Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland

CSBN 2021

Cybersecuritybeeld Nederland

CSBN 2021

Colofon

Het Cybersecuritybeeld Nederland 2021 (CSBN 2021) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en tot slot risico's. De focus ligt daarbij op de nationale veiligheid. Het CSBN is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC). Het wordt jaarlijks door de NCTV vastgesteld.

De NCTV draagt samen met zijn partners uit het veiligheidsdomein bij aan een veilig en stabiel Nederland door dreigingen te onderkennen en de weerbaarheid en bescherming van nationale veiligheidsbelangen te versterken. De NCTV is binnen de Rijksoverheid verantwoordelijk voor terrorismebestrijding, cybersecurity, nationale veiligheid, crisisbeheersing en statelijke dreigingen. Doel is het voorkomen en beperken van maatschappelijke ontwrichting.

Het 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.

Inhoud

Digitale veiligheid onlosmakelijk verbonden met nationale veiligheid

Kern-CSBN: Cyberaanvallen tasten zenuwstelsel maatschappij aan

Digitale processen vormen het 'zenuwstelsel' van de maatschappij, omdat ze onmisbaar zijn voor het ongestoord functioneren daarvan. Cyberaanvallen tasten dit zenuwstelsel aan en kunnen uiteindelijk leiden tot verlamming, zoals ook gesteld in het CSBN 2020. COVID-19 heeft de digitalisering van processen in een stroomversnelling gebracht, onder meer in de gezondheidszorg en het onderwijs. De digitale en de fysieke wereld zijn sterker verweven geraakt en steeds minder goed van elkaar te onderscheiden. Er zijn amper nog processen zonder digitale component.

Vanwege de verwevenheid tussen de digitale en fysieke wereld is bestuurlijke aandacht voor het belang van digitale veiligheid, de digitale dreiging en de weerbaarheid vanuit alleen een technische invalshoek te beperkt. Het gaat ook, en wellicht vooral, om de wijze waarop organisaties en mensen digitalisering gebruiken en daarmee om de functionaliteit voor de samenleving en economie. Een cyberincident raakt digitale processen en wanneer die niet naar behoren werken, heeft dat effect op het functioneren van organisaties. Keteneffecten kunnen hele sectoren of zelfs de gehele maatschappij raken. Zo maakt een aanval met ransomware op een gemeente, universiteit, ziekenhuis of elektriciteitsdistributeur systemen onbruikbaar: de techniek werkt niet meer. Het gevolg daarvan is dat de gemeente haar taken niet meer naar behoren kan uitvoeren, dat onderzoek en onderwijs stil komen te liggen, patiëntenzorg wordt belemmerd of stroomuitval plaatsvindt. Dat betekent dat de digitale dreiging meer en andere belangen raakt dan het functioneren van de techniek alleen. Dat betekent dat weerbaarheidsverhogende maatregelen niet alleen bijdragen aan het veilig houden van techniek, maar ook aan het veilig houden van onze samenleving en economie.

Digitale veiligheid blijft onlosmakelijk verbonden met de nationale veiligheid: een aantasting ervan kan leiden tot maatschappelijke ontwrichting. De digitale dreiging blijft zich ontwikkelen doordat actoren zich blijven ontwikkelen, de geopolitieke context aan verandering onderhevig is en actuele gebeurtenissen als COVID-19 daarop van invloed zijn. Ook de weerbaarheid blijft in ontwikkeling. Het is een vraagstuk van governance en/of risicomanagement of de belangen, de digitale dreiging en de weerbaarheid voldoende in balans zijn.

De NCTV signaleert in dit CSBN vier risico's voor de nationale veiligheid:

1. Ongeautoriseerde inzage in informatie (en eventueel publicatie daarvan), in het bijzonder door spionage. Denk aan spionage van communicatie binnen de Rijksoverheid of de ontwikkeling van innovatieve technologieën.
2. Ontoegankelijkheid van processen, als gevolg van (voorbereidingen voor) sabotage en de inzet van ransomware. Denk aan de innesteling in processen die zorgdragen voor de distributie van elektriciteit.
3. Schending van de (veiligheid van de) digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leveranciersketens.
4. Grootschalige uitval: een situatie waarin één of meer processen zijn verstoord als gevolg van natuurlijke of technische oorzaken of als gevolg van niet-moedwillig menselijk handelen.

In het CSBN 2020 is reeds uitgebreid stil gestaan bij spionage, sabotage en uitval.[1] De risico's die hiermee zijn verbonden (risico's 1, 2 en 4), zijn nog steeds actueel. Spionage en sabotage zijn tevens uitgebreid toegelicht in de publicatie 'Dreigingsbeeld statelijke actoren'.[2] In dit CSBN wordt uitgebreid ingegaan op de risico's 2 (specifiek ransomware, hoofdstuk 4) en 3 (schending van de digitale ruimte, hoofdstuk 5).

Terugblik: Nederland geraakt door breed scala aan cyberincidenten

In de periode maart 2020 t/m maart 2021 vonden talloze cyberincidenten plaats in of in relatie tot Nederland. Daarbij grepen kwaadwillenden vooral COVID-19 aan als actueel thema om aanvallen uit te voeren. Daarnaast zijn voorzieningen om op afstand te werken doelwit geweest van aanvallen. Ook zijn processen met een digitale component ontoegankelijk gemaakt en zijn organisaties in leveranciersketens aangevallen. Er zijn veel incidenten geweest waarbij grote hoeveelheden kwetsbare bedrijfs- en privacygevoelige informatie openbaar zijn geworden. Tot slot hebben niet-moedwillig veroorzaakte storingen geleid tot uitval.

Hoofdstuk 2 (Terugblik) licht de verschillende incidenten toe.

Dreiging blijft zich ontwikkelen

COVID-19 thema misbruikt voor uitvoeren aanvallen

COVID-19 heeft ook in Nederland geleid tot maatschappelijke ontwrichting, waarbij juist de gedigitaliseerde samenleving veerkracht en continuïteit mogelijk maakte. De maatschappij is als gevolg van de pandemie verder gedigitaliseerd. Commerciële, educatieve en sociale activiteiten die volledig stil dreigden te vallen, kunnen dankzij ICT toch (deels) doorgaan. Dat betekent dat we een zwaar beroep doen op de digitale ruimte en dat die nog belangrijker is geworden voor het functioneren van de maatschappij.

De pandemie heeft ook geleid tot verschuivingen in het dreigingsbeeld. Actoren grijpen actuele thema's waar wereldwijd veel aandacht voor is, aan om digitale aanvallen uit te voeren. Dat is ook met COVID-19 het geval. Zo hadden veel phishing-mails van cybercriminelen en statelijke actoren het afgelopen jaar COVID-19 als thema. Ook creëren actuele gebeurtenissen een inlichtingenbehoefte bij statelijke actoren. In relatie tot COVID-19 ontstond er een kennisbehoefte met betrekking tot vaccins, die digitale spionage en zelfs het verspreiden van desinformatie tot gevolg heeft gehad.[3] Desinformatie rond actuele thema's zoals de pandemie kan leiden tot polarisatie doordat desinformatie verschillen van inzicht aanwakkert en uitvergroot. Denk aan het wel of niet vertrouwen hebben in vaccins tegen COVID-19. Het is voorstelbaar dat polarisatie ook een digitale component krijgt. Zo kunnen tegenstanders van de COVID-19 maatregelen hun ongenoegen uiten door digitale processen te verstoren, bijvoorbeeld door het uitvoeren van DDoS-aanvallen tegen overheidsinstanties of partijen met andere ideeën. Ook kunnen ze proberen instanties te hacken om zo aan informatie die komen die een instantie in een kwaad daglicht kan stellen.

De pandemie heeft in Nederland ook geleid tot toegenomen aandacht voor risico's en het (versneld) treffen van weerbaarheidsverhogende maatregelen door bedrijven en organisaties, bijvoorbeeld in het onderwijs.[4] In hoeverre initiatieven ter vergroting van de weerbaarheid nu en in de nabije toekomst voldoende opwegen tegen de verder ontwikkelde dreiging is lastig te beoordelen, maar de balans lijkt vooralsnog niet positief uit te pakken (zie hieronder bij Weerbaarheid).

Hoofdstuk 2 (Terugblik) beschrijft een aantal cyberincidenten die zich rond COVID-19 hebben voorgedaan in en in relatie tot Nederland. Hoofdstuk 3 licht toe hoe de pandemie als belangrijkste actuele thema het dreigingsbeeld beïnvloed heeft.

Aanvallen kunnen organisaties en ketens langdurig schaden

De impact van digitale aanvallen varieert. Sommige leiden tot een kortdurende verstoring van processen, zoals een DDoS-aanval die een website een paar uur platlegt. Er zijn ook aanvallen die een langdurige impact hebben, zoals ransomware-aanvallen. Cybercriminelen nemen de tijd om netwerken van slachtoffers binnen te komen, uit te zoeken op welke wijze ze maximale ontwrichting van processen kunnen bereiken en wat een 'geschikt' (want reëel) bedrag aan te eisen losgeld is.[5] Ze brengen vaak langere tijd ongezien in een netwerk door. Door ook back-ups van systemen onbruikbaar te maken, vergroten ze de impact van de aanval verder. In het uiterste geval is de schade aan systemen zo ernstig, dat herstel niet mogelijk is. Dan rest alleen nog het opnieuw opbouwen van systemen (of zelfs het opnieuw vergaren van verloren gegane data). Ransomware-aanvallen kunnen ook langdurig impact hebben op processen wanneer er sprake is van de inzet van verschillende drukmiddelen. Het gaat hier niet alleen om het ontoegankelijk maken van processen, maar ook om diefstal van informatie, waarna de actor deze openbaart of daarmee dreigt. Aanvallers kunnen nog een stap verder gaan en klanten van hun doelwit proberen af te persen. Dat kan snel plaatsvinden, of pas na verloop van tijd, waardoor slachtoffers van een ransomware-aanval mogelijk langdurig worden geconfronteerd met de gevolgen van de oorspronkelijke aanval.

Niet alleen aanvallen van cybercriminelen, maar ook die van statelijke actoren kunnen langdurig impact hebben op processen. Ze verschaffen zich bijvoorbeeld met behulp van een achterdeur toegang tot een netwerk en houden zich daar lange tijd ongezien in op. Daarbij verkennen ze de systemen en creëren ze nieuwe toegangen. De Russische statelijke actor achter de SolarWinds aanvalscampagne bleek bij ontdekking al meer dan een jaar ongemerkt in systemen aanwezig te zijn (zie hoofdstuk 2. Terugblik). Daarnaast is gebleken dat statelijke actoren ook cybersecuritybedrijven en individuele onderzoekers gericht

aanvallen.[6] Zo krijgen ze inzicht in de werkwijze van verdedigers en eventuele zwakke plekken in de beveiliging van klanten van deze bedrijven. Actoren kunnen deze kennis vervolgens inzetten om nieuwe aanvallen uit te voeren.

In hoofdstuk 4 wordt de cybercriminele dreiging nader geduid door de politie, waarbij de focus ligt op de inzet van ransomware als sluitstuk van een veelomvattend cybercrimineel proces. De geopolitieke motieven achter de activiteiten van statelijke actoren worden nader geduid in hoofdstuk 6.

Cybercriminelen kunnen nationale veiligheid aantasten

Cybercriminelen kunnen met hun aanvallen omvangrijke schade toebrengen aan digitale processen. Een aantal cybercriminele groepen beschikt inmiddels over capaciteiten die niet onder doen voor het niveau van statelijke actoren.[7] Dat impliceert dat de impact van hun aanvallen vergelijkbaar kan zijn met die van statelijke actoren. Ook al zijn cybercriminelen vooral gericht op geld verdienen en hebben ze niet de intentie om de maatschappij te ontwrichten, hun aanvallen kunnen zoveel (neven)schade veroorzaken dat nationale veiligheidsbelangen geraakt worden.[8] Dat kan bijvoorbeeld het geval zijn wanneer zij vitale processen ontoegankelijk maken door middel van ransomware.

Alhoewel gerichte aanvallen op de vitale processen nog niet in Nederland zijn waargenomen, komen deze in het buitenland reeds voor. In het CSBN 2020 werd melding gemaakt van ransomware-aanvallen op industriële controlesystemen (ICS) die worden gebruikt voor bijvoorbeeld de drinkwater- en energievoorziening.[9] Het afgelopen jaar zijn opnieuw wereldwijd vitale processen in de sectoren elektriciteit, water, olie & gas, chemie, voedsel, transport en de zorg doelwit geweest van digitale aanvallen door criminele groepen.[10] Uit verschillende rapporten blijkt dat de weerbaarheid in vitale processen in Nederland soms tekortschiet. De Cyber Security Raad (CSR) concludeerde dat ook bij organisaties die onderdeel zijn van vitale processen de basis ICT- en beveiligingshygiëne regelmatig niet op orde zijn, waardoor basale dreigingen tegen hun processen niet gepareerd of gedetecteerd kunnen worden.[11] Daarnaast blijkt uit een rapport van de Inspectie Leefomgeving en Transport dat Waternet, dat drinkwater levert in Amsterdam en omgeving, onvoldoende 'in control' is over haar cybersecurity. Hierdoor is er een verhoogd risico op een cyberincident met mogelijke gevolgen voor de kwaliteit en/of de continuïteit van drinkwater.[12] Tot slot blijkt uit onderzoek naar aanleiding van een hack bij een watervoorzieningsbedrijf in de Verenigde Staten, dat veel ICS in Nederland eenvoudig toegankelijk zijn. De onderzoekers troffen via relatief eenvoudige Google-zoekopdrachten veel systemen aan in de vitale infrastructuur die niet of nauwelijks waren beveiligd.[13]

Naast het feit dat cybercriminelen zich (ook) richten op vitale processen, zijn de relaties die zij onderhouden met statelijke actoren een bron van zorg. Zo laten cybercriminele groepen zich in het land waarin ze verblijven inhuren door de staat om digitale aanvallen te plegen (hackers-for-hire).[14] Een variant hierop is dat cybercriminele groepen door staten gedoogd worden en onder druk worden gezet om in opdracht aanvallen uit te voeren. Soms wordt daarbij een beroep gedaan op hun 'patriottisme'.[15] Tot slot zijn er voorbeelden bekend van criminele hackers die (ook) werken voor overheidsdiensten die een publieke taak hebben in de bestrijding van cybercriminaliteit.[16]

Vanwege de mogelijke impact op de nationale veiligheid wordt in dit CSBN meer dan voorheen aandacht besteed aan cybercriminelen. Anno 2021 is er sprake van een volwassen cybercrimineel ecosysteem. Hierin worden actoren ondersteund door facilitatoren die technische, financiële en juridische dienstverlening aanbieden voor cyberaanvallen. Professionele en klantvriendelijke dienstverleners brengen ook nieuwe actoren op het toneel: criminelen uit de 'traditionele' misdaad (zoals drugs) gaan zich ook bezighouden met cyberaanvallen, zoals door middel van phishing.[17] Cyberaanvallen voor allerlei vormen van criminaliteit kunnen er in de toekomst toe leiden dat cybercriminaliteit ook een fysieke component krijgt, zoals het dreigen met of uitoefenen van geweld na phishing of ransomware of ontoegankelijke processen met fysieke gevolgen.

Hoofdstuk 4 licht de cybercriminele dreiging nader toe, waarbij de focus ligt op de inzet van ransomware.

Aanvallen schenden veiligheid digitale ruimte

Al onze digitale processen zijn sterk verweven met en afhankelijk van de mondiale digitale ruimte. Digitale processen van bijvoorbeeld aanbieders van vitale infrastructuur, maar ook die van grote en kleine organisaties en burgers, maken gebruik van de diensten en producten van wereldwijd opererende bedrijven. Voorbeelden daarvan zijn producten voor het werken op afstand, het beheer en verzenden van e-mails en de opslag en verwerking van informatie bij een cloudleverancier. Digitale processen zijn ook verweven met en maken gebruik van de technische infrastructuur van het internet, waaronder onderzeese kabels. Die verwevenheid heeft veel goeds gebracht en biedt nog steeds kansen, maar vormt tegelijkertijd een risico. Wat als statelijke actoren op grote schaal onderzeese kabels aftappen voor inlichtingenvergaring of de protocollen van het internet manipuleren in de gespannen geopolitieke context van nu? Wat als statelijke actoren– ten tijde van conflicten – die kabels saboteren? Wat als kwaadwillenden digitale processen of producten van mondiaal opererende bedrijven manipuleren of saboteren? Wat als een van de drie grootste mondiale cloudleveranciers door een storing korte of lange tijd niet meer beschikbaar is?

Dergelijke vormen van misbruik of uitval die de (veiligheid van de) digitale ruimte schenden, hebben grote gevolgen voor het functioneren van alle digitale processen. Gevoelige of kwetsbare persoonlijke, economische of politieke informatie is zo inzichtelijk voor kwaadwillenden. Dit kan de economie van Nederland raken of Nederland op achterstand zetten bij internationale onderhandelingen. Taken van organisaties kunnen niet meer worden uitgevoerd, zoals het distribueren van energie, het

uitvoeren van financiële transacties of het verzorgen van onderwijs. Naast die directe impact heeft schending van de digitale ruimte ook een bredere impact. Denk aan de kosten voor onderzoek en herstel van systemen, het eventueel opnieuw opbouwen van infrastructuur en de noodzaak om tijdelijk terug te vallen op analoge alternatieven. Schending van de digitale ruimte kan ook het vertrouwen van burgers en organisaties in processen aantasten. Daar komt bij dat verhoging van de weerbaarheid tegen uitval en misbruik van de digitale ruimte voor individuele staten en organisaties beperkt mogelijk is. Zo is er vaak geen zicht op de mate van weerbaarheid van verschillende onderdelen van ICT-leveranciersketens. Daardoor kunnen aanvullende risico's ontstaan die niet goed in beeld zijn, bijvoorbeeld bij de inkoop en aanbesteding van producten en diensten van een leverancier waarbij sprake is van een kwetsbaarheid in een product, of waarbij een (ingehuurde) medewerker toegang heeft tot digitale processen met gevoelige informatie. Schending van de veiligheid van de digitale ruimte is geen theoretische mogelijkheid, maar vindt daadwerkelijk plaats. Zo zijn er opnieuw geavanceerde aanvallen in ICT-leveranciersketens met een mondiale impact aan het licht gekomen en zijn aanwezige kwetsbaarheden in mondiaal gebruikte producten misbruikt.

Hoofdstuk 5 gaat nader in op het risico van schending van de digitale ruimte.

Weerbaarheid nog niet voldoende

Het NCSC signaleert positieve ontwikkelingen in de verhoging van de weerbaarheid van Nederland: een toename van het gebruik van multi-factor authenticatie, het uitfaseren van een aantal onveilige technologieën, een verbetering van detectie en respons en tot slot een breed scala aan concrete initiatieven om de weerbaarheid van organisaties te verbeteren.[18] Ondanks deze positieve ontwikkelingen blijkt uit de cyberincidenten die Nederland hebben geraakt dat de weerbaarheid nog niet voldoende is (zie hoofdstuk 2. Terugblik). De Algemene Rekenkamer stelde in mei 2021 dat de stand van informatiebeveiliging rijksbreed over de hele linie gezien in 2020 niet is veranderd.[19] Vrijwel alle organisaties die de informatiebeveiliging in 2019 niet op orde hadden, hebben hier in 2020 werk van gemaakt. Dit heeft echter nog niet geleid tot voldoende beheersing van de risico's, waardoor de onvolkomenheden nog niet zijn opgelost. De CSR constateerde dat in Nederland de komende jaren additionele inzet en investeringen nodig zijn om de weerbaarheid te versterken.[20]

Basismaatregelen niet of onvoldoende getroffen

Dat er sprake is van het niet of niet voldoende nemen van basismaatregelen tegen de digitale dreiging, zoals het gebruik van sterke wachtwoorden en het tijdig patchen van kwetsbaarheden, was reeds een kernboodschap van de CSBN's van de afgelopen jaren. Uit de incidenten die behandeld worden in de Terugblik blijkt dat basismaatregelen nog te vaak niet of onvoldoende getroffen worden. Actoren maken snel misbruik van ernstige kwetsbaarheden in hard- en software en doen dat gedurende lange tijd.[21] Zij zijn aanhoudend succesvol in het misbruiken van publiekelijk bekende kwetsbaarheden bij digitale aanvallen op wereldwijde schaal. De AIVD en MIVD signaleren dat statelijke actoren volharden in het misbruik van publiekelijk bekende kwetsbaarheden bij de uitvoer van digitale aanvallen.[22] Een voorbeeld is de ernstige kwetsbaarheid in Citrix-servers, die in december 2019 bekend werd en die onder andere door statelijke actoren misbruikt is.[23] Het NCSC concludeerde destijds dat ook veel Nederlandse Citrix-servers kwetsbaar waren voor aanvallen.[24] In juni 2020, zes maanden na de bekendmaking van de kwetsbaarheid, bleek uit een onderzoek van Fox-IT dat er nog 39 gecompromitteerde Citrix-servers in Nederland waren.[25] Een deel daarvan was door de organisatie in kwestie niet tijdig gepatcht, waardoor aanvallers al een achterdeur hadden kunnen installeren en digitale processen ontoegankelijk hadden kunnen maken of ongeautoriseerde inzage hadden kunnen krijgen in informatie. Ook bij de kwetsbaarheden in Microsoft Exchange die begin maart 2021 publiek bekend werden, bleek dat organisaties kwetsbare servers niet tijdig patchen. Het NCSC waarschuwde dat door misbruik van de kwetsbaarheden data wordt gestolen, criminelen malware en achterdeuren plaatsen en e-mails verkopen.[26] Hiermee kunnen nieuwe aanvallen worden uitgevoerd of in de nabije toekomst digitale processen worden geraakt, bijvoorbeeld door middel van identiteitsfraude op basis van buitgemaakte persoonlijke gegevens.

Verschillende incidenten zijn illustratief voor voor de structurele kloof tussen bekendwording van kritieke kwetsbaarheden en het (later) uitvoeren van beveiligingsupdates. Nederlandse bedrijven, organisaties en ministeries lopen hierdoor een verhoogd risico op digitale spionage door statelijke actoren.[27]

In het NCSC-product 'Handreiking Cybersecuritymaatregelen' zijn de belangrijkste basismaatregelen op een rij gezet.[28]

Grote verschillen op het gebied van weerbaarheid

Cybersecurity experts signaleren grote verschillen in weerbaarheid in Nederland.[28] Grote bedrijven kunnen investeren in kennis en kunde op het gebied van cybersecurity.[30] Aanbieders van essentiële diensten en digitale dienstverleners hebben daarnaast een wettelijke zorgplicht, vastgelegd in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Kleine bedrijven daarentegen, bijvoorbeeld in het Midden- en Kleinbedrijf (MKB), beschikken veelal niet over de expertise en de middelen om de weerbaarheid naar een hoger plan te tillen. Toch kan ook het MKB kan doelwit zijn van geavanceerde actoren. Zo stelde de MIVD dat de EXIM-kwetsbaarheid waar de Amerikaanse inlichtingendienst NSA voor waarschuwde ook in Nederland door een statelijke actor misbruikt is voor het compromitteren van slachtoffers in het MKB.[31] Daarnaast kunnen kwetsbare MKB deel uitmaken van de leveranciersketen van vitale processen. Tegelijkertijd neemt de afhankelijkheid van ICT-dienstverleners in het MKB toe, terwijl zij

de basisbeveiliging niet altijd voldoende op orde hebben en vaak niet duidelijk is wie verantwoordelijk is voor bijvoorbeeld updates of back-ups. Daardoor zijn digitale processen kwetsbaar voor allerlei vormen van misbruik. Experts vrezen dat de verschillen in het niveau van weerbaarheid de komende jaren verder zullen toenemen.[32] Om de verschillen te verkleinen zijn er verschillende initiatieven om publieke en private partijen van informatie te voorzien en om samen te werken aan de verhoging van de weerbaarheid. Hierbij is het NCSC het nationale informatieknooppunt binnen het Landelijk Dekkend Stelsel.[33]

Risicomanagement instrument in verhogen weerbaarheid

Securityspecialisten, toezichthouders en wetenschappers benadrukken het belang van risicomanagement als instrument om beter inzicht te krijgen in de weerbaarheid.[34] De risicoafweging bepaalt welke maatregelen nodig zijn om risico's voldoende te beheersen. Om risico's minder abstract te maken kunnen ze worden doorvertaald naar scenario's. Een risicogebaseerde benadering helpt bij het maken van keuzes welke digitale processen, en als afgeleide daarvan welke systemen, belangrijk zijn voor een organisatie en waar verstoring niet geaccepteerd is. Het maken van belangenafwegingen impliceert dat risicomanagement ook op de agenda van de bestuurslaag thuishoort.

Hoofdstuk 7 licht het belang van risicomanagement als instrument voor verhoging van de weerbaarheid verder toe. Hoofdstuk 8 schetst scenario's met betrekking tot uitval en compromittering van processen die gebruik maken van cloudvoorzieningen.

Spanning tussen veiligheid, vrijheid en economische groei neemt toe

Veiligheid is in een gedigitaliseerde maatschappij geen op zichzelf staand belang. Het hangt nauw samen met waarden als vrijheid en economische groei. In bepaalde opzichten is veiligheid zelfs randvoorwaardelijk voor de andere belangen. Idealiter is er sprake van een zekere balans. Die balans staat onder druk, omdat de spanning tussen de verschillende waarden toeneemt. De digitale ruimte is anno 2021 onderwerp van (geo)politiek. Digitalisering speelt een steeds belangrijker rol in de verhouding tussen staten. Het is een terrein waarop staten zich ten opzichte van elkaar willen onderscheiden met als doel hun concurrentiepositie te verbeteren. Ook hanteren groepen van staten andere uitgangspunten. Zo streven bepaalde staten vooral naar regulering van informatiestromen naar en vanuit het land, terwijl andere juist streven naar openheid en interoperabiliteit. Die verschillen van inzichten werken door in discussies over normen en waarden in de digitale ruimte, maar ook in de formulering van (toekomstige) standaarden.

Digitalisering heeft naast alle voordelen ook nadelen, doordat digitale processen bijvoorbeeld bron of doelwit kunnen zijn van spionage en sabotage. Geopolitieke en technologische ontwikkelingen versterken elkaar en noodzaken de overheid om de nationale veiligheid en publieke waarden te blijven borgen. Staten en internationale verbanden zoals de EU ervaren ongemak bij de invloed van techbedrijven zoals Google en Facebook en willen minder afhankelijk zijn van grote spelers uit een beperkt aantal staten.[35] De hele samenleving draait op een digitale infrastructuur waar slechts een paar technologiebedrijven eigenaar en poortwachter van zijn.[36] Ook kan de overheid voor de uitvoering van beleid afhankelijk zijn van die digitale infrastructuur.[37] Hierdoor ontstaat behoefte aan digitale of strategische autonomie, in Europese context wordt ook wel over digitale soevereiniteit gesproken.[38] In een situatie waarin de spanning tussen verschillende waarden toeneemt en de digitale ruimte ook een domein is voor spionage of acties tegen andere staten, is vertrouwen in de digitale ruimte extra van belang.

Inzicht in digitale dreiging, belangen en weerbaarheid

1 Inleiding

Het Cybersecuritybeeld Nederland 2021 bouwt voort op de voorgaande CSBN's. Het kader aan het eind van deze inleiding vat de kernboodschappen van 2020 nog eens samen. In de editie van 2021 ligt de focus op het duiden van de verschuivingen in het beeld van de belangen, de dreiging en de weerbaarheid.

Doel en afbakening

Het Cybersecuritybeeld Nederland (CSBN) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en risico's. Het accent ligt daarbij op de nationale veiligheid.[1] Digitalisering biedt kansen, maar leent zich ook voor allerlei vormen van misbruik en is kwetsbaar voor uitval. Het CSBN richt zich niet op de kansen van digitalisering. Het richt zich wél op verstoringen van processen met een digitale component, waaronder vormen van cybercriminaliteit waarbij het proces en/of de onderliggende ICT het doelwit is. Andere vormen van misbruik van processen, bijvoorbeeld verspreiding van propaganda, verspreiding van kinderporno en allerhande vormen van fraude vallen buiten de scope. Deze afbakening betekent niet dat andere vormen van misbruik niet belangrijk zijn. In de verdiepende hoofdstukken (nieuw voor 2021) kunnen wel bredere onderwerpen aan bod komen, indien ze gevolgen kunnen hebben voor de digitale dreiging, de belangen en de weerbaarheid.

Het CSBN is primair bedoeld voor strategie- en beleidsvorming op nationaal niveau (governance). Het beoogt het kabinet, de leden van de Eerste en Tweede Kamer, ambtenaren, beleidsmakers, overige bestuurders en directies inzicht te geven in de risico's voor Nederland. Ook cybersecuritybedrijven en –professionals gebruiken het CSBN als referentiekader richting de eigen bestuurders of klanten. Het CSBN is ook bedoeld als hulpmiddel voor risicomanagement, waarbij het zich specifiek richt op de identificatie en beoordeling van risico's, een van de stappen in een risicomanagementproces. Tot slot is het CSBN ook toegankelijk voor het brede publiek. De rapportageperiode van dit CSBN is maart 2020 t/m maart 2021. Wel zijn incidenten van januari/februari 2020 en incidenten tussen april 2021 en de publicatiedatum van dit CSBN (juni 2021) meegenomen indien er sprake was van relevante impact.

Sleutelbegrippen

In het CSBN zijn de belangrijkste begrippen als volgt gedefinieerd[39]:
Aanval: moedwillige activiteit van een actor die is gericht op het met digitale middelen verstoren van één of meer digitale processen.
Belangen: 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 de focus op nationale veiligheidsbelangen.
Cyberincident: (samenhangende set van) gebeurtenissen of activiteiten die leiden tot verstoring van één of meer digitale processen. Verzamelbegrip voor cyberaanval en uitval.
Cybersecurity: het geheel aan maatregelen om (relevante) risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risico-afweging.

1 De nationale veiligheid is in het geding wanneer een of meerdere nationale veiligheidsbelangen zodanig bedreigd worden, dat er sprake is van (potentiële) maatschappelijke ontwrichting. Nederland onderscheidt zes nationale veiligheidsbelangen: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit en tot slot de internationale rechtsorde. Alle veiligheidsbelangen kunnen ook via de digitale ruimte geraakt worden. Maatschappelijke ontwrichting heeft een fysiek aspect (slachtoffers, schade of uitval van vitale functies) en een sociaal-psychologisch aspect (zoals verstoring van het dagelijks leven). Maatschappelijke ontwrichting dreigt ook wanneer de continuïteit of beschikbaarheid van vitale processen wordt geraakt. Deze processen vormen samen de Nederlandse vitale infrastructuur. Transport en distributie van elektriciteit, toegang tot internet en levering van drinkwater zijn voorbeelden van vitale processen. Bron: 'Nationale Veiligheid Strategie 2019', NCTV, juni 2019.

Digitaal proces (hierna: proces): een proces dat geheel of gedeeltelijk wordt uitgevoerd door de complexe en onderling samenhangende interactie tussen mensen en vele componenten van hardware, software en/of netwerken. Volledig geautomatiseerde processen, zoals procesbesturingssystemen, vallen ook onder het begrip.
Digitale ruimte: de complexe omgeving die het resultaat is van onderling verweven digitale processen, ondersteund door wereldwijd gedistribueerde fysieke informatie- en communicatietechnologie (ICT-)apparaten en verbonden netwerken. De digitale ruimte wordt vanuit drie invalshoeken benaderd: 1) digitale processen waaronder het gedrag van mensen, 2) de technische laag, 3) risicomanagement en/of governance.
Dreiging: een cyberincident dat zich kan voordoen of een combinatie van gelijktijdige of opeenvolgende cyberincidenten.
Risico: de kans dat een dreiging leidt tot een cyberincident en de impact van het cyberincident op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid.
Uitval: een situatie waarin één of meer digitale processen zijn verstoord als gevolg van natuurlijke of technische oorzaken of als gevolg van menselijke fouten.
Verstoring: een aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie(verwerking).
Weerbaarheid: het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid, is de uitkomst van een risico-afweging. 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.

Leeswijzer

Dit CSBN bestaat uit een kern en zeven verdiepende hoofdstukken. Het hoofdstuk vòòr deze Inleiding, het kern-CSBN, bevat de hoofdboodschappen. Een deel daarvan is verder uitgewerkt in een hoofdstuk. De indeling in een kern en verschillende thema's beoogt dat lezers uit verschillende doelgroepen makkelijk door het CSBN kunnen navigeren en zich kunnen richten op de onderwerpen die aansluiten bij hun professionele rol of interesse. De verdiepende hoofdstukken hebben de volgende thema's:

- Hoofdstuk 2, de Terugblik, geeft een overzicht van relevante incidenten in Nederland in de periode maart 2020 t/m maart 2021. Dit hoofdstuk is feitelijk van aard.
- Hoofdstuk 3 duidt hoe COVID-19 het dreigingsbeeld heeft beïnvloed.
- Hoofdstuk 4 gaat nader in op ransomware als risico voor de nationale veiligheid.
- Hoofdstuk 5 schetst hoe schendingen van de digitale ruimte een risico vormen.
- Hoofdstuk 6 beschrijft de invloed van geopolitiek op de belangen en de dreiging.
- Hoofdstuk 7 gaat in op risicomanagement als instrument in het verhogen van de weerbaarheid.
- Hoofdstuk 8 schetst een dreigingsscenario met een uitwerking van verschillende aspecten van de grootschalige toename van het gebruik van clouddienstverlening en de risico's die daarmee gepaard kunnen gaan. Dit hoofdstuk is technischer dan de andere themahoofdstukken en is vooral bedoeld om de lezer te helpen anticiperen op mogelijke incidenten.

Bijlage 1 bevat een verantwoording van de totstandkoming van het CSBN. Bijlage 2 bevat de bronnen en referenties.

Kernboodschappen CSBN 2020

De kernboodschappen van het CSBN 2020 zijn nog van toepassing. In onderstaand kader worden ze nog eens in herinnering gebracht.

Cyberincidenten kunnen maatschappij verlammen

- Digitale veiligheid is een randvoorwaarde voor het functioneren van de maatschappij.
- De digitale dreiging is permanent.
- De digitale weerbaarheid is nog niet overal op orde vanwege het ontbreken van basismaatregelen.
- Vergroting van de weerbaarheid is het belangrijkste instrument om digitale risico's te beheersen.
- Een compleet en scherp beeld van de weerbaarheid van vitale processen ontbreekt (nog).
- Digitale risico's zijn onverminderd groot en staan niet los van andere risico's.
- De afhankelijkheid van Nederland van landen met een offensief cyberprogramma vormt een risicoverhogende factor.
- Risico's voor de Nationale Veiligheid: sabotage en spionage door staten, uitval. Daarnaast zijn cyberaanvallen door criminelen relevant.

Bron: CSBN 2020, NCTV, juni 2020.

Talloze cyberincidenten met moedwillige en niet-moedwillige oorzaken

2 Terugblik

In de periode maart 2020 t/m maart 2021 hebben zich in of in relatie tot Nederland talloze cyberincidenten voorgedaan, met zowel een moedwillige als een niet-moedwillige oorzaak. Geen van deze incidenten heeft geleid tot maatschappelijke ontwrichting. De impact van incidenten liep sterk uiteen, van een kortstondige onderbreking van processen tot de noodzaak van het opnieuw opbouwen van onderdelen van de technische infrastructuur. Cyberincidenten hebben niet alleen impact op directe slachtoffers, maar ook op (ketens van) leveranciers, klanten en burgers die gebruik maken van de dienstverlening van (publieke) organisaties. Bij publieke organisaties is er geen sprake van een keuze voor die dienstverlening door burgers, maar van een afhankelijkheidsrelatie. Bij een aantal incidenten zijn de belangen van individuele en soms kwetsbare burgers geraakt, bijvoorbeeld wanneer persoonsgegevens zijn buitgemaakt. In een open bronnen inventarisatie van incidenten komen de volgende thema's terug: COVID-19 als gelegenheid voor kwaadwillenden, voorzieningen om op afstand te werken als doelwit van aanvallen, doelbewust ontoegankelijk gemaakte processen, organisaties in leverancierskетens aangevallen, datalekken en tot slot uitval van processen. Het hoofdstuk Terugblik is rond deze thema's opgebouwd en geeft concrete voorbeelden van incidenten die hebben plaatsgevonden.

1. COVID-19 gelegenheid voor kwaadwillenden

De wereldwijde COVID-19 pandemie kleurt de Terugblik sterk. De pandemie werd én wordt misbruikt door kwaadwillenden.[40] Zo hebben statelijke actoren digitale spionageactiviteiten ingezet in hun zoektocht naar informatie over medische kennis en beleidsmatige opvolging rond COVID-19.[41] Het gaat bijvoorbeeld om onderzoeksdata over behandeling, testresultaten en vaccins, informatie over de geschatte infectieverspreiding en mogelijke beleidsstrategieën. Criminelen misbruik(t)en de COVID-19-pandemie voor aanvallen door middel van phishing, ransomware en verspreiding van malafide apps. Zij verhogen de druk om losgeld te betalen door ransomware-aanvallen op processen van organisaties die cruciaal zijn in de bestrijding van COVID-19, waaronder patiëntenzorginstellingen, medische leveranciers en laboratoria. De Nederlandse zorgsector is bijvoorbeeld geadviseerd door Z-CERT[II] in nauwe samenwerking met het NCSC naar aanleiding van een ransomware-aanval op een medische toeleverancier. De behoefte in de maatschappij aan informatie over en financiële steun in het kader van COVID-19 is veelvuldig misbruikt in phishing-campagnes als opstap voor aanvallen. Het betrof vaak al bestaande malwarecampagnes waarbij het thema van e-mails, malafide bijlagen en links aan COVID-19 werden aangepast. In Nederland is bijvoorbeeld sms-phishing (smishing) waargenomen waarin kwaadwillenden zich voordeden als het RIVM.[42] Volgens Z-CERT is het effect van de phishing-campagnes in de Nederlandse zorgsector beperkt gebleven. Tot slot heeft de hack op het Europees Geneesmiddelenbureau in december 2020 aangetoond dat zowel medische kennis als informatie over beleidsopvolging misbruikt is in een desinformatiecampagne.

II Z-CERT is sinds januari 2020 aangewezen als computer emergency response team voor de gehele zorgsector (Wet beveiliging netwerk- en informatiediensten).

Documenten Europees Geneesmiddelenbureau gebruikt voor desinformatie

In december 2020 is het Europees Geneesmiddelenbureau (EMA) doelwit geworden van een hack&leak aanval. Het bureau werkte op dat moment aan de goedkeuring van twee COVID-19 vaccins. Eind december 2020 verschenen delen van EMA-documenten op webfora zoals het Russische darknet forum Rutor. De gelekte bestanden zijn deels gewijzigd en voorzien van commentaar en context waarbij het moet lijken alsof er sprake is van frauduleus onderzoek door het EMA. Ook is e-mailconversatie aangepast waarbij de indruk wordt gewekt dat EU-autoriteiten het EMA onder druk hebben willen zetten om vaccins versneld goed te keuren. Het lijkt er daarom op dat het verkrijgen van inlichtingen niet de enige intentie was van de actor, maar dat het oogmerk ook was om een desinformatiecampagne te voeden richting het publiek vertrouwen in vaccinontwikkelaars en Europese instellingen.[43] De aanval op het EMA is volgens open bronnen mogelijk gemaakt door een gebrek aan cyberhygiëne, waardoor de tweefactorauthenticatie omzeild kon worden. [44]

2. Voorzieningen voor werken op afstand doelwit

In Nederland deed het kabinet in verband met COVID-19 in maart 2020 een beroep op werkend Nederland om, waar mogelijk, vanuit huis te werken. De technische voorzieningen om op afstand te werken werden noodzakelijk voor de continuïteit van de bedrijfsvoering. Daarnaast steeg de potentie om kwetsbaarheden uit te buiten; het aanvalsoppervlak is sterk vergroot. Vanwege het vele thuiswerken zijn er meer kwetsbare systemen aan het internet gekoppeld en vinden digitale processen thuis plaats. Daarmee is zowel de kans op als de impact van een cyberincident met of via thuiswerkvoorzieningen toegenomen.

Voorzieningen om op afstand te werken kunnen worden ingedeeld in drie categorieën:

- Voorzieningen om online te vergaderen zoals Zoom, Teams, Jitsi, Google meet en Webex.
- Voorzieningen om de kantooromgeving of kantoorapplicaties op afstand te bedienen zoals Virtual Desktop Infrastructure (VDI), Remote Desktop Service (RDS) en TeamViewer.
- Systemen om op netwerkniveau verbinding met kantoor te maken: VPN-oplossingen.

In alle categorieën zijn in de rapportageperiode kwetsbaarheden en onveilig gebruik waargenomen. Zo wist een journalist in november 2020 toegang te krijgen tot een geheim Europees defensieoverleg.[45] In juni 2020 werd een kwetsbaarheid gevonden in Teamviewer waarmee kwaadwillenden verhoogde rechten en toegang konden krijgen tot bestanden op een systeem waardoor ze ongeautoriseerd inzage kunnen krijgen in informatie of processen ontoegankelijk kunnen maken.[46] Op VPN- en VPN-SSL-oplossingen wordt door kwaadwillenden voortdurend gescand naar kwetsbaarheden. Het NCSC heeft regelmatig gewaarschuwd voor verhoogde scanactiviteiten naar VPN-kwetsbaarheden in onder andere Pulse Connect Secure en Fortigate SSL door statelijke actoren.[47] Ook buitenlandse CERT's zoals het CISA hebben hier regelmatig voor gewaarschuwd.[48]

Niet alle incidenten rond thuiswerkvoorzieningen hebben een vergelijkbare impact. Dat is afhankelijk van het soort misbruik, de processen die het betreft en de actor. Misbruik van vergadervoorzieningen wordt meestal uitgevoerd door cybervandalen. Misbruik van onderliggende netwerkoplossingen wordt niet snel opgemerkt, is vaker persistent en kent een groter risico voor processen. Uitbuiting van bestaande kwetsbaarheden heeft meer impact door het vergrote aanvalsoppervlak. De Citrix kwetsbaarheid waarover uitgebreid is bericht in CSBN 2020 heeft, enkele maanden nadat de patch werd uitgebracht, nog nieuwe slachtoffers gemaakt. Ook zijn er in juni 2020 nieuwe kwetsbaarheden in Citrix-producten aan het licht gekomen die door het NCSC werden ingeschaald als high/high (hoge kans op misbruik en grote schade).[49]

Nederlandse organisaties half jaar na Citrix crisis nog steeds geïnfecteerd

De Volkskrant berichtte over actief misbruik van de Citrix-kwetsbaarheden bij Nederlandse bedrijven, ook nadat de lekken zijn gedicht. Volgens een analyse van Fox-IT zijn zeker 25 Nederlandse bedrijven geïnfecteerd via een lek in Citrix, waaronder een farmaceutisch bedrijf en een organisatie voor gehandicaptenzorg. Het gaat om een kwetsbaarheid in de Citrix NetScaler en ADC. Ook bedrijven die gepatcht hadden, bleken geïnfecteerd. In sommige gevallen ging het niet om één crimineel of groep die een achterdeur achterliet, maar om verschillende. Fox-IT zag servers met wel vier of vijf achterdeuren. Fox-IT ontdekte in juni 2020 dat er in Nederland nog 39 servers stonden die geïnfecteerd zijn. Dat betekent niet dat er ook 39 bedrijven zijn getroffen; sommige bedrijven gebruiken bijvoorbeeld meerdere servers.[50]

Statelijke actoren scannen actief naar kwetsbare VPN-systemen

Statelijke actoren zijn actief op zoek naar kwetsbare VPN-systemen in netwerken van zowel (semi-) publieke als private partijen. Kwetsbare systemen kunnen ook op een later moment nog ingezet worden om een grotere aanval op bijvoorbeeld de gehele keten uit te voeren. Het NCSC ontving van diverse sectoren berichten over waargenomen scanactiviteiten en dat sommige organisaties kwetsbaar waren, maar dat geen misbruik heeft plaatsgevonden. Ook buitenlandse CERT's hebben in de periode maart 2020 t/m maart 2021 verhoogde scanactiviteiten waargenomen naar VPN-kwetsbaarheden. Onder andere de volgende VPN-kwetsbaarheden zijn veelvuldig misbruikt om toegang te verkrijgen tot een systeem: Pulse Connect Secure (CVE-2019-11510), Fortigate SSL (CVE-2018-13379, CVE-2018-13382 en CVE-2018-13383) en Citrix ADC (CVE-2019-19781). Inmiddels bestaan voor deze VPN-kwetsbaarheden patches en zijn meerdere waarschuwingen en beheersmaatregelen gepubliceerd. Desondanks zijn er ook in Nederland nog organisaties die gebruik maken van kwetsbare VPN-oplossingen. Met name organisaties in het MKB hebben de kwetsbaarheden nog niet altijd verholpen.[51]

Er bestaat nog een vierde (officieuze) categorie van voorzieningen om op afstand te werken, namelijk die van de schaduw-ICT: oplossingen die niet behoren tot de goedgekeurde kantoorapplicaties, maar waar wel werkgerelateerd een beroep op wordt gedaan. Voorbeelden zijn berichtenapps, privé-email en privécloudapplicaties. Ook deze categorie heeft aan betekenis gewonnen, omdat er als gevolg van COVID-19 behoefte bestond aan 'workarounds' om snel informatie en stukken te kunnen delen. De Algemene Rekenkamer wees in november 2020 in een rapport over veilig thuiswerken op de ernstige beveiligingsrisico's die het gebruik van schaduw-ICT met zich mee kan brengen.[52]

3. Processen doelbewust ontoegankelijk gemaakt

Er zijn allerlei manieren om digitale processen doelbewust ontoegankelijk te maken. De twee belangrijkste zijn verstoring met een DDoS-aanval of de inzet van ransomware.

DDoS: grotere, zwaardere en langduriger aanvallen

In de rapportageperiode zijn digitale processen van Internet Service Providers (ISP's), de financiële sector, het onderwijs en publieke organisaties getroffen door DDoS-aanvallen. Opvallend was de trend richting zwaardere en complexere aanvallen waarin meerdere aanvalsvectoren werden gecombineerd. Uitzonderlijk zware DDoS-aanvallen werden in de maand augustus 2020 uitgevoerd met pieken tot 260 Gigabits per seconde.[53] De aanvallen richtten zich met name op de gedeelde infrastructuur bij ISP's. In een aantal gevallen ondervonden niet alleen afnemers verstoringen in hun online dienstverlening, maar ook de providers zelf. De Nationale Beheersorganisatie Internet Providers (NBIP) stelt in haar jaarlijkse DDoS data rapport dat DDoS-aanvallen in 2020 krachtiger en complexer zijn geworden, terwijl ook het aantal en de duur van DDoS-aanvallen toenam.[54] Aanvallers zouden bovengemiddeld vaardig zijn. Zij richten zich op de achterliggende infrastructuur en de aanvallers wisselen vaak van misbruikte protocollen, wat verdedigen lastig maakt. Desondanks geeft de Anti-DDoS-Coalitie aan door samenwerking de gevolgen van de genoemde DDoS-aanvallen in Nederland te hebben kunnen beperken.[55]

DDoS is van oudsher het middel van cybervandalen of personen die uit frustratie jegens de doelwitorganisatie aanvallen uitvoeren. Daarnaast bestaat het fenomeen RDDoS (Ransom Distributed Denial-of-Service): afpersing met een DDoS-aanval als drukmiddel. Wereldwijd werd gewaarschuwd voor DDoS-afpersingsmails die onder meer naar financiële instellingen in diverse staten werden gestuurd, waaronder in Nederland.[56]

Verschillende providers kampten met DDoS-aanvallen, geen grote verstoringen

In augustus 2020 hadden verschillende Nederlandse providers te maken met DDoS-aanvallen. Verschillende providers waren daardoor tijdelijk uit de lucht. In het geval van een Zeeuwse provider zorgde de aanval ervoor dat er in grote delen van Zeeland enige tijd geen internet, TV en telefonie beschikbaar was. Dit zorgde ook voor een regionale pinstoring.[57]

Ransomware leidt tot ontoegankelijke processen en onomkeerbare schade

In de rapportageperiode hebben actoren door middel van ransomware-aanvallen essentiële systemen gegijzeld. Digitale processen van onder andere publieke organisaties kwamen daardoor (groten)deels stil te liggen en er is onomkeerbare schade aan ICT-systemen ontstaan. De methodiek waarmee ransomware-aanvallen worden uitgevoerd, is sterk veranderd in de afgelopen jaren. Er is een ontwikkeling geweest naar 'Big Game Hunting', het compromitteren van zorgvuldig geselecteerde organisaties. Meestal betreft het kapitaalkrachtige organisaties, verantwoordelijk voor continuïteit van processen of in bezit van unieke data. De druk op het slachtoffer wordt sterk opgevoerd doordat ransomware op de meest strategische plek in het netwerk wordt ingezet. Daarnaast is ook het drukmiddel veranderd. Waar aanvankelijk data of systemen werden versleuteld, wordt nu ook data gestolen en gedreigd om deze publiek te maken. Om die reden zijn datalekken met regelmaat zichtbaar als belangrijke nevenschade bij ransomware-aanvallen. Ook zijn er voorbeelden van actoren die een ransomware-aanval vergezeld laten gaan van een dreigende DDoS-aanval als extra drukmiddel.[58] Volgens de FBI komt ook het telefonisch dreigen met fysiek huisbezoek bij een

ransomware-aanval voor.[59] De combinatie van deze strategieën levert een verhoogd risico op voor organisaties waar veel personen van afhankelijk zijn, waar unieke en hoogwaardige kennis wordt gegenereerd en waar verantwoordelijkheid wordt gedragen voor de verwerking van persoonsgegevens op grote schaal. Dit verklaart de selectie van doelwitten zoals kennisinstellingen (universiteiten en hogescholen), ziekenhuizen en farmaceutische bedrijven en publieke organisaties zoals gemeenten.

In februari 2021 zijn verschillende kennisinstellingen in Nederland aangevallen door criminele actoren. Onder andere Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), Universiteit van Amsterdam (UvA) en Hogeschool van Amsterdam (HvA) werden getroffen door digitale aanvallen, waarbij de aanval op de UvA en HvA succesvol is afgeslagen.[60]

Hoewel wereldwijd verschillende ransomware-activiteiten tegen publieke en private organisaties binnen de gezondheidszorg worden waargenomen, bestaan er geen concrete aanwijzingen die duiden op statelijke aansturing. De AIVD en MIVD schatten in dat deze sabotageactiviteiten zeer waarschijnlijk tot nu toe crimineel van aard zijn geweest.[61]

Gemeente Hof van Twente slachtoffer van ransomware-aanval

In december 2020 werd de gemeente Hof van Twente getroffen door een ransomware-aanval. De aanval had tot gevolg dat meerdere dienstverlenende processen geen doorgang konden vinden, ook was de gemeente niet bereikbaar via e-mail. De data die op servers was opgeslagen was ontoegankelijk, data in de cloud bleef beschikbaar. Volgens de gemeente hebben hackers geen data openbaar gemaakt en is er geen losgeld betaald. De gemeente zal echter de ICT-infrastructuur moeten heropbouwen, wat naar verwachting twee jaar zal duren.[62] Begin maart 2021 werd bekend dat een deel van de administratie toch hersteld kon worden.[63] Toen bleek ook dat het wachtwoord waarmee de ICT-omgeving was beveiligd bestond uit het eenvoudig te kraken 'welkom2020'.

4. Organisaties in leveranciersketens aangevallen

Een aanval op leveranciersketens richt zich niet op een specifieke organisatie, maar op een (of meerdere) zwakke plek(ken) in de keten. Via die zwakke plek(ken) kan de actor veel organisaties treffen. Omgekeerd heeft iedere organisatie te maken met leveranciersketens en daardoor metkwetsbaarheden voor aanvallen via die ketens. Dè leveranciersketenaanval bestaat niet, het is een verzamelterm waarbij verschillende typen ketens kunnen worden onderscheiden. Ook bestaan er aanvallen op leveranciers van halffabrikaten waardoor leveringen in de keten worden verstoord.

In het CSBN 2020 is ook ingegaan op aanvallen op leveranciersketens, toen nog vooral gezien als springplank of opstap naar interessante(re) doelwitten. Deze aanvallen zijn de afgelopen maanden toegenomen in aantal, omvang en complexiteit.[64] Ook hier speelt de versnelde digitalisering een rol. Om ketens efficiënt te laten functioneren, is het noodzakelijk om steeds meer informatie met ketenpartners te delen. Daarmee worden digitale risico's ook een risico van de keten, omdat kwaadwillenden doelbewust op zoek gaan naar de zwakste schakel. Wereldwijd is de leveranciersketenstrategie door verschillende actoren ingezet, onder andere richting bedrijven die zich bezighouden met vaccinontwikkeling of –transport.[65] Het meest prominente voorbeeld van een aanval op de ICT-leveranciersketen was echter de aangebrachte kwetsbaarheid in de Orion-software van SolarWinds.

SolarWinds: ICT-leveranciersketenaanval met wereldwijde impact

In december 2020 werd bekend dat aanvallers een kwetsbaarheid hadden aangebracht in een update van Orion-software van SolarWinds. Dit bedrijf maakt softwareprogramma's voor overheidsinstanties en grote bedrijven om ICT-omgevingen te monitoren en beheren. Volgens SolarWinds heeft de opzettelijk gecreëerde kwetsbaarheid als achterliggend doel de systemen van de afnemers van de betreffende versie van SolarWinds Orion te compromitteren. Bij verschillende Amerikaanse overheidsinstanties is de kwetsbaarheid ook daadwerkelijk misbruikt. Meerdere cybersecuritybedrijven en techbedrijven die wereldwijd klanten hebben, zoals FireEye, Mimecast en Microsoft, hebben aangegeven gecompromitteerd te zijn via de kwetsbare versie van Orion. Microsoft stelde dat het de aanvallers waarschijnlijk uiteindelijk te doen was om toegang tot clouddiensten van de organisaties die doelwit waren. Experts gaan uit van spionage als motief. Ook in Nederland is de kwetsbare versie van SolarWinds aangetroffen, onder andere binnen de overheid en de vitale processen.[66] Er is door het NCSC vooralsnog geen misbruik geconstateerd.[67] In april 2021 werd de SolarWinds campagne door de VS geattribueerd aan de Russische inlichtingendienst SVR (APT29).[68] Deze attributie werd ondersteund door de EU en de Nederlandse regering. [69]

5. Grote hoeveelheden bedrijfs- en privacygevoelige informatie op straat

Digitale processen zijn deels gericht op het verzamelen, selecteren, veredelen en distribueren van informatie. Vrijwel elke verstoring van een digitaal proces levert dan ook datalekken op. Daarbij is het belangrijkste onderscheid tussen datalekken die moedwillig ontstaan (door het werk van een kwaadwillende actor) en niet-moedwillige datalekken door bijvoorbeeld het achterlaten van een USB-stick. In totaal vinden in Nederland jaarlijks tienduizenden

(moedwillige en niet-moedwillige) datalekken plaats. Vorig jaar zijn er 23.976 datalekmeldingen gedaan bij de Autoriteit Persoonsgegevens.[70] Deze kunnen omvangrijk zijn: in maart 2021 bleek dat privégegevens van mogelijk miljoenen Nederlandse autobezitters gestolen waren en te koop staan op internet. Het gaat om naam- en adresgegevens, e-mailadressen, kentekens, telefoonnummers en geboortedata. De gegevens zijn buitgemaakt bij RDC, een ICT-dienstverlener voor autobedrijven.[71]

Publieke organisaties behoren tot de grootste dataverwerkende entiteiten en zijn dan ook sterk vertegenwoordigd in het overzicht van datalekken van de Autoriteit Persoonsgegevens. Onbedoelde datalekken ontstaan vaak door een gebrek aan kennis of bewustzijn. Hierbij de kanttekening dat groei van bewustzijn ook tot meer meldingen kan leiden, omdat datalekken daardoor eerder worden onderkend. Datalekken kunnen leiden tot een stille ontwrichting, omdat buitgemaakte gegevens in bezit kunnen komen van kwaadwillende derden en aan de basis liggen van digitale aanvallen. De impact van een datalek is niet altijd direct duidelijk. Soms wordt dit pas achteraf zichtbaar, bijvoorbeeld wanneer gelekte data misbruikt worden voor spionagedoeleinden. Datalekken kunnen de organisatie waar het lek plaatsvindt zelf raken, maar veelal zijn vooral anderen, waaronder klanten of burgers, het slachtoffer van misbruik van de informatie die op straat ligt.

Datadiefstal uit coronasysteem GGD

De GGD verwerkt wekelijks honderdduizenden coronatesten, waarbij persoonsgegevens zoals BSN-nummers, geboortedata en adresgegevens in verschillende systemen worden opgeslagen. In november 2020 werd bekend dat GGD-medewerkers ongeoorloofd dossiers van (zeker) twee bekende Nederlanders hebben ingezien. De GGD liet destijds weten dat dat iedereen die met de database(s) werkt een geheimhoudingsverklaring moet tekenen, om misbruik tegen te gaan.[72] In januari 2021 kwam naar buiten dat al maanden op grote schaal zou zijn gehandeld in privégegevens van Nederlanders, afkomstig uit de coronasystemen van de GGD. Deze kenden serieuze kwetsbaarheden, welke langere tijd bekend waren. Zo hadden medewerkers toegang tot data die zij niet nodig hadden, was er geen sprake van structurele monitoring van (misbruik van) systemen en konden data worden geëxporteerd.[73] Uiteindelijk bleek dat de gegevens van 1.000 personen onbevoegd zijn ingezien, gestolen en mogelijk verkocht, via screenshots uit het systeem CoronIT.[74] In totaal zijn zeven verdachten aangehouden.[75] Hier was dus sprake van een insider threat. Datalekken zoals deze kunnen gevolgen hebben voor de bereidheid van burgers om zich te laten testen of vaccineren en daarmee voor het terugdringen van het aantal COVID-19 besmettingen.

Ook private organisaties verwerken grote hoeveelheden data en er zijn het afgelopen jaar incidenten geweest waarbij grootschalig werd gelekt. Hackers wisten bijvoorbeeld toegang te krijgen tot een database van de Koninklijke Nederlandsche Wielren Unie met daarin data van 90.000 personen.[76] Na 'ongewenste toegang' tot een mailbox van Transavia lekten de data van tienduizenden klanten die in januari 2020 met de maatschappij hebben gereisd.[77]

6. Niet functionerende processen door uitval

Een cyberincident leidt tot verstoring van één of meer processen. Het kan dan gaan om moedwillige verstoringen door een kwaadwillende actor. Het kan ook gaan om uitval door natuurlijke of technische oorzaken of door niet-moedwillig menselijk handelen. Voor de concrete impact maakt het weinig verschil of een proces niet beschikbaar is vanwege verstoring door een kwaadwillende actor of door uitval.

Het afgelopen jaar hebben zich met regelmaat storingen voorgedaan in processen, bij Internet Service Providers, financiële instellingen, in de telecomsector, in ziekenhuizen en in de publieke sector. Bij de GGD zorgde overbelasting van de systemen voor overlast voor de eigen digitale processen, maar het beperkte ook het landelijke inzicht in het aantal besmettingen.[78] Dit type uitval heeft als onmiddellijk gevolg dat digitale processen van vitale aanbieders die van deze organisaties afhankelijk zijn ook niet meer functioneren. Zo hebben storingen een domino-effect. De eerdergenoemde versnelde digitalisering maakt dat analoge en fysieke terugvalopties in evenredig tempo verdwijnen.

ICT-storing bij diverse ziekenhuizen door problemen bij hostingprovider

Op 8 oktober 2020 werd ICTZ, een ICT-dienstverlener voor Nederlandse ziekenhuizen, getroffen door een storing. Het onmiddellijk effect was de verstoring van digitale processen bij verschillende klanten van ICTZ. Patiënten konden zich niet digitaal aanmelden bij het ziekenhuis en konden hun online dossier niet inzien. Ook huisartsen konden door de storing niet inloggen bij een aantal ziekenhuizen. ICTZ liet in een verklaring weten dat het probleem lag in de connectiviteit met het datacenter waarbij ICTZ zelf weer klant was. De hostingprovider heeft de storing opgelost door herstelwerkzaamheden op het platform en heeft componenten vervangen in het datacenter.[79]

Pandemie zorgt voor versnelde digitalisering

3 COVID-19: actualiteit beïnvloedt dreigingsbeeld

Actuele gebeurtenissen waar wereldwijd veel aandacht voor is, beïnvloeden het dreigingsbeeld. Sinds begin 2020 is COVID-19 wereldwijd een van de belangrijkste actuele gebeurtenissen. Als gevolg van COVID-19 is de digitalisering van de maatschappij versneld. Dat betekent dat nog meer dan voor de pandemie een zwaar beroep wordt gedaan op de digitale ruimte. Digitale processen zorgen voor veerkracht en continuïteit tijdens de pandemie, maar cybercriminelen en statelijke actoren spelen snel in op het uitbuiten van nieuwe kwetsbaarheden. Cybercriminelen hebben phishing- en malware-campagnes met een COVID-19 thema uitgevoerd. Statelijke actoren hebben de pandemie aangegrepen voor spionage doeleinden. Ook in de toekomst zullen actoren wereldwijde gebeurtenissen blijven aangrijpen om aanvallen uit te voeren. Daarmee is opnieuw gebleken dat de digitale dreiging een permanent karakter heeft. De pandemie heeft in Nederland ook geleid tot toegenomen aandacht voor risico's en het (versneld) treffen van maatregelen door bedrijven en organisaties.

Digitale processen zorgen voor veerkracht en continuïteit

De samenleving is het afgelopen jaar geconfronteerd met de gevolgen van COVID-19. De dodelijke slachtoffers, de sluiting van scholen, horeca, cultuur- en sportlocaties, het tijdelijk stopzetten van contactberoepen en thuiswerken hebben grote economische en sociaal-maatschappelijke gevolgen. Processen met een digitale component zorgen in de huidige pandemie voor veerkracht en continuïteit.[80] Dankzij de verdergaande digitalisering van de maatschappij konden commerciële, educatieve en sociale activiteiten die anders volledig stil zouden vallen als gevolg van de pandemie toch (deels) doorgaan.

Digitale infrastructuur cruciaal tijdens pandemie

Op dit moment is continuering van het dagelijks leven, nog meer dan voor de pandemie, afhankelijk van de digitale ruimte. Grote verschuivingen en pieken in de vraag naar data en een toename in het mobiele belverkeer in Nederland laten het cruciale belang zien van de beschikbaarheid van de digitale infrastructuur.[81] Verstoring of uitval van de digitale ruimte kan leiden tot verstoring van het dagelijks leven of zelfs tot maatschappelijke ontwrichting.

Zwaar beroep op digitale ruimte

De digitale samenleving biedt volop kansen en oplossingen, zeker tijdens COVID-19, maar de grootschalige verschuiving naar 'online leven' en werken maakt ons ook kwetsbaar. De snelle overgang naar massaal thuiswerken heeft geleid tot een vergroting van het aanvalsoppervlak, de verschillende manieren waarop een aanvaller kan toeslaan, waardoor de kans op geslaagde aanvallen toeneemt.[82] Er wordt niet altijd gebruik gemaakt van beveiligde apparatuur die door de ICT-afdeling is geconfigureerd. Er wordt meer met thuis-apparatuur gewerkt waarvoor mensen zelf verantwoordelijk zijn, ook op veiligheidsgebied. Massaal thuiswerken vergroot de kans dat gevoelige of vertrouwelijke data van organisaties en bedrijven terechtkomt buiten het gebruikelijke beveiligde netwerk. Ook de digitale processen van organisaties betrokken bij de bestrijding van de pandemie, vormden een risico. Bij de GGD heeft zich het afgelopen jaar een aantal incidenten voorgedaan die het nieuws hebben gehaald (zie de Terugblik). Uit de verschillende incidenten komt het beeld naar voren dat

vertrouwelijkheid en privacy minder prioriteit hadden dan het operationeel krijgen van het bedrijfsproces.[83] Het grote maatschappelijke belang om snel te handelen tijdens de pandemie in combinatie met een grote hoeveelheid persoonsgegevens van burgers, maakten de kans op misbruik van coronasystemen groot.[84]

Actoren misbruiken actuele gebeurtenissen

Actoren zijn opportunistisch en acteren snel waar het aankomt op het exploiteren van nieuwe kwetsbaarheden in processen, technologie en menselijk gedrag. Parallel aan de wereldwijde verspreiding van het COVID-19 virus, veranderde ook het beeld van de dreiging. Sinds het begin van de pandemie zijn verscheidene digitale aanvallen waargenomen met COVID-19 als thema, waarbij verschillende modi operandi zijn toegepast.[85] Er zijn digitale aanvallen uitgevoerd op ziekenhuizen, onderzoeksinstituten en de Wereldgezondheidsorganisatie (WHO). Niet alleen de zorgsector was doelwit, ook overheden en bedrijven kregen te maken met uiteenlopende aanvallen.[86] De politie, het OM en Europol waarschuwden voor de verschillende vormen van misbruik, variërend van cybercriminele aanvallen tot het verspreiden van desinformatie.[87]

COVID-19 leent zich voor social engineering

Sinds het uitbreken van COVID-19 maken actoren misbruik van de informatiebehoefte en angst van mensen. De WHO waarschuwde voor phishing campagnes met COVID-19-thematiek.[88] Een phishing aanval is gericht op het buitmaken van inloggegevens van systemen of andere gevoelige informatie, door ontvangers van een phishing bericht over te halen te klikken op een malafide link.[89] Cybercriminelen gebruiken daarbij social engineering tactieken: ze spelen in op emoties zoals angst, benadrukken de urgentie van hun bericht of spelen in op positieve emoties, zoals collegialiteit. Via phishing werden verschillende ransomware varianten verstuurd. Ransomware-aanvallen kunnen ook plaatsvinden door gebruik te maken van kwetsbaarheden in systemen. Doelgerichte ransomware-aanvallen vormen een ernstige dreiging voor de zorgsector.[90] De zorgsector kan een lucratief doelwit voor cybercriminelen zijn, omdat het voorkomen van ontwrichting in deze sector van groot maatschappelijk belang is.[91] Meerdere Europese ziekenhuizen werden slachtoffer van ransomware-aanvallen.[92] Ook Nederlandse zorginstellingen ontvingen het afgelopen jaar op grote schaal malware per e-mail die geconfigureerd was om ransomware te downloaden. Ondanks het feit dat zij doelwit waren, zijn in de rapportageperiode geen impactvolle ransomware-aanvallen tegen Nederlandse zorginstellingen waargenomen.[93]

Pandemie creëerde ook inlichtingenbehoefte

De WHO verklaarde op 11 maart 2020 dat de uitbraak van COVID-19 officieel was uitgegroeid tot een pandemie.[94] Vlak daarna waarschuwden het Britse NCSC en de Amerikaanse autoriteiten voor spionagecampagnes van statelijke actoren.[95] De AIVD constateerde dat er sprake is van een wereldwijd toegenomen digitale spionagedreiging richting de farmaceutische en medische industrie en onderzoekscentra die geneesmiddelen, antistoffen of vaccins ontwikkelen in relatie tot COVID-19.[96] Nederlandse bedrijven en onderzoeksinstellingen die betrokken zijn bij de preventie en bestrijding van COVID-19 zijn een waarschijnlijk doelwit van deze digitale spionage. Ook is het mogelijk dat Nederlandse overheidsinstanties die de preventie en bestrijding van COVID-19 coördineren slachtoffer worden van digitale spionage. Daarnaast is het mogelijk dat digitale aanvallen uitgevoerd worden op (centrale) databases waarin, in het kader van COVID-19, persoonsgegevens van Nederlanders worden opgeslagen.

Een motief voor spionage kan het bevorderen van de volksgezondheid van het eigen land zijn. Het motief kan ook economisch van aard zijn. Buitgemaakte kennis kan voordeel opleveren voor de eigen farmaceutische industrie of andere organisaties die aan research en development doen.[97] De impact van de huidige digitale spionagedreiging zal langer duren dan de pandemie. Zowel gevestigde als opkomende statelijke actoren kunnen met de buitgemaakte kennis ook na de pandemie een economisch en strategisch voordeel behalen.[98] Waarschijnlijk zullen de COVID-19 gerelateerde digitale aanvallen blijven aanhouden zolang de pandemie voortduurt en vaccins en behandelmethoden nog niet wereldwijd verkrijgbaar zijn.

Toenemende polarisatie kan digitale component krijgen

Actuele thema's, waaronder de COVID-19 maatregelen, geven blijk van of aanleiding tot polarisatie in de samenleving. Die polarisatie kan leiden tot extremistische gedragingen, maar ook tot cyberincidenten. Daar waar een groot deel van de bevolking achter de COVID-19 maatregelen staat, zijn anderen daar fel tegenstander van. Rondom dergelijke thema's kunnen gelegenheidscoalities ontstaan van tegenstanders van uiteenlopende onderwerpen. Er is een (online) context ontstaan waarbinnen de drempel om over te gaan tot extremistische gedragingen wordt verlaagd. Deze context versterkt polarisatie en leidt in een enkel geval tot verharding, intimidatie of (oproepen tot) geweld.[99] De avondklokrellen zijn hier een voorbeeld van. Het is voorstelbaar dat polarisatie ook een digitale component krijgt in de vorm van digitale aanvallen. Zo kunnen tegenstanders van de COVID-19 maatregelen hun ongenoegen uiten door een digitaal proces te verstoren, zoals DDoS-aanvallen tegen overheidsinstanties of andere partijen met tegengestelde ideeën. Ook kunnen ze proberen instanties te hacken om zo aan informatie die komen die een instantie in een kwaad daglicht kan stellen. Uit de hack&leak operatie op het Europees Geneesmiddelenbureau is gebleken dat actoren buitgemaakte informatie in gemanipuleerde vorm gebruiken voor

de verspreiding van desinformatie (zie de Terugblik). In het Dreigingsbeeld Statelijke Actoren is toegelicht hoe statelijke actoren desinformatie inzetten bij beïnvloeding, ook in realtie tot de COVID-19 pandemie.[100] Het is bijzonder lastig voor het brede publiek om gemanipuleerde informatie van echte informatie te onderscheiden. Verschil van inzicht over de waarde van de informatie kan zo ook weer bijdragen aan processen van polarisatie.

COVID-19 leidt ook tot aandacht voor cybersecurity

Uit openbare rapporten en een expertraadpleging blijkt dat de pandemie in Nederland ook heeft geleid tot toegenomen aandacht voor cybersecurity risico's en het (versneld) treffen van maatregelen door bedrijven en organisaties, bijvoorbeeld in het onderwijs.[101] Zo heeft Z-CERT tot doel om de zorgsector weerbaarder te maken tegen digitale dreigingen als phishing en ransomware.[102] Het NCSC helpt Z-CERT om de zorgsector zo goed mogelijk te voorzien van kennis en (dreigings)informatie. Het NCSC heeft diverse (beveiligings)adviezen en dreigingsanalyses gedeeld met zijn doelgroepen met als doel deze weerbaarder te maken tegen COVID-19 gerelateerde digitale dreigingen. Vanwege de toegenomen dreiging richting de zorgsector is de doelgroep van het NCSC door een tijdelijke uitbreiding van de Wet beveiliging netwerk- en informatiesystemen (Wbni) verruimd met onder meer onderzoekscentra, farmaceuten en productiebedrijven die onderzoek doen naar de ontwikkeling of een rol hebben in de productie van een vaccin tegen COVID-19. Daarom heeft het NCSC ook dit type organisaties zijn dienstverlening aangeboden.

Ook het Nederlandse onderwijs investeerde het afgelopen jaar extra in cybersecurity. Het ransomware incident bij de Universiteit Maastricht en de pandemie waren belangrijke redenen hiervoor.[103] Tevens is de Nederlandse burger zich steeds meer bewust van risico's en hoe ze deze kunnen beperken.[104] Op 15 december 2020 zijn EU-Raadsconclusies aangenomen over het versterken van de weerbaarheid van de EU en haar lidstaten en het bestrijden van hybride dreigingen, waaronder desinformatie, in de context van de COVID-19 pandemie.[105] In hoeverre deze initiatieven ter vergroting van de weerbaarheid voldoende opwegen tegen de verder ontwikkelde dreiging, is lastig te beoordelen.

Financieel gewin belangrijkste drijfveer van cybercriminelen

4 Ransomware risico voor nationale veiligheid

Ransomware - het met crimineel oogmerk versleutelen van bestanden en systemen om losgeld te eisen voor het weer toegankelijk maken ervan – is dusdanig geëvolueerd dat het een risico vormt voor de nationale veiligheid van Nederland.[III] In eerdere edities van het CSBN hebben de NCTV en het NCSC ransomware al geïdentificeerd als een verschijnsel dat grote maatschappelijke impact kan hebben. Het kent bovendien een solide verdienmodel en is onderdeel van een omvangrijke, volwassen geworden cybercriminele economie. Het opsporen en vervolgen van daders achter ransomware is dan ook niet toereikend: het verhogen van de weerbaarheid en het verstoren van het verdienmodel verdienen evenveel aandacht. In dit hoofdstuk beschrijft de politie het fenomeen ransomware op daderniveau, op basis van observaties vanuit de opsporing aangevuld met open bronnen. Hieruit volgt een beeld van de huidige aard en omvang van ransomware, het cybercriminele ecosysteem waarvan het deel uitmaakt en de dreiging die daaruit voortvloeit.

Het cybercriminele ecosysteem

'Your files have been encrypted! To decrypt the files, follow the following instructions...' Achter deze gevreesde boodschap zit veel meer dan de cybercrimineel die hem verstuurt. Vaak is de inzet van ransomware de meest zichtbare (en pijnlijke) stap in een veel groter proces waarbij vele criminele actoren en activiteiten samen een complex geheel vormen.

Een volwassen cybercriminele economie

De belangrijkste drijfveer van cybercriminelen is financieel gewin.[106] Dat wordt onderstreept door het feit dat deze vorm van misdaad niet los te zien is van een omvangrijke ondergrondse dienstverleningseconomie. Specialisatie en diversificatie spelen daarbij een belangrijke rol: vrijwel elke stap voor zowel het plegen als het beschermen van cybercriminaliteit wordt als dienst aangeboden.[107] Het cybercriminele ecosysteem laat zich dan ook steeds meer kenschetsen als een volwassen, wereldwijde economische sector waar vraag en aanbod samenkomen op onder meer cybercriminele fora en waar rationele economische afwegingen worden gemaakt tussen investering, risico en rendement. Door deze dienstverlening is cybercriminaliteit toegankelijk voor een grote diversiteit aan daders. ICT (en het uitbesteden daarvan) heeft hier een aanzienlijk versterkend effect: met minimale inzet en middelen kan een dader een grote hoeveelheid criminele handelingen wereldwijd uitvoeren en daarmee maximaal effect sorteren.[108] Met deze vorm van schaalbaarheid onderscheidt cybercriminaliteit zich dan ook bij uitstek van andere criminaliteitsvormen.

Cybercriminaliteit is bovendien uiterst transnationaal. Daders, dienstverleners, slachtoffers en gebruikte of misbruikte infrastructuren kunnen zich verspreid over de hele wereld bevinden, wat uitdagingen met zich meebrengt voor de opsporing, vervolging en bestrijding ervan. Nederland onderscheidt zich daarbij als een land waar bovengemiddeld veel cybercriminele infrastructuur wordt gehost. Dit blijkt uit tal van opsporingsonderzoeken en buitenlandse rechtshulpverzoeken.[109]

III Ransomware kan ook ingezet worden door statelijke actoren met als oogmerk het veroorzaken van schade aan en uitval van processen (voorbeelden zijn WannaCry en NotPetya uit 2017). In dit hoofdstuk ligt de focus specifiek op de inzet van ransomware door criminele actoren en de risico's die daaruit voortvloeien voor de nationale veiligheid.

De mate waarin en de manier waarop daders gebruikmaken van cybercriminele dienstverlening verschilt per dadercategorie. Er kan onderscheid worden gemaakt tussen drie dadercategorieën: cybercriminele dienstverleners, afhankelijke plegers en autonome groepen. Deze ruwe indeling neemt niet weg dat deze categorieën overlap kunnen vertonen.

Cybercriminele dienstverleners

Deze dienstverleners bieden Cybercrime-as-a-Service (CaaS) aan. Vooral op ondergrondse, online platformen zoals gesloten cybercriminele fora, maar ook op zogeheten booter- en stressersites of Telegram-kanalen bieden zij hun producten en diensten aan. Zij zijn vaak in staat om hun bedrijfsprocessen te optimaliseren, te automatiseren en zeer gebruiksvriendelijk te maken, wat bijdraagt aan de schaalbaarheid van cybercriminaliteit.[110] Zo voerde Webstresser, een door de politie en het Openbaar Ministerie (OM) offline gehaalde aanbieder van DDoS-as-a-Service, in een halfjaar tijd wereldwijd zo'n 4 miljoen DDoS-aanvallen met voornamelijk crimineel motief uit voor ruim 150.000 gebruikers.[111]

Afhankelijke plegers

Hierbij gaat het om de voornaamste afnemers van cybercriminele diensten. Het betreft een zeer diverse en grote dadercategorie die zowel individueel als in groepen kan opereren en diverse vormen van cybercriminaliteit pleegt. Deze plegers beschikken daarbij niet zozeer over hoogwaardige technische capaciteiten om bijvoorbeeld zelf malware te ontwikkelen. Om cybercriminaliteit te kunnen plegen en zichzelf daarbij te beschermen voor opsporingsdiensten zijn zij dan ook grotendeels afhankelijk van producten en diensten van cybercriminele dienstverleners.[112]

Autonome groepen

Deze dadercategorie is kleiner qua omvang, maar verantwoordelijk voor vaak geavanceerde aanvallen met een hoge organisatiegraad en een wereldwijde impact. Het betreft veelal losse, niet-hiërarchische samenwerkingsverbanden die al langer actief zijn, daardoor veel kapitaal en expertise hebben en zo in staat zijn om langdurige cybercriminele aanvalscampagnes uit te voeren. Zulke campagnes vergen een lange aanlooptijd, in het begin gekenmerkt door veel investeringen en weinig opbrengst. Indien succesvol, kan de opbrengst echter in de miljoenen euro's lopen.[113] Deze groepen zijn autonoom, omdat ze hun cybercriminele proces hoofdzakelijk in eigen beheer ontwikkelen en uitvoeren.[114] Een uitzondering is gelegen in het afnemen van hele specifieke en gespecialiseerde diensten, zoals het witwassen van grote geldstromen.

De laatste jaren is er een toenemende onderlinge samenwerking tussen autonome groepen. Hierbij worden verschillende specialiteiten samengevoegd tot gecombineerde aanvallen die door hun persistentie, complexiteit en geavanceerdheid in de buurt komen van het niveau van digitale aanvallen door statelijke actoren.[115] Autonome groepen onderscheiden zich echter van statelijke actoren aangezien ze handelen uit individueel eigenbelang en niet uit nationale (geopolitieke) belangen. In sommige gevallen is er echter sprake van overlap of samenwerking tussen deze twee actorgroepen. Naast het transnationale karakter van cybercriminaliteit maakt deze verwevenheid de opsporing en vervolging van met name zware, georganiseerde cybercriminelen nog complexer.

Ransomware als solide verdienmodel

Ransomware biedt cybercriminelen van alle categorieën een solide en aantrekkelijk verdienmodel. Al halverwege de jaren '90 werden de eerste vormen van ransomware ontwikkeld. De eerste jaren leidde deze virusvorm een sluimerend bestaan, omdat het moeilijk bleek om het betaalde losgeld op een voor de crimineel veilige manier te ontvangen. De introductie van de Bitcoin in 2009 veranderde dit. Cryptovaluta bieden ransomware-aanvallers de mogelijkheid om het slachtoffer geld te laten overmaken op een snelle, onomkeerbare en relatief geanonimiseerde manier.[116] Bovendien is er geen toezicht op transacties en uitbetalingen, wat het uiterst aantrekkelijk maakt voor crimineel gebruik. Binnen vijf jaar ontwikkelde ransomware zich tot een lucratief verdienmodel dat bovendien versterkt werd door de intrede van het fenomeen Ransomware-as-a-Service (RaaS).[117]

Ransomware kill chain

Een ransomware-aanval staat niet op zichzelf, maar is vaak onderdeel van een breder proces waarbij verschillende stappen kunnen worden onderscheiden:

- Het begint met het verkrijgen van toegang tot een netwerk, toegang die later mogelijk kan worden doorverkocht.
- Vervolgens vindt consolidatie van de positie binnen het netwerk plaats, en het installeren van additionele malware.
- Daarna kan gekozen worden voor het wegsluizen van waardevolle, gevoelige informatie. Bijvoorbeeld om te koop aan te bieden op de ondergrondse cybercriminele markt, of als middel om het slachtoffer af te persen door (te dreigen met) publicatie.
- De inzet van ransomware betreft vaak het onderdeel van de aanval met de meeste impact.
- De laatste stap bestaat uit de uiteindelijke financiële afhandeling van de afpersing: de onderhandelingen tussen dader en slachtoffer, het eventueel betalen door het slachtoffer, het wegsluizen van het betaalde losgeld, en het witwassen door de dader.[118]

Figuur 1: De ransomware kill chain

Ook hier is diversificatie en specialisatie zichtbaar. Elke stap in deze *ransomware kill chain* kent specialisten die dit ofwel als dienst aanbieden, of samenwerken met andere specialisten om zo zeer effectieve, gecombineerde aanvallen uit te voeren.

Ook hier gelden heldere kosten-batenafwegingen. Bij een gerichte aanval worden bij het bepalen van een losgeldeis factoren meegewogen als de moeite die het binnendringen en onder controle krijgen van een netwerk kost, de risico's die gelden voor de aanvaller om ontdekt te worden, de kapitaalkracht van het slachtoffer en de mate waarin bedrijfscontinuïteit en/of gevoelige data een belangrijke rol spelen voor het slachtoffer.[119] Bovendien geldt dat hoe hoger de algemene betalingsbereidheid onder slachtoffers is, hoe hoger de eisen zullen zijn.[120] Daarbij stelt de politie vast dat een relevant deel van door slachtoffers betaalde losgelden rechtstreeks wordt geïnvesteerd in nieuwe aanvalsinfrastructuren. En dus in het aanvallen van nieuwe slachtoffers.[121]

Ransomware-as-a-Service: een plaag voor het MKB

Het merendeel van de ransomware-aanvallen kenmerkt zich als RaaS.[122] Ransomware-ontwikkelaars vonden hierin een middel om hun malware op grote schaal te verspreiden, zonder zelf direct risico te lopen. RaaS biedt de afnemers van dit product de kans om ook zonder noemenswaardige programmeervaardigheden ransomware toe te passen op netwerken of systemen. Deze afnemers, ook wel *affiliates* genoemd, vallen onder de categorie van afhankelijke plegers. Voor elke geslaagde ransomware-aanval betalen zij de ransomware-ontwikkelaar een vast overeengekomen percentage van het betaalde losgeld.[123]

De slachtoffers van deze veelal ongerichte aanvallen zijn over het algemeen kleine tot middelgrote bedrijven en in toenemende mate publieke instellingen zoals lagere overheden.[124] Dit zijn slachtoffers met doorgaans een lage tot beperkte digitale weerbaarheid, waarin relatief weinig tijd en moeite hoeft te worden gestoken door de aanvaller.[125] In april 2020 schatte Help Net Security naar aanleiding van een enquête onder meer dan 500 leidinggevenden binnen het internationale MKB in dat 46 procent van het MKB ooit slachtoffer was geweest van ransomware.[126]

Big Game Hunting: maatwerk voor maximale opbrengst

Hierbij gaat het om gerichte aanvallen op grote organisaties, waarbij maatwerk wordt verricht om tot maximaal financieel gewin te komen. Het zijn vooral autonome groepen - vaak Oost-Europees - die dergelijke aanvallen (kunnen) uitvoeren. Ransomware vormt hierbij vaak 'slechts' een onderdeel van een proces met meerdere gecombineerde aanvalstechnieken.[127]

In dit proces werken vaak verschillende groepen met ieder hun eigen specialisatie samen, wat de dreiging aanzienlijk verhoogt. Het in 2021 door de politie en het OM offline gehaalde Emotet-botnet bijvoorbeeld, besmette wereldwijd meer dan een miljoen systemen met aanvalsmethoden die niet heel geavanceerd waren. Veelal werden computers ongericht met spam besmet.[128] Dit was mogelijk, omdat optimaal geprofiteerd kon worden van de vaak lage digitale weerbaarheid van slachtoffers, zo bleek uit het opsporingsonderzoek. Een treffend voorbeeld: het aantreffen van tweefactorauthenticatie op een systeem was al een reden om de aanval niet voort te zetten.[129] De volgende stappen in het aanvalsproces waren vaak wél gericht en geavanceerd. De groep achter Emotet manifesteerde zich als dienstverlener door de toegang tot netwerken door te verkopen binnen een selecte klantenkring. Ergens in dit proces vond ook een vorm van triage plaats, waarbij de meest kapitaalkrachtige netwerken hoger werden ingeschaald. De afnemers, in de zin van andere autonome groepen, konden vervolgens hun additionele malware (laten) plaatsen. Bijvoorbeeld TrickBot, die werd ingezet om de positie te consolideren en informatie te stelen. Uiteindelijk waren actoren met behulp van Ryuk-ransomware in staat om op deze netwerken gericht ransomware in te zetten op strategische plekken, waarbij men in staat was om op reële wijze in te schatten wat de maximale losgeldeis kon zijn. Het (dreigen met) het publiceren van de eerder gestolen data kon hierbij fungeren als extra drukmiddel.[130]

Uit opsporingsonderzoeken wordt duidelijk dat dergelijke samenwerking steeds complexere vormen aanneemt. Bij een aanval op een netwerk kunnen daardoor verschillende actoren betrokken zijn, die verschillende rollen aannemen, waarbij het onderscheid tussen plegen en het verlenen van diensten sterk vervaagt. Ook kunnen actoren in verschillende omstandigheden kiezen voor verschillende malware-families, op een *plug-and-play* manier. Dit maakt de opsporing, maar ook de mitigatie ervan bijzonder complex.

Schade als blinde vlek

De totale economische schade van ransomware, in de zin van betaald losgeld, verlies aan bedrijfscontinuïteit, gevolgschade en herstelkosten van alle aanvallen bij elkaar opgeteld is moeilijk vast te stellen. Schattingen van de wereldwijde schade lopen in de miljarden euro's per jaar, waarbij de laatste jaren een scherpe stijging vertonen door een toename van zowel RaaS-, als Big Game Hunting-aanvallen.[131] Het is niet bekend hoeveel de schade voor Nederland betreft. Deze blinde vlek heeft meerdere oorzaken. Naast het sterk transnationale karakter van cybercriminaliteit, wat het ingewikkeld maakt om een beeld te schetsen van de schade voor Nederland, is de aangifte- en meldingsbereid onder slachtoffers van cybercriminaliteit structureel laag.[132]

Meerdere indicatoren wijzen er echter op dat de economische schade van ransomware ook voor Nederland aanzienlijk zal zijn. De geschatte gemiddelde losgeldeis piekte volgens het bedrijf Coveware in het derde kwartaal van 2020 op circa 200.000 euro. Dit betreft het gemiddelde over alle aanvallen wereldwijd: zowel RaaS-aanvallen waarbij misschien enkele duizenden euro's wordt geëist, als aanvallen die van de categorie Big Game Hunting en waarbij de eis in de miljoenen euro's kan lopen.[133] In 2020 zou zelfs een recordbedrag van 25 miljoen euro zijn geëist in de VS of Europa.[134] Volgens sommige schattingen wordt in zo'n 70 procent van alle ransomware-aanvallen losgeld betaald door het slachtoffer[135], al kan de politie dit cijfer niet verifiëren. De politie constateert wel dat ook in Nederland zowel geëiste, als uitbetaalde bedragen inmiddels in de miljoenen euro's lopen.

De totale kosten om een ransomware aanval te boven te komen zijn echter vaak hoger dan de geëiste losgeldbedragen.[136] De Not-Petya ransomware-aanval in 2017 laat zien hoe groot de totale schade van een zeer gedegen uitgevoerde aanval (in dit geval door een statelijke actor) kan zijn. Zo bedroeg deze voor logistiekbedrijf Maersk, dat ook in Rotterdam zwaar werd getroffen, meer dan 200 miljoen euro.[137]

Ransomware en de nationale veiligheid

Ransomware-aanvallen vormen een risico voor de nationale veiligheid als het gaat om de continuïteit van vitale processen, het weglekken en/of publiceren van vertrouwelijke of gevoelige informatie en de aantasting van de integriteit van de digitale ruimte; elementen zoals genoemd in de Geïntegreerde Risicoanalyse Nationale Veiligheid en het Dreigingsbeeld Statelijke Actoren.[138] Dit geldt vooral voor de dreiging die uitgaat van grondig uitgevoerde, gecombineerde aanvallen van de categorie Big Game Hunting. De nationale veiligheid is in het geding wanneer het doelwit van zo'n aanval onderdeel is van de vitale infrastructuur (waaronder de Rijksoverheid en alle vastgestelde vitale processen) en de aanval de continuïteit van vitale processen verstoort. Een ransomware-aanval kan bijvoorbeeld de kantoorautomatisering van zo'n organisatie treffen. Indien toegang tot de procesautomatisering via de kantoorautomatisering loopt, stelt dit de aanvaller in staat om ook de vitale processen te bereiken om daar ransomware te installeren.[139]

Hoewel gerichte ransomware-aanvallen op de vitale processen nog niet in Nederland hebben plaatsgevonden, komen deze reeds in het buitenland voor. Zo zijn in de Verenigde Staten federale overheidsinstellingen, de politie en de energiesector getroffen. Daarnaast hebben ransomware-aanvallen in zowel de Verenigde Staten als in de Europese Unie tijdens de coronapandemie ziekenhuizen, COVID-19-onderzoeksinstellingen en een distributiecentrum voor vaccins ernstig gehinderd.[140]

De combinatie van ransomware met het publiceren of doorverkopen van tijdens de aanval buitgemaakte gevoelige informatie komt ook in Nederland steeds vaker voor. De aanval op de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) begin 2021, waarbij interne documenten zijn gepubliceerd op een speciaal daartoe ingerichte leak site, laat bovendien zien dat dit de positie van Nederland als innovatieland kan raken.[141]

Ransomware-aanvallen op lagere overheden, zoals de aanval op gemeente Hof van Twente in december 2020, vormen een moedwillige aantasting van de integriteit van de digitale ruimte van de overheid. Dit kan gevolgen hebben voor de continuïteit van de dienstverlening door de overheid en het maatschappelijk vertrouwen daarin.[142]

Breaking the ransomware kill chain

De ransomware kill chain onderstreept dat een ransomware-aanval niet op zichzelf staat, maar vaak onderdeel is van een breder proces. Cybercriminelen maken in elke fase van dit proces een heldere kosten-batenanalyse ten aanzien van hun slachtoffers. Dit is de reden waarom politie en het NCSC slachtoffers van een ransomware-aanval adviseren om niet te betalen, omdat losgeldbetalingen een verdienmodel voor criminelen in stand houden. Door ransomware niet alleen als een technisch probleem te zien, maar ook aandacht te hebben voor deze economische kant van een cybercriminele aanval, ontstaat ruimte voor een meer holistische benadering van het probleem. Elke fase van de ransomware kill chain biedt kansen om in te grijpen, zowel offensief als defensief. Offensief door in internationaal verband de belangrijkste plegers en dienstverleners te bestrijden, zoals het offline halen van het Emotet-botnet en het opsporen van de verantwoordelijke criminelen. Of door slachtoffers in staat te stellen gratis hun bestanden te ontsleutelen, zoals bij NoMoreRansom mogelijk is.[143] Defensief door de weerbaarheid te verhogen voor alle fasen van de kill chain en zodoende de gelegenheid voor de aanvallers te beperken om toe te slaan. Dit is soms al mogelijk met eenvoudige stappen, zoals het toepassen van tweefactorauthenticatie.

De meest kansrijke oplossing ligt dan ook in het structureel laten stijgen van de kosten voor de criminelen ten opzichte van de baten van ransomware. Dit kan alleen als politie, het NCSC en OM samen met publieke en private partners en (potentiële) slachtoffers een vuist maken door proactief samen te werken en daarbij gericht informatie en inzichten te delen.

Verwevenheid met mondiale digitale ruimte betekent kwetsbaarheid

5 Schending digitale ruimte vormt risico

Schending van de (veiligheid van de) digitale ruimte vormt een risico voor de nationale veiligheid. Belangrijke elementen voor het functioneren van de digitale ruimte zijn namelijk kwetsbaar voor uitval en/of voor misbruik. Die schending is geen theoretische mogelijkheid, maar vindt daadwerkelijk plaats. Zo zijn er opnieuw geavanceerde aanvallen in de ICT-leveranciersketen met een mondiale impact aan het licht gekomen en zijn aanwezige kwetsbaarheden in mondiaal gebruikte producten misbruikt. Verhoging van de weerbaarheid daartegen is voor individuele staten en organisaties beperkt mogelijk.

Veiligheid digitale ruimte raakt nationale veiligheid

Digitale processen verweven met, en afhankelijk van, digitale ruimte

Al onze digitale processen zijn sterk verweven met de mondiale digitale ruimte. Digitale processen van bijvoorbeeld aanbieders van vitale infrastructuur, maar ook die van grote en kleine organisaties en burgers, maken gebruik van de diensten en producten van wereldwijd opererende bedrijven. Voorbeelden daarvan zijn producten voor het werken op afstand, het beheer en verzenden van e-mails en de opslag en verwerking van informatie bij een cloudleverancier. Die verwevenheid geldt ook voor de technische infrastructuur van het internet, waaronder onderzeese kabels.

Dat digitale processen gebruik kunnen maken van de digitale ruimte en daarmee verweven zijn, heeft veel goeds gebracht en biedt nog steeds kansen. Het vormt daarentegen ook een risico. De keerzijde van die verwevenheid is immers complexiteit, afhankelijkheid en kwetsbaarheid voor misbruik en uitval. Cyberincidenten kunnen daardoor onze maatschappij in het hart raken en gedurende korte of langere tijd verlammen. Veiligheid van de digitale ruimte is dan ook onlosmakelijk verbonden met de nationale veiligheid.

Het begrip digitale ruimte

De digitale ruimte is de complexe omgeving die het resultaat is van onderling verweven digitale processen, ondersteund door wereldwijd gedistribueerde fysieke ICT en verbonden netwerken. Drie invalshoeken kunnen worden onderscheiden[144]:

1. Digitale processen (proceslaag). Het gaat hier om de wijze waarop organisaties en mensen de digitale ruimte gebruiken en daarmee om de functionaliteit van de digitale ruimte voor de samenleving en economie.
2. ICT, netwerken en protocollen (technische laag). Deze laag maakt digitale processen mogelijk en omvat uiteenlopende en samenhangende vormen van hard- en software en netwerken. Internet, als netwerk van netwerken, vormt voor een groot deel die laag.
3. Risicomanagement en/of governance (governance-laag). Het gaat hier om de wijze waarop digitale processen en de technische laag kan en moet worden aangestuurd.

Dit hoofdstuk concentreert zich op de technische en de proceslaag.

De 'digitale ruimte' is een complex begrip, waarbij geen consensus bestaat over de belangrijkste elementen voor het functioneren ervan. Vanuit een technisch perspectief identificeerde TNO zes belangrijke elementen voor het functioneren van het internet.[145] De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) richtte zich op enkele zogeheten protocollen en stelde dat het internet een mondiale publieke kern heeft die de belangen van afzonderlijke staten en van particulieren overstijgt.[146] Verder zijn in ieder geval vitale processen die de digitale ruimte mede vorm geven en enkele mondiale ICT-leveranciersketens belangrijke elementen. Zo gebruiken veel organisaties clouddiensten van Amazon en Microsoft en software-suites als Microsoft Office.

Belangrijke elementen voor functioneren digitale ruimte

Belangrijke elementen voor het functioneren van het internet vanuit technisch perspectief (TNO)

1. Domain Name System (DNS): dit is een systeem en netwerkprotocol dat domeinnamen in tekst (leesbaar voor mensen) vertaalt naar IP-adressen (bruikbaar voor machines) en omgekeerd.
2. Border Gateway Protocol (BGP): dit is het belangrijkste routeringsprotocol van het internet.
3. Network Time Protocol (NTP): dit protocol wordt op zeer grote schaal gebruikt om tijdsynchronisatie tussen computers ofwel een netwerk tijdstandaard (Network Time) te regelen. Als tijdsbron voor het NTP worden veelal GPS-ontvangers gebruikt.
4. Fysieke internet infrastructuur
   - Zeekabels en glasvezel: de fysieke kabelinfrastructuur waarvan het internet afhankelijk is bestaat uit grote zeekabels en kabels over land (voornamelijk glasvezel).
   - Grote Internet Exchanges: Internet Exchanges vormen een netwerk platform voor internet Service Providers en andere aangesloten partijen om IP-verkeer uit te wisselen.
   - Grote datacenters: er zijn in toenemende mate grote datacenters van waaruit belangrijke (cloud)diensten worden geleverd.
5. Vertrouwensdiensten: veel digitale processen vereisen dat het dataverkeer wordt geverifieerd door middel van een vertrouwensdienst. Dit gebeurt met behulp van digitale certificaten die worden uitgegeven door zogeheten Certificate Authorities.[147] Onderdelen van die vertrouwensdiensten kunnen zijn authenticatie[IV], digitale ondertekening en versleuteling.[148]
6. Elementen die cruciaal zijn voor de vitale infrastructuur: het gaat hierbij enerzijds om de lokale fysieke infrastructuur in beheer van netwerkbeheerders die zorgt voor de connectiviteit van gebruikers en anderzijds om specifieke diensten, applicaties, peering-connecties[V] of servers die van belang zijn voor specifieke vitale infrastructuur.[149]

Belangrijke elementen die publieke kern van het internet vormen (WRR)

7. Transmission Control Protocol (TCP)[150]: TCP zorgt er voor dat de gegevens aankomen zoals ze zijn verstuurd en dat eventuele communicatiefouten, zowel in de gegevens zelf als in de volgorde van de gegevens, kunnen worden opgevangen.
8. Internet Protocol (IP)[151]: dit protocol zorgt voor de adressering van internetverkeer zodat het bij het beoogde doel aankomt.

Overige als belangrijk te beschouwen elementen in de proceslaag

9. De (Nederlandse) vitale processen 'Internet en datadiensten', 'Internettoegang en dataverkeer' en 'Spraakdiensten en SMS'. Deze processen geven mede vorm aan de digitale ruimte en zijn daardoor belangrijke elementen voor de wijze waarop organisaties en mensen de digitale ruimte (kunnen) gebruiken.
10. Mondiale ICT-leveranciersketens: ICT-leveranciersketens bestaan uit organisaties die hardware, software en (informatie) diensten produceren en verkopen, bijvoorbeeld ICT-dienstverleners of softwareleveranciers.[152] Welke belangrijk zijn voor het functioneren van de digitale ruimte en waarvoor geldt dat cyberincidenten de nationale veiligheid van Nederland kunnen aantasten, is niet vastgesteld.

Technische laag digitale ruimte kwetsbaar voor uitval en misbruik

Belangrijke elementen voor het functioneren van de (technische laag van de) digitale ruimte zijn potentieel kwetsbaar voor uitval en/of voor misbruik. Zo zijn enkele voorbeelden bekend van breuken in onderzeese kabels die het intercontinentale internetverkeer verzorgen. Deze hebben geleid tot (tijdelijke) verminderde beschikbaarheid in de regio waar dat optrad. Een voorbeeld van misbruik is het aftappen van het dataverkeer via onderzeese kabels voor inlichtingenvergaring door statelijke actoren.[153] Het CSBN 2020 vermeldde het wijzigen van DNS-instellingen als aanvalstechniek. Hierdoor kan inkomend netwerkverkeer van een organisatie tijdelijk worden omgeleid en onderschept voor bijvoorbeeld spionage.[154]

Schending van de technische laag kan impact hebben op de nationale veiligheid. Stel dat een kernprotocol zou worden gemanipuleerd of dat enkele onderzeese kabels zouden worden gesaboteerd. Dit kan dan snel en op grote schaal – door het zogeheten cascade effect – gevolgen hebben voor enkele nationale veiligheidsbelangen: economische veiligheid, fysieke veiligheid en sociale en politieke stabiliteit. Dit kan ook het vertrouwen van burgers en organisaties in de digitale ruimte en digitalisering

IV Een handeling, proces of methode om bijvoorbeeld de identiteit van een organisatie of financiële transactie te verifiëren.

V Peering is een proces waarbij twee internetnetwerken verbinding maken en dataverkeer uitwisselen. Via peering kunnen partijen rechtstreeks dataverkeer afhandelen zonder een derde partij te hoeven betalen. Ontleend aan: https://www.netnod.se/ix/what-is-peering.

aantasten. Vertrouwen in de werking van de digitale ruimte is essentieel, omdat daar het vertrouwen in digitale processen op is gebaseerd[155] en omdat die processen een sleutelrol vervullen in onze hedendaagse samenleving en economie.

Het verhogen van de weerbaarheid tegen uitval en misbruik van elementen van de technische laag is voor individuele staten en organisaties beperkt mogelijk. Een reden is dat de digitale ruimte een ecosysteem is dat bestaat uit vele componenten én waarin vele partijen een rol spelen. In het CSBN 2020 is toegelicht dat er diverse redenen zijn waardoor veiligheid van de digitale ruimte niet vanzelf tot stand komt. Ook zijn de risico's voor de gehele digitale ruimte en de doorwerking daarvan op de maatschappij lastig te doorgronden.[156] Wel is in de opzet van het internet rekening gehouden met kwetsbaarheden voor bijvoorbeeld uitval van onderdelen. Zo is sprake van een grote mate van redundantie en flexibiliteit in de infrastructuur. Ook in de opzet van de protocollen is rekening gehouden met uitval van onderdelen van de infrastructuur.

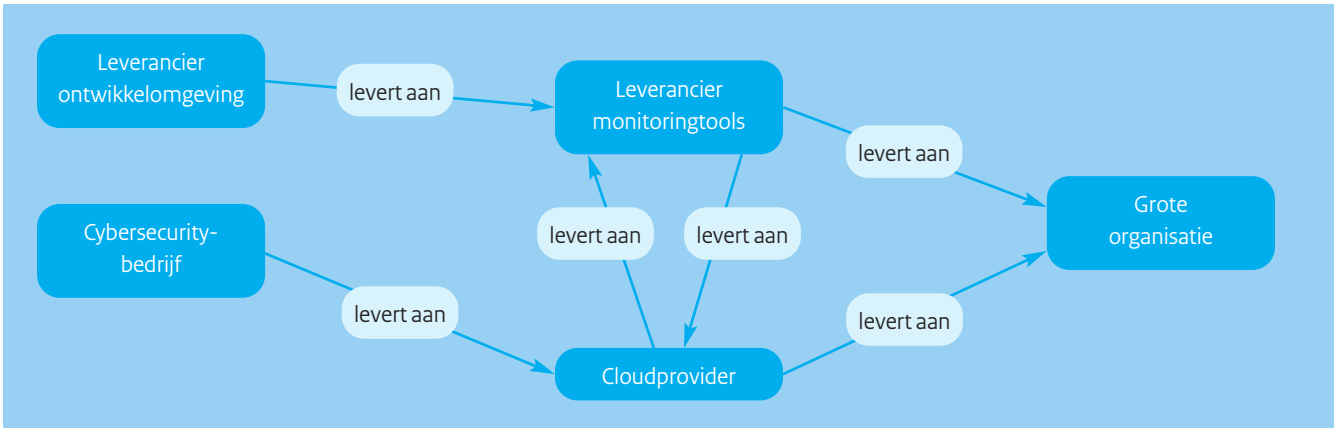
Misbruik kwetsbaarheden in soft- en hardware baart zorgen

Het misbruik van (zero day) kwetsbaarheden in veelgebruikte software of hardware baart zorgen vanwege de schaalgrootte van de impact. Zo maakte een actor sinds begin 2021 misbruik van (toen nog onbekende) kwetsbaarheden in Microsoft Exchange Server. Die kwetsbaarheden raakten potentieel honderdduizenden organisaties wereldwijd. Toen Microsoft de kwetsbaarheden op 2 maart bekendmaakte, gelijktijdig met patches om die te verhelpen, maakten ook andere actoren misbruik van die kwetsbaarheden bij organisaties die de patches niet (tijdig) hadden doorgevoerd (zie kern-CSBN). Het NCSC stelde dat de gevolgen van de kwetsbaarheden in Microsoft Exchange Server groot waren voor Nederlandse organisaties en bedrijven. Het NCSC constateerde dat er als gevolg van deze kwetsbaarheden data werd gestolen, malware werd geplaatst, achterdeurtjes werden ingebouwd en mailboxen werden aangeboden op de zwarte markt. Via de kwetsbaarheden in Microsoft Exchange server konden kwaadwillenden mogelijk ook in andere systemen komen.[157] Op 20 april 2021 waarschuwde Pulse Secure voor een actief aangevallen zero day kwetsbaarheid in de vpn-software van het bedrijf waardoor aanvallers op afstand kwetsbare VPN-servers konden overnemen. Een beveiligingsupdate was nog niet voorhanden en volgens Pulse Secure vormde het beveiligingslek een zeer groot risico voor organisaties. Wel was een 'workaround' gepubliceerd en een tool waarmee klanten kunnen kijken of hun VPN-server is gecompromitteerd.[158] Pulse Secure wordt wereldwijd gebuikt en de kwetsbaarheid maakt vele organisaties kwetsbaar voor misbruik door kwaadwillenden.

Misbruik mondiale ICT-leveranciersketens komt veelvuldig voor

Wat betreft de proceslaag, de wijze waarop organisaties en mensen de digitale ruimte gebruiken, baart vooral misbruik van mondiale ICT-leveranciersketens zorgen.[159] In de afgelopen drie CSBN's is gewezen op de dreiging die uitgaat van een aanval op ICT-leveranciersketens, gemakshalve aangeduid als 'ketens'.[160] Zo'n aanval is gericht op een of meer kwetsbare plekken in ketens in plaats van op een specifiek proces of een specifieke organisatie. Via zwakke plekken in ketens kan een actor vele processen of organisaties treffen. Omgekeerd zijn die verweven met talrijke ketens en ze zijn daardoor kwetsbaar voor aanvallen via en binnen elk van die ketens. Die connecties en dus kwetsbaarheden kunnen ver gaan (zie figuur 2). Alleen al in de onderstaande sterk vereenvoudigde weergave kan een actor die een proces van een grote organisatie wil aanvallen dat proberen via de processen van vier andere organisaties. Zo zou een aanvaller via een leverancier van monitoringtools kunnen proberen de cloudprovider aan te vallen en via die provider weer een grote organisatie.[161] Ook is grootschalige uitval binnen of van ketens denkbaar. Enkele techbedrijven hebben een dominante marktpositie voor bepaalde vormen van dienstverlening. De kans op uitval is wellicht niet heel groot, maar als sprake is van uitval dan werkt dat door naar digitale processen van vele staten en organisaties.

Figuur 2: Vereenvoudigde visualisatie ICT-leveranciersketen



Eind 2020 werd de zogeheten SolarWinds campagne[VI] ontdekt (zie ook de Terugblik). Hierin compromitteerde een actor op verschillende manieren software in ICT-leveranciersketens. Waar aanvallen in het verleden gericht leken, lijken deze breed ingezet te zijn door de actor. Deze campagne had potentieel een veel grotere impact dan eerder onderkende leveranciersketen aanvallen. Niet alleen is de door de actor initieel aangebrachte kwetsbaarheid in het product Orion van SolarWinds daadwerkelijk misbruikt bij verschillende Amerikaanse overheidsinstanties. Ook meerdere cybersecuritybedrijven en techbedrijven die wereldwijd klanten hebben, zoals FireEye, Mimecast en Microsoft, hebben aangegeven gecompromitteerd te zijn geweest via de kwetsbare versie van Orion. Wanneer de gecompromitteerde versie niet zou zijn ontdekt, had de actor mondiaal veel meer organisaties kunnen treffen.

Leveranciersketenaanval op ontwikkelomgeving van Codecov

Codecov, gevestigd in San Francisco, stelde in een verklaring dat een of meerdere hackers op 31 januari jongstleden begonnen te knoeien met software die in de technische industrie wordt gebruikt om code te testen op fouten en kwetsbaarheden. De aanvaller(s) wist toegang te krijgen tot de ontwikkelomgeving van Codecov en is erin geslaagd om malware in een script van het bedrijf te verbergen. Op die manier kon de aanvaller(s) wachtwoorden, tokens en keys van klanten buitmaken. Codecov waarschuwde dat de aanvaller(s) in potentie informatie kon exporteren die was opgeslagen op de CI-omgevingen[VII] van klanten. De hack werd op 1 april 2021 ontdekt toen een klant merkte dat er iets mis was met het script. Codecov stelt op zijn website dat het 29.000 klanten heeft, waaronder Procter & Gamble Co, webhostingbedrijf GoDaddy Inc, The Washington Post en het Australische softwarebedrijf Atlassian Corporation PLC. Hoeveel bedrijven daadwerkelijk slachtoffer zijn geworden van de hack op Codecov is niet bekend. Beveiligingsexperts die bij de zaak betrokken waren, stelden dat de omvang van de aanval en de vaardigheden die nodig zijn vergelijkbaar zijn met de SolarWinds-aanval (zie de Terugblik). Via klanten van Codecov konden potentieel ook andere bedrijven gecompromitteerd worden. De aanvallers zouden extra moeite hebben gedaan om door middel van Codecov toegang tot andere softwareontwikkelaars te krijgen, alsmede tot bedrijven die technische diensten leveren.[162]

Schending van bepaalde mondiale ICT-leveranciersketens kan impact hebben op de nationale veiligheid doordat bijvoorbeeld vitale processen gedurende langere of kortere tijd niet meer beschikbaar zijn of niet juist verlopen. Taken van organisaties kunnen dan niet meer of beperkt(er) worden uitgevoerd, zoals het distribueren van energie, het uitvoeren van financiële transacties of het verzorgen van onderwijs. Gevoelige of kwetsbare persoonlijke, economische of politieke informatie kan inzichtelijk worden voor kwaadwillenden. Dit kan de economie van Nederland raken of Nederland op achterstand zetten bij internationale onderhandelingen. Naast die directe impact, heeft schending van de digitale ruimte ook een bredere impact. Er moet bijvoorbeeld veel capaciteit en geld worden besteed aan het onderzoek naar misbruik en herstel daarvan. In sommige gevallen moet een gehele infrastructuur van organisaties opnieuw worden opgebouwd. In de tussentijd is onbekend in hoeverre actoren nog aanwezig zijn binnen de infrastructuur van organisaties en of misbruik nog steeds mogelijk is. Dat kan betekenen dat (deels) teruggevallen moet worden op analoge processen die veelal ontbreken of bijvoorbeeld tot hogere kosten kunnen leiden. Schending kan ook het vertrouwen van burgers en organisaties in digitale processen aantasten en mogelijk verdere digitalisering hinderen.

Het verhogen van de weerbaarheid tegen schending van ICT-leveranciersketens is in de praktijk beperkt mogelijk. Digitale processen zijn verweven met en maken gebruik van diverse complexe ketens.[163] Er is veel 'laaghangend fruit' voor aanvallers waarvan organisaties zich lang niet altijd bewust zijn, totdat het mis gaat.[164] Als er al een risicobeoordeling plaatsvindt van derde partijen, dan biedt dat geen zekerheid dat die partij niet indirect wordt misbruikt.[165] Niemand draagt bovendien de volledige verantwoordelijkheid voor de veiligheid van de hele keten[166] en de keten is niet transparant. Cybersecurity expert Bruce Schneier stelde in dat kader: "We can't trust anyone, yet we have no choice but to trust everyone".[167]

VI Hoewel deze campagne in media de 'SolarWinds campagne' wordt genoemd, is dit geen juiste weergave doordat bijna een derde van de door de actor getroffen organisaties geen directe connectie had met SolarWinds. Zie https://www.securityweek.com/cisa-says-many-victims-solarwinds-hackers-had-no-direct-link-solarwinds.

VII CI staat voor continuous integration. "Continuous integration is a software development process where developers integrate the new code they've written more frequently throughout the development cycle [....] continuous integration helps streamline the build process, resulting in higher-quality software and more predictable delivery schedules." https://www.ibm.com/cloud/learn/continuous-integration.

Beïnvloeding, inmenging, spionage en informatieconfrontatie veel gebruikt

6 Geopolitiek beïnvloedt dreiging en belangen

De binnenlandse verhoudingen en de verhoudingen tussen staten zijn bepalend voor de belangen die staten behartigen en de doelstellingen die zij nastreven. Dit zorgt voor een geopolitiek krachtenveld dat in beweging is en zich ook laat voelen in de digitale ruimte. Statelijke actoren gebruiken namelijk ook daar hun instrumentarium om hun belangen te behartigen. En soms vormt die belangenbehartiging een dreiging voor de nationale veiligheidsbelangen van anderen, zoals blijkt uit het Dreigingsbeeld Statelijke Actoren van AIVD, MIVD en NCTV.[168]

Dreiging ontwikkelt zich

De dreiging die van statelijke actoren uitgaat, is niet van vandaag of gisteren, maar ontwikkelt zich al langer. Soms wordt ze diffuser, soms juist meer manifest. Dit heeft niet alleen te maken met geopolitieke verschuivingen, zoals de opkomst van nieuwe machten die vraagtekens zetten bij de naoorlogse internationale orde of de hernieuwde assertiviteit van gevestigde machten.[169] Ook de middelen veranderen. Dat maakt dat de dreiging die uitgaat van statelijke actoren richting de Nederlandse samenleving divers en complex is. De toegenomen digitalisering en technologische mogelijkheden vergroten de risico's die daarmee samenhangen.

Verschillende staten ontplooien een breed scala aan activiteiten bij de behartiging van hun belangen. Ze kunnen daarbij alle middelen inzetten die binnen hun overheidsinstrumentarium ter beschikking staan. Hun activiteiten kunnen onze nationale veiligheid raken. De dreiging komt zowel van statelijke actoren met een andere strategische agenda als van statelijke actoren met een ander politiek systeem dan Nederland. De dreiging kan zich direct manifesteren of via proxy's, deze term verwijst naar derde partijen die door statelijke actoren worden ingezet. De afgelopen jaren zijn concrete manifestaties van dreigingen waargenomen vanuit verschillende staten. Beïnvloedings- en inmengingsactiviteiten, spionageactiviteiten en informatieconfrontatie zijn veelgebruikte werkwijzen. Bij informatieconfrontatie wordt het informatiedomein, waaronder media, sociale media en platforms, als strijdarena gezien en wordt informatie als wapen ingezet om schade aan te richten. Ook zetten statelijke actoren economische instrumenten in om geopolitieke doelen te behalen. Zelfs activiteiten die maar door weinig statelijke actoren ontplooid worden, zoals voorbereidingen op en daadwerkelijke sabotage, kunnen potentieel ernstige gevolgen hebben voor de nationale veiligheid.[170]

Motieven statelijke actoren variëren

De motieven van statelijke actoren voor het inzetten van middelen in of tegen andere staten variëren. Voor een belangrijk deel is er sprake van het behartigen van binnenlandse politieke en veiligheidsbelangen. Denk daarbij aan het bestrijden van dissidenten die in het buitenland wonen. Een belangrijke drijfveer hierbij is het streven naar het behoud van de status quo in het herkomstland: inclusief de bestaande statelijke structuur, rol en positie van het staatshoofd en rol en positie van de onderdanen (in zowel binnen- als buitenland). Activiteiten die hiermee samenhangen zijn weliswaar niet direct tegen Nederland of onze bondgenootschappen gericht, toch kunnen ze wel degelijk onze belangen schaden.

Andere motieven zijn vaak financieel-economisch. Ook hier speelt het behoud van de statelijke status quo in het herkomstland een grote rol. De diaspora (bevolkingsgroepen die buiten het land van herkomst wonen) vormt daarbij een bron van inkomsten, doordat zij investeringen doet (zoals de aankoop van onroerend goed) en financiële ondersteuning biedt aan achtergebleven familie. Opvallend zijn die staten voor wie het ontplooien van illegale digitale activiteiten een verdienmodel is geworden. Zo behaalt Noord- Korea een belangrijk deel van de staatsinkomsten uit

illegale digitale activiteiten zoals ransomware-aanvallen tegen internationale bedrijven en digitale diefstal.[171] Groot is ook het aandeel van economische spionage, waarmee statelijke actoren bijvoorbeeld beogen de eigen concurrentiepositie te verbeteren of hoogwaardige kennis en technologie te bemachtigen zonder zelf de kosten voor research en development te maken. Exemplarisch hiervoor is de Chinese economische spionage, die zich vooral richt op technologiediefstal en voorkennis inzake voorgenomen investeringen.[172]

Bij het derde cluster van motieven spelen de buitenlandse verhoudingen nadrukkelijker een rol. Het gaat hier bijvoorbeeld om het versterken van de strategisch-militaire positie ten opzichte van andere staten. Zo zoeken Iran, Syrië, Noord-Korea en Pakistan in Nederland en andere westerse landen naar kennis en goederen die zij nodig hebben voor de ontwikkeling van hun programma's voor massavernietigingswapens en overbrengingsmiddelen.[173] Andere drijfveren zijn bijvoorbeeld: het verkrijgen van politieke informatie over regeringsstandpunten en besluitvorming van andere staten; of het beïnvloeden van politiek-bestuurlijke processen in andere staten. Deze drijfveren kunnen ertoe leiden dat er allerlei activiteiten worden ontplooid die Nederlandse belangen schaden, zoals spionage, maar ook heimelijke politieke beïnvloeding, beïnvloeding en intimidatie van diaspora, sabotage en misbruik van de Nederlandse ICT-infrastructuur.[174] In eerdere CSBN's is al gewaarschuwd voor toenemende activiteiten die zijn gericht op het (in de toekomst) mogelijk maken van sabotage van vitale infrastructuren in Europa.[175] De afgelopen jaren zijn daarnaast toeleveranciers van vitale processen succesvol aangevallen. Door impliciet of expliciet te dreigen met verstoring of sabotage kan een actor economische, politieke, diplomatieke of militaire invloed uitoefenen op zijn doelwit. De dreiging die uitgaat van mogelijke verstoring en sabotage is daarmee een middel om besluitvormingsprocessen te beïnvloeden.

Digitale ruimte biedt schatkist aan opties

De digitale ruimte is bijzonder geschikt voor het behartigen van de belangen achter deze uiteenlopende motieven. In de eerste plaats omdat, door de toegenomen digitalisering en het Internet of Things, vrijwel ieder doelwit digitaal benaderbaar is en de toegankelijkheid van doelwitten ook nog relatief gemakkelijk en laagdrempelig is. Daarnaast is attributie aan een statelijke actor lastig, waardoor sprake is van een laag afbreukrisico bij de inzet van digitale middelen. Bovendien is die inzet aanzienlijk goedkoper en minder risicovol dan de inzet van andere middelen, want ze zijn tijds- en arbeidsextensief en tools en werkwijzen zijn herbruikbaar. Tot slot zijn digitale operaties flexibeler schaalbaar dan fysieke operaties en is de opbrengst ervan aanzienlijk gegroeid. Daarmee valt de kosten-batenanalyse dus gunstig uit.

Vrijwel elk land met basale capaciteiten en de intentie om digitaal binnen te dringen, zal in staat zijn om dit bij diverse organisaties in Nederland succesvol te doen. Dat zegt iets over de weerbaarheid, die bij diverse organisaties nog steeds tekortschiet (zie ook het kern-CSBN). Uit onderzoeken blijkt dat staten als China, Rusland en Iran offensieve cyberprogramma's hebben, gericht tegen Nederland.[176] Daaruit spreekt zowel de capaciteit als de intentie om in Nederlandse organisaties binnen te dringen. De cybercapaciteiten, kennis en expertise van China en Rusland zijn zelfs zo omvangrijk, dat de kans groot is dat zij slagen wanneer ze ergens digitaal binnen willen dringen.[177] In open bronnen maken cybersecuritybedrijven melding van een toename van offensieve cyberactiviteiten van staten die voorheen niet bekend stonden om hun digitale capaciteiten, zoals India, Vietnam, Kazachstan, Libanon, Marokko, Ethiopië en Soedan.[178] Deze staten ontwikkelen deels zelf die capaciteiten of besteden cyberoperaties uit aan derden. Zo gaat de opkomst van nieuwe cyberactoren samen met de opkomst van 'hackers for hire', geavanceerde hackersgroepen die hun (veelal spionage)diensten verhuren aan overheden of vermogende klanten. De activiteiten van nieuwe cyberactoren en hacker-for-hire groepen kunnen ook Nederlandse belangen raken. Zo kan een land of actorgroep zich in een conflictsituatie ineens of ook op Nederland gaan richten.

Een belangrijke vraag hierbij is, in hoeverre deze 'democratisering' van cybercapaciteiten ook weer invloed heeft op de geopolitieke intenties van statelijke actoren. Het feit dat staten eerst niet en nu wel beschikken over capaciteiten in de digitale ruimte kan ertoe leiden dat ze zich anders gaan gedragen. Het biedt hen immers mogelijkheden die ze eerst niet hadden, zoals het volgen van in het buitenland verblijvende dissidenten of digitale aanvallen op andere staten waarmee ze een conflict hebben. Het is voorstelbaar dat het groeiende beschikbare instrumentarium ook leidt tot een heroverweging van de eigen geopolitieke macht.

Middelen en doelwitten

Statelijke actoren beschikken over een breed palet aan middelen om hun doelstellingen te verwezenlijken, waarbij iedere actor een eigen specifiek doel en werkwijze heeft. Sommige van die middelen zijn niet per definitie illegaal of zelfs ongewenst. En niet alle statelijke actoren beschikken over dezelfde capaciteiten.

Middelen ingezet door statelijke actoren: zeven categorieën [VIII]

1. Beïnvloeding en inmenging (inclusief desinformatie). Het gaat hier bijvoorbeeld om hack&leak acties; het heimelijk beïnvloeden van personen, democratische processen, politieke besluitvorming; het toepassen van dwang (zoals bedreiging, chantage, afpersing of fysiek geweld) tegen personen; het beïnvloeden en censureren van wetenschappelijk onderzoek.
2. Spionage, zowel digitaal als fysiek, inclusief economische spionage.
3. (Digitale) voorbereidingshandelingen op en daadwerkelijke verstoring en sabotage.
4. Militaire activiteiten, zoals intimidatie en machtsvertoon via wapenwedloop, grootschalige oefeningen, militaire interventies in derde landen, inzet van onherkenbare troepen.
5. Inzet van economische instrumenten, zoals overnames en investeringen, maar ook het uitbuiten van strategische afhankelijkheden als economisch drukmiddel.
6. Diplomatieke en internationaal-politieke activiteiten, bijvoorbeeld het gebruik van hindermacht in internationale gremia om onwelgevallige besluiten tegen te houden.
7. Juridische activiteiten en/of lawfare, waarbij (inter)nationaal recht en rechtssystemen worden gebruikt om een zo groot mogelijk eigen voordeel te behalen ook als dat zeer tegen de geest van het recht ingaat.

De eerste drie categorieën lenen zich bij uitstek voor de inzet van digitale middelen. Beïnvloeding en inmenging speelt zich voor een belangrijk deel in het informatiedomein af. En dat informatiedomein is gedigitaliseerd, denk aan online platforms en sociale media. Dit vergemakkelijkt de inzet van beïnvloedingsmiddelen als het maken en/of verspreiden van desinformatie, het voeren van mediacampagnes, het verspreiden van informatie om te beschadigen of mensen lastig te vallen, of hack and leak-acties. Dat de inzet van digitale middelen voor spionage en (de voorbereiding op) sabotage zeer geschikt en aantrekkelijk is, behoeft inmiddels geen betoog meer. De AIVD concludeert in haar Jaarverslag 2020 dat spionage de Nederlandse economische veiligheid bedreigt.[179]

Een statelijke actor kan zijn middelen inzetten tegen een breed scala aan mogelijke doelwitten: van lokale verenigingen tot internationale veiligheidsorganisaties en van één individu tot hele gemeenschappen.

VIII De volgorde in dit kader impliceert geen rangorde van de verschillende middelen.

IX Een uitgebreider beschrijving van doelwitten en hoe zij geraakt worden is te vinden in het 'Dreigingsbeeld Statelijke Actoren' dat AIVD, MIVD en NCTV in februari 2021 publiceerden. De volgorde in dit kader impliceert geen rangorde van de verschillende doelwitten.

Doelwitten van statelijke actoren: vijftien categorieën [IX]

1. Diaspora, dat wil zeggen bevolkingsgroepen die van oorsprong uit een ander land komen en door het herkomstland nog worden gezien en behandeld als onderdanen.
2. Geloofsgemeenschappen.
3. Groepen en/of personen vatbaar voor polariserende boodschappen, zoals groepen bij wie sterke anti-sentimenten (bijvoorbeeld tegen de Nederlandse overheid) leven.
4. Gelegenheidsdoelwitten: personen die zich (on)bewust voor het karretje laten spannen.
5. High potentials: personen met potentie om op kennis- of invloedrijke posities terecht te komen.
6. Instituties en functionarissen van onze democratische rechtsstaat, op nationaal en lokaal niveau.
7. Democratische processen, zoals verkiezingen en referenda.
8. Adviesorganen, die door onderzoek en advisering een rol hebben bij politieke besluitvorming.
9. Onderwijsinstellingen.
10. Wetenschap, kennisinstellingen en denktanks.
11. Het maatschappelijk middenveld, uiteenlopend van media tot sportverenigingen.
12. In Nederland gevestigde internationale organisaties.
13. Het bedrijfsleven (en topsectoren).
14. Vitale infrastructuur (plus toeleveranciers).
15. Voor Nederland cruciale internationale verbanden, zoals EU, NAVO en VN.

Een in het oog springend doelwittype is de vitale infrastructuur, waar vitale processen, diensten, toeleveranciers en de Rijksoverheid onder worden verstaan.[X] Wat opvalt is dat vooral tegen dit type doelwit digitale sabotage (inclusief voorbereidingshandelingen) wordt ingezet.[180] Het is belangrijk hierbij aan te tekenen dat hiervan vooralsnog geen manifestaties zijn gezien in Nederland, maar wel in andere westerse en zelfs Europese landen. Er is met name sprake van een toenemende interesse om kwetsbare schakels in de ketens van toeleveranciers te misbruiken. De verregaande digitalisering en beperkte aanwezigheid van terugvalopties verhogen de kwetsbaarheid.

X De definitie van vitale infrastructuur is in ontwikkeling. De hier gebruikte omschrijving van dit doelwittype is gebaseerd op de definitie zoals die ultimo 2019 gehanteerd werd en is opgenomen in het Dreigingsbeeld Statelijke Actoren (DBSA) van AIVD, MIVD en NCTV. Het doelwittype vitale infrastructuur is hierbij aangevuld met toeleveranciers, omdat al enige jaren wordt geconstateerd (onder andere in het CSBN) dat toeleveranciers worden gebruikt als springplank naar doelwitten binnen de vitale infrastructuur. Er is sprake van toenemende interesse om kwetsbare schakels in leveranciersketens te misbruiken.

Bestuurders eindverantwoordelijk voor adequate omgang met digitale risico's

7 Risicomanagement instrumenteel voor verhogen weerbaarheid

In voorgaande CSBN's is veel gesproken over achterblijvende weerbaarheid. Daarbij dient weerbaarheid gezien te worden als het vermogen om relevante digitale risico's tot een aanvaardbaar niveau te reduceren. Kijkend naar de incidenten die Nederland geraakt hebben, blijft ook dit jaar de weerbaarheid achter bij de groeiende belangen en de verschuivende dreiging. Experts signaleren daarnaast grote verschillen in weerbaarheid tussen en binnen sectoren en ketens. Organisaties die er beter voor lijken te staan, hebben zich naast het nemen van basismaatregelen ook gericht op een risicogebaseerde manier van werken. Zij kunnen inzichten bieden in het weerbaarder maken van Nederland in den brede. Zo blijkt dat naast basismaatregelen aandacht voor risico's essentieel is. Hiervoor is een aantal breed toepasbare basisprincipes beschikbaar die ook door kleinere organisaties toegepast kunnen worden. Het is uiteindelijk aan bestuurders, zowel in het bedrijfsleven, de Rijksoverheid, als in de politiek, om te sturen op de beheersing van risico's.

Risico's behoeven continu aandacht

Zowel de belangen van organisaties als die van aanvallers zijn onderhevig aan verandering. Dat maakt dat een duidelijk beeld van het verschuivende dreigingslandschap en doorlopende aandacht voor risico's essentieel is. Weerbaarheid is immers het vermogen om relevante digitale risico's tot een aanvaardbaar niveau te reduceren. Een brede blik op risico's is van belang om te kunnen zeggen dat organisaties, ketens en staten een voldoende niveau van weerbaarheid hebben. Deze brede blik kan worden bereikt middels risicomanagement.

Een baseline is niet genoeg

Gezien de toenemende complexiteit en digitalisering van processen, de onderlinge verwevenheid van organisaties en sectoren, evenals een groeiende dreiging, is het nemen van basismaatregelen belangrijk, maar niet afdoende.

Basismaatregelen, waaronder de maatregelen genoemd in het product 'Handreiking Cybersecuritymaatregelen' van het NCSC, zorgen voor een minimum niveau van digitale veiligheid (oftewel security hygiëne). Daarnaast is scherper geschut nodig om te anticiperen op geavanceerde aanvallers en complexere problemen.[181] Organisaties en sectoren die weerbaarder lijken dan hun tegenhangers investeren niet alleen in basismaatregelen, maar kijken met een kritische blik naar de grootste risico's. Securityspecialisten, toezichthouders en wetgevers benadrukken dan ook het belang van risicomanagement als hét instrument voor het daadwerkelijk verhogen van de weerbaarheid in de praktijk.[182] Helaas zien veel organisaties risicomanagement nog als een langdurig en kostbaar traject, en niet als iets om periodiek op te pakken.

Het gaat om meer dan alleen risicoanalyse

In de afgelopen jaren lijkt het bewustzijn van de normen voor risicomanagement toegenomen. Ook is de vertaling van deze algemene kaders naar sectorspecifieke invullingen doorontwikkeld. Daarbij gaat het niet alleen om het identificeren van relevante risico's. Risicoanalyse is namelijk een onderdeel van risicomanagement in den brede, waar zowel het voorkomen van problemen alsook het genezen een rol speelt. Een aantal belangrijke activiteiten voor het beheersen van risico's zijn identificatie van relevante risico's, preventie middels het nemen van maatregelen, detectie van afgeslagen en geslaagde aanvallen, mitigatie van de impact van een succesvolle aanval, en reparatie om een proces weer volledig operationeel te laten zijn.[183] Daarbij speelt communicatie met stakeholders, waaronder terugkoppeling naar de directie, een belangrijke rol in de evaluatie van de effectiviteit van het proces.[184] Naast eerdergenoemde activiteiten komen overkoepelende aspecten steeds duidelijker terug in een bredere blik op risicomanagement. Regulering vanuit de markt en de overheid – zoals verzekering, certificering en aansprakelijkheidstelling – speelt een steeds belangrijker rol. Dit geldt ook voor governance, realistisch testen, situationele beeldvorming, en het leren van fouten.[185] Deze verschillende facetten van risicomanagement dienen elkaar te versterken: risicomanagement is een doorlopend proces met als doel ervoor te zorgen dat risico's scherp en eenduidig in beeld zijn en daadwerkelijk worden gereduceerd.

'Voorkomen én genezen' als adagium

In een gebalanceerde aanpak van digitale risico's gaat het niet alleen om het reageren op incidenten of om het uitrollen van maatregelen om aanvallen tegen te houden. In plaats daarvan zal er genuanceerd naar het probleem gekeken moeten worden. Er dient geaccepteerd te worden dat waterdichte beveiliging niet bestaat, en dat er altijd succesvolle aanvallen zullen zijn.[186] Dat betekent niet dat digitale dijkverzwaring geen nut heeft. Zulke activiteiten kunnen er wel degelijk voor zorgen dat aanvallen gepareerd worden en dat geslaagde aanvallen minder impact hebben. Door aanvallers in een vroeg stadium te detecteren en hier snel op te reageren kan de schade worden beperkt.[187] Aan de andere kant van het spectrum kan ook de 'security by design' en 'privacy by design' mentaliteit worden ingezet.[188] Hoe eerder securityvraagstukken worden meegenomen in het ontwikkeltraject van een proces, systeem of dienst, des te goedkoper en/of des te meer impact de genomen maatregelen normaliter hebben.[189] De uitdaging is om in dit speelveld een goede balans te vinden zodat risico's geadresseerd kunnen worden tegen een acceptabele prijs, zowel in termen van geld als in termen van afwegingen van andere belangen zoals vrijheid, toegankelijkheid en vooruitgang. Het 'usable security' vakgebied laat zien dat belangen elkaar niet hoeven uit te sluiten.[190] Als knelpunten bijtijds worden geïdentificeerd in samenspraak met eindgebruikers, dan is de kans groot dat er een passende afweging kan worden gemaakt.[191]

Basisprincipes kunnen breed worden toegepast

Hoewel het optuigen van een uitgebreid risicomanagement-systeem bij een grote organisatie meerdere jaren kan duren, zijn de onderliggende principes ook relevant voor kleinere organisaties. Risicomanagement is namelijk op veel verschillende manieren in te vullen. Het is vooral een kwestie van kijken wat werkt in de gegeven context. Elke organisatie is dan ook vrij om, in lijn met bestaande verplichtingen, een eigen aanpak voor risicomanagement vorm te geven.[192] Daarbij kunnen de onderstaande fundamentele principes van pas komen.[193]

Weerbaarheid is een teamprestatie

Traditioneel gezien wordt het management van technologie-gerelateerde risico's belegd binnen de ICT-afdeling. Dat maakt de kloof tussen technisch experts en de business groter. In plaats daarvan kan risicomanagement gezien worden als een teamaangelegenheid. Management van digitale risico's dient te gebeuren in samenspraak met de business, waarbij partijen aan horen te sluiten zoals business continuity managers, risicomanagers, proceseigenaren en domeinexperts. Voorbeelden van waar dit niet is gebeurd, laten zien dat basale problemen anders tussen wal en schip kunnen vallen. Verder is, naast het belang van een goede samenwerking tussen disciplines, een samenwerking tussen de verschillende lagen van een organisatie essentieel. De verkenning en aanpak van strategische, tactische en operationele risico's dient namelijk goed op elkaar afgestemd te zijn.[194]

Scenario's zetten aan tot nadenken

Vaak blijven risico's abstract. Om die reden kan het nuttig zijn om ze te vertalen naar scenario's. Voorbeelden van dergelijke scenario's zijn opgenomen in hoofdstuk 8 'Dreigingsscenario's'.[195] Zo'n scenario-gedreven manier van werken maakt dingen tastbaar, en het maakt het makkelijker om bruggen te slaan tussen verschillende disciplines. Een workshop om mensen kennis te laten maken met scenario's zou kunnen beginnen met alledaagse voorbeelden, zoals manieren waarop er ingebroken kan worden in een huis. Op basis van deze relatief eenvoudige scenario's kunnen complexere voorbeelden gegeven worden, zoals scenario's waarin cybercriminaliteit voorkomt. Bij een volgende stap zouden zelfs de perspectieven van verschillende disciplines eraan toegevoegd kunnen worden. Behalve dat deze scenario's ingezet kunnen worden voor het identificeren van risico's, kunnen ze ook gebruikt worden gedurende de overige stadia van de risicomanagement cyclus. Ze kunnen bijvoorbeeld gebruikt worden bij audits van processen, het testen van systemen en bij het oefenen van incident response.

Geld en uptime zijn universele maatstaven

Om verschillende scenario's met elkaar te kunnen vergelijken, is het belangrijk om afspraken te maken over een gezamenlijke interpretatie van het begrip risico en om dezelfde indicatoren te gebruiken voor meerdere risicoanalyses.[196] Hierdoor kunnen risico's vergeleken worden op een onderbouwde manier. Een voorbeeld van een set indicatoren die redelijk universeel is, is geld (oftewel financiële impact) en continuïteit (oftewel beschikbaarheid). Door ook bij andere typen risico's deze indicatoren te hanteren kunnen digitale risico's op dezelfde voet staan als bijvoorbeeld operationele risico's. Op deze manier kunnen de kroonjuwelen van een organisatie worden geïdentificeerd door te kijken naar wat de meeste impact heeft op de inkomsten en de continuïteit van de bedrijfsvoering. Deze kroonjuwelen kunnen dan extra aandacht krijgen, en het securitybudget kan slim worden ingezet. Zo worden die onderdelen van een organisatie weerbaarder gemaakt die het ook daadwerkelijk nodig hebben. Helaas zijn er echter ook organisaties die risicoanalyses uitvoeren die te wensen over laten: risico's zijn daarbij vaak vaag en wollig omschreven, waardoor deze onvoldoende geduid kunnen worden. Dit maakt het lastiger om de effectiviteit van maatregelen af te wegen voor het beschermen van de uitvoering van de kerntaken van een land of organisatie. Security wordt dan al snel gezien als kostenpost in plaats van als een integraal onderdeel van de bedrijfsvoering.

Testen legt problemen bloot

Een valkuil met betrekking tot risicomanagement en cybersecurity is om alles perfect geregeld te hebben op papier, maar serieuze steken te laten vallen in de praktijk. Het is daarom belangrijk om processen en systemen daadwerkelijk te testen zoals deze op de werkvloer en in het veld draaien. Deze testen kunnen worden gebaseerd op de scenario's die eerder geïdentificeerd zijn. Daarbij dienen ook tussentijdse verschuivingen in het dreigingsbeeld en de te beschermen belangen niet vergeten te worden. Testen kan op veel verschillende manieren, van een simpele tabletop oefening tot een uitgebreide threat-based red teaming oefening.[197] Bij de keuze van de scope en het type test is het van belang om dit ook risicogestuurd aan te pakken.[198] In algemenere zin dient het testplan aan te sluiten op de bredere risicomanagement cyclus. De effectiviteit van maatregelen behoeft daarbij speciale aandacht. Door te monitoren of maatregelen het beoogde effect hebben kan gekeken worden of de kosten opwegen tegen de baten. Naast de ervaringen van experts kunnen ook inzichten uit (academisch) onderzoek meegewogen worden.

Er kan van en met elkaar geleerd worden

Risico's manifesteren zich op een andere wijze bij verschillende organisaties. Deels hangt dit samen met de verschillen in weerbaarheid, maar grotendeels is dit ook een eigenschap van de risico's zelf. Een risico zal normaliter niet in alle gevallen tot uiting komen.[199] Dit kan het zicht op relevante risico's en op de effectiviteit van maatregelen bemoeilijken. Om hiermee om te gaan is het verstandig om met andere organisaties in gesprek te gaan. Kennis en ervaring kan uitgewisseld worden in het kader van ISAC's, met de ketenpartners van een kritiek proces, en in andere samenwerkingsverbanden.[200] Binnen een besloten overleg kunnen organisaties bijvoorbeeld verhalen delen over incidenten die zich bij hen hebben voorgedaan. Ook de uitwisseling en zelfs het vaststellen van standaarden behoren tot de mogelijkheden. Naast kennisuitwisseling kunnen in het kader van samenwerking ook gezamenlijke oefeningen uitgevoerd worden om de responscapaciteit te toetsen en te verbeteren. Dit helpt om elkaar snel te kunnen vinden en goed op elkaar in te spelen als de nood hoog is en er geen tijd is voor uitgebreid overleg. Bij dit alles is het achterliggend idee om op het vlak van security niet te concurreren, maar juist samen te werken.

Bestuurders zijn aan zet

Risicomanagement zonder buy-in van bestuurders zal hoogstwaarschijnlijk mislukken: CISO's die beveiliging op eigen houtje proberen te regelen komen er vroeg of laat achter dat de organisatie zich geen eigenaar voelt van het probleem.[201] Het is essentieel dat bestuurders nauw betrokken zijn bij risicomanagement. Ze zijn verantwoordelijk voor het identificeren van de strategische belangen binnen een organisatie en voor (het mandateren van) acceptatie van restrisico's. Hiervoor moeten de juiste gremia zijn ingesteld en passende verantwoordelijkheden zijn belegd. Lijnmanagers, oftewel de eigenaren van digitale processen, kunnen daarbij dagelijkse verantwoordelijkheid dragen voor de tactische en operationele risico's. Daarnaast dienen bestuurders zelf op de hoogte te blijven van de belangrijkste risico's. Dit alles geldt ook voor politieke bestuurders, die digitale risico's voor de nationale veiligheid in het oog dienen te hebben en houden, om zo op een onderbouwde manier afwegingen te kunnen maken tussen diverse en uiteenlopende belangen.

Zicht en sturing op risico's is noodzakelijk

Bestuurders zijn eindverantwoordelijk voor een adequate omgang met digitale risico's. Zowel strategische als tactische en operationele risico's kunnen middels gerichte sturing en zicht op voortgang worden geborgd. Hiervoor dienen heldere rapportagelijnen opgezet te worden. CISO's dienen rechtstreeks aan het bestuur te rapporteren en onafhankelijke interne en externe audits zijn ook van belang. Natuurlijk spelen de raad van toezicht evenals de toezichthouders hierbij een belangrijke rol. Zij hebben de verantwoordelijkheid om te kijken of bestuurders en lijnmanagers een adequaat beeld hebben van relevante risico's en of ze hier gepast op acteren. Dit vraagt van controlerende organen een scherpe blik op pertinente belangen, dreigingen en maatregelen. Inzicht in de informatie die binnen digitale processen wordt verwerkt is daarbij een cruciale factor. Organisaties hebben zelf niet altijd zicht op hun eigen weerbaarheid, waarbij de afwezigheid van een organisatiestructuur die grip houdt op informatie ook een rol speelt. De tactische laag kan, naast de dagelijkse verantwoordelijkheid voor geld en

personeel, ook verantwoordelijkheid dragen voor de informatie die binnen de eigen afdeling thuishoort (en de risico's die daaraan verbonden zijn). Binnen de tactische laag kunnen informatie-eigenaren aangewezen worden, die verantwoordelijkheid dragen, hiervoor de middelen krijgen, en die door bestuurders afgerekend worden op de invulling van deze verantwoordelijkheid.

Investeren in mensen vormt het fundament

Risicomanagement is een specialisme. Daarom kan van bestuurders – en van mensen die de dagelijkse verantwoordelijkheid dragen voor digitale processen en de bijbehorende risico's – niet worden verwacht dat ze expert zijn op dit gebied. In plaats daarvan dienen ze ervoor te zorgen dat ze de goede mensen op de goede plaats hebben gezet door te investeren in nieuwe aanwas en in de training van huidig personeel. Daarvoor is een gestructureerd personeelsbeleid nodig, evenals een trainingsprogramma dat is verankerd in de organisatie. Naast de experts op het gebied van cybersecurity risicomanagement moet ook de rest van de organisatie een minimale kennisbasis hebben om goed met elkaar in gesprek te kunnen gaan over belangrijke risico's voor de organisatie en hoe hiermee om te gaan. Daarbij gaat het voornamelijk over het hoe en waarom van de principes achter risicomanagement (bijvoorbeeld middels een workshop gebouwd rond organisatie-specifieke scenario's). Bij het aanstellen en trainen van mensen dient een balans gevonden te worden tussen de verschillende facetten van risicomanagement (zie de sectie 'Het gaat om meer dan alleen risicoanalyse').

Ook de overheid heeft een rol

Wat geldt voor de bestuurders van organisaties, geldt ook voor de bestuurders van landen.[202] Om digitale risico's het hoofd te bieden, is het belangrijk dat deze op een systematische manier geïdentificeerd en aangepakt worden.[203] Op nationaal niveau gaat het onder andere om structurele problemen zoals de groeiende afhankelijkheid van buitenlandse software en hardware producenten en dienstverleners.[204] Ook problemen zoals de afnemende diversiteit in technologische oplossingen en toeleveranciers kunnen een systeemrisico vormen. Verder heeft de overheid een rol in het aanpakken van marktfalen en andere 'collective action problems', waaronder de problematiek rondom risicomanagement in ketens van partijen die niet dezelfde belangen nastreven en waar transparantie ontbreekt.[205] Zo laat de beveiliging van onder andere veel Internet-of-Things apparatuur al een langere tijd te wensen over.[206] De noodzaak van regulering wordt dan ook steeds breder onderkend, maar een dynamische en complexe omgeving maakt het lastig om de nationale weerbaarheid te meten en de effectiviteit van maatregelen te voorspellen.[207]

Risico's vanwege grootschalige toename clouddiensten

8 Dreigingsscenario's

In de voorgaande hoofdstukken werd aandacht besteed aan digitale dreigingen, 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 scenariodelen rond uitval en misbruik van de cloud. Er is voor dit specifieke thema gekozen vanwege het belang van de cloud binnen de digitale ruimte. Er is sprake van een grootschalige toename van het gebruik van clouddienstverlening, hetgeen gepaard gaat met risico's. U kunt deze scenario's gebruiken om binnen uw organisatie na te gaan of gebeurtenissen zoals die worden beschreven in het scenario zich bij u zouden kunnen voordoen, welke voorbereidingen u hebt getroffen en hoe u uw cloudstrategie kunt verbeteren. Het scenario is in opdracht van de NCTV door TNO opgesteld.

Scenario Wolkbreuk

Dit scenario kent drie scenariodelen die elkaar opvolgen, maar ook afzonderlijk gelezen kunnen worden.

Scenariodeel a: de cloud komt weer snel in de lucht

Beschrijving gebeurtenissen

Extreem weer zorgt voor grote problemen in Nederland. Op verschillende locaties ontstaat hevige wateroverlast die gepaard gaat met uitval van elektriciteit. Als gevolg hiervan heeft Nubes Link-Exchange (NLeX)[XI], een grote cloud exchange provider, te kampen met een flinke verstoring van haar verbinding naar één van de Nederlandse datacentra van Cirrocumulus Networks[XII], een grote cloud service provider (CSP). NLeX levert directe, besloten verbindingen tussen klanten (overheden en bedrijven) en het cloudnetwerk van Cirrocumulus Networks, zonder tussenkomst van een Internet Service Provider (ISP). Door de storing bij NLeX valt voor alle klanten in de betreffende regio deze directe verbinding met hun Cirrocumulus Networks cloudomgeving uit.

Een deel van de getroffen organisaties is voorbereid op een dergelijke, tijdelijke, onbeschikbaarheid en heeft hiervoor extra (fallback) connectiviteitsvoorzieningen getroffen zoals vastgelegd in hun contract met NLeX en Cirrocumulus Networks. Dit deel van de getroffen organisaties wordt via NLeX overgeschakeld van de directe verbinding met Cirrocumulus Networks naar een verbinding via het (publieke) internet, geleverd door een Internet Service Provider (ISP). Voor deze organisaties is er nauwelijks sprake van verstoring. Het andere deel van de getroffen organisaties heeft geen extra (fallback) voorzieningen afgenomen en verliest tijdelijk de verbinding met hun cloudomgeving zoals geleverd door Cirrocumulus Networks. Na adequaat optreden van NLeX kan hun dienstverlening na ongeveer twee uur weer hervat worden.

De impact van de tijdelijke uitval varieert per getroffen organisatie, omdat dit afhangt van de inrichting van hun infrastructuur (variaties in het gebruik van publieke, (virtuele) private, hybride cloud- en on premise oplossingen). Organisaties met veel on premise infrastructuur hebben minder last van de uitval dan de organisaties waarvan veel diensten in de cloudomgeving zijn ondergebracht.

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

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

Duiding

Steeds meer partijen hebben in de afgelopen jaren gekozen voor een directe verbinding naar de cloudomgeving die niet via het publieke internet gaat, maar hen zo direct mogelijk (met zo min mogelijk partijen er tussen) met de cloud verbindt.[208] Redenen om hiervoor te kiezen zijn snelheid (minder delay), vertrouwelijkheid en betrouwbaarheid (minder schakels). Voorbeelden uit de praktijk zijn cloud connectiviteitsdiensten Direct Connect (AWS) en Express Route (Microsoft). In alle gevallen is het bij het afnemen van clouddienstverlening van belang na te denken over hoe afhankelijk je als organisatie wilt zijn van een clouddienstverlener en wat de risico's en voordelen zijn voor je organisatieprocessen. Dit zijn belangrijke afwegingen voor het bepalen van een eigen cloudstrategie. Organisaties die veel werken met gevoelige informatie kiezen er vaak voor om die gegevens alleen in een afgeschermde (private) omgeving te verwerken. Dit kan een private cloudomgeving bij een CSP zijn of een eigen 'on premise' infrastructuur. Sommige organisaties kiezen ervoor om gedeeltelijk gebruik te maken van een publieke clouddienst en gedeeltelijk een private oplossing (cloud of on premise) te kiezen. Bij zulke hybride cloud oplossingen kan gevoelige informatie goed afgeschermd worden, maar kan voor minder gevoelige processen gebruik gemaakt worden van de schaalvoordelen van een publieke cloudinfrastructuur. In de praktijk worden vele combinaties en configuraties toegepast. Extra maatregelen verhogen de veiligheid of beschikbaarheid, maar kennen een prijskaartje en vergen specifieke expertise. Het is belangrijk om als organisatie hierin een bewuste afweging te maken. Voor een veilige inkoop van clouddiensten heeft het NCSC in 2020 een factsheet uitgebracht.[209]

Sleutelbegrippen

Cloud exchange provider: zorgt voor on-demand (directe) verbindingen met cloud service providers, waarbij het digitale verkeer niet per se via het internet wordt geleid. Ze zijn daarmee een tussenpartij die veel klanten direct, zonder tussenkomst van een ISP, verbindt met cloud service providers.[210]
Cloud service, ook wel cloudcomputerdienst: digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit.[211]
Cloud service provider (CSP): levert on-demand diensten aan klanten in de vorm van een platform, infrastructuur, computer rekencapaciteit, opslag of een specifieke dienstverlening, zonder direct actief beheer van een klant of gebruiker.[212]
Internet service provider: levert faciliteiten aan organisaties om verbinding te krijgen met het Internet, al dan niet in combinatie met internetdiensten. Internetverbindingen worden typisch niet on-demand gerealiseerd en geïnstalleerd voor langdurig gebruik.[213]
Publieke cloud: hierin delen klanten de infrastructuur die beschikbaar is voor verhuur met andere klanten. Een CSP beheert deze infrastructuur en kan klanten tegen betaling de benodigde resources verlenen.[214]
Private cloud: hierin is de infrastructuur exclusief voor een enkele klant, waarbij de fysieke locatie van de resources ofwel op het terrein van de klant is (on premise) ofwel op locatie van een CSP, maar gescheiden van andere klanten. Een organisatie kan zijn eigen private cloudomgeving opzetten, of een contract afsluiten met een CSP om dit voor hen te doen. [215]
Hybride cloudomgeving: hierin wordt een publieke clouddienst, geleverd door een CSP, gecombineerd met ofwel een private cloudomgeving of private (eigen of gehuurde) capaciteit in een datacentrum, waarbij deze twee omgevingen gescheiden zijn, maar wel met elkaar kunnen communiceren en data en applicaties met elkaar kunnen delen. Hiervoor wordt soms gekozen, omdat organisaties over gevoelige data willen beschikken, waarvan zij het te risicovol achten om deze in een publieke cloudomgeving op te slaan. Tegelijkertijd willen ze wel gebruik maken van de rekenkracht van de publieke cloud voor het draaien van applicaties.[216]

Kernvragen voor de lezer

1. Bent u bekend met de cloudstrategie van uw organisatie en de afwegingen die daarin gemaakt zijn?
2. Is er een bewuste afweging geweest welke clouddienst ter ondersteuning van welke organisatieprocessen is ingezet?
3. Bent u er bekend mee hoe de connectiviteit naar de clouddienst gerealiseerd is en is daarbij een bewuste keuze gemaakt uit de mogelijke cloud connectiviteitopties?
4. Heeft u een duidelijk beeld wat de impact is op uw organisatieprocessen indien de clouddienstverlening of de connectiviteit er naartoe uitvalt?
5. Welke alternatieven of mitigerende maatregelen heeft u voorhanden indien de clouddienstverlening tijdelijk niet beschikbaar is?

Scenariodeel b: er is geen lucht zonder wolken[217]

Beschrijving gebeurtenissen

Een aantal weken nadat extreem weer een tijdelijke verstoring van de cloud exchange provider NLeX veroorzaakte, signaleert de CSP Cirrocumulus Networks een verdachte peering connectie bij een van haar klanten. De ontdekking wordt gedaan op basis van de Monitoring & Detectie (M&D) dienstverlening die door deze klant ook van de CSP is afgenomen (en die sterk is in detectie van afwijkingen). Het lijkt er op dat gegevens vanuit de cloudomgeving van de klant worden weggesluisd naar een onbekende locatie buiten het (virtuele) netwerk van de klant. Nader onderzoek wijst uit dat er inderdaad sprake is van een onrechtmatige connectie. Omdat een dergelijke peering connectie alleen opgezet kan worden met de juiste credentials wordt verder onderzoek ingesteld. Een actor heeft blijkbaar toegang tot de cloudomgeving van de klant verkregen en is in staat geweest om valse credentials te genereren en daarmee een verbinding op te zetten. Dit wordt in eerste instantie afgehandeld als een incident gericht op deze klant.

Omdat vermoed wordt dat in de buitgemaakte gegevens van de klant er ook sprake is van persoonsgevoelige data wordt dit gemeld bij de Autoriteit Persoonsgegevens (AP).

Een week later komt een vergelijkbaar geval in beeld via dezelfde M&D dienstverlening voor een andere klant uit dezelfde Nederlandse regio. Cirrocumulus Networks stelt op basis van dit incident verder onderzoek in en monitort uit voorzorg ook connecties van hun andere klanten in deze regio. Hieruit blijkt dat het probleem bij meer klanten speelt. Wel wordt duidelijk dat de problemen zich beperken tot klanten in deze regio. Na enkele dagen verschijnt er in de media berichtgeving hierover, waarin er uiteenlopende speculaties worden gedaan over het motief van de kwaadwillende actor en de veroorzaakte schade. De media-berichten benoemen enkele bedrijven die getroffen zijn en die reeds op de hoogte zijn gesteld door Cirrocumulus Networks. De cloud service provider heeft technische dreigingsinfomatie (IoCs) gedeeld met hun klanten, het CSIRT-DSP en het Agentschap Telecom. Het CSIRT-DSP heeft de dreigingsinformatie samen het NCSC verder gedeeld met vertrouwde schakelorganisaties Objectief Kenbaar Tot Taak (OKTTs) en biedt handelingsperspectief voor detectie van mogelijke afwijkingen in hun netwerkomgeving.

Er wordt nader (forensisch) onderzoek gedaan door Cirrocumulus Networks en een door een getroffen klant ingehuurd forensisch onderzoeksbedrijf. Dat wijst uit dat de inbraak terug is te leiden naar het tijdelijk herrouteren van de directe verbinding door NLeX enkele weken eerder toen een storm een storing veroorzaakte waardoor de dienstverlening van NLeX tijdelijk niet beschikbaar was. Bij het tijdelijk overzetten door NLeX van de directe peering connectie van een aantal klanten van Cirrocumulus Networks naar een verbinding via het Internet is in de onoverzichtelijke, tijd-sensitieve situatie een (menselijke) fout gemaakt waardoor een kwetsbaarheid is ontstaan. Van deze kwetsbaarheid is door een kwaadwillende actor slinks gebruik gemaakt, want de aangetroffen malware in een klantomgeving lijkt sinds het moment van de extreem-weer situatie geïnstalleerd te zijn. Omdat mogelijk meer klanten hierdoor geraakt kunnen zijn, bericht de Cirrocumulus Networks uit voorzorg al haar klanten in de betreffende regio.

Het blijkt inderdaad dat er bij meerdere, maar niet alle, klanten van Cirrocumulus Networks die tijdens de storm tijdelijk door NLeX zijn overgezet van een directe verbinding naar een verbinding via het internet verdachte activiteiten hebben plaatsgevonden. Er heerst nog veel onduidelijkheid over de omvang van de data die precies is buitgemaakt, maar wel is duidelijk dat het voor enkele klanten naast persoonsgevoelige (klant)informatie ook om bedrijfsgevoelige informatie en gevoelige informatie van enkele overheidsdiensten gaat. Deze informatie is extra olie op het vuur in de (sociale) media. Uiteenlopende speculaties van cybersecurityexperts zorgen voor onduidelijkheid over welke organisaties getroffen zijn, welke niet en wat de consequenties zijn van de aaneenschakeling van incidenten. Tevens worden Kamervragen gesteld zoals of Nederland niet te afhankelijk van clouddienstverlening is geworden en of de klanten die gebruik maken van de diensten van de CSP, de cloud exchange of de CSP zélf verantwoordelijk zijn voor de geleden schade.

Duiding

Veel organisaties beschouwen het verplaatsen van activiteiten naar een publieke of hybride cloudomgeving als een manier om de bescherming tegen cyberaanvallen te vergroten. Voor clouddienstverleners is het van groot belang om de veiligheid van hun dienstverlening te waarborgen en daarom hebben ze veel expertise en capaciteit op het gebied van cybersecurity.[218] Dit betekent echter niet dat cloudomgevingen onfeilbaar zijn. Er kunnen fouten gemaakt worden en kwaadwillende actoren liggen overal op de loer om kwetsbaarheden te misbruiken.

Incidenten zoals Solarwinds[219] hebben laten zien dat organisaties kwetsbaar kunnen zijn als ze afhankelijk zijn van een steeds complexer wordend netwerk van toeleveranciers van softwareproducten of van uitbestede ICT-diensten. Organisaties hebben niet altijd goed zicht op alle partijen die onderdeel zijn van dit netwerk, waardoor controle lastig is. Een aanval op een onderdeel in de keten van ICT-dienstverlening kan daarmee indirect impact veroorzaken op een organisatie (leveranciersketenaanval, zie ook het dreigingsscenario van het CSBN 2020)[220].

Sleutelbegrip

(Private) peering connectie: een methode die routering van verkeer tussen apparaten in twee verschillende netwerken mogelijk maakt zonder gebruik te hoeven maken van een derde partij (ISP) om het verkeer te routeren.[221] Grote organisaties gebruiken private peering connecties bijvoorbeeld om gegevens tussen verschillende locaties van hun organisatie uit te wisselen. Voor communicatie naar andere organisaties maken organisaties gebruik van een public peering connectie, meestal via een ISP die vervolgens weer peering connecties heeft met andere ISPs. Peering connecties tussen ISPs worden vaak gerealiseerd in een internet exchange. De aaneenschakeling van alle peering connecties vormt het Internet.

Kernvragen voor de lezer

1. Heeft u zelf monitoring en detectiecapaciteit beschikbaar of ingekocht als dienst? Bent u bekend wat precies gemonitord wordt en welk type dreigingen hiermee wel en niet mee worden gedetecteerd?
2. Hoe zijn de verantwoordelijkheden belegd tussen u als afnemer en de cloud service provider in het geval zich toch een incident voordoet? Wat zijn hierin de eigen en gezamenlijke verantwoordelijkheden? En zijn deze onderling voldoende afgestemd?
3. Bent u bekend met of gebruikt u een *assume breach* strategie? In andere woorden: indien uitgegaan wordt dat uw organisatie een keer te maken krijgt met een cybersecurity incident, wat is dan uw handelingsperspectief?

Scenariodeel c: operatie stofwolk leidt tot verschroeide aarde

Beschrijving gebeurtenissen

Een grote groep Nederlandse klanten van CSP Cirrocumulus Networks heeft plotseling geen toegang tot hun cloudomgeving. Berichten in de media wijzen direct op een grootschalige storing in de infrastructuur van Cirrocumulus Networks, waarbij de mogelijkheid dat het om een aanval gaat niet wordt uitgesloten. Opvallend is dat dit gebeurt in een periode waarin al eerder berichten naar buiten zijn gekomen over verdachte activiteiten in de cloudomgeving van meerdere klanten van Cirrocumulus Networks. Een woordvoerder van Cirrocumulus Networks geeft aan dat er inderdaad sprake is van een verstoorde dienstverlening door problemen in een van haar datacentra en dat zij bezig zijn met het zoeken naar de oorzaak en oplossing. Ondertussen groeit de onrust onder klanten van Cirrocumulus Networks, gevoed door berichten in de media. Zijn hun systemen en data nog wel betrouwbaar en veilig? Wat is hier aan de hand?

Na enkele uren komt Cirrocumulus naar buiten met de mededeling dat er sprake is van een geavanceerde aanval gericht tegen een datacentrum van het bedrijf in Nederland, waardoor een deel van de Nederlandse klanten geraakt is. De situatie is inmiddels onder controle en Cirrocumulus Networks doet er alles aan om de dienstverlening zo snel mogelijk weer te herstellen. Dit kan enkele uren tot enkele weken in beslag nemen, afhankelijk van de specifieke situatie van de getroffen gebruikers.

In de dagen die volgen komt langzaam meer informatie over het incident naar buiten. Het lijkt er op dat aanvallers in staat zijn geweest om van binnenuit, via een botnet van virtuele machines, een enorme hoeveelheid verkeer te genereren. Deze interne DDoS aanval heeft de virtual machine manager (VMM) overspoeld en deze is daardoor uitgevallen. De VMM is software die de virtualisatie van de hardware (servers in een datacentrum) bestuurt en de beschikbare resources zoals geheugen en CPU over de aangesloten gebruikers (virtuele machines van klanten) verdeelt. Doordat de VMM gecrasht is, zijn alle virtuele machines die verbonden waren met de VMM en die op dat moment in gebruik waren, verloren gegaan.

Voor het herstel van de dienstverlening is de VMM gereset. Cirrocumulus Networks stemt met alle getroffen klanten af of de virtuele machines van die klant ook gereset kunnen worden of dat er eerst nadere analyse nodig is om te bepalen of gegevens, waar ten tijde van de crash aan gewerkt werd, hersteld moeten en kunnen worden. Dit hangt af van de configuratie van de cloudomgeving van een gebruiker en het type werkzaamheden die de klant op de getroffen virtuele machines uitvoert. Voor klanten waarvan (een deel van) de virtuele machines gereset worden, geldt dat zij enkele minuten of maximaal een paar uur nadat de VMM gereset wordt weer de beschikbaarheid hebben over hun cloudomgeving. Bij gebruikers waar nader onderzoek nodig is kan dit dagen of zelfs enkele weken duren.

In de berichtgeving over het incident wordt ook veel aandacht besteed aan hoe deze aanval heeft kunnen plaatsvinden. Om de virtuele machines als een botnet te laten functioneren hebben de aanvallers malware in de virtuele machines geplaatst. Dat betekent dat zij toegang moeten hebben gehad tot deze virtuele machines. Dit gegeven leidt tot speculaties over een verband met een recent incident bij gebruikers van Cirrocumulus Networks, waarbij aanvallers in staat waren om een kwetsbaarheid te exploiteren tijdens een herstelactie na een door extreem weer veroorzaakte storing. Die aanvallers hebben zich toen toegang verschaft tot de cloudomgeving van verschillende gebruikers, vermoedelijk om data te exfiltreren. Het lijkt er nu op dat dezelfde daders toen ook zijn begonnen met het voorbereiden van deze interne DDoS aanval. Volgens experts is het goed mogelijk dat de aanvallers, nu hun activiteiten ontdekt zijn, deze DDoS aanval hebben uitgevoerd om het onderzoek te bemoeilijken en zoveel mogelijk schade en hinder te veroorzaken.

Duiding

Voor clouddienstverlening worden DDoS aanvallen als een concreet risico gezien.[222] Een voorbeeld is een aanval op de clouddiensten van Amazon in 2019. Sinds die tijd is er ook veel aandacht besteed aan maatregelen om DDoS aanvallen tegen te gaan, gericht op het identificeren en afweren van oneigenlijk verkeer. Echter, wanneer de aanval wordt uitgevoerd met legitiem verkeer (bijvoorbeeld vanuit de klanten van de dienst) is het identificeren en stoppen van de stroom aan verkeer veel moeilijker. DDoS aanvallen op cloudomgevingen kunnen zowel van buiten komen (bijvoorbeeld een extern botnet waarmee een set virtuele machines in een cloudomgeving wordt aangevallen) als van binnenuit (een intern botnet van virtuele machines valt een doelwit binnen dezelfde cloudomgeving aan).[223] Met name interne aanvallen worden als een ernstig risico gezien, omdat hiermee de hele virtuele infrastructuur verstoord kan worden.[224]

De gevolgen van het – door de crash van de VMM – wegvallen van virtuele machines is vergelijkbaar met een computer die crasht. De gegevens waar op dat moment aan gewerkt wordt en die nog niet zijn opgeslagen, zijn verloren. Hoeveel dataverlies er is, hangt af van de instellingen van de virtuele machine. Voor complexe berekeningen of dataverwerkingen die soms uren of dagen in beslag nemen, is een crash veel ingrijpender dan wanneer de laatste paar zinnen in een tekstverwerkingsdocument verloren zijn gegaan. Ook de wijze waarop data worden opgeslagen, beïnvloedt de impact van een dergelijk incident. Het is bijvoorbeeld mogelijk om data op verschillende plekken te repliceren. Dit zijn zaken die niet automatisch door een cloud service provider worden geregeld en waar een gebruiker dus zelf over na zou moeten denken bij het inrichten van de (cloud)netwerkinfrastructuur.

Sleutelbegrippen

Virtualisatie: een van de kerntechnologieën van clouddienstverlening. Bij virtualisatie wordt een virtuele (gesimuleerde) computeromgeving gecreëerd, waardoor één fysieke computeromgeving wordt opgedeeld in meerdere virtuele computers, ook wel **virtual machines** genoemd.[225] Cloud Service Providers hebben in een datacentrum fysieke servers staan en de cloudomgeving van de klanten worden via virtualisatie opgebouwd. Hierdoor hoeven deze partijen niet zelf over een fysieke server te beschikken.
Virtual Machine Manager (VMM) of Hypervisor: een software programma (opgebouwd uit verschillende modules) dat tussen de fysieke server (fysieke hardware en host operating system) van de CSP en de virtuele machines (guest operating system) van de klanten zit. Het maakt de virtualisatie mogelijk en reguleert onder andere de prestaties door geheugen, CPU en andere resources te verdelen over virtuele machines.[226]

Kernvragen voor de lezer

1. Heeft u bij het ontwerpen van uw cloudomgeving rekening gehouden met het falen van deze infrastructuur (*design for failure*)?
2. Welke activiteiten voert uw organisatie uit in de cloudomgeving en hoe gevoelig zijn deze processen voor onderbreking?
3. Hoe wordt de data die in de cloudomgeving wordt verwerkt opgeslagen? Is er voor complexe of gevoelige dataverwerkingsprocessen nagedacht over replicatie op meerdere data center locaties of 'availability zones'[227]? N.B. Door replicatie kan ervoor gezorgd worden dat belangrijke data ook bij verstoring op één locatie niet verloren raakt, maar op een andere locatie beschikbaar blijft.
4. Weet u voor uw organisatie op basis waarvan een keuze is gemaakt voor een publieke, private of hybride cloudomgeving? Is hierbij meegenomen welke complexe dataverwerkingen en gevoelige of unieke data in uw organisatieprocessen een rol spelen?

Bijlagen

Bijlage 1 Verantwoording

Het Cybersecuritybeeld Nederland is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC). Het wordt jaarlijks door de NCTV vastgesteld. Daarbij wordt dankbaar gebruik gemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen.

De totstandkoming van het CSBN kent drie fasen: 1) analyseren, 2) schrijven en collegiaal toetsen en 3) valideren.

Ad 1 Analyseren

De NCTV verzamelt relevante informatie over incidenten, trends en verschuivingen op het gebied van de driehoek belangen, dreiging en weerbaarheid en analyseert deze. Daarbij wordt een antwoord geformuleerd op de volgende vragen:

Terugblik: welke relevante incidenten hebben in de periode maart 2020 t/m maart 2021 in Nederland plaatsgehad? Om welk type incidenten gaat het? Waardoor zijn ze veroorzaakt en welke schade / impact hebben ze gehad?

Belangen: welke belangen kunnen worden aangetast wanneer cyberincidenten zich voordoen? Wat kan de impact daarvan zijn?

Dreiging: welke digitale dreigingen kunnen de nationale veiligheid aantasten? Van wie of wat gaan die dreigingen uit? Tegen welke doelwitten zijn ze gericht? Welke modi operandi worden door actoren gebruikt? Welke kwetsbaarheden worden door actoren misbruikt? Zijn er verschuivingen zichtbaar geworden in de dreiging?

Weerbaarheid: wat is de mate van weerbaarheid van Nederland tegen die digitale dreigingen? Welke concrete initiatieven voor het verhogen van de weerbaarheid zijn er?

Vooruitblik: welke bredere ontwikkelingen hebben naar verwachting de komende jaren invloed op digitale veiligheid? Welke ontwikkelingen kunnen gamechangers zijn?

In de analysefase wordt externe partners gevraagd input te leveren. In november 2020 heeft een schriftelijke expertraadpleging plaatsgehad, waarbij overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen verzocht zijn de volgende vragen te beantwoorden:

- Welke gebeurtenissen, incidenten of ontwikkelingen op het gebied van cybersecurity van het afgelopen jaar in relatie tot Nederland zijn volgens u opvallend en waarom? Wat is het effect hiervan op de belangen, de dreiging en weerbaarheid?
- Welke verschuivingen verwacht u in het beeld van: a) de belangen, b) de dreiging en c) de weerbaarheid in relatie tot Nederland in het komende jaar en waarom?

In de periode november 2020 t/m februari 2021 heeft een aantal partijen uit de financiële sector (waaronder equensWorldline) en de Inspectie Justitie en Veiligheid daarnaast input geleverd voor het thema Weerbaarheid. Die input is verwerkt in het hoofdstuk over Risicomanagement. Op basis van de verzamelde informatie zijn de analysevragen beantwoord en zijn de risico's voor de Nationale Veiligheid geformuleerd. Vervolgens heeft de NCTV een schematisch kern-CSBN geformuleerd. De kern bevat de belangrijkste 'rode draden' voor het nieuwste cybersecuritybeeld en benoemt de thema's die nadere uitwerking verdienen, bijvoorbeeld omdat ze een verschuiving in het bestaande beeld inhouden of niet eerder geadresseerd zijn in het CSBN. De thema's zijn vervolgens getoetst bij een aantal partners.

Ad 2 Schrijven en collegiaal toetsen

Vervolgens zijn zowel het kern-CSBN als de thema's uitgeschreven door auteurs binnen de NCTV (kern-CSBN, hoofdstukken 1, 3, 5 en 6), het NCSC (hoofdstuk 7), de politie (hoofdstuk 4) en TNO (hoofdstuk 8). Hoofdstuk 2 (de Terugblik) is geschreven door NCTV en NCSC. De gehele tekst wordt binnen de NCTV en het NCSC meerdere keren collegiaal getoetst. Alle hoofdstukken komen tot stand onder redactionele eindverantwoordelijkheid van de NCTV.

Ad 3 Valideren

Het CSBN kent een uitgebreid validatietraject, waarbij de concepttekst voorgelegd wordt aan externe partners ter commentaar. Het betreft de partners die in de analysefase ook gevraagd zijn om input te leveren. Na het verwerken van het verzamelde commentaar wordt de definitieve tekst opgemaakt en door de NCTV vastgesteld.

Na de publicatie van het CSBN vindt een uitgebreide interne en externe evaluatie plaats. De verzamelde feedback wordt vervolgens verwerkt in het CSBN-traject van het volgende jaar. De evaluatie heeft in het verleden tot concrete veranderingen geleid, zoals het opnemen van een scenariohoofdstuk (sinds 2020) en het aanscherpen van de gehanteerde begrippen (2021, in samenwerking met prof. dr. Bibi van den Berg en em. prof. dr. Jan van den Berg). Naar aanleiding van de evaluaties van de voorgaande jaren heeft het NCSC besloten om medio 2021 het product 'Handreiking Cybersecuritymaatregelen' uit te brengen.

Bijlage 2
Bronnen en referenties

1 'Cybersecuritybeeld Nederland 2020', NCTV, juni 2020.
2 'Dreigingsbeeld statelijke actoren', AIVD, MIVD en NCTV, februari 2021.
3 'Openbaar Jaarverslag AIVD 2020', AIVD, april 2021.
4 Expertraadpleging voor CSBN 2021, november 2020 (zie ook de Bijlage Verantwoording). Zie tevens 'SURF Cyberdreigingsbeeld 2020-2021 Onderwijs en onderzoek': https://www.surf.nl/files/2021-02/surf-cyberdreigingsbeeld-2020-2021.pdf.
5 Verzekeraars stellen dat bedrijven zo vaak doelwit zijn van hackers, dat het voor hen minder interessant of rendabel wordt om zogenoemde cyberpolissen te verkopen. Losgeld voor ransomware is slechts 20% van de schade, de rest van de onkosten zit in het herstellen van systemen en aansprakelijkheid naar klanten toe. https://www.rtlnieuws.nl/economie/tech-business/artikel/5221830/cyberverzekeringen-hacken-cyberpolis-ransomware
6 Zo richtte de aan Noord-Korea toegeschreven Lazarusgroep zich op individuele cybersecurity onderzoekers, zie: https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/; https://www.microsoft.com/security/blog/2021/01/28/zinc-attacks-against-security-researchers/; https://www.zdnet.com/article/google-north-korean-hackers-have-targeted-security-researchers-via-social-media/. In de omvangrijke SolarWinds-aanval werden ook cybersecuritybedrijven FireEye en Crowdstrike getroffen: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html; https://www.crn.com/news/security/crowdstrike-fends-off-attack-attempted-by-solarwinds-hackers.
7 'Anchor Project The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT', Sentinel Labs, 10 december 2019; https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data. https://www.zdnet.com/article/cybercrime-groups-are-selling-their-hacking-skills-some-countries-are-buying/; https://www.thecipherbrief.com/why-cyber-criminals-are-winning
8 Ook internationaal wordt de conclusie dat ransomware een risico is voor de nationale veiligheid gemeengoed. Zie bijvoorbeeld het rapport 'Combating ransomware. A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force' van de Amerikaanse Ransomware Task Force (opgericht door de FBI en het Amerikaanse Ministerie van Justitie), april 2021, dat stelt dat ransomware economisch destructief is en ook impact heeft in de fysieke wereld.
9 'Cybersecuritybeeld Nederland 2020', NCTV, juni 2020.
10 Zie het jaarlijkse rapport van Dragos over cyberaanvallen op ICS/OT-omgevingen (waaronder vitale processen): 'ICS Cybersecurity year in review 2020', februari 2021, het Europol-rapport 'EU SOCTA 2021. A corrupting influence: the infiltration and understanding and undermining of Europe's economy and society by organised crime', april 2021, p. 38, 'Critical infrastructure sees rising cybersecurity risk', Oxford Analytica, 18 mei 2021 en tot slot 'M-trends 2021', FireEye Mandiant, maart 2021, p. 18. In Nederland werd een tiental Nederlandse zorgorganisaties geraakt door hackersgroep SilverFish (op dit moment is de zorgsector echter niet vitaal verklaard in Nederland). Zie https://www.z-cert.nl/nieuws/hackergroep-silverfish-moeilijk-te-zien-lastig-om-vanaf-te-komen/
11 'Integrale aanpak cyberweerbaarheid. Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren', CSR Adviesrapport 2021, nr. 2.
12 'Onderzoeksrapport Stichting Waternet. Onderzoek naar de toestand van de cybersecurity en besturing bij Stichting Waternet in het kader van de leveringszekerheid en kwaliteit van drinkwater', Inspectie Leefomgeving en Transport, 31 maart 2021.
13 https://www.kpn.com/zakelijk/blog/veel-industriele-controlesystemen-onvoldoende-beveiligd.htm
14 https://www.axios.com/russia-spies-working-with-cyber-criminals-5c2f12f7-8f25-419a-a850-3bc89de346a3.html. https://www.insurancebusinessmag.com/ca/news/cyber/cyberattacks-by-nation-states-are-becoming-more-aggressive-250443.aspx
15 https://www.theregister.com/2017/06/06/russia_cyber_militia_analysis/; https://www.cybereason.com/blog/blog-russia-nation-state-hacking-the-countrys-dedicated-policy-of-strategic-ambiguity
16 Zie bijvoorbeeld het rapport 'Countering Cyber Proliferation: Zeroing in on Access-as-a-Service' van de Atlantic Council, maart 2021, waarin wordt ingegaan op de nauwe samenwerking tussen de Russische dienst FSB en criminele hackersgroepen. Zie ook https://home.treasury.gov/news/press-releases/sm845.

17 'EU SOCTA 2021. A corrupting influence: the infiltration and understanding and undermining of Europe's economy and society by organised crime', april 2021.
18 Een voorbeeld is de Risicoklassenindeling voor Digitale Veiligheid, een risicoclassificatiemodel voor het midden- en kleinbedrijf (MKB). Zie https://www.digitaltrustcenter.nl/risicoklasse.
19 'Staat van de rijksverantwoording 2020. Testen, controleren, waarderen', Algemene Rekenkamer, mei 2021, p.29-30.
20 'Integrale aanpak cyberweerbaarheid. Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren', CSR Adviesrapport 2021, nr. 2.
21 Een internationaal voorbeeld betreft onderzoek van RiskRecon naar bedrijven die de kwetsbare versie van SolarWinds Orion gebruiken. Op 13 december 2020 werden 1.785 organisaties waargenomen die de Orionsoftware verbonden met internet. Dit aantal betrof op 1 februari 2021 nog 1.330. Slechts 8% van de bedrijven zou een Orion-update hebben geïnstalleerd als reactie op de inbreuk. Volgens RiskRecon gebruikt 4% van de bedrijven nog steeds een versie die de Sunburst-malware bevat. Een derde van de organisaties heeft de kwetsbaarheid nog niet gepatcht. RiskRecon stelt dat de lijst van organisaties met kwetsbare Orion-software nationale en lokale overheidsinstanties, universiteiten, hostingproviders en Fortune 500-bedrijven omvat. Zie https://www.securityweek.com/many-solarwinds-customers-failed-secure-systems-following-hack.
22 Aanvulling MIVD en AIVD aan NCTV, juni 2021.
23 'Openbaar Jaarverslag AIVD 2020', AIVD, april 2021.
24 https://www.ncsc.nl/actueel/nieuws/2020/januari/13/vele-nederlandse-citrix-servers-kwetsbaar-voor-aanvallen.
25 https://www.volkskrant.nl/nieuws-achtergrond/half-jaar-na-citrix-crisis-zijn-25-nederlandse-organisaties-gehackt-en-ze-weten-zelf-van-niets~b26947bc/.
26 https://www.ncsc.nl/actueel/nieuws/2021/maart/16/schade-microsoft-exchange.
27 Aanvulling MIVD en AIVD aan NCTV, juni 2021.
28 'Handreiking Cybersecuritymaatregelen', NCSC, juni 2021. Zie https://www.ncsc.nl/documenten.
29 Expertraadpleging voor CSBN 2021, november 2020 (zie ook de Bijlage Verantwoording).
30 Zie bijvoorbeeld de Cybersecuritymonitor 2020 van het CBS (2021) p. 8, waaruit blijkt dat grotere bedrijven structureler ICT-veiligheidsmaatregelen nemen dan kleine bedrijven.
31 Zie voor de advisory van de NSA: https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/
32 Expertraadpleging voor CSBN 2021, november 2020 (zie ook de Bijlage Verantwoording).
33 Zie file:///H:/Downloads/Rapport_'Informatie-uitwisseling_landelijk_dekkend_stelsel_cybersecurity'_.pdf.
34 Expertraadpleging voor CSBN 2021, november 2020 (zie ook de Bijlage Verantwoording).
35 Zie bijvoorbeeld de Kamerbrief 'Verminderen strategische afhankelijkheden', 10 februari 2021 en 'CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity' Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?', Cyber Security Raad, 6 mei 2021.
36 De Correspondent spreekt in dit verband over de 'infrastructurele macht' van de techbedrijven. Zie 'Technologiebedrijven vormen de basis van de samenleving. Door Corona is dit een steeds groter probleem.', De Correspondent 24 maart 2021.
37 Voorbeelden zijn de apps die in Frankrijk en het VK ontwikkeld werden voor de bestrijding van COVID-19, maar die niet opgenomen werden in de app stores van Apple en Google omdat ze niet aan de voorwaarden voldeden. In de praktijk is het bereik van deze apps zonder steun van Aple en Google nihil. Zie 'Technologiebedrijven vormen de basis van de samenleving. Door Corona is dit een steeds groter probleem.', De Correspondent 24 maart 2021 en 'Apple en Google blokkeren nieuwste versie Britse corona-app wegens locatiedata', security.nl, 12 april 2021.
38 https://hcss.nl/report/soevereiniteit-en-digitale-autonomie; https://www.volkskrant.nl/nieuws-achtergrond/de-europese-ambitie-die-moet-flink-omhoog-wat-betreft-clingendael-onderzoekers~b63c54d3/.
39 In het CSBN 2021 wordt een herzien begrippenkader gehanteerd, dat tot stand is gekomen in samenwerking met prof. dr. Bibi van den Berg (Universiteit Leiden) en emeritus prof. dr. Jan van den Berg (TU Delft en Universiteit Leiden). Daarbij is dankbaar gebruik gemaakt van: J. van den Berg, 'A basic set of mental models for understanding and dealing with the cybersecurity challenges of today', Journal of Information Warfare 19:1 (2020). https://www.jinfowar.com/journal/volume-19-issue-1/basic-set-mental-models-understanding-dealing-cybersecurity-challenges-today
40 'Playing with lives: cyberattacks on healthcare are attacks on people', CyberPeace Institute, maart 2021.
41 'Openbaar Jaarverslag AIVD 2020', AIVD, april 2021.
42 'Ministerie waarschuwt voor nep-sms om CoronaMelder-app te downloaden', nu.nl, 22 juli 2020, https://www.nu.nl/tech/6066049/ministerie-waarschuwt-voor-nep-sms-om-coronamelder-app-te-downloaden.html
43 'Gehackte EMA-documenten verschijnen online: 'Is mee geknoeid'', NOS, 15 januari 2021, https://nos.nl/artikel/2364547-gehackte-ema-documenten-verschijnen-online-is-mee-geknoeid.html

44 https://www.volkskrant.nl/nieuws-achtergrond/chinese-en-russische-hackers-kraken-netwerk-geneesmiddelenbureau~b2f47502/ 6 maart 2021
45 'RTL Nieuws kwam binnen bij geheim defensieoverleg Europa na fout ministerie', RTL Nieuws, 20 november 2020, https://www.rtlnieuws.nl/tech/artikel/5198276/rtl-nieuws-hack-defensie-ministers-europa-overleg-bijleveld
46 Zie hiervoor advisory NCSC 2020-0105: https://advisories.ncsc.nl/advisory?id=NCSC-2020-0105
47 Zie hiervoor het NCSC beveiligingsadvies https://www.ncsc.nl/actueel/nieuws/2021/april/20/pulse-secure en https://www.ncsc.nl/actueel/advisory?id=NCSC-2021-0345
48 Zie bijvoorbeeld het CISA rapport over het toegenomen scannen naar VPN kwetsbaarheden: https://us-cert.cisa.gov/ncas/alerts/aa20-133a.
49 'Kwetsbaarheden verholpen in Citrix Application Delivery Controller, Gateway en SD-WAN WANOP appliance', NCSC, 16 juli 2020, https://www.ncsc.nl/actueel/advisory?id=NCSC-2020-0539
50 'Half jaar na Citrix-crisis zijn 25 Nederlandse organisaties gehackt. En ze weten zelf van niets', Volkskrant 1 juli 2020, https://www.volkskrant.nl/nieuws-achtergrond/half-jaar-na-citrix-crisis-zijn-25-nederlandse-organisaties-gehackt-en-ze-weten-zelf-van-niets~b26947bc/
51 https://www.ncsc.nl/actueel/nieuws/2020/mei/25/verhoogde-scanactiviteiten-door-statelijke-actoren-naar-vpn-kwetsbaarheden
52 'Focus op digitaal thuiswerken', Algemene Rekenkamer, 2 november 2020.
53 https://www.ncsc.nl/actueel/ontwikkelingen-cybersecurity september 2020.
54 'DDoS data rapport 2020. Aanvallen in 2020: krachtiger, complexer en duren langer', NBIP, maart 2021.
55 https://www.nomoreddos.org/ddos-coalitie-heeft-handenvol-aan-huidige-ddos-aanvallen/
56 https://www.ncsc.nl/actueel/nieuws/2020/september/4/toename-aan-intensiviteit-en-aantal-ddos-aanvallen ; https://tweakers.net/nieuws/171786/nederlandse-ddos-doelwitten-ontvingen-afpersingsmail-uit-naam-van-staatshackers.html
57 'DDoS-aanvallen treffen verschillende Nederlandse providers - update 3' , Tweakers, 28 augustus 2020, https://tweakers.net/nieuws/171522/ddos-aanvallen-treffen-verschillende-nederlandse-providers.html
58 'Ransomware gangs add DDoS attacks to their extortion arsenal', bleepingcomputer.com, 1 oktober 2020.
59 FBI+PIN+-+12.10.2020.pdf (nj.gov).
60 Zie: Ontwikkelingen cybersecurity | Actueel | Nationaal Cyber Security Centrum (ncsc.nl).
61 Aanvulling MIVD en AIVD aan NCTV, juni 2021.
62 'Update cyberaanval', Hof van Twente, 21 januari 2021, https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2021/01/artikel/update-cyberaanval-1811
63 'Meevaller voor de gemeente Hof van Twente: deel van gestolen gegevens toch teruggevonden', Trouw, 5 maart 2021.
64 'Openbaar Jaarverslag AIVD 2020', AIVD, april 2021.
65 'IBM warns hackers targeting COVID vaccine 'cold chain' supply process' , Reuters, 3 december 2020, https://www.reuters.com/article/health-coronavirus-vaccines-cyber-idUSL1N2II05A.
66 Zie het door het NCSC op 14 december uitgebrachte beveiligingsadvies H/H: NCSC Advisories.
67 'Backdoor in SolarWinds Orion', NCSC, 19 december 2020, https://www.ncsc.nl/actueel/nieuws/2020/december/19/solarwinds-orion
68 https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/
69 https://www.consilium.europa.eu/nl/press/press-releases/2021/04/15/declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation/ en https://twitter.com/ministerBlok/status/1382686027341516810
70 'Rapportage Datalekken 2020', Autoriteit Persoonsgegevens, 1 maart 2020.
71 https://nos.nl/artikel/2374024-datalek-bij-autobedrijven-treft-mogelijk-miljoenen-nederlanders.html
72 'GGD-medewerkers gluurden ongeoorloofd naar BN'ers in coronadatabase', AD.nl, 3 november 2020.
73 'Twee GGD-medewerkers aangehouden voor datadiefstal', politie.nl, 25 januari 2021.
74 https://ggdghor.nl/actueel-bericht/datadiefstal-goed-dat-om-tot-vervolging-overgaat/
75 https://ggdghor.nl/thema/vragen-antwoorden-datadiefstal/
76 'Datahack oude MijnKNWU-omgeving', KNWU, 27 november 2020, https://www.knwu.nl/nieuws/datahack-oude-mijnknwu-omgeving
77 'Transavia: 'Data 80.000 passagiers mogelijk gestolen'', RTL, 24 februari 2020, https://www.rtlnieuws.nl/tech/artikel/5033051/datalek-bij-transavia-gegevens-80000-passagiers-mogelijk-gestolen
78 https://www.gelderlander.nl/nijmegen/ggd-door-het-stof-na-overbelaste-systemen-dit-was-niet-onze-meest-publieksvriendelijke-dag~a46c6ed0/?referrer=https%3A%2F%2Fwww.bing.com%2F
79 'Hostingprovider heeft storing ziekenhuizen opgelost door vervangen componenten', Tweakers, 9 oktober 2020, https://tweakers.net/nieuws/173162/hostingprovider-heeft-storing-ziekenhuizen-opgelost-door-vervangen-componenten.html

80 'Toont Corona de veerkracht van de digitale samenleving?', Capgemini, 7 april 2020. https://www.capgemini.com/nl-nl/2020/04/toont-corona-de-veerkracht-van-de-digitale-samenleving/
81 'KPN Verkort Jaarverslag 2020, Nederland in digitale stroomversnelling', KPN, 2020. https://www.jaarverslag2020.kpn/downloads/KPN-Verkort-Jaarverslag 2020-Update.pdf.
82 'Cybercriminals now using malware and adware to exploit virtual meeting apps', iGRC, 8 april 2020 (igrc.eu); 'Report 2020 Nowhere to Hide', CrowdStrike, 2020; 'Prospects for cybersecurity to end 2020', Ofxord Analytica, 4 juni 2020.
83 'Digitale Pandemie', iBestuur, Bart Jacobs, 24 februari 2021. https://ibestuur.nl/podium/digitale-pandemie.
84 'Waar blijft voor GGD het vaccin tegen datalekken?', Computable, 1 februari 2021. https://www.computable.nl/artikel/opinie/security/7130143/1509029/waar-blijft-vaccin-voor-ggd-tegen-datalekken.html
85 'Cyberaanval op Amerikaans ministerie van Gezondheid', RTLZ, 16 maart 2020. https://www.rtlz.nl/tech/artikel/5058191/cyberaanval-ministerie-gezondheid-corona-coronavirus ; 'Steeds meer cyberaanvallen gerelateerd aan coronavirus', NPOradio1, 5 april 2020. https://www.nporadio1.nl/onderzoek/22830-steeds-meer-'cyberaanvallen-met-link-naar-coronavirus.
86 'Cybersecurity beeld Nederland 2020', NCTV, juni 2020.
87 'OM waarschuwt voor toename cybercrime tijdens coronacrisis', AGConnect, 23 maart 2020. https://www.agconnect.nl/artikel/om-waarschuwt-voor-toename-cybercrime-tijdens-coronacrisis ; 'Cybercriminelen spelen in op coronavirus', politie.nl, 31 maart 2020. https://www.politie.nl/nieuws/2020/maart/31/cybercriminelen-spelen-in-op-coronavirus.html ; 'Staying safe during COVID-19: what you need to know', Europol, 17 maart 2020. https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know.
88 'WHO waarschuwt voor phishingmails over het coronavirus', security.nl, 18 februari 2020.
89 'Cyberdreigingsbeeld Zorg 2020', Z-CERT, 1 februari 2021.
90 'Cyberdreigingsbeeld Zorg 2020', Z-CERT, 1 februari 2021.
91 'Tighter targeting will make ransomware more risky', Oxford Analytica, 8 februari 2020; 'Report 2020 Nowhere to Hide', CrowdStrike, 2020; 'Prospects for cybersecurity to end 2020', Ofxord Analytica, 4 april 2020; 'Ziekenhuizen in regio schroeven door corona hun digitale beveiliging op: deze bedrijven staan als 'The A-Team' klaar als het misgaat', Gelderlander, 20 mei 2020. https://www.security.nl/posting/692457/Ransomware+kost+Amerikaanse+ziekenhuisketen+67+miljoen+dollar
92 'Thrid French Hospital Hit by Cyberattack', Security Week, 9 maart 2021. https://www.securityweek.com/third-french-hospital-hit-cyberattack; 'Cyberattaque à l'hôpital Nord-Ouest : des opérations reportées', Le Progres, 15 februari 2021; 'Duits ziekenhuis raakte via Citrix-lek besmet met ransomware', Tweakers, 18 september 2020. https://tweakers.net/nieuws/172362/duits-ziekenhuis-raakte-via-citrix-lek-besmet-met-ransomware.html; 'Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak', ZDNet, 13 maart 2020. https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/; 'Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic', BleepingComputer, 26 maart 2020; 'Netwalker Ransomware Infecting Users via Coronavirus Phishing', BleepingComputer, 21 maart 2020; 'Overheid waarschuwt ziekenhuizen voor cyberaanval', DeTijd, 25 maart 2020. https://www.tijd.be/ondernemen/algemeen/overheid-waarschuwt-ziekenhuizen-voor-cyberaanval/10216656.html.
93 'Cyberdreigingsbeeld Zorg 2020', Z-CERT, 1 februari 2021.
94 'WHO Director-General's opening remarks at the media briefing on COVID-19', World Health Organization, 11 maart 2020.
95 'Advisory: COVID-19 exploited by malicious cyber actors', National Cyber Security Centre, 8 april 2020. NCSC.GOV.UK; 'Advisory: APT groups target healthcare and essential services', National Cyber Security Centre, 5 mei 2020. NCSC.GOV.UK; 'Cyber warning issued for key healthcare organisations in UK and USA, National Cyber Security Centre, 5 mei 2020. NCSC.GOV.UK; 'People's Republic of China (PRC) Targeting of COVID-19 Research Organizations', FBI National Press Office, 13 mei 2020; 'Alert (AA20-126A)', US Cybersecurity & infrastructure security agency, 5 mei 2020. APT Groups Target Healthcare and Essential Services, CISA.
96 'Kamerbrief over jaarplan AIVD voor het jaar 2021', AIVD, 15 december 2020.
97 'Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus', Reuters, 2 april 2020; 'Kremlin-linked hackers steal medical trial records from British coronavirus lab', NewEurope, 11 mei 2020; 'Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead', Reuters, 8 mei 2020; 'APT Groups Target Firms Working on COVID-19 Vaccines', InfoRisk today, 13 november 2020; 'Hackers 'try to steal Covid vaccine secrets in intellectual property war', The Guardian, 22 november 2020.
98 'COVID-19 alters focus of cyberespionage', Oxford Analytica , 11 juni 2020.
99 'Dreigingsbeeld Terrorisme Nederland 53', NCTV, 15 oktober 2020.
100 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, 3 februari 2021, p. 19.
101 Expertraadpleging voor CSBN 2021, november 2020 (zie ook de Bijlage Verantwoording). Zie tevens SURF Cyberdreigingsbeeld 2020-2021 Onderwijs en onderzoek: https://www.surf.nl/files/2021-02/surf-cyberdreigingsbeeld 2020-2021.pdf.
102 'Cyberdreigingsbeeld Zorg 2020', Z-CERT, 1 februari 2021.
103 'Cyberdreigingsbeeld 2020-2021 onderwijs en onderzoek', SURF, 8 februari 2021.
104 'Visierapport Trends in Veiligheid 2020', Capgemini, 28 augustus 2020. https://ibestuur.nl/partner-capgemini/trends-in-veiligheid 2020-nederlanders-steeds-meer-bewust-van-eigen-verantwoordelijkheid-in-zorg-dragen-voor-online-veiligheid.

105 'Council calls for strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic', European Council, 15 december 2020. https://www.consilium.europa.eu/en/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/.
106 https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf?mkt_tok=eyJpIjoiTkRoaE1qVmtZMlU1Tm1GbSIsInQiOiJXcnozaW9sS1VwWCtZaE1oU1YyNWluNot3YlpFeStDaWhxa1RveWJvSlNSNoNKTzlLUoMyajQ5cFJycjMrbzUrRkErSlZhZTgrV3Z2cUJXeFhDTjRaaHh4cVAweVZldkgwSnQ1dVZkTHZIVnRlU25ZcUtNUW85WUhHQ2N2MGdUZiJ9.
107 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019.
108 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019.
109 'Politie jaarverantwoording over 2020'; 'Politie jaarverantwoording over 2019'; 'Cybersecuritybeeld Nederland 2020', NCTV, juni 2020.
110 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019.
111 https://www.politie.nl/nieuws/2019/januari/28/11-politie-en-justitie-gaan-wereldwijd-achter-de-gebruikers-van-%E2%80%98ddos-for-hire-websites%E2%80%99-aan.html.
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down.
112 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019.
113 https://www.sentinelone.com/blog/inside-emotet-banking-trojan-malware-distributor/
114 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019.
115 'Anchor Project The Deadly Planeswalker: How The TrickBot Group United High-Tech Crimeware & APT', Sentinel Labs, 10 december 2019; https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data.
116 https://www.researchgate.net/publication/343009039_Laundering_the_Profits_of_Ransomware_Money_Laundering_Methods_for_Vouchers_and_Cryptocurrencies. Zie ook 'Digital Currencies' Role in Facilitating Ransomware Attacks: A Brief Explainer', 3 mei 2021: https://www.thirdway.org/memo/digital-currencies-role-in-facilitating-ransomware-attacks-a-brief-explainer?utm_source=Third+Way+Subscribers&utm_campaign=689ac6b6f1-EMAIL_CAMPAIGN_2019_02_21_03_29_COPY_01&utm_medium=email&utm_term=0_8952c391fb-689ac6b6f1-228870509.
117 https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-understanding-ransomware-strategies-defeat.pdf.
118 Deze procesbeschrijving is een door de politie aangepaste variant van de Cyber Kill Chain van Lockheed Martin.
119 'F-Secure: Het ransomware-incident bij Norsk Hydro: LockerGoga versleutelt werkelijk alles, zeggen onderzoekers van F-Secure', 26 maart 2019; 'FireEye: A Nasty Trick: From Credential Theft Malware to Business Disruption', 11 januari 2019;
120 https://www.zdnet.com/article/largest-ransomware-demand-now-stands-at-30-million-as-crooks-get-bolder/#:~:text=Largest%20ransomware%20demand%20now%20stands%20at%20%2430%20million%20as%20crooks%20get%20bolder&text=ZDNet
121 https://www.politie.nl/nieuws/2020/februari/6/00-politie-%E2%80%98niet-betalen-bij-ransomware.%E2%80%99.html.
122 https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer/;
https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020; https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report;
123 https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-understanding-ransomware-strategies-defeat.pdf
124 https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020.
125 https://www.coveware.com/blog/2020/11/30/why-small-professional-service-firms-are-ransomware-targets.
126 https://www.techzine.nl/nieuws/security/440301/46-procent-van-mkbers-getroffen-door-ransomware/.
127 https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.
128 https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html
129 https://www.bnr.nl/brandstories/de-cyberstelling/10434887/betaal-nooit-bij-een-ransomware-gijzeling
130 https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html; 'Triple threat: Emotet deploys Trickbot to steal data & spread Ryuk ransomware', Cybereason, 2 april 2019; 'A One-two Punch of Emotet, TrickBot, & Ryuk Stealing & Ransoming Data', Cybereason, 2 april 2019.
131 Oa: https://cybersecurityventures.com/ransomware-is-a-real-pain-in-the-wallet/#:~:text=Damage%20Costs%20Rise%2057X%20From%202015%20To%202021&text=The%20damages%20for%202018%20were,than%20it%20was%20in%202015; https://www.otorio.com/blog/understanding-the-ransomware-victim-profile-part-one/;
https://www.helpnetsecurity.com/2020/11/26/ransomware-cost-2020/.
132 https://www.criminaliteitinbeeld.nl/onderwerpen/slachtofferschap/slachtofferschap-criminaliteit/melding-en-aangifte.
133 https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

134 https://www.zdnet.com/article/largest-ransomware-demand-now-stands-at-30-million-as-crooks-get-bolder/#:~:text=Largest%20ransomware%20demand%20now%20stands%20at%20%2430%20million%20as%20crooks%20get%20bolder&text=ZDNet
135 https://www.pindrop.com/blog/70-percent-of-enterprise-ransomware-victims-paid-up-data-shows/#:~:text=Ransomware%20gangs%20have%20been%20targeting,to%20get%20their%20data%20back; https://www.techzine.nl/nieuws/security/440301/46-procent-van-mkbers-getroffen-door-ransomware/.
136 https://www.sophos.com/en-us/press-office/press-releases/2020/05/paying-the-ransom-doubles-cost-of-recovering-from-a-ransomware-attack-according-to-sophos.aspx
137 https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff.
138 'Geïntegreerde risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid (2019); 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, 3 februari 2021, p. 11, 'Kamerbrief Tegengaan statelijke dreigingen', 18 april 2019.
139 Het Onderzoeksrapport Stichting Waternet, Inspectie Leefomgeving en Transport, Ministerie van Infrastructuur en Waterstaat (31 maart 2021) wijst op de risico's die voortvloeien uit een connectie tussen de kantoorautomatisering en de procesautomatisering.
140 https://www.sentinelone.com/blog/how-ransomware-attacks-are-threatening-our-critical-infrastructure/; https://www.forbes.com/sites/guidehouse/2020/12/11/ransomware-threat-to-critical-infrastructure-is-a-new-priority/?sh=5f1bdaf55adb; https://cyberpeaceinstitute.org/news/criminals-and-hostile-states-attack-healthcare-with-impunity-the-cyberpeace-institute-calls-for-accountability; https://www.varonis.com/blog/how-has-ransomware-impacted-the-us-government/
141 https://www.nwo.nl/nieuws/nwo-netwerk-gehackt#
142 https://www.volkskrant.nl/nieuws-achtergrond/hello-need-data-back-contact-us-fast-hackers-eisen-geld-van-gemeente-hof-van-twente~b6c46cff/; https://www.techrepublic.com/article/local-governments-continue-to-be-the-biggest-target-for-ransomware-attacks/
143 Zie https://www.nomoreransom.org
144 De driedeling en beschrijving is ontleend aan: Jan van den Berg, 'A Basic Set of Mental Models for Understanding and Dealing with the Cybersecurity Challenges of Today', Journal of Information Warfare, 19:1, 2020.
145 'Verkenning t.b.v. de risicocategorie Aantasting functioneren Internet', TNO, 29 maart 2018.
146 'De publieke kern van het internet. Naar een buitenlands internetbeleid', Wetenschappelijke Raad voor het Regeringsbeleid, 2015.
147 'Verkenning t.b.v. de risicocategorie Aantasting functioneren Internet', TNO, 29 maart 2018.
148 Aanvulling op basis van externe feedback tijdens het validatieproces.
149 'Verkenning t.b.v. de risicocategorie Aantasting functioneren Internet', TNO, 29 maart 2018.
150 'De publieke kern van het internet. Naar een buitenlands internetbeleid', Wetenschappelijke Raad voor het Regeringsbeleid, 2015.
151 'De publieke kern van het internet. Naar een buitenlands internetbeleid', Wetenschappelijke Raad voor het Regeringsbeleid, 2015.
152 'Vraagstukken en perspectieven voor ICT Supply Chain Risk Management (SCRM) – een initiële verkenning', TNO 2021 R10245, februari 2021 https://www.ncsc.nl/documenten/rapporten/2021/april/28/tno-2021-r10245-vraagstukken-en-perspectieven-voor-ict-scrm-%E2%80%93-een-initiele-verkenning
153 R.J. Aldrich en A. Karatzogianni, 'Postdigital war beneath the sea? The Stack's underwater cable insecurity' in: Digital War, mei 2020, p. 3, https://link.springer.com/article/10.1057/s42984-020-00014-x; A. Blum, 'Tubes. A journey to the center of the internet', 2012, p. 193; A. Brzozowski, 'NATO seeks ways of protecting undersea cables from Russian attacks', EURACTIV.com, 23-10-2020, https://www.euractiv.com/section/defence-and-security/news/nato-seeks-ways-of-protecting-undersea-cables-from-russian-attacks/.
154 'Cybersecuritybeeld Nederland CSBN 2020', NCTV, juni 2020.
155 'Bases for Trust in a Supply Chain', LAWFARE, 1 februari 2021, https://www.lawfareblog.com/bases-trust-supply-chain.
156 'Cybersecuritybeeld Nederland 2020', NCTV, juni 2020.
157 'Gevolgen van Microsoft Exchange kwetsbaarheden groot voor Nederlandse organisaties en bedrijven', NCSC, 16 maart 2021, https://www.ncsc.nl/actueel/nieuws/2021/maart/16/schade-microsoft-exchange.
158 'Pulse Secure waarschuwt voor actief aangevallen zerodaylek in vpn-software', 20 april 2021, https://www.security.nl/posting/699977/Pulse+Secure+waarschuwt+voor+actief+aangevallen+zerodaylek+in+vpn-software.
159 'Annual threat assessment of the US intelligence community', Director of National Intelligence, 9 april 2021, p. 21.
160 Zie voor een historisch overzicht van aanvallen op de ICT-leveranciersketen: 'Breaking trust: Shades of crisis across an insecure software supply chain', Atlantic Council, juli 2020.
161 Zie bijvoorbeeld 'SolarWinds hack raises risks for cloud services', Oxford Analytica, 26 april 2021.

162 'US investigators probing breach at code testing company Codecov', Reuters, 17 april 2021, https://www.reuters.com/technology/us-investigators-probing-breach-san-francisco-code-testing-company-firm-2021-04-16/; 'Codecov hackers breached hundreds of restricted customer sites', Reuters.com, 19 april 2021, https://www.reuters.com/technology/codecov-hackers-breached-hundreds-restricted-customer-sites-sources-2021-04-19/; 'CodeCov supply-chain compromise likened to SolarWinds attack', Malwarebytes, 20 april 2021, https://blog.malwarebytes.com/awareness/2021/04/codecov-supply-chain-compromise-likened-to-solarwinds-attack/; 'Codecov breach impacted 'hundreds' of customer networks: report', ZDNet, 21 april 2021, https://www.zdnet.com/article/codecov-breach-impacted-hundreds-of-customer-networks/; 'Honderden bedrijven getroffen door backdoor in Bash Uploader Codecov', Security.nl, 20 april 2021, https://www.security.nl/posting/699903/%22Honderden+bedrijven+getroffen+door+backdoor+in+Bash+Uploader+Codecov%22.

163 'Vraagstukken en perspectieven voor ICT Supply Chain Risk Management (SCRM) – een initiële verkenning', TNO 2021 R10245, februari 2021 https://www.ncsc.nl/documenten/rapporten/2021/april/28/tno-2021-r10245-vraagstukken-en-perspectieven-voor-ict-scrm-%E2%80%93-een-initiele-verkenning

164 'Russian hack of US agencies exposed supply chain weaknesses', Associated Press International, 25 januari 2021.

165 'Supply chain security is actually worse than we think', ZDNet, 10-02-2021, https://www.zdnet.com/article/supply-chain-security-is-actually-worse-than-we-think/.

166 'Russian hack of US agencies exposed supply chain weaknesses', Associated Press International, 25 januari 2021.

167 'Chinese Supply-Chain Attack on Computer Systems', Schneier on Security, 13 februari 2021, https://www.schneier.com/blog/archives/2021/02/chinese-supply-chain-attack-on-computer-systems.html.

168 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, 3 februari 2021.

169 'Speler of speelbal?', L. van Middelaar, F-P van der Putten en M. Sie Dhian Ho, De Groene Amsterdammer, 3 februari 2021.

170 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, 3 februari 2021; 'Cybersecuritybeeld Nederland 2019', NCTV juni 2019 en 'Cybersecuritybeeld Nederland 2020', NCTV, juni 2020.

171 'Noord Korea stal 316 miljoen dollar aan cryptovaluta voor nucleaire wapens', NOS, 10 februari 2021 https://nos.nl/artikel/2368081-noord-korea-stal-316-miljoen-dollar-aan-cryptovaluta-voor-nucleaire-wapens.html.

172 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, 3 februari 2021.

173 'Openbaar Jaarverslag AIVD 2019', AIVD, april 2020.

174 'Openbaar Jaarverslag AIVD 2019', AIVD, april 2020; 'Openbaar Jaarverslag AIVD 2020', AIVD, april 2021.

175 'Cybersecuritybeeld Nederland 2019', NCTV juni 2019 en 'Cybersecuritybeeld Nederland 2020', NCTV, juni 2020.

176 'Offensief cyberprogramma als ideaal businessmodel', AIVD, juni 2019.

177 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV 3 februari 2021.

178 Deze trend is gesignaleerd door BitDefender ('The 'New Normal' State of Cybersecurity. 2020 - Business Threat Landscape Report'), de Electronic Frontier Foundation ('Global cyber community can do more to stop state-sponsored malware, EFF researcher says', Cyberscoop 18 februari 2021), BlackBerry ('BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps, 2020'), het rapport 'The CostaRicto Campaign: Cyber-Espionage Outsourced', 2020), Bellingcat ('Bahamut, Pursuing a Cyber Espionage Actor in the Middle East', 12 juni 2017), Citizen Lab ('Dark Basin. Uncovering a Massive Hack-For-Hire Operation, 9 juni 2020') en Amnesty International ('German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed', 25 september 2020).

179 'Openbaar Jaarverslag AIVD 2020', AIVD, april 2021.

180 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV 3 februari 2021.

181 In het product 'Handreiking Cybersecuritymaatregelen' van het NCSC worden onder andere de volgende basismaatregelen genoemd: patching, multifactorauthenticatie, logging, backups en netwerksegmentatie (https://www.ncsc.nl/documenten).

182 Er heeft in november 2020 een expertraadpleging plaatsgevonden. Daarnaast is door het NCSC met diverse partijen gesproken voor de totstandkoming van dit CSBN. Voor het perspectief van de wetgever kan gekeken worden naar de voorstellen voor de nieuwe NIB-richtlijn (https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52020PC0823) en de DORA-verordening (https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52020PC0595). Wat betreft de toezichthouders geeft het 'Plan van aanpak informatiebeveiliging van meldkamers' een goed beeld van de blik op risicomanagement vanuit de Inspectie JenV (https://www.inspectie-jenv.nl/actueel/nieuws/2020/12/09/inspectie-onderzoekt-informatiebeveiliging-meldkamers). Het 'Onderzoeksrapport Stichting Waternet' van de ILT schetst de rol van risicomanagement voor grip op beveiliging (https://www.ilent.nl/documenten/rapporten/2021/4/2/onderzoeksrapport-stichting-waternet).

183 'Framework for improving critical infrastructure cybersecurity', National Institute of Standards and Technology (2018), version 1.1, https://doi.org/10.6028/NIST.CSWP.04162018.

184 'ISO/IEC 27005:2018 – Information technology – Security techniques – Information security risk management', International Organization for Standardization (2018), https://www.iso.org/standard/75281.html.

185 'Guidance on cyber resilience for financial market infrastructures', Bank for International Settlements (2016), https://www.bis.org/cpmi/publ/d146.pdf.

186 'Voorbereiden op digitale ontwrichting', Wetenschappelijke Raad voor het Regeringsbeleid (2019), https://www.wrr.nl/adviesprojecten/digitale-ontwrichting/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.
187 'Handreiking voor implementatie van detectie-oplossingen', Nationaal Cyber Security Centrum (2015), https://www.ncsc.nl/documenten/publicaties/2019/mei/01/handreiking-voor-implementatie-van-detectie-oplossingen.
188 'The security development lifecycle', Michael Howard en Steve Lipner (2006), ISBN 9780735622142.
189 'Software engineering', Barry Boehm (1976), IEEE Transactions on Computers, vol. C-25, no. 12.
190 'Security and usability', Lorrie Cranor en Simson Garfinkel (2005), ISBN 9780596008277.
191 'Security-by-design in de vitale sector', Nobis Policy Lab (2020), https://hdl.handle.net/20.500.12832/3007.
192 Er zijn veel raamwerken die structuur kunnen bieden bij het implementeren van een risicomanagementsysteem en bij het uitvoeren van risicoanalyses. Relevante internationale standaarden zijn ISO 31000:2018 en ISO 27005:2018. NIST heeft SP 800-30 (https://doi.org/10.6028/NIST.SP.800-30r1) en SP 800-37 (https://doi.org/10.6028/NIST.SP.800-37r2) gepubliceerd.
193 De genoemde fundamentele principes zijn gedestilleerd uit gesprekken met sectoren en organisaties die weerbaarder lijken dan anderen. De principes zijn niet uitputtend en ze dienen niet als instructie, maar enkel ter illustratie en inspiratie.
194 Strategische risico's zijn risico's die op tafel liggen bij bestuurders. Tactische risico's zijn risico's waar lijnmanagers voor aan de lat staan. Operationele risico's zijn risico's voor het niveau van de werkvloer.
195 Bij het opstellen van scenario's kunnen historische aanvallen en incidenten een goede voedingsbodem vormen. Naast algemene problemen zoals spionage, ransomware en DDoS, kunnen de inzichten uit het hoofdstuk Terugblik dienen ter inspiratie voor de dreigingen achter incidenten, de geraakte belangen en de (niet) genomen maatregelen. Ook kan het 'Nationaal Crisisplan Digitaal' van de NCTV daarbij gebruikt worden als taxonomie voor verschillende typen incidenten (https://www.nctv.nl/actueel/nieuws/2020/02/21/nationaal-crisisplan-digitaal-schade-beperken-en-snel-herstel).
196 Dit CSBN ziet een risico als 'de kans dat een dreiging leidt tot een cyberincident en de impact van het cyberincident op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid'. De internationale norm ISO 27005:2018 ziet een risico als 'a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event'.
197 Een voorbeeld van een tabletop oefening is de pandemiesimulatie van RAND uit 2006 voor lokale zorgverleners in de VS (https://www.rand.org/health/surveys_tools/panflu_ttx.html). Een voorbeeld van een red teaming oefening is het TIBER-NL 3.0 raamwerk van de Nederlandsche Bank uit 2020 voor financiële instellingen (https://www.dnb.nl/actueel/algemeen-nieuws/nieuwsberichten-2020/nieuwe-en-verbeterde-versie-tiber-nl-guide/). Met betrekking tot red teaming blijkt uit de kamerbrief 'Voortgang informatiebeveiliging overheid' dat steeds meer overheden deze vorm van testen toepassen, met een positief effect op de veiligheid (https://www.rijksoverheid.nl/documenten/kamerstukken/2021/03/18/kamerbrief-voortgang-informatieveiligheid-overheid).
198 Ongeacht de soort securitytest die wordt toegepast is het van belang om een geschikte uitvoerende partij te vinden. Zo blijkt dat bij Gemeente Hof van Twente kwetsbaarheden over het hoofd zijn gezien tijdens een penetratietest. Deze test schijnt geen standaard methodiek te hebben gevolgd en de resultaten stroken niet met informatie uit open bronnen (https://www.hofvantwente.nl/fileadmin/files/hofvantwente/inwoners/actueel/Te-goed-van-vertrouwen.pdf). Om de kans op dergelijke problemen te verkleinen is in Engeland de CREST-certificering in het leven geroepen voor het borgen van de kwaliteit van securitytesters. In Nederland heeft het CCV in 2021 een keurmerk geïntroduceerd voor aanbieders van penetratietesten (https://hetccv.nl/keurmerken/expert/keurmerk-pentesten/).
199 Zeker 'unknown unknowns' of 'black swans' zijn lastig te voorspellen. Dat neemt alleen niet weg dat er veel 'known knowns' zijn, waaronder fouten die al meer dan 25 jaar voorkomen. Verder kan samenwerking helpen om hiaten in kennis op te vullen door middel van het uitwisselen van inzichten (voor 'unknown knowns') en door het doen van onderzoek (voor 'known unknowns').
200 Het NCSC speelt een belangrijke rol bij het aanjagen van verbinding en samenwerking tussen partijen, bijvoorbeeld in het kader van ISAC's. Zo heeft het NCSC in 2020 o.a. de handreiking 'Haal meer uit je ISAC' gepubliceerd, met tips voor het uitbouwen van ISAC's (https://www.ncsc.nl/documenten/publicaties/2020/februari/24/handreiking-haal-meer-uit-je-isac). ISAC's en andere vormen van samenwerkingsverbanden kunnen plaatsvinden op een lokaal, regionaal, nationaal en internationaal niveau.
201 Problemen gerelateerd aan het toepassen van risicomanagement zonder buy-in van bestuurders spelen ook bij organisaties die geen CISO in dienst hebben. Als IT-verantwoordelijken in een dergelijke situatie op eigen houtje een risicoanalyse uitvoeren, dan is de kans groot dat de bevindingen niet landen binnen de organisatie.
202 Vanuit een breder perspectief blijkt dat methoden voor risicomanagement die traditioneel gezien worden toegepast bij het beheersen van risico's voor organisaties ook relevant zijn op een nationaal en internationaal niveau. Dezelfde principes en valkuilen lijken bij beide abstractieniveaus terug te komen, waaronder het nut van het identificeren van kroonjuwelen, de uitdaging van zicht op informatie, en de problematiek rondom de versnippering van inzichten over verschillende spelers.

203 Zie de risicogebaseerde aanpak die ten grondslag ligt aan de in 2020 gepubliceerde EU-toolbox voor 5G-beveiliging (https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures).
204 Zie bijvoorbeeld het rapport 'Overzicht Financiële Stabiliteit Najaar 2020', de Nederlandsche Bank, 2020, p. 37, dat ook ingaat op de afhankelijkheid van dienstverleners in de financiële sector.
205 'Kaders voor code: beleid voor veilige digitale middelen', Centraal Planbureau (2020), https://www.cpb.nl/kaders-voor-code-beleid-voor-veilige-digitale-middelen.
206 Het probleem van onveilige hard- en software is het onderwerp van het rapport 'Roadmap veilige hard- en software' uit 2018 (https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software). In opdracht van Agentschap Telecom is in 2020 een rapport gepubliceerd met daarin een voorzet voor een set basiseisen voor IoT apparaten (https://www.agentschaptelecom.nl/documenten/rapporten/2020/08/26/onderzoeksrapport-essential-requirements-for-securing-iot-consumer-devices). De verwachting is dat in de EU vanaf de zomer van 2021 een aantal eisen gaat gelden voor de beveiliging van draadloze consumentenapparatuur. Daarnaast wordt er, in het kader van de Cybersecurity Act, gewerkt aan verschillende raamwerken voor cybersecurity certificering, waaronder voor clouddiensten.
207 Relevante publicaties met betrekking tot de meetbaarheid van nationale weerbaarheid zijn 'Advies CSR inzake focus en aanpak evaluatie NCSA' van de Cyber Security Raad (https://www.cybersecurityraad.nl/actueel/nieuws/2020/07/24/cyber-security-raad-adviseert-over-focus-en-aanpak-evaluatie-ncsa), de set rapporten 'Cybersecurity: a state-of-the-art review' van RAND Europe (https://hdl.handle.net/20.500.12832/2423 en https://hdl.handle.net/20.500.12832/3016), en het rapport 'Verkenning brede evaluatie NCSA' van InnoValor (https://hdl.handle.net/20.500.12832/2483).
208 J. Bosman, en B. Gijsen, 'Evolution of Internet interconnection', TNO, 2020. http://publications.tno.nl/publication/34637029/2Lu7U6/bosman-2020-evolution.pdf.
209 'Factsheet 5 adviezen voor veilig inkopen van clouddiensten, Nationaal Cyber Security Centrum (ncsc.nl).
210 https://searchnetworking.techtarget.com/answer/How-does-a-WAN-cloud-exchange-work.
211 NIB-Richtlijn. https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32016L1148&from=EN#d1e689-1-1
212 https://azure.microsoft.com/nl-nl/overview/what-is-a-cloud-provider/; https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-providers.
213 Wikipedia – Internet Service Provider.
214 T. Maurer en G. Hinck, 'Cloud Security: A Primer for Policymakers', Carnegie Endowment for International Peace, 2020.
215 T. Maurer en G. Hinck, 'Cloud Security: A Primer for Policymakers', Carnegie Endowment for International Peace, 2020.
216 T. Maurer en G. Hinck, 'Cloud Security: A Primer for Policymakers', Carnegie Endowment for International Peace, 2020.
217 Spreekwoord. Betekenis: Niemand (niets) is zonder gebreken.
218 https://www.theregister.com/2009/10/05/amazon_bitbucket_outage/
219 https://www.ncsc.nl/actueel/nieuws/2020/december/19/solarwinds-orion
220 https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
221 https://blog.stackpath.com/peering.
222 J. Latanicki, P. Massonet, S. Naqvi, B. Rochwerger en M. Villari, 'Scalable Cloud Defenses for Detection, Analysis and Mitigation of DDoS Attacks', Future Internet Assembly 2010, p. 127-137; M. Masdari en M. Jalali, 'A survey and taxonomy of DoS attacks in cloud computing. Security and Communication Networks', 2016, 9(16), p. 3724-3751.
223 J. Latanicki, P. Massonet, S. Naqvi, B. Rochwerger en M. Villari, 'Scalable Cloud Defenses for Detection, Analysis and Mitigation of DDoS Attacks', Future Internet Assembly 2010, p. 127-137.
224 J. Latanicki, P. Massonet, S. Naqvi, B. Rochwerger en M. Villari, 'Scalable Cloud Defenses for Detection, Analysis and Mitigation of DDoS Attacks', Future Internet Assembly 2010, p. 127-137; M. Masdari en M. Jalali, 'A survey and taxonomy of DoS attacks in cloud computing. Security and Communication Networks', 2016, 9(16), p. 3724-3751.
225 https://azure.microsoft.com/en-in/overview/what-is-virtualization/.
226 R. Chandramouli, 'Security recommendations for server-based hypervisor platforms' (No. NIST Special Publication (SP) 2018, 800-125A Rev. 1, National Institute of Standards and Technology; T. Maurer en G. Hinck, 'Cloud Security: A Primer for Policymakers', Carnegie Endowment for International Peace, 2020; P. Sheinidashtegol en M. Galloway, 'Performance impact of DDoS attacks on three virtual machine hypervisors', 2017 IEEE International Conference on Cloud Engineering (IC2E), p. 204-214, IEEE 2017.
227 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html; https://docs.microsoft.com/nl-nl/azure/availability-zones/az-overview

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 2021