[14] en/of waarvoor bedrijfscontinuïteit en waardevolle unieke data een belangrijke rol spelen. Kenmerkend voor de werkwijze is de uitgebreide verkenning van het bedrijfsnetwerk. Dit stelt de actor in staat om de waarde van de data en de schade voor het slachtoffer in te schatten en om de ransomware op de meest effectieve wijze te plaatsen. Op basis van dat inzicht varieert het gevraagde losgeld van enkele tienduizenden tot miljoenen euro's.[15] Er lijkt een toename te zijn van ransomware-aanvallen waarbij data niet alleen versleuteld wordt, maar ook gekopieerd. Wanneer een organisatie het losgeld niet wilde betalen, dan publiceerden criminelen in sommige gevallen de data.[16]

Begin februari 2020 publiceerden cybersecurity experts over nieuwe ransomware, genaamd EKANS, die zich richt op industriële controlesystemen (ICS) en zou zijn ontwikkeld door criminelen. Deze systemen worden gebruikt voor bijvoorbeeld de drinkwater- en energievoorziening. De aanvalsmethode is relatief eenvoudig, maar de ransomware lijkt speciaal ontwikkeld om ICS aan te vallen. Tot de slachtoffers van EKANS behoren waarschijnlijk de staatsoliemaatschappij van Bahrein en bedrijven in de maakindustrie. EKANS is mogelijk de eerste ICS-gerichte ransomware die het werk is van een criminele actor.[17]

III CEO-fraude is een vorm van Business Email Compromise (BEC)-fraude, waarbij getracht wordt een medewerker te misleiden om geld over te maken naar een rekening van een crimineel.

Inzet van ransomware veroorzaakt wereldwijd financiële schade

In maart 2019 werd bekend dat het Noorse energie- en aluminiumconcern Hydro besmet was geraakt met de LockerGoga-ransomware.[18] Hydro, dat ook vestigingen in Nederland heeft, werd door de aanval gedwongen om op verschillende locaties in Europa en de Verenigde Staten de productie stop te zetten en waar mogelijk over te schakelen op handmatige bediening.[19] De herstelwerkzaamheden hebben lang geduurd en de financiële schade voor het concern in de eerste helft van 2019 alleen al wordt geschat op 55 tot 66 miljoen euro.[20]

In Nederland is het NCSC in samenwerking met (inter)nationale partners in maart 2019 gestart met een aan de LockerGoga-ransomware gerelateerd onderzoek. Daaruit is naar voren gekomen dat de actoren meerdere ransomwarevarianten gebruikten, waaronder MegaCortex, Ryuk en Maze. Gebleken is dat er een grote tijdsspanne (maanden) kan zitten tussen het tijdstip van binnendringen en de inzet van de ransomware. Vermoedelijk gebruiken de aanvallers deze tijd om informatie over de organisatie te verzamelen om vervolgens een op de organisatie afgestemd bedrag als losgeld te kunnen eisen. Andere motieven, zoals spionage en sabotage, zijn echter niet uit te sluiten. Waar mogelijk zijn (potentiële) slachtoffers op de hoogte gebracht, zodat zij maatregelen konden treffen om verdere schade te voorkomen. Het aantal slachtoffers in Nederland was medio 2019 beperkt. Er waren geen slachtoffers binnen de vitale infrastructuur en de rijksoverheid bekend.

Ransomware-aanval Universiteit Maastricht

De Universiteit Maastricht werd op 23 december 2019 slachtoffer van een ransomware-aanval. De aanvaller verkreeg toegang tot het netwerk van de universiteit, nadat medewerkers twee maanden eerder de link in een phishing e-mail hadden geopend. Nadat toegang was verkregen, heeft de aanvaller meerdere servers gecompromitteerd en het netwerk verkend om zo de toegang tot het netwerk te vergroten. Het is de aanvaller gelukt om volledige administratie-rechten te krijgen over servers van de universiteit doordat twee servers een zeer belangrijke beveiligingsupdate van mei 2017 misten.[24]

Op 23 december 2019 heeft de aanvaller op een deel van de servers de Clop-ransomware uitgerold. Bestanden werden versleuteld op minimaal 267 servers. Daardoor waren onder andere e-mails, onderzoeken en computers ontoegankelijk en was een aantal websites niet meer bereikbaar. Omdat ook back-up servers geraakt waren, was het herstel complex. De universiteit besloot om €197.000,- losgeld te betalen aan de (vermoedelijk Russische) criminelen om weer toegang te krijgen tot de versleutelde bestanden.[25] De Universiteit heeft aangifte gedaan bij de politie.

Uit onderzoek naar de ransomware-aanval bleek dat dit *"[....] kon ontstaan door een combinatie van enkele ontbrekende belangrijke beveiligingsupdates, beperkte segmentatie binnen het netwerk, het niet opvolgen van verschillende alarmsignalen en ongelukkig menselijk handelen".*[26]

Generieke malware gebruikt voor de inzet van ransomware-aanvallen

Emotet en Trickbot zijn generieke malwarevarianten die in verband worden gebracht met ransomware-aanvallen.[21] Zij zijn omgezet in multifunctionele aanvalsplatformen die bijvoorbeeld worden gebruikt voor het plaatsen van additionele malware zoals ransomware. De Nederlandse politie ziet dat ransomware het sluitstuk van een cyberaanval kan zijn. Het kan niet worden uitgesloten dat in de tijdsspanne tussen de initiële besmetting en de inzet van ransomware ook andere activiteiten hebben plaatsgevonden. Hierbij kan het bijvoorbeeld gaan om het kopiëren van informatie, of het verzekeren van toegang tot het netwerk op een later moment.[22] In veel gevallen wordt Emotet als opstap gebruikt om Trickbot te installeren.[23] Trickbot is een malwarefamilie die middels losse modules extra functionaliteiten in kan zetten. Daarmee krijgt de aanvaller bijvoorbeeld zicht op de toetsaanslagen en muisbewegingen.

Misbruik van legitieme middelen en generieke diensten

Een van de kernbevindingen van het CSBN 2019 is dat geavanceerde aanvallen tot stand komen met middelen die laagdrempelig te verwerven zijn.[27] Vrij verkrijgbare middelen (voor bijvoorbeeld ICT-beheer) en generieke diensten (bijvoorbeeld publieke cloud- of e-maildienstverlening) worden gebruikt om cyberaanvallen uit te voeren. IBM ziet een toename van het gebruik van legitieme hulpmiddelen in plaats van het gebruik van malware: bij meer dan de helft van de cyberaanvallen (57 procent) werd gebruik gemaakt van algemene beheertoepassingen zoals PowerShell en PsExec.[28] Uit een analyse van beveiligingsbedrijf Positive Technologies naar de middelen die 29 aanvallers momenteel in hun aanvalscampagnes gebruiken, blijkt dat meer dan de helft van hen legitieme, publiek beschikbare penetratietest- en systeembeheertools gebruikt.[29] Een bekend voorbeeld van het misbruik van legitieme middelen is Cobalt Strike.[30] Het gebruik van legitieme middelen en generieke diensten bemoeilijkt zowel detectie als attributie.[31]

Cyberaanval gemeente Lochem via Remote Desktop Protocol (RDP)

Bij een cyberaanval op de gemeente Lochem begin juni 2019 is misbruik gemaakt van een kwetsbaarheid in Remote Desktop Protocol (RDP). RDP wordt gebruikt om computers op afstand te beheren. Bij het incident in Lochem is via brute force-aanvallen op de RDP-poort toegang tot een thuiswerkserver verkregen. Na het inloggen op de server installeerde de aanvaller(sgroep) verschillende applicaties. Hiermee verkreeg hij inzicht in het netwerk en de gebruikers. Ook werd ransomware ingezet waardoor een aantal bestanden werd versleuteld. Na de aanval is besloten om de computersystemen opnieuw in te richten. Zaken als het aanvragen van paspoorten, het registreren van een verhuizing en het aangeven van een geboorte waren hierdoor tijdelijk niet mogelijk. De aanval resulteerde in een schadepost van 200.000 euro.[32]

Actoren spelen in op actualiteit

Actief misbruik van diverse kwetsbaarheden

In 2019 en begin 2020 is actief misbruik waargenomen van verschillende kwetsbaarheden door statelijke en criminele actoren.[33] De AIVD en MIVD bevestigen dat statelijke actoren misbruik hebben gemaakt van kwetsbaarheden in Fortigate en Pulse secure VPN-software. Daarom hebben de AIVD en MIVD ook bedrijven en andere organisaties geadviseerd over maatregelen.[34] De kwetsbaarheden in Citrix ADC en Citrix Gateway servers werden snel na de beschikbare exploit – die op 9 januari 2020 werd gepubliceerd - actief misbruikt door actoren.[35] De AIVD en MIVD bevestigen dat een statelijke actor de publiek gemaakte kwetsbaarheid in Citrix-servers heeft misbruikt bij voorbereidingen voor cyberspionage.[36] Criminelen maakten gebruik van de kwetsbaarheden in Citrix-servers om organisaties met ransomware te infecteren.[37]

Actoren spelen in op Covid-19 pandemie

Al vrij snel na het uitbreken van de Covid-19 pandemie waren er aanwijzingen dat actoren de situatie (opportunistisch) misbruikten om 'gethematiseerde' cyberaanvallen uit te voeren. Zo zijn er cyberaanvallen uitgevoerd op ziekenhuizen, onderzoeksinstituten en de Wereldgezondheidsorganisatie.[38] Maar niet alleen de zorgsector was doelwit, ook overheden[39] en burgers[40] kregen te maken met uiteenlopende cyberaanvallen.[41]

Het wijzigen van DNS-instellingen als aanvalstechniek

Incidenten in deze rapportageperiode geven (hernieuwde) interesse aan in het wijzigen van Domain Name System (DNS)-instellingen[IV] als aanvalstechniek, ook wel bekend als een DNS-hijack.[42] Door DNS-instellingen van organisaties te wijzigen, bijvoorbeeld via het hacken van een registrar, kan inkomend netwerkverkeer tijdelijk omgeleid en onderschept worden. Dit kan onder andere worden gebruikt voor spionagedoeleinden. Cyberaanvallen op DNS kunnen aanzienlijke impact hebben op de integriteit van het internet.[43]

Toename van phishing via sms

Phishing is al jaren een veelgebruikte manier voor onder meer cybercriminelen om doelwitten aan te vallen en is ook dit jaar weer de meest gebruikte – eerste stap voor een - aanvalsmethode.[44] Incidenten laten zien dat criminelen ook een nieuwe vorm gebruiken, namelijk phishing via sms (smishing) of via WhatsApp. Ook spelen zij in op een toenemend gebruik van apps voor een betaalverzoek tussen particulieren via een berichtenapp.[45] Niet uit te sluiten valt dat deze techniek breder wordt ingezet dan alleen voor fraude, bijvoorbeeld voor overname van accounts als opstap voor een grotere aanval. Ook andere actoren zouden deze techniek kunnen inzetten.

Misbruik Nederlandse ICT-infrastructuur

De Nederlandse ICT-infrastructuur wordt ook door statelijke actoren misbruikt bij cyberaanvallen op andere landen. Nederland is hiervoor aantrekkelijk doordat de digitale infrastructuur van hoge kwaliteit is en ICT-capaciteit relatief simpel kan worden gehuurd. Deze vorm van misbruik kan het internationale imago van Nederland schaden en slecht zijn voor bondgenootschappelijke belangen en de integriteit van de Nederlandse ICT-infrastructuur.[46]

De Nederlandse ICT-infrastructuur werd net als eerdere jaren ook voor verschillende manieren van cybercriminaliteit misbruikt, waaronder voor het faciliteren van cyberaanvallen.[47] Nederlandse servers worden ook misbruikt voor botnetspam. Van alle servers die cybercriminelen wereldwijd inzetten voor spammen via botnets, staat ongeveer 6,3 procent in Nederland.[48]

Grotere DDoS-aanvallen

In 2019 heeft de Nationale Beheersorganisatie Internet Providers (NBIP) *"[....] 919 DDoS-aanvallen geregistreerd. In geheel 2018 waren dit er 938. De maximale grootte van een DDoS aanval lag op 124 Gbps, tegenover 2018 met 68 Gbps en in 2017 36 Gbps. Daarmee lag de maximale grootte op bijna 2x keer zoveel als in 2018. In 2019 waren er 29 aanvallen die langer dan 4 uur duurden, tegenover 22 in heel 2018. Ook dit neemt dus toe."* De NBIP ziet *"[....] een trend waarbij grotere DDoS-aanvallen worden ingezet om een service onbereikbaar te maken."*[49] Geraadpleegde experts gaven wel aan dat de gevreesde technische complexiteitsverhoging is uitgebleven.[50] Het Centraal Plan Bureau (CPB) stelt dat DDoS-aanvallen een risico voor Nederland blijven en dat de potentiële financiële gevolgen aanzienlijk kunnen zijn.[51]

IV DNS is het netwerkprotocol dat op internet gebruikt wordt om domeinnamen naar ip-adressen te vertalen en omgekeerd.

Uiteenlopende doelwitten van actoren

Leveranciersketen misbruikt door gecompromitteerde ICT-producten

Actoren gaan meer op zoek naar de zwakke schakel in ketens waar het beoogde doelwit van afhankelijk is. Dat kan een eenvoudigere manier zijn dan een directe aanval op de organisatie waar ze het op voorzien hebben.[52] In deze rapportageperiode zijn vooral aanvallen op veel door organisaties gebruikte producten om toegang te krijgen tot beoogde doelwitten opgevallen. Zo werd begin 2019 een cyberaanval ontdekt waarbij het software-updateprogramma ASUS Live Update is misbruikt om via een malafide update een backdoor te verspreiden.[53] In oktober maakte antivirussoftwarebedrijf Avast bekend dat een actor er in was geslaagd het bedrijfsnetwerk binnen te dringen.[54] Beide aanvallen worden in verband gebracht met aan een staat gelieerde actoren.[55] Vermoedelijk was de actor achter de recente aanval op Avast er op uit om CCleaner te compromitteren als opstap naar andere doelwitten, net als eerder in 2017.[56] Die toegang kan misbruikt worden voor digitale spionage en sabotage. De AIVD wijst op nieuwe risico's op (digitale) spionage als gevolg van onvoldoende beveiligingsmaatregelen bij toeleveranciers. Delen van het productieproces zijn immers door globalisering versplinterd en verspreid over landsgrenzen heen verspreid.[57]

Uiteenlopende sectoren en organisaties doelwit, waaronder vitale

Onderzoek van Ponemon in onder andere het VK, de VS, Duitsland, Mexico, Australië en Japan wijst uit dat ten minste 90% van de onderzochte organisaties met procesbesturingssystemen, waaronder in de sectoren zorg, transport en nutsvoorzieningen, getroffen zijn door een succesvolle cyberaanval.[58] Andere bronnen melden aanvallen op de sectoren energie, nucleair, olie en chemie.[59] Ook Dragos signaleert een toename in zowel de frequentie als de complexiteit van digitale aanvallen op vitale infrastructuur.[60]

Statelijke actoren hebben in het verleden meermaals laten zien over de capaciteit en intentie te beschikken om digitale aanvallen uit te voeren op de vitale infrastructuur of toeleveranciers van (ICS-)systemen[V] die daarin worden gebruikt. Bij een digitale aanval in 2019 op een energieleverancier in het Midden-Oosten is waarschijnlijk gebruik gemaakt van destructieve malware die het mogelijk maakte om harde schijven te herschrijven om zo de computer van gebruikers onbruikbaar te maken.[61] Eerder werd bekend dat een statelijke actor zich ook richt op de leveranciersketen van ICS, wellicht met sabotage als einddoel.[62] De AIVD constateert dat statelijke actoren zich innestelen in ICT-systemen van onder meer vitale infrastructuur.[63]

Wereldwijd zijn meerdere spionagecampagnes waargenomen die waren gericht op organisaties uit verschillende sectoren. Uit onderzoek van de AIVD en MIVD blijkt dat meerdere Nederlandse topsectoren doelwit zijn (geweest) van digitale spionage. Het gaat daarbij vooral om hightech, energie, maritiem en life sciences & health. Doelwitten zijn ook toeleveranciers van Defensie of andere ministeries, vitale sectoren, het verkrijgen van persoonsgegevens en gegevens van andere organisaties, zoals telecomproviders, universiteiten, onderwijsinstellingen, onderzoeksinstituten, denktanks, biotechnologiebedrijven, startups, handel en defensieorderbedrijven.[64] Drie Nederlandse universiteiten en een HBO-instelling waren eind 2019 en begin 2020 doelwit van overheidshackers. Ze zouden academische kennis zoals boeken en lesmateriaal hebben willen stelen.[65] In februari 2020 was een onderzoeksgroep van de Vrije Universiteit kortstondig slachtoffer van een cyberaanval waarbij de aanvaller uiteindelijk verregaande rechten kreeg op een van de servers waar onderzoeksresultaten op staan.[66] In het buitenland zijn aanvallen op Europese ambassades opgevallen.[67] De AIVD meldt dat onder andere ministeries, inlichtingen- en veiligheidsdiensten, politieke partijen en cultureel-maatschappelijke organisaties doelwit waren van politieke spionage.[68]

Naast de financiële sector zijn ook de industriële sector, gemeenten en onderwijsinstellingen doelwit geweest van criminelen in Nederland. In de VS, Frankrijk en Duitsland hebben dergelijke aanvallen op gemeentelijke instellingen en ziekenhuizen geleid tot ernstige verstoring van de publieke dienstverlening.[69]

Diverse kwetsbaarheden met potentieel grote gevolgen

Ook in deze onderzoeksperiode kwamen allerlei kwetsbaarheden, met potentieel grote gevolgen voor vele organisaties, in de publiciteit. Een kwetsbaarheid is een eigenschap die een aanvaller de mogelijkheid biedt een cyberaanval uit te voeren of een eigenschap die kan leiden tot uitval. Dit kan zich voordoen in een digitale dienst, proces of systeem, maar ook in de samenleving als geheel of in een specifieke organisatie.

Kwetsbaarheden hardware met (potentieel) grote gevolgen bekend gemaakt

Het afgelopen jaar liet een verdere groei zien in het aantal kwetsbaarheden in hardware. Een bepaald type aanval (transient execution attack) leidde ook dit jaar weer tot wijzigingen in alle Intel processoren en alle populaire besturingssystemen. SSDs[VI] met hardware encryptie bevatten zulke ernstige kwetsbaarheden dat de encryptie geen enkele waarde heeft. Zelfs nieuw op de markt gekomen geheugenchips (DRAM) blijken nog bekende kwetsbaarheden te hebben. Vooral de 'DRAM-kwetsbaarheid' is zorgwekkend, omdat daar geen oplossing voor is en deze nog jaren aanwezig zal blijven. Alternatieven zijn er op dit moment niet.[70]

V Industriële controlesystemen (ICS) zijn meet- en regelsystemen, bijvoorbeeld voor de aansturing van industriële processen of gebouwbeheersystemen.

VI Een solid state drive (SSD) is een specifiek medium waarop digitaal gegevens bewaard kunnen worden. SSD's worden voornamelijk gebruikt in systemen waar traditioneel een harde schijf gebruikt werd.

Nederlandse organisaties maandenlang kwetsbaar via VPN-servers

In augustus 2019 waarschuwde een beveiligingsonderzoeker dat ernstige beveiligingslekken in VPN-servers van zowel Fortigate als Pulse Secure actief werden misbruikt.[71] Hoewel er voor beide kwetsbaarheden sinds het voorjaar updates beschikbaar waren, waren in augustus nog tal van kwetsbare systemen online. Zo zouden volgens de media verschillende Nederlandse organisaties de twee beschikbare patches voor kwetsbaarheden in Pulse Secure in augustus 2019 nog niet hebben doorgevoerd, waaronder twee onderdelen van het ministerie van Justitie en Veiligheid.[72] De Fortigate kwetsbaarheden stellen een kwaadwillende in staat om aanvallen uit te voeren die mogelijk leiden tot Denial-of-Service (DoS), manipulatie van gegevens en toegang tot gevoelige gegevens. Die laatste twee risico's zijn er ook met de Pulse Secure kwetsbaarheden. In september kregen de kwetsbaarheden opnieuw aandacht in de media toen bleek dat verschillende Nederlandse organisaties nog steeds kwetsbaar waren.[73]

Kwetsbaarheden in Citrix-servers stelden veel organisaties bloot aan misbruik

Op 17 december 2019 maakte Citrix bekend dat er kwetsbaarheden in Citrix ADC en Citrix Gateway (voorheen bekend als Netscaler) geconstateerd waren. Bij misbruik van deze kwetsbaarheden kan een kwaadwillende in bepaalde situaties toegang krijgen tot het lokale netwerk en de lokale systemen.[74] In de bekendmaking werd ook een tijdelijke oplossing gepubliceerd. Citrix adviseerde aan alle gebruikers van de betreffende systemen om mitigerende maatregelen te nemen. Volgens Citrix was de reden voor openbaarmaking dat drie verschillende beveiligingsonderzoekers in een tijdbestek van twee dagen dezelfde melding deden van de kritieke kwetsbaarheid. Dit vergrootte de kans dat het beveiligingslek vroegtijdig naar buiten zou komen zonder dat een oplossing beschikbaar zou zijn. Bovendien zou een van de drie beveiligingsbedrijven de kwetsbaarheid hoe dan ook op 23 december 2019 publiceren. Volgens Citrix was er dus geen mogelijkheid het lek nog een aantal weken stil te houden om eerst een patch te ontwikkelen.[75] Het NCSC heeft 24 december 2019 een High/High beveiligingsadvies[VII] over deze kwetsbaarheden uitgebracht.[76]

Op 8 januari 2020 maakten beveiligingsonderzoekers bekend dat actoren actief zochten naar kwetsbare Citrix ADC en Citrix Gateway servers.[77] Kort daarop zijn exploits bekend gemaakt waarmee misbruik van deze kwetsbaarheden mogelijk werd. Nederland telde toen volgens onderzoekers honderden kwetsbare Citrix-servers.[78] Na de bekendmaking van de exploits zijn verschillende organisaties aangevallen[79] en gecompromitteerd.[80] Om misbruik zoveel mogelijk te voorkomen, heeft het NCSC continu de situatie gemonitord, adviezen uitgebracht, aangescherpt en technisch onderzoek verricht.

Op 20 januari 2020 zijn de eerste patches beschikbaar gesteld door Citrix. Deze boden een oplossing voor ongeveer 50 procent van de kwetsbare Citrix-systemen in Nederland. De overige benodigde patches kwamen op 24 januari uit.[81] In de periode tussen de publicatie van de exploits en implementatie van patches waren organisaties (potentieel) kwetsbaar voor misbruik.

Er rees kritiek op de handelwijze van Citrix. Door de publiciteit over de kwetsbaarheid en volgens sommigen "een halve oplossing" konden onderzoekers en kwaadwillenden achterhalen wat precies de kwetsbaarheid was en een exploit ontwikkelen.[82]

VII De beveiligingsadviezen van het NCSC worden ingeschaald op twee elementen: de kans dat de kwetsbaarheid wordt misbruikt en de ernst van de schade die optreedt wanneer de kwetsbaarheid misbruikt wordt. De mogelijke waarden per onderdeel zijn Low, Medium of High.

Kwetsbaarheden door ketenafhankelijkheid

Doordat organisaties gebruik maken van diensten en producten van vele andere partijen, kunnen incidenten doorwerken in de keten.[83] De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) wijst bijvoorbeeld op kwetsbaarheid als gevolg van complexe en grensoverschrijdende toeleverings- en productieketens en het gebruik van generieke hard- en software.[84] De NSA waarschuwt voor de risico's die het gebruik van clouddiensten met zich meebrengt. Dergelijke diensten kunnen weliswaar de security van een organisatie verbeteren, maar ook risico's introduceren waarmee rekening moet worden gehouden.[85]

Uitval met doorwerking in digitale en fysieke ketens

Onbereikbaarheid 112 illustreert ketenafhankelijkheid

De onbereikbaarheid van de nationale noodnummers op 24 juni 2019 maakte de (keten)afhankelijkheid van ICT-netwerken inzichtelijk en de impact van een storing. Die dag ontstond een storing in het telefonienetwerk van KPN, waardoor het nationale noodnummer 112 en het landelijke telefoonnummer van de politie 0900-8844 een aantal uren onbereikbaar waren. Ook andere organisaties, waaronder ziekenhuizen, waren niet of minder bereikbaar door de KPN-storing. Door de onbereikbaarheid van 112 waren vervolgens hulpdiensten verminderd bereikbaar voor hulpzoekenden.[86] De aanwezige noodplannen beantwoordden niet aan een situatie waarin sprake was van een gelijktijdige onbereikbaarheid van 112 en 0900-8844.[87] Bestaande back-up-faciliteiten van KPN zouden niet gewerkt hebben.[88]

Keteneffecten van storingen via of bij grote technologiebedrijven

In 2019 verschenen er berichten in de media over enkele storingen bij wereldwijd opererende grote technologiebedrijven waaronder Cloudflare, Amazon Web Services (AWS) en Google Cloud. Die storingen hadden niet alleen wereldwijde gevolgen voor vele andere organisaties, maar soms ook voor andere grote technologiebedrijven. Zo had volgens media een storing bij Cloudflare, dat (onder andere) bedoeld is om storingen en vertragingen te voorkomen, op 24 juni 2019[VIII] gevolgen voor 16 miljoen apps en websites wereldwijd, waaronder in Nederland. Die storing werd veroorzaakt door een netwerkconfiguratiefout bij een lokale provider in de Amerikaanse stad Pittsburgh die foutief werd overgenomen door Verizon, een internationale provider. Deze 'fout-op-fout' zou tot de genoemde storing bij Cloudflare hebben geleid, maar ook bij Amazon en Facebook. Oorzaken van in de media genoemde storingen varieerden van een netwerkcongestie, softwarefout, DDoS-aanval, storing bij een andere partij of stroomstoring. Bij een stroomstoring bij AWS zou volgens media een backup-generator niet hebben gefunctioneerd.[89]

Storingen bij Nederlandse organisaties illustreren afhankelijkheid ICT

In 2019 haalden diverse storingen bij Nederlandse organisaties het nieuws. Er waren landelijke en regionale storingen bij telecomproviders met soms niet alleen gevolgen voor de eigen klanten, maar ook klanten daarvan. Zo resulteerde een storing bij Tele2 in het niet of slecht bereikbaar zijn van overheidsdiensten, gemeenten, de rechtspraak en de RDW en konden personen met enkelbanden niet worden gevolgd. Ook kwamen storingen bij meerdere ziekenhuizen in het nieuws. Daardoor moesten bijvoorbeeld operaties worden afgezegd en patiënten worden doorverwezen naar andere ziekenhuizen.[90] De Onderzoeksraad Voor Veiligheid (OVV) constateert dat de bewustwording van het risico op ICT-uitval in ziekenhuizen niet in gelijke mate is meegegroeid met de toegenomen afhankelijkheid van ICT.[91]

Diverse aspecten van weerbaarheid

Voorbeelden van twijfels bij weerbaarheid

Illustratief voor twijfels bij digitale weerbaarheid is de casus van ernstige kwetsbaarheden in VPN-servers van Fortigate en Pulse Secure. In augustus 2019 bleek dat die nog in tal van kwetsbare systemen te vinden waren, ondanks de beschikbaarheid van patches en waarschuwingen voor misbruik. Ook de casus van kwetsbaarheden in Citrix ADC en Gateway servers is illustratief: bepaalde organisaties bleken begin januari 2020 de aanbevolen mitigerende maatregelen niet getroffen te hebben, zelfs niet nadat een exploit beschikbaar was gekomen.[92] Ondanks de beschikbaarheid van beveiligingsupdates en de publiciteit in Nederland, waren er volgens media op 7 februari toch nog bij 150 bedrijven in Nederland kwetsbare Citrix ADC en Gateway servers te vinden.[93] Volgens de OVV hebben onvolkomenheden in de gemaakte keuzes bij de inrichting en het beheer van het ICT-fundament, alsmede bij de voorbereiding op ICT-uitval, bijgedragen aan het langdurig uitvallen van de ICT in de onderzochte ziekenhuizen.[94] Het hoofd van de AIVD wijst er op dat de weerbaarheid tegen de onzichtbare dreiging van statelijke en criminele actoren moet worden verbeterd.[95] Agentschap Telecom stelde vast dat de digitale veiligheid van Internet-of-Things (IoT)-apparaten in het algemeen niet op orde is. Zeventien van de tweeëntwintig onderzochte apparaten scoorden matig tot zeer slecht op het gebied van basisveiligheid en privacyaspecten.[96] De Algemene Rekenkamer stelde in mei 2019 en mei 2020 dat de ministeries en onderzochte rijksorganisaties de informatiebeveiliging nog steeds niet op orde hebben.[97]

VIII Er is geen aanwijzing dat deze storing een relatie heeft met de eerdergenoemde storing die dag in Nederland bij KPN.

Perceptie van drempels door privacywetgeving

Enkele geraadpleegde experts geven aan dat privacywetgeving een negatief effect lijkt te sorteren op samenwerking, informatiedeling en opsporing, al was het maar omdat nog niet duidelijk is hoe met de Algemene Verordening Gegevensbescherming (AVG) om te gaan. *"Daar waar in de afgelopen jaren het belang van samenwerking en informatiedeling is gegroeid, lijken met de nieuwe wetgeving nieuwe drempels te worden opgeworpen."*[98] 'Zo menen organisaties dat de AVG geen grondslag biedt om informatie te verwerken of te delen met partners, vooral niet buiten de EU.

Kritiek op reactie overheid richting bedrijfsleven

Enkele geraadpleegde experts geven kritiek op de scherpe reactie van de overheid richting het bedrijfsleven over het niet op orde hebben van beveiligingsmaatregelen naar aanleiding van de VPN (Pulse) kwetsbaarheid, terwijl de overheid zelf ook kwetsbaar is gebleken. Volgens hen is door de kritiek van de overheid samenwerking op het gebied van cybersecurity tussen overheid en bedrijfsleven onder druk komen te staan.[99] Die kritiek vanuit 'de overheid' richtte zich op het feit dat organisaties maandenlang kwetsbaar waren door het niet doorvoeren van beschikbare patches, terwijl misbruikmogelijkheden en misbruik bekend waren (zie Nederlandse organisaties maandenlang kwetsbaar via VPN-servers).

Nederland onvoldoende voorbereid op digitale incidenten volgens WRR

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) vindt het opvallend dat vrijwel alle maatregelen en ambities van de overheid en andere belangrijke partijen zijn gericht op het voorkomen van cyberincidenten. De voorbereiding op ontwrichting krijgt echter weinig aandacht. Waar bij een fysieke ramp als een dijkdoorbraak in grote lijnen duidelijk is wat er moet of kan gebeuren, is bij verstoringen met een digitale component nog veel onbekend en onzeker. Verder heeft de overheid onvoldoende middelen om adequaat te handelen, bijvoorbeeld doordat veel infrastructuur in handen is van (buitenlandse) private partijen.[100]

Opsporingsonderzoeken

De politie verrichtte diverse onderzoeken naar cybercriminaliteit, onder meer naar actoren die zich bezighouden met het uitvoeren of faciliteren van cyber(criminele)aanvallen. Zo pakte de Nederlandse politie in 2019 een bulletproof hoster[IX] aan waardoor een botnet uit de lucht werd gehaald en twee verdachten zijn aangehouden. Met het aanhouden van een Nederlander op verdenking van het ontwikkelen en verkopen van malware, heeft de politie de verspreiding van het populaire Rubella-virus gestopt. In februari 2019 werd een groep cybercriminelen op heterdaad betrapt toen zij in een hotelkamer in Soest phishingmails verstuurden en slachtoffers telefonisch inloggegevens voor online bankieren ontfutselden. Ook zijn in 2019 door diverse eenheden van de politie verdachten aangehouden van het hacken van sociale media accounts. Met ondersteuning van Europol maakte een aantal landen een einde aan de activiteiten van het internationaal crimineel GozNym-netwerk, dat gebruik maakte van de GozNym-malware. Hiermee probeerden de criminelen naar schatting in totaal 100 miljoen euro te stelen van meer dan 41.000 slachtoffers.[101] De politie heeft in het kader van een internationale opsporingsoperatie in januari 2020 een Nederlandse verdachte aangehouden op verdenking van het online aanbieden van omstreeks 12 miljard inlognamen en gestolen wachtwoorden.[102]

Preventieve samenwerkingsverbanden

Er zijn diverse preventieve samenwerkingsverbanden ontstaan of verstevigd.[X] De politie verhoogt bijvoorbeeld in samenwerkingsverbanden barrières tegen cyberaanvallen of de facilitering daarvan. Zo werkt de politie samen met andere partijen in projecten als 'NoMoreRansom', 'NoMoreDDoS', 'NoMorePhishing', 'Hack_Right' en in projecten om helpdeskfraude terug te dringen.[103] Verder zijn er onder de Wbni (Wet beveiliging netwerk- en informatiesystemen) in 2019 vier sectorale computercrisisteams aangewezen: voor de zorg (Z-CERT), gemeenten (Informatiebeveiligingsdienst IBD), waterschappen (CERT Watermanagement) en onderwijs en onderzoek (SURFcert). Daardoor wordt intensievere informatie-uitwisseling over cyberaanvallen en samenwerking met het NCSC mogelijk in het kader van het landelijk dekkend stelsel.[104] In 2019 hebben ook de deelnemende partijen aan het Nationaal Respons Netwerk (NRN) een samenwerkingsconvenant getekend, met als doel om bij grootschalige cyberincidenten de kennis en capaciteiten van de deelnemers te bundelen en daardoor de respons op dit soort incidenten verder te versterken.[105]

Belangenafwegingen en zorgen afhankelijkheid buitenlandse partijen

Voorbeelden van afwegingen digitale veiligheid en andere belangen

Partijen wegen het belang van digitale veiligheid af tegen andere belangen. Zo blijft cybersecurity een ingewikkelde afweging tussen een optimaal dienstverlenende en een veilige overheid.[106] Onderwijsinstellingen zien een dilemma tussen open toegankelijke onderwijs- en kennisinstellingen aan de ene kant en digitale veiligheid aan de andere kant.[107] Er bestaat spanning tussen het gebruik van encryptie als beveiligingsmaatregel en de behoefte aan toegang tot informatie door inlichtingen- en opsporingsinstanties in het kader van hun taakuitoefening. Zo is door de VS en het VK druk uitgeoefend op Facebook om end-to-end-encryptie niet uit te rollen.[108]

IX Een bulletproof hoster biedt servers aan voor criminele doeleinden en schermt deze af voor opsporingsdiensten.

X Dit is niet bedoeld als een limitatief overzicht. Het betreft enkele voorbeelden.

Nog steeds zorgen over afhankelijkheid van buitenlandse partijen

In voorgaande CSBN's werd geconcludeerd dat de continuïteit van maatschappelijke kernprocessen sterk afhankelijk is geworden van grote buitenlandse aanbieders van digitale voorzieningen. De WRR onderschrijft dat nu ook. Statelijke actoren richten zich op deze voorzieningen en medewerking van die aanbieders is nodig als zich incidenten voordoen. Bevoegdheden van nationale overheden zijn mogelijk ontoereikend om medewerking af te dwingen.[109] Die afhankelijkheid bleek bijvoorbeeld uit de Citrix-casus. Zo creëerden volgens onderzoekers de kwetsbaarheden voor 80.000 organisaties in 158 landen een risico. In Nederland zou het gaan om meer dan 3700 organisaties.[110] Een cybersecurity bedrijf stelde dat we op onze hoede moeten zijn voor de verscheidenheid aan producten en diensten en de grote hoeveelheid data die deze genereren. Een dergelijke bundeling kan immers ook leiden tot een groter falen.[111] Het Analistennetwerk Nationale Veiligheid wees op het ontbreken van goede alternatieven bij uitval van producten of diensten van een groot technologiebedrijf.[112] Enkele experts signaleren toegenomen aandacht voor digitale soevereiniteit en de afhankelijkheid van buitenlandse systemen in onze kerninfrastructuur.[113] In media komen regelmatig zorgen over Huawei in relatie tot de aanleg van 5G naar voren in berichtgeving, mede in het licht van geopolitieke spanningen tussen de VS en China.[114]

Geopolitieke spanningen verhogen digitale dreiging

3 Vooruitblik

Voortschrijdende digitalisering zal zowel de dreiging als de weerbaarheid beïnvloeden en het belang van digitale veiligheid vergroten. Oplopende geopolitieke spanningen zullen de digitale dreiging van statelijke actoren verhogen. Technieken en technologieën waar al langer over geschreven en gesproken wordt, zoals kunstmatige intelligentie, zullen de komende jaren verder geïmplementeerd worden. Dit heeft zowel positieve als negatieve consequenties voor digitale veiligheid. Digitale veiligheid zal de komende jaren ook beïnvloed worden door de wisselwerking tussen technologie en andere ontwikkelingen. Zo zal de verdere transitie naar een datagedreven economie, met bijkomende zorgen rond privacy en digitale veiligheid, het belang van digitale veiligheid doen toenemen. Door de COVID-19 pandemie is het gebruik van digitale diensten en de digitale ruimte verder toegenomen. Dit kan een stimulans zijn voor verdere digitalisering. Ook dat maakt het belang van digitale veiligheid groter.

Thema's CSBN 2019 nog relevant

In de Vooruitblik van het CSBN 2019 werd reeds ingegaan op de toepassing van kunstmatige intelligentie en de consequenties voor digitale veiligheid. Ook werd gewezen op het feit dat geopolitieke ontwikkelingen de dreiging vanuit statelijke actoren verder zullen vergroten. Fundamentele belangentegenstellingen tussen landen en verschillen van inzicht over internationale normen en waarden versterken deze dreiging. Het is onduidelijk of de prikkels voor vergroting van de weerbaarheid gelijke tred houden met de dreiging en het belang. Rondom technologie en dominantie hierin lijkt een geopolitiek spanningsveld te ontstaan. In het CSBN 2019 werd ook geconstateerd dat digitalisering leidt tot een vergroting van het aanvalsoppervlak en een groei en verschuiving van de aandacht van actoren naar andere en nieuwe waardevolle doelwitten. Uitval zal een grotere impact op het maatschappelijk leven kunnen krijgen door de verdere digitalisering en daardoor verdergaande afhankelijkheid van gedigitaliseerde processen en systemen.[115]

Digitale veiligheid beïnvloed door verdere implementatie technologie

De komende jaren zullen vooral gekenmerkt worden door de verdere implementatie van technieken en technologieën waar al langer over geschreven en gesproken wordt. Een voorbeeld is de toepassing van kunstmatige intelligentie.[116] Daarnaast zal onze samenleving steeds meer worden vormgegeven door het beleid van grote commerciële technologie- en sociale media bedrijven. Deze brede maatschappelijke ontwikkelingen hebben ook consequenties voor digitale veiligheid, zowel positieve als negatieve, die hier nader verkend worden.

Verspreiding autonome systemen vergroot digitale kwetsbaarheid

De verspreiding van autonome systemen, zoals zelfrijdende auto's en allerlei internet-of-things producten, heeft naast allerlei positieve kanten ook consequenties voor digitale veiligheid.[117] Zo bevatten IoT-apparaten regelmatig kwetsbaarheden die niet of moeilijk gepatcht kunnen worden.[118] Daarnaast kan uitval van autonome systemen leiden tot ongelukken (denk aan storingen van zelfrijdende auto's) of in het uiterste geval zelfs tot maatschappelijke ontwrichting. Ook vergroot de verspreiding van autonome systemen het aanvalsoppervlak voor kwaadwillenden: het aantal methodes dat een aanvaller kan gebruiken voor een

cyberaanval neemt toe. Tot slot is het grote aantal apparaten dat de wereld om ons heen observeert en data daarvan vastlegt, zoals slimme camera's, interessant voor spionagedoeleinden.

Slimme algoritmes hebben positief en negatief effect op digitale veiligheid

De ontwikkeling dat systemen steeds meer zelfstandig kunnen leren, begrijpen en redeneren, zet door.[119] Dat heeft implicaties voor digitale veiligheid. Slimme algoritmes zijn deels openbaar beschikbaar en bieden nieuwe mogelijkheden voor de koppeling van verschillende databronnen. Die koppeling kan leiden tot misbruik van persoonlijke gegevens. Omdat het voor gebruikers niet duidelijk is wat er met hun data gebeurt, is verdediging tegen kwaadwillenden lastig. Aan de andere kant kunnen slimme systemen ook worden ingezet ter verdediging tegen digitale aanvallen en een rol spelen in preventie, bescherming, detectie en respons.

Ontstaan van grote, gekoppelde netwerken uitdaging voor weerbaarheid

In de digitaliserende wereld worden netwerken van data, diensten en systemen die aan elkaar zijn gekoppeld, steeds omvangrijker.[120] Vanuit het perspectief van weerbaarheid is de grote vraag hoe dit veilig georganiseerd kan worden. Het is nu vaak onduidelijk hoe netwerken en onderdelen daarvan worden aangestuurd. Door connected clouds is data onzichtbaar met elkaar verbonden, waarbij het ingewikkeld is om toezicht te houden op die data, laat staan deze te beheren. Dat beheer zal nog uitdagender worden, doordat gebruikers en beheerders inzicht in en begrip van het eigen digitale ecosysteem mogelijk verliezen. Daar staat een professionalisering van dergelijke diensten door deze aanbieders tegenover. Idealiter is er op termijn sprake van een vergroting van het inzicht in beheer van data en security by design.

Afhankelijkheid van buitenlandse technologie maakt kwetsbaar

Door de snelle digitalisering is een afhankelijkheid van technologie ontstaan die van buiten de landsgrenzen komt en buiten de Nederlandse controle valt.[121] Afhankelijkheid van technologie biedt kansen, maar maakt ook kwetsbaar voor acties van kwaadwillenden, vooral waar het buitenlandse partijen betreft die assertief hun eigen geopolitieke agenda nastreven, en voor uitval. In het uiterste geval kunnen incidenten leiden tot maatschappelijke ontwrichting. Bij uitval van systemen blijkt steeds meer hoezeer de maatschappij afhankelijk is geworden van deze diensten, zonder goede alternatieven. De afhankelijkheid van externe technologie en de kwetsbaarheid worden nog versterkt door de verdere transformatie naar een datagedreven economie (zie Maatschappelijke ontwikkelingen vergroten belang van digitale veiligheid).

Digitale veiligheid beïnvloed door ontwikkelingen

Ook de wisselwerking tussen technologie en andere ontwikkelingen heeft gevolgen voor de digitale veiligheid.

Geopolitieke spanningen werken door op mondiale ICT-markt

Het is de verwachting dat geopolitiek het digitale domein de komende jaren verder zal beïnvloeden. Zo proberen landen de totstandkoming van nieuwe internetstandaarden te beïnvloeden. Ook zullen veiligheidsbelangen een grotere rol krijgen in keuzes die gemaakt worden rond ICT-infrastructuur. Door oplopende geopolitieke spanningen en het ontstane wantrouwen in hard- en software, producenten en dienstverleners zal het aantal vertrouwde producten en leveranciers per land of regio mogelijk afnemen. Dit kan leiden tot een versnippering van ICT-markten op basis van geopolitieke overwegingen.[122] Het gaat dan om streven naar meer digitale soevereiniteit.[123]

Digitale veiligheid wordt hiermee een belang dat landen steeds centraler zullen stellen voor hun veilig functioneren. Landen veraf en dichtbij zullen pogen om grip te krijgen op de ICT-infrastructuur vanuit veiligheidsbelangen. Daarbij is het denkbaar dat Europa op dit vlak als het ware klem komt te zitten tussen de grote machtsblokken China en de VS. Door de implementatie van nieuwe technologie en de hoge doordringingsgraad van ICT en netwerken zullen risico-afwegingen er anders uitzien dan voorheen. Veiligheidsbelangen zullen een prominentere rol spelen.

Maatschappelijke ontwikkelingen vergroten belang van digitale veiligheid

Een andere maatschappelijke ontwikkeling die het belang van digitale veiligheid vergroot, is de verdere transformatie naar een datagedreven economie, met alle bijkomende zorgen rond privacy en digitale veiligheid.[124] In een gedigitaliseerde economie worden mens en machine steeds meer complementair. Nieuwe technologieën vormen de basis voor de 'vierde industriële revolutie' waarin autonome systemen in productieketens nauw met elkaar verbonden worden, en data-gedreven werken. In de data-gedreven economie ontstaan diepe, omvangrijke en complexe afhankelijkheden doordat platformen afkomstig uit politieke grootmachten steeds meer gebruikt worden. Daarbij krijgen grote technologiebedrijven met hun producten steeds meer toegang tot vitale processen. Ze creëren hiermee machtposities in nationale economieën. Daar staat tegenover dat landen mogelijk proberen juist meer grip te krijgen op de eigen infrastructuur (zie hierboven).

Een recente ontwikkeling is die van de maatschappelijke gevolgen van de COVID-19 pandemie. Dankzij digitalisering kunnen commerciële, educatieve en sociale activiteiten die anders volledig stil zouden vallen, deels toch doorgaan. De keerzijde van de huidige situatie, waarin veel thuis gewerkt wordt, privé-activiteiten zich ook primair thuis afspelen en veel dienstverlening digitaal verloopt, is dat de digitale ruimte zwaarder dan ooit belast wordt. Met de komst van de 1,5 meter samenleving zal continuering van de maatschappij nog meer dan voor de pandemie afhankelijk zijn van de digitale ruimte. De huidige situatie laat daarmee het cruciale belang van digitale veiligheid zien. Grootschalige uitval kan nog meer dan voorheen leiden tot maatschappelijke ontwrichting. Het toegenomen gebruik van de digitale ruimte biedt ook meer mogelijkheden voor kwaadwillenden. Zo speelden criminelen al snel in op deze toename en voor statelijke actoren biedt het ook verdere kansen voor bijvoorbeeld spionage.

Organisaties ook doelwit als springplank naar andere organisaties

4 Dreiging

Net als in 2019 kan ook nu worden geconcludeerd dat de digitale dreiging een permanent karakter heeft en dat cyberincidenten kunnen leiden tot maatschappij-ontwrichtende schade. Vooral spionage, (voorbereidingen voor) sabotage en uitval van digitale diensten, processen en systemen vormen een dreiging voor de nationale veiligheid. De dreiging is vooral afkomstig van statelijke actoren wat betreft moedwillige kwaadaardige activiteiten (cyberaanvallen). Er gaat ook een dreiging uit van cybercriminelen, onder meer van criminele afpersers. Als de dreiging zich manifesteert tegen de digitale ruimte en Nederlandse vitale processen als (primair) doelwit, kan de impact op de nationale veiligheid groot zijn. Ook cyberincidenten bij andere voor de (Nederlandse) maatschappij cruciale sectoren, partijen en processen kunnen grote impact hebben. De digitale ruimte, de (mondiale) leveranciersketen, vitale processen en andere organisaties kunnen ook een doelwit zijn als springplank naar andere doelwitten. Afhankelijkheid van producten of diensten uit landen met een offensief cyberprogramma tegen Nederland is een risicoverhogende factor.

Incidenten die zijn beschreven in Hoofdstuk 2 Jaarbeeld (verder jaarbeeld) schetsen een mogelijke doorontwikkeling van de dreiging. Statelijke actoren zetten informatie-operaties in voor geopolitieke doeleinden. Ook blijkt een statelijke actor complexe aanvallen uit te voeren op een brede doelgroep. Integriteitsaantasting van systemen en/of de daarin opgeslagen informatie kan eveneens verregaande gevolgen hebben voor de nationale veiligheid. De mogelijkheden en gevolgen hiervan zijn onduidelijk.

Dreiging vanuit vooral statelijke en criminele actoren

Staten houden zich - naast spionage en sabotage - bezig met informatie-operaties

Statelijke actoren houden zich vooral bezig met spionage en sabotage (zie Spionage, sabotage en uitval dreiging voor nationale veiligheid). Ook voeren ze informatie-operaties uit en tasten zo de integriteit en vertrouwelijkheid van systemen en informatie aan.[125] Er is geen enkele reden om aan te nemen dat zij zullen stoppen met deze activiteiten. Staten kunnen informatie als wapen gebruiken om het eigen imago te bevorderen (propaganda) of om anderen te beïnvloeden, door twijfel, angst of besluiteloosheid te zaaien. Wanneer staten daarvoor onware, inaccurate of misleidende informatie gebruiken, spreken we van desinformatie. Propaganda en desinformatie hebben niet per definitie een cybercomponent zoals bedoeld in het CSBN. Dat is wel het geval bij zogeheten hack&leak operaties, waarbij via een digitale aanval buitgemaakte echte informatie op een specifiek moment wordt gelekt.[126] Vaak wordt bij het lekken van de informatie een bepaald frame neergezet, een context die niet noodzakelijkerwijs juist is, maar waarmee de informatie een schadelijker effect krijgt. Dit soort hack&leak acties overkomt zowel bedrijven, politici als overheidsinstanties.[127] Ook beïnvloedingsoperaties (een vorm van informatie-operaties) hebben vaak een digitale component doordat zij de integriteit of vertrouwelijkheid van informatie aantasten.

Dreiging vanuit cybercriminelen onverminderd groot

Naast de dreiging die uitgaat van statelijke actoren, blijft de dreiging vanuit cybercriminelen onverminderd groot voor aantasting van de vertrouwelijkheid, integriteit en beschikbaarheid van digitale diensten, processen en systemen.[128] Zo blijven mondiaal opererende geavanceerde cybercriminele groepen actief die zich onder meer op de financiële sector richten. De Cobalt-groep bijvoorbeeld probeert onder meer het interne netwerk van

banken onder controle te krijgen om vervolgens grote geldbedragen weg te sluizen via manipulatie van geldautomaten, bankrekeningdatabases of SWIFT-transacties.[129] Ook blijft er een dreiging uitgaan van cybercriminele dienstverleners die uiteenlopende actoren diensten aanbieden waardoor die in staat zijn cyberaanvallen uit te voeren: cybercrime-as-a-service.

Dreiging van afpersing toegenomen

Uit het jaarbeeld blijkt dat de dreiging van afpersing door cybercriminelen door middel van aantasting van de beschikbaarheid en vertrouwelijkheid is toegenomen. Zij zetten ransomware in tegen organisaties waarvan ze verwachten dat die de mogelijkheid hebben om grotere geldbedragen te betalen en/of waarvoor bedrijfscontinuïteit en waardevolle unieke data een belangrijke rol spelen. Het is gebleken dat organisaties daadwerkelijk losgeld betalen. Als ze dat niet doen, dreigen criminelen in sommige gevallen gekopieerde data te openbaren. Een dreigement dat ze soms ook uitvoeren.[130] Het is te verwachten dat cybercriminelen hiermee door gaan zolang het een aantrekkelijk verdienmodel is voor hen.

De dreiging van cybercriminelen tegen industriële controlesystemen (ICS) neemt mogelijk verder toe. In het jaarbeeld is melding gemaakt van nieuwe gijzelsoftware genaamd EKANS, die zich richt op ICS en die waarschijnlijk het werk is van criminele hackers.[131] Mogelijk is er onder cybercriminelen sprake van toenemende intenties en capaciteiten om kritieke infrastructuur te raken voor financieel gewin.[132] ICS zijn immers een aantrekkelijk doelwit doordat de beschikbaarheid essentieel is voor het functioneren van organisaties. Dat vergroot de prikkel om losgeld te betalen na aanvallen met gijzelsoftware. Aanvallen op ICS kunnen een ontwrichtende werking hebben, bijvoorbeeld wanneer het elektriciteitsnet getroffen wordt. Bekende digitale aanvallen op ICS tot nu toe werden hoofdzakelijk uitgevoerd door statelijke actoren.[133] Ook valt niet uit te sluiten dat statelijke actoren doelbewust de indruk willen wekken criminele motieven te hebben om zo attributie lastiger te maken. Het kan ze dan te doen zijn om bijvoorbeeld spionage of sabotage. Ook is vermenging van activiteiten of samenwerking tussen statelijke en criminele actoren mogelijk, zoals vermeld in het jaarbeeld.

Dreiging van andere actorgroepen laag

De dreiging die uitgaat van ideologisch gemotiveerde actorgroepen (hacktivisten en terroristen) en actorgroepen die handelen uit een persoonlijk motief (insiders, cybervandalen en scriptkiddies) is relatief klein. Al jaren zijn vanuit deze actorgroepen geen substantiële aanvallen tegen Nederland of Nederlandse belangen waargenomen. Er is geen aanleiding te veronderstellen dat dit komende jaren anders is. Polarisatie binnen de samenleving over vraagstukken als het stikstofbeleid en de uitrol van 5G kunnen daarentegen leiden tot een toename van cyberaanvallen door hacktivisten of fysieke aanvallen met digitale gevolgen. Een voorbeeld daarvan is de recente brandstichtingen in zendmasten voor mobiele telefonie en dataverkeer. Deze kunnen uitval van telefonie en het noodnummer 112 tot gevolg hebben.[134]

Spionage, sabotage en uitval dreiging voor nationale veiligheid

Dreiging digitale spionage en sabotage door staten onverminderd groot

In het jaarbeeld werd reeds gesignaleerd dat spanningen tussen mogendheden een vervolg krijgen in de digitale ruimte. Een toenemend aantal statelijke actoren is actief op het gebied van politieke, economische en militaire spionage en (voorbereidingen voor) sabotage.[135]

Digitale spionage tast de vertrouwelijkheid van systemen aan. Een bijzonder internationaal voorbeeld van een digitale spionagecampagne in de afgelopen rapportageperiode was het grootschalig misbruik van ernstige kwetsbaarheden in iOS en Android software, waaronder een zero-day kwetsbaarheid voor Android.[136] Via deze kwetsbaarheden werden complexe aanvallen uitgevoerd op een brede groep doelwitten. Het is voor zover bekend nog niet eerder waargenomen dat statelijke actoren zulke complexe middelen hebben ingezet voor een dergelijke brede aanval. Aangenomen werd dat actoren die heel gericht en beperkt zouden inzetten om niet op te vallen en maximaal profijt te halen uit de kennis van die kwetsbaarheid.

Digitale sabotage tast de beschikbaarheid van systemen aan en lijkt vooral tot doel te hebben om de besluitvorming in het getroffen land te beïnvloeden in een tijd van conflict of crisis.[137] Het dreigen met het digitaal platleggen van vitale systemen van een land of dat daadwerkelijk doen, kan een statelijke actor immers macht over een andere staat geven. Of deze dreiging zich daadwerkelijk manifesteert, is afhankelijk van geopolitieke conflicten, aangezien spanningen tussen landen een vervolg kunnen krijgen in de digitale ruimte.

Dreiging van uitval nog relevant

Uitval in de categorie niet-moedwillige dreigingen heeft een potentieel grote impact op de samenleving. De toenemende verbondenheid en de complexiteit van digitale diensten, processen en systemen maken het waarschijnlijk dat er in Nederland vaker uitval zal voorkomen. In het jaarbeeld zijn voorbeelden gegeven van storingen die de ketenafhankelijkheid van ICT-netwerken illustreerden.[138]

Snelheid misbruik van kwetsbaarheden werkt dreigingsverhogend

Uit het jaarbeeld blijkt dat criminelen en statelijke actoren misbruik maken van kwetsbaarheden. Zij zijn in staat om snel en op grote schaal toe te slaan, bijvoorbeeld na het bekend worden van een exploit.[139] De intentie en capaciteit om snel in te spelen op kwetsbaarheden werken dreigingsverhogend.

Aantasting integriteit digitale diensten, processen en systemen: mogelijkheden en gevolgen onduidelijk

De mogelijkheden van (on)opzettelijke aantasting van de integriteit van digitale diensten, processen en systemen, en de gevolgen daarvan, zijn onduidelijk, maar lijken een grote impact te hebben.[140] Burgers, bedrijven en organisaties moeten kunnen vertrouwen op de integriteit daarvan, terwijl statelijke en criminele actoren met hun activiteiten soms juist de integriteit van informatie(verwerking) aantasten.[141] In het jaarbeeld bleek dat actoren opnieuw interesse getoond hebben in het wijzigen van Domain Name System (DNS)-instellingen. Door het wijzigen van deze instellingen van organisaties kan inkomend netwerk- en e-mailverkeer worden omgeleid en onderschept. Het grootschalig compromitteren van DNS-servers kan aanzienlijke impact hebben op de integriteit van het internetverkeer en kan het vertrouwen in de digitale ruimte aantasten.[142]

Het manipuleren van informatie kan grote gevolgen hebben en vormt vooral een risico in sectoren waar informatie vaak gemuteerd wordt, zoals de financiële sector. Cyberincidenten kunnen financiële informatie vernietigen, versleutelen of veranderen, terwijl in de tussentijd wel transacties in het grotere financiële stelsel plaatsvinden die dus niet meer juist verwerkt kunnen worden. Dat kan de stabiliteit van het financiële systeem bedreigen, met potentieel ernstige consequenties voor de economie. In dat scenario kan een cyberincident ertoe leiden dat een operationele verstoring uitmondt in een crisis met een grote impact op de maatschappij. Een dergelijke crisis treedt echter niet zomaar op, maar is het gevolg van een combinatie van specifieke factoren én het verlies van vertrouwen in het systeem.[143]

Dreiging tegen primaire doelwitten en doelwitten als springplank

Als de dreiging zich zou manifesteren tegen de digitale ruimte en Nederlandse vitale processen als (primair) doelwit, kan de impact op de nationale veiligheid groot zijn. Dat laat onverlet dat er ook andere voor het functioneren van de (Nederlandse) maatschappij cruciale sectoren, partijen en processen bestaan. Te denken valt aan kennisintensieve bedrijven die wereldwijd toonaangevend zijn (topsectoren), de defensie-industrie, lagere overheden, semipublieke instellingen en ziekenhuizen.

De dreiging tegen die doelwitten bestaat doordat actoren de intentie en de capaciteiten hebben om cyberaanvallen uit te voeren en gelegenheden daartoe, zoals kwetsbaarheden, benutten. Het jaarbeeld laat zien dat vele soorten organisaties doelwit zijn van aanvallers. Het kan variëren per land en per type spionage waar statelijke actoren hun politieke spionage-activiteiten op richten. Zo zijn topsectoren in Nederland een voor de hand liggend doelwit voor economische spionage en de rijksoverheid voor politieke spionage. Vitale processen zijn een populair doelwit voor sabotage door statelijke actoren. Kapitaalkrachtige organisaties vormen een geliefd doelwit van cybercriminelen.

Naast de genoemde ‘primaire’ doelwitten, richten aanvallers zich ook op doelwitten die een springplank naar andere doelwitten kunnen vormen.[144] De digitale ruimte, de veelal mondiale leveranciersketens en concentraties van persoonsgegevens zijn hiervoor bij uitstek geschikt. Het gaat hier bijvoorbeeld om leveranciers van hard- en software, om vitale processen, zoals die van telecombedrijven, of om organisaties die op grote schaal persoonsgegevens vergaren en verwerken, waaronder medische en medewerkersgegevens. Voor deze ‘afgeleide’ doelwitten gaan actoren actief op zoek naar zwakke schakels in ketens, als opstap naar interessante(re) doelwitten. Dit betekent dat ogenschijnlijk voor aanvallers niet interessante sectoren of organisaties toch interessant kunnen zijn als opstap naar een ander primair doelwit.

De dreiging bestaat ook doordat zich uitval kan voordoen bij of via deze doelwitten. Zo kan uitval van systemen door technisch falen of uitval door menselijke fouten bij de uitvoering van hun taken doorwerken naar andere organisaties.

Afhankelijkheid van landen met offensief cyberprogramma is risicoverhogende factor

Afhankelijkheid van ICT-producten of -diensten uit landen waarvan is vastgesteld dat ze een offensief cyberprogramma hebben gericht tegen Nederland, is een risicoverhogende factor. Ook in 2019 waren er zorgen over de keerzijde van de afhankelijkheid van een beperkt aantal aanbieders uit een beperkt aantal landen. Die aanbieders houden niet vanzelfsprekend rekening met Nederlandse belangen.[145] Die afhankelijkheid vormt een risicofactor voor onder andere digitale spionage en sabotage. Landen proberen ook op andere wijze dan via cyberaanvallen hun doelen op de langere termijn te halen. De inzet van economische middelen en het creëren van strategische en technologische afhankelijkheden zijn onderdeel van machtspolitiek. Wanneer een land een dominantie heeft of krijgt over een bepaalde technologie, dan bepaalt het uiteindelijk ook de technologische standaarden voor de toekomst. Dat versterkt de afhankelijkheid van dat land voor de rest van de wereld. Ook buitenlandse investeringen en overnames in Nederland kunnen leiden tot verlies van (gedeeltelijke) zeggenschap over vitale infrastructuren. Daarmee is de continuïteit van vitale processen in het geding en dreigt het weglekken van kennis en vertrouwelijke of gevoelige informatie. Ook versplintering en verspreiding van delen van het productieproces over landsgrenzen heen kunnen een risicofactor vormen.[146] Landen kunnen immers eisen stellen aan buitenlandse bedrijven waardoor die zich bijvoorbeeld moeten houden aan wetten inzake toezicht of medewerking aan de overheid. De AIVD vindt het daarom onwenselijk dat Nederland voor de uitwisseling van gevoelige informatie of voor vitale processen afhankelijk is van bedrijven uit landen die een offensief cyberprogramma tegen Nederlandse belangen uitvoeren.[147]

Digitale veiligheid ontstaat niet uit zichzelf

5 Belang

Digitale veiligheid is een randvoorwaarde voor het functioneren van onze maatschappij. Dat geldt in het bijzonder voor veiligheid van de digitale ruimte en vitale processen. Aantasting daarvan kan leiden tot maatschappij-ontwrichtende schade. Om diverse redenen komt die veiligheid niet vanzelf tot stand. Zo lijken digitale risico's te worden onderschat. Ondanks de potentieel grote impact van cyberincidenten, zijn deze lastig te agenderen. Het helpt daarbij niet dat het creëren van een volledig beeld van de investeringen in digitale veiligheid niet eenvoudig is.

Digitale veiligheid randvoorwaarde voor functioneren maatschappij

Digitale veiligheid is onlosmakelijk verbonden met de nationale veiligheid. Dat geldt in het bijzonder voor de (mondiale) digitale ruimte, die het digitale fundament vormt van onze maatschappij en voor vitale processen die essentieel zijn voor samenleving en economie. Beide zijn nauw met elkaar verweven. Enkele vitale processen geven de digitale ruimte mede vorm, waaronder 'Internet en datadiensten'. Andere kunnen beschouwd worden als randvoorwaarden, zoals 'Landelijk transport en distributie elektriciteit'. Vitale processen zijn vrijwel volledig afhankelijk van digitale diensten, processen en onderliggende systemen en daarmee ook van de digitale ruimte.

Ook digitale veiligheid van andere voor de maatschappij cruciale organisaties, diensten en processen, is van belang evenals die van ogenschijnlijk voor de nationale veiligheid minder belangrijke (zie hoofdstuk Dreiging). Voor de betreffende diensten (e.d.) zelf, en omdat aanvallers zich ook richten op doelwitten die een springplank naar andere doelwitten kunnen vormen. Voorts kan uitval bij ogenschijnlijk minder belangrijke diensten (e.d.) doorwerken naar andere.

Digitale veiligheid ontstaat niet uit zichzelf

Hoewel digitale veiligheid onlosmakelijk is verbonden met de nationale veiligheid van Nederland, komt die veiligheid niet uit zichzelf tot stand, noch van het grotere geheel, noch van individuele partijen.

Invloed Nederland op (mondiale) digitale veiligheid beperkt

Mondiaal spelen vele partijen een rol bij het veilig maken en houden van de digitale ruimte. De mogelijkheden voor de Nederlandse overheid en Nederlandse partijen zijn daarin logischerwijze beperkt. De digitale ruimte is niet gebonden aan landsgrenzen. Een relatief kleine groep aanbieders van hard- en software, digitale diensten en platforms uit een beperkt aantal landen speelt een cruciale rol, maar ook weer niet als enige. Vele organisaties en landen realiseren uiteindelijk samen de digitale ruimte en de veiligheid daarvan. Een gegeven daarbij is dat normen en waarden van landen(groepen) en bedrijven verschillen wat betreft bijvoorbeeld de omgang met mensenrechten, privacy en de digitale veiligheid. Landen stellen bijvoorbeeld uiteenlopende wettelijke eisen aan bedrijven. Verder hebben sommige landen een offensief cyberprogramma tegen Nederland.

Prikkels niet (altijd) toereikend voor bijdrage aan bredere digitale veiligheid

Wanneer de juiste prikkels ontbreken, is het geen uitgemaakte zaak dat partijen in hun belangenafweging rekening houden met het grotere belang van digitale veiligheid voor anderen of de maatschappij. In vooral economische literatuur wordt gesproken over mogelijke 'externe effecten' of derde-partij-effecten van besluitvorming. Die effecten kunnen leiden tot verkeerde prikkels en/of tot maatschappelijk ongewenste uitkomsten.[148] Wanneer een webhoster bijvoorbeeld relatief weinig aandacht zou besteden aan veiligheid, valt zijn prijs waarschijnlijk lager uit dan concurrenten die wel veel investeren. Ook een klant, bijvoorbeeld de eigenaar van een webwinkel, zou die afweging kunnen maken. Mogelijk is diegene zich niet bewust van de risico's of kan hij de afweging maken dat incidenten weinig directe schade veroorzaken voor hemzelf. Hij laat daarbij de schade voor anderen buiten

beschouwing. Naast negatief, kunnen externe effecten ook positief uitpakken. Een internet service provider die wel fors investeert in cybersecurity en systemen die onderdeel uitmaken van een botnet actief verwijdert, draagt bij aan de veiligheid van directe klanten, maar ook aan die van potentiële slachtoffers van het botnet. Die provider en zijn klanten betalen dan de kosten, terwijl de baten ook bij anderen terechtkomen.

Ook de landelijke overheid en het kabinet maken afwegingen tussen het belang van digitale veiligheid en andere belangen. Capaciteit en geld dat aan digitale veiligheid wordt besteed, kan immers niet voor andere zaken worden aangewend. Ook kunnen onder andere economische of buitenlandse belangen meespelen in de afweging.

Afweging dreiging, belang en weerbaarheid voor 5G-netwerken

Voor de verdere ontwikkeling van 5G-netwerken is de vraag naar de onderlinge verhouding tussen dreiging, belang en weerbaarheid expliciet op nationaal niveau gesteld. De kritieke onderdelen van netwerken van telecomaanbieders zijn in kaart gebracht en het belang van de beschikbaarheid, vertrouwelijkheid en integriteit daarvan bepaald. De dreiging daartegen en al getroffen maatregelen zijn beoordeeld. In de uiteindelijke afweging zijn ook het economische belang van 5G en diplomatieke belangen met andere landen meegewogen. Als gevolg van die afweging worden (onder andere) extra hoge eisen gesteld aan leveranciers van diensten en producten in de kritieke onderdelen in het telecomnetwerk.[149]

Grote technologiebedrijven houden niet vanzelfsprekend rekening met Nederlands belang

Nederland is in brede zin (keten)afhankelijk van een relatief kleine groep aanbieders van hard- en software, digitale diensten en platforms uit een beperkt aantal landen. Deze houden niet vanzelfsprekend rekening met de nationale veiligheid van Nederland. Sommige landen benutten potentieel die bedrijven zelfs voor hun offensieve cyberprogramma tegen andere landen. Veel technologiebedrijven vergaren bovendien veel informatie en bieden hun producten en diensten mondiaal aan. Zij zijn daardoor een aantrekkelijk doelwit voor cyberactoren. Cyberincidenten kunnen via die bedrijven wereldwijde keteneffecten tot gevolg hebben.

Losgeldbetalingen na ransomware-aanval: individueel versus algemeen belang

Een kwestie waar het belang van een organisatie botst met het algemene belang, is losgeldbetaling voor ontsleuteling van bestanden na een ransomware-aanval. Het is in het belang van een slachtoffer om zo snel mogelijk de eigen dienstverlening en bedrijfsvoering weer op te starten. Vanuit maatschappelijk oogpunt is er het belang om geen crimineel verdienmodel in stand te houden dat leidt tot nieuwe slachtoffers. Zo betaalde de Universiteit Maastricht, slachtoffer van een ransomware-aanval, 197.000 euro (30 bitcoin) losgeld.[150] Volgens onderzoek van Sophos zou een derde van de getroffen bedrijven overgaan tot betaling van losgeld. Betaling kan het herstel vereenvoudigen en kan goedkoper lijken voor een getroffen organisatie. Zo kostte het herstel na een ransomware-aanval de Amerikaanse stad Baltimore $5,3 miljoen, terwijl het losgeld $76.000,- bedroeg. Toch moet een organisatie ook na betaling van losgeld nog investeren om een nieuwe aanval te voorkomen, waardoor de verhouding er anders uit komt te zien.[151] Cyberverzekeraars zijn in voorkomende gevallen bereid losgeld te betalen wanneer een verzekerde is getroffen, soms zelfs terwijl herstel mogelijk is.[152] Een Nederlandse verzekeraar stelt daarentegen dat betaling van losgeld slechts een vangnet is en dat uiteindelijk een organisatie zelf beslist over betaling.[153] De politie en het NCSC adviseren om niet te betalen, omdat losgeldbetalingen een verdienmodel voor criminelen in stand houden. Zo constateert de politie in opsporingsonderzoeken dat het betaalde geld deels wordt gebruikt om nieuwe aanvallen uit te voeren.[154] Criminelen richten zich bovendien mogelijk juist op vermogende of verzekerde bedrijven omdat er een grotere kans is dat die betalen. Ook is het niet zeker dat gegijzelde bestanden na betaling weer beschikbaar komen,[155] zoals NotPetya in het verleden heeft geïllustreerd. Voorts kunnen bestanden al voor het versleutelen zijn gekopieerd om na betaling het slachtoffer alsnog verder af te persen.[156]

Cyberincidenten kunnen zich op grote schaal, gelijktijdig of opeenvolgend voordoen

Cyberincidenten kunnen zich op verschillende manieren voordoen en ook optreden in samenhang met geheel andersoortige incidenten. Dat komt onder andere door de sterke - veelal internationale - connectiviteit tussen digitale diensten en processen, systemen en het gebruik van generieke hard- en software(componenten). Cyberincidenten kunnen daardoor een onvoorziene kettingreactie in gang zetten waarvan de gevolgen het functioneren van delen van de maatschappij in gevaar kunnen brengen.[157] Die effecten kunnen nog versterkt worden als het vertrouwen verdwijnt, bijvoorbeeld door desinformatie. Ook is niet altijd direct helder wat de oorzaak van een incident is.[158] Is het een menselijke fout, bijvoorbeeld verkeerde routering, uitval door een softwarefout of een cyberaanval?

Risico's voor gehele digitale ruimte en doorwerking lastig te doorgronden

De risico's van cyberincidenten voor de gehele digitale ruimte en de doorwerking daarvan in de samenleving zijn lastig te doorgronden. Het gaat dan om de risico's voor het grotere geheel in plaats van de losse domeinen en componenten, zogeheten 'systemische digitale risico's.[XI] Men herkent die eigenlijk pas als ze zich voordoen. Bij zulke risico's moet rekening worden gehouden met vele factoren, verbindingen en afhankelijkheden. Deze kunnen afzonderlijk of gezamenlijk resulteren in een kettingreactie met veelal onverwachte en complex te doorgronden gevolgen.[159] Dat maakt de beoordeling van risico's complex, evenals de afweging om wel of

geen maatregelen te treffen om risico's te beheersen. Ook is niet op voorhand helder welke partijen de prikkels, mogelijkheden en bereidheid hebben om risico's te beperken.

Gevolgen al dan niet openbaar maken kwetsbaarheden niet altijd te overzien

Het openbaar maken van kwetsbaarheden heeft voor- en nadelen. Misbruik van zowel gepubliceerde als (nog) niet gepubliceerde kwetsbaarheden kan een risico voor de veiligheid van de digitale ruimte vormen. De gevolgen daarvan zijn niet altijd te overzien. Voor de meeste gepubliceerde kwetsbaarheden zijn een afdoende patch of mitigerende maatregelen aanwezig, maar soms ook (nog) niet. En ook wanneer die wel beschikbaar zijn, worden ze lang niet altijd direct doorgevoerd, terwijl actoren in staat zijn snel misbruik te maken van kwetsbaarheden. Er zijn diverse wetenschappelijke onderzoekers en bedrijven permanent op zoek naar kwetsbaarheden in hard- en software. Grote bedrijven zijn bereid veel geld voor ontdekte kwetsbaarheden te betalen. Zo gaf Bugbounty platform HackerOne gaf begin 2020 aan zich te kunnen beroepen op 600.000 ethische hackers. Ze verdienden wereldwijd 40 miljoen dollar in twaalf maanden.[160] Inmiddels is een wachttermijn van 90 dagen gangbaar tussen de melding aan een organisatie en publicatie van de kwetsbaarheid. Dit biedt organisaties de gelegenheid een patch te ontwikkelen voor de kwetsbaarheid. Toch komt niet iedere organisatie binnen die termijn met een oplossing. Dat kan zijn omdat ze het belang er niet van ziet. Het kan ook zijn dat er meerdere bedrijven nodig zijn om een oplossing te creëren. In dat laatste geval kan de kwetsbaarheid voortijdig uitlekken met een kans op misbruik. Ook kunnen er in dat geval meer dan 90 dagen nodig zijn voor die organisaties om op hetzelfde moment met een patch te komen. Tot slot kunnen organisaties kennis dragen van kwetsbaarheden en besluiten deze niet te openbaren zolang anderen hierover niet aan de bel trekken.

De afweging om wel of niet kwetsbaarheden te publiceren, roept diverse vragen op in relatie tot digitale veiligheid. Kunnen de onderzoekers(groepen) en organisaties de gevolgen voldoende overzien om de tegenstrijdige belangen tussen het wel of niet publiceren in de specifieke situatie af te wegen? Geven zij zich in alle gevallen rekenschap van de juridische grenzen van Coordinated Vulnerablity Disclosure? Als een bedrijf na 90 dagen nog geen patch beschikbaar stelt, is het dan in alle gevallen legitiem om de kwetsbaarheid publiek te maken? Wanneer het gaat om een fundamentele kwetsbaarheid in miljoenen apparaten waarvoor geen patch beschikbaar is, is het dan nog wenselijk om te publiceren? Mag een bedrijf zelf beslissen geen patch uit te brengen op grond van de stelling dat misbruik een kleine impact heeft of hopend dat die kwetsbaarheden niet bekend raken?

Digitale risico's lijken te worden onderschat

Digitale risico's lijken te worden onderschat: de digitale weerbaarheid is nog niet overal op orde, terwijl digitale risico's al jaren groot zijn.

Cyberincidenten: grote gevolgen, maar lastig te agenderen

Om een afweging te kunnen maken moeten partijen zich bewust zijn van digitale risico's. De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) stelt dat het ontbreken van echt ontwrichtende gebeurtenissen het lastig maakt om verstoring te agenderen, laat staan om de urgentie daarvan te onderstrepen en breed geaccepteerd te krijgen. De WRR vindt het echter onterecht om incidenten te bagatelliseren en ontwrichtende scenario's af te doen als onrealistisch.[161] Het hoofd van de AIVD wijst er op dat mensen moeite hebben ons iets voor te stellen bij de onzichtbare dreiging van bijvoorbeeld spionage.[162] De Onderzoeksraad Voor Veiligheid (OVV) constateert dat de bewustwording van het risico op ICT-uitval in ziekenhuizen niet in gelijke mate is meegegroeid met de toegenomen afhankelijkheid van ICT.[163] Wel leiden incidenten, zoals de ransomware-aanval op de Universiteit Maastricht tot extra bewustwording en mogelijk extra maatregelen door soortgelijke organisaties.[164] Enkele experts signaleren dat het rapport van de WRR heeft bijgedragen aan het belang dat in Nederland aan digitale veiligheid wordt gehecht.[165]

Onvolledig beeld voor investeringen in digitale veiligheid

Voor een afweging is idealiter ook een beeld nodig van risico's, mogelijkheden en kosten van het verhogen van de weerbaarheid, maar dat is niet eenvoudig. Volgens het Centraal Planbureau (CPB) hebben organisaties een onvolledig beeld van de kosten en baten[XII] van investeringen in cyberveiligheid en is er sprake van diverse onzekerheden. Het investeringsniveau kan dan te hoog of te laag zijn. Een eerste reden voor het onvolledige beeld is dat er meerdere adviezen en richtlijnen circuleren over het optimale niveau van investeringen en over noodzakelijke maatregelen. Een tweede reden is dat informatie ontbreekt over de omvang van digitale risico's en de financiële gevolgen doordat organisaties: 1) niet iedere aanval opmerken, 2) niet iedere aanval publiek bekend willen maken en 3) niet altijd kunnen inschatten wat de gevolgen van een aanval op de lange termijn zijn.[166] Een derde reden is dat een deel van de gevolgen van inadequate cyberveiligheid bij derden kan neerslaan,[167] de eerder genoemde externe effecten. Ook wetenschappelijke – vooral economische – literatuur wijst op een 'informatieprobleem' voor het nemen van beslissingen over cybersecurity.[168]

XI Systemische cyberrisico's zijn in literatuur vooral gerelateerd aan het financiële systeem en financiële markten. Een reden voor deze focus is zeker gelegen in de lessen die te leren zijn uit de krediet-/bankencrisis die is ontstaan in de VS en die zich wereldwijd als een olievlek verspreidde.

XII Baten moet in dit kader worden beschouwd als de positieve effecten van weerbaarheidsverhogende maatregelen. Het gaat dan om het voorkomen van de gevolgen van cyberincidenten of, wanneer die zich toch voordoen het snel ontdekken daarvan, het beperken van de schade en het vereenvoudigen van het herstel.

Digitale weerbaarheid nog niet overal op orde

6 Weerbaarheid

De weerbaarheid tegen digitale dreigingen is nog niet overal op orde. Partijen zijn daardoor extra kwetsbaar voor cyberincidenten. Dat geldt zeker wanneer onvoldoende basismaatregelen zijn getroffen, die eerste barrières opwerpen tegen aanvallen, schade beperken en herstel eenvoudiger maken wanneer incidenten zich toch voordoen.

Hoewel basismaatregelen de digitale weerbaarheid van organisaties verhogen, blijft dit een weerbarstige opgave. Digitale diensten en processen zijn onderling verweven. Systemen bestaan uit vele componenten van hard- en software en zijn verbonden met allerlei andere systemen. Er zijn onveilige producten en diensten in de markt en 'gebruikers' gedragen zich in de digitale ruimte (onbewust) niet veilig. Dit alles introduceert potentiële bronnen voor technisch of menselijk falen en kwetsbaarheden die mogelijkheden creëren voor kwaadwillende actoren. Die actoren maken doelbewust misbruik van de digitale ruimte voor aanvallen.

Het ongestoord functioneren van vitale processen is essentieel voor de nationale veiligheid. Een compleet en scherp beeld van de digitale weerbaarheid van vitale processen en bijbehorende systemen ontbreekt (nog). De toezichthouders op aanbieders van vitale processen schetsen een divers beeld. Sommige instellingen zijn voldoende 'in control', andere niet. De informatiebeveiliging van de ministeries en onderzochte rijksorganisaties blijkt volgens de Algemene Rekenkamer nog steeds niet op orde te zijn.

Onvoldoende weerbaarheid vanwege ontbreken basismaatregelen

Bij veruit de meeste cyberaanvallen wordt nog steeds gebruik gemaakt van eenvoudige methoden. Deze blijven effectief doordat basismaatregelen onvoldoende zijn geïmplementeerd. Basismaatregelen kunnen ook tegen geavanceerde aanvallen helpen.

Organisaties niet opgewassen tegen phishing

Het is complex voor organisaties (en burgers) zich te wapenen tegen phishing, ook de afgelopen rapportageperiode weer de meest gebruikte (eerste stap voor) aanvalsmethodes.[169] Toch zijn er met basismaatregelen wel barrières op te werpen of kan verdere schade worden beperkt. Om phishing minder effectief te maken, voeren steeds meer organisaties campagnes uit onder werknemers om het bewustzijn van de gevaren van phishing te verhogen. Ook de overheid startte een bewustwordingscampagne. Uit onderzoek blijkt dat dit effect heeft: bij phishing-oefeningen dalen de clickrates.[170] In 2018 rapporteerde Google dat, door de inzet van security keys (fysieke hardware matige sleutels, bijvoorbeeld USB), geen enkele van hun meer dan 85.000 medewerkers succesvol is gephisht. Door de inzet van de keys was het klikgedrag van de gebruiker niet meer relevant.[171] De inzet van security keys wordt (nog) niet beschouwd als een basismaatregel, het laat wel zien dat het mogelijk is om de slagingskans van phishing zeer sterk te reduceren.

Phishing vraagt om voortdurende alertheid. Er wordt steeds minder geklikt op verkeerde links, maar het gebeurt nog wel. Aanvallers passen bovendien hun werkwijze aan. Phishing vindt traditioneel plaats via e-mail, maar het jaarbeeld geeft aan dat cybercriminelen ook gebruik maken van phishing via sms (smishing). Ook ontfutselen aanvallers steeds vaker succesvol gevoelige informatie via sociale media om iemand gericht te benaderen, zogeheten spear phishing.[172] Daardoor is voor een ontvanger lastig om te onderkennen dat het gaat om phishing.

Organisaties beschermen zich niet (altijd) tijdig tegen kwetsbaarheden

Organisaties blijken er niet altijd in te slagen om alle beveiligingsupdates tijdig te installeren. Uit onderzoek blijkt dat nog niet de helft van de kwetsbaarheden binnen 90 dagen wordt gepatcht.[173] Systemen zijn soms zelfs jarenlang kwetsbaar omdat beveiligingsupdates niet zijn geïnstalleerd. Bij veel geslaagde cyberaanvallen is gebruik gemaakt van een kwetsbaarheid die al jaren bekend is en waarvoor ook al jaren een update beschikbaar is.[174]

Doordat organisaties zich onvoldoende beschermen tegen kwetsbaarheden, is misbruik van bekende kwetsbaarheden in hard- en software nog steeds een succesvolle aanvalstechniek. Het is ook laagdrempelig. Volgens onderzoek van IBM groeit de populariteit van het gebruik van scanningtools door actoren. Daarmee zoeken ze eenvoudig en op grote schaal naar kwetsbare systemen. Zodra dit gevonden is, wordt het systeem binnengedrongen en gecompromitteerd.[175]

Snelle detectie kan gevolgen beperken, maar over het algemeen lang duurt het lang

Het vroegtijdig detecteren van aanvallen is een basismaatregel. Des te eerder, des te beter. Dat blijft echter voor veel organisaties een complexe opgave. Volgens een onderzoek was in 2019 de gemiddelde detectietijd van een aanval 56 dagen.[176] Deze gemiddelde detectietijd is niet in verhouding met de snelheid waarmee een aanvaller zijn doel kan bereiken. Die heeft slechts enkele uren nodig.[177] In het jaarbeeld staat dat actoren snel misbruik maken van gepubliceerde kwetsbaarheden.[178] Ook wanneer de aanvaller op minder snel succes uit is, bijvoorbeeld voor spionage, kan snelle detectie de schade beperken.

Ontbrekende maatregelen maken geslaagde aanvallen mogelijk

Criminelen worden steeds geavanceerder in hun aanpak en statelijke actoren zetten geavanceerde aanvalscapaciteiten breder in. Hoewel bescherming hiertegen complexer is dan tegen eenvoudige aanvalsmethoden, helpen basismaatregelen ook hier wel degelijk. Omdat die niet altijd worden getroffen, zijn organisaties extra kwetsbaar. De ransomware-aanval op de Universiteit Maastricht is een voorbeeld van een geavanceerde aanval waarbij basismaatregelen de impact waarschijnlijk hadden kunnen reduceren. In een periode van twee maanden hebben de criminelen het universiteitsnetwerk verkend en back-ups onbruikbaar gemaakt, voordat zij overgingen tot versleuteling van bestanden. Diverse basismaatregelen waren niet op orde, zoals een juiste afhandeling van meldingen van phishing, installatie van beveiligingsupdates, segmentatie van het netwerk, toepassing van monitoring en detectie en het opslaan van offline back-ups.[179] Ook bij het gebruik van zero-day kwetsbaarheden door bijvoorbeeld statelijke actoren, kan een combinatie van basismaatregelen, zoals segmentatie van het netwerk en goede monitoring en detectie, de impact reduceren.

Basisniveau weerbaarheid niet gehaald om diverse redenen

Geraadpleegde experts[XIII] geven aan dat het basisniveau voor cybersecurity *"[....] van veel organisaties c.q. ketenpartners (industrie, leveranciers) niet gehaald wordt, ofwel dat verbeteringen achterblijven, zeker gezien het zich steeds verder ontwikkelende dreigingslandschap"*. Wel geven zij aan dat bewustwording in organisaties is toegenomen en dat dit heeft geleid tot een toename van genomen maatregelen. Ook zien zij een verbetering op het gebied van investeringen in cybersecurity door verschillende organisaties.[180]

Expertraadpleging

Uit een expertraadpleging komen verschillende redenen naar boven waarom het basisniveau van cybersecurity niet gehaald wordt:

- *"Organisaties lijken zich onvoldoende te hebben voorbereid op bekende kwetsbaarheden. [....]*
- *Bestaande beveiligingsupdates worden niet of te laat geïmplementeerd. [....]*
- *Fouten in de I(C)T-architectuur met gebrek aan degelijke zonering, waardoor de impact van kwetsbaarheden hoger is dan nodig.*
- *Misconfiguratie van (IoT) apparaten, IT-systemen en cloud services waardoor ze onbedoeld van buitenaf benaderbaar zijn.*
- *Gebruik blijven maken van zwakke authenticatiemethoden.*
- *Onvoldoende eigen kennis en expertise van belangrijke (proces)systemen in een organisatie en informatiebeveiliging.*
- *Onvoldoende cyberveilig gedrag en cyberhygiëne van medewerkers zodat via steeds betere social engineering technieken (phishing, social media misbruik) medewerkers gemanipuleerd worden en de organisaties waar ze werken kwetsbaar blijven.*
- *Cybersecuritymaatregelen worden binnen organisaties nog heel vaak gezien als kostenpost en niet als (potentiële) business enabler.*
- *(Veelal kleinere) organisaties gebruiken een reactieve aanpak bij cybersecurity omdat deze het meest (kosten)efficiënt blijkt. Ze zullen pas gaan investeren wanneer ze geraakt worden door een cyberaanval of - incident. [....]".*[180]

XIII Zie hoofdstuk 1 Wijze van totstandkoming.

Digitale weerbaarheid is weerbarstige opgave

Hoewel basismaatregelen de digitale weerbaarheid van organisaties verhogen, blijft dit een weerbarstige opgave. Digitale diensten, processen en systemen zijn met elkaar en met fysieke processen, activiteiten en apparaten verweven. Er zijn onveilige producten en diensten in de markt en 'gebruikers' gedragen zich in de digitale ruimte (onbewust) niet veilig. Dit alles introduceert potentiële bronnen voor technisch of menselijk falen en kwetsbaarheden die mogelijkheden creëren voor kwaadwillende actoren. Die actoren maken doelbewust misbruik van de digitale ruimte voor aanvallen. Dit alles vermindert de digitale veiligheid, terwijl zwakke plekken voor een individuele partij en zelfs een land lastig te beïnvloeden zijn.

Negatieve effecten verwevenheid, complexiteit en connectiviteit

Het realiseren van een weerbare digitale infrastructuur is een uitdaging. Digitale diensten en processen zijn onderling verweven. Systemen bestaan uit vele componenten van hard- en software en zijn verbonden met allerlei andere systemen. Het jaarbeeld wijst op kwetsbaarheden door ketenafhankelijkheid en storingen met doorwerking in digitale en fysieke ketens. Aanvallers zijn zich goed bewust van de mogelijkheden van bijvoorbeeld compromittering van de leveranciersketen, generieke diensten en veel gebruikte producten.[182]

Onveilige producten en diensten achilleshiel digitale veiligheid

Digitaal onveilige producten en diensten zijn nog steeds een fundamentele oorzaak van cyberincidenten. Ze werken voor aanvallers drempelverlagend omdat ze het makkelijker maken om succesvolle aanvallen uit te voeren. De onveiligheid kan bijvoorbeeld ontstaan doordat leveranciers standaard onveilige configuraties leveren. Zo was er in 2019 een toename van misbruik van verkeerd geconfigureerde cloudtoepassingen. Het ging hier onder andere om openbaar toegankelijke cloudopslag, onbeveiligde databases en niet-afgeschermde back-upservers.[183] Onveiligheid kan ook ontstaan doordat leveranciers geen beveiligingsupdates (meer) beschikbaar stellen, deze updates niet eenvoudig te installeren zijn of updatemechanismen gecompromitteerd kunnen worden.

Compleet en scherp beeld weerbaarheid vitale processen ontbreekt (nog)

Het ongestoord functioneren van vitale processen is essentieel voor de nationale veiligheid. Relatief nieuw is het toezicht op (vooral) aanbieders van vitale processen[XIV] in het kader van de Wet beveiliging netwerk- en informatiesystemen (Wbni) door in die wet aangewezen toezichthouders. In de beleidsreactie op CSBN2019 is aangegeven dat de Inspectie Justitie en Veiligheid samen met andere Rijksinspecties zorg draagt voor een samenhangend inspectiebeeld over het digitale veiligheidsniveau van vitale processen.[184] Het eerste samenhangende inspectiebeeld verschijnt naar verwachting in 2021.

Een compleet en scherp beeld van de digitale weerbaarheid van vitale processen en bijbehorende systemen ontbreekt (nog). Het verkrijgen van een compleet inzicht, inclusief de mate waarin maatregelen effectief en efficiënt zijn, is complex. Zo zijn betrouwbare methoden en technieken om de weerbaarheid te meten voor een beoordeling van de risico's voor de nationale veiligheid nog in ontwikkeling. Het toezicht op cybersecurity in het kader van de Wbni bestaat voor een aantal toezichthouders nog niet heel lang. Wel zijn dit jaar de eerste effecten zichtbaar van een beter inzicht bij toezichthouders in de digitale weerbaarheid van aanbieders van vitale processen.[XV]

De toezichthouders op aanbieders van vitale processen schetsen een divers beeld. De weerbaarheid van de onder toezicht staande instellingen varieert. Sommige instellingen zijn voldoende in control, andere niet. Enerzijds menen de toezichthouders een duidelijke focus te zien op de continuïteit van processen en systemen en de implementatie van bijbehorende maatregelen. Anderzijds vinden ze dat er op het gebied van detectie, respons en herstel nog een wereld te winnen is. Basismaatregelen in relatie tot autorisaties en het doorvoeren van beveiligingsupdates lijken niet bij alle organisaties de aandacht te krijgen die ze verdienen. Dit zijn indicaties van een onvoldoende niveau van volwassenheid als het gaat om weerbaarheid tegen de digitale dreiging.

Ook uit onderzoeken van de Algemene Rekenkamer blijkt dat de weerbaarheid achterblijft. Zo constateerde de Algemene Rekenkamer in 2019 dat digitale beveiliging van vitale waterwerken in Nederland niet voldoende was.[185] In 2020 was de Algemene Rekenkamer zeer kritisch over een ander vitaal proces, namelijk het grenstoezicht. De cyberveiligheid van het grenstoezicht door de Koninklijke Marechaussee op Schiphol is onvoldoende en niet toekomstbestendig. Beveiligingstesten op de IT-systemen vinden niet tot nauwelijks plaats en systemen zijn operationeel zonder dat is vastgesteld of ze aan de beveiligingseisen voldoen. Ook zijn systemen niet aangesloten op de detectiecapaciteit van een Security Operations Center. Hierdoor bestaat het risico dat cyberaanvallen niet (tijdig) worden gedetecteerd. Een geslaagde aanval kan als consequentie hebben dat het grenstoezicht nauwelijks is uit te voeren met alle consequenties van dien. Het onderzoek liet ook zien dat, met geavanceerdere middelen, reizigersinformatie was te manipuleren. Daardoor kunnen personen die gesignaleerd zouden moeten zijn toch ongemerkt de grens passeren.[186]

XIV De Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) onderscheidt uiteenlopende categorieën aanbieders. Die van vitale processen zijn ondergebracht in diverse categorieën. Gemakshalve wordt hier gesproken van één categorie, namelijk 'aanbieders van vitale processen'.

XV Idem.

Informatiebeveiliging ministeries en rijksorganisaties niet op orde

In mei 2020 constateerde de Algemene Rekenkamer dat het belang van informatiebeveiliging beter op het netvlies staat dan eerder bij ministeries en rijksorganisaties en dat er rijksbreed inspanningen zijn geleverd. Zes van de zestien onderzochte ministeries en rijksorganisaties hebben de informatiebeveiliging op orde[187] in plaats van het jaar daarvoor drie.[188] Negen andere zijn nog niet zo ver. De Algemene Rekenkamer stelt vast dat het niveau van beveiliging verschilt per ministerie en wijst er op dat de ministeries van elkaar afhankelijk zijn bij uitwisseling van (geheime) informatie. Hier bepaalt de zwakste schakel de sterkte van de keten.[189]

Net als eerdere jaren plaatst de Algemene Rekenkamer kritische kanttekeningen bij het beheer en onderhoud van ICT. Bij beheer gaat het over de vraag of de systemen goed werken en of er weinig storingen zijn. Het IT-beheer laat nog te wensen laat. Goed beheer houdt onder meer in dat alleen bevoegden toegang hebben tot de systemen, dat medewerkers geen ruimere rechten hebben dan nodig is en dat wijzigingen worden getest voor ingebruikname. Onderhoud moet ertoe leiden dat de systemen met hun tijd meegaan en ook in de toekomst blijven werken. De Rekenkamer constateert dat er op zes van de elf onderzochte ministeries voldoende kennis is over de staat van de ICT-systemen, wat het kost om ze in de lucht te houden en hoe groot het risico is op storingen. Over de andere ministeries oordeelt de Rekenkamer kritischer.[190]

Wat als u wordt getroffen door een ransomware-aanval?

7 Dreigingsscenario's

In de voorgaande hoofdstukken werd aandacht besteed aan digitale dreigingen, digitale weerbaarheid en belangen die in het geding zijn wanneer cyberincidenten zich voordoen. Maar wat betekent dat voor u of uw organisatie?

Om te helpen bij de beantwoording van die vraag, beschrijft dit hoofdstuk drie samenhangende scenario's. Ze schetsen verschillende aspecten van 'inzet van ransomware', een werkwijze van actoren die zich in 2019 veelvuldig voordeed. U kunt deze scenario's gebruiken om binnen uw organisatie na te gaan of het scenario zich bij u zou kunnen voordoen, welke voorbereidingen u hebt getroffen en wat u zou doen wanneer u ooit in die situatie terecht komt. Functionarissen die een rol kunnen krijgen bij grotere incidenten, kunnen zich de vraag stellen in hoeverre zij zijn voorbereid op deze scenario's en wat zij dan zouden kunnen doen. Voor verdere voorbereiding op schade beperking en snel herstel verwijzen we ook naar Het Nationaal Crisisplan Digitaal. [191]
Het schetsen van dreigingsscenario's is nieuw ten opzichte van eerdere CSBN's. De scenario's zijn in opdracht van de NCTV door TNO opgesteld.

Scenario 1a: grootschalige aanval met ransomware via de leverancierskeketen

Beschrijving gebeurtenissen

Cybercriminelen hebben via spear phishing toegang gekregen tot het klantenbestand van Vendorizon[XVI], een verkoper van onder andere populaire administratiesoftware. Het bedrijf verkoopt wereldwijd softwarepakketten en beheeroplossingen van verschillende leveranciers aan publieke en private organisaties in diverse sectoren. De aanvallers zijn in staat om een malafide beveiligingsupdate specifiek voor de administratiesoftware beschikbaar te stellen aan de organisaties die deze software via Vendorizon gebruiken. Op het moment dat een gebruiker deze beveiligingsupdate uitvoert, wordt toegang verkregen tot diens netwerk en wordt er ransomware geïnstalleerd en uitgevoerd.

Doordat de update van een vertrouwde bron afkomstig is, voeren veel organisaties deze snel uit, vooral omdat het ogenschijnlijk om een kritieke kwetsbaarheid in de software gaat. Hierdoor verspreidt de ransomware zich in korte tijd onder honderden organisaties in diverse sectoren, waaronder in Nederland. Mediageruchten over een grote ransomware-aanval verspreiden zich snel. In eerste instantie wordt de oorzaak gezocht bij de fabrikant van de software. Al vrij snel daarna wordt duidelijk dat alleen organisaties die bij Vendorizon deze software hebben afgenomen, zijn getroffen via de malafide beveiligingsupdate. Andere klanten stoppen uit voorzorg tijdelijk met het uitvoeren van updates.[XVII] Hierdoor verspreidt de ransomware zich na een dag nauwelijks verder.

Duiding

Spear phishing is nog altijd een aantrekkelijke tactiek voor cybercriminelen om toegang te krijgen tot het netwerk van een organisatie.[192] Vervolgens worden andere middelen ingezet om de aanval verder te ontplooien.

Aanvallen die uitgevoerd worden via ketenpartners komen in het jaarbeeld naar voren als een belangrijke dreiging. Hierbij is het van

XVI Elke gelijkenis met een bestaand bedrijf berust puur op toeval en is niet zo bedoeld.
XVII Normaliter is het zo snel mogelijk doorvoeren van updates een weerstandsverhogende maatregel. In een situatie waarin een ketenpartner gecompromitteerd is, kan dat anders uitpakken.

belang om te beseffen dat afhankelijkheden tussen partijen zich op vele manieren kunnen manifesteren. Er hoeft niet altijd een directe technische verbinding te bestaan. Ook functionele afhankelijkheden kunnen voor kwaadwillende actoren een ingang vormen. Zo kan een ketenpartner informatie hebben of toegang tot gevoelige informatie over kwetsbaarheden bij een organisatie, bijvoorbeeld door outsourcing.

Cybercriminelen zijn in staat ransomware steeds beter te verhullen in ogenschijnlijk betrouwbare software. Doordat in dit scenario de aanvallers gebruik maken van vertrouwde communicatiekanalen, is deze nog moeilijker te detecteren dan wanneer het via (spear) phishing gebeurt.

Dit scenario laat tevens zien dat er een belangenafweging is tussen het snel patchen om de digitale veiligheid van de systemen te waarborgen versus de impact die het patchen kan hebben op de bedrijfscontinuïteit. Zo kan een juiste beslissing tot het snel uitvoeren van een beveiligingsupdate die van een betrouwbare partner afkomstig is, toch tot een ongewenste situatie leiden wanneer deze ketenpartner gecompromitteerd blijkt te zijn. Dit onderstreept het belang van informatie-uitwisseling (zoals Indicators of Compromise -IoCs-)[193] tussen ketenpartners.

Kernvragen voor de lezer

1. Heeft u een goed beeld van de hard- en software die u gebruikt in uw organisatie en ontvangt u van de leveranciers actuele informatie over kwetsbaarheden en updates?
2. Welke afspraken zijn er met uw ketenpartners gemaakt over het uitwisselen van relevante soorten cybersecurity informatie (zoals IoCs, technische en incident respons informatie)[194]?
3. Heeft u nagedacht over mogelijke risico's die uw organisatie loopt als gevolg van interactie met klanten, leveranciers en overige dienstverleners en heeft u maatregelen getroffen om de risico's van deze ketenafhankelijkheden te beheersen?
4. Heeft u bestaande contacten binnen relevante overheidsorganisaties, waaronder ook de politie, om in het geval van een cyberincident melding te maken, hulp in te roepen en/of aangifte te doen?

Scenario 1b: belang van basismaatregelen om impact van ransomware te beperken

Beschrijving gebeurtenissen

Een grote groep organisaties is via een malafide beveiligingsupdate van administratiesoftware getroffen door ransomware. Het blijft onduidelijk hoeveel organisaties precies getroffen zijn omdat sommige organisaties transparant en open zijn over de aanval, terwijl andere veel terughoudender zijn. Dit doet vermoeden dat er wellicht ook organisaties zijn getroffen die hier helemaal geen openbaarheid aan geven.

Uit de informatie van de organisaties die wel openheid tonen, blijkt dat de aanvallers aanzienlijke bedragen losgeld vragen in ruil voor het weer vrijgeven van de gegevens. Een klein deel van de getroffen organisaties is zelf in staat met behulp van back-ups hun getroffen systemen weer in de lucht te krijgen. Zij die het niet zelf kunnen, schakelen hulp in om vanuit een back-up (handmatig) alle getroffen computers opnieuw te installeren en configureren. Dit neemt, afhankelijk van de organisatie, enkele dagen tot twee weken in beslag. Een aanzienlijk deel van de getroffen organisaties heeft echter geen recente back-up, of een back-up die niet toegankelijk is doordat die verbonden is met een gecompromitteerd deel van het netwerk. Zij zien zich genoodzaakt om over te gaan tot betaling van het losgeld omdat anders alle gegijzelde gegevens als verloren moeten worden beschouwd.

Een deel van de getroffen organisaties heeft een cyberverzekering afgesloten en maakt daar aanspraak op. Ook gaan er geruchten op sociale media dat een aantal organisaties weliswaar een back-up heeft, maar op basis van een kostenafweging toch overgaat tot losgeldbetaling. Het opnieuw installeren van de computers en opschonen van systemen is namelijk voor veel organisaties een omvangrijke en daarmee kostbare exercitie. In het publieke debat wordt veel kritiek geuit op de organisaties die losgeld betaald hebben. Er komt een felle discussie op gang over de mogelijkheden van het beboeten van organisaties die overgaan tot betaling van losgeld, zeker nu de dreiging van ransomware aanvallen blijft toenemen.

Duiding

Het jaarbeeld besteed aandacht aan ransomware aanvallen.[195] Een discussiepunt is of het wel of niet acceptabel is om losgeld te betalen. Er wordt hierbij vaak aangegeven dat het een afweging is tussen enerzijds het belang van het bedrijf en anderzijds het maatschappelijk belang om het verdienmodel voor dit type criminaliteit te ondermijnen. In de praktijk is het voor veel organisaties een lastige afweging omdat ze maar één optie hebben als ze hun data terug willen krijgen, wanneer ze geen backups hebben of deze ook zijn getroffen. Het op orde hebben van een aantal basismaatregelen is dus essentieel bij dit vraagstuk. Hoe kan ervoor gezorgd worden dat er wel realistische opties zijn om af te wegen?

Een ander aspect dat in dit scenario naar voren komt, is de mate van openheid over dit soort aanvallen en het gevolg daarvan voor het getroffen bedrijf. Hoewel openheid over een geslaagde cyberaanval in eerste instantie tot imagoschade kan leiden, kan het ook tot waardering leiden in de publieke opinie als een organisatie zich kwetsbaar en transparant opstelt en de geleerde lessen beschikbaar maakt voor andere organisaties.

Weer een ander aspect is het doen van aangifte bij de politie. Dat leidt ertoe dat de daders mogelijk kunnen worden opgespoord en verantwoordelijk gehouden voor hun criminele daden. Zo kunnen nieuwe slachtoffers worden voorkomen.

Kernvragen voor de lezer

1. Heeft uw organisatie een procedure voor het gebruik van back-ups en test u geregeld of die back-ups werken?
2. Heeft u andere maatregelen getroffen zoals het scheiden van de netwerken binnen uw organisatie zodat malware zich moeilijker kan verspreiden?
3. Als u getroffen zou worden door ransomware, weet u dan wat u kan doen?
4. Zou u bij een geslaagde aanval wel of niet informatie over de aanval en geleerde lessen delen en/of daarmee de publiciteit opzoeken en/of aangifte doen bij de politie? En waarom?

Scenario 1c: probleem opgelost! Of toch niet...?

Beschrijving gebeurtenissen

Enkele maanden nadat hightech bedrijf zMART-Veder[XVIII] getroffen bleek door ransomware komt het bedrijf opnieuw in het nieuws vanwege een cyberaanval. zMART-Veder maakt onder hoge druk van diverse anonieme berichten op sociale media (die melden dat hun innovatieve technologie gestolen zou zijn) melding van een datalek, dat een grote hoeveelheid bedrijfsvertrouwelijke gegevens van hun innovatieve technologie betreft. Het bedrijf ziet haar aandelen op de financiële beurzen kelderen. Een ingehuurd forensisch onderzoeksbedrijf maakt bekend dat er aanwijzingen zijn dat het datalek gerelateerd kan worden aan een Advanced Persistent Threat (APT) groep van een statelijke actor in Azië. Het vermoeden is dat een professionele groep cybercriminelen, gespecialiseerd in het verkrijgen van toegang via phishing aanvallen, toegang tot enkele organisaties heeft doorverkocht aan deze statelijke actor. Dat vond plaats in dezelfde periode als de ransomware aanval.[196]

In dezelfde periode worden in het IT-netwerk van energieleverancier Current Streams[XIX] sporen gevonden van de voorbereiding op een cyberaanval die - indien uitgevoerd - zou leiden tot een grootschalige verstoring van de energielevering door het bedrijf. Current Streams was ook één van de organisaties die een aantal maanden geleden te maken kreeg met ransomware in hun IT systemen. De gevolgen van de ransomware bleven beperkt tot de kantoorautomatisering. De nu ontdekte inbraaksporen laten zien dat de aanvallers ook toegang hebben verkregen tot de operationele technologie van het bedrijf. De sporen lijken bovendien kenmerken te vertonen van modi operandi van een APT groep die bekend staat om hun sabotage- en beïnvloedingsgerichte activiteiten (het verstoren van vitale infrastructuur en manipuleren van democratische processen). Deze APT groep is sterk gelieerd aan een land in het Midden-Oosten, dat het afgelopen jaar veel in het nieuws is geweest als gevolg van diverse geopolitieke disputen met de Verenigde Staten en de Europese Unie.

Duiding

Nadat organisaties zijn hersteld van een ransomware aanval en het stof weer lijkt te zijn neergedaald, is het begrijpelijk dat de indruk bestaat dat de aanval hiermee is beëindigd. Zeker wanneer een grotere groep organisaties is getroffen door dezelfde ransomware, is er het beeld dat ze niet bewust een doelwit waren, maar vooral pech hebben gehad. Cybercriminelen specialiseren zich in toenemende mate in onderdelen van een aanval om hun verdienmodel te verbeteren. Hier wordt het voorbeeld gegeven van een groep die via geavanceerde ransomware toegang heeft verkregen tot de bedrijfsnetwerken van de slachtoffers. Dit leidt er toe dat ze naast het versleutelen van gegevens ook in staat zijn om toegangsgegevens en mogelijk andere waardevolle gegevens te bemachtigen. Hiermee kunnen ze naast het eventuele losgeld ook geld verdienen door deze gegevens door te verkopen aan andere actoren (in dit scenario APTs).

De grens tussen criminele en statelijke activiteiten lijkt te vervagen, waardoor aanvallen opgebouwd uit verschillende (gecoördineerde) stappen ook vaker voorkomen. Het is dus belangrijk om alert te blijven, ook nadat een aanval lijkt te zijn afgelopen. Is de aanval wel echt voorbij? Wat heeft zich nog meer in de systemen afgespeeld? Zijn er ook gevoelige gegevens buitgemaakt? Of hebben de criminelen nog een manier gevonden om geld te verdienen, bijvoorbeeld door de toegang door te verkopen aan andere kwaadwillende partijen? En hebben andere partijen zich niet allang in de systemen genesteld?

Kernvragen voor de lezer

1. Waarom zou een statelijke actor geïnteresseerd kunnen zijn in uw organisatie? Kan uw organisatie een interessante opstap zijn voor bijvoorbeeld een klant van u of anderen in de keten?
2. Welke maatregelen heeft uw organisatie getroffen om de ICT infrastructuur te monitoren en verdachte activiteiten te detecteren?
3. Welke gegevens in uw organisatie beschouwt u als uw "kroonjuwelen"? Hoe zijn deze extra beschermd tegen potentiële compromittering?
4. Zijn de cyberprofessionals in uw organisatie voldoende getraind in het herkennen van de mogelijke complexiteit van cyberaanvallen?

XVIII Elke gelijkenis met een bestaand bedrijf berust puur op toeval en is niet zo bedoeld.

XIX Elke gelijkenis met een bestaand bedrijf berust puur op toeval en is niet zo bedoeld.

Bijlagen

Bijlage 1
Afkortingen- en begrippenlijst

Aanval	Zie cyberaanval.
Actor	Een persoon of samenstelling van personen die een cyberaanval uitvoert of de intentie daartoe heeft. Voorbeelden zijn: a) staten/ staatsgelieerde actor, b) criminelen, c) terroristen, d) hacktivisten, e) cybervandalen en scriptkiddies en f) insiders.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst.
AP	Autoriteit Persoonsgegevens.
Authenticatie	Het vaststellen van de identiteit van een gebruiker, computer of applicatie.
Basismaatregelen	Activiteiten die zijn gericht op realisatie van minimaal noodzakelijke fysieke, procedurele, gedragsmatige en technische waarborgen opdat cyberincidenten kunnen worden voorkomen en wanneer cyberincidenten zich toch hebben voorgedaan deze kunnen worden ontdekt, schade kan worden beperkt en herstel eenvoudiger kan worden gemaakt. Dit wordt ook wel cyberhygiëne genoemd. Het gaat bijvoorbeeld (maar niet alleen) om het maken van (online en offline) back-ups.
Belang(en)	Waarden, verworvenheden, materiele en immateriële zaken waaraan schade kan ontstaan als een cyberincident zich voordoet en het gewicht dat de maatschappij of een partij aan de verdediging ervan toekent. In het CSBN ligt de focus op nationale veiligheidsbelangen.
Beschikbaarheid	De zekerheid dat gebruikers in een digitaal systeem of bij informatie kunnen of gebruik kunnen maken van digitale diensten of processen wanneer zij dat willen of zouden moeten kunnen. Gepland onderhoud telt niet mee.
Bitcoin	Digitale munteenheid, zie cryptovaluta.
Botnet	Een verzameling van besmette systemen die door actoren centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
Clouddienst	ICT-infrastructuur die via het internet beschikbaar wordt gesteld als dienst.
Crimineel/ criminele actor	Actor die aanvallen pleegt met economische of financiële motieven.
Cryptovaluta	Verzamelnaam voor digitale munteenheden die cryptografische berekeningen gebruiken als echtheidskenmerk en voor transacties.

Cvd	Coordinated vulnerability disclosure is de praktijk van het gecoördineerd melden van aangetroffen beveiligingslekken. Hierbij worden afspraken gehanteerd die doorgaans neerkomen op dat de melder de ontdekking niet deelt met derden totdat het lek verholpen is, en de getroffen partij geen juridische stappen tegen de melder zal ondernemen. Voorheen werd dit responsible disclosure genoemd.
Cyber	Iets wat te maken heeft met digitale informatie en systemen die verbonden zijn met het internet.
Cyberaanval	Moedwillige activiteit van een cyberactor die is gericht op het met digitale middelen aantasten van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen.
Cybercrime/ cybercriminaliteit	Hierbij kan onderscheid worden gemaakt tussen cybercrime in enge zin (computer-focused) en cybercrime in ruime zin (computer-assisted en computer-enabled). • Computer-focused crime: ICT is hierbij het doelwit van aanvallen met behulp van ICT. Voorbeelden zijn hacking, DDoS-aanvallen en ransomware. • Computer-assisted crime: criminaliteit die voorheen analoog, maar nu hoofdzakelijk digitaal wordt gepleegd. Bijvoorbeeld CEO-fraude. • Computer-enabled crime: analoge criminaliteit die alleen maar in de fysieke wereld kan bestaan, maar waarvan delen van de modus operandi ondersteund worden door ICT. Zo kunnen drugs wel digitaal verhandeld worden, maar niet digitaal gesmokkeld of geconsumeerd. In toenemende mate zijn zo alle vormen van criminaliteit in zekere zin computer-enabled. Alle vormen van cybercrime kunnen een meer of minder geavanceerd karakter hebben. CSBN beperkt zich tot computer-focused cybercrime.
Cybercrime-as-a-service	Cybercrime-as-a-service betreft een omvangrijke online cybercriminele dienstverlening waarbij vrijwel elke stap voor het plegen en het beschermen van cybercrime verhandeld wordt. In het CSBN ligt de focus op 'dienstverlening' voor cyberaanvallen.
Cyberincident	Alle gebeurtenissen of activiteiten die de beschikbaarheid, integriteit of vertrouwelijkheid aantasten van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen. Verzamelbegrip voor cyberaanval en uitval.
Cybersecurity	Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Die schade kan bestaan uit de aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.
Cyberspace	Zie digitale ruimte.
Cybervandaal	Zie scriptkiddie.
DDoS	Distributed Denial of Service is een vorm van DoS waarbij een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal verschillende bronnen.
Digital domein	Zie digitale ruimte.
Digitale aanval	Zie cyberaanval
Digitale risico (risico cyberincidenten)	De kans dat een cyberincident zich voordoet en de impact daarvan, beide in relatie tot het actuele niveau van weerbaarheid.

Digitale ruimte	De digitale ruimte is de complexe omgeving die het resultaat is van de interactie tussen mensen, software en diensten op het internet, ondersteund door wereldwijd gedistribueerde fysieke informatie- en communicatietechnologie (ICT) -apparaten en verbonden netwerken. [XX] De digitale ruimte wordt ook wel omschreven als het 'digitale domein' of 'cyberspace'.
Digitale veiligheid	Het ongestoord functioneren van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen. De focus in het CSBN ligt op digitale veiligheid van de digitale ruimte, vitale processen en andere voor het functioneren van de (Nederlandse) maatschappij cruciale sectoren, digitale diensten en processen.
DNS	Het Domain Name System is het systeem dat internetdomeinnamen koppelt aan ip-adressen en omgekeerd. Zo staat het adres www.ncsc.nl bijvoorbeeld voor ip-adres 159.46.193.36. Verder vermeldt een DNS-record onder meer hoe e-mails aan dat domein afgehandeld moeten worden.
Doelwit	De digitale dienst of organisatie of het digitale proces of systeem waar een actor zich op richt met een cyberaanval.
DoS	Denial of Service is de benaming voor een type aanval die een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar maakt voor de gebruikelijke afnemers. Bij websites wordt meestal een DDoS-aanval uitgevoerd.
Dreiging	Een cyberincident dat zich kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten. In het CSBN gaat het primair om dreigingen die nationale veiligheidsbelangen kunnen aantasten.
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
Exploit	Software, gegevens of een opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om ongewenste functies of gedrag te veroorzaken.
Exploitkit	Hulpmiddel om een aanval op te zetten door te kiezen uit kant-en-klare exploits, in combinatie met gewenste gevolgen en besmettingsmethode.
Hacker/Hacken	De meest gangbare en de in dit document gehanteerde betekenis van hacker is iemand die met kwaadaardige bedoelingen probeert in te breken in ICT-systemen. Oorspronkelijk werd de term hacker gebruikt voor iemand die op onconventionele wijze gebruikmaakt van techniek (waaronder software), veelal om beperkingen te omzeilen of onverwachte effecten te bereiken.
Hacktivist	Samentrekking van hacker en activist: actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt.
ICS	ICS staat voor Industriële controlesystemen. Zie procesbesturingssystemen.
Impact	De aantasting van belangen wanneer een cyberincident zich voordoet. De focus in het CSBN ligt op de impact voor de nationale veiligheid in het algemeen of meer specifiek de impact op de digitale ruimte, vitale processen en andere voor het functioneren van de (Nederlandse) maatschappij cruciale digitale diensten en processen.
Incident	Zie cyberincident.
Industriële controlesystemen	Zie procesbesturingssysteem.

XX Betreft (vertaling van) definitie van cyberspace zoals opgenomen in ISO/IEC standard 27032: 2012 (E).

Informatiediefstal	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
Informatiemanipulatie	Het opzettelijk wijzigen van informatie; aantasting van de integriteit van informatie.
Insider	Een interne actor die met toegang tot systemen of netwerken van binnenuit een dreiging vormt, met als motief wraak, geldelijk gewin of ideologie. Een insider kan ook worden ingehuurd of opgedragen van buitenaf.
Integriteit	1. Bij informatie: juiste en volledige informatie, en verwerking van informatie. 2. Bij personen: de betrouwbaarheid van iemand. 3. Bij digitale diensten, processen of systemen: hun correcte werking.
IoT	Het Internet-of-Things is een netwerk van slimme apparaten, sensoren en andere objecten die (vaak verbonden met het internet) gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi-) autonome beslissingen of acties nemen die van invloed zijn op hun omgeving.
IP	Het internetprotocol zorgt voor de adressering van internetverkeer zodat het bij het beoogde doel aankomt.
Kwetsbaarheid	Een kwetsbaarheid is een eigenschap die een aanvaller de mogelijkheid biedt een cyberaanval uit te voeren of een eigenschap die kan leiden tot uitval. Dit kan zich voordoen in een digitale dienst, proces of systeem, maar ook in de samenleving als geheel of in een specifieke organisatie.
Lek	Aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.
Leverancierskеten	Een ecosysteem van dienstverleners die hard- en software, netwerken of diensten levert die door allerlei partijen worden gebruikt in hun netwerken en/of dienstverlening. Te denken valt aan cloud leveranciers.
Maatschappelijke ontwrichting	Er is sprake van een mogelijk ontwrichtend effect op de samenleving als één of meer van de zes nationale veiligheidsbelangen ernstig worden aangetast. (zie definitie nationale veiligheidsbelangen)
Malware	Samentrekking van malicious software. Malware is de term die als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en trojans.
Middel	Aanvalstechniek(en), software en hardware die een actor gebruikt of kan gebruiken voor een cyberaanval. Een voorbeeld is ransomware of DDoS-aanval. De focus ligt hier op 'de tool(box)' zelf en bij Modus operandi op de inzet ervan door een actor.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst.
MO	Zie Modus operandi.
Modus operandi	Een werkwijze die een actor gebruikt of kan gebruiken voor een cyberaanval. Denk aan voorbeelden zoals het combineren van middelen voor een aanval, het ongericht inzetten van het middel (schot hagel) of juist heel gericht inzetten e.d.. De focus ligt hier op de werkwijze en bij Middel op 'de tool(box)' zelf.
Nationale Veiligheid	De nationale veiligheid is in het geding wanneer een of meerdere nationale veiligheidsbelangen ernstig worden bedreigd. Nationale veiligheid gaat over alle opzettelijke en niet-opzettelijke risico's en dreigingen die kunnen leiden tot maatschappelijke ontwrichting in Nederland. Van overstroming tot terrorisme en van een grieppandemie tot een cyberaanval.

Nationale Veiligheidsbelangen	De zes nationale veiligheidsbelangen zijn: • Territoriale veiligheid: Het ongestoord functioneren van Nederland en haar EU en NAVO bondgenoten als onafhankelijke staten in brede zin, dan wel de territoriale veiligheid in enge zin. • Fysieke veiligheid: Het ongestoord functioneren van de mens in Nederland en zijn omgeving. • Economische veiligheid: Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie. • Ecologische veiligheid: Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland. • Sociale en politieke stabiliteit: Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtstaat en daarin gedeelde waarden. • Internationale rechtsorde: Het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid.
Partij	Verzamelbegrip voor organisaties, bedrijven, overheden en burgers.
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben informatie aan mensen te ontfutselen. Deze informatie kan worden misbruikt voor bijvoorbeeld toegang tot systemen.
Procesbesturingssysteem	Algemene naam voor verschillende typen systemen die fysieke processen aansturen zoals SCADA, DCS's, PLC's. Deze systemen openen bijvoorbeeld een sluis of zetten een windmolen uit. Ook wel aangeduid als industriële controlesystemen (ICS).
Ransomware	Gijzelsoftware. Type malware dat systemen of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt.
Sabotage	Het opzettelijk, zeer langdurig, aantasten van de beschikbaarheid van digitale diensten, processen of systemen. In extreme gevallen leidend tot vernietiging.
Scriptkiddie	Actor met beperkte kennis die hulpmiddelen gebruikt die door anderen zijn bedacht en ontwikkeld, voor digitale aanvallen, om kwetsbaarheden aan te tonen of voor de eigen uitdaging.
Spam	Ongewenste e-mail, doorgaans commercieel van aard.
Spear phishing	Spear phishing is een variant van phishing die zich richt op één persoon of beperkte groep mensen, die specifiek wordt uitgekozen op basis van hun toegangspositie, om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.
Spionage	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
Staatsgelieerde actor	Actor gelieerd aan een statelijke actor.
Statelijke actor	Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage).
Storing	Zie uitval.
Systeemmanipulatie	Het aantasten van de integriteit van digitale diensten, processen of systemen.

Terrorist	Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolkingsgroepen angst wil aanjagen of politieke besluitvorming probeert te beïnvloeden, door geweld tegen mensen te gebruiken of ontwrichtende schade aan te richten.
Tweefactorauthenticatie	Een manier van identiteit vaststellen waarvoor twee onafhankelijke bewijzen van identiteit zijn vereist.
Uitval	Een situatie waarin de beschikbaarheid of integriteit van informatie- en procesbesturingssystemen, daardoor verwerkte en opgeslagen informatie en daarvan afhankelijke diensten en processen is aangetast ongeacht de oorzaak daarvan. Een cyberaanval valt buiten het begrip uitval. In het CSBN gaat het vooral om uitval met (potentiële) keteneffecten in de digitale ruimte, vitale processen en andere voor het functioneren van de (Nederlandse) maatschappij cruciale processen.
Vertrouwelijkheid	De zekerheid dat informatie en/of digitale diensten, processen of systemen alleen toegankelijk zijn voor personen of software die hiertoe zijn geautoriseerd.
Vitale processen	Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur. Elektriciteit, toegang tot internet, drinkwater en betalingsverkeer zijn voorbeelden van vitale processen. Formeel zijn in Nederland achtentwintig processen benoemd als vitaal.[197]
Weerbaarheid	Het vermogen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Dat kan met technische, procedurele of organisatorische maatregelen. Andere manieren zijn bijvoorbeeld wetgeving, subsidieverlening, scholing om gebruikers te bekwamen in veilig gedrag, voorlichtings- en bewustwordingscampagnes, samenwerking tussen partijen en normerende kaders voor digitalisering van diensten en processen en ontwerp van systemen.
Zero-day kwetsbaarheid	Een kwetsbaarheid waarvoor nog geen patch beschikbaar is, omdat de maker van de kwetsbare software nog geen tijd (nul dagen) heeft gehad om de kwetsbaarheid te verhelpen.

Bijlage 2
Bronnen en referenties

1 ‘Cybersecuritybeeld Nederland 2019’, NCTV, 12-06-2019.
2 'VOORUITZIEND VERMOGEN VOOR VREDE&VEILIGHEID. De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is. Openbaar jaarverslag 2019, april 2020.
3 ‘AIVD Jaarverslag 2019’, AIVD, april 2020.
4 'VOORUITZIEND VERMOGEN VOOR VREDE&VEILIGHEID. De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is. Openbaar jaarverslag 2019, april 2020.
5 ‘AIVD Jaarverslag 2019’, AIVD, april 2020.
6 ‘AIVD Jaarverslag 2019’, AIVD, april 2020, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2020/04/29/jaarverslag-2019/Jaarverslag+2019+webversie.pdf; 'VOORUITZIEND VERMOGEN VOOR VREDE&VEILIGHEID. De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is. Openbaar jaarverslag 2019, april 2020.
7 ‘AIVD Jaarverslag 2019’, AIVD, april 2020; 'VOORUITZIEND VERMOGEN VOOR VREDE&VEILIGHEID. De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is. Openbaar jaarverslag 2019, april 2020.
8 'VOORUITZIEND VERMOGEN VOOR VREDE&VEILIGHEID. De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is. Openbaar jaarverslag 2019, april 2020.
9 ‘AIVD Jaarverslag 2019’, AIVD, april 2020.
10 'VOORUITZIEND VERMOGEN VOOR VREDE&VEILIGHEID. De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is. Openbaar jaarverslag 2019, april 2020.
11 ‘Jaarverantwoording 2019 politie’, Politie Nederland, 13-1-2020.
12 ‘A Guide to LockerGoga, the Ransomware Crippling Industrial Firms ‘, Wired, 25-03-2019, https://www.wired.com/story/lockergoga-13ransomware-crippling-industrial-firms/ geraadpleegd op 16-01-2020
13 'Threat Research. APT41: A Dual Espionage and Cyber Crime Operation', FireEye, 7-8-2019, https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html.
14 ‘Jaarverantwoording 2019 politie’, Politie Nederland, 13-1-2020; ‘Resultaten online expertraadpleging CSBN 2020’; ‘Internet Organised Crime Threat Assessment’ (IOCTA) 2019, Europol, 09-10-2019, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019; NCSC Magazine Editie 1, NCSC, 01-12-2019, https://magazines.ncsc.nl/ncscmagazine/2019/01; ‘Targeted Ransomware: Proliferating Menace Threatens Organizations’, Symantec, 18-07-2019, https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat.
15 ‘Jaarverantwoording 2019 politie’, Politie Nederland, 13-1-2020; 'Travelex being held to ransom by hackers', BBC.com, 7-1-2020, https://www.bbc.com/news/business-51017852.
16 ‘Maze Ransomware Gang Dumps Purported Victim List’, Bank Infosecurity, 17-12-2019, https://www.bankinfosecurity.com/blogs/maze-ransomware-gang-dumps-purported-victim-list-p-2839 geraadpleegd op 22-01-2020; ‘Allied Universal Breached by Maze Ransomware, Stolen Data Leaked’, Bleeping Computer, 21-11-2019, https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/ geraadpleegd op 22-01-2020; ‘Ransomware Hackers Have Started Leaking City Of Pensacola Data’, Forbes, 31-12-2019, https://www.forbes.com/sites/leemathews/2020/12/31/ransomware-hackers-have-started-leaking-city-of-pensacola-data/#14b3872f994b geraadpleegd op 22-01-2020; ‘Nemty Ransomware to Start Leaking Non-Paying Victim's Data’, Bleeping Computer, 13-01-2010, https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data/ geraadpleegd op 22-01-2020; ‘Sodinokibi Ransomware Publishes Stolen Data for the First Time’, Bleeping Computer, 11-01-2020, https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time/ geraadpleegd op 16-01-2020.

17 'Mysterious New Ransomware Targets Industrial Control Systems', Wired, 3 februari 2020, https://www.wired.com/story/ekans-ransomware-industrial-control-systems/; 'EKANS Ransomware and ICS Operations', Dragos, 3 februari 2020, https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations.

18 'Hydro subject to cyber attack, Hydro', Hydro, 19-03-2019, https://www.hydro.com/en-NL/media/news/2019/hydro-subject-to-cyber-attack/ geraadpleegd op 02-01-2020.

19 'Big Norwegian Aluminum Producer Suffers Extensive Cyber Attack', Bloomberg, 19-03-2019, https://www.bloomberg.com/news/articles/2019-03-19/hydro-says-victim-of-extensive-cyber-attack-impacting-operations-jtfgz6td geraadpleegd op 02-01-2020.

20 'Third quarter 2019: Ramping up production in Brazil, declining market prices', Hydro, 23-10-2019, https://www.hydro.com/en-DE/media/news/2019/third-quarter-2019-ramping-up-production-in-brazil-declining-market-prices/ geraadpleegd op 02-01-2020.

21 'Jaarverantwoording 2019 politie', Politie Nederland, 13-1-2020; 'Ryuk ransomware targeting organisations globally', NCSC-UK, 21-06-2019, https://www.ncsc.gov.uk/news/ryuk-advisory geraadpleegd op 17-01-2020; Severe Ransomware Attacks Against Swiss SMEs, GovCERT.ch, 09-05-2019, https://www.govcert.ch/blog/36/severe-ransomware-attacks-against-swiss-smes geraadpleegd op 17-01-2020; 'BSI warnt vor gezielten Ransomware-Angriffen auf Unternehmen', BSI, 24-04-2019, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/BSI_warnt_vor_Ransomware-Angriffen-240419.html geraadpleegd op 17-01-2020.

22 'Jaarverantwoording 2019 politie', Politie Nederland, 13-1-2020.

23 'A One-two Punch of Emotet, TrickBot, & Ryuk Stealing & Ransoming Data', Cybereason, 02-04-2019, https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data geraadpleegd op 27-01-2020.

24 'UM Cyber Attack Symposium – Lessons learnt', Maastricht Universiteit, 05-02-2020, https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt geraadpleegd op 12-02-2020; 'Servers Universiteit Maastricht misten belangrijke update uit 2017', Security.nl, 6-2-2020, https://www.security.nl/posting/642659/Servers+Universiteit+Maastricht+misten+belangrijke+update+uit+2017.

25 'UM Cyber Attack Symposium – Lessons learnt', Maastricht Universiteit, 05-02-2020, https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt geraadpleegd op 12-02-2020; 'Cyberveiligheid in het onderwijs' [kamerbrief], Ministerie van Onderwijs, Cultuur en Wetenschap, 14-2-2020, https://www.tweedekamer.nl/downloads/document?id=4186214c-16fe-4891-842d-571b86e41a19&title=Reactie%20op%20het%20verzoek%20van%20het%20lid%20Wiersma%2C%20gedaan%20tijdens%20de%20Regeling%20van%20Werkzaamheden%20van%2014%20januari%202020%2C%20over%20een%20cyberaanval%20bij%20de%20Universiteit%20Maastricht.docx.

26 'Cyberveiligheid in het onderwijs' [kamerbrief], Ministerie van Onderwijs, Cultuur en Wetenschap, 14-2-2020, https://www.tweedekamer.nl/downloads/document?id=4186214c-16fe-4891-842d-571b86e41a19&title=Reactie%20op%20het%20verzoek%20van%20het%20lid%20Wiersma%2C%20gedaan%20tijdens%20de%20Regeling%20van%20Werkzaamheden%20van%2014%20januari%202020%2C%20over%20een%20cyberaanval%20bij%20de%20Universiteit%20Maastricht.docx.

27 'Cybersecuritybeeld Nederland 2019', NCTV, 12-06-2019.

28 'IBM X-Force Report: Ransomware Doesn't Pay in 2018 as Cybercriminals Turn to Cryptojacking for Profit', IBM, 26-02-2019, https://newsroom.ibm.com/2019-02-26-IBM-X-Force-Report-Ransomware-Doesnt-Pay-in-2018-as-Cybercriminals-Turn-to-Cryptojacking-for-Profit geraadpleegd op 17-01-2020.

29 'Hack at all cost: putting a price on APT attacks', Positive Technologies, 14-08-2019, https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/ geraadpleegd op 27-01-2020.

30 'Identifying Cobalt Strike team servers in the wild', Fox-IT, 26-02-2019, https://blog.fox-it.com/2019/02/26/identifying-cobalt-strike-team-servers-in-the-wild/ geraadpleegd op 28-01-2020.

31 '8 Legit Tools and Utilities That Cybercriminals Commonly Misuse', Dark Reading, 18-07-2019, https://www.darkreading.com/attacks-breaches/8-legit-tools-and-utilities-that-cybercriminals-commonly-misuse/d/d-id/1335254 geraadpleegd op 27-01-2020; 'AIVD Jaarverslag 2018', AIVD, april 2019.

32 'RDP-aanval kostte gemeente Lochem zo'n 200.000 euro', Security.nl, 26-09-2019, https://www.security.nl/posting/625572/RDP-aanval+kostte+gemeente+Lochem+zo%27n+200_000+euro geraadpleegd op 10-01-2020; 'Lochem legt computers dag plat na hack', Lochems Nieuws, 12-06-2019, https://www.lochemsnieuws.nl/2019/06/12/lochem-legt-computers-dag-plat-na-hack/ geraadpleegd op 28-01-2020.

33 'A Chinese APT is now going after Pulse Secure and Fortinet VPN servers', ethhack, 05-09-2019, https://ethhack.com/2019/09/a-chinese-apt-is-now-going-after-pulse-secure-and-fortinet-vpn-servers/ geraadpleegd op 17-02-2020; 'Continued Exploitation of Pulse Secure VPN Vulnerability', US-CERT, 10-01-2020, https://www.us-cert.gov/ncas/alerts/aa20-010a geraadpleegd op 17-02-2020; 'VPN warning: REvil ransomware targets unpatched Pulse Secure VPN servers', ZDNet, 06-01-2020, https://www.zdnet.com/article/vpn-warning-revil-ransomware-targets-unpatched-pulse-secure-vpn-servers/ geraadpleegd op 17-02-2020; 'Continued Exploitation of Pulse Secure VPN Vulnerability', US-CERT, 10-01-2020, https://www.us-cert.gov/ncas/alerts/aa20-010a geraadpleegd op 17-02-2020; 'Cybercriminals are Focusing on Vulnerable Edge Services', Fortinet, 19-11-2020, https://www.fortinet.com/blog/industry-trends/cybercriminals-target-entire-digital-footprint.html geraadpleegd op 17-02-2020; 'Criminelen verspreiden ransomware via Citrix-kwetsbaarheid', Security.nl, 24-1-2020, https://www.security.nl/posting/640914/Criminelen+verspreiden+ransomware+via+Citrix-kwetsbaarheid.

34 'Analyse van de gelopen risico's door de kwetsbaarheden in de virtual private network (VPN) software van het bedrijf Pulse Secure', tweedekamer, 11-02-2020, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z02670&did=2020D05619.

35 'Na de hack zou de Citrix-crisis aan Lochem voorbij gaan. Fout gedacht', NRC, 22-01-2020, https://www.nrc.nl/nieuws/2020/01/22/na-de-hack-zou-de-citrix-crisis-lochem-nu-niet-raken-fout-gedacht-a3987772 geraadpleegd op 20-02-2020

36 Informatie AIVD en MIVD.

37 'Criminelen verspreiden ransomware via Citrix-kwetsbaarheid', Security.nl, 24-1-2020, https://www.security.nl/posting/640914/Criminelen+verspreiden+ransomware+via+Citrix-kwetsbaarheid.

38 Microsoft is Alerting Hospitals Vulnerable to Ransomware Attacks, Bleepingcomputers, 01-04-2020, https://www.bleepingcomputer.com/news/security/microsoft-is-alerting-hospitals-vulnerable-to-ransomware-attacks/ geraadpleegd op 29-04-2020; FBI: groot aantal ziekenhuizen besmet met malware, security.nl, 31-03-2020, https://www.security.nl/posting/650102/FBI%3A+groot+aantal+ziekenhuizen+besmet+met+malware? Geraadpleegd op 29-04-2020; Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic, Bleepingcomputers, 26-03-2020, https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/ geraadpleegd op 29-04-2020; Overheid waarschuwt ziekenhuizen voor cyberaanval, Tijd.be, 25-03-2020, https://www.tijd.be/ondernemen/algemeen/Overheid-waarschuwt-ziekenhuizen-voor-cyberaanval/10216656 geraadpleegd op 29-04-2020; En pleine crise du coronavirus, les hôpitaux de Paris victimes d'une cyberattaque, lexpansion, 23-03-2020, https://lexpansion.lexpress.fr/high-tech/en-pleine-crise-du-coronavirus-les-hopitaux-de-paris-victimes-d-une-cyberattaque_2121692.html geraadpleegd op 29-04-2020; Hackers linked to Iran target WHO staff emails during coronavirus, Reuters, 02-04-2020, https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC geraadpleegd op 29-04-2020.

39 WHO Chief Impersonated in Phishing to Deliver HawkEye Malware, Bleepingcomputer, 19-03-2020, https://www.bleepingcomputer.com/news/security/who-chief-impersonated-in-phishing-to-deliver-hawkeye-malware/ geraadpleegd op 29-04-2020; Netwalker Ransomware Infecting Users via Coronavirus Phishing. Bleepingcomputer, 21-03-2020, https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/ geraadpleegd op 29-04-2020; HHS.gov Open Redirect Used by Coronavirus Phishing to Spread Malware, Bleepingcomputer, 23-03-2020, https://www.bleepingcomputer.com/news/security/hhsgov-open-redirect-used-by-coronavirus-phishing-to-spread-malware/ geraadpleegd op 29-04-2020.

40 Klanten Rabobank weer doelwit van phishingmail over corona, Security.nl, 26-03-2020, https://www.security.nl/posting/649516/Klanten+Rabobank+weer+doelwit+van+phishingmail+over+corona geraadpleegd op 29-04-2020.

41 Hackers are messing with routers' DNS settings as telework surges around the world, Cyberscoop, 25-03-2020, https://www.cyberscoop.com/dns-hijacking-covid-19-oski-bitdefender-telework/ geraadpleegd op 29-04-2020; Hackers Hijack Routers' DNS to Spread Malicious COVID-19 Apps, Bleepingcomputer, 23-03-2020, https://www.bleepingcomputer.com/news/security/hackers-hijack-routers-dns-to-spread-malicious-covid-19-apps/ geraadpleegd op 29-04-2020; Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book, MalwareBytes, 18-03-2020, https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/ geraadpleegd op 29-04-2020; Security researcher Marco Ramilli analyzed a new Coronavirus (COVID-19)-themed attack gathering evidence of the alleged involvement of an APT group, securityaffairs, 19-03-2020, https://securityaffairs.co/wordpress/99977/apt/apt27-abusing-covid-19.html geraadpleegd op 29-04-2020.

42 'Aanvallers wijzigen wereldwijd dns-instellingen domeinen', Security.nl, 11-01-2019, https://www.security.nl/posting/593796/Aanvallers+wijzigen+wereldwijd+dns-instellingen+domeinen geraadpleegd op 17-01-2020; 'DNS Attacks Grow More Frequent and Costly', Infosecurity Magazine, 18-06-2019, https://www.infosecurity-magazine.com/news/dns-attacks-grow-more-frequent/ geraadpleegd op 17-01-2020; 'Worst DNS attacks and how to mitigate them', Network World, 18-07-2019, https://www.networkworld.com/article/3409719/worst-dns-attacks-and-how-to-mitigate-them.html geraadpleegd op 17-01-2020 'Ongoing DNS hijacking and mitigation advice', NCSC-UK, 12-07-2019, https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice geraadpleegd op 17-01-2020; 'Exclusive: Hackers acting in Turkey's interests believed to be behind recent cyberattacks – sources', Reuters, 27-01-2020, https://www.reuters.com/article/us-cyber-attack-hijack-exclusive/exclusive-hackers-acting-in-turkeys-interests-believed-to-be-behind-recent-cyberattacks-sources-idUSKBN1ZQ10X geraadpleegd op 29-01-2020. 'DNS Infrastructure Hijacking Campaign, US-CERT, 10-01-2019, https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign geraadpleegd op 17-01-2020; 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', FireEye, 10-01-2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html geraadpleegd op 17-01-2020.

43 'Aanvallers wijzigen wereldwijd dns-instellingen domeinen', Security.nl, 11-01-2019, https://www.security.nl/posting/593796/Aanvallers+wijzigen+wereldwijd+dns-instellingen+domeinen; 'DNS Attacks Grow More Frequent and Costly', Infosecurity Magazine, 18-06-2019, https://www.infosecurity-magazine.com/news/dns-attacks-grow-more-frequent; 'Worst DNS attacks and how to mitigate them', Network World, 18-07-2019, https://www.networkworld.com/article/3409719/worst-dns-attacks-and-how-to-mitigate-them.html; 'Ongoing DNS hijacking and mitigation advice', NCSC-UK, 12-07-2019, https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice; 'DNS Infrastructure Hijacking Campaign', US-CERT, 10-01-2019, https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign; 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', FireEye, 10-01-2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html. Alle bronnen geraadpleegd op 17-01-2020.

44 Voor dat laatste: 'X-Force Threat Intelligence Index 2020', IBM, 2-2020.

45 'Resultaten online expertraadpleging CSBN 2020', TNO, 15-01-2020; 'Phishing verschuift naar SMS en WhatsApp', Betaalvereniging Nederland, 26-11-2019, https://www.betaalvereniging.nl/actueel/nieuws/phishing-sms-whatsapp; '1.105.987 euro schade door Smishing al dit jaar!', Cybercrime Info, 06-10-2019, https://www.cybercrimeinfo.nl/cybercrime/smishing/360597_1-105-987-euro-schade-door-smishing-al-dit-jaar.

46 'AIVD Jaarverslag 2019', AIVD, april 2020.

47 'Jaarverantwoording 2019 politie', Politie Nederland, 13-1-2020.

48 'Veel Nederlandse servers misbruikt voor botnetspam', Computable, 11-02-2020, https://www.computable.nl/artikel/nieuws/security/6877213/250449/nederland-in-top-drie-van-botnetspam.html geraadpleegd op 13-02-2020.

49 'DDoS rapportage 2019', Nationale Beheersorganisatie Internet Providers, concept 17-3-2020.

50 'Resultaten online expertraadpleging CSBN 2020', TNO, 15-01-2020.

51 'Risicorapportage cyberveiligheid economie 2019', CPB, oktober 2019, https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.

52 'Resultaten online expertraadpleging CSBN 2020', TNO, 15-01-2020; 'Jaarverslag 2018', AIVD, april 2019; 'MIVD Openbaar Jaarverslag 2018', MIVD, april 2019.

53 'Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers', Vice, 25-03-2019, https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers geraadpleegd op 17-01-2020.

54 'Avast deploys hardened self-defense and wider intelligence industry collaboration', Avast, 21-10-2019 https://blog.avast.com/ccleaner-fights-off-cyberespionage-attempt-abiss geraadpleegd op 03-01-2020.

55 'ASUS releases fix for Live Update tool abused in ShadowHammer attack', ZDNet, 26-03-2019, https://www.zdnet.com/article/asus-releases-fix-for-live-update-tool-abused-in-shadowhammer-attack/ geraadpleegd op 03-01-2020; 'Some ASUS Updates Drop Backdoors on PCs in 'Operation ShadowHammer', threatpost, 25-03-2019, https://threatpost.com/asus-pc-backdoors-shadowhammer/143129/ geraadpleegd op 20-02-2020;
'BIS spolupracovala se společností Avast na odvrácení útoku na její produkty', Czech Security Information Service (BIS), 21-10-2019, https://www.bis.cz/aktuality/bis-spolupracovala-se-spolecnosti-avast-na-odvraceni-utoku-na-jeji-produkty-6acda7bf.html geraadpleegd op 03-01-2020.

56 'Avast deploys hardened self-defense and wider intelligence industry collaboration', Avast, 21-10-2019 https://blog.avast.com/ccleaner-fights-off-cyberespionage-attempt-abiss geraadpleegd op 17-01-2020.

57 'AIVD Jaarverslag 2019', AIVD, april 2020.

58 'Cybersecurity in Operational Technology: 7 Insights You Need to Know', Ponemon Institute, maart 2019, https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report geraadpleegd op 16-03 2020.
59 'FBI and Federal Partners Brief Pipeline Industry Leaders on National Security Threats to Energy Infrastructure', FBI, 07-11-2019, https://www.fbi.gov/contact-us/field-offices/houston/news/press-releases/fbi-and-federal-partners-brief-pipeline-industry-leaders-on-national-security-threats-to-energy-infrastructure geraadpleegd op 22-01-2020 ; 'India confirms cyber attack on nuclear power plant', Financial Times, 31-10-2019, https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6 geraadpleegd op 22-01-2020; 'Drilling Deep: A Look at Cyberattacks on the Oil and Gas Industry', Trend Micro, 12-12-2019, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry geraadpleegd op 22-01-2020. 'Global Oil and Gas Cyber Threat Perspective', Dragos, augustus 2019, https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf geraadpleegd op 22-01-2020.
60 '2019 Year in review. The ICS landscape and threat activity groups', Dragos, 2020.
61 'New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East', Securityintelligence, 04-12-2019, https://www.computable.nl/artikel/nieuws/security/6877213/250449/nederland-in-top-drie-van-botnetspam.html geraadpleegd op 13-02-2020, 'A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems', Wired, 20-11-2019, https://www.wired.com/story/iran-apt33-industrial-control-systems/, geraadpleegd op 13-02-2020
62 'More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting', TrendMicro, 12-12-2019, https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting/, geraadpleegd op 13-02-2020
63 'AIVD Jaarverslag 2019', AIVD, april 2020.
64 'AIVD Jaarverslag 2019', AIVD, april 2020; 'VOORUITZIEND VERMOGEN VOOR VREDE&VEILIGHEID. De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is. Openbaar jaarverslag 2019, april 2020; 'Nederland-China: een nieuwe balans', Ministerie van Buitenlandse Zaken, mei 2019, https://www.rijksoverheid.nl/documenten/rapporten/2019/05/15/nederland-china-een-nieuwe-balans; 'Speech Dick Schoof op Dutch Transformation Forum over economische veiligheid', AIVD.nl, 21-11-2019, https://www.aivd.nl/documenten/toespraken/2019/11/20/speech-dick-schoof-op-dutch-transformation-forum-over-economische-veiligheid, geraadpleegd op 15-2-2020.
65 'Iraanse overheidshackers vallen Nederlandse onderwijsinstellingen aan', NOS, 14-2-2020, https://nos.nl/artikel/2322945-iraanse-overheidshackers-vallen-nederlandse-onderwijsinstellingen-aan.html.
66 Feedback van een externe partner. Toestemming verkregen dit op te nemen.
67 'FINTEAM: Trojanized TeamViewer Against Government Targets', Check Point, 22-04-2019, https://research.checkpoint.com/2019/finteam-trojanized-teamviewer-against-government-targets/ geraadpleegd op 17-01-2020.
68 'AIVD Jaarverslag 2019', AIVD, april 2020.
69 'Jaarverantwoording 2019 politie', Politie Nederland, 13-1-2020.
70 Feedback professor Herbert Bos, Computer Systems Section van de Vrije Universiteit Amsterdam.
71 'Fortinet SSL VPN vulnerability from May 2019 being exploited in wild', Kevin Beaumont, 22-08-2019 https://twitter.com/GossiTheDog/status/1164536461665996800 geraadpleegd op 06-01-2020; 'Pulse Secure SSL VPN vulnerability being exploited in wild', Kevin Beaumont, 22-08-2019 https://twitter.com/GossiTheDog/status/1164553625881972739 geraadpleegd op 06-01-2020.
72 'Intern netwerk honderden bedrijven en ministerie lag maandenlang wagenwijd open', De Volkskrant, 28-9-2019, https://www.volkskrant.nl/nieuws-achtergrond/intern-netwerk-honderden-bedrijven-en-ministerie-lag-maandenlang-wagenwijd-open~b9c96034/.
73 'Bedrijven en overheid maandenlang kwetsbaar door groot beveiligingslek', NOS, 28-09-2019, https://nos.nl/artikel/2303667-bedrijven-en-overheid-maandenlang-kwetsbaar-door-groot-beveiligingslek.html geraadpleegd op 03-01-2020; 'Opnieuw groot risico door beveiligingslek bij thuiswerksysteem', NOS, 29-09-2019, https://nos.nl/artikel/2303866-opnieuw-groot-risico-door-beveiligingslek-bij-thuiswerksysteem.html geraadpleegd op 03-01-2020.
74 'Mitigation Steps for CVE-2019-19781', Citrix, 17-12-2019 https://support.citrix.com/article/CTX267679 geraadpleegd op 22-01-2020.
75 'Exclusief: Interview Citrix CISO, Fermín Serna, waar ging het mis?', Techzine, 23-1-2020, https://www.techzine.nl/blogs/security/436866/exclusief-interview-citrix-ciso-fermin-serna-waar-ging-het-mis/.
76 'Kwetsbaarheid gevonden in Citrix ADC, Citrix Gateway en Citrix SD-WAN WANOP', Nationaal Cyber Security Centrum, 24-12-2019, https://www.ncsc.nl/actueel/advisory?id=NCSC%2D2019%2D0979.
77 'Aanvallers zoeken actief naar kwetsbare Citrix-servers', Security.nl, 09-01-2020, https://www.security.nl/posting/638551/Aanvallers+zoeken+actief+naar+kwetsbare+Citrix-servers geraadpleegd op 22-01-2020.
78 'Honderden Nederlandse Citrix-servers kwetsbaar voor aanvallen' Security.nl, 13-01-2020, https://www.security.nl/posting/639015/Honderden+Nederlandse+Citrix-servers+kwetsbaar+voor+aanvallen geraadpleegd op 22-01-2020.

79 'Antwoord op vragen van het lid Van den Berg over het bericht 'MCL legt dataverkeer stil na cyberaanval', Tweedekamer, 10-02-2020, https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D05339&did=2020D05339.
80 'College Beoordeling Geneesmiddelen slachtoffer Citrix-aanval', security, 10-02-2020, https://www.security.nl/posting/643318/College+Beoordeling+Geneesmiddelen+slachtoffer+Citrix-aanval.
81 'Citrix releases final fixes for CVE-2019-19781', Citrix, 24-02-2020, https://www.citrix.com/blogs/2020/01/24/citrix-releases-final-fixes-for-cve-2019-19781/ geraadpleegd op 27-01-2020.
82 'Citrix: we volgden na lek standaardprocedure, gebeurt duizenden keren per jaar', NOS.nl, 18-1-2020, https://nos.nl/nieuwsuur/artikel/2319236-citrix-we-volgden-na-lek-standaardprocedure-gebeurt-duizenden-keren-per-jaar.html.
83 'Resultaten online expertraadpleging CSBN 2020', TNO, 15-01-2020.
84 'Voorbereiden op digitale ontwrichting', WRR, 2019, blz. 11, https://www.wrr.nl/binaries/wrr/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting/R101-Voorbereiden-op-digitale-ontwrichting.pdf geraadpleegd op 13-02-2020.
85 'NSA waarschuwt voor beveiligingsrisico's clouddiensten', Security.nl, 28-1-2020, https://www.security.nl/posting/641329/NSA+waarschuwt+voor+beveiligingsrisico%27s+clouddiensten.
86 'De storing bij KPN liet zien waarom de waarschuwing van de NCTV niet voorbarig is', Volkskrant.nl, 24-6-2019, https://www.volkskrant.nl/nieuws-achtergrond/de-storing-bij-kpn-liet-zien-waarom-de-waarschuwing-van-de-nctv-niet-voorbarig-is~bb9e2e41/; 'Onderzoek naar storing 112', Agentschap Telecom, 26-6-2019, https://www.agentschaptelecom.nl/actueel/nieuws/2019/06/26/onderzoek-naar-storing-112; 'KPN: softwarefout was oorzaak van storing 112, drie backups lieten het afweten', Volkskrant.nl, 25-6-2019, https://www.volkskrant.nl/nieuws-achtergrond/kpn-softwarefout-was-oorzaak-van-storing-112-drie-backups-lieten-het-afweten~b73d62b4/; 'Had de storing van 112 voorkomen kunnen worden?', Volkskrant.nl, 28-6-2019, https://www.volkskrant.nl/nieuws-achtergrond/had-de-storing-van-112-voorkomen-kunnen-worden~b235b093/; 'Ook dode in Den Haag tijdens 112-storing', RTL Nieuws, 3-7-2019, https://www.rtlnieuws.nl/nieuws/nederland/artikel/4767526/dode-den-haag-112-storing.
87 'Politie oefende niet voor 'zwaarste scenario' noodnummerstoring', de Volkskrant, 4-7-2019.
88 'Landelijke storing KPN' [Kamerbrief], Ministerie van Justitie en veiligheid', 25-6-2019, https://www.tweedekamer.nl/downloads/document?id=cc85aa5e-1e2b-4f4c-82b3-b9b20e215e9c&title=Brief%20van%20KPN%20inzake%20landelijke%20storing%20.pdf.
89 'Grote Google-storing trof Gmail, YouTube en diensten van derden', Tweakers.net, 3-6-2019, https://tweakers.net/nieuws/153510/grote-google-storing-trof-gmail-youtube-en-diensten-van-derden.html; 'Als het internet een hartaanval krijgt; Internet Door techniek uit 1989 kan het web stilvallen', NRC.NEXT, 13-7-2019, https://www.nrc.nl/nieuws/2019/07/12/als-het-internet-een-hartaanval-krijgt-a3966947; 'BGP Route Leak Causes Cloudflare and Amazon AWS Problems', Bleepingcomputer.com, 24-6-2019, https://www.bleepingcomputer.com/news/technology/bgp-route-leak-causes-cloudflare-and-amazon-aws-problems;, 'Major websites and services across the internet went down Tuesday because of a hosting-platform outage', Businessinsider.nl, 2-7-2019, https://www.businessinsider.nl/cloudflare-outage-causes-major-websites-across-internet-to-go-down-2019-7?international=true&r=US; 'Major websites and services across the internet went down Tuesday because of a hosting-platform outage', Businessinsider.nl, 2-7-2019, https://www.businessinsider.nl/cloudflare-outage-causes-major-websites-across-internet-to-go-down-2019-7?international=true&r=US; 'Amazon AWS Outage Shows Data in the Cloud is Not Always Safe', Bleepingcomputer.com, 5-92019, https://www.bleepingcomputer.com/news/technology/amazon-aws-outage-shows-data-in-the-cloud-is-not-always-safe/; 'AWS-diensten acht uur lang slecht bereikbaar door DDoS-aanval AG Connect', 24-10-2019, https://www.agconnect.nl/artikel/aws-diensten-acht-uur-lang-slecht-bereikbaar-door-ddos-aanval
90 'Grote storing in vast telefoonnetwerk Tele2', AGConnect, 12-5-2019, https://www.agconnect.nl/artikel/grote-storing-vast-telefoonnetwerk-tele2; 'Storing bij Tele2 door kabelbreuk treft overheidsinstanties - update 3', Tweakers.net, 25-11-2019, https://tweakers.net/nieuws/160342/storing-bij-tele2-door-kabelbreuk-treft-overheidsinstanties.html; 'Deskundige na ICT-storing bij Amphia: ziekenhuizen steeds kwetsbaarder', BN de stem 12 oktober 2019, https://www.bndestem.nl/breda/deskundige-na-ict-storing-bij-amphia-ziekenhuizen-steeds-kwetsbaarder~a8f9429c/; 'Grote storing bij Gelre ziekenhuizen, operaties afgezegd', Omroep Gelderland, 2 september 2019, https://www.omroepgelderland.nl/nieuws/2423232/Grote-computerstoring-bij-Gelre-ziekenhuizen-opgelost; '' Netwerkstoring verholpen', Tergooi.nl, 15-8-2019, https://www.tergooi.nl/netwerkstoring-storing-verholpen/; 'Storing aan computers in Meander verholpen AD.nl, 2-4-2019, https://www.ad.nl/amersfoort/storing-aan-computers-in-meander-verholpen~a1b4ba75/; 'Pinprobleem Albert Heijn veroorzaakt door storing firewall', AD.nl, 11-6-2019, https://www.ad.nl/amersfoort/storing-aan-computers-in-meander-verholpen~a1b4ba75/; 'Zwitsers bedrijf routeerde KPN- en ander Europees verkeer via China Telecom', Tweakers.net, 7-6-2019, https://tweakers.net/nieuws/153726/zwitsers-bedrijf-routeerde-kpn-en-ander-europees-verkeer-via-china-telecom.html.
91 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen', Onderzoeksraad voor Veiligheid, 13-2-2020, p. 57-63, https://www.onderzoeksraad.nl/nl/media/attachment/2020/2/13/patientveiligheid_bij_ict_uitval_in_ziekenhuizen.pdf.

92 Zie Jaarbeeld.
93 'Duizenden bedrijven met Citrix-systemen nog steeds kwetsbaar', Security.nl, 7-2-2020, https://www.security.nl/posting/642973/Duizenden+bedrijven+met+Citrix-systemen+nog+steeds+kwetsbaar.
94 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen', Onderzoeksraad voor Veiligheid, 13-2-2020, p. 64, https://www.onderzoeksraad.nl/nl/media/attachment/2020/2/13/patientveiligheid_bij_ict_uitval_in_ziekenhuizen.pdf.
95 'AIVD-baas Dick Schoof: spanning tussen privacy en mogelijkheden inlichtingendienst', WNL Op Zondag, 16-2-2020, https://wnl.tv/2020/02/16/aivd-baas-dick-schoof-spanning-tussen-privacy-en-mogelijkheden-inlichtingendienst/. Schoof is in de uitzending te horen vanaf ongeveer 40 minuten t/m 48 minuten.
96 'Agentschap Telecom: digitale veiligheid IoT-apparaten niet op orde', Security.nl, 25-9-2019, https://www.security.nl/posting/625469/Agentschap+Telecom%3A+digitale+veiligheid+IoT-apparaten+niet+op+orde.
97 'Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde', Algemene Rekenkamer, 15-5-2019, https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde; 'Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde', Algemene Rekenkamer, 15-5-2019, https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde.
98 'Resultaten online expertraadpleging CSBN 2020'.
99 'Resultaten online expertraadpleging CSBN 2020'.
100 'Voorbereiden op digitale ontwrichting', WRR, 2019, p. 9-14, 11https://www.wrr.nl/binaries/wrr/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting/R101-Voorbereiden-op-digitale-ontwrichting.pdf.
101 'Jaarverantwoording 2019 politie', Politie Nederland, 13-1-2020.
102 'Twee verdachten aangehouden in onderzoek naar gestolen wachtwoorden', Politie.nl, 17-01-2020, https://www.politie.nl/nieuws/2020/januari/17/02-twee-verdachten-aangehouden-in-cybercrimeonderzoek-naar-gestolen-wachtwoorden.html geraadpleegd op 29-1-2020.
103 'Jaarverantwoording 2019 politie', Politie Nederland, 13-1-2020.
104 'Minister JenV wijst vier computercrisisteams aan', 27-1-2020, https://www.ncsc.nl/actueel/nieuws/2020/januari/27/aanwijzing-certs.
105 'Convenant Nationaal Response Netwerk ondertekend', NCSC, 7-2-2020, https://www.ncsc.nl/actueel/nieuws/2020/februari/7/nrn.
106 'Cybersecurity is a matter for the top brass', Arno Visser, in CSR Magazine, Cybersecurity Raad, oktober 2019, p. 24.
107 'Cyberveiligheid in het onderwijs' [kamerbrief], Ministerie van Onderwijs, Cultuur en Wetenschap, 14-2-2020, https://www.tweedekamer.nl/downloads/document?id=4186214c-16fe-4891-842d-571b86e41a19&title=Reactie%20op%20het%20verzoek%20van%20het%20lid%20Wiersma%2C%20gedaan%20tijdens%20de%20Regeling%20van%20Werkzaamheden%20van%2014%20januari%202020%2C%20over%20een%20cyberaanval%20bij%20de%20Universiteit%20Maastricht.docx.
108 'VS en VK willen niet dat Facebook end-to-end-encryptie uitrolt', Security.nl, 4-10-2019, https://www.security.nl/posting/626523/VS+en+VK+willen+niet+dat+Facebook+end-to-end-encryptie+uitrolt; voor de brief zelf: https://www.justice.gov/opa/press-release/file/1207081/download.
109 'Voorbereiden op digitale ontwrichting', WRR, 2019, p. 48, 11https://www.wrr.nl/binaries/wrr/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting/R101-Voorbereiden-op-digitale-ontwrichting.pdf.
110 'Het Citrix-beveiligingslek: de laatste stand van zaken', Security.nl, 19-1-2020 (laatst bijgewerkt: 23-01-2020), https://www.security.nl/posting/639997/Het+Citrix-beveiligingslek%3A+de+laatste+stand+van+zaken, geraadpleegd op 27-1-2020; 'Positive Technologies: Citrix vulnerability allows criminals to hack networks of 80,000 companies', Positive Technologies, 23-12-2019, https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of-80000-companies/.
111 'The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture' Recorded Future, Moriuchi, Priscilla, 10-6-2019, https://www.recordedfuture.com/huawei-technology-risks/. Zie ook 'Huawei security threat derives from its sheer scale, says analysis; Cybersecurity report warns Chinese tech firm's breadth exposes customers to risk', The Guardian. 10-6-2019.
112 'Horizonscan Nationale Veiligheid 2019', Analistennetwerk Nationale Veiligheid, oktober 2019.
113 'Resultaten online expertraadpleging CSBN 2020'.
114 'Europa sluit Huawei niet uit – nog niet', NRC Next, 4-12-2019; 'Wees niet passief, doe als de Chinezen', NRC Handelsblad, 30-9-2019.
115 'Cybersecuritybeeld Nederland 2019', NCTV, 12-06-2019.
116 'The Inevitable. Understanding the 12 technological forces that shape our future', Kevin Kelly (2016).
117 Horizonscan Nationale Veiligheid 2019, Analistennetwerk Nationale Veiligheid, oktober 2019.
118 'Vulnerabilities in IoT Devices Have Doubled Since 2013', 17-09-2019, https://www.infosecurity-magazine.com/news/vulnerabilities-in-iot-devices/ geraadpleegd 06-04-2020.
119 Horizonscan Nationale Veiligheid 2019, Analistennetwerk Nationale Veiligheid, oktober 2019.

120 Horizonscan Nationale Veiligheid 2019, Analistennetwerk Nationale Veiligheid, oktober 2019.
121 Horizonscan Nationale Veiligheid 2019, Analistennetwerk Nationale Veiligheid, oktober 2019.
122 'How Today's Geopolitics Are Creating an Uncertain Future for Global Tech', Entrepreneur Europe, Yifat Oron, 16-10 2019, https://www.entrepreneur.com/article/340714 geraadpleegd 06-04-2020.
123 'Russia 'successfully tests' its unplugged internet', BBC News Online, 24-12 2019, https://www.bbc.com/news/technology-50902496 geraadpleegd 03-04-2020; China moves to ban foreign software and hardware from state offices', TechCrunch, Devin Coldewey, 09-12 2019, https://techcrunch.com/2019/12/09/china-moves-to-ban-foreign-software-and-hardware-from-state-offices geraadpleegd 03-04-2020.
124 Horizonscan Nationale Veiligheid 2019, Analistennetwerk Nationale Veiligheid, oktober 2019.
125 'Jaarverslag 2018', AIVD, april 2019, p. 9-10; 'MIVD Openbaar Jaarverslag 2018', MIVD, april 2019, p. 17.
126 'MIVD Openbaar Jaarverslag 2018', MIVD, april 2019, p. 16.
127 'Former Facebook security chief: hack and leak campaigns are the new normal', Federal Computer Week, 11-06 2019 https://fcw.com/articles/2019/06/11/stamos-campaign-hacks-new-normal.aspx geraadpleegd op 16-03 2020.
128 Zie voor algemene informatie over de dreiging van cybercriminelen bijvoorbeeld '2020 Global Threat Report', Crowdstrike, 2020 en M-trends 2020, FireEye Mandiant, 2020.
129 'Jaarverantwoording 2019 politie', Politie Nederland, 13-1-2020.
130 'Internet Organised Crime Threat Assessment' (IOCTA) 2019, Europol, 09-10-2019, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019; 'Targeted Ransomware: Proliferating Menace Threatens Organizations', Symantec, 18-07-2019, https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat.
131 Jaarbeeld.
132 Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT, FireEye blog 24-02 2020, geraadpleegd op 05-03 2020.
133 'U.S. government concludes cyber attack caused Ukraine power outage', Reuters, 26-02 2016, https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K geraadpleegd 19-03 2020; 'How an Entire Nation Became Russia's Test Lab for Cyberwar', Wired, 20-06 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/ geraadpleegd 19-03 2020; 'Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks', Jackson School of International Studies (JSIS), 11-10 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ geraadpleegd 19-03 2020.
134 https://nos.nl/artikel/2330187-waarom-worden-door-heel-nederland-zendmasten-in-brand-gestoken.html.
135 'Jaarverslag 2018', AIVD, april 2019; 'MIVD Openbaar Jaarverslag 2018', MIVD, april 2019.
136 'Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs', Volexity, 02-09-2019, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/, geraadpleegd op 12-03-2020; 'Missing Link', The Citizen Lab, 24-09-2019, https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/, geraadpleegd op 12-03-2020.
137 'Voorbereiden op digitale ontwrichting', Wetenschappelijke Raad voor het Regeringsbeleid, rapport nr. 101, september 2019, p. 45-46 https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.
138 'Onderzoek naar storing 112', Agentschap Telecom, 26-6-2019, https://www.agentschaptelecom.nl/actueel/nieuws/2019/06/26/onderzoek-naar-storing-112; 'Had de storing van 112 voorkomen kunnen worden?', Volkskrant.nl, 28-6-2019, https://www.volkskrant.nl/nieuws-achtergrond/had-de-storing-van-112-voorkomen-kunnen-worden~b235b093/; 'Ook dode in Den Haag tijdens 112-storing', RTL Nieuws, 3-7-2019, https://www.rtlnieuws.nl/nieuws/nederland/artikel/4767526/dode-den-haag-112-storing.
139 'VPN warning: REvil ransomware targets unpatched Pulse Secure VPN servers', ZDNet, 06-01-2020, https://www.zdnet.com/article/vpn-warning-revil-ransomware-targets-unpatched-pulse-secure-vpn-servers/ geraadpleegd op 17-02-2020; 'Continued Exploitation of Pulse Secure VPN Vulnerability', US-CERT, 10-01-2020, https://www.us-cert.gov/ncas/alerts/aa20-010a geraadpleegd op 17-02-2020; 'Continued Exploitation of Pulse Secure VPN Vulnerability', US-CERT, 10-01-2020, https://www.us-cert.gov/ncas/alerts/aa20-010a geraadpleegd op 17-02-2020.
140 CSBN2019.
141 'What are Data Manipulation Attacks, and How to Mitigate Against Them', Threatpost, 06-02 2019, https://threatpost.com/what-is-a-data-manipulation-attack-and-how-to-mitigate-against-them/141563/ geraadpleegd op 16-03 2020.

142 'Aanvallers wijzigen wereldwijd dns-instellingen domeinen', Security.nl, 11-01-2019, https://www.security.nl/posting/593796/Aanvallers+wijzigen+wereldwijd+dns-instellingen+domeinen; 'DNS Infrastructure Hijacking Campaign', US-CERT, 10-01-2019, https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign; 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', FireEye, 10-01-2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html. Alle bronnen geraadpleegd op 03-03 2020.

143 'Systemic cyber riskFebruary 2020', European System Risk Board, 19-2-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf; 'ESRB publishes report on systemic cyberattacks', ESRB, 19 February 2020, https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html, geraadpleegd op 25-02-2020.

144 Zie Jaarbeeld

145 Hoofdstuk Jaarbeeld; hoofdstuk Belang.

146 'AIVD Jaarverslag 2019', AIVD, april 2020; 'VOORUITZIEND VERMOGEN VOOR VREDE&VEILIGHEID. De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is. Openbaar jaarverslag 2019, april 2020.

147 'AIVD Jaarverslag 2019', AIVD, april 2020.

148 Moore, T., 'The economics of cybersecurity: Principles and policy options' in International Journal of Critical Infrastructure Protection(Volume 3), 2010, p. 103-117.

149 'Maatregelen bescherming telecomnetwerken en 5G' [Kamerstuk], Ministerie van Justitie en Veiligheid, 1-7-2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/07/01/kamerbrief-maatregelen-bescherming-telecomnetwerken-en-5g/Maatregelen+bescherming+telecomnetwerken+en+5G.pdf; 'Reactie op bericht Nederland kiest harde lijn tegen Huawei in 5Gnetwerk' [kamerstuk], Ministerie van Economische Zaken, 3-2-2020, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2020/02/03/kamerbrief-met-reactie-op-bericht-nederland-kiest-harde-lijn-tegen-huawei-in-5g-netwerk/kamerbrief-over-reactie-op-bericht-nederland-kiest-harde-lijn-tegen-huawei-in-5g-netwerk.pdf.

150 'Universiteit Maastricht werd besmet via phishingmail en verouderde software', Security.nl, 5-2-2020, https://www.security.nl/posting/642452/Universiteit+Maastricht+werd+besmet+via+phishingmail+en+verouderde+software.

151 Feedback van een externe partner op een conceptversie.

152 'Losgeld betalen aan cybercriminelen? Experts weten: soms is er amper keus', AD, 4-1-2020, https://www.ad.nl/tech/losgeld-betalen-aan-cybercriminelen-experts-weten-soms-is-er-amper-keus~a8451ffb/; 'Universiteit Maastricht betaalde ransomware-aanvallers losgeld' NOS.nl, 2-1-2020, https://nos.nl/artikel/2317078-universiteit-maastricht-betaalde-ransomware-aanvallers-losgeld.html; 'Universiteitsblad: Universiteit Maastricht betaalde tonnen losgeld aan hackers', Volkskrant, 2-1-2020, https://www.volkskrant.nl/nieuws-achtergrond/universiteitsblad-universiteit-maastricht-betaalde-tonnen-losgeld-aan-hackers~b70d0f6b/, 'Verzekeraars moeten stoppen met losgeld bij digitale afpersing', Het Financiële Dagblad', 27-12-2019; 'Microsoft: betalen van ransomware vaak enige optie voor bedrijven', Security.nl,17-12-2019, https://www.security.nl/posting/635699/Microsoft%3A+betalen+van+ransomware+vaak+enige+optie+voor+bedrijven; 'The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks', ProPublica, 27-08-2019, https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

153 'Cyberverzekeringen: goed voor erbij of noodzakelijk?', BNR Digitaal podcast, Herbert Blankesteijn & Wesley Schouwenaars, 8-1-2020, https://www.bnr.nl/podcast/digitaal/10399508/cyberverzekeringen-goed-voor-erbij-of-noodzakelijk.

154 'Ransomware is nu een businessmodel vancriminelen', NOS.nl, 6-2-2020, https://nos.nl/op3/artikel/2321876-ransomware-is-nu-een-businessmodel-van-criminelen.html.

155 'Losgeld betalen aan cybercriminelen? Experts weten: soms is er amper keus', AD, 4-1-2020, https://www.ad.nl/tech/losgeld-betalen-aan-cybercriminelen-experts-weten-soms-is-er-amper-keus~a8451ffb/; 'Universiteit Maastricht betaalde ransomware-aanvallers losgeld' NOS.nl, 2-1-2020, https://nos.nl/artikel/2317078-universiteit-maastricht-betaalde-ransomware-aanvallers-losgeld.html; 'Universiteitsblad: Universiteit Maastricht betaalde tonnen losgeld aan hackers', Volkskrant, 2-1-2020, https://www.volkskrant.nl/nieuws-achtergrond/universiteitsblad-universiteit-maastricht-betaalde-tonnen-losgeld-aan-hackers~b70d0f6b/, 'Verzekeraars moeten stoppen met losgeld bij digitale afpersing', Het Financiële Dagblad', 27-12-2019; 'Microsoft: betalen van ransomware vaak enige optie voor bedrijven', Security.nl,17-12-2019, https://www.security.nl/posting/635699/Microsoft%3A+betalen+van+ransomware+vaak+enige+optie+voor+bedrijven; 'The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks', ProPublica, 27-08-2019, https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

156 'Ransomware is nu een businessmodel vancriminelen', NOS.nl, 6-2-2020, https://nos.nl/op3/artikel/2321876-ransomware-is-nu-een-businessmodel-van-criminelen.html.

157 'Systemic cyber risk February 2020', European System Risk Board, 19-2-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf; 'Understanding Systemic Cyber Risk', World Economic Forum, 21-10-2016, https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk; Lincoln Kaffenberger and Emanuel Kopp, 'Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment', Carnegie Endowment For International Peace, SEPTEMBER 2019; Jonathan William Welburn and Aaron Strong, 'Systemic Cyber Risk and Aggregate Impacts', RAND Institute for Civil Justice, september 2019; 'Quantifying Systemic Cyber Risk. Report on the "Connectedness in Cyber Risk" Workshop', Global CRQ Network, 2018; 'ADDRESSING SYSTEMIC CYBERSECURITY RISK. APPLIED RESEARCH PROGRAM', The Henry M. Jackson School of International Studies, 22-5-2018, https://jsis.washington.edu/wordpress/wp-content/uploads/2019/02/JSIS_ARP_Report_1_Risk_2018_FINAL.pdf.

158 'Systemic cyber risk February 2020', European System Risk Board, 19-2-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

159 'Systemic cyber risk February 2020', European System Risk Board, 19-2-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf; Lincoln Kaffenberger and Emanuel Kopp, 'Cyber Risk Scenarios,the Financial System, and Systemic Risk Assessment', Carnegie Endowment For International Peace, SEPTEMBER 2019; Jonathan William Welburn and Aaron Strong, 'Systemic Cyber Risk and Aggregate Impacts', RAND Institute for Civil Justice, september 2019; 'Quantifying Systemic Cyber Risk. Report on the "Connectedness in Cyber Risk" Workshop', Global CRQ Network, 2018; 'Understanding Systemic Cyber Risk', World Economic Forum, 21-10-2016, https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk.

160 'Seven hackers have now made a million dollars each from bug bounties, says HackerOne', ZDNet, 25-2-2020, https://www.zdnet.com/article/seven-hackers-have-now-made-a-million-dollars-each-from-bug-bounties-says-hackerone.

161 'Systemic cyber riskFebruary 2020', European System Risk Board, 19-2-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf; 'ESRB publishes report on systemic cyberattacks', ESRB, 19 February 2020, https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html, geraaadpleegd op 25-2-2020.

162 'AIVD-baas Dick Schoof: spanning tussen privacy en mogelijkheden inlichtingendienst', WNL Op Zondag, 16-2-2020, https://wnl.tv/2020/02/16/aivd-baas-dick-schoof-spanning-tussen-privacy-en-mogelijkheden-inlichtingendienst/. Schoof is in de uitzending te horen vanaf ongeveer 40 minuten t/m 48 minuten.

163 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen', Onderzoeksraad voor Veiligheid, 13-2-2020, p. 57-63, https://www.onderzoeksraad.nl/nl/media/attachment/2020/2/13/patientveiligheid_bij_ict_uitval_in_ziekenhuizen.pdf.

164 'Cyberveiligheid in het onderwijs' [kamerbrief], Ministerie van Onderwijs, Cultuur en Wetenschap, 14-2-2020, https://www.tweedekamer.nl/downloads/document?id=4186214c-16fe-4891-842d-571b86e41a19&title=Reactie%20op%20het%20verzoek%20van%20het%20lid%20Wiersma%2C%20gedaan%20tijdens%20de%20Regeling%20van%20Werkzaamheden%20van%2014%20januari%202020%2C%20over%20een%20cyberaanval%20bij%20de%20Universiteit%20Maastricht.docx.

165 'Resultaten online expertraadpleging CSBN 2020'.

166 'Risicorapportage cyberveiligheid economie 2019', Centraal Planbureau, 17-10-2019, https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.

167 'Risicorapportage cyberveiligheid economie 2019', Centraal Planbureau, 17-10-2019, https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.

168 Moore, T., 'Economics of Cybersecurity Market failures', 21-1-2015, https://delftxdownloads.tudelft.nl/EconSec101x-EconomicsCybersecurity/Week%204/EconSec101x-4a-slides.pdf; Pasquinucci, A., 'Economics of ICT security', in Computer Fraud & Security, 2008, p. 4-6; Moore, T., 'The economics of cybersecurity: Principles and policy options' in International Journal of Critical Infrastructure Protection(Volume 3), 2010, p.103-117; Jalali, M. S., Siegel, M. en Madnick, S., 'Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment' in The Journal of Strategic Information Systems, 28(1), 2019, p. 66-82.

169 Voor dat laatste: 'X-Force Threat Intelligence Index 2020', IBM, 2-2020.

170 '2019 Data Breach Investigations Report', Verizon, 8-5-2019

171 'Google: Security Keys Neutralized Employee Phishing', Brian Krebs, 23-7-2018, https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/ geraadpleeg op 12-3-2020

172 '2020 Cyber Security Report', CheckPoint, 18-1-2020.

173 '2019 Data Breach Investigations Report', Verizon, 8-5-2019

174 'X-Force Threat Intelligence Index 2020', IBM, 2-2020.

175 'X-Force Threat Intelligence Index 2020', IBM, 2-2020.

176 'M-trends 2020', FireEye, 20-2-2020

177 ‘2020 Global Threat Report’, Crowdstrike, 4 -3-2020
178 Jaarbeeld.
179 ‘Reactie Universiteit Maastricht op rapport FOX-IT’, Maastricht University, 5-2-2020; ‘UM Cyber Attack Symposium – Lessons learnt’, Maastricht Universiteit, 05-02-2020, https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt, geraadpleegd op 11-03-2020; 'Servers Universiteit Maastricht misten belangrijke update uit 2017', Security.nl, 06-02-2020, https://www.security.nl/posting/642659/Servers+Universiteit+Maastricht+misten+belangrijke+update+uit+2017, geraadpleegd op 11-03-2020.
180 ‘Resultaten online expertraadpleging CSBN 2020’.
181 ‘Resultaten online expertraadpleging CSBN 2020’.
182 Jaarbeeld.
183 ‘X-Force Threat Intelligence Index 2020’, IBM, 2-2020; ‘M-trends 2020’, FireEye, 20-2-2020
184 'Beleidsreactie CSBN2019 en voortgangsrapportage NCSA', [Kamerbrief] Ministerie van Justitie en Veiligheid, 12-6-2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/06/12/tk-beleidsreactie-csbn2019-en-voortgangsrapportage-ncsa/tk-beleidsreactie-csbn2019-en-voortgangsrapportage-ncsa.pdf.
185 ‘Digitale dijkverzwaring: cybersecurity en vitale waterwerken’, Algemene Rekenkamer, 28-03-2019
186 ‘Digitalisering aan de grens: Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol’, Algemene Rekenkamer, 20-04-2020
187 ‘Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde’, Algemene Rekenkamer, 15-5-2019, https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde.
188 ‘Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde’, Algemene Rekenkamer, 15-5-2019, https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde.
189 'Staat van de rijksverantwoording 2019. Breekt nood wet?', Algemene Rekenkamer, 20-5-2020, https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2020/05/20/staat-van-de-rijksverantwoording-2019/SRV-wr.pdf.
190 'Staat van de rijksverantwoording 2019. Breekt nood wet?', Algemene Rekenkamer, 20-5-2020, https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2020/05/20/staat-van-de-rijksverantwoording-2019/SRV-wr.pdf.
191 Nationaal Crisisplan Digitaal', NCTV, 21-2-2020, https://www.nctv.nl/actueel/nieuws/2020/02/21/nationaal-crisisplan-digitaal-schade-beperken-en-snel-herstel.
192 'Initial Access', MITRE ATT&CK, 17-10-2018 (updated 19-7-2019), https://attack.mitre.org/tactics/TA0001, geraadpleegd op 12-3-2020.
193 'Factsheet Indicators of Compromise, NCSC, 8-12-2016, https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-indicators-of-compromise.
194 'Factsheets informatiedeling binnen de keten', Digital Trust Center, https://www.digitaltrustcenter.nl/factsheets-informatiedeling-binnen-de-keten, geraadpleegd op 12-3-2020.
195 Zie Jaarbeeld.
196 'Double Dragon APT41, a dual espionage andcyber crime operation', FireEye, 4-9-2019, https://content.fireeye.com/apt-41/rpt-apt41.
197 ‘Overzicht vitale processen', NCTV, https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen; ‘Vitale infrastructuur’, NCTV, https://www.nctv.nl/onderwerpen/vitale-infrastructuur.

Uitgave
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
csbn@nctv.minjenv.nl
@nctv_nl

Juni 2020