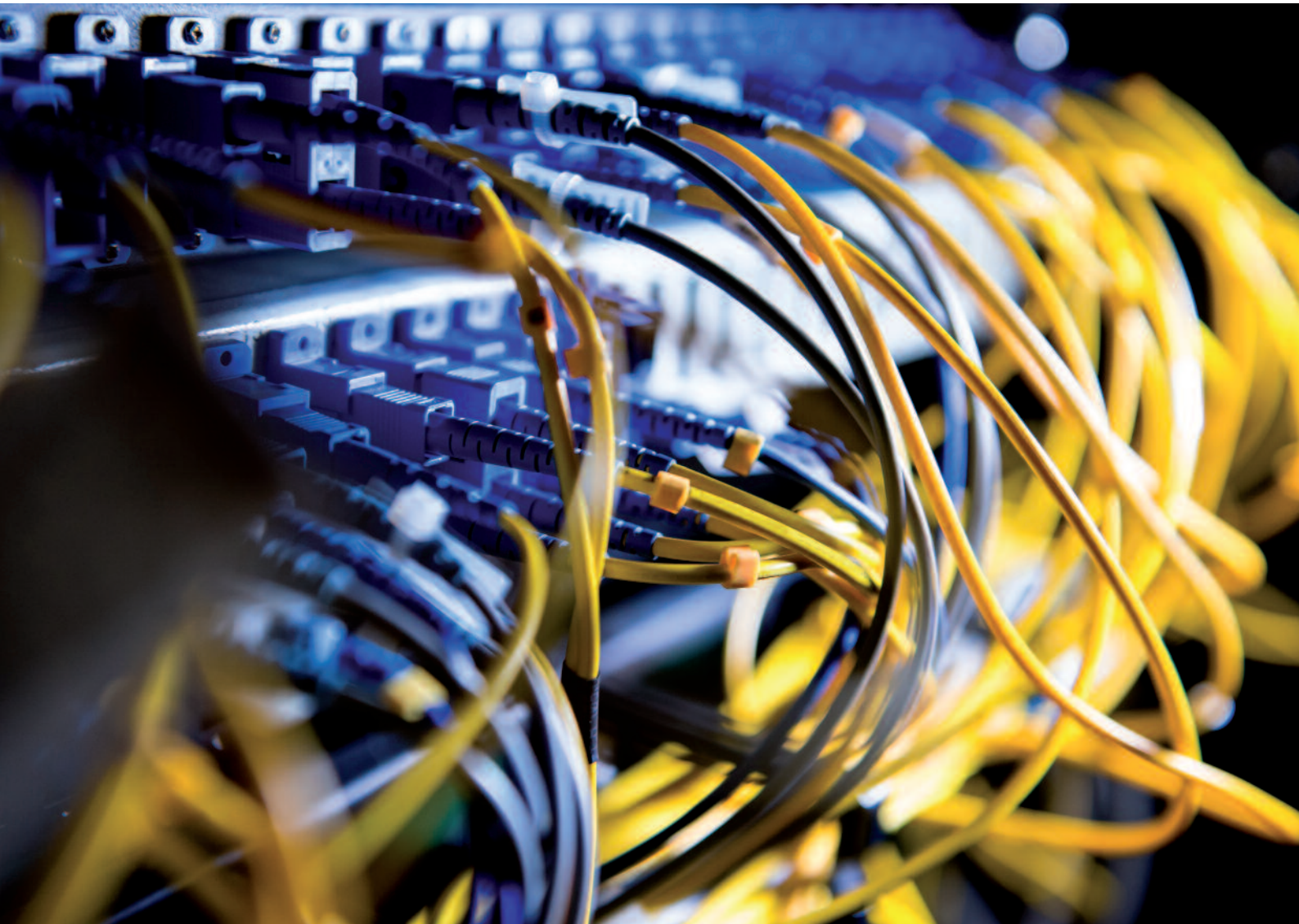
Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland

CSBN 2018



Colofon

Het Cybersecuritybeeld Nederland (CSBN) 2018 biedt inzicht in de dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid vastgesteld.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) beschermt Nederland tegen bedreigingen die de maatschappij kunnen ontwrichten. Samen met zijn partners binnen overheid, wetenschap en bedrijfsleven zorgt de NCTV ervoor dat de Nederlandse vitale infrastructuur veilig is én blijft.

Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC draagt bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving. Het NCSC is een onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Het CSBN is opgesteld door de NCTV en het NCSC en is tot stand gekomen op basis van de inzichten en de expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen. De NCTV heeft dankbaar gebruik gemaakt van hun expertise en informatie, zowel tijdens expertsessies als tijdens de validatie.

Inhoud

Aanvallers succesvol door ontbreken basismaatregelen

Cybersecurity onder druk

Het Cybersecuritybeeld Nederland (CSBN) 2018 biedt inzicht in de dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid gepubliceerd en komt tot stand in samenwerking met publieke en private partners.

Sabotage en verstoring door staten grootste dreiging voor nationale veiligheid

Staten voeren vanuit geopolitieke motieven steeds meer digitale aanvallen uit op andere landen, organisaties of individuen. Zij hebben als doel verwerving van strategische informatie via spionage, beïnvloeding van de publieke opinie of democratische processen en verstoring of zelfs sabotage van vitale systemen. Digitale aanvallen door staten zijn het afgelopen jaar concreet waargenomen. Opvallend is dat eenvoudige aanvalstechnieken succesvol worden ingezet en dat de Nederlandse ict-infrastructuur wordt misbruikt om aanvallen op andere landen uit te voeren.

Grote incidenten laten zien dat actoren het risico van nevenschade niet voorzien of mogelijk zelfs accepteren. In het buitenland heeft nevenschade geleid tot maatschappelijke verstoring, in Nederland tot economische schade. Door de afhankelijkheid van (buitenlandse) partijen groeit de kwetsbaarheid voor spionage, verstoring en sabotage. Buitenlandse partijen kunnen in specifieke landen wettelijk verplicht worden mee te werken aan het ondersteunen van operaties zoals spionage of voorbereidingen voor sabotage.

Beroepscriminelen blijven zich ontwikkelen op digitaal vlak. Daardoor neemt de dreiging verder toe. Vanuit een professionele criminele dienstensector worden hulpmiddelen geleverd waarmee minder toegeruste actoren digitale aanvallen kunnen uitvoeren.

Aanvallers blijven succesvol door ontbreken basismaatregelen

De digitale weerbaarheid van Nederland staat onder druk. Organisaties worden succesvol aangevallen met eenvoudige methoden. De afgelopen periode laat zien dat incidenten voorkomen hadden kunnen worden of dat de schade beperkt had kunnen worden met behulp van basismaatregelen. Die worden door lang niet alle organisaties getroffen. Onder andere tekortkomingen in configuraties en het niet tijdig implementeren van beveiligingsupdates zorgen ervoor dat aanvallers succesvol zijn.

De weerbaarheid staat verder onder druk door een toenemende complexiteit en connectiviteit in het ict-landschap en in voorkomende gevallen door te weinig aandacht voor digitale veiligheid. Tegelijkertijd werken onveilige producten en diensten drempelverlagend voor aanvallers. Wereldwijd zijn verscheidene malen leverancierskketens misbruikt om aanvallen uit te voeren. Ook in Nederland heeft dit geleid tot schade.

Blijvend functioneren samenleving en economie afhankelijk van cybersecurity

Digitale veiligheid is noodzakelijk voor het functioneren van de sterk gedigitaliseerde Nederlandse samenleving en economie en als barrière tegen digitale dreigingen. De gevolgen van aanvallen en van uitval van systemen kunnen groot en zelfs maatschappij-ontwrichtend zijn. Kosten en baten van cybersecurity liggen niet altijd bij dezelfde partij, mede daarom doen partijen concessies aan het belang van digitale veiligheid. Dit brengt op nationaal niveau risico's met zich mee en kan verstrekkende gevolgen hebben. Het vertrouwen in de digitale samenleving wordt ondergraven door onder andere succesvolle digitale aanvallen. Diefstal van waardevolle informatie kan het vertrouwen in het economisch verkeer schaden en in potentie de Nederlandse economie aantasten. Spionage, verstoring en sabotage door staten ondermijnen Nederlandse belangen.

De digitale dreiging is permanent. Cyberaanvallen zijn nog steeds profijtelijk, laagdrempelig en weinig riskant voor aanvallers. In de context van recente geopolitieke ontwikkelingen zullen staten naar verwachting digitale aanvallen instrumenteel blijven inzetten en mogelijk op grotere schaal toepassen. In combinatie met de vergaande en toenemende digitalisering van de samenleving past dit in de beweging van een verdere toename van het risico op maatschappelijke ontwrichting.

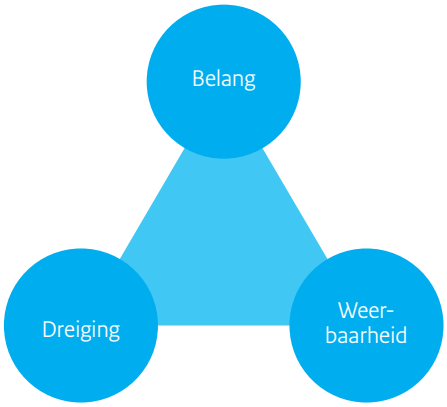
Leeswijzer

Het CSBN 2018 biedt inzicht in de dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de nationale veiligheid. Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ict te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan.[1] Die schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.

Het CSBN is tot stand gekomen op basis van de inzichten en expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen. De ontwikkelingen zijn in kwalitatieve vorm beschreven. Indien in betrouwbare vorm beschikbaar wordt dit ondersteund met een kwantitatieve onderbouwing of een verwijzing naar bronnen.

Het monitoren van de dreigingen, de belangen en de weerbaarheid is een continu proces, met het CSBN als een van de jaarlijkse resultaten. Zaken die ten opzichte van vorige edities van het CSBN niet of nauwelijks zijn veranderd, zijn niet of slechts beknopt beschreven. Aan de analyse in het CSBN ligt de driehoek dreiging, belang en weerbaarheid ten grondslag. Deze drie factoren bepalen in samenhang het risico.

Figuur 1 **Model belang, dreiging en weerbaarheid**



De hoofdvragen van het CSBN 2018 zijn:

- Welke dreigingen kunnen de beschikbaarheid, vertrouwelijkheid en integriteit van informatie, informatiesystemen of -diensten aantasten, of hebben deze aangetast in de rapportageperiode mei 2017 tot en met april 2018? Welke dreigingen vormen het grootste risico voor de nationale veiligheid?
- Wat zijn de potentiële gevolgen voor de nationale veiligheid indien geïdentificeerde dreigingen zich manifesteren?
- Welke combinaties van kwetsbaarheden en middelen hebben zich binnen de rapportageperiode mei 2017 tot en met april 2018 mondiaal gemanifesteerd en (kunnen) worden toegepast in Nederland?
- In welke mate is Nederland en de nationale veiligheid van Nederland weerbaar tegen de ingezette of inzetbare middelen, te misbruiken kwetsbaarheden en het manifest worden van dreigingen?
- In hoeverre zijn er onderliggende oorzaken of factoren te identificeren die ten grondslag liggen aan het dreigingsbeeld?

Hoofdstuk 1 beschrijft de kernproblematiek, de onderliggende oorzaken en factoren die ten grondslag liggen aan het dreigingsbeeld. In hoofdstuk 2 wordt de dreiging nader beschreven en toegelicht. Het belang voor de samenleving en de nationale veiligheid wordt beschreven in hoofdstuk 3. Het vierde hoofdstuk bevat het jaarbeeld over de rapportageperiode mei 2017 tot en met april 2018 en beoogt de meest relevante ontwikkelingen uit te lichten. De weerbaarheid van Nederland komt in het vijfde en laatste hoofdstuk aan de orde. De bijlagen bieden tot slot een overzicht van de door het NCSC afgehandelde incidenten en een toelichting op de gebruikte afkortingen.

Cyberaanvallen veelal profijtelijk, laagdrempelig en weinig riskant voor actor

1 Kernproblematiek

Zes kernproblemen die elkaar beïnvloeden liggen ten grondslag aan het dreigingsbeeld. Een cyberaanval is veelal profijtelijk, laagdrempelig en weinig riskant voor een actor. De eenvoudige toegankelijkheid van aanvalsmiddelen en het gebruik van onveilige producten en diensten zijn oorzaken van deze laagdrempeligheid. Belangentegenstellingen leiden tot concessies aan de weerbaarheid. De toenemende complexiteit en connectiviteit zetten de weerbaarheid verder onder druk. Tot slot hebben buitenlandse producenten en dienstverleners een positief en negatief effect op weerbaarheid.

Cyberaanvallen veelal profijtelijk, laagdrempelig en weinig riskant voor actor

Ongeacht het motief – persoonlijk, economisch, ideologisch of geopolitiek – is een cyberaanval al jaren een profijtelijk middel voor de realisatie van uiteenlopende doelen van actoren. Door de nog steeds toenemende digitalisering neemt de potentiële schade die een actor kan berokkenen met een digitale aanval en het profijt dat hij ervan kan hebben verder toe.

Vele soorten digitale aanvallen zijn laagdrempelig uit te voeren als gevolg van de hieronder beschreven fundamentele oorzaken. Daardoor hoeft een aanvaller zelf lang niet altijd over veel capaciteiten te beschikken voor een aanval. Zelfs actoren die daarover wel beschikken, kunnen vaak al volstaan met eenvoudige aanvalsvormen.

Een digitale aanval is vaak weinig riskant om uit te voeren. De kans bestaat dat de aanval lange tijd onopgemerkt blijft. Als de aanval wel ontdekt wordt, is de attributie aan en de opsporing van de actoren complex.[2] Indien attributie wel mogelijk is, blijft dat in vele gevallen zonder consequenties, zeker in het geval van statelijke of staatsgelieerde actoren. Wel lijkt er een kentering te hebben plaatsgevonden in het publiekelijk attribueren van digitale aanvallen door overheden. Verscheidene landen hebben aanvallen toegeschreven aan andere landen.

Aanvalsmiddelen eenvoudig toegankelijk door aanvalsfacilitatoren

Digitale aanvallen zijn onder meer laagdrempelig uit te voeren door diensten van aanvalsfacilitatoren. Deze dienstverleners stellen infrastructuur, hulpmiddelen en technieken voor digitale aanvallen tegen betaling beschikbaar. Minder ervaren of minder toegeruste actoren kunnen hiermee digitale aanvallen uitvoeren. De laagdrempelige toegankelijkheid van aanvalsmiddelen leidt tot een vergroting van de dreiging.

Onveilige producten en diensten de achilleshiel van digitale veiligheid

Digitaal onveilige producten en diensten zijn een fundamentele oorzaak van vele incidenten.[3] Onveilige producten en diensten werken drempelverlagend omdat deze het voor aanvallers makkelijker maken succesvolle aanvallen uit te voeren. De onveiligheid kan ontstaan omdat leveranciers geen updates (meer) beschikbaar stellen of omdat deze updates niet eenvoudig te installeren zijn. Ook als deze wel beschikbaar zijn, worden zij niet altijd ingezet bij organisaties. Voor producenten zijn er weinig economische drijfveren om veilige hard- en software te produceren. Hierdoor ontstaat een belangentegenstelling tussen enerzijds het bedrijfseconomische belang van producenten en het cybersecuritybelang van de maatschappij anderzijds.

Belangentegenstellingen leiden tot concessies

Ook in brede zin leiden belangentegenstellingen tot concessies aan het cybersecuritybelang. Burgers, bedrijven, sectoren en overheden zullen altijd een belangenafweging moeten maken. Cybersecuritymaatregelen kosten immers tijd en geld, twee schaarse middelen die ook anders ingezet kunnen worden. Soms ligt het belang van digitale veiligheid direct in het verlengde van andere belangen, soms ontstaan er tegenstellingen. Deze bestaan binnen organisaties, bijvoorbeeld een tegenstelling tussen gebruiksgemak voor het individu en het cybersecuritybelang, maar ook tussen organisaties. Een ongelijkheid in de verdeling van kosten en baten is hier een van de oorzaken van.

Toenemende complexiteit en connectiviteit zet weerbaarheid onder druk

Naarmate de complexiteit en connectiviteit toenemen, wordt het steeds uitdagender om een weerbare digitale infrastructuur te realiseren. Enerzijds zorgen de organische groei en de relatief lange levensduur van systemen voor een steeds ingewikkelder landschap. Anderzijds maakt het toegenomen gebruik van gedeelde voorzieningen, zoals clouddiensten, in de vorm van losse bouwblokken, dat het overzicht lastiger te bewaren is. Waar in het verleden diensten binnen een organisatie ingericht werden, worden ze nu vaker bij verschillende partijen ingekocht en extern uitgevoerd. Regie op het ict-landschap blijft binnen de organisatie, terwijl de uitvoering ervan versnipperd raakt over meerdere partijen. Dit zorgt voor nieuwe afhankelijkheden en een vergroting van het aanvalsoppervlak.

De digitale infrastructuur is complex, niet alle essentiële onderdelen zijn even robuust en de afhankelijkheid van individuele onderdelen is groot. Bepaalde software wordt generiek door ontwikkelaars en leveranciers gebruikt als bouwsteen voor hun werk. Sommige populaire protocollen voor gegevensuitwisseling via het internet zijn decennia oud en niet bestand tegen hedendaagse aanvallen.

Buitenlandse producenten en dienstverleners positief en negatief voor de weerbaarheid

Nederlandse organisaties zijn sterk afhankelijk van een beperkt aantal buitenlandse leveranciers van producten en diensten. Hoewel deze bedrijven meer middelen hebben om zich tegen aanvallen te wapenen, kan de maatschappelijke impact bij verstoringen groot zijn, omdat veel verschillende diensten afhankelijk zijn van een klein aantal aanbieders.
De producten of diensten van (buitenlandse) leveranciers kunnen naast verstoord ook gecompromitteerd worden door actoren, met of zonder medeweten van deze leverancier. Daarnaast zijn producenten en dienstverleners onderworpen aan de wet- en regelgeving van het land waarin zij mede gevestigd zijn. Zij zouden door overheden in het buitenland gedwongen kunnen worden tot een vorm van medewerking aan bijvoorbeeld (politieke, militaire of economische) inlichtingenoperaties. Indien overheden besluiten alleen producten en diensten van het eigen land of bondgenoten te accepteren, dan zal dit leiden tot fragmentatie van het internet.

Staten vormen grootste digitale dreiging

2 Dreiging

De digitale dreiging is permanent. Digitale aanvallen van statelijke actoren met als doel spionage, beïnvloeding, verstoring en sabotage, vormen de grootste digitale dreiging voor de nationale veiligheid. Daarnaast hebben de activiteiten van cybercriminelen grote impact. Het dreigingslandschap lijkt het afgelopen jaar niet fundamenteel veranderd. Het is wel diverser geworden door een aantal verschuivingen, waarvan sommige reeds enkele jaren geleden ingezet zijn. In de dreigingsmatrix in dit hoofdstuk wordt het complete dreigingsbeeld weergegeven. Daarnaast passeren de opvallendste elementen van het dreigingsbeeld de revue.

Grenzen tussen actoren vervagen

Het aantal actoren dat digitale aanvallen uitvoert, is de afgelopen jaren toegenomen.[4] Ook zijn er nu actoren actief in het digitale domein die een aantal jaren geleden nog geen rol van betekenis hadden.[5] Het is voor hen relatief eenvoudig om capaciteiten in te zetten, door de steeds bredere toegankelijkheid van hulpmiddelen om digitale aanvallen uit te voeren.

Om het dreigingsbeeld inzichtelijk te maken, wordt onderscheid gemaakt tussen verschillende categorieën aanvallers die ieder een eigen werkwijze en motivatie hebben (zie dreigingsmatrix). In de praktijk zijn de grenzen tussen verschillende actoren steeds minder zichtbaar.[6] Zo kunnen verschillende actorgroepen gebruik maken van dezelfde middelen en technieken. Dit komt onder andere door het doorsijpeleffect, waarbij hoogwaardige aanvalstechnieken breed bekend worden of in verkeerde handen vallen. Een voorbeeld uit 2017 zijn de door de hackergroep Shadow Brokers gelekte hulpmiddelen die toegeschreven worden aan de Amerikaanse National Security Agency (NSA). Een specifiek hulpmiddel (de exploit EternalBlue) is vervolgens ingezet in de WannaCry-aanval.[7]

Een ander voorbeeld van het vervagen van de grenzen, zijn de schijnbare technische overeenkomsten tussen de Petya ransomware en de NotPetya sabotagesoftware. In de media zijn voorbeelden beschreven van actoren die een andere hackersgroep aanvallen en hun opbrengst buitmaken.[8] Aanvalsmiddelen verspreiden zich tegenwoordig over het hele spectrum van aanvallers, van staten tot criminelen. De grenzen tussen actoren vervagen ook doordat verschillende actorgroepen samenwerken, actoren zich bewust voordoen als iemand anders, of valse sporen creëren in de richting van andere actoren.[1]

Het aanwijzen van de actor achter een digitale aanval, attributie, is nog complexer wanneer de actoren moeilijk van elkaar te onderscheiden zijn. Hoe geavanceerd een aanval is en welke hulpmiddelen gebruikt zijn, is van invloed op het aantal aanknopingspunten voor het herkennen van de actor. Het vervagen van grenzen tussen actoren heeft als consequentie dat de kans op onjuiste attributie groter wordt, met mogelijk grote gevolgen, zoals bijvoorbeeld verdere escalatie in een conflictsituatie.[9]

1 Een recent voorbeeld van een valsevlagoperatie is de cyberaanval op de organisatoren van de Olympische Spelen in Zuid-Korea, waarbij de indruk werd gewekt dat het om een aanval uit Noord-Korea ging. Als gevolg van de aanval was de website van de Olympische Spelen uit de lucht en werkten uitzendkanalen niet. In open bronnen wordt de aanval toegeschreven aan Rusland, mogelijk gemotiveerd door hun uitsluiting van de Olympische Spelen vanwege dopingschandalen.

Dreigingsmatrix

De dreigingsmatrix geeft een inzicht in de dreigingen die uitgaan van verschillende actoren tegen verschillende doelwitten. De tabel is niet uitputtend en bevat niet alle dreigingen die voorstelbaar zijn, maar beperkt zich tot de dreigingen waarvan ingeschat wordt dat actoren voldoende intentie en middelen hebben of waarvan eerder activiteiten zijn waargenomen. De dreigingsmatrix heeft enkele conceptuele veranderingen ondergaan ten opzichte van voorgaande jaren. Enerzijds zijn vitale processen en aanbieders toegevoegd als aparte doelwitcategorie. Anderzijds is de actortypologie aangepast. De volgende dreigingen worden onderscheiden:

- Verstoring: het opzettelijk tijdelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten.
- Sabotage: het opzettelijk, zeer langdurig, aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten, mogelijk leidend tot vernietiging.
- Informatiemanipulatie: het opzettelijk wijzigen van informatie; aantasting van de integriteit van informatie.
- Informatiediefstal: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
- Spionage: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
- Systeemmanipulatie: het aantasten van informatiesystemen of -diensten; gericht op de vertrouwelijkheid of integriteit van informatiesystemen of -diensten. Deze systemen of diensten worden daarna ingezet om andere aanvallen uit te voeren.
- Storing/uitval: aantasting van de integriteit of beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.
- Lek: aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.

	Overheid	Vitaal	Privaat	Burgers
Staten/ staatsgelieerd	Spionage Informatiemanipulatie	Sabotage Verstoring Spionage	Spionage Systeemmanipulatie	Spionage
Criminelen	Verstoring Systeemmanipulatie Informatiediefstal	Verstoring Systeemmanipulatie	Informatiediefstal Informatiemanipulatie Verstoring Systeemmanipulatie	Informatiemanipulatie Verstoring Systeemmanipulatie Informatiediefstal
Terroristen	Sabotage	Sabotage		
Hacktivisten	Verstoring Informatiemanipulatie	Verstoring Informatiemanipulatie	Verstoring Informatiediefstal Informatiemanipulatie	
Cybervandalen en scriptkiddies	Verstoring Informatiediefstal	Verstoring Informatiediefstal	Verstoring Informatiediefstal	Informatiediefstal
Insiders	Informatiediefstal Verstoring	Informatiediefstal Verstoring	Informatiediefstal Verstoring	
Niet opzettelijk handelen	Storing/uitval Lek	Storing/uitval Lek	Storing/uitval Lek	Lek

Deze dreigingsmatrix is gebaseerd op de actortypologie in: M. de Bruijne, M. van Eeten, C. Hernandez Ganan, W. Pieters, Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment (TU Delft 2017). Verschillende criminele actoren zijn samengevoegd omdat er qua dreiging geen kenmerkend onderscheid aanwezig was. De in de methode onderscheiden statelijke en staatsgelieerde actoren zijn samengevoegd vanwege onvoldoende beschikbare informatie om het onderscheid te kunnen maken.

Staten vormen grootste digitale dreiging

Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage). Er zijn het afgelopen jaar verscheidende digitale aanvallen door staten waargenomen. Deze hadden impact op de nationale veiligheid.[10]

Digitale aanvalsmiddelen worden veelvuldig ingezet

Digitale aanvallen vormen inmiddels een vast onderdeel van het scala aan middelen dat staten kunnen inzetten om hun geopolitieke belangen te beschermen. Er zijn nog maar weinig interstatelijke conflictsituaties waarin geen digitale middelen worden ingezet. Daarbij spelen ook economische belangen mee. Los van deze conflicten doen landen aan economische spionage, bijvoorbeeld om de concurrentiepositie van hun economie te verbeteren of om snel innovatieve kennis te verwerven. De grotere bereidheid van landen om digitale middelen in te zetten, gaat samen met een toename van de impact van digitale aanvallen.[11] Cyberaanvallen kunnen een grote impact en omvangrijke neveneffecten hebben[12] (voorbeelden zijn WannaCry en NotPetya).

Het gebruik van derde partijen

Staten kunnen bij de voorbereiding en uitvoering van digitale aanvallen gebruik of misbruik maken van andere partijen. Deze partijen hoeven zich niet bewust te zijn van het misbruik. Staten kunnen geavanceerde aanvalshulpmiddelen kopen, zodat zij niet zelf hoeven te investeren in de ontwikkeling ervan.[13] Ook kunnen staten de voorbereiding en uitvoering van digitale aanvallen 'uitbesteden' aan een derde partij.[14] Tot slot kunnen ze de producten en diensten van een derde partij misbruiken voor het uitvoeren van aanvallen. Zo compromitteerde de actor achter de NotPetya-aanval softwarebedrijf M.E.Doc om malware te verspreiden via legitieme updates.

Daarnaast kunnen aanvallers, soms op eenvoudige wijze, gebruik maken van legitieme hulpmiddelen, eigenschappen van systemen of eigenschappen van (cloud)diensten om binnen te dringen in de systemen van slachtoffers.[15] Actoren maken hierbij misbruik van het vertrouwen van consumenten in ict-producten. Deze aanvallen zijn vaak moeilijk te detecteren.

Significante schade NotPetya

Op 27 juni 2017 werd de wereld opgeschrikt door de snelle verspreiding van malware die bestanden leek te gijzelen. De malware werd door Kaspersky Lab NotPetya (ook wel New Petya, Nyetya, ExPetr) genoemd.[16] De naam refereert aan de ransomware die zich in mei 2016 verspreidde onder de naam Petya. Veel partijen dachten aanvankelijk dat er overeenkomsten mee waren. Uiteindelijk bleek de NotPetya-malware significant anders dan Petya of WannaCry (dat zich in mei 2017 verspreidde).

NotPetya is gebaseerd op de exploit EternalBlue die toegeschreven is aan de NSA.[17] Daar was in maart 2017 al een patch voor verkrijgbaar.[18] Wat in eerste instantie ransomware leek te zijn, bleek wiperware (software die gegevens wist) omdat er geen mogelijkheid was om de gegijzelde bestanden daadwerkelijk terug te krijgen.[19]

De malware verspreidde zich snel over verschillende landen, waaronder Oekraïne (met 80 procent van de infecties[20]), Frankrijk, Denemarken, Engeland en de Verenigde Staten.[21] In Oekraïne vielen overheidssystemen uit, reed de metro niet meer, ondervond het vliegveld in Kiev hinder en hadden elektriciteitscentrales problemen.[22] Maersk, een Deens maritiem transportbedrijf dat ook gevestigd is in de Rotterdamse haven, ondervond ook overlast van de NotPetya-aanval. Uiteindelijk leed Maersk wereldwijd zo'n 300 miljoen euro schade door de aanval[23] en moest het 45.000 computers opnieuw installeren.[24] Ook de Nederlandse pakketvervoerder TNT Express ondervond problemen als gevolg van geïnfecteerde computers.[25]

Na onderzoek bleek dat de malware zich verspreid had via een software-update voor M.E.Doc, boekhoudsoftware afkomstig uit Oekraïne.[26] Hiermee was de leverancierssketen van de afnemers van de boekhoudsoftware gecompromitteerd. De software kon zich snel verspreiden en veiligheidsbarrières omzeilen wanneer de laatste patches voor de exploit EternalBlue niet geïnstalleerd waren.

De NotPetya-aanval is door onder andere de Verenigde Staten, Denemarken en het Verenigd Koninkrijk geattribueerd aan Rusland.[27] Het motief zou de verstoring Oekraïense zijn, zoals in het verleden ook al gebeurde met de verspreiding van de zogenoemde BlackEnergy-malware.[28] Dit zou passen binnen de geopolitieke spanningen tussen Rusland en Oekraïne.

Inzet eenvoudige technieken

Statelijke actoren hebben veel expertise en zijn in staat om geavanceerde aanvallen uit te voeren. Desondanks is duidelijk geworden dat staten ook veelvuldig gebruik maken van eenvoudige aanvalstechnieken. Zo maakt volgens openbare rapporten Rusland veel gebruik van (spear)phishing.[29] Hetzelfde geldt voor Noord-Korea, dat ook malware via e-mail verspreidt.[30] China heeft in 2017 op eenvoudige wijze misbruik gemaakt van LinkedIn om in Duitsland mensen te benaderen, om hen vervolgens te kunnen rekruteren.[31] Staten beseffen net als andere actoren dat eenvoudige technieken zeer effectief zijn.[32] Een aanvaller probeert doelwitten te verleiden om gevoelige of vertrouwelijke informatie weg te geven, die weer gebruikt kan worden bij een vervolgaanval of voor andere doeleinden.

Het veelvuldig gebruik van eenvoudige aanvalstechnieken door statelijke actoren laat zien dat deze voldoende doelgericht en doelmatig zijn. Tegen eenvoudige aanvalstechnieken kunnen drempels opgeworpen worden, die potentiële doelwitten van aanvallen minder kwetsbaar en ook minder interessant maken. Maatregelen die tot de 'basishygiëne' van ict-systemen en -netwerken behoren, een basisniveau van cybersecurity, verhogen de weerbaarheid tegen digitale aanvallen aanzienlijk, ook als het gaat om aanvallen van statelijke actoren.[33] Hiermee wordt de kans op en de impact van deze dreiging gereduceerd.

Aanvallers accepteren nevenschade of voorzien deze niet

Wereldwijd hebben enkele aanvallen een grote impact gehad. Naast NotPetya verspreidde WannaCry zich in mei 2017 in 150 landen[34] met een grote economische en maatschappelijke impact. In het Verenigd Koninkrijk werden bijvoorbeeld van vele ziekenhuizen de processen verstoord. Deze aanvallen zijn door andere landen geattribueerd aan statelijke actoren. Aanvallers lijken het risico te accepteren dat nevenschade veroorzaakt wordt of ze voorzien deze nevenschade niet,[35] bijvoorbeeld door de infectie van de leveranciersketen of door het gebruik van een worm die in staat is zichzelf te verspreiden. Deze technieken brengen het risico van een ongecontroleerde verspreiding met zich mee.

Vanuit het perspectief van de nationale veiligheid kunnen ongecontroleerde en moeilijk voorspelbare aanvallen met een destructieve werking potentieel een maatschappij-ontwrichtende impact hebben. Dit kan vooral wanneer vitale processen getroffen worden, al dan niet per ongeluk als neveneffect, en zeker indien het meerdere systemen of processen betreft.

Leveranciersketens verhogen kwetsbaarheid

Het afgelopen jaar is er bij verschillende aanvallen gebruik gemaakt van een leveranciersketen (supply chain) om schadelijke software te verspreiden. Een van de meest prominente voorbeelden is NotPetya dat zich verspreidde via een update van Oekraïense boekhoudsoftware. Deze aanvalswijze heeft een aantal voordelen voor de actor. Ten eerste zorgt het gebruik van een vertrouwde leverancier als bron van verspreiding dat bestaande beveiligingsmaatregelen bij het doelwit grotendeels ontweken kunnen worden. Ook is de actor in staat om te bepalen wie precies besmet wordt, van één specifiek doelwit tot en met alle afnemers van een bepaalde leverancier. Ten derde is het bij een aanval via de supply chain complex om de beoogde doelwitten en doelen van de aanval te bepalen. Dit maakt attributie moeilijker.

Nederlandse organisaties zijn sterk afhankelijk van een beperkt aantal buitenlandse leveranciers van producten en diensten. Hoewel deze bedrijven meer middelen hebben om zich tegen aanvallen te wapenen, kan de maatschappelijke impact bij verstoringen groot zijn, omdat veel verschillende diensten afhankelijk zijn van een klein aantal aanbieders.[36]

Naast verstoringen kunnen producten of diensten van (buitenlandse) leveranciers echter ook, met of zonder medeweten van deze leverancier, gecompromitteerd worden door actoren. Vanwege de leverancierssketens zijn producenten en dienstverleners een aantrekkelijk doelwit voor actoren. Daarnaast zijn producenten en dienstverleners onderworpen aan de wet- en regelgeving van het land waarin zij gevestigd zijn en zouden door overheden in het buitenland gedwongen kunnen worden tot een vorm van medewerking aan bijvoorbeeld spionage of voorbereiding voor sabotage. Dit vormt een risico voor de nationale veiligheid. In dat kader heeft het kabinet de Kamer geïnformeerd dat, als voorzorgsmaatregel, Kaspersky antivirussoftware bij de Rijksoverheid zal worden uitgefaseerd. Bedrijven en organisaties met vitale diensten en processen en bedrijven die vallen onder de Algemene Beveiligingseisen Defensie Opdrachten (ABDO) is geadviseerd hetzelfde te doen.

Dit jaar is gebleken dat supplychain-aanvallen effectief en destructief zijn. De verspreiding en impact van dergelijke aanvallen zijn moeilijk te voorspellen, zeker wanneer de actor accepteert dat de aanval ook andere doelwitten kan raken. Het is de verwachting dat actoren deze methode vaker zullen inzetten.[37]

Actoren geïnteresseerd in persoonsgegevens

In de rapportageperiode speelden gestolen en gelekte persoonsgegevens een opvallende rol.[38] Een breed scala aan actoren (statelijk, crimineel, hactivist) heeft interesse in persoonsgegevens. Om die te verwerven worden aanvallen uitgevoerd op de partijen die beschikken over deze gegevens, zoals dienstverleners, overheden en onderwijsinstellingen. Persoonsgegevens kunnen gebruikt worden voor criminele activiteiten, zoals creditcard- en identiteitsfraude, maar ook voor spionageactiviteiten. Hiervan zijn ook voorbeelden in Nederland bekend.[39]

Daarnaast kunnen fouten of storingen leiden tot het lekken van persoonsgegevens, zoals bijvoorbeeld het opslaan van gegevens in publiek toegankelijke cloudtoepassingen.[40] Ook in Nederland speelt dit probleem, zo werden in 2017 tienduizend datalekken gemeld bij de Autoriteit Persoonsgegevens (AP).[41] Hierbij is van belang dat sommige persoonsgegevens, zoals geboortedatum en burgerservicenummer, onveranderlijk zijn. Dat maakt het minder eenvoudig om de impact van een lek van deze gegevens te verminderen.

Dreiging terroristen en hacktivisten stabiel

Het dreigingsbeeld is op een aantal punten stabiel. Zo is de dreiging die uitgaat van terroristen en hacktivisten onveranderd. Jihadisten zijn al jaren actief op het internet, bijvoorbeeld op het gebied van propaganda en fondsenwerving, maar ze hebben vooralsnog geen terroristische aanvallen gepleegd met behulp van digitale middelen. De ambitie is aanwezig, maar die is nog niet omgezet in concrete intenties of de ontwikkeling van expertise en capaciteiten.[42] Voor terroristische groeperingen blijft het plegen van fysieke aanslagen de prioriteit of eenvoudiger om uit te voeren. Hacktivisten zijn wel actief, bijvoorbeeld met bekladding van websites, defacements, en datadiefstal, maar ook zij vormen op dit moment geen dreiging die impact heeft op de nationale veiligheid.[43]

Aanvalsfacilitatoren vergroten toegankelijkheid aanvalsmethoden

Aanvalsfacilitatoren vormen bijzondere categorieën in het cyberdomein. Zij voeren zelf geen digitale aanvallen uit, maar spelen wel een rol in de dreiging.[44] Enerzijds zijn dit criminelen die gestolen informatie, zoals creditcardgegevens of persoonsgegevens, verhandelen voor financieel gewin. Ze verkopen informatie die vervolgens gebruikt kan worden voor een aanval. Anderzijds zijn dit actoren die faciliteiten realiseren voor aanvallers, bijvoorbeeld door botnets te verhuren. Op zowel de open als de meer gesloten delen van het internet kunnen informatie en aanvalsmiddelen voor relatief lage bedragen gekocht worden. Daarmee stellen deze producten en diensten actoren met beperkte capaciteiten in staat om toch digitale aanvallen uit te voeren. De facilitatoren hebben een drempelverlagend effect en ze vergroten de toegankelijkheid tot aanvalsmethoden.

DDoS-aanvallen in Nederland januari 2018

In januari 2018 kreeg Nederland te maken met DDoS-aanvallen op verschillende overheids- en financiële instellingen met als gevolg dat zij tijdelijk slecht bereikbaar waren voor klanten. Onder andere de Belastingdienst, DigiD en enkele banken werden getroffen. In de media werd gespeculeerd over de actor achter de aanval.[45]

Terwijl de DDoS-aanvallen aanhielden en de verschillende financiële instellingen tijdelijk slecht bereikbaar waren, werd er een opsporingsonderzoek uitgevoerd. Op 1 februari 2018 werd een man van 18 jaar uit Noord-Brabant gearresteerd op verdenking van het uitvoeren van de DDoS-aanvallen.[46] Volgens zijn verklaring kon hij de aanvallen uitvoeren door 40 euro te betalen voor een zogenoemde stresser,[47] een dienst die ingeschakeld kan worden om systemen te testen op de belastbaarheid.

Actoren die cybercriminele diensten aanbieden, besteden veel aandacht aan de verbetering van hun dienstverlening. Cybercrime-as-a-service[II] (CaaS) bestaat al langer,[48] maar is breder toegankelijk geworden. De middelen die verhuurd worden, zijn veelzijdig en geavanceerd en groeien sterk in aantal.[49] De koppeling van steeds meer alledaagse apparaten aan het internet, het internet of things (IoT), speelt hierin een rol. Talloze IoT-apparaten zijn besmet met malware, onder andere om botnets te creëren die multifunctioneel kunnen worden ingezet. De sector vertoont overeenkomsten met een traditionele markt van vraag en aanbod, waar onder meer differentiatie in prijs, kwaliteit en dienstverleningsniveau een belangrijke rol spelen en waarin taken worden gespecialiseerd.

Uit de ontwikkelingen van de afgelopen jaren blijkt dat de CaaS-sector continu innoveert en nieuwe, lucratieve manieren ontwikkelt om geld te verdienen. Dit blijkt onder meer uit de continue doorontwikkeling van producten en diensten. Denk hierbij bijvoorbeeld aan ransomware. Dit is niet nieuw, maar wordt continu doorontwikkeld. Cryptomining en cryptojacking[III] is een relatief nieuwe ontwikkeling.[50] Deze toepassing is gericht op het verdienen van geld door de rekenkracht van computers te gebruiken voor het delven (mining) van cryptografische munten. In eerste instantie door het inbreken op wifi-netwerken[51], computers[52] en websites[53], in tweede instantie door op websites de gebruiker een keuze te geven tussen advertenties of cryptomining.[54] Een van de partijen is Coinhive[55] die cryptominingcode als dienst aanbiedt voor website-eigenaren. Cryptojacking is een aantrekkelijk verdienmodel voor criminelen dat weinig risico's met zich meebrengt.

II De omschrijving cybercrime-as-a-service verwijst naar de traditie van dienstverleners om 'as-a-service' achter de titel van hun product te zetten. Zo worden op de reguliere markt diensten als platform-as-a-service en software-as-a-service geleverd.

III Er wordt over cryptojacking gesproken als de cryptominingsoftware zonder toestemming ingezet wordt.

De cybercriminele dienstensector lijkt, door het verdergaand toegankelijk maken van midden, professioneler te worden.[56] Dit leidt tot een vergroting van de dreiging, die op lange termijn het vertrouwen in de economie en de digitale infrastructuur kan schaden.

Uitval en storing

Naast aanvallen door actoren vinden er incidenten plaats die per ongeluk gebeuren, maar wel een dreiging vormen voor systemen en de informatie die zij bevatten: uitval en storingen. Deze dreigingen kunnen een significante impact hebben. Zo was er begin april 2018 een grote storing bij Eurocontrol, de organisatie verantwoordelijk voor het coördineren van routes van passagiersvluchten in Europa.[57] Door de storing liep ten minste 10 procent van de vluchten vertraging op. Volgens een rapport[58] uit maart 2018 van de US Federal Communications Commission (FCC) werd de grootste Amerikaanse telefoonstoring ooit veroorzaakt door een softwarefout. Op 4 oktober 2016 heeft het Amerikaanse telefoonnetwerk te kampen gehad met een 84 minuten durende storing.[59] Meer dan 100 miljoen telefoongesprekken werden geblokkeerd. Op 29 april onstond door een verstoring op Schiphol grote drukte op de luchthaven en op toegangswegen. Vluchten liepen vertraging op of werden geannuleerd.[60]

Tot slot

De digitale dreiging is permanent. Digitale aanvallen van statelijke actoren met als doel spionage, beïnvloeding, verstoring en sabotage vormen de grootste dreiging. Daarnaast hebben de activiteiten van cybercriminelen grote impact. Het dreigingslandschap lijkt het afgelopen jaar niet fundamenteel veranderd. Het is wel diverser geworden door een aantal verschuivingen, waarvan sommige reeds enkele jaren geleden ingezet zijn. Cyberaanvallen zijn nog steeds profijtelijk, laagdrempelig en weinig riskant voor aanvallers. In de context van recente geopolitieke ontwikkelingen zullen staten digitale aanvallen instrumenteel blijven inzetten en mogelijk op grotere schaal toepassen.

Cybersecurity noodzakelijk voor samenleving, economie en nationale veiligheid

3 Belang

Cybersecurity is noodzakelijk voor het functioneren van de sterk gedigitaliseerde Nederlandse samenleving en economie. Hoe noodzakelijk ook als barrière tegen digitale dreigingen, soms doen partijen concessies aan het belang van digitale veiligheid. Die concessies kunnen de nationale veiligheid aantasten: de ketting is immers zo sterk als de zwakste schakel. In dit hoofdstuk wordt het belang beschreven.

Cybersecurity noodzakelijk voor functioneren samenleving en economie

Nederland heeft zich volgens het rapport "De economische en maatschappelijke noodzaak van meer Cybersecurity" ontwikkeld tot een van de meest ict-intensieve economieën van Europa, dankzij onze uitstekende digitale infrastructuur. Digitalisering biedt enorme kansen voor de samenleving en economie, maar de digitale wereld moet dan wel veilig en vertrouwd blijven. Net als voor de bescherming tegen overstromingen, moet Nederland ook in de digitale wereld de dijkbewaking op orde brengen.[61]

Het kabinet onderstreept in het regeerakkoord het belang van digitalisering en cybersecurity. Het kabinet wil dat Nederland digitaal koploper wordt in Europa. Een veilige digitale infrastructuur en cybersecurity zijn daarvoor randvoorwaarden.[62] Het Centraal Planbureau stelt dat door de digitalisering het economische belang van cybersecurity toeneemt.[63] Digitale veiligheid is dus noodzakelijk voor het functioneren van onze samenleving en economie en voor het benutten van kansen.

Digitale veiligheid is ook van belang voor het mondiale internet en voor de internationale rechtsorde. Juist doordat het digitale domein grensoverschrijdend is, zijn landen sterk afhankelijk van elkaar. Zo leidt misbruik van de digitale infrastructuur in Nederland door Nederlandse of buitenlandse actoren tot problemen in andere landen. Die kunnen Nederland daarop aanspreken. Omgekeerd kan Nederland last hebben van actoren in andere landen. Verder is het internet uitgegroeid tot een mondiaal publiek goed waarvan de publieke kern moet worden beschermd.[64] Nederland is met zijn open en geglobaliseerde economie en vrije samenleving gebaat bij een vrij, open en veilig internet, ook in landen buiten Europa.[65]

Cybersecurity noodzakelijk voor nationale veiligheid

Voor de nationale veiligheid zijn vijf veiligheidsbelangen[66] gedefinieerd (zie tabel 2). Er is sprake van een mogelijk ontwrichtend effect op de samenleving als een of meer van die veiligheidsbelangen ernstig wordt aangetast.[67] Dat geldt zeker wanneer vitale processen verstoord raken of uitvallen. Vitale processen houden bijvoorbeeld onze voeten droog, ons voedsel vers en ons water zuiver. Verder gaat het over elektriciteit en warmte, het functioneren van het betalingsverkeer, het weg- water- en luchtverkeer en de handhaving van de openbare orde en veiligheid.[IV]

IV Er zijn zesentwintig processen benoemd als vitaal. Zie hiervoor: 'Weerbare vitale infrastructuur', NCTV, 2016 (https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx).

Tabel 2 De vijf nationale veiligheidsbelangen

Territoriale veiligheid	Het ongestoord functioneren van Nederland als onafhankelijke staat in brede zin, dan wel de territoriale integriteit in enge zin. *Dit betreft zowel het fysieke grondgebied en de bijbehorende infrastructuur als het imago en de reputatie van ons land.*
Fysieke veiligheid	Het ongestoord functioneren van de mens in Nederland en zijn omgeving. *Dit betreft de gezondheid en het welzijn van mensen. Criteria zijn aantallen doden en zwaargewonden en gebrek aan primaire levensbehoeften zoals voedsel, energie, drinkwater en adequate huisvesting.*
Economische veiligheid	Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie. *Dit betreft zowel economische schade (kosten) als de vitaliteit van onze economie (bijvoorbeeld sterke toename werkloosheid).*
Ecologische veiligheid	Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland. *Dit betreft aantasting van natuur, milieu en ecosystemen.*
Sociale en politieke stabiliteit	Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtsstaat en daarin gedeelde waarden. *Dit betreft aantasting van vrijheid van handelen, de democratische rechtsstaat, de kernwaarden van onze samenleving en het al dan niet optreden van grootschalige sociaal-maatschappelijke onrust en daarmee gepaard gaande emoties (angst, woede, verdriet).*

Bron: Strategie nationale veiligheid

Vitale processen zijn sterk gedigitaliseerd en dus kwetsbaar voor digitale dreigingen. Analoge alternatieven verdwijnen.[68] De Raad voor de leefomgeving en infrastructuur (Rli) wijst erop dat de Nederlandse stroomvoorziening steeds meer verweven raakt met digitale technologie. Voorgeprogrammeerde of zelflerende technologie neemt besluiten over opslag, levering en gebruik. De Rli benoemt risico's zoals cyberaanvallen en storingen als gevolg van bijvoorbeeld softwarefouten of onvoorzien gedrag van autonome systemen. Verstoring of uitval van de stroomvoorziening kan leiden tot ongevallen met persoonlijke, materiële of financiële schade. Bij langdurige uitval kan bovendien maatschappelijke onrust ontstaan.[69]

Dat cyberincidenten de veiligheidsbelangen kunnen aantasten, blijkt bijvoorbeeld uit het Nationaal Veiligheidsprofiel dat een overzicht geeft van potentiële rampen en dreigingen die Nederland kunnen ontwrichten. Hierin zijn vier cyberscenario's[V] beoordeeld op gevolgen voor de nationale veiligheid. De impact van twee scenario's, 'Aantasting internetfundament' en 'Cyberverstoring vitale sector', is als ernstig beoordeeld en de impact van de scenario's 'Cyberspionage overheid' en 'Cyberaanval hoogwaardig betalingsverkeer' als aanzienlijk.[VI 70]

Illustratief zijn ook twee voorbeelden in het laatste jaarverslag van de AIVD. De AIVD ziet steeds vaker activiteiten die erop gericht zijn om digitale sabotage van vitale infrastructuur in Europa mogelijk te maken.[71] Dit tast in ieder geval de territoriale veiligheid aan en mogelijk ook de fysieke, economische en ecologische veiligheid, evenals de sociale en politieke stabiliteit. Voorts meldt de AIVD dat in 2017 bij digitale inbraken bij diverse Europese multinationals en onderzoeksinstellingen in de energie-, hightech- en chemische sector, terabytes aan vertrouwelijke gegevens zijn gestolen. Die vertegenwoordigen een substantiële economische waarde. Dergelijke hardnekkige digitale aanvallen vormen een bedreiging van het economisch verdienvermogen van Nederland[72] en daardoor een aantasting van de economische veiligheid.

Gevolgen van cyberincidenten niet eenduidig te bepalen

De grote complexiteit en verwevenheid van het digitale domein met het fysieke domein maken het bepalen van gevolgen van cyberincidenten lastig. Zo bestaan digitale aanvallen vaak uit verschillende stappen waarbij een of meer onderdelen van een informatiesysteem worden aangetast en waaruit in sommige gevallen een aantasting van fysieke systemen, bijvoorbeeld een waterkering, kan voortkomen.

V Een scenario is een fictieve situatie die een mogelijke ramp, dreiging of crisis beschrijft. Een scenario is opgebouwd uit een specifieke combinatie van een oorzaak, actor, motief, doelwit, aard van een aantasting, doordringingsgraad en duur.

VI Er zijn vijf categorieën van impact benoemd in oplopende mate van impact: beperkt, aanzienlijk, ernstig, zeer ernstig en catastrofaal.

Omdat veel van deze stappen en de effectiviteit van getroffen maatregelen onzeker zijn, is de onzekerheid over de impact van digitale aanvallen groot.[73] Van invloed op de impact zijn eveneens andere factoren die elkaar onderling ook nog eens beïnvloeden.[VII] Zo heeft structurele, systematische en langdurige digitale spionage door een statelijke actor op topsectoren in Nederland, andere gevolgen dan een eenmalige en kortstondige spionage op een individueel bedrijf in een topsector. Beide vallen wel onder de dreiging 'digitale spionage', maar de aard en de omvang van de gevolgen zijn anders.

Ondanks deze complicaties verschijnen toch regelmatig rapportages over de financiële gevolgen van incidenten. Deze zijn opgesteld vanuit bepaalde uitgangspunten, gevolgcategorieën of impactcriteria, werkwijzen, afbakeningen in scope, tijd en geografisch gebied. Vergelijkbaarheid tussen rapportages is hierdoor lastig, zo niet onmogelijk. Het Centraal Planbureau stelt dat er relatief weinig bekend is over de schade van cybercriminaliteit[VIII] [74] en bedrijven als McAfee en CSIS noemen diverse complicaties voor het schatten van de schade hiervan.[75]

De gevolgen van cyberincidenten zijn dus niet eenduidig te bepalen. Daarvoor is het aantal variabelen waar rekening mee moet worden gehouden te groot. Bovendien moeten ook nog eens aannames worden gemaakt over de mogelijke interactie tussen variabelen. Ook kunnen keteneffecten optreden. Een verstoring van de ict in de elektriciteit kan allerlei andere vitale processen verstoren en daardoor ook vele gevolgen krijgen. Dat de gevolgen niet eenduidig te bepalen zijn, beperkt voor een deel een betere bewustwording over digitale risico's. Dit kan een optimale afweging van het belang van digitale veiligheid ten opzichte van andere belangen in de weg staan.

Gevolgen cyberincidenten kunnen groot zijn, potentieel maatschappij-ontwrichtend

Nederland is tot op het moment van schrijven gevrijwaard gebleven van een grootschalig maatschappij-ontwrichtend cyberincident. In potentie hadden enkele cyberincidenten uit het verleden onder net andere omstandigheden heel anders kunnen uitpakken, zoals in het geval van het beveiligingslek bij DigiNotar in 2011.[76] Ook WannaCry (juni 2017) had misschien maatschappij-ontwrichtend kunnen uitwerken als de uitbraak in plaats van aan het einde van een werkweek aan het begin van de werkweek zou zijn geweest en wanneer de zogeheten 'kill-switch' waarmee de malware onschadelijk werd gemaakt niet was ontdekt door een veiligheidsexpert.

In deze gevallen kan Nederland ontsnapt zijn aan een ontwrichting van de maatschappij door min of meer toevallige omstandigheden. Juist door de volledige afhankelijkheid van digitale middelen lijkt het mogelijk dat een cyberincident kan leiden tot maatschappij-ontwrichtende schade. Voorbeelden zijn een conflict tussen andere staten of een conflict van een staat met Nederland. Zo heeft de regering van (onder andere) het Verenigd Koninkrijk Rusland beschuldigd van de NotPetya-aanval. Het primaire doel was Oekraïne, maar ook organisaties in andere landen, waaronder Nederland, werden geraakt.[77] Zeker in het geval van een conflict met een statelijke actor die al voorbereidende handelingen heeft getroffen voor digitale sabotage, kunnen de gevolgen maatschappij-ontwrichtend zijn. Ook de Europese Raad heeft naar aanleiding van WannaCry en NotPetya geconstateerd dat de gevolgen van incidenten en aanvallen erg groot kunnen zijn.[78]

Belangentegenstellingen leiden tot concessies

Cybersecuritymaatregelen zijn noodzakelijk als barrière tegen digitale dreigingen. Tegelijkertijd zullen burgers, bedrijven, sectoren of overheid altijd een belangenafweging (moeten) maken. Cybersecuritymaatregelen kosten immers tijd en geld, twee schaarse middelen die ook anders ingezet kunnen worden. Soms ligt het belang van digitale veiligheid direct in het verlengde van andere belangen, soms ontstaan tegenstellingen tussen verschillende belangen.

Deze tegenstellingen bestaan binnen organisaties, bijvoorbeeld een tegenstelling tussen gebruiksgemak voor het individu en het cybersecuritybelang, maar ook tussen organisaties. Het bedrijfseconomische belang van een bedrijf kan strijdig zijn met het maatschappelijke belang. Een ongelijkheid in de verdeling van kosten en baten is een van de oorzaken van deze belangen-tegenstellingen. Kosten en baten liggen niet altijd bij dezelfde partij. Dit komt in verschillende situaties tot uiting, bijvoorbeeld:

- digitaal onveilige producten en diensten, de bedrijfseconomische belangen van producten versus het cybersecuritybelang van de maatschappij;
- de kosten van maatregelen voor een organisatie versus de baten bij andere organisaties of het collectief;
- de afweging tussen de continuïteit van een proces versus de implementatie van maatregelen;
- het individuele gebruikersongemak van een maatregel versus de toegevoegde waarde van deze maatregel voor een organisatie;

VII Die factoren zijn: a) het type dreiging, b) het type actor of gebeurtenis, c) de getroffen doelwitten, d) het type getroffen informatiesysteem (procesbesturingssysteem, kantoorautomatisering, website e.d.), e) de aard van de informatie (bijvoorbeeld de digitale kroonjuwelen van een bedrijf), f) doordringingsgraad (organisatie, sector, sectoren, meerdere provincies e.d.), g) (potentiële) duur, h) de mate waarin een cyberaanval structureel en systematisch plaatsvindt en i) de mate waarin de gevolgen zich voordoen op de korte termijn of lange termijn.

VIII Cybercriminaliteit omvat volgens het CPB, dat zich baseert op het CBS, ook delicten als marktplaatsfraude, die buiten de scope van dit CSBN vallen.

- het brede maatschappelijke belang van cybersecurity versus het specifieke belang van inlichtingen- en opsporingsinstanties;
- internationale belangentegenstellingen.

Digitaal onveilige producten en diensten

Leveranciers van hard- of software kunnen andere, vooral bedrijfseconomische, belangen laten prevaleren boven het maatschappelijke belang van digitale veiligheid. Zo constateerde de Cyber Security Raad (CSR) voor internet-of-things-toepassingen dat er weinig drijfveren zijn om veilige hard- en software te produceren en te onderhouden. Voor de meeste producenten is de time-to-market en een lage kostprijs belangrijker dan de kwaliteit en bedrijven spannen zich onvoldoende in om verplichtingen na te komen.

Het gevolg is dat er een wildgroei ontstaat van onveilige apparaten en toepassingen die met elkaar verbonden zijn en een bedreiging vormen voor onze digitale veiligheid en privacy.[79] Het bedrijfseconomische belang van deze producenten en het cybersecuritybelang van de maatschappij vormt een belangentegenstelling.

Individuele belangenafweging kan leiden tot collectieve schade

De belangentegenstelling uit de vorige paragraaf geldt niet alleen voor leveranciers van producten en diensten. Het is ook van toepassing op alle andere organisaties in het digitale domein. Ook zij maken een afweging tussen de kosten en baten van cybersecuritymaatregelen. De baten worden gevormd door een vermindering van de impact van een incident of het volledig voorkomen van een incident; schade wordt verminderd of voorkomen.

De belangenafweging die een organisatie maakt zal onder andere bepaald worden door de kosten en baten voor de organisatie zelf, en het inzicht in de risico's door deze organisatie. Tegelijkertijd kan het niet nemen van maatregelen bij een organisatie leiden tot schade bij andere organisaties of tot maatschappelijke schade. Als een organisatie bijvoorbeeld haar software-updates niet op orde heeft, dan kan de ict-infrastructuur van deze organisatie misbruikt worden om andere organisaties aan te aanvallen. Ook hier kan de bedrijfseconomische afweging van een organisatie tegengesteld zijn aan het belang van een andere organisatie of het belang van het collectief.

Continuïteit proces versus implementatie maatregelen

Een specifieke situatie doet zich voor bij aansturingssystemen. Dit zijn systemen die fysieke processen en activiteiten besturen en controleren. Daarbij kan bijvoorbeeld gedacht worden aan procescontrolesystemen in fabrieken (ICS), besturing van medische apparatuur in ziekenhuizen, enzovoorts.

Voor het doorvoeren van veiligheidsmaatregelen zoals updates, is het soms noodzakelijk om processen tijdelijk stil te leggen. Dit heeft gevolgen voor de continuïteit en kost ook geld. Bovendien kunnen updates ongewenste impact hebben op het functioneren van processen en moeten updates daar derhalve vooraf op worden beoordeeld.

Voor de continuïteit van de processen (en vertrouwelijkheid en integriteit) zijn dus aan de ene kant updates nodig, maar kan aan de andere kant tijdelijk de continuïteit of functionaliteit belemmerd worden. Uitstel of afstel van updates kan dan voor een organisatie een keuze zijn, maar wanneer het misgaat grote gevolgen hebben voor andere organisaties.

Cybersecurity leidt soms tot minder gebruikersgemak

Cybersecurity beperkt soms het gebruiksgemak. Het gebruik van afzonderlijke gebruikersnamen en wachtwoorden voor accounts en tweefactorauthenticatie vergroot de veiligheid voor een organisatie, maar vraagt in de praktijk om extra inspanning van de gebruikers. Een organisatie verantwoordelijk voor een vitaal proces zou daarom kunnen besluiten tot het gebruik van dezelfde gebruikersnaam en hetzelfde wachtwoord en tot het niet inzetten van tweefactor-authenticatie. Wanneer een actor die gegevens heeft weten te bemachtigen, heeft hij toegang tot alle systemen waar dat account toegang toe heeft, met alle gevolgen van dien. De kosten van de maatregel (gebruiksongemak) liggen bij de individuele gebruiker, de baten liggen bij de organisatie, of zelfs de maatschappij.

Spanning tussen maatschappelijke belang cybersecurity en inlichtingen- en opsporingsbelang

Tussen het brede maatschappelijke belang van cybersecurity en het specifieke belang van inlichtingen- en opsporingsinstanties bestaat in sommige gevallen spanning. Door de overheid, bedrijven en burgers wordt encryptie steeds vaker toegepast om de vertrouwelijkheid en integriteit van de communicatie en opgeslagen data te beschermen. Tegelijkertijd vormt encryptie soms een barrière, bijvoorbeeld bij gebruik door criminelen, voor het verkrijgen van informatie die noodzakelijk is voor opsporings-, inlichtingen- en veiligheidsdiensten.[80]

Een ander voorbeeld van spanning is de omgang met zogeheten zero-daykwetsbaarheden door operationele diensten. Diensten in binnen- en buitenland kunnen, in het belang van hun nationale veiligheid, zero-daykwetsbaarheden inzetten om dreigingen te onderzoeken. Het niet melden van (zero-day)kwetsbaarheden zorgt dat producenten geen oplossingen ter beschikking kunnen stellen. Dit zorgt voor soms grote risico's voor de samenleving, omdat ook anderen deze kwetsbaarheid kunnen ontdekken en misbruiken. Het (gecoördineerd) informeren van producenten en leveranciers over kwetsbaarheden biedt de gelegenheid tot het oplossen van deze kwetsbaarheiden waardoor misbruik niet meer mogelijk is.[81]

Internationale belangentegenstellingen

In internationaal verband is er sprake van tegenstellingen tussen verschillende landen in de benadering van het cyberdomein. Er bestaat verschil van inzicht over de toepassing van internationaal recht, gedragsnormen in cyberspace en de afhankelijkheid van en

toegang tot digitale middelen. Een voorbeeld daarvan is de verplichting van sommige landen aan leveranciers van software, waaronder antivirusbedrijven, om inzage te geven in de broncodes met als motivatie de controle op mogelijke achterdeurtjes voor bijvoorbeeld spionage.

De keerzijde daarvan is dat die landen daarmee ook inzicht krijgen in eventuele kwetsbaarheden die zij zelf zouden kunnen misbruiken.[82] Mogelijk misbruik tast het vertrouwen aan in die software. Indien overheden besluiten alleen producten en diensten van het eigen land of bondgenoten te accepteren dan zal dit leiden tot fragmentatie van het internet.

Cybersecurity: de ketting is zo sterk als de zwakste schakel

Concessies aan het belang van cybersecurity door individuele partijen, kunnen gevolgen hebben voor de hele Nederlandse samenleving en economie en uiteindelijk resulteren in een aantasting van de nationale veiligheid. Een concessie door een individuele partij kan voor die partij optimaal zijn, maar de som van alle concessies is zeker niet altijd optimaal voor het grotere geheel.[83]

Ook voor cybersecurity geldt dat de ketting zo sterk is als de zwakste schakel. Grootschalig misbruik van een kwetsbaarheid in één apparaat kan bijvoorbeeld grote gevolgen hebben voor het functioneren van vitale processen. De in 2017 in de media bekend geworden kwetsbaarheid in omvormers van zonnepanelen van een marktleider kan dienen als illustratie. Via de kwetsbaarheid zou het volgens de onderzoeker mogelijk zijn om een groot aantal omvormers tegelijkertijd op afstand uit te schakelen. Een dergelijke grootschalige uitschakeling zou kunnen leiden tot een verstoring in de stroomvoorziening in grote delen van Europa.[84] De Raad voor de leefomgeving en infrastructuur wijst er dan ook op dat de stabiliteit van het totale elektriciteitssysteem vooral wordt ondergraven vanuit onderdelen die niet in publiek eigendom zijn.[85]

Tot slot

Digitale veiligheid is noodzakelijk voor het functioneren van de sterk gedigitaliseerde Nederlandse samenleving en economie en als barrière tegen digitale dreigingen. Dat geldt in het bijzonder voor de nationale veiligheid. Wat de gevolgen van cyberincidenten kunnen zijn, is niet eenduidig te bepalen. Toch kunnen die gevolgen groot zijn, zeker in bepaalde omstandigheden. Hoe noodzakelijk ook als barrière tegen digitale dreigingen, soms doen partijen concessies aan het belang van digitale veiligheid, omdat ze daarnaast ook andere belangen hebben. Die concessies kunnen onder bepaalde omstandigheden de nationale veiligheid aantasten: de ketting is immers zo sterk als de zwakste schakel en kosten en baten liggen niet altijd bij dezelfde partij.

Twee ontwikkelingen dragen bij aan de blijvende noodzaak van digitale veiligheid. Al jaren is er sprake van een verdergaande digitalisering en het einde is nog niet in zicht. Steeds kritiekere processen voor de samenleving worden gedigitaliseerd, analoge alternatieven verdwijnen en steeds grotere volumes informatie worden digitaal verwerkt.

Toepassing van nieuwe technologische ontwikkelingen als robotisering, e-health en intelligente transportsystemen creëren geheel nieuwe vormen van informatie waardoor het volume aan informatie nog verder zal toenemen. Daardoor groeit ook het aantal potentiële kwetsbaarheden.

Verder moet in de context van recente geopolitieke ontwikkelingen rekening worden gehouden dat statelijke of staatsgelieerde actoren digitale aanvallen instrumenteel blijven inzetten en zich nog meer inspannen, complexere werkwijzen gaan hanteren of die op grotere schaal toepassen. Als gevolg hiervan blijft cybersecurity noodzakelijk voor het functioneren van de maatschappij.

Ketenafhankelijkheden en leveranciersketens vergroten kwetsbaarheid

4 Jaarbeeld

Het jaarbeeld laat zien dat staten in toenemende mate zowel digitale spionage- als sabotageaanvallen uitvoeren op organisaties wereldwijd. Tekortkomingen in configuraties maken aanvallen mogelijk en verscheidene incidenten tonen aan dat ketenafhankelijkheid een aanzienlijk risico vormt voor digitale veiligheid. Onderzoekers vinden kwetsbaarheden en aanvalstechnieken die in potentie op grote schaal schade zouden kunnen veroorzaken, maar deze komen nog niet verder dan het laboratorium. E-mail blijft een populair middel voor (spear)phishing en de verspreiding van malware. Naast de inzet van bekendere malwarevarianten, zoals ransomware, lijken criminelen cryptojacking als nieuw middel te hebben ontdekt om geld mee te verdienen.

Staten zetten malware in tegen kwetsbaarheden in de vitale infrastructuur

De goed ontwikkelde ict-infrastructuur van Nederland blijft aantrekkelijk als doorvoerhaven voor digitale aanvallen. De Nederlandse infrastructuur wordt misbruikt voor aanvallen op derde landen.[86] De AIVD heeft vastgesteld dat staten in toenemende mate zowel gerichte als ongerichte digitale aanvallen uitvoeren op organisaties wereldwijd. De inlichtingendienst ziet hierbij steeds vaker activiteiten die erop gericht zijn om sabotage van vitale infrastructuur in Europa (in de toekomst) mogelijk te maken, doordat andere landen zich nestelen in bepaalde systemen.[87]

In september 2017 bericht beveiligingsbedrijf Symantec over nieuwe aanvallen van de actorgroep Dragonfly.[92] Deze campagne, ook wel bekend onder de namen Havex, Crouching Yeti, Koala Team en Energetic Bear, is gericht op het verkennen van de operationele omgeving van de energiebedrijven en het plaatsen van backdoors. Hierbij gaat het om spionage als mogelijk voorwerk voor sabotage. De onderzoekers hebben aanvallen geconstateerd in de VS, Turkije en Zwitserland die sinds 2015 worden uitgevoerd. Volgens Symantec had de campagne de potentie om zich in de toekomst te richten op sabotage van energiebedrijven, al is nog niet met zekerheid te zeggen dat dit het uiteindelijke doel was.

Meer details bekend over de malware die de eerdere stroomuitval in Oekraïne veroorzaakte

In de vorige rapportageperiode leidde een cyberaanval op het energienet in Oekraïne tot stroomuitval. In juni 2017 kwam beveiligingsbedrijf ESET met een onderzoeksrapport naar buiten over de malware die hier mogelijk voor is ingezet.[88] De gebruikte malware, door de onderzoekers Industroyer genoemd, is in staat te communiceren met industriële controlesystemen (ICS) die (onder andere) worden gebruikt voor de aansturing van energienetwerken. De malware is echter ook toepasbaar op andere organisaties in andere industrieën en andere landen, mogelijk ook in Nederland.[89] Een belangrijke voorwaarde om de malware in te kunnen zetten, is dat de aanvaller toegang moet hebben tot het netwerk van het doelwit.

De aanval werd ook geanalyseerd door onderzoekers van beveiligingsbedrijf Dragos, die de malware CrashOverride hebben genoemd.[90] Zij attribueren de aanval aan de Russische actorgroep Electrum. Deze groep zou nauwe banden hebben met de actorgroep Sandworm, die zich al een aantal jaar zou bezighouden met spionagecampagnes op bedrijven en instellingen uit Oekraïne en diverse sectoren in Europa en de Verenigde Staten, waaronder de energiesector, overheid, telecommunicatie en wetenschap.[91] In tegenstelling tot eerdere campagnes van deze actor, was systeemmanipulatie (beïnvloeding van het elektriciteitsnetwerk) volgens de onderzoekers het enige doel van de malware en dus niet spionage.

De malware die wordt gebruikt is geschikt voor het saboteren van ICS, maar wordt in de praktijk vooral gebruikt voor digitale spionage. De groep maakt gebruik van twee exploitkits (LightsOut en Hello) en diverse remote access tools (RAT's) (Havex, Karagany en Oldrea). In maart 2018 stellen onderzoekers van beveiligingsbedrijf Cylance dat tevens gecompromitteerde Cisco-routers worden ingezet bij aanvallen door deze actor.[93]

In oktober 2017 meldt het Amerikaanse US-CERT aanvallen van geavanceerde actoren op vitale infrastructuur, waarbij een link wordt gelegd met de Dragonfly-campagne.[94] Om binnen te komen in de netwerken van grote organisaties binnen de energiesector, richten de aanvallers zich op zwak beveiligde punten en kleine netwerken. Er is sprake van twee soorten doelwitten. De initiële doelwitten zijn organisaties aan de buitenkant, zoals vertrouwde leveranciers met minder goed beveiligde netwerken. De aanvaller gebruikt de netwerken van de vertrouwde leveranciers als uitvalsbasis om hun uiteindelijke doelwitten aan te vallen.

Uit analyse van US-CERT blijkt dat de inloggegevens die door de aanvallers werden verkregen, op die plekken waar geen tweefactorauthenticatie werd toegepast, zijn gebruikt om toegang te krijgen tot het netwerk van de slachtoffers. De aanvallers richtten zich op de ICS-infrastructuur en voerden verkenningsoperaties uit in het netwerk. Er zijn geen directe aanwijzingen dat doelwitten in Nederland met deze campagne werden aangevallen. In maart 2018 attribueerde de Amerikaanse overheid deze aanvallen aan de Rusland.[95]

Dit illustreert een opvallende ontwikkeling in de rapportageperiode: de publiekelijke attributie van cyberaanvallen aan specifieke landen. Rusland werd bijvoorbeeld ook door de Oekraïense geheime dienst SBU, de Verenigde Staten en het Verenigd Koninkrijk beschuldigd van betrokkenheid bij de NotPetya-aanval.

Malware Triton/Trisis gericht op veiligheidssystemen

In december 2017 werd malware ontdekt die Schneider Electric Triconex Safety Instrumented Systems kan herprogrammeren. Deze safety controllers worden ingezet als back-up voor de veiligheid van bijvoorbeeld chemische of nucleaire industriële processen, ook als er problemen zijn met het reguliere controlesysteem. Deze Triconex-systemen worden wereldwijd in duizenden fabrieken gebruikt. In maart 2018 was er hernieuwde aandacht voor deze malware; de New York Times berichtte dat de malware zou zijn ingezet voor een sabotagepoging van een petrochemische fabriek in Saoedi-Arabië.[96] De malware bleek in staat te zijn om een controlesysteem aan te passen, volgens de New York Times, met als doel de operatie te saboteren en een explosie te veroorzaken. Een bug in de malware lijkt een explosie te hebben voorkomen. Vanwege het geavanceerde niveau van de aanval wordt deze in verband gebracht met een statelijke actor. Bij het NCSC zijn geen besmettingen met de Triconex-malware binnen Nederland bekend.

In de vorige rapportageperiode zijn er door hackersgroep 'the Shadow Brokers' hackingtools gepubliceerd die afkomstig zouden zijn van Amerikaanse inlichtingendiensten.[97] De meest besproken middelen waren EternalBlue en EternalRomance, exploits die het bestandsdelingsprotocol SMB op Windowssystemen misbruiken om die systemen te compromitteren, en Doublepulsar, een achterdeur die op gecompromitteerde systemen geïnstalleerd kan worden om diverse malafide code uit te voeren. In deze rapportageperiode is de toepassing van deze exploits in het openbaar zichtbaar geworden. Dit heeft veel schade veroorzaakt.

Begin mei 2017 verspreidde de malware WannaCry zich wereldwijd door misbruik van de kwetsbaarheid die EternalBlue uitbuit. Veel organisaties werden hierdoor zwaar getroffen. In Nederland was de impact beperkt. Onder de getroffen organisaties waren het Spaanse Telefónica, FedEx en de Britse National Health Service (NHS). Doordat een beveiligingsonderzoeker een zogenoemde killswitch vond in de malware en deze activeerde, is verdere verspreiding beperkt gebleven.

Actoren zetten middelen in tegen kwetsbaarheden in de leverancierskete

In juni 2017 heeft de grootschalige digitale aanval NotPetya[IX] wereldwijd organisaties getroffen. De aanval, die ook andere namen heeft gekregen, waaronder PetrWrap, GoldenEye en ExPtr, heeft ook in Nederland diverse slachtoffers gemaakt. De initiële aanvalsvector bleek de boekhoudsoftware van het bedrijf M.E.Doc te zijn: aanvallers waren in staat om met gestolen inloggegevens kwaadaardige code aan een update voor de software toe te voegen.

Na besmetting verspreidde de malware zich als een worm binnen de getroffen organisaties. Hoewel het zich manifesteerde als ransomware, bleek na onderzoek dat ontsleuteling in de praktijk niet mogelijk was. Dit maakt dat NotPetya eigenlijk alleen gericht was op het wissen van bestanden, waarbij de enige oplossing na besmetting het terugzetten van back-ups is. De malware gebruikte onderdelen van verschillende bronnen, zoals de EternalBlue-exploit, die ook al eerder werd toegepast in WannaCry. Volgens diverse beveiligingsbedrijven was NotPetya specifiek gericht op Oekraïne. Naast de Oekraïense geheime dienst SBU beschuldigen de Verenigde Staten en het Verenigd Koninkrijk Rusland van betrokkenheid bij de cyberaanval.[98]

IX De recente NotPetya-malware is een afgeleide van het reeds bekende Petya-ransomwarevirus uit 2016. De oorspronkelijke auteur heeft echter te kennen gegeven niet achter de huidige variant te zitten. Om die reden wordt de huidige malware ook wel NotPetya genoemd.

2017: het jaar van de cryptoworm

In mei raakten honderdduizenden computers wereldwijd besmet met WannaCry.[99] In juni raakten duizenden computers in voornamelijk Oekraïne, Rusland en West-Europa (waaronder Nederland) besmet met de NotPetya-malware.[100] Ook was er in oktober een uitbraak van de BadRabbit-ransomware in Oekraïne, Rusland, Turkije en Duitsland.[101] Bij elk van deze campagnes werd gebruik gemaakt van exploits die eerder naar buiten waren gebracht. Anders dan bij veel andere ransomwarecampagnes, waarbij gebruikers op een malafide link moeten klikken of een besmette bijlage moeten openen om geïnfecteerd te raken, was bij deze campagnes sprake van een zogeheten worm die voor de verspreiding van de malware zorgde.

Deze wereldwijde ransomware-aanvallen tonen aan hoe gevaarlijk en desastreus een cryptoworm kan zijn, ook als er misbruik wordt gemaakt van een kwetsbaarheid waar al langere tijd een patch voor beschikbaar is. In vergelijking met eerdere grootschalige ransomwarecampagnes, viel vooral de wereldwijde reikwijdte van besmetting en de veroorzaakte financiële schade op. In Nederland is die met name veroorzaakt door NotPetya. Containervervoerder Maersk schat de schade als gevolg van deze aanval op 200 tot 300 miljoen dollar.[102]

De populaire opschoonsoftware CCleaner werd in augustus en september 2017 besmet met de Floxif-trojan.[103] Deze malware was tijdens het ontwikkelproces in het programma geïnjecteerd, waardoor het in de officiële versie terechtkwam en de digitale ondertekening van het programma geldig was. Aanvankelijk meldde uitgever Avast dat nergens daadwerkelijk kwaadaardige code is uitgevoerd op getroffen systemen, ondanks dat de besmette software op dat moment ruim twee miljoen keer gedownload was.

Uit nader onderzoek door beveiligingsbedrijf Cisco Talos is gebleken dat het om een gerichte aanval ging. Van de 700.000 systemen die contact maakten met de command-&-controlserver werden er ten minste twintig een besmetting van de tweede fase waargenomen, die zich goed verborgen hield in het systeem. De slachtoffers waren grote bedrijven uit de technologiesector. Volgens Cisco Talos zijn er geen besmettingen van de tweede fase in Nederland waargenomen.

Belangrijke kwetsbaarheden blootgelegd, uitbuiting valt te verwachten

In deze rapportageperiode is een aantal technische kwetsbaarheden aan het licht gekomen die in potentie op grote schaal schade zouden kunnen veroorzaken en daarom veel aandacht hebben gegenereerd, maar waarvan nog nauwelijks of geen misbruik is waargenomen. De aanvalstechnieken om misbruik te kunnen maken van de kwetsbaarheden waren vaak complex, of er moest aan bepaalde voorwaarden worden voldaan die het lastig maakten om deze op grote schaal uit te voeren, zoals de noodzaak om fysiek dichtbij een doelwit aanwezig te zijn. De verwachting is dat kwetsbaarheden die nu nog complex uit te buiten zijn, maar mogelijk wel waardevol voor aanvallers zijn, in de toekomst wel uitgebuit zullen worden.

In juli 2017 werd een kwetsbaarheid bekend in Broadcom wifi-chips, die worden gebruikt in telefoons en andere apparaten van onder andere Samsung, Google en Apple. Daarmee kan een aanvaller de volledige controle krijgen over het toestel, code uitvoeren op de wifi-chip en toegang krijgen tot ontsleuteld wifi-verkeer.[104] Deze kwetsbaarheid is Broadpwn genoemd.

Twee maanden later vonden onderzoekers een soortgelijke kwetsbaarheid in de Broadcom wifi-chips, waarbij de onderzoekers ook de exploitcode, waarmee een aanvaller code kan uitvoeren op de wifi-chip, publiek hebben gemaakt.[105] Misbruik van de kwetsbaarheid met deze exploitcode lijkt alleen mogelijk als een gebruiker verbinding maakt met een nieuw wifinetwerk. Dit vereist dat een aanvaller fysiek dichtbij een slachtoffer is. De kwetsbaarheden zijn bij Apple en Google gemeld en op gecoördineerde wijze opgelost in nieuwe versies van hun besturingssystemen iOS en Android. Apparaten waarvoor de fabrikanten nog updates uitbrengen, konden hierdoor gepatcht worden.

In oktober 2017 publiceerden onderzoekers van de Katholieke Universiteit Leuven een rapport over aanvalstechnieken waarvoor elk apparaat dat wifi gebruikt op basis van WPA- of WPA2-versleuteling kwetsbaar zou zijn, de zogenoemde Krack-aanval.[106] Omdat de aanvaller fysiek in de buurt moet zijn van het wifinetwerk dat hij aan wil vallen, zijn de aanvalstechnieken lastig op grote schaal efficiënt uit te voeren.

In januari 2018 brachten onderzoekers naar buiten dat ze twee nieuwe families van kwetsbaarheden hadden gevonden, Spectre en Meltdown, in moderne processoren. Een aanvaller die deze kwetsbaarheden misbruikt, kan vertrouwelijke informatie bemachtigen door programmacode uit te voeren op de computer van een slachtoffer.[107] Een aantal leveranciers heeft bij de bekendmaking van de kwetsbaarheden patches aangekondigd of al beschikbaar gesteld.

De openbaarmaking van proof-of-conceptcode om deze kwetsbaarheden te misbruiken leidde niet direct tot verhoogd risico, omdat niet iedereen een dergelijk complexe aanval kan uitvoeren.[108] De verwachting is dat deze kwetsbaarheden in de toekomst wel uitgebuit zullen worden. In mei 2018 werden nieuwe kwetsbaarheden gevonden, die een vergelijkbaar effect hebben als Spectre.[109]

In maart 2018 lanceerden onderzoekers van beveiligingsbedrijf CTS-labs een website over dertien ernstige kwetsbaarheden en backdoors die ze zouden hebben ontdekt in AMD-processoren, AMDflaws genoemd.[110] Al snel werden in de media twijfels geuit over de legitimiteit van CTS-labs, mede omdat de onderzoekers AMD slechts 24 uur voor de publicatie van de kwetsbaarheden op de hoogte hadden gebracht.[111] Uiteindelijk bevestigde AMD dat ze wel aanwezig waren en dat er werd gewerkt aan patches. Zij gaven hierbij echter ook aan dat de kwetsbaarheden een beperkt risico vormen omdat deze alleen zijn te misbruiken als een aanvaller het systeem al heeft gecompromitteerd en over beheerdersrechten beschikt.[112]

In mei 2018 maakten onderzoekers van de Vrije Universiteit de GLitch-kwetsbaarheid bekend. Dit is een nieuwe manier om zogenoemde Rowhammer-aanvallen uit te voeren via de grafische processor (GPU) van een computer.[113]

Veel datalekken door tekortkomingen in configuraties en het ontbreken van maatregelen

Grote datalekken nog steeds aan de orde van de dag

Gegevens uit datalekken kunnen worden gebruikt voor spearphishing of voor directe identiteitsfraude. De grootte van datalekken die ontdekt zijn en gemeld worden, en de mate van vertrouwelijkheid van gelekte informatie, vallen deze rapportageperiode opnieuw op. Het niet juist configureren of het niet tijdig verhelpen van ontdekte kwetsbaarheden was in de meeste gevallen de oorzaak. De schade die een datalek veroorzaakt is lastig vast te stellen, omdat er vaak geen indicatie is van de schaal van het eventuele misbruik.

In september 2017 maakte de Amerikaanse kredietbeoordelaar Equifax bekend dat een datalek mogelijk 143 miljoen Amerikanen zou treffen. In oktober 2017 en maart 2018 meldde Equifax dat de aanvallers de gegevens van nog eens 4,9 miljoen Amerikanen hadden gestolen.[114] [115] De oorzaak van het datalek lag in een Apache Struts-kwetsbaarheid, waar redelijk snel na ontdekking en het uitkomen van een patch misbruik van is gemaakt. De complexiteit die het patchen met zich mee bracht zorgde ervoor dat de kwetsbaarheid niet tijdig werd verholpen. De aanval heeft Equifax in het derde kwartaal van vorig jaar 87,5 miljoen dollar gekost.[116]

In november 2017 kwam naar buiten dat taxi-app Uber in 2016 een grote hack verzweeg waarbij data van 57 miljoen mensen op straat kwam te liggen.[117] In december volgde het bericht dat hierbij naar schatting de gegevens van 174.000 Nederlandse passagiers en chauffeurs van Uber zijn buitgemaakt.[118] Uber bleek per ongeluk sleutels op GitHub te hebben gezet die toegang gaven tot de Amazon-cloud met daarop alle persoonlijke gegevens van passagiers en chauffeurs van Uber. Dit werd ontdekt en gemeld aan het bedrijf. Na overleg besloot Uber uiteindelijk om 100.000 dollar uit te betalen aan de melder, op voorwaarde dat die een overeenkomst ondertekende waarin werd toegezegd dat alle gegevens gewist zouden worden. Uber heeft besloten om geen melding te maken van dit datalek, omdat dit volgens hen onder het reguliere coordinated-vulnerability-disclosureprogramma (cvd) viel. Uiteindelijk zijn de advocaten die bij deze beslissing betrokken waren ontslagen toen het incident aan het licht kwam en veel mensen hier vraagtekens bij plaatsten.[119]

In diezelfde maand werd bekend dat het energieverbruik van alle Nederlandse huishoudens door een datalek was op te vragen op postcode en huisnummer via de website van een energieleverancier.[120]

In februari 2018 ontdekte het Duitse beveiligingsbedrijf Kromtech een foutief geconfigureerde Amazon S3-bucket, een type cloudopslagserver.[121] De server bevatte meer dan 119.000 gescande documenten, waaronder identiteitsbewijzen. Het lek werd de dag na ontdekking verholpen. In april 2018 kwam naar buiten dat hier ook gescande identiteitsbewijzen met adresgegevens van 3.000 Nederlanders uit de periode 2009-2012 tussen zaten.[122] Naar verluidt zouden er ook legitimatiebewijzen van defensiemedewerkers tussen zitten.

Ruim 10.000 datalekken gemeld bij de Autoriteit Persoonsgegevens in 2017

Het aantal meldingen van datalekken bij de Autoriteit Persoonsgegevens (AP) is in 2017 met ruim 70 procent toegenomen ten opzichte van het jaar ervoor, van 5.849 naar 10.009. Net als in 2016 kwamen de meeste meldingen van datalekken van organisaties uit de sectoren gezondheid en welzijn (3.105 meldingen), openbaar bestuur (2.000) en financiële dienstverlening (1.984). Bij bijna de helft van de datalekken (47 procent) die in 2017 zijn gemeld, gaat het om persoonsgegevens die aan een verkeerde ontvanger zijn gestuurd. Verloren of gestolen apparaten, gegevensdragers of papier waren in 14 procent van het totale aantal gemelde datalekken de oorzaak.

In de meeste gevallen gaat het om naw-gegevens, geslacht, geboortedatum en burgerservicenummer. De grootte van de gemelde datalekken varieert. In 80 procent van de gevallen gaat het om een datalek waarbij de gegevens van 1 tot 100 personen zijn gelekt, bij 17 procent gaat het om de gegevens van 101 tot 5.000 personen, in 2 procent van de gevallen zijn de gegevens van 5.001 tot 100.000 mensen gelekt en bij minder dan 1 procent werden meer dan 100.000 mensen getroffen.[123]

DDoS-aanvallen via publiek beschikbare systemen

Het aantal DDoS-aanvallen wereldwijd is in de eerste drie kwartalen van 2017 gestegen. De laatste drie maanden van het jaar was het rustiger.[124] [125] [126] Politiek gemotiveerde DDoS-aanvallen, door bijvoorbeeld hacktivisten, krijgen nog steeds geregeld aandacht,[127] maar lijken weinig maatschappelijke impact te hebben. In de vorige rapportageperiode werd grootschalig misbruik van het internet of things gemaakt door IoT-botnets DDoS-aanvallen te laten uitvoeren. In deze rapportageperiode is duidelijk geworden dat ook andere typen systemen kunnen worden ingezet voor het uitvoeren van grootschalige DDoS-aanvallen, wanneer deze niet of onvoldoende worden beveiligd.

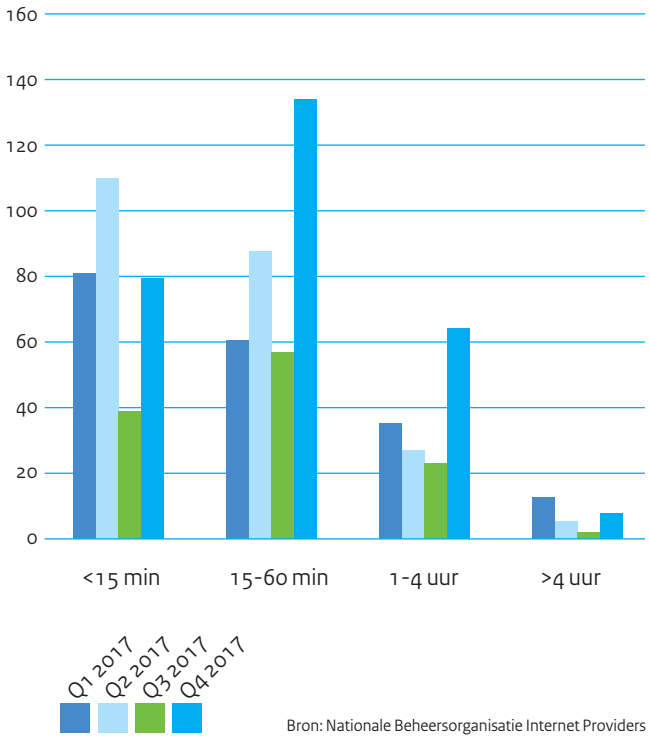
In februari 2018 werden wereldwijd publiek beschikbare memcached-systemen gebruikt bij DDoS-aanvallen.[128] Memcached-systemen zijn bedoeld om tijdelijk kleine hoeveelheden data op te slaan uit andere bronnen om websites sneller te maken, zoals databases en API's. De systemen vereisen geen authenticatie voor de communicatie en zijn niet ontwikkeld om publiek toegankelijk te zijn. Ten tijde van de aanvallen zouden er ongeveer drieduizend publiek beschikbare memcached-systemen in Nederland zijn.

Er zijn scenario's mogelijk waarbij deze memcached-systemen ingezet worden voor het uitvoeren van amplificatie-aanvallen. Daarbij verstuurt de aanvaller ogenschijnlijk een verzoek namens het doelwit door diens ip-adres te vervalsen. Doordat de antwoorden groter zijn dan de verzoeken, kan een aanvaller met relatief weinig bandbreedte een grotere aanval op dat doelwit opzetten. Voor aanvallers is een publiek beschikbaar systeem met een zeer grote amplificatie-factor, zoals een niet-afgeschermd memcached-systeem, een aantrekkelijk middel om aanvallen uit te voeren.

DDoS-aanvallen worden steeds complexer, omdat ze van steeds meer soorten bronnen afkomstig zijn, die overal ter wereld kunnen staan en meerdere doelen tegelijk kunnen treffen. Voorbeelden hiervan zijn onveilige IoT-apparaten, open memcached-systemen, of 'booter-sites' waar DDoS-aanvallen voor enkele tientjes te koop zijn.[129] [130] In maart 2018 kwam naar buiten dat het ontwikkelaars-platform GitHub in januari van dat jaar was getroffen door een DDoS-aanval van 1,35 terabit per seconde, de krachtigste DDoS-aanval die tot dat moment werd geregistreerd. Hierbij werd ook gebruik gemaakt van memcached-systemen.[131]

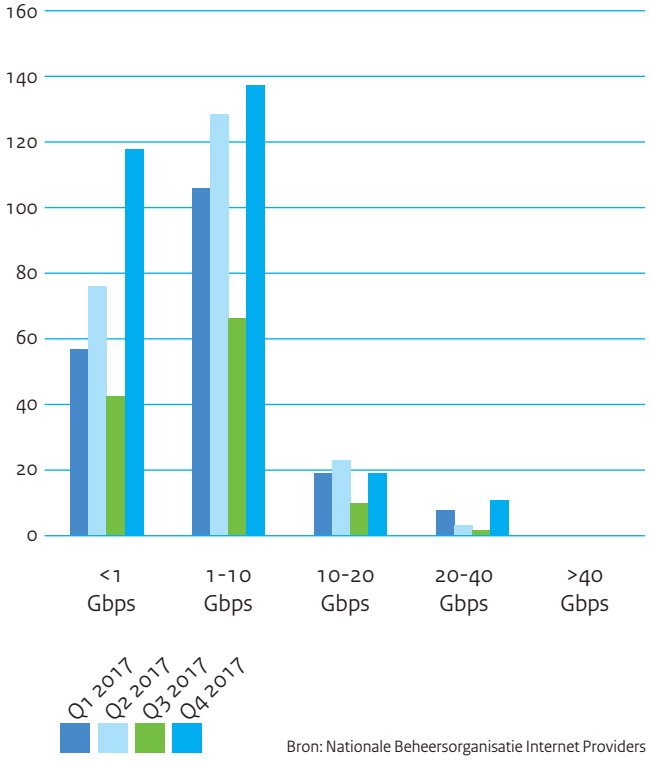
In 2017 heeft de Nationale Beheersorganisatie Internet Providers (NBIP) 826 DDoS-aanvallen verwerkt. Net als in 2016 had meer dan de helft van de verwerkte aanvallen een omvang van tussen de 1 en 10 Gbps. In 2017 duurde meer dan 40 procent van de aanvallen tussen de 15 en 60 minuten. Ruim 3 procent van de aanvallen duurde langer dan 4 uur.

Figuur 2 **Duur van DDoS-aanvallen**



Bron: Nationale Beheersorganisatie Internet Providers

Figuur 3 **Omvang van DDoS-aanvallen**



Bron: Nationale Beheersorganisatie Internet Providers

E-mail blijft een populair middel voor het uitvoeren van digitale aanvallen

(Spear)phishing wordt door verschillende actoren gebruikt als eerste stap in een digitale aanval

Phishing is vaak de eerste stap in een cyberaanval[132] en omdat het in veel gevallen succesvol is,[133] wordt het middel door alle soorten actoren ingezet. E-mail wordt als middel gebruikt om binnen te dringen in systemen voor spionage- en sabotagedoeleinden. Ruim 90 procent van de malwarebesmettingen vindt per e-mail plaats.[134] Wanneer aanvallers zich de toegang hebben verschaft tot het netwerk, dan wordt er gezocht naar specifieke bedrijfsinformatie of wordt er verkend hoe de digitale infrastructuur van de organisatie in elkaar zit.

Opnieuw aandacht voor e-mailspoofing

Bij (spear)phishing en het verspreiden van malware per e-mail maken aanvallers soms gebruik van 'e-mailspoofing'. In de rapportageperiode hebben onderzoekers laten zien hoe mensen e-mail kunnen versturen die afkomstig lijkt te zijn van @tweedekamer.nl.[135] Ook andere domeinen blijken kwetsbaar te zijn voor dergelijk misbruik, zoals @aivd.nl en @defensie.nl.[136] In de Verenigde Staten werden duizenden domeinen van de federale overheid gespoofd. Media schrijven dit toe aan statelijke actoren.[137] Hoewel het geen nieuw fenomeen is, zijn er nog steeds veel organisaties die geen maatregelen treffen zoals het implementeren van de SPF-, DKIM- en DMARC-standaarden. Dat beveiligingsmaatregelen echter ook omzeild kunnen worden, kwam in december 2017 aan het licht toen 'Mailsploit'-kwetsbaarheden bekend werden gemaakt, waarmee het mogelijk was om ondanks maatregelen toch succesvol andermans e-mailadres als afzender te gebruiken.[138]

De traditionele vorm van phishing via spam bestaat nog steeds, maar het is niet langer de enige vorm in het huidige dreigingslandschap. Er is steeds meer sprake van gerichte spearphishingaanvallen.[139] Door zich in het bijzonder te richten op rijke individuen of individuen die toegang hebben tot financiële accounts of gevoelige gegevens van bedrijven of overheden, hopen aanvallers op groter financieel gewin dan ze kunnen verwachten van wijdverspreide en ongerichte spamcampagnes.

Statelijke actoren zetten spearphishing in voor digitale spionage

De AIVD onderkent in Europa ten opzichte van 2016 een lichte toename van economische spionage door statelijke actoren.[140] In maart 2018 bracht het Amerikaanse ministerie van Justitie een aanklacht tegen negen Iraniërs naar buiten. Daarin worden zij beschuldigd van het ontvreemden van 31 terabyte aan documenten en data bij meer dan 140 Amerikaanse universiteiten, 30 Amerikaanse bedrijven, 5 Amerikaanse overheidsorganisaties en meer dan 176 universiteiten in 21 andere landen, waaronder in Nederland.

Om de diefstal, die van 2013 tot en met 2017 zou hebben plaatsgevonden, mogelijk te maken zouden de aanvallers inloggegevens van medewerkers hebben ontvreemd via spearphishing-e-mails.[141] De verdachten worden gelinkt aan het Mabna Institute, een Iraans bedrijf dat in 2013 is opgericht met als expliciet doel illegaal toegang te krijgen tot niet-Iraanse wetenschappelijke bronnen door middel van computerinbraken. De aanvallers zouden uit zijn geweest op onderzoeksgegevens, wetenschappelijke data, bedrijfsgeheimen en intellectueel eigendom.

Volgens de FBI wordt het instituut ingehuurd door verschillende onderdelen binnen de Iraanse overheid, waaronder de Islamitische Revolutionaire Garde – een van de verschillende entiteiten die verantwoordelijk zijn voor het verzamelen van inlichtingen. De aanvallers stalen data voor de Iraanse overheid en ze boden de gestolen data aan via twee Iraanse websites (megapaper.ir en gigapaper.ir).

Het aantal meldingen van phishing was wereldwijd tussen mei en september 2017 redelijk stabiel en wijkt ook niet veel af van het gemiddeld aantal meldingen in de vorige rapportageperiode.[142] [143] [144] Microsoft detecteerde helemaal aan het eind van 2017 een aanzienlijk aantal phishing-e-mails.[145] In deze rapportageperiode zijn vooral manifestaties van digitale aanvallen waargenomen waarbij (spear)phishing is ingezet door criminelen en staten of staatsgelieerde actoren. Volgens telecommunicatieconcern Verizon zetten die laatste twee phishing in bij 70 procent van hun digitale aanvallen.[146]

Sterke toename van phishingwebsites die misbruik maken van bekende Nederlandse merken

Met een deel van de phishing-e-mails worden slachtoffers naar een phishingwebsite gelokt, bijvoorbeeld een namaakversie van een bankwebsite waarmee criminelen hun inlog- of creditcardgegevens proberen te achterhalen. Uit een analyse van Stichting Internet Domeinregistratie Nederland (SIDN) blijkt dat het aantal phishingsites dat misbruik maakt van bekende Nederlandse merken het afgelopen jaar met ruim 40 procent is gestegen.[147] Volgens beveiligingsbedrijf Webroot worden er maandelijks gemiddeld 1,4 miljoen unieke phishingwebsites opgezet.[148] De vele verkrijgbare (en soms ook gratis) 'phishingkits', softwarepakketten die het snel en makkelijk opzetten van een nieuwe phishingwebsite mogelijk maken, zouden hierbij een belangrijke rol spelen.[149] Een van de tactieken die actoren gebruiken om legitiem en veilig over te komen, is door de sites te voorzien van een TLS-certificaat.[150]

Ontwikkelingen op het vlak van malware

Er is een afname te zien in exploits voor Adobe Flash Player en kwetsbaarheden in Internet Explorer, terwijl Microsoft Office-exploits zijn toegenomen.[151] In 2017 kwamen veel van de documenten die een exploit voor Microsoft Office bevatten ook met een phishingcomponent, voor het geval het doelwit de kwetsbaarheid al had gepatcht. Volgens beveiligingsbedrijf Kaspersky Lab bevatte meer dan 90 procent van de gedetecteerde malafide Office-documenten exploits voor twee specifieke kwetsbaarheden.[X 152]

Grote hoeveelheid e-mails met bankiermalware verspreid in Nederland

In december 2017 zagen analisten van beveiligingsbedrijf Fox-IT in Nederland de verspreiding van een grote hoeveelheid phishing-e-mails met een link naar een downloadbaar zipbestand. Ontvangers die de bijlage openden, werden geïnfecteerd met de Zeus Panda-malware. Die was erop gericht om inloggegevens voor internetbankieren en creditcardinformatie te achterhalen. Hoewel de verstuurde e-mails niet heel erg professioneel oogden en bijvoorbeeld spelfouten bevatten, klikten toch zo'n 48.000 mensen op de link. Het aantal besmettingen lag lager, omdat er ongeveer 11.000 keer op de link werd geklikt vanaf een Windows-computer, het enige platform waarop de malware werkte.

De gebruikte malware was niet nieuw, maar uniek aan deze phishingcampagne is dat de criminelen naast banken ook webwinkels betrokken in hun aanval. De malware probeerde niet alleen de inlog- en creditcardgegevens van de slachtoffers te achterhalen bij het bezoeken van een bankwebsite, maar ook bij het bezoeken van een webwinkel.

Hoewel malware de meest voorkomende digitale dreiging blijft,[153] ziet de AIVD dat staten steeds vaker legitieme softwarefunctionaliteit en bonafide toeleveranciers misbruiken om toegang te krijgen tot specifieke slachtoffers.[154] Hiervan zijn ook in Nederland organisaties in het bedrijfsleven, de vitale infrastructuur en de overheid doelwit. De inzet van malware wordt hiermee overbodig, wat preventie en detectie van dergelijke aanvallen lastiger maakt.

Cryptojacking aantrekkelijker en opvallender

Cryptovaluta werken op basis van cryptografische principes en worden gedolven door cryptomining: het uitvoeren van complexe berekeningen.[155] Criminelen proberen steeds vaker geld te verdienen met cryptojacking, waarbij ze het rekenvermogen van computersystemen van nietsvermoedende derden gebruiken voor cryptomining.[156] De reden hiervoor kan zijn dat de waarde van cryptovaluta de laatste jaren gestegen is. Naast criminelen zijn ook voorbeelden waargenomen waarbij interne actoren een dreiging kunnen vormen, wanneer deze de systemen van hun werkgever voor eigen financieel gewin gebruiken voor cryptomining.[157] [158] [159]

Criminelen proberen zoveel mogelijk systemen tot hun beschikking te krijgen, bijvoorbeeld door ze met cryptominingmalware te besmetten en hiermee onderdeel te maken van een botnet. Onderzoekers van het beveiligingsbedrijf Proofpoint hebben het Smominru-botnet gevolgd, waarbij meer dan 526.000 Windows-machines werden besmet met cryptominingmalware.[160] [161] Hierbij werd, net als bij WannaCry, gebruik gemaakt van de eerder gelekte EternalBlue- en DoublePulsar-kwetsbaarheden. Het botnet zou de criminelen meer dan 2 miljoen dollar hebben opgeleverd.

Naast de meer traditionele computersystemen worden ook IoT-apparaten gebruikt om cryptovaluta te delven.[162] Hoewel ze vaak beschikken over een beperkte rekenkracht, maakt het hoge aantal apparaten dat kwetsbaar is voor publiek beschikbare exploits ze toch een aantrekkelijk doelwit voor cryptojacking door criminelen.[163]

X CVE-2017-0199 of CVE-2017-8759.

Cryptominingmalware ook aangetroffen op industriële controlesystemen

In februari 2018 meldde beveiligingsbedrijf Radiflow dat zij voor het eerst cryptominingmalware in een netwerk met industriële controlesystemen hadden aangetroffen. Tijdens reguliere monitoring-activiteiten werd Monero-miningmalware aangetroffen in het netwerk van een klant, een afvalwaterfaciliteit in Europa.[164] De malware werd aangetroffen op een aantal servers, waaronder een HMI (Human Machine Interface). Deze computers stonden indirect in verbinding met het internet, om monitoring op afstand mogelijk te maken. Volgens het beveiligingsbedrijf lijkt het erop dat een van deze computers is gebruikt om een website te bezoeken die besmet was met de malware. Vervolgens zouden de andere servers via het interne netwerk besmet zijn geraakt.

Websites laten hun bezoekers ook steeds vaker cryptovaluta delven.[165] [166] [167] Hiervoor wordt gebruik gemaakt van een JavaScript-bestand dat automatisch wordt uitgevoerd wanneer een bezoeker de desbetreffende website opent. Sinds eind 2017 lijkt cryptomining via websites steeds professioneler te worden. Een van de partijen hierachter is het bedrijf Coinhive[168] dat deze code als dienst aanbiedt voor website-eigenaren. Coinhive presenteert dit als alternatief voor het tonen van advertenties op websites. In ruil voor een commissie van 30 procent van de opbrengst, verstrekt dit bedrijf de code die ervoor zorgt dat de computers van alle bezoekers van de website worden ingezet voor het delven van cryptovaluta.[169] In veel gevallen wordt hiervoor geen expliciete toestemming gevraagd aan de bezoekers.[170] Deze werkwijze is onder meer geconstateerd bij zowel 'discutabele' websites, zoals torrentwebsite The Pirate Bay[171], als bij legitieme videostreamingdiensten[172] [173].

Omdat cryptomining op de achtergrond plaatsvindt, kan het lang duren voordat het wordt ontdekt.[XI] Het is aannemelijk dat de stijgende populariteit van cryptojacking samenhangt met de enorme waardestijging van veel cryptovaluta. Volgens beveiligingsbedrijf Cisco Talos kan een aanvaller die tweeduizend systemen in gebruik heeft (wat volgens de experts goed haalbaar is) zo'n 500 dollar per dag of 182.500 dollar per jaar verdienen. De onderzoekers hebben botnets gezien met miljoenen geïnfecteerde systemen, waarmee in theorie dus meer dan 100 miljoen dollar per jaar verkregen zou kunnen worden.[174]

Cryptojackingaanvallen lijken in deze rapportageperiode te zijn toegenomen, terwijl het aantal ransomwarebesmettingen in de tweede helft van 2017 daalt. In een aantal bronnen wordt een relatie gelegd tussen de afname van ransomware en de toename van cryptojacking.[175] [176] [177] Naast de relatieve onzichtbaarheid van de aanval, zou een voordeel van cryptojacking ten opzichte van ransomware zijn dat het geld oplevert zonder dat de slachtoffers hier iets voor moeten doen, zoals het betalen van bitcoins in ruil voor de toegang tot het systeem. Het is nog te vroeg om met zekerheid te kunnen zeggen dat er daadwerkelijk een verschuiving plaatsvindt van ransomware naar cryptominingmalware. Volgens beveiligingsbedrijf Malwarebytes is het gebruik van beide gestegen in het eerste kwartaal van 2018 met respectievelijk 27 en 28 procent, maar blijft spionagemalware nog het meest populair.[178]

Tot slot

In de rapportageperiode was opnieuw te zien dat criminelen, staten en staatsgelieerde actoren de meeste schade aanrichten. Ook de middelen die worden ingezet zijn voor een groot deel herkenbaar uit eerdere jaren. Zo is e-mail verreweg het meest ingezette middel voor (spear)phishing en het verspreiden van malware.

Een ontwikkeling ten aanzien van criminelen is dat er een toename is in het gebruik van cryptojacking voor financieel gewin. Verder verdienen ze nog steeds geld met het gebruiken of verkopen van gestolen informatie. Staten voeren in toenemende mate zowel gerichte als ongerichte digitale aanvallen uit op organisaties wereldwijd. Naast spionage zijn deze aanvallen ook gericht op verstoring of sabotage van de vitale infrastructuur.

Veel incidenten, zoals datalekken en DDoS-aanvallen, konden plaatsvinden door configuratiefouten of technische gebreken van software of systemen. Bij een aantal grootschalige digitale aanvallen die organisaties wereldwijd hebben getroffen is duidelijk geworden dat ketenafhankelijkheid een aanzienlijk risico vormt voor softwareveiligheid.

XI Doordat een deel van het rekenvermogen van de besmette computer wordt ingezet om de cryptomunten te delven, kan de computer erg traag worden. Dat kan voor de gebruiker een indicatie zijn dat er iets aan de hand is.

Basismaatregelen lang niet altijd getroffen, weerbaarheid onder druk

5 Weerbaarheidsbeeld

De digitale weerbaarheid van Nederland staat onder druk. Lang niet alle organisaties treffen basismaatregelen. Incidenten hadden daarmee voorkomen kunnen worden of de schade beperkt. De kroonjuwelen van organisaties worden succesvol aangevallen zonder de inzet van geavanceerde methoden. De weerbaarheid staat verder onder druk door een toenemende complexiteit en connectiviteit van het ict-landschap en in voorkomende gevallen weinig aandacht voor cybersecurity. Het beeld van de weerbaarheid is generiek en niet toegespitst op organisaties.

Organisatiespecifieke inschatting weerbaarheid niet mogelijk

Het is niet mogelijk om een specifieke inschatting te geven van de weerbaarheid van organisaties in Nederland tegen de dreigingen zoals die in dit CSBN zijn geïdentificeerd. Er ontbreekt eenvoudigweg inzicht in alle getroffen maatregelen door organisaties. Regelmatig duiken nieuwe kwetsbaarheden op, ontwikkelen cyberactoren zich en kunnen ook onvoorziene verstoringen en uitval optreden als gevolg van bijvoorbeeld de fragiliteit van het internet. Maatregelen die nu resulteren in een acceptabel niveau van weerbaarheid, kunnen op basis van nieuwe inzichten ontoereikend worden.

Maatregelen veelal beschikbaar, maar niet altijd toegepast

Het nemen van basismaatregelen zorgt ervoor dat de cybersecurity binnen een organisatie op een bepaald niveau wordt gebracht. Deze maatregelen bieden bescherming tegen een breed scala aan aanvallen van verschillende actoren. Uit incidenten blijkt dat organisaties niet altijd basismaatregelen treffen.

De rapportageperiode kende veel incidenten waar basismaatregelen de schade hadden kunnen beperken of het incident hadden kunnen voorkomen. Bij manifestaties met grote gevolgen, zoals WannaCry en BadRabbit, werden bekende kwetsbaarheden misbruikt. De beveiligingsupdates hiervoor waren al maanden beschikbaar maar klaarblijkelijk niet toegepast.[179] In andere gevallen waren kwetsbaarheden (nog) niet bekend, maar zouden basismaatregelen wel een barrière hebben gevormd of de gevolgen hebben verkleind.

De impact van wormen, zoals bijvoorbeeld WannaCry, NotPetya en BadRabbit had verkleind kunnen worden door, onder meer, de basismaatregel segmentering. De uitbraken van zowel WannaCry (12 mei 2017) als NotPetya (27 juni 2017) maakten misbruik van de kwetsbaarheid EternalBlue, terwijl voor ondersteunde systemen al in maart kritieke beveiligingsupdates beschikbaar waren. Het niet kunnen nemen van basismaatregelen leidt tot een verlaagde weerbaarheid. Dat effect is bijvoorbeeld zichtbaar bij de uitrol van zakelijke telefoons. Leveranciers van Android-telefoons zijn onduidelijk over de termijn waarbinnen zij beveiligingsupdates beschikbaar stellen. Als organisaties hier geen expliciete afspraken met de leverancier over maken lopen ze sterk het risico dat hun product direct bij ingebruikname verouderd is.

Ook configuratiefouten leiden tot incidenten. Zo waren bijvoorbeeld gegevens over energiecontracten van Nederlandse huishoudens voor iedereen online beschikbaar doordat verkeerd geconfigureerde S3-buckets, gebruikt voor gegevensopslag, toegankelijk waren. Verkeerd geconfigureerde memcached-servers zijn misbruikt om grote DDoS-aanvallen uit te voeren. Traditionele aanvalsmethoden, zoals phishing, worden ingezet om de kroonjuwelen van organisaties te compromitteren.

Een indicatie dat basismaatregelen niet op orde zijn, kan ook worden ontleend aan het feit dat cyberaanvallen lange tijd onopgemerkt blijven. Uit onderzoek blijkt dat bedrijven, overheden en organisaties in Europa pas na maanden ontdekken dat zij slachtoffer van een cyberaanval zijn geweest.[180] De kroonjuwelen van organisaties worden succesvol aangevallen zonder de inzet van geavanceerde middelen.

Dat organisaties niet altijd bekende basismaatregelen treffen heeft uiteenlopende oorzaken.[XII] Deze liggen soms binnen de invloedssfeer van een organisatie en soms daarbuiten. Een voorbeeld is het groeiende tekort aan cybersecurityspecialisten op de arbeidsmarkt.[181] [182] Aangenomen mag worden dat het komend jaar organisaties nog steeds niet alle basismaatregelen zullen treffen, tenzij daartoe een aanleiding is. Die zou kunnen liggen in een cyberincident waar de organisatie slachtoffer van is geworden. Dit gebrek aan basismaatregelen beperkt de weerbaarheid van organisaties.

Weerbaarheid verder onder druk

Naarmate de complexiteit en connectiviteit toenemen, wordt het steeds ingewikkelder om een weerbare digitale infrastructuur te realiseren. Enerzijds zorgen organische groei en de relatief lange levensduur van systemen voor een steeds complexer landschap. Anderzijds is het overzicht lastiger te bewaren door het toegenomen gebruik van gedeelde voorzieningen, zoals clouddiensten in de vorm van losse bouwblokken.

Waar in het verleden diensten binnen een organisatie ingericht werden, wordt het nu bij meerdere partijen ingekocht en extern uitgevoerd. Regie op het ict-landschap blijft binnen de organisatie, terwijl de uitvoering ervan versnipperd raakt over verschillende partijen. Het gebruik van diverse dienstenleveranciers en clouddiensten zorgt voor nieuwe afhankelijkheden en een vergroting van het aanvalsoppervlak.

De digitale infrastructuur is complex, niet alle essentiële onderdelen zijn even robuust en de onderlinge afhankelijkheid van onderdelen is groot. Bepaalde software wordt generiek door ontwikkelaars en leveranciers gebruikt als bouwsteen voor hun werk. Vaak gaat het daarbij om software die ontwikkeld wordt door samenwerkingsverbanden van vrijwilligers. Capaciteiten of middelen voor onderhoud of onderzoek naar de kwaliteit ervan ontbreken vaak. Sommige populaire protocollen voor gegevensuitwisseling via het internet zijn decennia oud en niet bestand tegen hedendaagse aanvallen. Verbeterde versies van oude internetstandaarden (zoals IPv6 of https) worden langzaam in gebruik genomen, waardoor de nadelen van oude versies (IPv4 en http) nog lang blijven spelen.

Op diverse plaatsen in dit CSBN is gewezen op kwetsbaarheden in de leverancierskeketen en de wijze waarop die zijn te misbruiken of tot misbruik hebben geleid.[XIII] Cyberincidenten ergens in de keten kunnen elders in de keten ook resulteren in cyberincidenten.

Complicerend is dat iedere leverancier keuzes maakt voor het belang dat hij aan cybersecurity toekent. Wat optimaal is voor de leverancier zelf, kan suboptimaal zijn voor de klanten die hij bedient.[XIV] Omgekeerd kan een partij de eigen zaken nog zo goed voor elkaar hebben, maar kunnen als gevolg van een incident bij de leverancier alsnog problemen ontstaan. Het vinden van een oplossing voor kwetsbaarheden in de leverancierskeketen is voor een individuele partij niet eenvoudig.

Het jaarbeeld noemt enkele fundamentele kwetsbaarheden die gedurende de rapportageperiode bekend zijn geworden. Weliswaar zijn deze vooral in een laboratorium-setting misbruikt, toch valt uitbuiting buiten het laboratorium zeker niet uit te sluiten. Vanwege de complexiteit en connectiviteit is lang niet altijd eenvoudig te achterhalen waar de kwetsbaarheden zich in de eigen infrastructuur bevinden en bij welke ketenleveranciers. Als er al oplossingen bekend zijn, kan het de nodige tijd duren voordat die zijn aangebracht en bestaat de kans dat er toch een kwetsbaarheid over het hoofd wordt gezien. Het treffen van maatregelen, als die al bestaan, is dus lastig en kost tijd.

Door die toenemende complexiteit en connectiviteit is het voor organisaties moeilijk te voorspellen welke kwetsbaarheden in de toekomst misbruikt zullen worden en welke bijbehorende maatregelen daartegen vandaag al genomen moeten worden. Organisaties zullen geconfronteerd worden met verrassingen, zoals onverwachte incidenten en (keten)effecten. Deze onzekerheden, de zogenoemde “unknown unknowns”, zijn de consequenties van de complexiteit van de digitale infrastructuur.

Weerbaarheid organisaties: kat-en-muis-spel

Hoewel het dreigingsbeeld niet fundamenteel is veranderd, is het wel zo dat cyberactoren innoveren. Zo spelen cyberactoren in op nieuw bekend geworden kwetsbaarheden. De makers van WannaCry zijn daarvan een voorbeeld: relatief kort na het openbaar worden van de kwetsbaarheid wisten zij die op grote schaal te misbruiken.

Voor cybercriminelen was het innen van geld met geldezels lange tijd een kwetsbaar onderdeel van de criminele bedrijfsvoering. Ransomware maakte het innen van geld minder kwetsbaar en het relatief nieuwe cryptojacking maakt het innen van geld robuuster. Ook bestaat er een professionele sector van laagdrempelig beschikbare producten en diensten waarmee digitale aanvallen uitgevoerd kunnen worden. Daarbinnen is eveneens sprake van innovatie.

XII In de paragraaf Belangentegenstellingen leiden tot concessies (hoofdstuk 3) worden enkele redenen beschreven.

XIII Zie Buitenlandse producenten en dienstverleners positief en negatief voor de weerbaarheid (hoofdstuk 1), Leverancierskeketens verhogen kwetsbaarheid (hoofdstuk 2) en hoofdstuk 4.

XIV Zie paragraaf Belangentegenstellingen leiden tot concessies (hoofdstuk 3).

Aannemelijk is dat cyberactoren zich mede ontwikkelen en aanpassen aan de getroffen maatregelen binnen organisaties. Zo zetten statelijke actoren, die in beginsel kunnen beschikken over geavanceerde kennis en middelen, bij voorkeur minder geavanceerde en eenvoudige middelen in. Afhankelijk van het gepercipieerde belang zullen actoren meer tijd, geld en middelen inzetten om het beoogde doel te bereiken. In de rapportageperiode is bijvoorbeeld opgevallen dat cyberactoren kwetsbaarheden misbruiken in de leveranciersketen.[XV]

Omgekeerd passen organisaties met hun cybersecuritymaatregelen zich ook aan cyberincidenten aan. Zo zag Microsoft zich na de initiële uitbraak van WannaCry genoodzaakt de MS17-010 patch ook voor niet-ondersteunde Windows-versies beschikbaar te stellen en treffen organisaties maatregelen wanneer ze getroffen zijn door een ransomwarebesmetting.

Tot slot

Het is niet mogelijk om een specifieke inschatting te geven over de weerbaarheid van organisaties in Nederland tegen de dreigingen zoals die in dit CSBN zijn geïdentificeerd. Wel blijkt keer op keer uit cyberincidenten dat lang niet alle organisaties basismaatregelen treffen. Deze organisaties zijn met oog op de huidige dreiging vrijwel onverdedigbaar tegen kwaadwillenden en kunnen ook onbedoeld slachtoffer worden van cyberaanvallen op, via of tegen anderen.

Incidenten hadden voorkomen kunnen worden of de schade had beperkt kunnen worden met deze basismaatregelen. De kroonjuwelen van organisaties worden succesvol aangevallen zonder de inzet van geavanceerde methoden. De weerbaarheid staat verder onder druk door een toenemende complexiteit en connectiviteit van het ict-landschap en in voorkomende gevallen weinig aandacht voor cybersecurity. Er is sprake van een kat-en-muis-spel met cyberactoren. De digitale weerbaarheid van Nederland staat onder druk.

XV Zie paragraaf Leveranciersketens verhogen kwetsbaarheid (hoofdstuk 2).

Bijlagen

Bijlage 1 NCSC-statistieken

Deze bijlage geeft een overzicht van gemelde kwetsbaarheden, beveiligingsadviezen en incidenten die door het NCSC zijn afgehandeld. Ook wordt een overzicht gegeven van activiteiten binnen het Nationaal Detectie Netwerk. Incidenten worden geregistreerd en bijgehouden met behulp van een registratiesysteem, dit systeem is de bron voor alle onderstaande grafieken. In de afgelopen rapportageperiode is het aantal kwetsbaarheidsmeldingen substantieel toegenomen. Het aantal overige meldingen is echter licht gedaald.

Het NCSC faciliteert het doen en het verwerken van meldingen in het kader van gecoördineerde kwetsbaarheidsbekendmaking (coordinated vulnerability disclosure, cvd-meldingen) voor zowel haar eigen infrastructuur als voor die van de rijksoverheid en enkele private partijen. Ook brengt het beveiligingsadviezen uit aan haar deelnemers en handelt het cybersecurityincidenten af. Daarnaast werkt het NCSC aan de uitbreiding van het Nationaal Detectie Netwerk (NDN). Hierover zijn voor deze rapportageperiode (mei 2017 tot en met april 2018) statistieken berekend die hieronder worden gepresenteerd. Door deze te vergelijken met eerdere rapportageperiodes kunnen trends en ontwikkelingen worden geïdentificeerd.

Meldingen van kwetsbaarheden

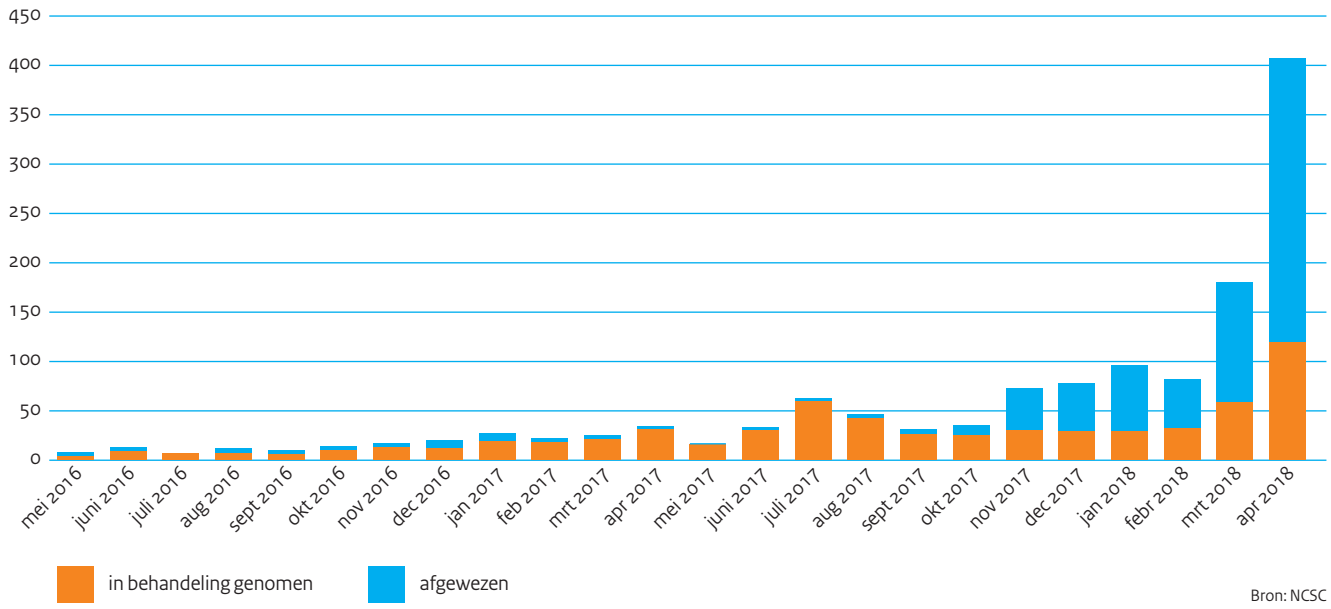
In de rapportageperiode heeft het NCSC in totaal 1.140 cvd-meldingen ontvangen. Voorheen werden dergelijke meldingen beschreven als responsible-disclosuremeldingen. Per maand zijn gemiddeld 95 meldingen gedaan. Dit zijn zowel meldingen voor eigen systemen als voor overige rijksoverheidssystemen en systemen van derden. Ook zijn meldingen opgenomen die geresulteerd hebben in het gecoördineerd verhelpen en openbaar maken van nieuw ontdekte kwetsbaarheden in hard- en software. In enkele gevallen is er sprake van een dubbele melding van dezelfde kwetsbaarheid door twee of meer onderzoekers. Hierdoor is het totale aantal meldingen niet overeenkomt met het totale aantal kwetsbaarheden.

In de voorgaande rapportageperiode waren er 194 cvd-meldingen. Dit betekent bijna een verzesvoudiging in de huidige periode. Dit kan worden verklaard door een substantiële toename in het aantal meldingen vanuit het buitenland, voornamelijk uit India. Uit communicatie met een aantal van deze melders blijkt het melden van een kwetsbaarheid en het ontvangen van een beloning daarvoor (vaak een t-shirt) een manier is om hun cybersecuritykennis te bewijzen richting potentiële werkgevers.

Figuur 4 toont het aantal cvd-meldingen per maand voor de afgelopen twee rapportageperiodes. Hierin is een explosieve groei te zien, die vooral in de afgelopen zes maanden heeft plaatsgevonden. Dit figuur laat ook de verhouding zien tussen meldingen die wel of niet in behandeling zijn genomen. Niet alleen is het totale aantal meldingen toegenomen maar ook het percentage dat afgewezen is. In de afgelopen periode waren dat er 640 (56 procent). In de vorige periode waren er 43 (28 procent) afgewezen.

Een melding kan worden afgewezen om verschillende redenen. Als een melding is gemaakt voor een organisatie die buiten de doelgroep van het NCSC valt, wordt deze afgewezen met het advies om eerst rechtstreeks contact op te nemen met die organisatie. Ook wordt een melding afgewezen als bij nader onderzoek blijkt dat er geen sprake is van een kwetsbaarheid of dat het beveiligingsrisico verwaarloosbaar is. Verder wordt een melding afgewezen als er al eerder melding is gemaakt over dezelfde kwetsbaarheid in hetzelfde systeem.

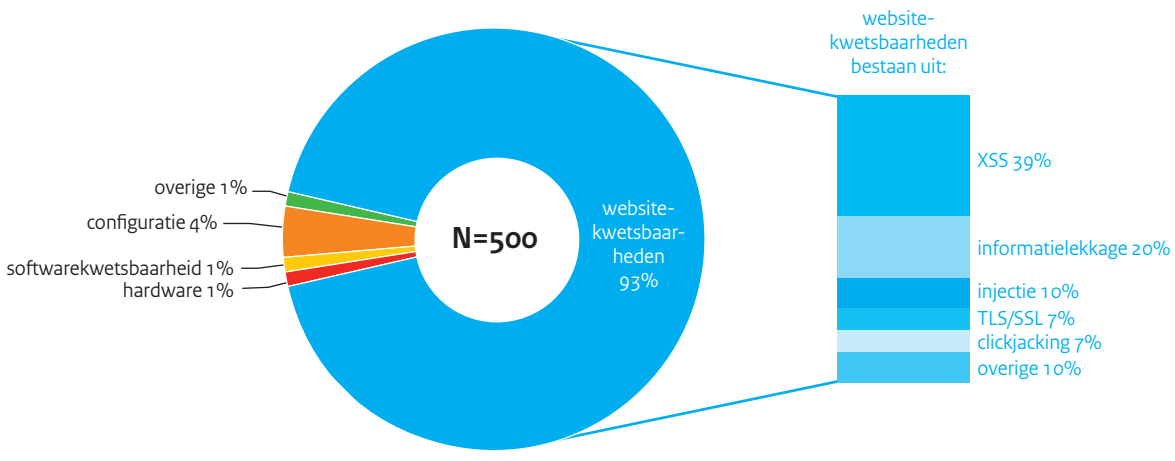
Figuur 4 **Aantal cvd-meldingen per maand**



Bron: NCSC

Figuur 5 toont de verschillende typen cvd-meldingen. De meerderheid (93 procent) van alle meldingen heeft te maken met een kwetsbaarheid in een website, een webapplicatie, of infrastructuur waarop webapplicaties draaien. Voorbeelden van zulke meldingen zijn zwakke TLS-parameters, cross-site scripting (XSS), SQL-, XML- en HTML-injectie en informatielekkage. Een voorbeeld van dat laatste is een kwetsbaarheid waardoor het mogelijk is om een configuratiebestand te zien. Slechts 4 procent van alle meldingen heeft te maken met configuratiefouten in hard- en software. Relatief weinig meldingen gaan over kwetsbaarheden in software of hardware (exclusief webservers en -applicaties). In tegenstelling tot het vorige CSBN, worden hier alleen meldingen getoond wanneer die in behandeling zijn genomen. Hiervoor is gekozen omdat het aantal afgewezen meldingen anders dit figuur kan verkleuren.

Figuur 5 **Typen cvd-meldingen**



Bron: NCSC

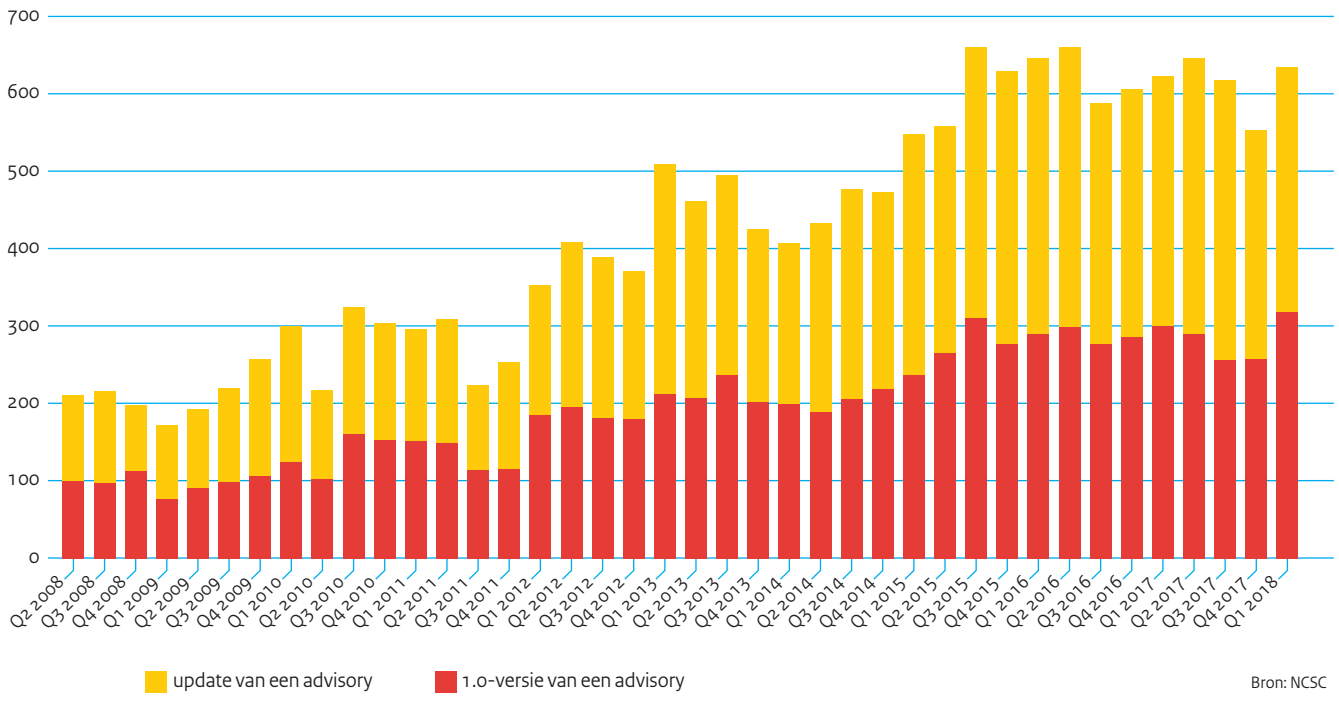
Beveiligingsadviezen

Het NCSC publiceert beveiligingsadviezen naar aanleiding van software- en hardwarekwetsbaarheden of geconstateerde dreigingen. In een beveiligingsadvies wordt beschreven wat er aan de hand is, welke systemen getroffen zouden kunnen zijn en wat er moet gebeuren om te voorkomen dat een kwetsbaarheid wordt misbruikt.

Figuur 6 toont het aantal beveiligingsadviezen dat het NCSC heeft gepubliceerd per kwartaal, van het tweede kwartaal van 2008 tot en met het eerste kwartaal van 2018. Hierbij wordt onderscheid gemaakt tussen nieuwe beveiligingsadviezen (met versienummer 1.0) en updates van bestaande beveiligingsadviezen. In totaal heeft het NCSC 1.100 nieuwe beveiligingsadviezen gepubliceerd in de afgelopen rapportageperiode. Dit is ongeveer 7 procent minder dan het jaar daarvoor. Ook is het aantal updates van bestaande beveiligingsadviezen licht gedaald naar 1.289. Dit is een afname van ongeveer 4 procent.

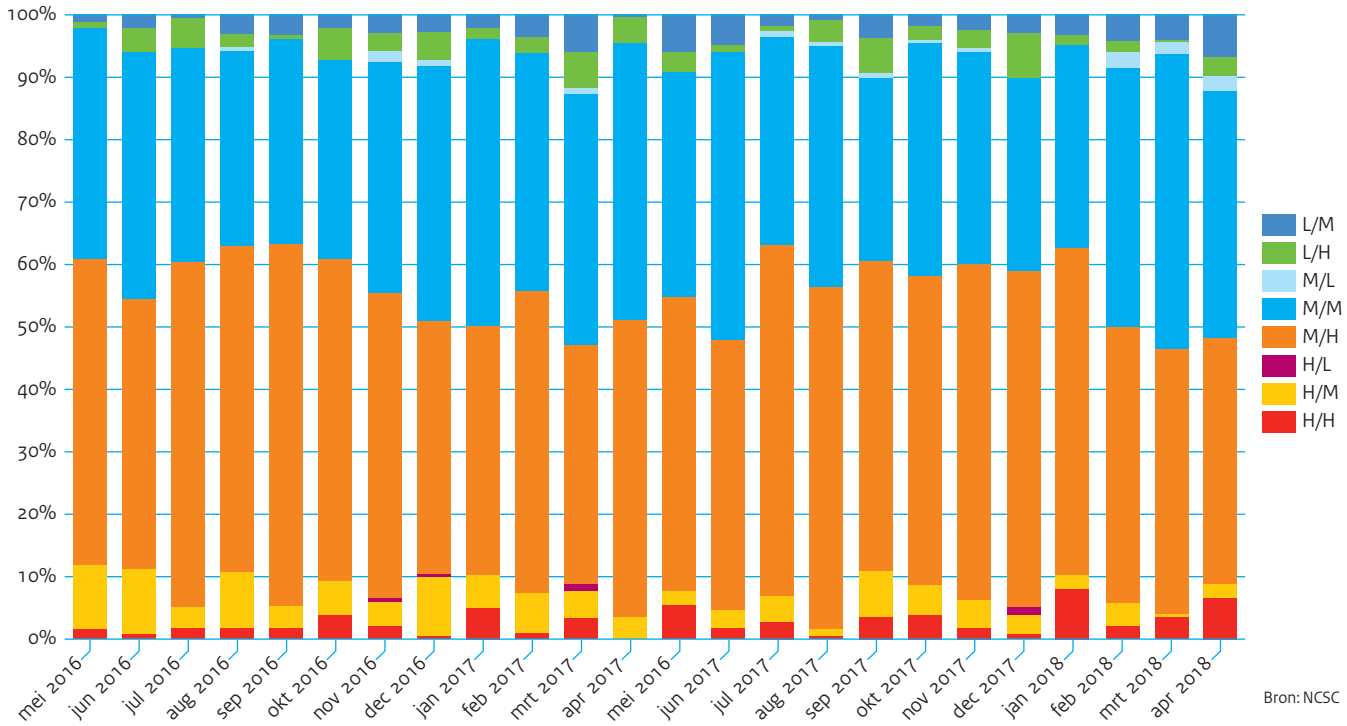
De beveiligingsadviezen van het NCSC worden ingeschaald op twee elementen. Ten eerste stelt men vast wat de kans is dat de kwetsbaarheid misbruikt wordt. Ten tweede bepaalt men de schade die optreedt wanneer de kwetsbaarheid misbruikt wordt. Voor beide criteria (kans en schade) wordt, op basis van meerdere aspecten, een niveau geschat: hoog (H), gemiddeld (M) of laag (L). Bijvoorbeeld: als er een hoge kans is dat een bepaalde kwetsbaarheid misbruikt wordt, maar de verwachte schade van misbruik is laag, krijgt het bijbehorende beveiligingsadvies een H/L-inschaling. Figuur 7 toont de verhoudingen tussen deze niveaus voor alle gepubliceerde adviezen (inclusief updates) per maand voor de afgelopen twee rapportageperiodes.

Figuur 6 **Aantal beveiligingsadviezen per kwartaal (2008Q2 – 2018Q1)**



Bron: NCSC

Figuur 7 **Inschaling beveiligingsadviezen per maand (mei 2016 – april 2018)**



Bron: NCSC

Schade van kwetsbaarheden

Bij ieder beveiligingsadvies hoort een omschrijving van de mogelijke schade die een kwaadwillende zou kunnen verrichten als het advies niet gevolgd wordt. Voor de afgelopen drie rapportageperiodes wordt het percentage adviezen per schadeomschrijving in tabel 3 getoond. Hierin is te zien dat beveiligingsadviezen die te maken hebben met denial-of-service (DoS) nog altijd het grootste aandeel hebben (51 procent). Hierna volgen het uitvoeren van willekeurige code met gebruikersrechten (37 procent), toegang tot gevoelige gegevens (33 procent), het omzeilen van een beveiligingsmaatregel (19 procent) en het verhogen van gebruikersrechten (17 procent). Dit waren ook in de vorige rapportageperiode de meest voorkomende beveiligingsadviezen. Regelmatig zijn bij een advies meerdere schadeomschrijvingen van toepassing. Dit leidt tot een totaalpercentage van meer dan 100 procent.

Tabel 3 **Percentage beveiligingsadviezen per schadeomschrijving CSBN2016 t/m CSBN2018**

Schadeomschrijving	2016	2017	2018
Denial-of-Service (DoS)	56%	61%	51%
Remote code execution (gebruikersrechten)	37%	42%	37%
Toegang tot gevoelige gegevens	32%	32%	33%
Omzeilen van beveiligings-maatregelen	25%	17%	19%
Verhoogde gebruikersrechten	21%	19%	17%
Toegang tot systeemgegevens	13%	13%	14%
Cross-Site Scripting (XSS)	9%	8%	9%
Manipulatie van gegevens	8%	10%	8%
Remote code execution (admin/rootrechten)	6%	7%	6%
Omzeilen van authenticatie	5%	3%	6%
Spoofing	5%	5%	4%
Cross-Site Request Forgery (XSRF)	2%	2%	1%
SQL-injectie	2%	1%	1%

Bron: NCSC

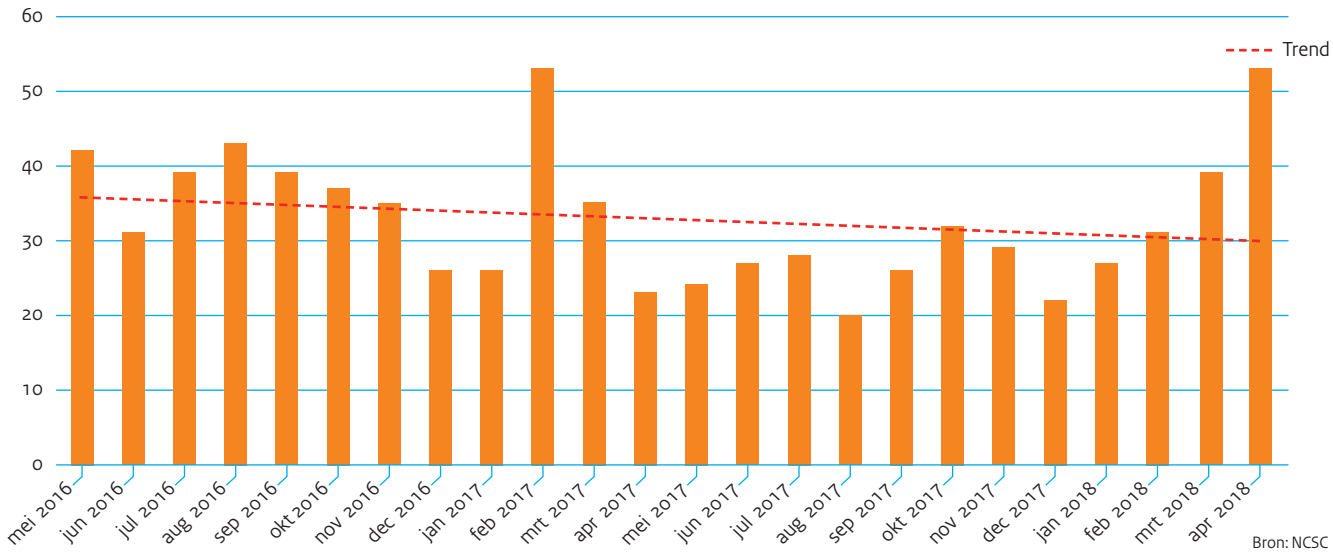
Cybersecurityincidenten geregistreerd bij het NCSC

Het NCSC ondersteunt de rijksoverheid en organisaties in vitale processen bij het afhandelen van incidenten op het gebied van ICT-veiligheid. In die rol worden bij het NCSC incidenten en kwetsbaarheden gemeld en worden deze ook door het NCSC zelf geïdentificeerd, bijvoorbeeld op basis van diverse detectiemechanismen en eigen onderzoek. Daarnaast acteert het NCSC op verzoek van (inter)nationale partijen richting Nederlandse internetserviceproviders om hen te ondersteunen bij het bestrijden van cyberincidenten die hun oorsprong vinden in Nederland (bijvoorbeeld vanaf een malafide webserver of vanaf geïnfecteerde computers in Nederland).

Aantallen afgehandelde incidenten

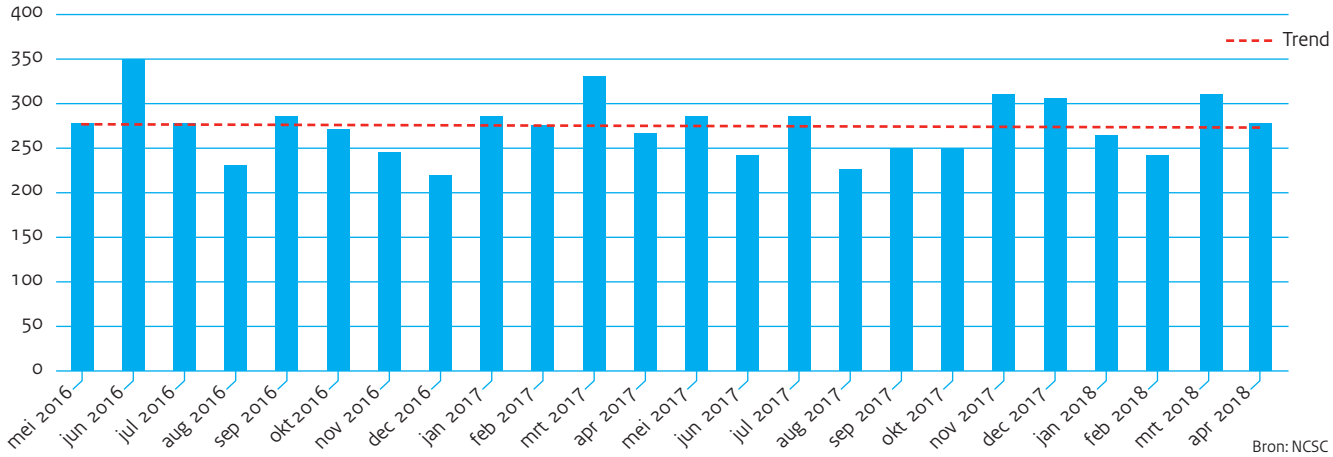
Het aantal afgehandelde incidenten per maand de laatste twee rapportageperiodes wordt in figuur 8 getoond. Hierin ontbreken de geautomatiseerde controles en cvd-meldingen. Deze worden allebei in losse grafieken getoond in deze bijlage. In de afgelopen rapportageperiode werden er in totaal 358 incidenten gemel, ongeveer 30 per maand. In de vorige rapportageperiode waren dat er 429, ongeveer 36 per maand. Vergeleken met vorig jaar zijn de grootste verschillen te vinden in het aantal meldingen over phishing (20 procent afname) en malware infecties (30 procent

Figuur 8 **Afgehandelde incidenten (exclusief geautomatiseerde controles en cvd-meldingen)**



Bron: NCSC

Figuur 9 **Geautomatiseerde controles**



Bron: NCSC

afname). De afname kan mogelijk verklaard worden doordat organisaties basale incidenten minder melden omdat deze beschouwd worden als "going-concern". De verscherping van de doelgroepen van het NCSC, naar aanleiding van de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc), heeft als consequentie dat incidenten van bepaalde organisaties niet meer bij het NCSC gemeld worden. Er zijn in de rapportageperiode geen meldingen gedaan in het kader van de meldplicht Wgmc.

Figuur 9 toont de resultaten van geautomatiseerde controles voor de laatste twee rapportageperiodes. In de afgelopen periode waren er gemiddeld 270 incidentmeldingen per maand. In de vorige periode was dat gemiddeld 275. Een melding kan meerdere geïnfecteerde systemen binnen een organisatie betreffen.

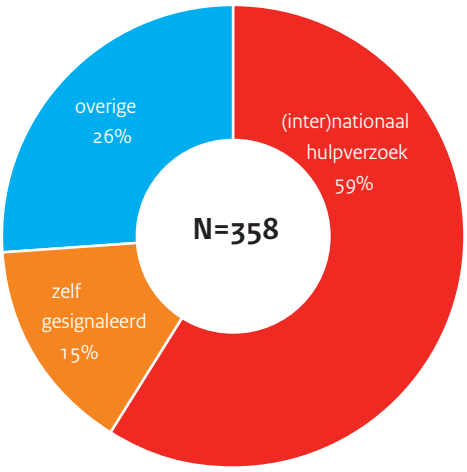
Verdeling incidenten per melding, categorie en afhandeling

De verdeling van incidenten naar meldingstype wordt in figuur 10 getoond. Dit geeft aan hoe een incident bij het NCSC gemeld is. Het merendeel van incidentmeldingen (59 procent) komt van buitenaf: van nationale of internationale bronnen. In 20 procent van alle gevallen wordt een incident in behandeling genomen naar aanleiding van eigen signalering. Voorbeelden hiervan zijn een waarschuwing uit een eigen detectiemechanisme of een bericht uit een openbare bron. In het overige 21 procent van de meldingen was er sprake van informatie die ter kennisgeving is aangenomen of andere diverse meldingen.

De verdeling van incidenten per categorie wordt in figuur 11 getoond. Voor deze verdeling heeft het NCSC gebruikgemaakt van de door CERT.PT en ENISA vastgestelde incidententaxonomie.[183] In de binnenste ring worden de hoofdcategorieën getoond, in de buitenste ring de subcategorieën. Het komt weleens voor dat één incident meer aspecten heeft die verschillende mogelijke categorieën van de taxonomie treffen. Om overlap te voorkomen heeft het NCSC in deze gevallen gekozen om de voornaamste of belangrijkste aspect van dat incident leidend te laten zijn bij het selecteren van één categorie.

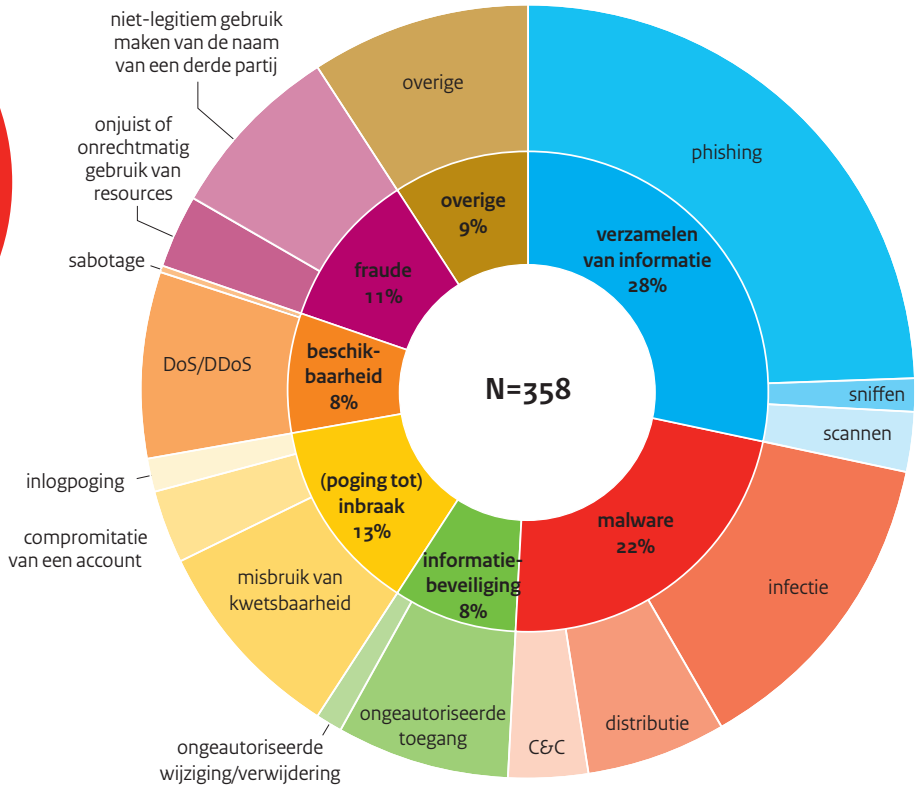
In meer dan een kwart (28 procent) van de incidenten blijkt dat het om informatieverzameling gaat. Het overgrote merendeel hiervan betreft phishing. Incidenten waarbij er sprake is van malware leveren 22 procent van alle incidenten op. Het merendeel hiervan heeft met malwarebesmetting te maken. In 8 procent van alle gevallen was er sprake van ongeautoriseerde toegang of misbruik van een kwetsbaarheid en in 13 procent van (poging tot) inbraak.

Figuur 10 **Afgehandelde incidenten per meldingstype**



Bron: NCSC

Figuur 11 **Afgehandelde incidenten per categorie**



Bron: NCSC

Ook hier gaat het voornamelijk om misbruik van een kwetsbaarheid. Ongeveer 8 procent van alle incidenten hadden te maken met beschikbaarheid. Bijna al deze incidenten hadden te maken met (D)DoS-aanvallen of -dreigingen. In 11 procent van alle incidenten was er sprake van fraude. Een voorbeeld hiervan is het niet-legitiem gebruikmaken van de naam of het logo van een derde partij. Het resterende deel (9 procent) heeft te maken met diverse incidenten waaronder het versturen van spam.

Vergeleken met de verdeling van incidenten in de vorige rapportageperiode, zien we een afname in het percentage van zowel informatiebeveiliging als (poging tot) inbraak. Dit is grotendeels te verklaren door het feit dat er, anders dan voorheen, geen cvd-meldingen in deze grafiek worden meegeteld. Gezien de forse toename in cvd-meldingen, worden die tegenwoordig in aparte grafieken hierboven getoond.

De verdeling incidenten per afhandeling wordt in figuur 12 getoond. De afhandeling van incidenten staat los van hoe de melding is binnengekomen of in welke categorie het incident valt. Hier gaat het alleen om de uitgevoerde acties. Bij 67 procent van alle incidenten levert het NCSC ondersteuning op afstand. Bij 20 procent van alle incidenten heeft het NCSC een 'notice-and-take-down' (NTD)-verzoek gedaan. Dit gebeurt bijvoorbeeld als een malafide website, bijvoorbeeld een phishingsite, offline moet worden gehaald. Als een incident een false positive blijkt te zijn, of als informatie ter kennisgeving is aangenomen, wordt het incident geregistreerd als niet in behandeling genomen. Dit is bij 9 procent van alle meldingen het geval geweest. In enkele gevallen (3 procent) heeft het NCSC ondersteuning op locatie geleverd. Deze verhoudingen zijn in grote lijnen hetzelfde als in de vorige rapportageperiode.

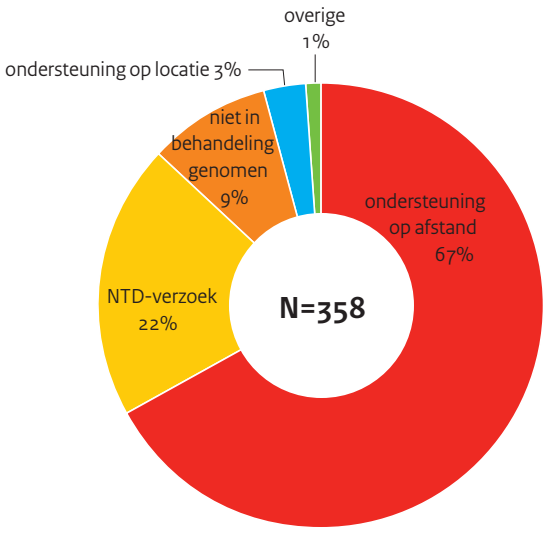
Verdeling incidenten tussen overheid en vitale sectoren

Het NCSC ondersteunt zowel de Rijksoverheid als de vitale infrastructuur bij beveiligingsincidenten. Daarnaast treedt het NCSC op als contactpunt voor internationale hulpverzoeken met betrekking tot informatiebeveiliging. In figuur 13 is te zien wat de verdeling is van het aantal afgehandelde incidenten tussen publieke, private en internationale partijen. In totaal was bij ongeveer 38 procent van de incidenten een publieke organisatie betrokken. Bij 42 procent ging het om een private organisatie. De resterende 20 procent betrof een internationale partij. Een voorbeeld hiervan is het ontvangen van een malwarerapport van een collega CSIRT-organisatie in een ander land. Ook kan een buitenlandse organisatie het NCSC vragen om een in Nederland gehoste malafide website offline te laten halen.

Figuur 14 toont de verdeling tussen incidentcategorieën per type organisatie. Onderaan iedere staaf wordt aangegeven over welke type organisatie de verdeling gaat en hoeveel incidenten daarin vertegenwoordigd worden.

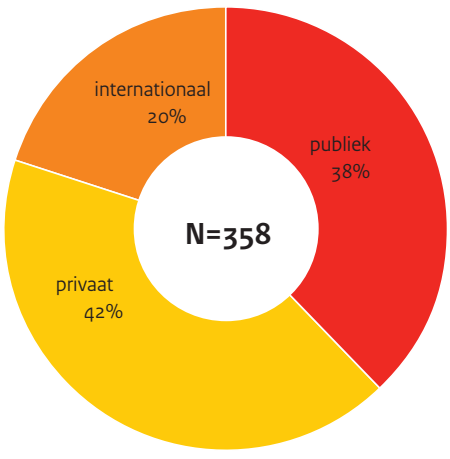
In ongeveer 20 procent van alle incidenten is er sprake van malware, ongeacht het type organisatie. Bij incidenten die onder de categorie verzameling van informatie vallen, is het verschil groter. In 36 procent van alle gevallen waar er een internationale partij betrokken is, gaat het hierom. In de praktijk heeft het merendeel van deze incidenten met phishingcampagnes te maken. Uit deze figuur blijkt verder dat (poging tot) inbraak vaker voorkomt (17 procent) bij incidenten in de private sector dan die waarbij een publieke (12 procent) of een internationale partij (9 procent) betrokken is.

Figuur 12 **Afgehandelde incidenten per afhandeling**



Bron: NCSC

Figuur 13 **Afgehandelde incidenten per type organisatie**

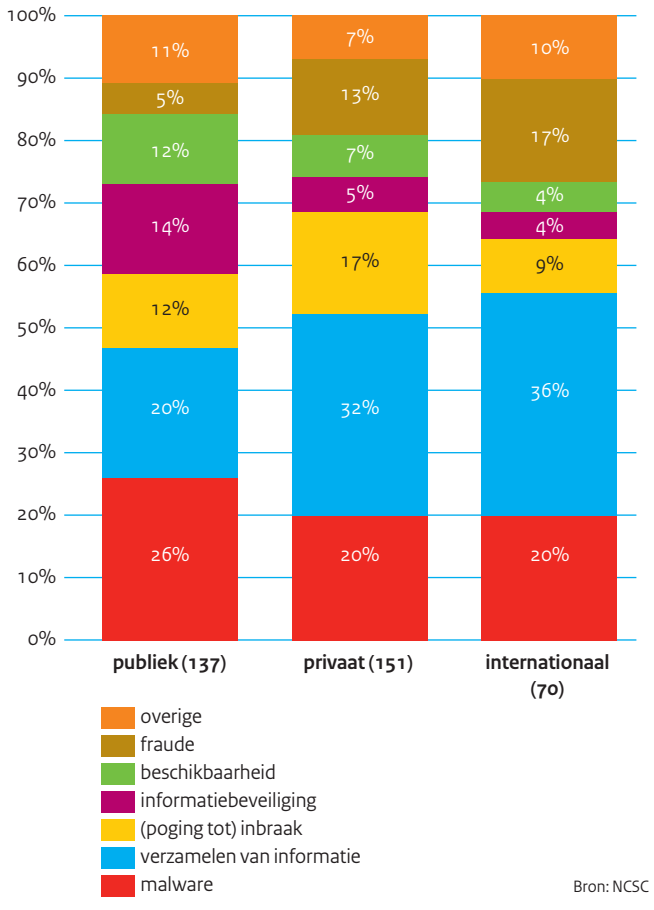


Bron: NCSC

Een dergelijke verdeling is ook te zien bij incidenten op het gebied van informatiebeveiliging. Zulke incidenten hebben vaak te maken met ongeautoriseerde toegang tot gevoelige informatie of systemen. Dit type incident wordt vaker gemeld vanuit de publieke sector (14 procent) dan vanuit de private sector (5 procent) of een internationale partij (4 procent). Een voorbeeld hiervan is het melden van een websitekwetsbaarheid die een aanvaller in staat zou kunnen stellen om een klantenbestand in te zien. Ook incidenten waar er sprake is van een aanval op de beschikbaarheid van een organisatie worden vaker gemeld vanuit de publieke sector (12 procent) dan vanuit de private sector (7 procent) of een internationale partij (4 procent).

Op het gebied van phishing wordt onderscheid gemaakt tussen phishingcampagnes die gericht zijn op het ophalen van inloggegevens, die onder verzameling van informatie vallen, en websites die bij phishingcampagnes worden gebruikt die zonder toestemming de naam, het logo of huisstijl van een derde partij misbruiken, deze vallen onder fraude. Net zoals bij verzamelen van informatie komt de categorie fraude veel vaker voor vanuit internationale partijen (17 procent) dan vanuit private (13 procent) of publieke (5 procent) partijen.

Figuur 14 **Incidentencategorieën per type organisatie**



Bron: NCSC

Nationaal Detectie Netwerk

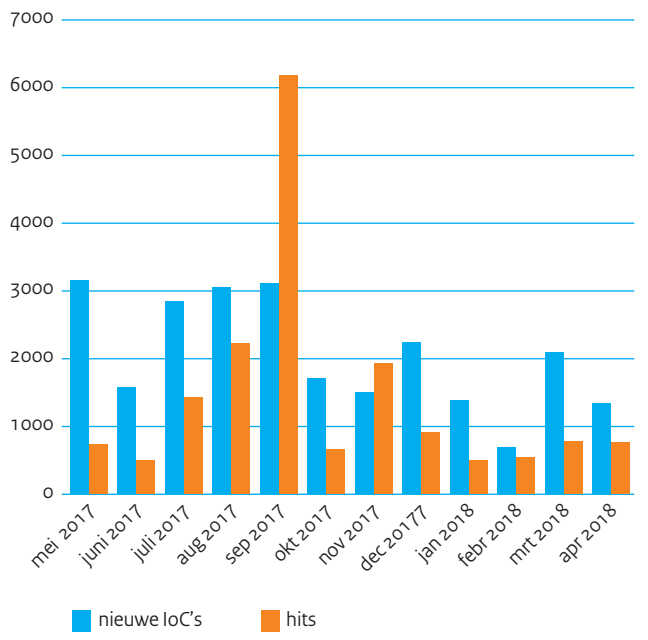
Het Nationaal Detectie Netwerk (NDN) is een samenwerking voor het beter en sneller waarnemen van digitale dreigingen en risico's. Door het delen van dreigingsinformatie kunnen partijen vanuit de eigen verantwoordelijkheid tijdig gepaste maatregelen nemen om mogelijke schade te beperken of voorkomen.

Binnen het NDN worden 'indicators of compromise' (IoC's) gedeeld met deelnemende partijen. Een IoC is informatie die kan helpen bij het identificeren van specifiek malafide gedrag op een systeem of binnen een netwerk. In de praktijk zijn dit vaak ip-adressen of domeinnamen. In het geval dat een gedeelde IoC leidt tot het waarnemen van malafide gedrag bij een deelnemende partij, is er sprake van een 'hit'.

Een hit geeft alleen aan dat er gedrag waargenomen is dat overeenkomt met de gedeelde informatie. Dit zegt echter niet dat een deelnemende partij per se is gecompromitteerd. Als een defensieve maatregel, zoals een firewall, antivirus of intrusion detection system (IDS) de malafide software of netwerkverkeer tegenhoudt, wordt dit als een 'hit' geregistreerd terwijl geen werkelijke besmetting plaats heeft gevonden.

Figuur 15 toont het aantal nieuwe IoC's dat actief gedeeld worden binnen het NDN. Ook het aantal hits wordt hierin weergegeven. In totaal zijn er 25.049 nieuwe IoC's gedeeld, ongeveer 2.087 per maand. Slechts een klein aantal hiervan wordt daadwerkelijk aangetroffen. In totaal werden 17.506 hits waargenomen, ongeveer 1.459 per maand. Er waren in september relatief veel hits. Dit was het gevolg van een grote phishingcampagne.

Figuur 15 **Actieve IoC's en Hits**



Bron: NCSC

Bijlage 2
Afkortingen- en begrippenlijst

o-day	Zie Zero-daykwetsbaarheid.
Aanval	Een digitale aanval is een opzettelijke inbreuk op cybersecurity.
Aanvalsfacilitator	Crimineel die middelen en infrastructuur ontwikkelt en uitbaat om andere actoren tegen betaling in staat te stellen digitale aanvallen uit te voeren.
Actor	Persoon, groep of organisatie die een dreiging vormt.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst.
AP	Autoriteit Persoonsgegevens.
Authenticatie	Het vaststellen van de identiteit van een gebruiker, computer of applicatie.
Beschikbaarheid	Beschikbaarheid betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).
Bitcoin	Digitale munteenheid, zie cryptovaluta.
Botnet	Een verzameling van besmette systemen die door actoren centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
Clouddienst	Ict-infrastructuur die via het internet beschikbaar wordt gesteld als dienst.
Crimineel	Actor die aanvallen pleegt met economische of financiële motieven.
Cryptojacking	Het (zonder medeweten van de eigenaar) gebruiken van de rekenkracht van systemen om cryptovaluta te delven.
Cryptomining	Het delven van cryptovaluta door het uitvoeren van cryptografische berekeningen.
Cryptovaluta	Verzamelnaam voor digitale munteenheden die cryptografische berekeningen gebruiken als echtheidskenmerk en voor transacties.
Cvd	Coordinated vulnerability disclosure is de praktijk van het gecoördineerd melden van aangetroffen beveiligingslekken. Hierbij worden afspraken gehanteerd die doorgaans neerkomen op dat de melder de ontdekking niet deelt met derden totdat het lek verholpen is, en de getroffen partij geen juridische stappen tegen de melder zal ondernemen. Voorheen werd dit responsible disclosure genoemd.

Cybercrime	Vorm van criminaliteit gericht op ict of de informatie die een ict-systeem verwerkt. Er zijn verschillende soorten cybercrime: • in enge zin, een vorm van criminaliteit met ict als doelwit (high tech crime); • een vorm van criminaliteit waarbij voor de uitvoering het gebruik van ict van overwegende betekenis is (cybercriminaliteit); • in brede zin, iedere vorm van (traditionele) criminaliteit waarbij gebruik wordt gemaakt van ict (gedigitaliseerde criminaliteit).
Cybercrime-as-a-service	Cybercrime-as-a-service is een werkwijze in de ondergrondse economie waarbij actoren gebruik kunnen maken van de (betaalde) diensten van aanvalsfacilitatoren om aanvallen te plegen.
Cybervandaal	Zie scriptkiddie.
Cybersecurity	Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ict te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan. Die schade kan bestaan uit de aantasting van de beschikbaarheid, vertrouwelijkheid of integriteit van informatiesystemen en informatiediensten en de daarin opgeslagen informatie.
DDoS	Distributed Denial of Service is een vorm van DoS waarbij een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar wordt gemaakt door deze te bestoken met veel netwerkverkeer vanuit een groot aantal verschillende bronnen.
Defacement	Een defacement (of bekladding) is het vervangen van een webpagina met de boodschap dat deze gehackt is, eventueel met aanvullende boodschappen van activistische, idealistische of aanstootgevende aard.
DKIM	DomainKeys Identified Mail is een protocol om legitieme e-mail door de verzendende e-mailserver digitaal te laten ondertekenen. De eigenaar van het verzendende domein publiceert legitiem sleutels in een DNS-record.
DMARC	Domain-based Message Authentication, Reporting and Conformance is een protocol waarmee de eigenaar van een domein aangeeft wat er met niet-authentieke e-mail vanaf zijn domein moet gebeuren. De authenticiteit van de e-mail wordt eerst vastgesteld aan de hand van SPF en DKIM. De domeineigenaar publiceert het gewenste beleid in een DNS-record.
DNS	Het Domain Name System is het systeem dat internetdomeinnamen koppelt aan ip-adressen en omgekeerd. Zo staat het adres www.ncsc.nl bijvoorbeeld voor ip-adres 159.46.193.36. Verder vermeldt een DNS-record onder meer hoe e-mails aan dat domein afgehandeld moeten worden.
DoS	Denial of Service is de benaming voor een type aanval die een bepaalde dienst (bijvoorbeeld een website) niet beschikbaar maakt voor de gebruikelijke afnemers. Bij websites wordt meestal een DDoS-aanval uitgevoerd.
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
Exploit	Software, gegevens of een opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om ongewenste functies of gedrag te veroorzaken.
Exploitkit	Hulpmiddel om een aanval op te zetten door te kiezen uit kant-en-klare exploits, in combinatie met gewenste gevolgen en besmettingsmethode.
Hacker/Hacken	De meest gangbare en de in dit document gehanteerde betekenis van hacker is iemand die met kwaadaardige bedoelingen probeert in te breken in ict-systemen. Oorspronkelijk werd de term hacker gebruikt voor iemand die op onconventionele wijze gebruikmaakt van techniek (waaronder software), veelal om beperkingen te omzeilen of onverwachte effecten te bereiken.

Hacktivist	Samentrekking van hacker en activist: actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt.
ICS	Industriële controlesystemen zijn meet- en regelsystemen, bijvoorbeeld voor de aansturing van industriële processen of gebouwbeheersystemen. ICS verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten.
Incident	Een incident is een gebeurtenis waarbij informatie, informatiesystemen of -diensten verstoord worden, uitvallen of misbruikt worden.
Informatiebeveiliging	Informatiebeveiliging is het proces van het vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit, alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiediefstal	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
Informatiemanipulatie	Het opzettelijk wijzigen van informatie; aantasting van de integriteit van informatie.
Injectie	Aanvalstechniek waarbij gebruikersinvoer wordt gemanipuleerd om naast gegevens ook systeemopdrachten te bevatten. SQL-injectie wordt vaak gebruikt om communicatie tussen een applicatie en de achterliggende database te beïnvloeden, om gegevens te manipuleren of stelen.
Insider	Een interne actor die met toegang tot systemen of netwerken van binnenuit een dreiging vormt, met als motief wraak, geldelijk gewin of ideologie. Een insider kan ook worden ingehuurd of opgedragen van buitenaf.
Integriteit	Integriteit omhelst het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan.
IoT	Het internet of things is een netwerk van slimme apparaten, sensoren en andere objecten die (vaak verbonden met het internet) gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi-) autonome beslissingen of acties nemen die van invloed zijn op hun omgeving.
Ip	Het internetprotocol zorgt voor de adressering van internetverkeer zodat het bij het beoogde doel aankomt.
Kwetsbaarheid	Eigenschap van een samenleving, organisatie of informatiesysteem (of een onderdeel daarvan) die een kwaadwillende partij de kans geeft om de legitieme toegang tot informatie of functionaliteit te verhinderen en te beïnvloeden, of om die ongeautoriseerd te benaderen.
Lek	Aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.
Malware	Samentrekking van malicious software. Malware is de term die als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en trojans.
Middel	Een techniek of computerprogramma waarmee een aanvaller misbruik kan maken van bestaande kwetsbaarheden of deze kan vergroten.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst.
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben informatie aan mensen te ontfutselen. Deze informatie kan worden misbruikt voor bijvoorbeeld fraude of identiteitsdiefstal.
Ransomware	Gijzelsoftware. Type malware dat systemen of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt.

Sabotage	Het opzettelijk, zeer langdurig, aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten. In extreme gevallen leidend tot vernietiging.
Scriptkiddie	Actor met beperkte kennis die hulpmiddelen gebruikt die door anderen zijn bedacht en ontwikkeld, voor digitale aanvallen, om kwetsbaarheden aan te tonen of voor de eigen uitdaging.
Spam	Ongewenste e-mail, doorgaans commercieel van aard.
Spearphishing	Spearphishing is een variant van phishing die zich richt op één persoon of beperkte groep mensen, die specifiek wordt uitgekozen op basis van hun toegangspositie, om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.
SPF	Sender Policy Framework is een protocol waarmee de eigenaar van een domeinnaam aangeeft welke servers er legitiem e-mail namens zijn domein mogen versturen. De domeinnaameigenaar publiceert de lijst met geautoriseerde servers in een DNS-record.
Spionage	Aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
Staatsgelieerde actor	Actor gelieerd aan een statelijke actor.
Statelijke actor	Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage).
Storing	Zie uitval of verstoring.
Systeemmanipulatie	Het aantasten van informatiesystemen en -diensten gericht op de vertrouwelijkheid of integriteit van informatiesystemen en -diensten. Deze systemen of diensten worden daarna ingezet om andere aanvallen uit te voeren.
Terrorist	Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolkingsgroepen angst wil aanjagen of politieke besluitvorming probeert te beïnvloeden, door geweld tegen mensen te gebruiken of ontwrichtende schade aan te richten.
Trojan	Type malware dat heimelijk toegang tot een systeem biedt aan een aanvaller via een achterdeur.
Tweefactorauthenticatie	Een manier van identiteit vaststellen waarvoor twee onafhankelijke bewijzen van identiteit zijn vereist.
Uitval	Aantasting van de integriteit en beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.
Verstoring	Het opzettelijk, tijdelijk, aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten.
Vertrouwelijkheid	Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoen zijn geautoriseerd.
Wiperware	Type malware dat sabotage pleegt door gegevens te verwijderen of permanent ontoegankelijk te maken.
Worm	Type malware dat zichzelf automatisch verspreidt onder andere systemen.
Zero-daykwetsbaarheid	Een zero-daykwetsbaarheid is een kwetsbaarheid waarvoor nog geen patch beschikbaar is, omdat de maker van de kwetsbare software nog geen tijd (nul dagen) heeft gehad om de kwetsbaarheid te verhelpen.

Bijlage 3
Bronnen en referenties

1 Nederlandse Cybersecurity Agenda 2018.
2 Economic Impact of Cybercrime - No Slowing Down, McAfee & CSIS, februari 2018, blz. 3 en Risicorapportage Cyberveiligheid Economie, Centraal Planbureau, Den Haag, 3 juli 2017, blz. 8-11.
3 ENISA Threat Landscape Report 2017. 15 Top Cyber-Threats and Trends, ENISA, januari 2018, blz. 107.
4 Jaarverslag AIVD 2017, DNI Worldwide threat assessment (2018).
5 Jaarverslag AIVD 2017, blz 8 e.v.
6 ENISA Threat Landscape Report 2017 (2018).
7 Crowdstrike 2018 Global Threat Report. Blurring the lines between statecraft and tradecraft.
8 Kaspersky, Spy wars: how nation-state backed threat actors steal from and copy each other, oktober 2017. Vervagende grenzen ook in FireEye Looking ahead: cyber security in 2018 en DNI Worldwide threat assessment (2018).
9 FireEye Looking ahead: cyber security in 2018.
10 Jaarverslag AIVD 2017.
11 DNI Worldwide threat assessment (2018).
12 MMC CYBER HANDBOOK 2018. Perspectives on the next wave of cyber.
13 https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/, geraadpleegd op 7 mei 2018.
14 M-trends 2018.
15 FireEye Looking ahead: cyber security in 2018.
16 https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/, geraadpleegd op 9 april 2018.
17 https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/, geraadpleegd op 9 april 2018.
18 http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch, geraadpleegd op 11 april 2018.
19 https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/, geraadpleegd op 9 april 2018.
20 http://www.bbc.com/news/technology-40428967, geraadpleegd op 9 april 2018.
21 https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe, geraadpleegd op 9 april 2018.
22 https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe, geraadpleegd op 9 april 2018.
23 http://www.ictmagazine.nl/maersk-lijdt-rond-300-miljoen-schade-ransomware-aanval/, geraadpleegd op 9 april 2018.
24 https://tweakers.net/nieuws/134473/maersk-herinstalleerde-45000-pcs-in-10-dagen-na-notpetya-aanval.html, geraadpleegd op 9 april 2018.
25 https://nos.nl/artikel/2180251-nieuwe-aanvallen-met-gijzelvirus-ook-pakketbezorger-tnt-getroffen.html, geraadpleegd op 11 april 2018.
26 http://blog.talosintelligence.com/2017/07/the-medoc-connection.html, geraadpleegd 9 april 2018.
27 https://www.wired.com/story/white-house-russia-notpetya-attribution/, geraadpleegd op 9 april 2018.
28 https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf, geraadpleegd 12 april 2018.
29 Het gebruik van spear phishing door Russische actoren is bijvoorbeeld uitgebreid gedocumenteerd in F-Secure, The Dukes. 7 years of Russian cyberespionage.
30 Bijvoorbeeld in 'Study reveals North Korean cyber-espionage has reached new heights', The Guardian 20 februari 2018, geraadpleegd op 12 april 2018.

31 Jaarverslag AIVD 2017; https://nos.nl/artikel/2207027-duitse-inlichtingenchef-china-rekruteert-via-linkedin.html, geraadpleegd op 30 maart 2018.
32 ENISA Threat Landscape Report 2017 (2018) en Verizon 2018 Data Breach Investigations Report.
33 In de brochure Bent u zich bewust van de risico's van cyberspionage? (AIVD, MIVD 2017) wordt ingegaan op basismaatregelen die getroffen kunnen worden.
34 IBM X-Force Threat Intelligence Index 2018, 24.
35 DNI Worldwide threat assessment (2018).
36 Cybersecuritybeeld Nederland 2017.
37 Symantec 2018 cyber security predictions.
38 Crowdstrike 2018 Global Threat Report. Blurring the lines between statecraft and tradecraft; IBM X-Force Threat Intelligence Index 2018.
39 AIVD Jaarverslag 2017.
40 https://www.nu.nl/internet/5206289/duizenden-nederlandse-identiteitsdocumenten-jarenlang-openbaar-datalek.html, geraadpleegd op 4 april 2018.
41 Persbericht Autoriteit Persoonsgegevens, '10.000 datalekken gemeld in 2017', 29 maart 2018.
42 Jaarverslag AIVD 2017; ENISA Threat Landscape Report 2017 (2018).
43 ENISA Threat Landscape Report 2017 (2018).
44 M. de Bruijne, M. van Eeten, C. Hernandez Ganan, W. Pieters, Towards a new cyber threat actor typology. A hybrid method fort he NCSC cyber security assessment (TU Delft 2017).
45 https://nos.nl/artikel/2214400-zware-ddos-aanvallen-wie-wat-waar-en-waarom.html, geraadpleegd op 11 april 2018.
46 https://nos.nl/artikel/2215746-verdachte-ddos-aanvallen-banken-moeten-het-op-orde-hebben.html, geraadpleegd op 11 april 2018.
47 https://nos.nl/artikel/2215507-18-jarige-brabander-opgepakt-voor-recente-ddos-aanvallen.html, geraadpleegd op 11 april 2018.
48 Cybersecuritybeeld Nederland 2016 en Cybersecuritybeeld Nederland 2014.
49 https://www.bankinfosecurity.com/interviews/crime-as-service-top-cyber-threat-for-2017-i-3406, geraadpleegd op 29 maart 2018.
50 Cybersecuritybeeld Nederland 2016 en Cybersecuritybeeld Nederland 2013, blz. 64.
51 https://nakedsecurity.sophos.com/2017/12/14/starbucks-wi-fi-hijacked-customers-laptops-to-mine-cryptocurrency/, geraadpleegd op 11 april 2018.
52 https://www.security.nl/posting/552971/Microsoft+detecteert+uitbraak+van+cryptomining-malware, geraadpleegd op 11 april 2018.
53 https://www.security.nl/posting/555742/Cryptominers+in+browser+steeds+lastiger+te+detecteren, geraadpleegd op 11 april 2018.
54 https://www.telegraph.co.uk/technology/2018/02/14/salon-website-asks-readers-mine-cryptocurrency/, geraadpleegd op 11 april 2018.
55 https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/, geraadpleegd op 30 maart 2018
56 MMC CYBER HANDBOOK 2018. Perspectives on the next wave of cyber; ENISA Threat Landscape Report 2017 (2018).
57 https://www.independent.co.uk/travel/news-and-advice/eurocontrol-air-traffic-systems-failure-flights-cancelled-delays-a8286651.html, geraadpleegd 9 april 2018.
58 https://www.documentcloud.org/documents/4427886-Level-3-FCC-report.html, geraadpleegd op 11 mei 2018.
59 https://www.bleepingcomputer.com/news/software/software-bug-behind-biggest-telephony-outage-in-us-history/, geraadpleegd op 7 mei 2018.
60 https://nos.nl/artikel/2229927-reconstructie-hoe-het-zondag-misging-op-schiphol.html, geraadpleegd op 3 mei 2018.
61 De economische en maatschappelijke noodzaak van meer Cybersecurity. Nederland digitaal droge voeten, september 2016 (https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf).
62 Vertrouwen in de toekomst. Regeerakkoord 2017 – 2021 VVD, CDA, D66 en ChristenUnie, 2017 (https://www.tweedekamer.nl/sites/default/files/atoms/files/regeerakkoord20172021.pdf).
63 Risicorapportage Cyberveiligheid Economie, Centraal Planbureau, 3 juli 2017, blz. 1 (https://www.cpb.nl/publicatie/risicorapportage-cyberveiligheid-economie), geraadpleegd op 28-3-2018.
64 De publieke kern van het internet. Naar een buitenlands internetbeleid, Wetenschappelijke Raad voor het Regeringsbeleid, Amsterdam: Amsterdam University Press, 2015.
65 Wereldwijd voor een veilig Nederland. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022, Ministerie van Buitenlandse Zaken, 2018 (https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs).
66 https://www.nctv.nl/binaries/strategie-nationale-veiligheid-2007_tcm31-32502.pdf, geraadpleegd op 7 mei 2018.
67 Nationaal Veiligheidsprofiel 2016, Bilthoven, 2016, blz. 9.
68 Cybersecuritybeeld Nederland 2015, blz 64.

69 Stroomvoorziening onder digitale spanning, Rli, maart 2018 (http://www.rli.nl/publicaties/2018/advies/stroomvoorziening-onder-digitale-spanning), geraadpleegd op 30 maart 2018.
70 Nationaal Veiligheidsprofiel 2016, Bilthoven, 2016, blz. 117-133.
71 Jaarverslag 2017, AIVD, maart 2018, blz. 10 (www.aivd.nl/jaarverslag2017).
72 Jaarverslag 2017, AIVD, maart 2018, blz. 8,9 (www.aivd.nl/jaarverslag2017).
73 Nationaal Veiligheidsprofiel 2016, Bilthoven, 2016, blz. 123.
74 Risicorapportage Cyberveiligheid Economie, Centraal Planbureau, Den Haag, 3 juli 2017, blz. 3.
75 Economic Impact of Cybercrime - No Slowing Down, McAfee & CSIS, February 2018, blz. 8-9.
76 Onderzoek NRC: platgaan computers Rijk nét afgewend, NRC, 10 september 2011 geraadpleegd op 26 maart 2018.
77 https://www.security.nl/posting/550347/Britse+overheid+beschuldigt+Rusland+van+NotPetya-aanval, geraadpleegd op 26 maart 2018.
78 http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en, geraadpleegd op 11 mei 2018.
79 Naar een veilig verbonden digitale samenleving. Advies inzake de cybersecurity van het Internet of Things (IoT), CyberSecurityRaad, 11 februari 2018 (https://www.cybersecurityraad.nl/binaries/CSR%20Advies%20IoT%20digitale%20versie%20DEF%20NED_tcm56-298518.pdf), geraadpleegd op 5 april 2018.
80 Kamerbrief over Kabinetsstandpunt encryptie, 4 januari 2016 (https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie/tk-kabinetsstandpunt-encryptie.pdf), geraadpleegd op 30 maart 2018 en Cyber Resilience Playbook for Public-Private Collaboration, World Economic Forum, januari 2018 (http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf), geraadpleegd op 6 april 2018.
81 Cyber Resilience Playbook for Public-Private Collaboration, World Economic Forum, januari 2018 (http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf), geraadpleegd op 6 april 2018 en Risicorapportage Cyberveiligheid Economie, Centraal Planbureau, Den Haag, 3 juli 2017, blz. 2.
82 https://www.security.nl/posting/534770/Symantec+geeft+overheden+geen+toegang+meer+tot+broncode, geraadpleegd op 6 april 2018 en https://www.security.nl/posting/537021/McAfee+geeft+overheden+geen+toegang+meer+tot+broncode, geraadpleegd op 6 april 2018.
83 Cyber Resilience Playbook for Public-Private Collaboration, World Economic Forum, January 2018, blz. 6 (http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf, geraadpleegd op 6 april 2018).
84 https://www.security.nl/posting/526657/Onderzoeker%3A+Lek+in+zonnepanelen+kan+stroomvoorziening+ontregelen, geraadpleegd op 7 mei 2018.
85 http://www.rli.nl/publicaties/2018/advies/stroomvoorziening-onder-digitale-spanning, geraadpleegd op 30 maart2018.
86 Cybersecuritybeeld Nederland 2017.
87 https://www.aivd.nl/publicaties/jaarverslagen/2018/03/06/jaarverslag-aivd-2017, geraadpleegd op 30 maart 2018.
88 https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, geraadpleegd op 13 april 2013.
89 https://nos.nl/artikel/2177859-waarschuwing-voor-industroyer-het-virus-dat-stroomnet-kan-platleggen.html, geraadpleegd op 13 april 2018.
90 https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, geraadpleegd op 13 april 2018.
91 https://www.zscaler.com/blogs/research/analysis-sandworm-cve-2014-4114-0-day, geraadpleegd op 13 april 2018.
92 https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html, geraadpleegd op 13 april 2018.
93 https://threatmatrix.cylance.com/en_us/home/energetic-dragonfly-dymalloy-bear-2-0.html, geraadpleegd op 13 april 2018.
94 https://www.us-cert.gov/ncas/alerts/TA17-293A, geraadpleegd op 13 april 2018.
95 https://www.us-cert.gov/ncas/alerts/TA18-074A, geraadpleegd op 13 april 2018.
96 https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html, geraadpleegd op 5 april 2018.
97 https://www.nctv.nl/binaries/CSBN2017_tcm31-267075.pdf, geraadpleegd op 13 april 2018.
98 http://www.bbc.com/news/uk-politics-43062113, geraadpleegd op 13 april 2018.
99 http://www.bbc.com/news/technology-39913630, geraadpleegd op 13 april 2018.
100 https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html, geraadpleegd op 13 april 2018.
101 https://securelist.com/bad-rabbit-ransomware/82851/, geraadpleegd op 13 april 2018.
102 https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/, geraadpleegd op 5 april 2018.
103 https://www.forbes.com/sites/thomasbrewster/2017/09/18/ccleaner-cybersecurity-app-infected-with-backdoor/#4206ad12316a, geraadpleegd op 13 april 2018.
104 http://blog.exodusintel.com/2017/07/26/broadpwn/, geraadpleegd op 13 april 2018.
105 https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2017-0838+1.00+Twee+kwetsbaarheden+ontdekt+in+Broadcom+WiFi-driver.html, geraadpleegd op 13 april 2018.

106 https://www.krackattacks.com/, geraadpleegd op 13 april 2018.
107 https://meltdownattack.com/, geraadpleegd op 13 april 2018.
108 https://www.ncsc.nl/actueel/nieuwsberichten/meltdown-en-spectre.html, geraadpleegd op 13 april 2018.
109 https://www.heise.de/ct/artikel/Super-GAU-fuer-Intel-Weitere-Spectre-Luecken-im-Anflug-4039134.html, geraadpleegd op 3 mei 2018.
110 https://amdflaws.com/, geraadpleegd op 12 april 2018.
111 https://www.wired.com/story/amd-backdoor-cts-labs-backlash/, geraadpleegd op 13 april 2018.
112 https://blog.trailofbits.com/2018/03/15/amd-flaws-technical-summary/, geraadpleegd op 12 april 2018.
113 https://www.vusec.net/projects/glitch/, geraadpleegd op 3 mei 2018.
114 https://www.bloomberg.com/news/articles/2017-10-02/urgent-equifax-2-5-million-more-americans-may-be-affected-by-hack, geraadpleegd op 5 april 2018.
115 https://investor.equifax.com/news-and-events/news/2018/03-01-2018-140531340, geraadpleegd op 5 april 2018.
116 https://investor.equifax.com/news-and-events/news/2017/11-09-2017-211550295, geraadpleegd op 5 april 2018.
117 https://www.nu.nl/internet/5017448/uber-verzweeg-datalek-van-57-miljoen-accounts.html, geraadpleegd op 30 maart 2018.
118 https://www.nu.nl/internet/5046449/data-174000-nederlanders-gelekt-bij-uber-hack.html, geraadpleegd op 30 maart 2018.
119 https://www.reuters.com/article/us-uber-cyber-payment-exclusive/exclusive-uber-paid-20-year-old-florida-man-to-keep-data-breach-secret-sources-idUSKBN1E101C, geraadpleegd op 5 april 2018.
120 https://www.nu.nl/internet/4989794/energieverbruik-alle-nederlandse-huishoudens-was-in-zien-datalek.html, geraadpleegd op 30 maart 2018.
121 https://mackeepersecurity.com/post/fedex-customer-records-exposed, geraadpleegd op 5 april 2018.
122 https://www.nu.nl/internet/5206289/duizenden-nederlandse-id-bewijzen-jarenlang-openbaar-datalek.html, geraadpleegd op 5 april 2018.
123 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_2018-02-23_2017_jaarrapportage_algemeen.pdf, geraadpleegd op 30 maart 2018.
124 https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf, geraadpleegd op 6 april 2018.
125 https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q3-2017-state-of-the-internet-security-report.pdf, geraadpleegd op 6 april 2018.
126 https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf, geraadpleegd op 6 april 2018.
127 https://www.arbornetworks.com/blog/insight/hacktivism-political-protest-ddos-attacks-target-czech-republic-spain/, geraadpleegd op 13 april 2018.
128 https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-waarschuwt-voor-misbruik-publiek-beschikbare-memcached-systemen-bij-ddos-aanvallen.html, geraadpleegd op 13 april 2018.
129 https://www.sidnlabs.nl/a/nieuws/een-proactieve-en-collectieve-ddos-bestrijdingsstrategie-voor-de-nederlandse-vitale-infrastructuur, geraadpleegd op 6 april 2018.
130 https://www.armor.com/app/uploads/2018/03/2018-Q1-Reports-BlackMarket-DIGITAL.pdf, geraadpleegd op 6 april 2018.
131 https://www.wired.com/story/github-ddos-memcached/, geraadpleegd op 5 april 2018.
132 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf, geraadpleegd op 11 april 2018.
133 https://businesstech.co.za/news/industry-news/206328/why-phishing-attacks-are-so-effective/, geraadpleegd op 11 april 2018.
134 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf, geraadpleegd op 11 april 2018.
135 https://nos.nl/artikel/2199450-na-apen-mailadressen-tweede-kamer-relatief-makkelijk.html, geraadpleegd op 30 maart 2018.
136 https://www.ad.nl/politiek/iedereen-kan-mailen-namens-de-aivd~a0200b89/, geraadpleegd op 30 maart 2018.
137 https://www.cyberscoop.com/russians-foreigners-spoofing-gov-email-dmarc-proofpoint/, geraadpleegd op 30 maart 2018.
138 https://tweakers.net/nieuws/132585/apple-mail-outlook-2016-en-veel-andere-mailclients-zijn-kwetsbaar-voor-spoofing.html, geraadpleegd op 30 maart 2018.
139 https://nos.nl/op3/artikel/2176061-hang-op-klik-weg-of-bel-je-oom.html, geraadpleegd op 5 april 2018.
140 https://www.aivd.nl/publicaties/jaarverslagen/2018/03/06/jaarverslag-aivd-2017, geraadpleegd op 5 april 2018.
141 https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary, geraadpleegd op 24 maart 2018.
142 http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf, geraadpleegd op 30 maart 2018.
143 http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf, geraadpleegd op 30 maart 2018.
144 https://www.nctv.nl/binaries/CSBN2017_tcm31-267075.pdf, geraadpleegd op 30 maart 2018.
145 https://info.microsoft.com/rs/157-GQE-382/images/EN-US_CNTNT-eBook-SIR-volume-23_March2018.pdf, geraadpleegd op 5 april 2018.

146 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf, geraadpleegd op 11 april 2018.
147 https://www.sidn.nl/a/veilig-internet/aantal-phishingsites-met-nederlandse-topmerken-ruim-40-toegenomen-, geraadpleegd op 11 april 2018.
148 https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf, geraadpleegd op 12 april 2018.
149 https://www.imperva.com/blog/2018/01/our-analysis-of-1019-phishing-kits/, geraadpleegd op 11 april 2018.
150 https://info.phishlabs.com/blog/quarter-phishing-attacks-hosted-https-domains, geraadpleegd op 12 april 2018.
151 https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_EN_final.pdf, geraadpleegd op 4 april 2018.
152 https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_EN_final.pdf, geraadpleegd op 5 april 2018.
153 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017, geraadpleegd op 5 april 2018.
154 https://www.aivd.nl/publicaties/jaarverslagen/2018/03/06/jaarverslag-aivd-2017, geraadpleegd op 5 april 2018.
155 https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-3.html, geraadpleegd op 29 maart 2018.
156 https://pages.checkpoint.com/global-cyber-attack-trends-2017.html?utm_source=research&utm_medium=cp-website&utm_campaign=CM_WR_18Q1_WW_Threat_Intelligence_Trends_Report_2017_H2, geraadpleegd op 11 april 2018.
157 http://www.bbc.com/news/world-europe-43003740, geraadpleegd op 11 april 2018.
158 https://www.bitsonline.com/australian-meteorology-staffers-questioned-sneaky-mining-operation/, geraadpleegd op 11 april 2018.
159 https://www.nu.nl/cryptovaluta/5154917/bedrijf-mocht-werknemer-niet-staande-voet-ontslaan-minen-bitcoins.html, geraadpleegd op 11 april 2018.
160 https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/, geraadpleegd op 11 april 2018.
161 https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators, geraadpleegd op 11 april 2018.
162 https://press.avast.com/cybercriminals-could-build-cryptomining-armies-using-vulnerable-iot-devices-at-mobile-world-congress-2018, geraadpleegd op 11 april 2018.
163 http://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html, geraadpleegd op 11 april 2018.
164 https://www.darkreading.com/attacks-breaches/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/d/d-id/1331017?piddl_msgorder=asc, geraadpleegd op 5 april 2018.
165 https://arxiv.org/pdf/1803.02887.pdf, geraadpleegd op 4 april 2018.
166 https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency, geraadpleegd op 5 april 2018.
167 https://blog.checkpoint.com/2018/01/15/decembers-wanted-malware-crypto-miners-affect-55-businesses-worldwide/, geraadpleegd op 5 april 2018.
168 https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/, geraadpleegd op 30 maart 2018.
169 https://medium.com/pcmag-access/why-hackers-love-cryptocurrency-miner-coinhive-e808c1b527fb, geraadpleegd op 13 april 2018.
170 https://tweakers.net/nieuws/135735/opt-in-variant-van-coinhive-cryptominer-wordt-nauwelijks-gebruikt.html, geraadpleegd op 12 april 2018.
171 https://wccftech.com/the-pirate-bay-cryptojacking-mine-monero/, geraadpleegd op 30 maart 2018.
172 https://www.theguardian.com/technology/2017/dec/13/video-site-visitors-unwittingly-mine-cryptocurrency-as-they-watch-report-openload-streamango-rapidvideo-onlinevideoconverter-monero, geraadpleegd op 5 april 2018.
173 https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/, geraadpleegd op 11 april 2018.
174 http://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html, geraadpleegd op 11 april 2018.
175 https://cloudblogs.microsoft.com/microsoftsecure/2018/03/13/invisible-resource-thieves-the-increasing-threat-of-cryptocurrency-miners/, geraadpleegd op 11 april 2018.
176 https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#420b1f905ae8, geraadpleegd op 11 april 2018.
177 http://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html, geraadpleegd op 11 april 2018.
178 https://www.malwarebytes.com/pdf/white-papers/CTNT-Q1-2018.pdf, geraadpleegd op 11 april 2018.
179 https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/, geraadpleegd op 2 mei 2018.
180 https://www.telegraaf.nl/nieuws/1905093/cyberaanval-pas-na-half-jaar-ontdekt, geraadpleegd op 12 april 2018.
181 https://www.uwv.nl/overuwv/Images/factsheet-arbeidsmarkt-ict.pdf, geraadpleegd op 11 mei 2018.
182 https://fd.nl/economie-politiek/1251379/noodklok-over-nederlandse-braindrain-bij-cybersecurity, geraadpleegd op 7 mei 2018.
183 https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy, geraadpleegd op 7 mei 2018.

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

Meer informatie
https://www.nctv.nl
info@nctv.minvenj.nl
@nctv_nl

Juni 2018