Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Cybersecuritybeeld Nederland

CSBN 2017

Nationaal Coördinator Terrorismebestrijding en Veiligheid

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.

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het bieden van expertise en advies, respons op dreigingen en het versterken van de crisisbeheersing. Daarnaast biedt het NCSC informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Het NCSC is een onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Samenwerking en bronnen

Bij het opstellen van dit rapport heeft het NCSC dankbaar gebruik gemaakt van informatie die de volgende partijen beschikbaar hebben gesteld:

- De ministeries
- Nederlandse ambassades
- Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
- DefCERT
- Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
- Politie (Team High Tech Crime)
- Openbaar Ministerie
- Vertegenwoordigers van organisaties in de vitale infrastructuur, leden van de information sharing & analysis centres (isacs) en andere NCSC-partners
- Nationale Beheersorganisatie Internet Providers
- Platform Internetstandaarden
- Bits of Freedom
- FME
- Nederland ICT
- Betaalvereniging Nederland
- VNO-NCW
- Wetenschappelijke instellingen
- Universiteiten
- Experts uit het cybersecuritywerkveld

De bijdragen van deze partijen hebben samen met inhoudelijke reviews, openbaar toegankelijke bronnen, een enquête, informatie van de vitale infrastructuur en analyses van het NCSC bijgedragen aan de inhoudelijke kwaliteit van het Cybersecuritybeeld Nederland.

Inhoud

Kernbevindingen

Beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan

Digitale aanvallen worden gebruikt om democratische processen te beïnvloeden

De kwetsbaarheid van het internet of things heeft tot verstorende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven

Veel organisaties zijn afhankelijk van een beperkt aantal buitenlandse aanbieders van digitale infrastructuurdiensten waardoor de maatschappelijke impact bij verstoring groot is

Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging

Samenvatting

Het Cybersecuritybeeld Nederland (CSBN) 2017 biedt inzicht in de belangen, dreigingen en weerbaarheid en daarmee samenhangende ontwikkelingen op het gebied van cybersecurity. Dit CSBN richt zich primair op Nederland, over de periode mei 2016 tot en met april 2017. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid gepubliceerd en komt tot stand in samenwerking met publieke en private partners.

Kernbevindingen

- Beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan
- Digitale aanvallen worden gebruikt om democratische processen te beïnvloeden
- De kwetsbaarheid van het internet of things heeft tot verstorende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven
- Veel organisaties zijn afhankelijk van een beperkt aantal buitenlandse aanbieders van digitale infrastructuurdiensten waardoor de maatschappelijke impact bij verstoring groot is
- Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging

De afgelopen jaren werd duidelijk welke impact digitale aanvallen op de samenleving kunnen hebben. De vrijwel onbeperkte schaalbaarheid van aanvallen zorgt ervoor dat het voor criminelen interessant is zich toe te leggen op cybercrime. Deze dreiging groeit: beroepscriminelen richten zich in steeds grotere mate op grote bedrijven, met als doel financieel gewin. Statelijke actoren blijven zich bezighouden met digitale sabotage en economische en politieke spionage. Zij intensiveren hun activiteiten en hebben zich daarnaast het afgelopen jaar ook gericht op digitale beïnvloeding van democratische processen voor geopolitiek gewin. De omvang van de digitale dreiging neemt toe. Wereldwijd spioneren meer dan honderd landen met digitale middelen.

Cyberaanvallen hebben geleid tot het uitlekken van informatie rond de Amerikaanse presidentsverkiezingen en in meerdere landen is beïnvloeding van democratische processen waargenomen of zijn pogingen daartoe geconstateerd. Nederland heeft in de aanloop naar de Tweede Kamerverkiezingen voorlichting gegeven om de digitale weerbaarheid van politieke partijen en organisaties betrokken bij de verkiezingen voor te vergroten.

Kosten en baten van cybersecurity liggen niet altijd bij dezelfde partij: misbruik van kwetsbaarheden kan tot schade leiden bij andere partijen dan de gebruikers van apparaten. Het internet of things laat zien dat dit mis kan gaan: veel van deze apparaten bevatten kwetsbaarheden waarvoor geen beveiligingsupdates uitkomen. Het afgelopen jaar zijn kwetsbare apparaten een aantal keer misbruikt om grote DDoS-aanvallen uit te voeren met botnets, waardoor verstoringen opgetreden zijn. Gebruikers van de apparaten hebben hiervan veelal geen last, aangevallen doelwitten wel. Dat deze aanvallen mogelijk uitgevoerd zijn door cybervandalen laat zien dat niet alleen geavanceerde beroepscriminelen of statelijke actoren verstorende aanvallen kunnen uitvoeren.

Nederland is sterk afhankelijk van dienstverlening van een beperkt aantal buitenlandse aanbieders van infrastructuurdiensten, zoals Amazon Web Services, Microsoft en Google. Hoewel grote dienstenleveranciers 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.

Het inzicht in de maatregelen die organisaties en individuen treffen om hun digitale weerbaarheid te vergroten is beperkt. De groei van het aantal manifestaties geeft echter de indicatie dat de weerbaarheid in Nederland achterblijft bij de groei van de dreiging.

Inzicht in dreigingen en actoren

Tabel 1 geeft inzicht in de dreigingen die de verschillende actoren vormden over de periode mei 2016 tot en met april 2017 voor de doelwitten 'overheden', 'private organisaties' en 'burgers'. Beroepscriminelen en statelijke actoren blijven onverminderd een grote dreiging voor overheid, private organisaties en burgers. Dreigingen die aangegeven zijn met een rode kleur kunnen toenemen terwijl het niveau al als hoog wordt geïdentificeerd.

Dreigingen die ten opzichte van het CSBN 2016 gegroeid of gekrompen zijn, worden aangegeven met een pijl. Statelijke actoren richten zich ook op diefstal en publicatie van informatie, bijvoorbeeld op democratische processen te beïnvloeden, naast spionage en het uitvoeren van offensieve activiteiten. De dreiging die uitgaat van hacktivisten is voor alle doelwitten gegroeid waar het gaat om defacements en voor burgers de overname van ict. Zij hebben het afgelopen jaar aangetoond in staat te zijn defacements uit te voeren en ict-systemen over te kunnen nemen, en dit ook te doen. De dreiging van manipulatie van informatie van burgers door beroepscriminelen is gekrompen ten opzichte van vorig jaar.

Tabel 1 **Dreigingsmatrix**

		Doelwitten	
Bron van dreiging	Overheden	Private organisaties	Burgers
Beroepscriminelen	Verstoring ICT	Verstoring ICT	Verstoring ICT
	Manipulatie van informatie	Manipulatie van informatie	Manipulatie van informatie ↓
	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie
	Overname ICT	Overname ICT	Overname ICT
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten	
	Diefstal en publicatie van informatie	Diefstal en publicatie van informatie	
Terroristen	Verstoring/overname van ICT	Verstoring/overname van ICT	
Cybervandalen en scriptkiddies	Diefstal informatie	Diefstal informatie	Diefstal en publicatie van informatie
	Verstoring ICT	Verstoring ICT	
Hacktivisten	Diefstal en publicatie verkregen informatie	Diefstal en publicatie verkregen informatie	
	Defacement ↑	Defacement ↑	
	Verstoring ICT	Verstoring ICT	
	Overname ICT	Overname ICT	Overname ICT ↑
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie	Diefstal en publicatie of verkoop verkregen informatie	
	Verstoring ICT	Verstoring ICT	
Private organisaties		Diefstal informatie (bedrijfsspionage)	Commercieel ge-/misbruik of 'doorverkopen' gegevens
Geen actor	Uitval ICT	Uitval ICT	Uitval ICT

Legenda relevantie

Geel: *Er worden geen nieuwe trends of fenomenen onderkend waar de dreiging van uitgaat.*
OF Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen.
OF Er hebben zich geen noemenswaardige incidenten van de dreiging voorgedaan in de rapportageperiode.

Oranje: *Er worden nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat.*
OF Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen.
OF Incidenten hebben zich voorgedaan buiten Nederland, enkele kleine in Nederland.

Rood: *Er zijn duidelijke ontwikkelingen die de dreiging acuut maken.*
OF Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft.
OF Incidenten hebben zich voorgedaan in Nederland.

Wijzigingen ten opzichte van CSBN 2016:
↑ Dreiging is toegenomen
↓ Dreiging is afgenomen

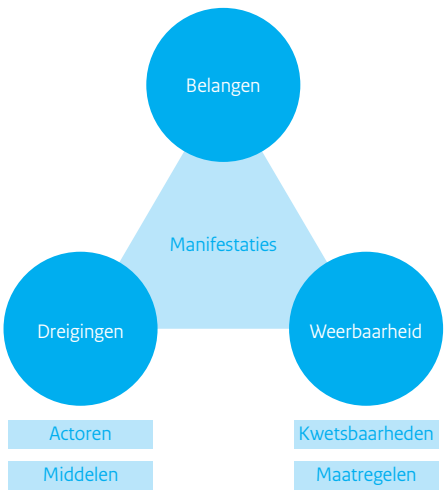
Leeswijzer

Het CSBN 2017 biedt inzicht in belangen, dreigingen, weerbaarheid en manifestaties op het gebied van cybersecurity, en daarmee samenhangende ontwikkelingen. Er wordt zowel een feitelijk overzicht als een duiding gegeven, over de periode mei 2016 tot en met april 2017. Het CSBN is tot stand gekomen op basis van de inzichten en de expertise van overheidsdiensten en organisaties in vitale processen. 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 ontwikkelingen 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 dan ook niet of beknopt beschreven.
Het CSBN is onderverdeeld in beschrijvingen van manifestaties, dreigingen, weerbaarheid en belangen.

De hoofdvragen van het CSBN 2017 zijn:
- Welke gebeurtenissen of welke activiteiten van welke actoren kunnen ict-belangen aantasten, welke middelen gebruiken zij en welke ontwikkelingen doen zich daarbij voor? (dreigingen)
- In hoeverre is Nederland weerbaar tegen kwetsbaarheden in ict, kunnen die leiden tot aantasting van ict-belangen en welke ontwikkelingen doen zich daarbij voor? (weerbaarheid)
- Welke Nederlandse belangen worden in welke mate geschaad door beperkingen van de beschikbaarheid en betrouwbaarheid van ict, schending van de vertrouwelijkheid van in ict opgeslagen informatie of schade aan de integriteit van die informatie en welke ontwikkelingen doen zich daarbij voor? (belangen)

De driehoek belangen, dreigingen, weerbaarheid en manifestaties staat model voor de hoofdstukindeling van het CSBN.



Hoofdstuk 1 beschrijft manifestaties die zich tijdens de rapportageperiode hebben voorgedaan binnen de driehoek belangen, dreigingen en weerbaarheid. Het hoofdstuk geeft een overzicht van relevante manifestaties in Nederland en daarbuiten. Buitenlandse manifestaties worden genoemd, daar waar ze relevant zijn voor Nederland, hoewel Nederland niet direct geraakt hoeft te zijn.

De dreigingen worden beschreven in hoofdstukken over actoren en middelen. Hoofdstuk 2 beschrijft de capaciteiten, kenmerken en methoden van actoren. Hoofdstuk 3 beschrijft de middelen die deze actoren gebruiken en deze middelen zich ontwikkelen.

In hoofdstuk 4 wordt een beeld gegeven van de weerbaarheid van Nederland. De weerbaarheid heeft invloed op de kans dat een dreiging zich manifesteert en kan de impact van manifestaties beperken. Hoofdstuk 4 benoemt zowel kwetsbaarheden als de maatregelen die genomen zijn om die kwetsbaarheden te beperken, samen vormen deze de weerbaarheid van Nederland.

Hoofdstuk 5 gaat in op de Nederlandse belangen op het gebied van cybersecurity. In het hoofdstuk ligt de nadruk op de veranderingen in deze belangen gedurende de rapportageperiode, en wat daarvan de impact op cybersecurity is.

De bijlagen bieden tot slot een overzicht van de door het NCSC afgehandelde incidenten, een beeld van cybersecurity binnen de verschillende sectoren en een toelichting op de gebruikte afkortingen.

Democratische instituties in meerdere westerse landen zijn doelwit geweest van digitale aanvallen

1 Manifestaties

Informatie verzameld via digitale aanvallen is misbruikt in campagnes om de publieke opinie te beïnvloeden. Onder meer democratische instituties in het buitenland zijn hiervan het slachtoffer geweest. De digitale diefstal en publicatie van informatie wordt strategisch ingezet door statelijke actoren. Misbruik van kwetsbare apparaten zorgt ervoor dat grotere verstoringsaanvallen uitgevoerd kunnen worden.

Dit hoofdstuk beschrijft manifestaties van digitale aanvallen. Het motief van een aanval kan verschillen. In dit hoofdstuk wordt ingegaan op activiteiten gericht op beïnvloeding, verstoring, het verwerven van informatie en geldelijk gewin. In dit hoofdstuk zijn manifestaties uit Nederland en uit het buitenland opgenomen. De manifestaties uit het buitenland zijn relevant omdat deze impact kunnen hebben op Nederlandse belangen of de weerbaarheid van organisaties in Nederland.

Activiteiten gericht op beïnvloeding

Democratische instituties zijn het slachtoffer van digitale aanvallen

Er is volop aandacht voor digitale beïnvloeding van democratische instituties in meerdere westerse landen. Zo zijn de Duitse politieke partij CDU, de beweging En Marche! van de Franse president Emmanuel Macron en de Amerikaanse Democratische Partij slachtoffer geweest van digitale aanvallen. Deze activiteiten lijken gericht op het verstoren en het beïnvloeden van het democratische proces. De kwetsbaarheid van de kiezer is hierbij aangevallen, en niet de (eventuele) kwetsbaarheid van het stemproces.

In Frankrijk is een grote hoeveelheid e-mails en documenten van de beweging van de toenmalige presidentskandidaat Macron kort voor de presidentsverkiezingen in mei 2017 online geplaatst. In december constateerde de beweging al dat medewerkers doelwit waren van een phishing-e-mailcampagne.[1]

Beveiligingsbedrijf TrendMicro maakte in mei 2016 bekend dat de partij van bondskanselier Angela Merkel slachtoffer was van digitale aanvallen. Medewerkers van de CDU kregen spearphishing-e-mails die verwezen naar een nagemaakt inlogscherm voor de door hun gebruikte webmaildienst. De aanvaller hoopte zo inloggegevens te bemachtigen. Het is onduidelijk of dit is gelukt.[2][3]

In de zomer van 2016 werd bekend dat de Amerikaanse Democratische Partij meermaals succesvol is aangevallen. Hierbij zou politiek gevoelige informatie zijn gestolen. De aanvallen maakten onderdeel uit van een campagne, aldus een rapport van inlichtingendiensten uit de VS, gericht op het beïnvloeden van de presidentsverkiezingen. Amerikaanse beveiligingsbedrijven en de Amerikaanse overheid delen de opvatting dat Russische actoren achter de aanvallen zaten.[4][5][6][7] In het rapport wordt beschreven hoe de beïnvloeding in zijn werk is gegaan. Bovendien wordt benadrukt dat er geen aanwijzingen zijn dat het fysieke stemproces gemanipuleerd is.

Deze activiteiten richtten zich op beïnvloeding van besluitvormingsprocessen en de publieke opinie. De FBI maakte in januari 2017 bekend dat ook de Republikeinse Partij doelwit is geweest, maar dat gestolen informatie niet is gelekt. Volgens de FBI werd onder andere een in onbruik geraakt e-mailsysteem van het Republikeinse partijbestuur (RNC) gecompromitteerd.[8] Voor zover bekend is niet eerder op deze schaal getracht de Amerikaanse verkiezingen te beïnvloeden door digitale aanvallen op haar democratische instituties.

In december kondigde de Amerikaanse overheid diplomatieke maatregelen aan tegen Rusland.[9] Rusland ontkende herhaaldelijk iedere betrokkenheid[10][11] en de hacker van de Democraten die zichzelf Guccifer 2.0 noemt, zegt geen banden te hebben met Rusland.[12]

De verschillende aanvallen op de Amerikaanse Democratische partij

In het CSBN 2016 werd de in juni 2016 bekend geworden hack van het netwerk van het partijbestuur van de Democratische Partij (DNC) al beschreven. Er zouden uiteindelijk verschillende aanvallen plaatsvinden op de partij. Ook de Democratische campagne voor het Huis van Afgevaardigden (DCCC) en vele e-mailaccounts van prominente medewerkers werden gecompromitteerd.

- Campagneleider John Podesta klikt in maart 2016 op een link in een door de aanvallers gefabriceerde beveiligings-e-mail van Google en geeft zijn inloggegevens prijs. Het geeft de aanvallers toegang tot zijn persoonlijke Gmail-account met daarin duizenden politiek gevoelige e-mails. In juli 2016 start Wikileaks met de publicatie van delen van de gestolen e-mails.[13] Podesta was niet het enige doelwit. Beveiligingsbedrijf SecureWorks stelt dat de e-mail deel uitmaakt van een spearphishingcampagne gericht op 108 accounts van personen verbonden aan de presidentiële campagne van Hillary Clinton.[14]

- In juni 2016 verschenen er berichten in de media[15] waarin gemeld werd dat hackers gegevens gestolen zouden hebben van de computers van de Democratische Partij in de Verenigde Staten. De hackers richtten zich hierbij specifiek op de systemen van het DNC. Zij zouden e-mail- en chatverkeer van de Democraten hebben kunnen lezen. Het beveiligingsbedrijf CrowdStrike relateerde de gevonden malware aan twee Russische actoren, waarvan zij vermoedden dat deze sterke banden hadden met Russische inlichtingen- en veiligheidsdiensten.[16] [17] Later werd de hack ook geclaimd door een onbekende persoon. Deze probeerde door het vrijgeven van meerdere documenten uit de hack de verantwoordelijkheid op te eisen.[18] In de nasleep van de hack zei de FBI dat het tien maanden duurde voordat een forensische analyse van de aanval voor de FBI beschikbaar was.[19]

- In augustus 2016 werden contactgegevens van Democratische leden van het Huis van Afgevaardigden en medewerkers van de Democratische campagne (DCCC) gepubliceerd door “Guccifer 2.0”. Kort daarna werden ook partijdocumenten gelekt afkomstig uit dezelfde diefstal, waaronder de te voeren campagnestrategie in verschillende staten. De gepubliceerde informatie zou vervolgens zijn gebruikt door politieke tegenstanders.[20]

De lekken vonden plaats via het blog van “Guccifer 2.0”, Wikileaks, de website DCLeaks.com en direct aan verschillende media. Er volgt een storm aan onthullingen over de Democratische partij. Vier hooggeplaatste bestuurders van het DNC stapten op naar aanleiding van openbaar geworden informatie.[21] DNC verving met spoed zijn computersystemen en telefoons. De DCCC sluit haar computernetwerk voor een week af.

Digitale veiligheid Nederlandse verkiezingen voor het voetlicht gebracht

De media berichtten ook in Nederland volop over digitale veiligheid van politieke partijen, kieshulpen en de overheid in aanloop naar de Tweede Kamerverkiezingen. RTL nam sociale-media-accounts van twee politici over door gepubliceerde wachtwoorden uit oudere datalekken te gebruiken.[22] De verschillende kieshulpen werden direct na lancering van hun websites kritisch aangesproken op kwetsbaarheden door burgers en toezichthouders.[23] In het weekeinde van zaterdag 11 en zondag 12 maart waren diverse Nederlandse organisaties het doelwit van DDoS-aanvallen en defacements. De websites van Stemwijzer en Kieskompas waren de dag voor de verkiezingen door DDoS-aanvallen beperkt beschikbaar totdat er passende maatregelen waren getroffen.[24]

Activiteiten gericht op verstoring

Mirai: botnets van (consumenten)elektronica zorgen voor schaalvergroting DDoS

Botnet Mirai nam in de zomer van 2016 tienduizenden (consumenten)apparaten uit het internet of things (IoT) over, deels door ook andere botnets over te nemen.[25] Het botnet viel eind september de website van cybersecurityjournalist Brian Krebs aan. Het gevolg was dat Akamai, een leverancier van anti-DDoS-diensten, zich terugtrok als pro-bonosponsor van Krebs. Het bedrijf zegt dat de kosten uit de hand liepen en dat het betalende klanten prioriteit geeft.[26] Ook de Franse hostingprovider OVH werd slachtoffer van Mirai. De websites van klanten van OVH waren voor bezoekers uit Zuid-Europa tijdelijk trager of niet beschikbaar.[27]

Eerder in 2016 werden DDoS-aanvallen uitgevoerd met het LizardStresser-botnet. Ook dit botnet maakte gebruik van besmette IoT-apparaten. Botnets met de grootte van LizardStresser en Mirai zijn op zich niet nieuw. Wel zijn de aanvallen de eerste keer dat botnets van deze omvang, waarbij misbruik is gemaakt van kwetsbare (consumenten)elektronica, gebruikt zijn om grootschalige DDoS-aanvallen uit te voeren. Het is onbekend wie de aanvallen met Mirai uitvoerde. Het hacktivistische collectief ‘New World Collective’ heeft de aanvallen opgeëist.

Op 21 oktober troffen grote DDoS-aanvallen DNS-dienstverlener Dyn, uitgevoerd met botnets gebaseerd op de broncode van Mirai. Dyn verzorgt DNS-dienstverlening voor 14 procent van de 1000 populairste domeinen ter wereld[28] en is leverancier voor onder andere Twitter, Spotify en Netflix. Deze en andere dienstverleners waren door de aanval op Dyn slecht of niet bereikbaar. Ondanks het feit dat met name systemen aan de oostkust van de Verenigde Staten geraakt zijn, zorgde dit ook voor gebruikers in Nederland voor verstoringen en verminderde beschikbaarheid van veelgebruikte diensten.

DDoS-aanvallen met de omvang van de aanvallen op OVH, Krebs en Dyn zijn enkel af te weren door grootschalige inzet van middelen die gepaard gaan met forse investeringen. Alleen de grootste partijen of coalities van uitstekend samenwerkende kleinere partijen zullen hiertoe in staat zijn. Dyn stelt in een analyse van de aanvallen door concurrenten te zijn bijgestaan met mitigatie.[29]

Fysieke infrastructuur als doelwit

In de nacht van 17 op 18 december 2016 viel de stroom uit in diverse districten van Kiev. Het Oekraïense energiebedrijf Ukrenergo meldde dat een cyberaanval de uitval heeft veroorzaakt.[30] [31] Beveiligingsonderzoekers van ISSP en Honeywell bevestigden in januari 2017 dat het om een cyberaanval ging, net als de aanval een jaar eerder.[32] De aanval zou zijn gericht op het testen van aanvalstechnieken en het gebruik van het verdeelstation als proeftuin.[33] Reuters meldde in dezelfde periode aanvallen op de Oekraïense ministeries van Financiën en Defensie.[34]

Uit berichtgeving blijkt [35] dat de aanval in december 2016 zorgde voor een beperkte stroomuitval van ongeveer een uur. Bij de aanvallen in 2015 en 2016 is gebruik gemaakt van geavanceerde malware. De BlackEnergy-malware is door de aanvallers in 2016 uitgebreid met modules gericht op het aanvallen van systemen in gebruik bij beheerders van energiedistributienetwerken. Besmetting zou plaatsgevonden hebben door het openen van phishing-e-mails door beheerders in Oekraïne, op werkstations waar ook het beheer over energienetwerken uitgevoerd werd. Ook de energienetwerken van Saoedi-Arabië zijn in 2017 het slachtoffer geweest van aanvallen, waarbij de malware Shamoon gebruikt is. Naast de energienetwerken waren ook overheidsinstanties en de financiële sector in Saoedi-Arabië het slachtoffer.[36]

Activiteiten gericht op verwerven van informatie

Overheidsinstellingen herhaaldelijk doelwit van omvangrijke en hardnekkige digitale spionageaanvallen

De AIVD en de MIVD hebben gezien dat Nederlandse overheidsinstellingen het afgelopen jaar herhaaldelijk doelwit waren van omvangrijke en hardnekkige digitale spionage-aanvallen. Zo zijn het ministerie van Buitenlandse Zaken en het ministerie van Defensie meerdere malen aangevallen, ook door landen die niet eerder zijn waargenomen als dreiging tegen Nederlandse overheidsnetwerken.

Er zijn, onder andere met het Nationaal Detectie Netwerk, vroegtijdig aanvallen onderkend waarna betrokken instanties zijn geïnformeerd. De aanvallen geven blijk van omvangrijke en structurele interesse in de Nederlandse overheid.

Buitenlandse inlichtingendiensten voeren spionagecampagnes uit om de economie en defensie van hun land te verbeteren

Digitale spionage met een economisch motief blijft een bron van zorg voor Nederland. De inlichtingendiensten hebben in 2016 in Nederland activiteiten van verschillende digitale spionage-campagnes waargenomen. Deze activiteiten waren onder andere gericht op Nederlandse bedrijven die veel aan onderzoek en ontwikkeling doen, in het bijzonder in de sectoren ICT, maritieme technologie, biotechnologie en lucht- en ruimtevaart. De activiteiten varieerden van enkel voorbereidingshandelingen tot het daadwerkelijk exfiltreren van vertrouwelijke bedrijfsgegevens.[37]

Verschillende digitale spionagecampagnes met economisch motief zijn al jaren actief en het merendeel heeft in de afgelopen jaren in Nederland herhaaldelijk meerdere binnen- en buitenlandse bedrijven aangevallen. Hierbij zijn naast persoonsgegevens ook vertrouwelijke en geavanceerde ICT-, maritieme, energie- en defensietechnologieën gestolen. Dergelijke aanvallen vormen een bedreiging van het economisch verdienvermogen en de militaire slagkracht en bevestigen een structurele interesse in gevoelige informatie van het Nederlandse bedrijfsleven.

Op woensdag 15 juni 2016 publiceerde de Volkskrant een artikel [38] over de hack op het Nederlands-Duitse defensiebedrijf Rheinmetall. Dit bedrijf zou vanaf 2012 aangevallen zijn door Chinese hackers. De hack zou volgens de Volkskrant eind 2015 ontdekt zijn door het beveiligingsbedrijf Fox-IT.

In december 2016 werd bekend dat eerder dat jaar gevoelige handelsinformatie van het Duitse bedrijf ThyssenKrupp via cyberaanvallen is gestolen.[39]

Vijf jaar oude gelekte accountgegevens nu misbruikt voor phishing

LinkedIn werd in 2012 gehackt. Daarbij lekten accountgegevens van 167 miljoen gebruikers uit.[40] De gelekte namen, e-mailadressen en wachtwoordhashes bleven echter lange tijd uit beeld. Vanaf mei 2016 werd de dataset publiekelijk te koop aangeboden en werd misbruik zichtbaar: Fox-IT meldde in juni phishingcampagnes in Nederland, gepersonaliseerd op basis van de LinkedIn-gegevens.[41] Ook vanuit diverse sectoren ontving het NCSC het signaal dat op basis van de LinkedIn-dataset phishing-e-mails werden verzonden.[42]

Kwetsbare (consumenten)elektronica is af te luisteren

De iPhone van mensenrechtenactivist Ahmed Mansoor werd in augustus 2016 aangevallen met technologie voor overheidssurveillance. Met de installatie van spionagesoftware Pegasus kon de aanvaller de microfoon, camera en communicatie afluisteren en de verplaatsing van de telefoon volgen. Beveiligingsonderzoekers ontdekten in de aanval drie onbekende kwetsbaarheden in Apple-producten met een geschatte marktwaarde van 1 miljoen dollar.[43] Apple zag zich genoodzaakt wereldwijd een kritieke beveiligingsupdate uit te rollen.[44]

Ook minder geavanceerde (consumenten)elektronica is kwetsbaar. Kinderpop "My Friend Cayla" was door aanvallers in te zetten als afluisterapparatuur, bleek uit onderzoek van de Noorse consumentenbond.[45] De ook in Nederland verkochte kinderpop was niet beveiligd en op eenvoudige wijze af te luisteren, bijvoorbeeld door nieuwsgierige buren. Nederlandse speelgoedwinkels haalden de pop uit de winkels en vroegen de leverancier om uitleg, aldus de Nederlandse Consumentenbond.[46]

Activiteiten gericht op geldelijk gewin

In Nederland zijn de manifestaties gericht op geldelijk gewin beperkt veranderd ten opzichte van het CSBN 2016. Managed service providers geven aan dat het reageren op ransomware vrijwel dagelijkse kost is geworden. Enerzijds resulteert dit in aandacht voor het maken en terugzetten van back-ups. Anderzijds laten deze manifestaties zien dat de weerbaarheid tegen ransomwarebesmettingen nog sterk te wensen over laat. De Nederlandse banken constateren een verdere terugloop van schade door fraude met internetbankieren.[47] De Tweede Kamer kampte in maart 2017 met een ransomwarebesmetting,[48] [49] verspreid via e-mail naar verschillende Kamerleden.

CxO-fraude maakte in Nederland wel een groei door. Afgelopen jaar ontvingen het NCSC, de Fraudehelpdesk en de politie opvallend veel meldingen van CxO-fraude. Ook de financiële sector en managed service providers maakten melding van toegenomen aantallen fraudepogingen. Bij deze vorm van fraude proberen criminelen via een e-mail naar de financiële afdeling van een organisatie, uit naam van een directeur of afdelingshoofd, geld te laten storten op de rekening van een handlanger.[50] Meestal maken zij hierbij gebruik van domeinnamen die sterk lijken op de domeinnaam van het betreffende bedrijf. Voor dit doeleinde registreren fraudeurs massaal valse domeinnamen, hoewel deze trend aan het einde van 2016 in Nederland leek af te nemen.[51]

Het buitenland kent in 2016 meerdere manifestaties van aanvallen direct gericht op banken. Tesco Bank legde op 7 november de online betalingsmogelijkheden voor al haar rekeninghouders stil nadat er de voorgaande dagen frauduleuze transacties hadden plaatsgevonden op 9.000 accounts voor een totale waarde van 2,5 miljoen Britse pond.[52] Op 3 februari werd door onderzoekers gerapporteerd over een serie van malwarebesmettingen binnen de Poolse financiële sector. De website van de financiële toezichthouder bleek door criminelen ingezet als centrale bron voor de verspreiding van malware (wateringhole) naar interne systemen van verschillende banken.[53]

Hacks als basis voor beursbeïnvloeding en koersspeculatie

De Italiaanse politie arresteerde in januari twee verdachten op verdenking van hacken en het stelen van staatsgeheimen. De politie stelde dat de verdachten wilden investeren op basis van de gestolen informatie. Er zouden onder andere accounts zijn gecompromitteerd van advocaten, accountants, vakbonden, politie, ambtenaren van Economische Zaken en het Vaticaan.[54] Antivirusbedrijf Kaspersky analyseerde de gebruikte malware en classificeerde het duo als zeer effectieve amateurs.[55]

Beveiligingsonderzoekers van startup MedSec werkten samen met het hedgefonds Muddy Waters om te profiteren van gevonden kwetsbaarheden in pacemakers van het Amerikaanse St. Jude Medical. Investeerder Muddy Waters speculeerde op de beurs op een verwachte koersdaling na publicatie van een rapport over deze kwetsbaarheden.[56] Een rechtszaak volgde.[57] De kwetsbaarheden zelf bleken ernstig, ze konden gebruikt worden om pacemakers en defibrillators te manipuleren en de werking ervan te beïnvloeden.

In januari werd gemeld dat de leverancier een update uitgebracht had waarmee de kwetsbaarheden verholpen zouden worden. De onderzoekers die de kwetsbaarheid hadden gevonden, concludeerden echter dat de update niet alle kwetsbaarheden adresseerde.[58] De Amerikaanse Food & Drug Administration (FDA) stuurde St. Jude Medical in april 2017 een waarschuwing waarin gemeld werd dat de genomen acties om de beveiliging te verbeteren niet voldoende waren.[59]

Datalekken nemen toe in volume en vertrouwelijkheid

Datalekken manifesteren zich gedurende de gehele rapportageperiode. De Autoriteit Persoonsgegevens ontving bijna 5700 meldingen van datalekken in 2016.[60] Hierbij gaat het om alle gemelde datalekken, niet alleen lekken die betrekking hebben op cybersecurity.

In het eerste kwartaal van 2017 ontving de Autoriteit Persoonsgegevens 2317 meldingen van datalekken. In 12 procent van de gevallen betrof het datalekken waarbij incidenten op het gebied van cybersecurity aan de orde waren, 7 procent daarvan betrof hacking, malware en/of phishing, 5 procent betrof het tonen van persoonsgegevens van een verkeerde klant in een klantportaal.[61]

Opvallend zijn de verder toenemende volumes en de mate van vertrouwelijkheid van gelekte informatie die bij de incidenten ontdekt zijn en gemeld worden. De Autoriteit Persoonsgegevens ziet ook dat datalekken niet altijd worden gemeld, voorbeelden hiervan zijn malware-infecties en datalekken bij bewerkers, zoals cloudproviders.

Yahoo meldde in 2016 twee keer het grootste bekende datalek ter wereld. In september meldde het bedrijf een verlies van persoonsgegevens voor 500 miljoen accounts als gevolg van een hack in 2014.[62] In december doet Yahoo een tweede melding over een hack in 2013 waarbij persoonsgegevens van 1 miljard gebruikers zouden zijn buitgemaakt.[63] Yahoo sloeg wachtwoorden onveilig en niet versleuteld op en lekte naast persoonsgegevens een schat aan wachtwoordinformatie voor misbruik bij andere dienstverleners, in het geval van hergebruik van wachtwoorden.[64]

Beide hacks werden bekend tijdens het overnametraject van Yahoo door Verizon, dat in februari 2017 een negatieve herwaardering van 350 miljoen dollar bekendmaakte.[65] Beurswaakhond SEC onderzoekt de tijdigheid van de meldingen van Yahoo.[66]

Netbeheer Nederland en Energie-Nederland maakten in september 2016 bekend dat energiegegevens van 2 miljoen huishoudens waren gestolen door een medewerker van een bedrijf dat werkte voor een energieleverancier. Het ging om gegevens uit een centraal registratiesysteem over afgesloten energiecontracten, die kunnen worden misbruikt om consumenten ongevraagd aanbiedingen te doen.[67]

De salarisgegevens van enkele duizenden (oud-)medewerkers van ASML en Philips stonden in november op Pastebin.[68] Het bleek te gaan om loonstroken uit 2010 die via een leverancier van deze bedrijven op straat kwamen te liggen. Erasmus Universiteit Rotterdam meldde een datalek als gevolg van een inbraak op een webserver. Persoonsgegevens van 17.000 mensen werden gelekt, waaronder ook financiële gegevens, burgerservice- en documentnummers, nationaliteiten en gegevens over de gezondheid.

Lang niet alle datalekken worden gemeld. Tegelijkertijd blijken veel meldingen achteraf niet nodig, maar wordt er proactief gemeld, onder andere in verband met de sanctiemogelijkheid. Op basis van een steekproef onder 66 gemeenten met beroep op de Wet openbaarheid van bestuur stelde NPO Radio 1 dat de helft van de datalekken niet door de gemeente wordt gemeld.[69]

Minder geavanceerde actoren zijn in staat aanvallen uit te voeren met grote maatschappelijke impact

2 Dreigingen: Actoren

Ten opzichte van de voorgaande jaren is het dreigingsniveau dat van diverse actorengroepen uitgaat, grotendeels stabiel; statelijke en criminele actoren vormen nog altijd de grootste dreiging voor de Nederlandse digitale veiligheid en ontwikkelen zich sneller dan andere actoren. Statelijke actoren hebben het afgelopen jaar via de digitale weg campagnes gevoerd om de publieke opinie te beïnvloeden.

Dit hoofdstuk gaat in op actoren die de vertrouwelijkheid, integriteit en beschikbaarheid van informatie of informatiesystemen aantasten. De aandacht gaat daarbij uit naar de intentie van de afzonderlijke actoren, hun capaciteiten en de ontwikkelingen op dit vlak.

Attributie, het achterhalen wie achter een aanval zit, is lastig. Redenen daarvoor zijn onder andere dat actoren proberen hun identiteit te verbergen en proberen te misleiden met dwaalsporen. Begin 2017 berichtten nieuwssites dat digitale bankrovers Russische teksten in hun malware stoppen terwijl op basis van taalfouten het vermoeden bestaat dat het niet om Russische cybercriminelen gaat.[70] Een andere reden waarom attributie lastig is, is dat diverse actoren soms vergelijkbare hulpmiddelen gebruiken. Dat kan wijzen op dezelfde actor, maar het kan ook zijn dat ze slechts van dezelfde middelen gebruik hebben gemaakt. Ook is lang niet altijd helder welke intentie een actor bij een aanval heeft. Een DDoS-aanval kan bijvoorbeeld worden gebruikt om processen te verstoren, maar ook om andere activiteiten te verhullen.

Beroepscriminelen

De dreiging die criminele actoren vormen voor de Nederlandse digitale veiligheid, ontwikkelt zich nog steeds in een hoog tempo. Succesvolle verdienmodellen worden verder uitgediept, nieuwe scenario's worden ontwikkeld[71] [72] en aanvallen worden op minder traditionele doelwitten uitgevoerd.

Criminelen variëren met inzet ransomware

Het ontwikkelen van nieuwe methodes door criminelen uit zich onder andere in het uitdiepen van het lucratieve[73] verdienmodel van ransomware.[74] Naast ongerichte aanvallen zetten criminelen ransomware ook vaker gericht in op organisaties waar de impact groot is en die sneller geneigd zullen zijn om een hoger bedrag aan losgeld te betalen.[75] Dit jaar manifesteert de trend van deze gerichte aanvallen wereldwijd zich vooral bij scholen,[76] ziekenhuizen en andere gezondheidsinstellingen.[77] [78] Ook krijgen aanvallen door criminelen steeds meer impact op het gewone leven doordat processen of diensten (onbedoeld) verstoord kunnen raken. Voorbeelden hiervan zijn de ransomware-aanval die het betaalsysteem van het openbaar vervoer in San Francisco raakte[79] [80] en de aanval op de systemen van een Oostenrijks hotel, waardoor sleutelpassen niet meer werkten.[81]

Onderzoekers hebben gedemonstreerd dat ransomware ook ingezet kan worden op industriële controlesystemen (ICS) en consumentenelektronica als onderdeel van het internet of things.[82] Het is voorstelbaar dat criminelen zich in de komende periode ook op deze gebieden zullen richten. Met name bij ransomware in ICS zou dit kunnen leiden tot veranderingen in het verdienmodel, aangezien het belang groot kan zijn om de getroffen systemen weer functionerend te krijgen.

Criminelen richten zich vaker op financiële instellingen

Vaker dan voorheen is waargenomen dat criminelen hun digitale aanvallen richten op de systemen van bedrijven, banken en andere financiële instellingen (de zogenaamde 'high value' doelwitten) in plaats van dat zij zich alleen op consumenten richten. Criminelen kijken hierbij op welke wijze de toegang tot het netwerk maximaal kan worden uitgebuit en verzilverd.[83] Hoewel deze ontwikkeling zich nog niet in Nederland gemanifesteerd heeft, werden in 2016 diverse Europese banken doelwit van cybercriminelen.

Diverse opzichzelfstaande incidenten illustreren dit. De Britse Tesco Bank kondigde aan tijdelijk alle online transacties stil te

leggen, nadat ongeveer 9000 klanten slachtoffer waren geworden van frauduleuze overboekingen.[84] Een criminele groepering, onder de naam Cobalt, infiltreerde in het netwerk van enkele Europese banken. Via de inzet van geldezels wisten zij vervolgens een groot aantal geldautomaten leeg te halen.[85]

Verder zijn wereldwijd banken beroofd door toegang tot het SWIFT-(betalings)systeem te verkrijgen en te misbruiken. Enkele onderzoeksbedrijven suggereerden betrokkenheid van Noord-Korea.[86] [87] SWIFT kondigde in september 2016 als reactie op de aanvallen wereldwijd verplichtingen af op het gebied van informatiebeveiliging voor deelnemende banken.[88] [89] Ook misbruikten criminelen toegang tot de systemen van een bank in Liechtenstein om buitenlandse rekeninghouders af te persen.[90]

Hoewel deze opzichzelfstaande aanvallen criminelen meer voorbereidingstijd en middelen kosten, is het financieel gewin groter dan (eenvoudige) aanvallen op consumenten.

Statelijke actoren

Professionaliteit van landen om digitaal te spioneren groeit en aantal landen dat dit doet neemt toe

Steeds meer landen hebben zich de afgelopen jaren de mogelijkheden verschaft om inlichtingen in te winnen via het digitale domein. Het is een relatief goedkoop middel, snel, en heeft minder risico's dan traditionele spionage omdat het gebruik ervan eenvoudig te ontkennen is. Nederlandse overheidsinstellingen waren het afgelopen jaar herhaaldelijk het slachtoffer van omvangrijke en hardnekkige digitale spionageaanvallen door andere landen, ook door landen die niet eerder zijn geïdentificeerd als dreiging voor Nederlandse overheidsnetwerken.

Meer dan honderd landen bezitten momenteel de capaciteit om digitaal te spioneren en hun professionaliteit groeit, evenals de dreiging die ervan uitgaat. Deze groeiende digitale spionagedreiging is gericht op zowel publieke als private partijen en is afkomstig van landen die zichzelf politiek dan wel economisch beter willen positioneren in de wereld. Vooral inlichtingen- en veiligheidsdiensten worden hiervoor ingezet.

Staten blijven investeren in offensieve cybercapaciteiten en zetten deze in

De AIVD en MIVD hebben onderkend dat veel landen investeren in het opzetten van (militaire) offensieve digitale capaciteiten. Digitale middelen worden daarbij ook gebruikt voor beïnvloedings- en informatieoperaties. Accounts worden gehackt waarbij vertrouwelijke informatie wordt ingewonnen die later door een (ogenschijnlijk) onafhankelijke partij wordt gepubliceerd om verwarring en verdeeldheid te zaaien bij tegenstanders.

Daarbij hebben de inlichtingendiensten onderkend dat veel landen investeren in het opzetten van digitale capaciteiten gericht op de (toekomstige) sabotage van vitale processen. De digitale aanval op Oekraïense energiecentrales in december 2015 werd in december 2016 gevolgd door een nieuwe aanval op de Oekraïense vitale infrastructuur. Deze keer had een deel van de hoofdstad Kiev tijdelijk geen elektriciteit. In Saoedi-Arabië waren meerdere overheidsinstellingen en bedrijven[91] slachtoffer van een destructief virus (Shamoon 2.0). Deze gebeurtenissen in het afgelopen jaar illustreren de potentie van digitale aanvallen tot het toebrengen van politieke en fysieke schade, evenals de bereidheid om dit middel daadwerkelijk in te zetten.

Hackers in dienst van een staat kunnen zich op het internet zeer professioneel afschermen. De inlichtingendiensten nemen ook waar dat meerdere statelijke actoren structureel particuliere ICT-bedrijven als dekmantel gebruiken om hun digitale spionageactiviteiten te verhullen. Daarnaast worden ICT-bedrijven en academische instellingen ingezet voor de ontwikkeling van malware. Hierdoor groeit de potentie van statelijke actoren voor het uitvoeren van offensieve cyberaanvallen.

Statelijke actoren zoeken nieuwe methoden

Om ongezien computernetwerken binnen te komen, zoeken statelijke actoren naar nieuwe digitale methoden, eventueel gecombineerd met traditionele methoden. Hoewel veel digitale aanvallers nog steeds gebruik maken van spearphishing, usb-sticks en wateringholes om via malwarebesmettingen toegang te krijgen tot een computernetwerk, zijn de methodes van de meer professionele en geavanceerde staten steeds moeilijker te detecteren.

Er wordt gericht te werk gegaan, bijvoorbeeld tegen hardware als routers, of met malware-injectie via wifinetwerken. Een aanval kan zelfs malwarevrij zijn. Protocollen waarop het internet functioneert zijn ooit ontworpen om zo efficiënt mogelijk data te transporteren en niet zozeer met het oog op veiligheid. Staten kunnen kwetsbaarheden in deze protocollen mogelijk gebruiken voor digitale spionage.

De goed ontwikkelde ICT-infrastructuur van Nederland blijft aantrekkelijk als doorvoerhaven voor digitale aanvallen. De AIVD en de MIVD hebben diverse statelijke actoren gedetecteerd die misbruik maken van Nederlandse infrastructuur voor aanvallen op derde landen. Hierdoor wordt Nederland ongewild betrokken bij de verspreiding van digitale aanvallen die een inbreuk vormen op de economische, militaire en politieke belangen van andere landen.

Terroristen

Vooral jihadisten zijn verantwoordelijk voor de hedendaagse terroristische dreiging. In de rapportageperiode hebben vooral ISIS en ISIS-sympathisanten (verder ISIS) zich op digitaal vlak gemanifesteerd.

Intentie tot cyberaanvallen aanwezig

Hoewel jihadisten de afgelopen rapportageperiode nog niet in staat zijn gebleken tot het uitvoeren van geavanceerde digitale aanvallen, is de intentie voor het uitvoeren van cyberaanvallen bij jihadisten en zeker bij ISIS aanwezig. De uitgevoerde aanvallen, defacements[92] en DDoS-aanvallen[93], hadden primair een propagandistisch oogmerk. Dat gold ook voor de gepubliceerde lijsten met informatie over personen waarvan ISIS claimde dat die via hacks waren verkregen en die vergezeld gingen van oproepen om deze personen te doden:[94] de dodenlijsten. Overigens bleek het merendeel van die informatie al op het internet te vinden[95] en is het nog niet voorgekomen dat personen die op deze lijsten stonden daadwerkelijk zijn gedood.

Jihadisten hebben ook de intentie tot destructieve cyberaanvallen die zijn gericht op mensenlevens gericht geweld of op het ontwrichten van de maatschappij. Voor zover bekend hebben deze zich nog niet gemanifesteerd.

Digitale capaciteiten van jihadisten voor cyberaanvallen beperkt

Jihadisten – en breder terroristen – zijn volgens de inschatting van experts nog niet in staat tot geavanceerde complexe aanvallen. Voor de eenvoudige cyberaanvallen die jihadisten hebben uitgevoerd, waren relatief weinig expertise en middelen nodig. Doordat enkele hackers en hackersgroepen van ISIS zich hebben verenigd in het 'United Cyber Caliphate'[96] neemt hun slagkracht en wervingspotentieel mogelijk toe. Zo roepen zij hackers op om zich aan te sluiten.[97] Verder doen jihadisten met eenvoudige cyberaanvallen wel ervaring op.

Het is zorgelijk dat via diverse fora veel producten en diensten voor cyberaanvallen te koop zijn. Dit kan de drempel voor cyberaanvallen door jihadisten verlagen. Ten opzichte van eerdere jaren beschikt in ieder geval ISIS over minder geld,[98] wat de financiële mogelijkheden voor aanschaf van de meest geavanceerde producten en diensten minder aannemelijk maakt.

Jihadisten voerden meestal aanvallen uit op willekeurige doelwitten

Voor zover terroristen cyberaanvallen hebben uitgevoerd, betrof dat merendeels willekeurige doelwitten die kwetsbaarheden vertoonden. In publicaties wordt vooral gewaarschuwd voor het gevaar van cyberaanvallen door jihadisten op de vitale infrastructuur,[99] veelal vanwege de ontwrichting en de publicitaire waarde die daarvan het gevolg kan zijn. Voor het uitvoeren van gerichte geavanceerde aanvallen is echter meer ict-deskundigheid vereist dan die zij tot nu toe hebben laten zien bij uitgevoerde cyberaanvallen. Daardoor zijn gerichte geavanceerde aanvallen minder waarschijnlijk. Dat neemt niet weg dat kleinschalige aanvallen door jihadisten, die vooral propagandistisch van aard zijn, media-aandacht genereren en daardoor kunnen leiden tot gevoelens van angst.

Hacktivisten, cybervandalen en scriptkiddies

Hacktivisten plegen digitale aanvallen uit ideologisch of activistisch motief. Cybervandalen en scriptkiddies doen dat uit baldadigheid, voor de uitdaging of om de eigen capaciteiten aan te tonen. Zowel hun motieven als hun vaardigheden kunnen zeer divers zijn. In maart 2017 vormden bijvoorbeeld de oplopende diplomatieke spanningen met Turkije voor diverse personen een aanleiding om (kleinschalige) digitale aanvallen te plegen met een activistisch of nationalistisch motief.[100] [101]

In Vietnam vertoonden informatieschermen van een aantal vliegvelden anti-Vietnamese en anti-Filipijnse slogans die expliciet refereerden aan het dispuut in de Zuid-Chinese Zee op 29 juli 2016. Media rapporteerden dat hackgroep 1937CN achter de operatie zat.[102] Hoewel de herkomst van de aanval moeilijk is vast te stellen, is een hacktivistisch motief voorstelbaar. Het escalatiepotentieel van dergelijke aanvallen is substantieel omdat de intenties van de aanvallers vaak moeilijk te achterhalen is.

Voorstelbare dreiging van hacktivisten, cybervandalen en scriptkiddies neemt toe

Hoewel er zich het afgelopen jaar geen noemenswaardige ontwikkelingen hebben gemanifesteerd op het gebied van hacktivisme, neemt de voorstelbare dreiging vanuit deze actoren toe. Dit komt doordat digitale aanvallen die een grote maatschappelijke impact kunnen hebben, eenvoudiger zijn uit te voeren. Dit komt mede door de groeiende beschikbaarheid van laagdrempelige producten, diensten en hulpmiddelen om deze aanvallen te plegen.

Een eerder genoemd voorbeeld van deze beschikbaarheid die tot een groot effect kan leiden, is de grootschalige DDoS-aanval op de DNS-provider Dyn, waarbij gebruik werd gemaakt van de (publiek beschikbare) 'Mirai'-botnet code.[103] Deze grote aanval werd opgeëist door het onbekende 'New World Collective', naar eigen zeggen een hacktivistisch collectief dat de beveiliging van websites wil testen.[104] Het is echter niet te controleren dat deze verklaring van de aanvallers ook daadwerkelijk het motief was achter de aanval.

Interne actoren

Dreiging vanuit interne actoren blijft gelijk

De drijfveer van interne actoren is veelal persoonlijk van aard. Zij handelen uit financiële, politieke of persoonlijke motieven zoals wraak bij ontslag. Dreiging door interne actoren kan echter ook afkomstig zijn van onbewuste acties en onzorgvuldigheid. Hoewel interne actoren zich ook het afgelopen jaar gemanifesteerd hebben, is er geen indicatie dat de dreiging vanuit interne actoren is veranderd ten opzichte van de vorige rapportageperiode.

Private organisaties

Dreiging door legale private organisaties kan drie vormen aannemen: organisaties kunnen de vertrouwelijkheid van systemen aantasten voor financieel gewin, om de concurrentiepositie te verbeteren of om de verzamelde data commercieel te gebruiken zonder dat daarvoor expliciet toestemming is gegeven. Wat dat laatste betreft lijkt in de VS een verschuiving waarneembaar. Het Amerikaanse Congres heeft in april 2017 een wet aangenomen die de weg vrijmaakt voor providers om het surfgedrag van gebruikers te verkopen.[105]

Private organisaties delen soms informatie met anderen zonder toestemming

Private organisaties kunnen door het aanbieden van producten of diensten zoals apps veel gegevens verkrijgen van klanten. Die gegevens kunnen ze vervolgens zelf commercieel gebruiken, doorgeven of verkopen aan anderen.

Hoewel gebruikers daarvoor veelal (bewust of onbewust) toestemming geven, meldden media in 2016 en begin 2017 enkele malen dat bedrijven data commercieel gebruikten of doorgaven zonder dat voldoende helder was of daarvoor toestemming was gegeven. Het betrof bijvoorbeeld het ongevraagd plaatsen van trackingcookies door websites die zelftesten aanbieden voor depressie, drankgebruik of stress of het plaatsen van trackingcookies door de Stemwijzer.

Andere voorbeelden waren het commercieel gebruik van gebruikersinformatie van smart-tv's, het doorgeven van informatie door WhatsApp aan moederbedrijf Facebook of het verzenden van wifi-gegevens vanuit Windows 10.[106]

Conclusie en vooruitblik

De doelstellingen van de afzonderlijke actoren zijn niet gewijzigd ten opzichte van eerdere jaren. Het afgelopen jaar zijn er wel meer activiteiten waargenomen waarbij statelijke actoren op digitale wijze de publieke opinie probeerden te beïnvloeden. De groei van capaciteiten van verschillende actoren is grotendeels stabiel gebleven. De via diverse fora verkrijgbare producten, hulpmiddelen en diensten werken nog steeds drempelverlagend voor cyberaanvallen (met potentieel grote maatschappelijke impact) door actoren met minder eigen capaciteiten.

De dreiging vanuit criminele en statelijke actoren voor de Nederlandse digitale en maatschappelijke veiligheid neemt toe en blijft zich verder ontwikkelen. Hierbij worden succesmodellen verder ontwikkeld en uitgebreid. Aanvallen door beroepscriminelen kunnen hierbij steeds meer impact krijgen op het gewone leven doordat veelgebruikte processen of services verstoord kunnen raken. Criminelen richten hun digitale aanvallen daarnaast steeds vaker op de systemen van bedrijven, banken en andere financiële instellingen in plaats van op consumenten.

Veel landen investeren juist in het opzetten van digitale capaciteiten gericht op de (toekomstige) sabotage van vitale processen, maar ook in digitale middelen die gebruikt kunnen worden als middel voor beïnvloedings- en informatieoperaties.

Het is aannemelijk dat statelijke actoren en criminelen de komende jaren verder blijven investeren en innoveren. Hoewel van terroristen wat betreft cyberaanvallen nog geen dreiging tegen de nationale veiligheid is waargenomen, is dat wel voorstelbaar vanwege de intentie voor cyberaanvallen, de bundeling van krachten, wervende oproepen aan ict-deskundigen en de mogelijkheden om producten, hulpmiddelen en diensten aan te schaffen.

Hacktivisten hebben zich tijdens de rapportageperiode incidenteel gemanifesteerd, maar dit is sterk afhankelijk van gebeurtenissen die hacktivisten op ideologisch gebied sterk kunnen aansporen. Te denken valt aan aanslagen, conflicten en politieke thema's. Voor de aanvallen met Mirai en gerelateerde botnets bestaat nog geen duidelijkheid over de identiteit van de aanvallers en hun motief, maar het is waarschijnlijk dat niet alleen statelijke actoren en beroepscriminelen in staat zijn om dit soort grote, verstorende aanvallen uit te voeren.

Het internet of things wordt misbruikt om DDoS-aanvallen uit te voeren

3 Dreigingen: Middelen

Het internet of things is het afgelopen jaar ingezet voor cyberaanvallen. Bestaande technieken zoals ransomware blijven in trek bij criminelen. Daarnaast zoeken criminelen naar nieuwe soorten systemen en manieren om deze middelen in te zetten. Ook verbeteren ze deze middelen om efficiënter te werken en hun winst te vergroten. Door tegenstrijdige belangen bij leveranciers, blijven IoT-apparaten de komende jaren nog kwetsbaar.

Dit hoofdstuk beschrijft ontwikkelingen op het gebied van middelen die in de rapportageperiode ingezet zijn door actoren om aanvallen uit te voeren.

Internet of things

De afgelopen jaren waarschuwden verschillende securityexperts over de toenemende dreiging vanuit het internet of things (IoT).[107] IoT-apparaten, (consumenten)elektronica, hebben over het algemeen een matige tot slechte beveiliging.[108] Dit komt onder andere door het gebruik van standaardwachtwoorden en zwakke wachtwoorden, het ontbreken van encryptie, het ontbreken van software-updates om kwetsbaarheden te verhelpen en basale ontwerpfouten. Het afgelopen jaar is er meerdere malen misbruik gemaakt van deze kwetsbaarheden en zijn IoT-apparaten als middel ingezet voor het uitvoeren van aanvallen. Daarnaast zijn in enkele gevallen apparaten misbruikt om gebruikers ervan af te luisteren of de omgeving van de gebruikers te manipuleren.

Internet of things opgenomen in botnets

In de eerste helft van 2016 was er relatief weinig grootschalig misbruik van IoT-apparaten. In september 2016 kwamen er echter meerdere signalen dat kwaadwillenden grootschalig misbruik maken van deze apparaten. In die maand is een IoT-botnet gedetecteerd met meer dan 1 miljoen apparaten. Botnets hebben toen grote DDoS-aanvallen uitgevoerd. Op 20 september 2016 werd de website van securityjournalist Brian Krebs platgelegd door een DDoS-aanval met een omvang van 665 Gbps,[109] wat bijna twee keer zo groot was als de daarvoor grootste bekende aanval. Kort daarna werd dit record weer gebroken toen hostingprovider OVH werd aangevallen met een DDoS-aanval van meer dan 1 Tbps.[110] Grote DDoS-aanvallen zijn niet nieuw en worden vaker uitgevoerd, met en zonder botnets. Opmerkelijk aan deze twee grote aanvallen is dat ze zijn uitgevoerd met behulp van grote botnets van gecompromitteerde IoT-apparaten; thuisrouters, webcams en digitale televisie-ontvangers.

De broncode van het Mirai-botnet, dat gebruikt is voor de DDoS-aanval op de website van Brian Krebs, is eind september 2016 vrijgegeven en publiekelijk beschikbaar.[111] De daarmee vrijgekomen kennis heeft ertoe geleid dat de eerder minder succesvolle IoT-malware, genaamd NyaDrop, terugkeerde met een verbeterde aanvalstechniek.[112]

In november werden 900.000 klanten van Deutsche Telekom het slachtoffer van een ander Mirai-botnet.[113] De Speedport-router van deze groep mensen werd geïnfecteerd door het botnet, waardoor hun internetverbinding wegviel. In diezelfde maand werd bekend dat een twaalf jaar oude kwetsbaarheid in OpenSSH misbruikt werd om toegang te krijgen tot embedded apparaten met een internetaansluiting.[114] Deze apparaten werden vervolgens misbruikt om verdere aanvallen op andere systemen uit te voeren.

Weinig aandacht voor veiligheid apparaten maakt misbruik mogelijk

DDoS-aanvallen uitgevoerd met behulp van IoT-apparaten zijn zeer lastig om tegen te gaan. Er is weinig aandacht voor de beveiliging van IoT-apparaten. Standaardwachtwoorden worden door de gebruiker niet gewijzigd en het installatieproces van het apparaat verplicht dit niet. Software-updates vanuit de leverancier voor het verhelpen van kwetsbaarheden zijn bij IoT-apparaten ook nog niet gebruikelijk.[115] Hierdoor kunnen IoT-botnets makkelijk ontstaan en voor lange tijd onopgemerkt blijven voor de eigenaar van een IoT-apparaat. De snelheid waarmee apparaten geïnfecteerd worden ligt door de lage weerbaarheid van deze apparaten een stuk hoger dan bij reguliere werkstations.

Denial-of-service

Omvang van DDoS-aanvallen groeit

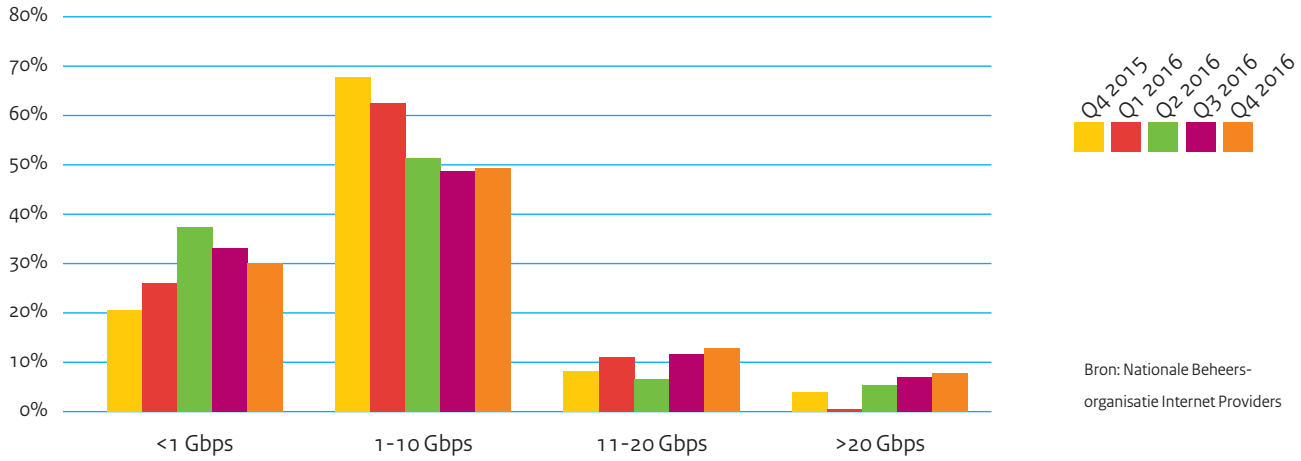
Naast de omvang van de grootste DDoS-aanval, neemt ook de omvang van de gemiddelde DDoS-aanval toe.[116]
Kwetsbare IoT-apparatuur levert een belangrijke bijdrage aan de stijging van de omvang van DDoS-aanvallen.[117] Opmerkelijk daarbij is dat, in tegenstelling tot andere DDoS-aanvallen, bij IoT-apparaten geen gebruik gemaakt wordt van speciale technieken om het effect van de aanval te vergroten. Tot nu toe is alleen het aantal kwetsbare IoT-apparaten dat gebruikt wordt maatgevend voor de omvang van aanvallen die ermee uitgevoerd worden.

In mei 2017 maakte Trend Micro melding van het Persirai-botnet, dat is staat is om 100 verschillende ip-cameramodellen aan te vallen[118] en daarmee DDoS-aanvallen uit te voeren. Op dat moment liepen naar schatting 120.000 camera's risico om onderdeel te worden van het botnet als gevolg van een kwetsbaarheid in de camera.

In 2016 heeft de Nationale Beheersorganisatie Internet Providers (NBIP) 681 DDoS-aanvallen verwerkt, wat neerkomt op een gemiddelde van bijna twee aanvallen per dag. Meer dan de helft van deze aanvallen hadden een omvang van tussen de 1 en 10 Gbps. Ongeveer 5 procent was groter dan 20 Gbps en rond de 30 procent was kleiner dan 1 Gbps. De grootste aanval bedroeg 53 Gbps en duurde 14 minuten. In 2016 duurde meer dan de helft van de aanvallen korter dan 15 minuten. Bijna 5 procent van de aanvallen duurder langer dan 4 uur, met een drietal aanvallen langer dan 5 achtereenvolgende dagen.

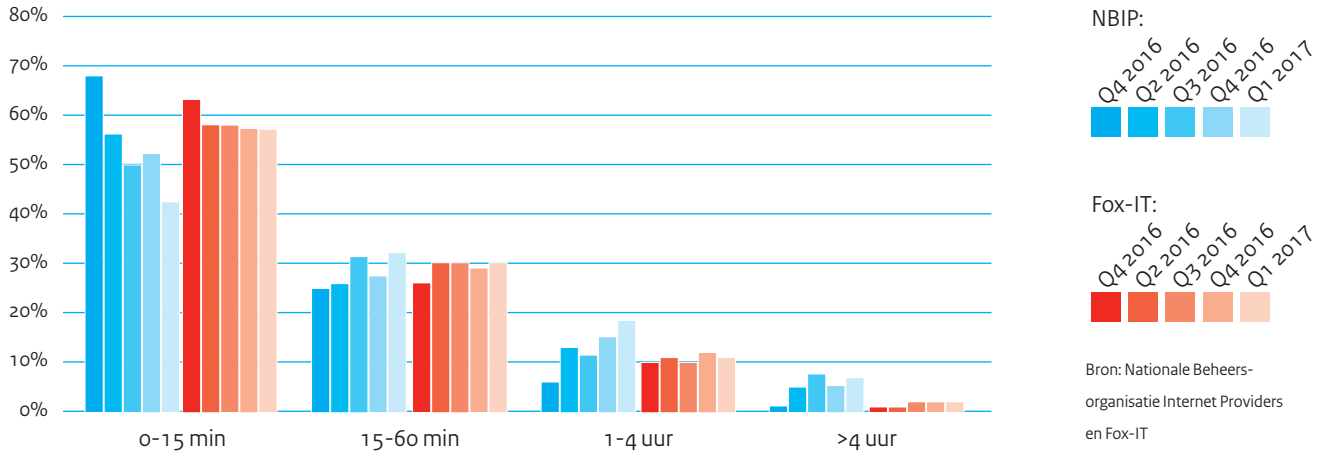
In 2016 heeft Fox-IT in samenwerking met DDoS.Watch met een monitoringsysteem ongeveer 1,3 miljoen DDoS-aanvallen geobserveerd naar binnen- en buitenland. Ongeveer 25.000

Figuur 1 **Omvang van DDoS-aanvallen**



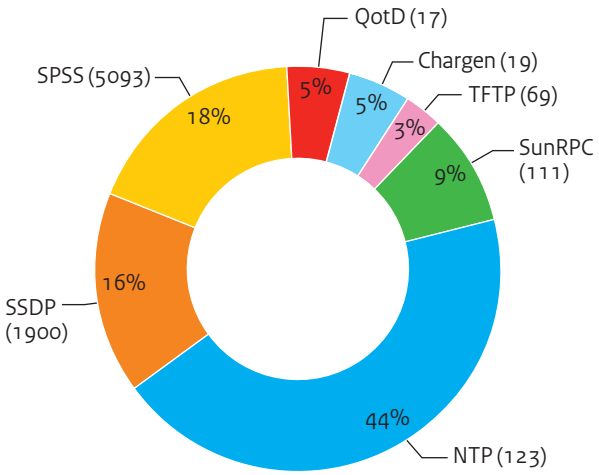
Bron: Nationale Beheers-organisatie Internet Providers

Figuur 2 **Duur van DDoS-aanvallen**



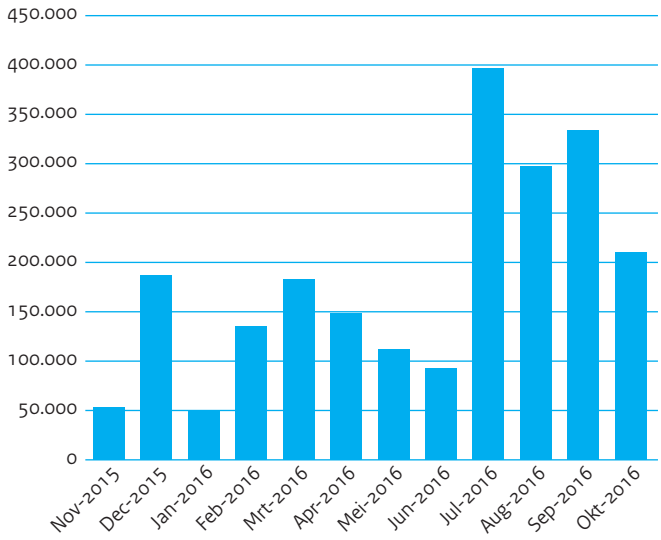
Bron: Nationale Beheers-organisatie Internet Providers en Fox-IT

Figuur 3 **Gebruikte protocollen voor reflectie-aanvallen via Nederland**



Bron: Akamai

Figuur 4 **Aantal gebruikers aangevallen door ransomware**



Bron: Kaspersky Lab

daarvan waren gericht op ip-adressen in Nederland. Hiermee staat Nederland op de negende plek van landen die het vaakst slachtoffer waren van DDoS aanvallen in 2016. Een groot aantal van de aanvallen was gericht op de internetverbindingen van consumenten en was slechts van korte duur. Slechts een klein percentage van de aanvallen was langer dan 4 uur. In 2016 waren DNS-amplificatie-aanvallen nog steeds het populairst, maar op NTP gebaseerde aanvallen lijken in 2017 een opmars te maken.

Een Turkse hackersgroep beloont anderen voor het uitvoeren van aanvallen. Zij hebben daarvoor een DDoS-tool beschikbaar gesteld en geven punten aan hen die een vooraf gekozen website aanvallen.[119] Deze punten kunnen vervolgens ingewisseld worden voor andere hacking tools.

Ransomware

Ransomware blijft lucratief

Ransomware is nog steeds een zeer lucratieve en groeiende tak van cybercriminaliteit.[120] Van het aantal erkende cyberaanvallen is het percentage ransomware-aanvallen in de tweede helft van 2016 gestegen van 5,5 naar 10,5 procent.[121]

Naast de gebruikelijke betalingsmethoden, vaak bitcoin, zijn in 2016 ook ransomwarevarianten opgedoken waarbij gevraagd werd om iTunes- of Amazon-cadeaubonnen voor de betaling van het losgeld.[122] [123] Een opmerkelijke keuze, omdat deze veel eenvoudiger te traceren zijn dan de gebruikelijke betalingsmethoden.

Onderzoek wijst uit dat wereldwijd de zorgsector het vaakst getroffen wordt door ransomware.[124] De Nederlandse zorgsector heeft daar ook last van. Hoewel het waarschijnlijk meestal gaat om ongerichte verspreiding, geeft de sector aan het vermoeden te hebben soms te maken te hebben met gerichte aanvallen.[125]

Het afgelopen jaar was een verbreding van het speelveld van ransomware zichtbaar. Naast de klassieke aanvallen per e-mail op werkstations, zijn er ook aanvallen uitgevoerd waarbij exploits werden gebruikt om servers te besmetten.[126] Ook de informatie in slecht beveiligde online databases kunnen worden gegijzeld, waarbij losgeld betaald moet worden om deze informatie weer terug te krijgen. Dit ondervonden vele gebruikers van de databasesoftware MongoDB rond de jaarwisseling van 2016-2017.[127]

Het uitvoeren van ransomwarecampagnes wordt ook steeds gemakkelijker. Beroepscriminelen kunnen door middel van ransomware-as-a-service malware afnemen om deze vervolgens zelf te verspreiden.[128] Deze ontwikkeling is niet nieuw, maar heeft zich het afgelopen jaar wel voortgezet. In april 2017 werd bericht over de ransomwarevariant Karmen die aangeboden wordt als ransomware-as-a-service voor het bedrag van slechts 175 dollar.[129]

Android-apparaten zijn ook het doelwit van ransomware

Ransomware op mobiele Android-apparaten neemt toe.[130] Gebruikers worden verleid tot het installeren of updaten van een app, waarna het toestel geïnfecteerd raakt. Het apparaat wordt vervolgens vergrendeld en de gebruiker moet losgeld betalen om weer toegang te krijgen. Daarbij wordt gevraagd om betaling via

prepaid-kaarten. Net als in de begindagen van ransomware op de pc, leidt betalen niet altijd tot daadwerkelijk vrijgeven van het mobiele apparaat. Ransomware op een mobiel apparaat lijkt minder impact te hebben dan op de pc, omdat dit soort apparaten vaker een automatische cloudback-up hebben. Het potentiële bereik van ransomware op smartphones is echter groter dan op andere apparaten: de smartphone heeft de laptop gepasseerd en was in Nederland in 2016 het meest gebruikte apparaat voor internetgebruik.[131] [132]

Besmettingen via nieuwe methoden en op andere apparaten dienen zich aan

Een nieuwe manier om ransomware op de computer van een slachtoffer te krijgen is door middel van een aanval op Remote Desktop Protocol (RDP).[133] Via een dergelijke aanval wordt toegang verkregen tot het systeem, dat vervolgens geïnfecteerd wordt met ransomware. De WannaCry-ransomware maakte misbruik van een kwetsbaarheid in bestandsdelingsprotocol SMB om zichzelf te verspreiden.

Criminelen zijn creatief in het zoeken naar nieuwe mogelijkheden om aan geld te komen. Dit werd duidelijk door een geval van ransomware op een televisietoestel.[134]

Cybercriminelen worden steeds brutaler in hun aanpak

Aanvallen door criminelen worden niet alleen technologisch gezien geavanceerder. Ook op andere vlakken zoeken criminelen naar meer en betere mogelijkheden om hun doel te bereiken. Ze zoeken daarbij vaker direct contact met hun potentiële slachtoffers. Zo werd begin 2016 melding gemaakt van ransomware met een live-chatfunctionaliteit.[135] Daarmee boden de cybercriminelen de slachtoffers ondersteuning bij het betalen van het losgeld om de decryptiesleutel te ontvangen.

Slachtoffers van de Popcorn Time-ransomware hadden, naast de optie om te betalen voor het verkrijgen van de decryptiesleutel, de mogelijkheid om twee anderen te besmetten met de ransomware om zo gratis de decryptiesleutel te ontvangen.[136] Voorwaarde daarbij was dat de twee nieuwe slachtoffers daadwerkelijk zouden betalen voor hun decryptiesleutel.

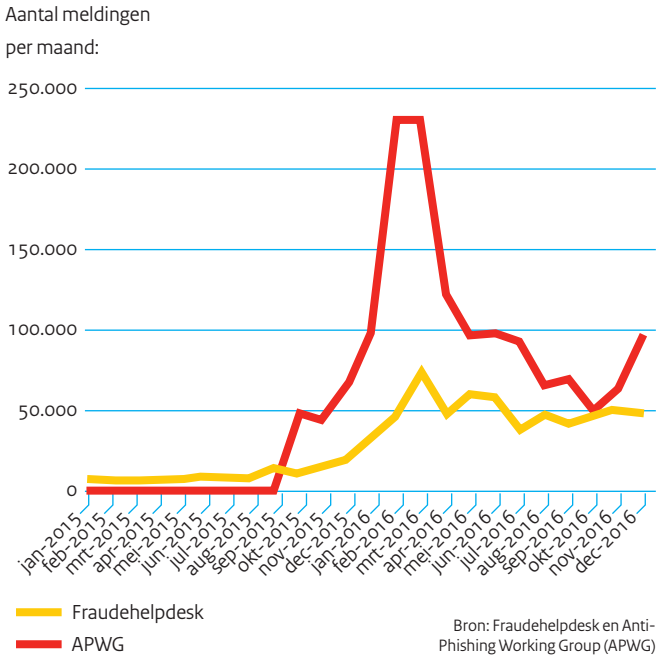
Slachtoffers van de CryptXXX ransomware kregen eind 2016, bij wijze van een kerstaanbieding, korting op de aankoop van de decryptiesleutel.[137] Deze tijdelijke korting had als doel om twijfelaars over te halen om alsnog te betalen.

E-mail

E-mail is nog altijd populair bij aanvallers

E-mail is ook in 2016 het meest gebruikte medium om ransomware te verspreiden.[138] E-mail kent niet overal een juiste wijze van beveiliging. Criminelen kunnen daarmee eenvoudig grote hoeveelheden potentiële slachtoffers bereiken. Het is voor de gemiddelde ontvanger van een e-mail niet vast te stellen of de afzender wel authentiek is.

Figuur 5 **Aantal meldingen van phishing-e-mails sterk toegenomen in 2016**



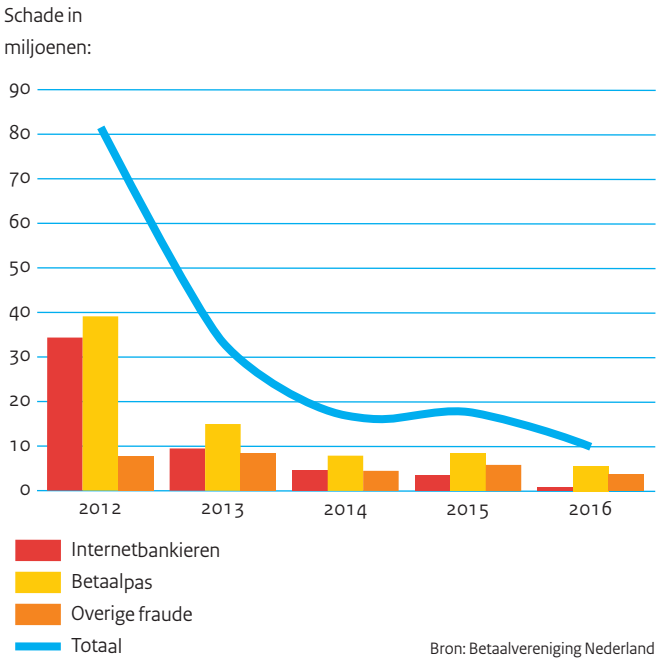
Bron: Fraudehelpdesk en Anti-Phishing Working Group (APWG)

Phishing, met name via e-mail, is nog steeds veel gebruikt door cybercriminelen. Berichten worden geraffineerder en ogen professioneler. In 91 procent van de gevallen[139] werd phishing gebruikt om een cyberaanval te beginnen. Vorig jaar berichtte de Fraudehelpdesk over een groot aantal meldingen van phishing-e-mails.[140]

Begin april verscheen een onderzoeksrapport over de 'Cloud Hopper'-campagne.[141] Deze campagne richt zich met name op managed service providers. Voor het verschaffen van toegang tot netwerken van deze providers worden spearphishing-e-mails met malware verzonden. Na een succesvolle malware-infectie wordt vervolgens naar gevoelige gegevens van klanten gezocht, zoals intellectueel eigendom en persoonsgegevens. De gevonden informatie wordt van systemen van de klant van de provider weggesluisd naar het netwerk van de provider zelf, en vervolgens doorgeleid naar de infrastructuur van de aanvallers.

CxO-fraude, waarvoor vaak spearphishing gebruikt wordt, heeft in het afgelopen jaar wereldwijd voor een flinke schadepost gezorgd.[142] Het NCSC heeft de afgelopen periode vanuit verschillende sectoren meerdere meldingen ontvangen over pogingen tot CxO-fraude. Bij slechts enkele van deze pogingen heeft dit geleid tot daadwerkelijke diefstal van financiële middelen.

Figuur 6 **Schade door fraude in het betalingsverkeer in Nederland**



Bron: Betaalvereniging Nederland

Hoewel bestaande middelen volop worden ingezet en lucratief zijn, zijn cybercriminelen voortdurend op zoek naar nieuwe middelen. Daarnaast zoeken ze naar nieuwe manieren om de bestaande middelen effectiever in te zetten. Zodra de weerbaarheid tegen middelen toeneemt, gaan cybercriminelen op zoek naar andere middelen.

Financiële sector

Banken bestrijden fraude steeds effectiever

Banken weten fraude bij internetbankieren steeds beter te bestrijden. De schade die door fraude ontstaat is in 2016 met 78 procent gedaald ten opzichte van 2015.[143] [144] Cybercriminelen richten zich daardoor niet alleen op consumenten, maar steeds vaker ook op bedrijven en de banken zelf. Hierbij is een differentiatie zichtbaar: er blijft een grote groep criminelen die zich richt op consumenten en het eenvoudig geld verdienen. Een andere, kleinere groep beroepscriminelen is in staat grote campagnes uit te voeren. Het aantal aanvallen dat ze daarbij uitvoeren is lager dan het aantal aanvallen richting consumenten, maar de middelen die ze daarbij inzetten zijn geavanceerder en de opbrengst per aanval kan vele malen groter zijn.[145] Bij aanvallen op zakelijke transacties profiteren criminelen van het feit dat deze transacties minder gebonden zijn aan vaste patronen, waardoor ze minder goed te beschermen zijn met transactiemonitoring.

In november 2016 verscheen een rapport van de veiligheidsonderzoeker Group-IB over een criminele groep, genaamd Cobalt, die het gemunt heeft op geldautomaten.[146] Met behulp van spearphishing-e-mails is bij enkele buitenlandse banken toegang verkregen tot het lokale netwerk van de bank. Hierdoor kon Cobalt stap voor stap het van internet afgeschermde geldautomatennetwerk besmetten. In korte tijd haalde men vervolgens een groot aantal geldautomaten leeg.

Malware op geldautomaten manifesteert zich buiten Nederland

Beveiligingsbedrijven TrendMicro en FireEye constateren een groei in het gebruik van malware voor geldautomaten: ATM-malware. De bedrijven publiceren analyses over nieuwe varianten die gericht zijn op middleware, een softwareplatform, waarmee geldautomaten van meerdere producenten kunnen worden aangevallen. Beide typen malware worden gebruikt als hulpmiddel bij een fysieke aanval en hebben zich niet in Nederland gemanifesteerd. De Nederlandse banken hebben bovendien al eerder maatregelen genomen waardoor dergelijke aanvallen grotendeels onmogelijk gemaakt worden.

TrendMicro rapporteert over ATM-malware Alice die zij hebben gevonden in een gezamenlijk onderzoeksproject met Europol EC3.[147] FireEye heeft ATM-malware Ploutus-D, een nieuwe variant van de reeds bekende malware Ploutus, waargenomen bij onderzoeken in Latijns-Amerika.[148] Het bedrijf stelt dat dit type malware vooral effectief zal zijn in landen met minder strikte fysieke beveiligingsmaatregelen op geldautomaten. Het blijft onduidelijk of Alice en Ploutus-D gerelateerd zijn.

Advertentie-industrie

Klikfraude zorgt voor schade in de advertentie-industrie

Cybercriminelen wisten eind 2016 met het Methbot-botnet grote hoeveelheden geld te stelen van de advertentie-industrie. Zij registreerden daarvoor domeinnamen op een dusdanige manier dat het leek alsof deze toebehoorden aan grote, bekende organisaties. Deze domeinnamen werden vervolgens aangemeld bij een advertentienetwerk om daar advertenties op te plaatsen.

Het algoritme vanuit het advertentienetwerk werd door de wijze van domeinnaamregistratie misleid, waardoor deze ten onrechte bepaalde dat het om een grote, interessante website zou gaan, om daar vervolgens een advertentie op te plaatsen. Met behulp van het botnet werd daarna geautomatiseerd op de advertenties geklikt, waarbij de adverteerder per klik een bedrag aan de eigenaar van de domeinnaam betaalde. Door geautomatiseerd in te loggen op socialemedia-accounts en het nabootsen van muisbewegingen en muisklikken vanuit een speciaal daarvoor ontwikkelde browser, werden echte gebruikers nagebootst.

Minder gevallen van malvertising

Het besmetten van systemen door het verspreiden van malware via advertenties op websites, malvertising, lijkt in Nederland minder vaak voor te komen. Vanuit de sectoren worden slechts enkele gevallen gemeld waarin organisaties ermee te maken hebben gehad. Hoewel er wereldwijd berichten zijn dat het aantal gevallen van malvertising blijft groeien ten opzichte van eerdere jaren,[149] lijkt Nederland hierdoor niet getroffen. RiskIQ meldt een groei van het totale aantal gevallen van malvertising van ruim 132 procent wereldwijd. Zowel aan de kant van de gebruiker als aan de kant van de website-eigenaren zijn het afgelopen jaar maatregelen getroffen om besmettingen door malvertising te voorkomen. Het gebruik van adblockers in Nederland is het afgelopen jaar gestegen tot 17 procent, tegen 13,9 procent in het tweede kwartaal van 2015,[150] [151] volgens cijfers van PageFair.

Spionagesoftware

Spionagesoftware van inlichtingendiensten wordt gecompromitteerd

In augustus 2016 beweren onbekende hackers die zichzelf the Shadow Brokers noemen een Amerikaanse spionagecampagne te hebben gecompromitteerd. Zij zouden door middel van een hack spionagemalware gestolen hebben.[152] Deze malware, hacktools en exploits stelden zij vervolgens voor een deel beschikbaar om hun claim kracht bij te zetten dat het hier daadwerkelijk om materiaal van Amerikaanse inlichtingendiensten zou gaan. Het deel dat de groep niet openbaar heeft gemaakt is in bulk aangeboden via een publieke veiling[153] en later worden delen openbaar gemaakt. De gepubliceerde bestanden bevatten spionagemalware om verschillende firewalls aan te kunnen vallen, waaronder die van bedrijven als Cisco, Fortigate en Juniper. Onderdeel hiervan betrof malware die wordt geassocieerd met actor the Equation Group, volgens Kaspersky Labs gelieerd aan Amerikaanse inlichtingendiensten.[154]

In maart 2017 publiceert Wikileaks[155] informatie over een ander lek. Het zou gaan om een interne wiki van de CIA die hackingtools en malware van de CIA documenteert. De hackingtools en malware zelf zijn niet vrijgegeven.[156] Wikileaks zegt toe deze informatie te delen met de leveranciers van producten of diensten waarin kwetsbaarheden worden uitgebuit.[157]

In april 2017 is er door the Shadow Brokers weer spionagemalware gepubliceerd. Ook hierbij claimen zij dat het gaat om malware afkomstig van Amerikaanse inlichtingendiensten. De meest besproken hulpmiddelen waren Eternalblue, een exploit die het bestandsdelingsprotocol SMB op Windowssystemen misbruikt om die systemen te compromitteren, en Doublepulsar, een achterdeur die op gecompromitteerde systemen geïnstalleerd kan worden om diverse malafide code uit te voeren.[158] Opvallend is dat de misbruikte kwetsbaarheid door Microsoft al een maand voor publicatie verhopen werd met een beveiligingsupdate voor Windows.[159]

Begin mei 2017 werd de kwetsbaarheid die met Eternalblue uitgebuit wordt, grootschalig misbruikt. De ransomware WannaCry verspreidde zich door misbruik van de kwetsbaarheid naar computers in hetzelfde netwerk. Wereldwijd werden veel organisaties hierdoor zwaar geraakt, in Nederland was de impact beperkt. Onder de getroffen organisaties waren het Spaanse Telefónica, FedEx en de Britse National Health Service (NHS).[160] [161] Bij veel NHS-organisaties in Engeland en Schotland was de dienstverlening door de ransomwarebesmettingen ernstig verstoord.[162]

Conclusie en vooruitblik

De opkomst van het internet of things (IoT) brengt een hoop mogelijkheden en toepassingen met zich mee. Het biedt echter ook vele mogelijkheden voor cybercriminelen. Onveilige apparaten worden besmet om vervolgens misbruikt te worden voor verschillende aanvallen. Op beperkte schaal zorgt dit voor een dreiging richting de eigenaren van de apparatuur. Groter is het probleem dat besmette apparaten misbruikt worden om aanvallen uit te voeren op derden, zoals DDoS-aanvallen.

Uit de gebeurtenissen van het afgelopen jaar kan geconcludeerd worden dat cybercriminelen de reeds bekende middelen nog steeds veelvuldig inzetten. Middelen als ransomware, CxO-fraude en phishing blijven zeer effectief en lucratief. Naast de bekende wijze van inzet, zoeken criminelen ook naar manieren om deze middelen op een efficiëntere en meer winstgevende manier in te zetten. Aanvallers blijven inspelen op kwetsbaarheden in software die vaak niet tijdig opgelost worden, gecombineerd met het bespelen van gebruikers, bijvoorbeeld via phishing-e-mails.

Onderzoekers toonden meerdere malen aan dat, naast de besproken IoT-apparaten, ook in industriële controlesystemen (ICS)[163] in productieomgevingen en computers in voertuigen kwetsbaarheden zitten. Het is niet ondenkbaar dat criminelen de kwetsbaarheden in dit soort systemen ontdekken en gaan misbruiken om hun doel te bereiken.

Het verleden laat ons zien dat beveiliging niet op de eerste plaats komt bij de ontwikkeling van nieuwe producten. Zeker de laatste jaren geldt voor veel organisaties dat omzet, naamsbekendheid en marktaandeel belangrijker gevonden worden dan het leveren van een veilig product.[164] [165] De verwachting is daardoor dat, naast alle reeds aangeschafte en op internet aangesloten IoT-apparaten, ook nieuw ontworpen IoT-apparaten relatief makkelijk te misbruiken kwetsbaarheden zullen bevatten.

Het gebruik van clouddienstverlening voor schaduw-ict levert extra risico's op

4 Weerbaarheid

Nederland neemt op digitaal gebied steeds meer maatregelen, maar het kan de ontwikkelingen op het gebied van kwetsbaarheden nog niet bijbenen. Het internet of things is het afgelopen jaar in het bijzonder kwetsbaar gebleken. Organisaties kiezen nog altijd graag voor de makkelijkste wegen, maar het bewustzijn groeit.

Weerbaarheid is de mate waarin maatregelen zijn getroffen om de kwetsbaarheid voor beveiligingsproblemen te verminderen. Dit hoofdstuk beschrijft de ontwikkelingen op het gebied van de maatregelen die worden genomen en de kwetsbaarheden die nog blootliggen. De weerbaarheid van Nederland wordt hieronder behandeld aan de hand van de mens, de techniek en de organisatie.

De mens

Medewerkers regelen zelf online diensten: schaduw-ict beperkt de grip op beveiliging

Organisaties krijgen in toenemende mate te maken met schaduw-ict. [I][166] Hierbij wordt gebruikgemaakt van ict-oplossingen die niet via de formele weg zijn ingekocht, zoals zelfgekochte hardware of online diensten. Dit heeft tot gevolg dat de beheerprocessen niet altijd worden toegepast op die systemen en processen. Daardoor kan het beveiligingsniveau ervan niet beheerst worden. Het gebruik van clouddienstverlening voor schaduw-ict levert extra risico's op.

Eindgebruikers hebben behoefte aan makkelijke manieren om hun werk uit te voeren. Waarschijnlijk ligt die overweging ten grondslag aan de toename van schaduw-ict. Organisaties noemen vooral het aanwenden van privé-e-mail, clouddiensten (vaak voor bestandsuitwisseling), online bestandsconverters en chatapps voor zakelijke doeleinden als punten van zorg.[167]

Browserontwikkelaars helpen gebruikers zichzelf beter te beschermen

Internetbrowsers nemen maatregelen om gebruikers beter te informeren. Zo hebben Google Chrome[168] en Mozilla Firefox[169] aangekondigd alle websites die geen gebruik maken van https te bestempelen als onveilig. In eerste instantie kiezen de browsermakers ervoor alleen de veiligheidsopmerking te tonen wanneer een webpagina over http een formulier met wachtwoordveld bevat. Uiteindelijk zijn de makers van plan bij alle http-pagina's te wijzen op het risico.

Hoewel een doorsnee gebruiker mogelijk weinig waarde hecht aan een dergelijke melding bij een informatieve webpagina, kan deze maatregel website-eigenaren wel aansporen om https toe te passen.

Het als onveilig bestempelen van onversleuteld http-verkeer helpt gebruikers zich te beschermen tegen het afluisteren van communicatie. Het gebruik van https is echter geen garantie dat er gecommuniceerd wordt met de juiste partij. De opkomst van *domain validated* certificaten zorgt ervoor dat iedereen die de controle over een domeinnaam heeft, een geldig certificaat voor die domeinnaam kan aanvragen. Wanneer dit echter gedaan wordt met domeinnamen die lijken op legitieme namen, kan de gebruiker alsnog misleid worden.

I Schaduw-ict zijn ict-middelen die buiten het zicht van de beheerorganisatie in gebruik zijn.

De techniek

Sms voor tweefactorauthenticatie wordt minder toereikend

Het Amerikaanse National Institute of Standards and Technology (NIST) heeft in juli 2016 een conceptrichtlijn openbaar gemaakt waarin sms niet meer geschikt wordt geacht voor tweefactor-authenticatie.[170] Het onderscheppen van sms-berichten zou dusdanig laagdrempelig zijn geworden voor aanvallers, dat NIST adviseert om alternatieve tweede factoren te overwegen.

In januari 2017 is in Azië een aanval waargenomen waarbij ge-sms'te tancodes voor internetbankieren zijn onderschept. Deze aanval werd uitgevoerd met vervalste berichten volgens het SS7-protocol. De kwetsbaarheid van dit protocol was al langer bekend en is inherent aan sms-verkeer. Naast het onderscheppen van sms-berichten door misbruik van het SS7-protocol vormt ook de mogelijkheid om sms-berichten tussen verschillende apparaten te synchroniseren een dreiging voor het gebruik van sms voor tweefactorauthenticatie. Onderzoekers hebben aangetoond dat voor zowel Android als iOS aanvallen mogelijk zijn waarmee ontvangen sms-berichten vanaf de computer van de ontvanger te benaderen zijn.[171]

Twee belangrijke gebruikers van sms voor tweefactorauthenticatie in Nederland zijn internetbankieren van ING (voor tancodes) en DigiD van de overheid (voor inlogcodes). Minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties heeft verklaard de huidige authenticatiemogelijkheden van DigiD niet voor alle doeleinden veilig genoeg te achten.[172] DigiD zal daarom worden versterkt met het zogenaamde DigiD Substantieel, waarvan de uitrol het tweede kwartaal van 2017 zal starten. Voor DigiD Substantieel is een tweede factor vereist, bijvoorbeeld een paspoort of rijbewijs. Ook is er een DigiD-app ontwikkeld als alternatief voor sms-authenticatie.[173]

Daarnaast zullen de pilots met Idensys en iDIN in 2017 worden voortgezet.[174] Idensys en iDIN zijn beide stelsels van verschillende aanbieders van en middelen voor authenticatie. Het is vergelijkbaar met iDeal voor betalingen, waarmee een gebruiker de keuze krijgt via welke weg hij wil inloggen. Idensys en iDIN passen binnen het nieuwe Europese juridische kader van de Europese Verordening elektronische identiteiten en vertrouwensdiensten (eIDAS).

Internet of things kwetsbaar en misbruikt

De kwetsbaarheid van het internet of things heeft zich in het najaar van 2016 zichtbaar gemanifesteerd door Mirai-botnets. Omdat de softwarebroncode van het Mirai-botnet openbaar gemaakt is, werden door diverse actoren varianten verspreid.[175] Een groot aantal apparaten raakte besmet; de besmettingen die tot defecten leidden werden daarmee zichtbaar, maar dit is mogelijk slechts het topje van de ijsberg.[176] De Europese Commissie heeft begin mei 2017 in een verklaring laten weten later in het jaar te komen met maatregelen voor certificering om IoT-apparaten meer 'cyber ready' te maken.[177]

Mirai besmet apparaten door misbruik te maken van standaardwachtwoorden. De eigenaar van een apparaat heeft de verantwoordelijkheid om dit wachtwoord te wijzigen, maar de praktijk wijst uit dat de gebruiker geen weet heeft van het feit dat het apparaat een standaardwachtwoord gebruikt. Omdat de fabrikant noch de gebruiker de nadelen of aansprakelijkheid rechtstreeks ervaart bij een verminderde beveiliging ontbreekt bij hen het gevoel voor urgentie. Dit leidt tot een gebrek aan duurzaamheid van ict.

Mirai-botnets zijn betrokken geweest bij buitengewoon grote DDoS-aanvallen. Verdedigen tegen aanvallen op deze schaal is nu alleen voor grote partijen financieel haalbaar. Er is nog geen oplossing voor de ongewenste bijwerkingen van het internet of things, daarom zal een gebrek aan duurzaamheid van ict een probleem blijven. Er gaan stemmen op om wettelijke kaders te stellen voor productverantwoordelijkheid, als de sector zichzelf niet kan reguleren.[178]

Uit onderzoek van het WODC naar kansen en bedreigingen van het internet of things blijkt dat de slechte beveiliging van IoT-toepassingen een bedreiging vormt voor veiligheid en privacy. Het onderzoeksrapport noemt vier factoren die de ontwikkeling en het gebruik van veilige en privacygevoelige IoT-toepassingen belemmeren: complexiteit van technologie, omgaan met big data en het speelveld; gebrek aan kennis en bewustzijn; gebrek aan prikkels; gebrek aan toezicht en handhaving.[179]

Kwetsbaarheden worden fundamenteler van aard

Leveranciers verhelpen softwarekwetsbaarheden sinds jaar en dag door middel van een security-update. De rapportageperiode heeft echter enkele kwetsbaarheden laten zien die fundamenteler van aard zijn en minder goed verholpen kunnen worden.

In augustus 2016 werd een aantal kwetsbaarheden in Android bekendgemaakt onder de noemer QuadRooter.[180] De kwetsbaarheden bevinden zich in drivers voor de chipsets van toeleveranciers, zoals een veelvoorkomende chip van het bedrijf Qualcomm voor wifi. Hierdoor kan een patch voor het bovenliggende besturingssysteem Android deze kwetsbaarheden niet verhelpen. De patch moet via de telefoonfabrikanten worden verspreid. Omdat dit een langere doorlooptijd had dan een reguliere patch kregen Androidgebruikers tot die tijd enkele adviezen voor mitigerende maatregelen.[181]

Onderzoekers van de Vrije Universiteit Amsterdam publiceerden gedurende de rapportageperiode meerdere aanvalstechnieken die dieper reiken dan doorgaans het geval is. Dedup Est Machina,[182] gepubliceerd in mei 2016, maakt misbruik van geheugen-deduplicatie om een browser over te nemen. Flip Feng Shui[183] kwam uit in augustus 2016 en stelt aanvallers in sommige gevallen

in staat vanuit een virtuele machine geheugen te beïnvloeden in andere virtuele machines. ASLR⊕Cache[184] werd in februari 2017 bekendgemaakt, hiermee kan beveiligingsmaatregel Address Space Layout Randomization (ASLR) worden omzeild.

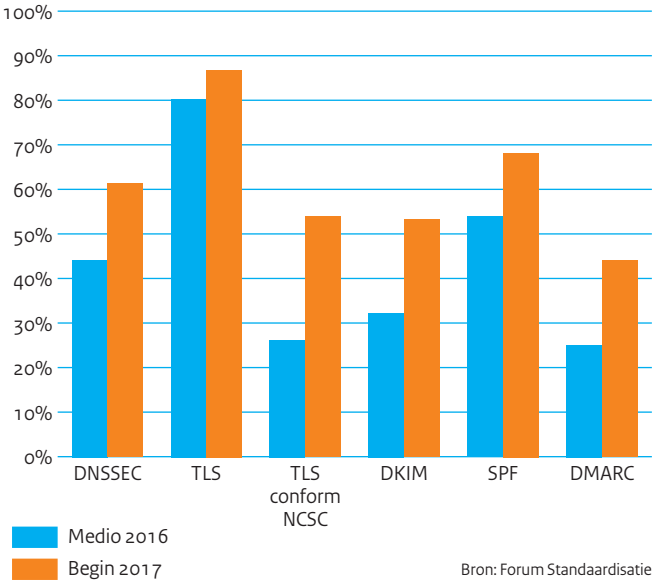
Standaarden om e-mail veiliger te maken vinden langzaam toepassing

De Nederlandse overheid en het bedrijfsleven lanceerden in februari 2017 een coalitie voor veiligere e-mail.[185] De coalitie beoogt het e-mailverkeer in Nederland beter te beveiligen om misbruik zoals afluisteren en phishing te voorkomen. E-mail is een techniek die van zichzelf geen enkele beveiligingsmaatregel tegen vervalsen, afluisteren of manipuleren bevat. Door een aantal aanvullende standaarden toe te passen in de e-mailbezorgingsketen wordt e-mailverkeer beter beveiligd.

De coalitie wil de toepassing van de standaarden SPF, DKIM, DMARC en STARTTLS met DANE en DNSSEC promoten. Deze standaarden moeten er onder meer voor zorgen dat e-mail geen vervalst afzenderadres kan hebben, niet inhoudelijk gewijzigd kan worden en niet gelezen kan worden door derden.[186] Omdat e-mail bezorgd wordt via steeds verschillende tussenliggende partijen is het belangrijk dat die standaarden door alle partijen worden toegepast. Adoptie van de standaarden door deze partijen is belangrijk, omdat zij een groot deel van het e-mailverkeer voor hun rekening nemen.

Uit onderzoek van het Forum Standaardisatie blijkt dat de adoptie van de standaarden om e-mail veiliger te maken door overheidsinstellingen het afgelopen jaar sterk gegroeid is.[187] De groei van onder andere het gebruik van TLS volgens de ICT-beveiligingsrichtlijnen voor TLS van het NCSC,[188] DKIM en DMARC heeft zich sterk doorgezet. De ambitie ligt echter hoger; het Nationaal Beraad heeft een streven naar 100 procent adoptie in 2017 uitgesproken. Dit lijkt op basis van de eerste meting niet te worden gehaald.

Figuur 7 **Adoptie van beveiligingsstandaarden door overheidsinstellingen**



Bron: Forum Standaardisatie

Encryptie vindt gretig aftrek

De toepassing van encryptie wordt steeds populairder. Er zijn bijvoorbeeld steeds meer websites die https toepassen. Dit is voor een deel het gevolg van lagere kosten voor de benodigde hardware en bandbreedte en gratis certificaten. Dankzij het initiatief Let's Encrypt zijn certificaten zonder aanschafkosten en eenvoudiger toepasbaar.[189]

Daarnaast is er ook steeds meer aandacht in de media en bewustzijn bij eindgebruikers waardoor de vraag naar https groter wordt. Publiciteit over de toepassing van https bij de overheid heeft minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties doen beslissen https voor alle overheidswebsites te verplichten.[190]

Chatapps passen ook end-to-endencryptie toe. Vanaf het moment dat marktleider in Nederland WhatsApp dit in april 2016 invoerde, is het ontbreken ervan ondenkbaar geworden. Berichten over een vermeende backdoor waarmee de encryptie in WhatsApp zou kunnen worden omzeild leverden dan ook enige ophef op.[191] Er bleek uiteindelijk geen sprake te zijn van een backdoor; het ging om functionaliteit die voorkomt dat reeds verzonden maar nog niet ontvangen berichten verloren gaan als een ontvanger van telefoon wisselt.[192] De kwetsbaarheid blijft wel bestaan.

De onrust die dergelijke berichtgeving met zich meebrengt lijkt erop te duiden dat een deel van de eindgebruikers het belang van encryptie bij allerlei netwerktoepassingen inziet. Hier wordt steeds vaker om gevraagd bij leveranciers.

De toenemende toepassing van encryptie vraagt ook om vertrouwen in certificaatleveranciers. Mozilla schortte in oktober 2016 het vertrouwen op in certificatiedienstverleners WoSign en StartCom. WoSign handelde in strijd met vertrouwensafspraken door certificaten uit te geven met een geldigheidsdatum in het verleden. Daarnaast verzweeg WoSign informatie over de aankoop van concurrent StartCom. Klanten van WoSign en StartCom moeten op zoek naar een nieuwe leverancier, nieuwe certificaten van beide bedrijven worden niet meer vertrouwd door Mozilla[193], Apple[194] en Google[195].

Encryptie beschermt gegevens voor een beperkte termijn. Naarmate computers krachtiger worden kan encryptie die in het verleden als sterk werd gezien steeds eenvoudiger worden gekraakt. De komst van kwantumcomputers kan grote gevolgen hebben voor gegevens die vandaag met sterke encryptie worden beschermd. Kwantumcomputers werken fundamenteel anders dan huidige computers en kunnen de momenteel meest gebruikte vormen van encryptie breken. Het NCSC heeft hierover een factsheet gepubliceerd.[196]

De organisatie

Organisaties hebben te weinig grip op informatiebeveiliging bij toeleveranciers

Grote organisaties zijn steeds beter in staat hun informatiebeveiliging goed te organiseren met beleid en procedures. Vaak maken zij echter gebruik van (kleinere) toeleveranciers waar het volwassenheidsniveau minder is. Bij de inkoop van hard- en software worden vaak security-eisen gesteld waar een product aanvankelijk aan voldoet. Voor de inkopende partij is het alleen niet altijd duidelijk hoe beheersmaatregelen bij de toeleverancier zijn ingericht. Hierdoor wordt soms bij latere wijzigingen niet meer aan de security-eisen voldaan.[197] Dit probleem doet zich voor in de gehele keten.

Grotere cloudleveranciers vormen hier een positieve uitzondering op. Doordat beveiligingsproblemen bij cloudleveranciers direct impact hebben op alle klanten tegelijk, krijgt cybersecurity daar veel aandacht. Het gevolg hiervan is dat deze partijen de naleving van hun informatiebeveiligingsbeleid doorgaans beter op orde hebben en compliance kunnen aantonen.[198]

Rapporten benadrukken behoefte aan cybersecurity

In een adviesrapport dat Herna Verhagen van PostNL aan het Kabinet heeft aangeboden, wordt de noodzaak van cybersecurity onder de aandacht gebracht.[199] Het rapport, opgesteld in opdracht van de Cyber Security Raad, stelt dat cybersecurity in Nederland met spoed versterkt moet worden. Er wordt gepleit voor meer ruimte voor coördinerende sturing vanuit de overheid, en voor het stimuleren van de verantwoordelijkheid van het bedrijfsleven. Er wordt een norm geopperd om 10 procent van het ict-budget aan cybersecurity te besteden.

Het Rathenau Instituut bracht eveneens een rapport uit over weerbaarheid van Nederland in het cybersecuritydomein.[200] Hierin wordt onder meer geconcludeerd dat er sprake is van marktfalen; de economische prikkels om cybersecurity in te bouwen ontbreken. Het Rathenau Instituut adviseert de overheid om het goede voorbeeld te geven als opdrachtgever, voldoende capaciteit te scheppen bij toezichthouders en veiligheidsdiensten, en te toetsen of de wetsvoorstellen Computercriminalieit III en modernisering Wet op de Inlichtingen- en Veiligheidsdiensten in de praktijk werken. Het bedrijfsleven krijgt de aanbevelingen zich aan zorgplichten te houden en samen met de overheid te investeren in cybersecurity-opleidingen.

De Algemene Rekenkamer concludeert in het verantwoordingsonderzoek bij de Rijksoverheid over 2016 dat er bij diverse ministeries onvoldoende aandacht is voor informatiebeveiliging. Er is volgens de Rekenkamer bestuurlijke aandacht vereist om gevoelige gegevens van burgers over een strafrechtelijk verleden, orgaandonatie, belasting- of medische informatie beter te beschermen. Identiteitsfraude, het hacken van systemen voor de bediening van bruggen en sluizen of andere kritieke systemen moet beter worden tegengegaan. Ook bij de Tweede Kamer is de beveiliging en het beheer van het financieel systeem nog niet voldoende.[201]

Ook op lokaal niveau kent de overheid uitdagingen. De Rekenkamer Rotterdam maakt in april 2017 een rapport openbaar waarin gemeld wordt dat de tekortschietende informatiebeveiliging van de gemeente leidt tot 'reële risico's op fysieke onveiligheid'. Gevoelige informatie is bij de gemeente Rotterdam onvoldoende in veilige handen, aldus de Rekenkamer Rotterdam.[202]

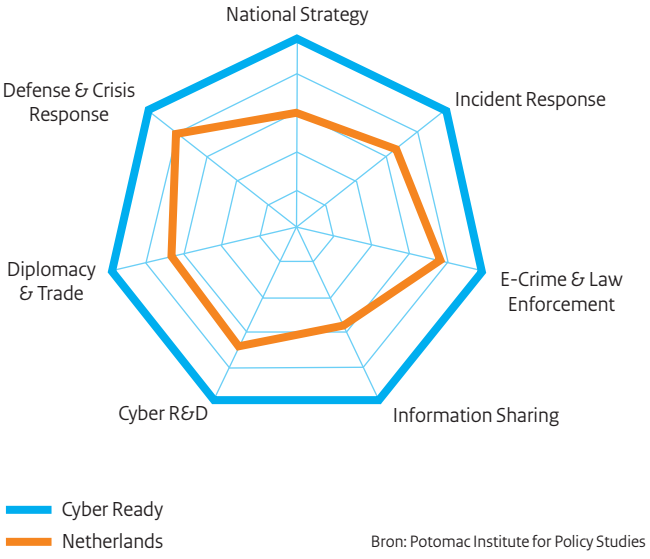
De Studiegroep Informatiesamenleving en Overheid die door het kabinet is ingesteld om een advies op te stellen over het verbeteren van het functioneren van de digitale overheid bracht op 18 april haar rapport uit.[203] Ze stelde vast dat in het huidige tijdsgewricht veiligheid, en specifiek bij digitalisering, cybersecurity een toenemend punt van aandacht is en adviseerde om de financiering van de Generieke Digitale Infrastructuur (GDI) als vitale infrastructuur voor Nederland structureel te borgen.

De Cyber Security Raad heeft een handreiking gepubliceerd met daarin een overzicht van zorgplichten op het gebied van cybersecurity. De publicatie maakt duidelijk dat elk bedrijf dat gebruik maakt van ict zorgplichten heeft op het gebied van cybersecurity, en geeft handvatten om deze in te vullen.[204]

Cyber Readiness Index duidt een gebrek aan financiële middelen voor cybersecurity in Nederland

Uit de in mei 2017 gepubliceerde Cyber Readiness Index voor Nederland blijkt dat Nederland een stevige cybersecuritystrategie heeft en goed op weg is met het versterken van digitale veiligheid, maar nog niet volledig *cyber ready* is. In het rapport, opgesteld door

Figuur 8 **Het Cyber Readiness Assessment voor Nederland**



Bron: Potomac Institute for Policy Studies

het Potomac Institute for Policy Studies, wordt het Nederlandse beleid op basis van 7 criteria geanalyseerd.

Nederland heeft een heldere visie, relevante strategieën en ambitie en doet het goed op het gebied van onderzoek en innovatie. Voldoende financiële middelen voor cybersecurity ontbreken echter, aldus de onderzoekers. Er wordt slechts 0,004 procent van het bruto binnenlands product aan cybersecurity besteed. Daarnaast wordt geconcludeerd dat informatiedeling verbeterd kan worden. De onderzoekers zien het als een aandachtspunt dat centrale besturing ontbreekt, omdat op het gebied van cyber security wordt geïnvesteerd in publiek-private samenwerking. Ook de informatiedeling vanuit de private sector kan meer worden gestimuleerd.

Verkiezingen: papieren proces leidend

In Nederland wordt er in het stemlokaal met een papieren stembiljet gestemd en worden de stembiljetten door het stembureau met de hand geteld. Deze processen zijn dus niet kwetsbaar voor cyberaanvallen.

In januari 2017 zijn er berichten verschenen over mogelijke kwetsbaarheden in de programmatuur (Ondersteunende Software Verkiezingen) die bij verkiezingen door gemeenten, hoofdstembureaus en de Kiesraad werd gebruikt om de tellingen van de stembureaus te verwerken tot de totaaluitslag van verkiezing.[205] De minister van Binnenlandse Zaken en Koninkrijkrelaties besloot daarom op 1 februari 2017 om maatregelen te treffen om te voorkomen dat er een schaduw van twijfel zou komen te hangen over de betrouwbaarheid van de uitslag van de verkiezing.[206] Zo is de digitale overdracht van de telresultaten verboden en zijn extra handmatige controletellingen toegevoegd. Door de getroffen maatregelen is bereikt dat in de hele keten, vanaf het stemmen tot en met het bepalen van de totaaluitslag het papieren proces leidend is geweest.

Ransomware en DDoS-aanvallen zijn dagelijkse kost voor grote organisaties

DDoS-aanvallen en ransomwarebesmettingen zijn aan de orde van de dag. Grote organisaties worden zo vaak getroffen dat mitigatie als een alledaagse activiteit wordt gezien.[207] Door investeringen in mitigatieprocessen en -middelen slagen organisaties er vaak in om DDoS-aanvallen af te slaan.[208] Bescherming tegen aanvallen van grote omvang, zoals de aanvallen met het Mirai-botnet, zijn echter niet gemakkelijk af te slaan. Het herstellen vanuit een back-up na een ransomwarebesmetting is routine geworden voor organisaties die daar inmiddels ervaring mee hebben. Desondanks kunnen hersteloperaties nog steeds kostbaar en tijdrovend zijn, en kan dataverlies niet altijd geheel ongedaan gemaakt worden.

Voor kleinere organisaties kunnen deze aanvallen nog steeds verstorend werken. Zij missen de nodige expertise en investeringsruimte voor DDoS-mitigatie, en hebben niet altijd een goed werkend back-upmechanisme om te herstellen van ransomwarebesmettingen.[209]

Bovendien zijn veel organisaties kwetsbaar doordat beveiligingsupdates niet tijdig geïnstalleerd worden. Uit onderzoek blijkt dat kleine organisaties relatief weinig maatregelen treffen. De maatregelen die zij treffen, zijn beperkt: vrijwel alle onderzochte bedrijven gebruikt een virusscanner, maar andere maatregelen zoals het hebben van beleid, getraind personeel en herstelprocedures bij incidenten worden bij slechts een derde of minder van de bedrijven genomen. Dit terwijl 79 procent van de bedrijven zegt dat de bedrijfsprocessen volledig afhankelijk zijn van ict.

Politie bestrijdt ransomware

Ransomware is in 2016 explosief gegroeid. Team High Tech Crime van de Nationale Politie doet onderzoek naar verschillende ransomwarevarianten zoals Locky, Shade, CTB-Locker, Torrentlocker, Cerber en Wildfire. Vooral Wildfire trof relatief veel Nederlanders. Wildfire richtte zich daarbij op het mkb en werd verspreid in phishing-e-mails met een malafide Worddocument met macro's.

Wildfire werd door de politie bedwongen na het lokaliseren en in beslag nemen van de command-and-controlserver. Deze server bevatte de decryptiesleutels van duizenden slachtoffers. Na het bemachtigen van deze sleutels heeft de politie in samenwerking met private partijen een decryptiehulpmiddel voor Wildfire kunnen uitbrengen. Tevens is de criminele infrastructuur met een gerechtelijk bevel definitief neergehaald. Meer dan 20 procent van alle Wildfire-slachtoffers heeft met het hulpmiddel bestanden teruggekregen. Dit past in de nieuwe aanpak van THTC waarin disruptie één van de vier pilaren van aanpak is.

De opvolgers van Wildfire maakten weinig slachtoffers in Nederland; de malware leek zich voornamelijk op Vlaanderen te richten.

No more ransom

THTC heeft in samenwerking met Europol EC3, Kaspersky Lab en Intel Security de website No more ransom[II] opgezet. Deze samenwerking loopt steeds beter en meer partijen sluiten zich aan. Sinds de start in juli 2016 zijn internationaal ongeveer 75.000 succesvolle decrypties uitgevoerd. Het zwaartepunt in de gegevens van 2016 was de Shade-ransomware, waarvan de slachtoffers voornamelijk in Rusland zaten.

De No more ransom-website is sinds de introductie meer dan 51.000 keer aangevallen en is dus blijkbaar succesvol in het disruptief optreden tegen cybercriminelen en het ontsleutelen van bestanden van slachtoffers.

II https://www.nomoreransom.org/

Conclusie en vooruitblik

Overheid, bedrijfsleven, wetenschap en burgers in Nederland verrichten veel inspanningen om de digitale weerbaarheid te vergroten. Toch blijft het bijhouden van de groeiende kwetsbaarheid van de maatschappij als geheel een grote uitdaging. Vooralsnog lijkt dit gat eerder groter te worden dan kleiner. Mensen blijven gebruiksgemak het belangrijkst vinden in hun digitale activiteiten. Zowel privé als op het werk verkiezen zij de snelste en makkelijkste oplossing boven de veiligste. Toch groeit ook het bewustzijn: het encryptiedebat heeft meerdere keren het nieuws gehaald, waardoor de vraag van eindgebruikers naar encryptie in de vorm van https op websites en end-to-endencryptie in chatapps groter is dan ooit. Encryptietoepassingen voor e-mail komen minder goed van de grond.

De kwetsbaarheid van het internet of things heeft zich ongekend sterk gemanifesteerd. De productverantwoordelijkheid en -aansprakelijkheid is op dat gebied nog niet helder en de slachtoffers van misbruik zijn vooralsnog niet de producteigenaren zelf. Hierdoor voelt uiteindelijk niemand zich verantwoordelijk en is er sprake van marktfalen. Er lijkt vooralsnog weinig verandering te komen in deze situatie, terwijl de hoeveelheid apparaten die met het internet wordt verbonden gestaag toeneemt.

Organisaties worden steeds bewuster, mede door wet- en regelgeving. Grote organisaties hebben hun aandeel in DDoS-aanvallen en ransomware voor de kiezen gehad en zijn daardoor noodgedwongen naar een hoger volwassenheidsniveau geklommen. Toch worden basale maatregelen als het installeren van beveiligingsupdates vaak niet getroffen. Zowel grote als kleine organisaties doen dit vaak niet tijdig, waardoor malwarebesmettingen mogelijk worden. Kleine organisaties blijven achter, maar zijn als toeleveranciers van grote organisaties mede verantwoordelijk voor hun schakel in de keten. Een toenemende kwaliteit van opdrachtgeverschap van grote bedrijven en overheden zouden hun toeleveranciers in de toekomst naar een hoger niveau kunnen tillen.

Kosten en baten van cybersecurity komen niet altijd bij dezelfde partij terecht

5 Belangen

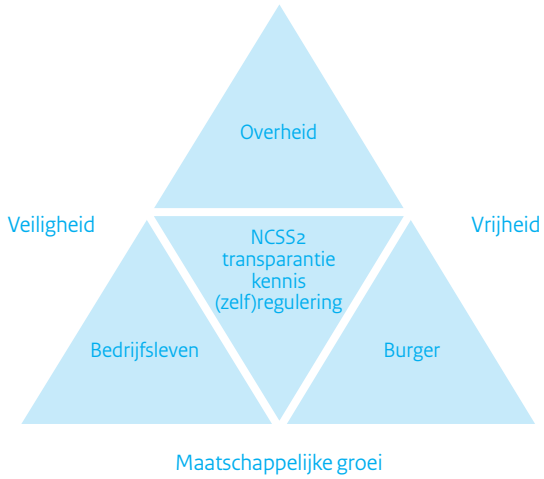
De toename van de afhankelijkheid van de Nederlandse samenleving van ict en het belang van cybersecurity gaan hand in hand. De belangen van het individu, organisaties, ketens en de maatschappij komen niet altijd overeen en de kosten en baten van cybersecurity komen niet altijd bij dezelfde partij terecht. Door het toenemend belang van ict is er vraag naar meer duidelijkheid over veiligheidseigenschappen van producten en diensten. De overheid past juridische kaders aan om de verantwoordelijkheid bij marktpartijen die nieuwe rollen vervullen of bestaande rollen overnemen te leggen. De internationalisering van ict-aanbieders raakt aan nationale veiligheidsbelangen. De besturing van het internet en internationale gedragsnormen voor staten in het digitale domein zijn onderwerp van aandacht. De opvattingen over het verantwoord onthullen van kwetsbaarheden lopen uiteen.

Samenspel van belangen

Verschillende afwegingen liggen ten grondslag aan balans van belangen

Bij het maken van keuzes ten aanzien van cybersecurity spelen verschillende belangen, waaronder individuele, organisatorische, keten- en maatschappelijke belangen. Deze kunnen samenvallen maar ook tegenstrijdig zijn. Individuen en organisaties maken vanuit hun eigen positie en vaak vanuit hun eigen belang kosten-batenafwegingen over cybersecuritymaatregelen. Keuzes van burgers, bedrijfsleven en de overheid raken aan vrijheid, veiligheid en maatschappelijke groei, waarbij altijd een balans gezocht moet worden.[210]

Figuur 9 **Afweging van belangen volgens de Nationale Cybersecurity Strategie 2**



Toename van afhankelijkheid van ict en belang van cybersecurity gaan hand in hand

De Nederlandse maatschappij blijft in toenemende mate afhankelijk van het goed functioneren van ict. De technologie maakt efficiëntie- en effectiviteitsverbeteringen mogelijk en het aantal toepassingsgebieden van ict neemt steeds verder toe.

De zichtbaarheid van deze toepassingsgebieden verschilt. Digitalisering van processen zoals communicatie met de overheid en bedrijven raakt het individu direct en is zo zichtbaar. De steeds bredere toepassing van de Berichtenbox voor communicatie met de overheid is daar een voorbeeld van.[211] Binnen de EU is Nederland koploper op het gebied van connectiviteit en het aantal burgers dat het internet gebruikt en daar de vaardigheid voor heeft.[212] Een andere zichtbare toepassing betreft de integratie van ict in auto's die zich vertaalt in (semi-)autonoom rijdende auto's en de toename van smart-hometoepassingen. Innovaties op het gebied van energievoorziening[213] en landbouw[214] zijn daarentegen minder zichtbaar voor het individu.

Cybersecurity en daarmee het ongestoord functioneren van ict vormt zo steeds meer een randvoorwaarde voor veel maatschappelijke processen en voor de verdere ontwikkeling van de digitale economie.[215] Deze persistente trend is in vorige edities van het CSBN meermaals gesignaleerd en zal zich naar verwachting de volgende jaren doorzetten. Het aantal systemen waarvoor geen analoog alternatief meer voorhanden is neemt toe. Tegelijkertijd wordt er ook specifiek voor gekozen om vanuit het belang van individuen en de maatschappij bepaalde analoge alternatieven zoals contant geld niet uit te faseren.[216]

Manifestaties van belangen

Belangen van het individu, organisaties, ketens en de maatschappij blijven in algemene zin en door de tijd heen constant. Zonder specifieke context blijven ze bovendien abstract. Belangen worden echter zichtbaar en concreter wanneer ze daadwerkelijk geraakt worden, wat vaak tot reacties van belanghebbenden leidt. De volgende paragrafen geven een duiding van illustratieve ontwikkelingen op het vlak van belangen in de rapportageperiode van dit CSBN.

Kosten en baten cybersecurity komen niet altijd bij dezelfde partij terecht

De belangen van individuen, organisaties en maatschappij als geheel lopen soms uiteen, zoals bij DDoS-aanvallen die veroorzaakt worden door misbruik van slecht beveiligde apparaten uit het internet of things.[217] Gebruikers van de apparaten zijn gebaat bij een werkend apparaat, en ondervinden vaak zelf niet direct schade als het apparaat misbruikt wordt. Deze groep heeft daarom ook niet direct baat bij het investeren in de veiligheid van deze apparaten, bijvoorbeeld door het betalen van een meerprijs voor een veiliger apparaat of het installeren van beveiligingsupdates.

Omdat gebruikers in die context niet vragen naar een betere beveiliging, hebben leveranciers geen directe prikkel om te investeren in de veiligheid. Aan de andere kant zijn de maatschappelijke gevolgen en schade voor derden groot als het apparaat misbruikt wordt om bijvoorbeeld DDoS-aanvallen uit te voeren. De slachtoffers hiervan zullen bovendien erg grote investeringen moeten doen om deze aanvallen af te kunnen slaan. De kosten voor het treffen van cybersecuritymaatregelen komen zo bij een andere partij terecht dan die ze veroorzaakt.

Verlangen naar meer duidelijkheid over veiligheidseigenschappen producten

De Consumentenbond eist in een bodemprocedure tegen Samsung dat deze minimaal twee jaar na aankoop of vier jaar na introductie (Android-)toestellen van updates voorziet.[218] Daarnaast eist de Consumentenbond dat Samsung duidelijke informatie hierover verstrekt aan consumenten. In de vorige editie van het CSBN werd opgemerkt dat gebruikers impliciet kwaliteitseisen stellen aan ict in de breedste zin.

De actie van de consumentenbond laat zien dat door het toegenomen belang van ict-producten gebruikers de behoefte hebben om deze eisen explicieter en veiligheidseigenschappen transparanter te maken. Alleen zo kunnen zij een afgewogen keuze maken. De maatschappij heeft hier ook belang bij, omdat zonder transparantie de keuze voor een product voornamelijk door de prijs en snelheid van marktintroductie wordt beïnvloedt. Meer marktbrede transparantie biedt leveranciers de mogelijkheid om zich te onderscheiden op het vlak van beveiliging.

Maatschappelijke rollen brengen verantwoordelijkheden met zich mee

Europese juridische kaders worden aangepast om verplichtingen op te leggen aan (nieuwe) marktspelers. Deze marktspelers vervullen een nieuwe rol in het maatschappelijk verkeer, of ze nemen al dan niet gedeeltelijk de rol over van al bestaande en vaak al gereguleerde spelers. De Europese Commissie heeft bijvoorbeeld voorgesteld om de ePrivacy-richtlijn te vervangen door een verordening,[219] waarbij naast traditionele telecommunicatie-aanbieders ook veel communicatiediensten op hogere systeemlagen onder het bereik vallen, zoals WhatsApp, Facebook Messenger en e-mailaanbieders.[220]

Op deze manier wordt getracht om eindgebruikers op gelijke wijze te beschermen en een gelijk speelveld te creëren voor marktaanbieders.[221] De nieuwe marktpartijen verzetten zich tegen regulering, terwijl de gevestigde marktpartijen het ondersteunen.[222] In de Verenigde Staten wordt duidelijk dat een dergelijke ontwikkeling ook andersom kan werken, waarbij gevestigde partijen voor minder regulering pleiten om zo tot een gelijk speelveld met de nieuwkomers te komen.[223]

De eIDAS-verordening is een voorbeeld van regulering van marktspelers die een belangrijke relatief nieuwe rol vervullen in de digitale samenleving, de zogenaamde vertrouwensdiensten.[224] De verordening vormt de juridische basis voor elektronische handtekeningen, zegels, tijdstempels, documenten en websitecertificaten, en de verantwoordelijkheden voor de aanbieders daarvan.

Ook de op 27 april 2016 aangenomen Algemene verordening gegevensbescherming brengt nieuwe verantwoordelijkheden voor verwerkers van persoonsgegevens met zich mee, waaronder op het gebied van informatiebeveiliging en privacy-by-design.[225] Ook krijgt de gebruiker het recht om zijn persoonsgegevens op eenvoudige wijze te verkrijgen en over te zetten naar een andere aanbieder, ook wel dataportabiliteit genoemd. Dit voorkomt een vendor-lock-in, waarbij gebruikers vastzitten aan één dienstverlener.

Besturing van het internet overgedragen aan een non-profit organisatie

De Amerikaanse overheid heeft op 1 oktober 2016 de formele zeggenschap over essentiële functies van het internet overgedragen van de Amerikaanse National Telecommunications and Information Administration naar de private organisatie ICANN.[III] Om een vrij en open internet te behouden is de bestuursstructuur van ICANN volgens het multistakeholdermodel ingericht, waarbij zowel bedrijven, overheden, technische experts en civil society zijn vertegenwoordigd. Zo wordt geprobeerd om tot een evenwichtige belangenbehartiging te komen.[226]

III De essentiële (IANA-)functies omvatten de coördinatie van de uitgifte van ip-adressen en nummers van autonomous systems, het beheer van de dns-rootservers en het beheer van een aantal internetprotocollen.

De bovenstaande ontwikkeling sluit aan bij de visie van het Nederlandse kabinet op de besturing van het internet, ook wel internet governance genoemd. Het kabinet stelt in zijn reactie op de rapporten van de Adviesraad Internationale Vraagstukken (AIV) en de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) vast dat een open model van internetgovernance cruciaal is geweest voor de ontwikkeling van het internet en dat zelforganisatie en zelfregulering een cruciale rol hebben gespeeld.[227]

Niet alle landen denken hetzelfde over de rol van de overheid in de besturing van het internet. Onderliggende motieven zijn vaak van politiek-economische en sociaal-maatschappelijke aard. Denk daarbij aan opvattingen over fundamentele rechten zoals de vrijheid van meningsuiting, of aan economische belangen samenhangend met wereldwijde digitale dienstverlening. Rusland en China streven bijvoorbeeld naar meer nationale zeggenschap over internetinfrastructuur en de informatie die daarmee wordt verstuurd.[228] Staten zouden, volgens deze landen, ook in het digitale domein soeverein moeten zijn en dus controle moeten kunnen uitoefenen.

Dit botst met westerse uitgangspunten over internetvrijheid. Ook Nederland heeft uitgesproken opvattingen op dit terrein. Het Nederlandse kabinet is, zoals verwoord in zijn Internationale Cyberstrategie, voor een open en ongefragmenteerd internet, waarbij economische kansen van wereldwijde digitalisering gegrepen worden, en waarbij fundamentele rechten en vrijheden en veiligheid gewaarborgd worden.[229]

Internationalisering van ict-aanbieders raakt nationale veiligheidsbelangen

De Nederlandse samenleving is steeds meer afhankelijk van ict en daarmee ook van de aanbieders daarvan. Internationalisering van deze aanbieders kan de nationale veiligheidsbelangen van Nederland raken. Het kabinet signaleert dat door verschuivende economische machtsverhoudingen de kans op overnames in de telecommunicatiesector, mede ingegeven door geopolitieke motieven, toeneemt.

Vanwege zorgen over oneigenlijke politieke druk vanuit het buitenland en over vertrouwelijkheid van communicatie stelt het kabinet een nieuwe bevoegdheid voor de minister van Economische Zaken voor om vanuit perspectief van openbare orde en nationale veiligheid ongewenste zeggenschap in een telecommunicatiepartij te kunnen verbieden.[230] Telecommunicatiepartijen betreffen naast telecomproviders ook bijvoorbeeld hostingdiensten, internetknooppunten, datacenters, vertrouwensdiensten en andere nog bij algemene maatregel van bestuur aan te wijzen categorieën van netwerken of diensten.

Ook overgang van niet-telecompartijen in buitenlandse handen kan gevolgen voor de nationale veiligheid met zich meebrengen, bijvoorbeeld partijen betrokken bij de bescherming van staatsgeheimen.[231] Dit kan leiden tot eisen voor aanvullende waarborgen. Daarnaast kunnen sociaaleconomische belangen een rol spelen, bijvoorbeeld in het kader van vijandelijke buitenlandse overnames van grote Nederlandse bedrijven.[232] Internationalisering brengt zo een duidelijke spanning met zich mee tussen het belang van economische vrijhandel en groei enerzijds, en bescherming van de nationale veiligheid anderzijds.

Belang van internationale gedragsnormen in het digitale domein neemt toe

In de aanloop naar de Nederlandse Tweede Kamerverkiezingen in maart 2017 zijn er zorgen geuit over mogelijke beïnvloeding van de Nederlandse verkiezingen door digitale aanvallen. Dit gebeurde naar aanleiding van gebeurtenissen rondom de Amerikaanse presidentsverkiezingen. Het ongestoord functioneren van de democratische instituties zonder beïnvloeding door buitenlandse mogendheden is van groot maatschappelijk belang.

Het beschermen van de soevereiniteit van landen is een belangrijk beginsel van het internationaal recht. De interpretatie en toepassing van het internationale recht in het digitale domein is echter niet altijd eenduidig. Met behulp van de Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations kan er meer duidelijkheid over de interpretatie van het huidige recht worden verkregen.[233]

Interpretatie van gedragsregels kan vergaande gevolgen hebben. De NAVO heeft wederom aangegeven dat een cyberaanval een grondslag kan vormen voor het inroepen van artikel 5 (collectieve verdediging) van het Noord-Atlantisch Verdrag. Het cyberdomein is door de NAVO erkend als vierde domein van oorlogsvoering.[234] Het belang van internationale gedragsnormen in het digitale domein neemt toe.[235] Door meer transparantie en voorspelbaarheid te creëren over wat wel en niet toegestaan is en hoe daarop gereageerd mag worden, worden conflicten in de toekomst beheersbaarder.

Opvattingen over het verantwoord onthullen van kwetsbaarheden lopen uiteen

Onthullingen over kwetsbaarheden in ict-systemen, -diensten en hardware- en softwareproducten kunnen een grote impact hebben. Coordinated vulnerability disclosure of responsible disclosure is dan ook een onderwerp dat veel in de belangstelling staat.[236] Enerzijds kunnen onthullingen ervoor zorgen dat verantwoordelijke partijen de kwetsbaarheden kunnen verhelpen en dat gebruikers tegenmaatregelen kunnen nemen. Anderzijds kunnen onthullingen kwaadwillende partijen in staat stellen kwetsbaarheden vroegtijdig uit te buiten.

De tijdsduur waarna een kwetsbaarheid openbaar wordt gemaakt door de ontdekker blijft een spanningspunt.[IV] Zo heeft Googles Project Zero in de rapportageperiode meerdere kwetsbaarheden in Microsoft-producten openbaar gemaakt, voordat er een patch beschikbaar was.[237] Openbaarmaking vond conform het Google

IV In de NCSC Leidraad Responsible Disclosure wordt een standaardtermijn van 60 dagen aangehouden.

Project Zero beleid automatisch 90 dagen na het ontdekken van de kwetsbaarheid plaats. De belangen van gebruikers kunnen hiermee op korte termijn worden geschaad, omdat kwaadwillenden er misbruik van kunnen maken. Google stelt hiermee echter de reactiesnelheid van de industrie te willen verbeteren, wat uiteindelijk alle gebruikers en de maatschappij ten goede zou moeten komen.[238]

Een ander spanningspunt is de bewoording van een vermeende kwetsbaarheid. Naar aanleiding van een melding tweette de New York Times dat inlichtingendiensten de versleuteling van WhatsApp, Signal en Telegram konden omzeilen, maar dat bleek te kort door de bocht.[239] Berichtgeving in de media kan enerzijds een belangrijke bijdrage leveren aan bewustwording over cybersecurity, anderzijds kan onvoldoende nauwkeurige berichtgeving tot overreacties in de maatschappij zorgen, waardoor bijvoorbeeld het vertrouwen in ict(-diensten) afneemt. Het is daarom voor mediabedrijven en individuele journalisten balanceren tussen het belang van een aantrekkelijk en daardoor veelgelezen verhaal en het aanbrengen van de benodigde nuance. De toegenomen belangstelling en publiciteit rondom technische kwetsbaarheden werd al eerder opgemerkt in het CSBN.[240]

Conclusie en vooruitblik

Cybersecurity is een randvoorwaarde voor het goed functioneren van maatschappelijke processen en de verdere ontwikkeling van de digitale economie. Bij onderwerpen die cybersecurity raken spelen individuele, organisatorische, keten- en maatschappelijke belangen, die soms tegenstrijdig kunnen zijn. Individuen en organisaties maken vanuit hun eigen positie en vaak vanuit hun eigen belang kosten-batenafwegingen over cybersecuritymaatregelen.

Kosten en baten komen niet altijd bij dezelfde partij terecht en er is een verlangen naar meer duidelijkheid over veiligheidseigenschappen van producten om zo een afgewogen keuze bij aanschaf te kunnen maken. Het is de verwachting dat de roep om (overheids)interventie zal toenemen indien door slecht beveiligde en op internet aangesloten apparatuur vaker of op grotere schaal verstoring van dienstverlening via het internet optreedt. Juridische kaders worden aangepast om de verantwoordelijkheden van marktpartijen te laten aansluiten bij de rol die zij in de maatschappij spelen.

De besturing van en nationale controle over het internet en de onderliggende infrastructuur zijn belangrijke discussieonderwerpen, evenals internationale gedragsnormen voor staten in het digitale domein. Naar verwachting zullen deze discussies in de komende jaren nog intensiever gevoerd worden, in het bijzonder wanneer geopolitieke spanningen oplopen.

De opvattingen over het verantwoord onthullen van kwetsbaarheden lopen uiteen, onder andere op het vlak van tijdsduur tot openbaarmaking van en de bewoording in berichtgeving over kwetsbaarheden. Het is niet te verwachten dat de onenigheid hierover zal verdwijnen en dat de grote publicitaire aandacht voor technische kwetsbaarheden op korte termijn zal afnemen.

Bijlagen

Bijlage 1 NCSC-statistieken

Deze bijlage geeft een overzicht van de responsible-disclosuremeldingen, beveiligingsadviezen en incidenten die door het NCSC zijn afgehandeld. Incidenten worden geregistreerd en bijgehouden met behulp van een registratiesysteem. Dit systeem is de bron voor alle onderstaande grafieken. Dit jaar heeft het NCSC ongeveer evenveel incidenten afgehandeld en 4 procent meer nieuwe beveiligingsadviezen geschreven dan het jaar daarvoor. Hoewel het aantal afgehandelde incidenten nauwelijks veranderd is ten opzichte van vorig jaar, is de verdeling over het soort incidenten wel veranderd.

Het NCSC faciliteert het doen en verwerken van responsible-disclosuremeldingen (RD-meldingen) voor zowel haar eigen infrastructuur als die van de Rijksoverheid en enkele private partijen, het uitbrengen van beveiligingsadviezen voor haar deelnemers en het afhandelen van cybersecurityincidenten. Hierover zijn voor deze rapportageperiode (mei 2016 tot en met april 2017) statistieken berekend die hieronder worden gepresenteerd. Door deze statistieken te vergelijken met eerdere rapportageperiodes kunnen trends en ontwikkelingen worden geïdentificeerd.

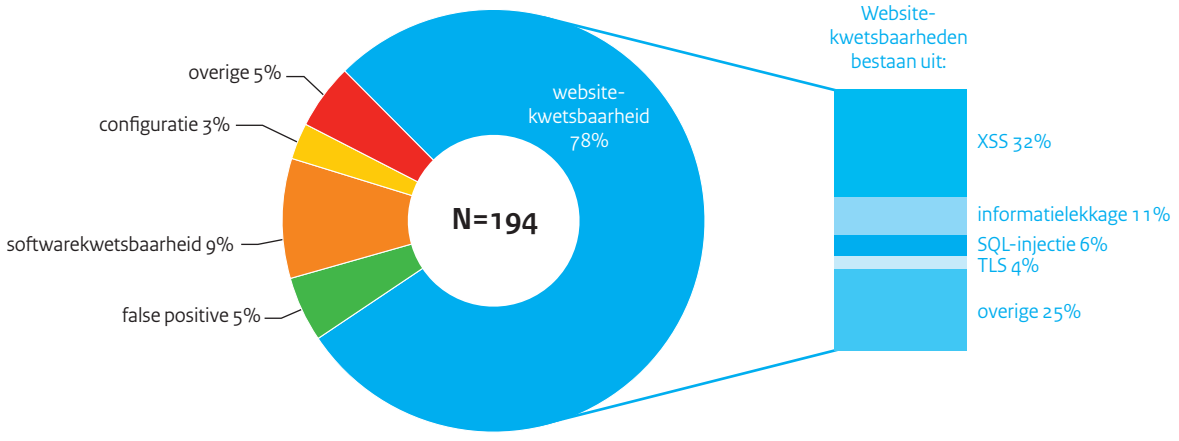
Responsible disclosure

In de rapportageperiode heeft het NCSC 194 RD-meldingen ontvangen. Dit zijn zowel meldingen voor eigen systemen als voor overige overheidssystemen en systemen van private partijen. In sommige gevallen is er sprake van een dubbele melding, bijvoorbeeld als twee of meer onderzoekers dezelfde kwetsbaarheid melden. Hierdoor is het totaal aantal meldingen niet representatief voor het totaal aantal kwetsbaarheden.

Vorig jaar waren er 113 meldingen. Dit betekent dat er dit jaar meer dan 70 procent meer meldingen gemaakt zijn. Deze toename kan deels worden verklaard door de uitbreiding van de rol van het NCSC als RD-meldloket van de Rijksoverheid.

In 5 procent van alle meldingen was er bij nader onderzoek of geen sprake van een kwetsbaarheid of sprake van een geaccepteerd risico. Een voorbeeld hiervan is de inlogpagina op een website die geen specifieke maatregelen heeft tegen bruteforce-aanvallen. Deze gevallen werden geclassificeerd als *false positive*. Vorig jaar was

Figuur 10 **Typen kwetsbaarheden in responsible-disclosuremeldingen**



dit 20 procent van alle meldingen. Deze afname kan deels worden verklaard door de toenemende volwassenheid van dit proces, voornamelijk aan de kant van de melder.

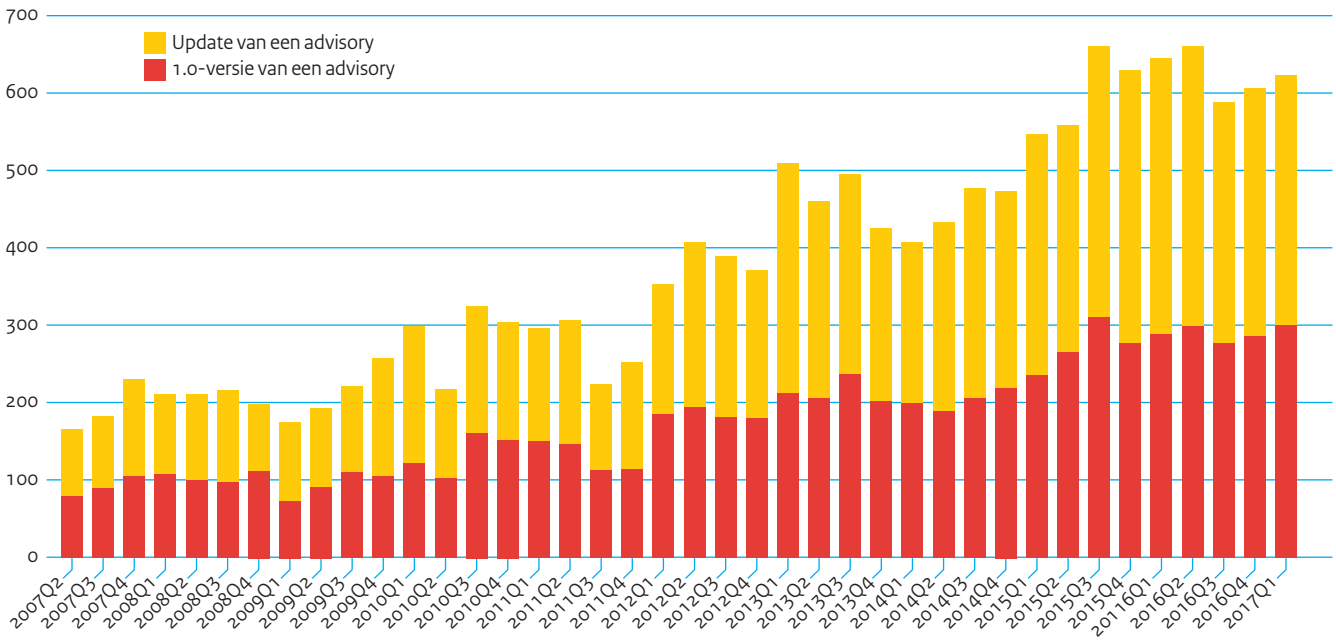
Figuur 10 toont de verschillende typen kwetsbaarheden die worden gemeld. De meerderheid (78 procent) van alle meldingen heeft te maken met een kwetsbaarheid in een website, een webapplicatie of infrastructuur waarop webapplicaties draaien. Voorbeelden van zulke meldingen zijn zwakke TLS-parameters, cross-site scripting (XSS), SQL-injectie en informatielekkage. Een voorbeeld van dat laatste is een kwetsbaarheid waardoor het mogelijk is om een configuratiebestand of een versienummer van een webapplicatie te zien. In 9 procent van alle meldingen is er sprake van een kwetsbaarheid in software (exclusief webservers en -applicaties). Relatief weinig meldingen (3 procent) hebben te maken met configuratiefouten in hard- en software.

Beveiligingsadviezen

Het NCSC publiceert beveiligingsadviezen (oftewel advisories) naar aanleiding van softwarekwetsbaarheden 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 organisatie slachtoffer wordt. Figuur 11 toont het aantal advisories dat het NCSC heeft gepubliceerd per kwartaal van het tweede kwartaal van 2007 tot en met het eerste kwartaal van 2017. Hierbij wordt onderscheid gemaakt tussen nieuwe advisories (met versienummer 1.0) en updates van bestaande advisories. In totaal heeft het NCSC 1179 nieuwe advisories gepubliceerd in de afgelopen rapportageperiode. Dit is ongeveer 4 procent meer dan het jaar daarvoor. Ook is het aantal updates van bestaande advisories licht gestegen naar 1336. Dit is een toename van ongeveer 1 procent.

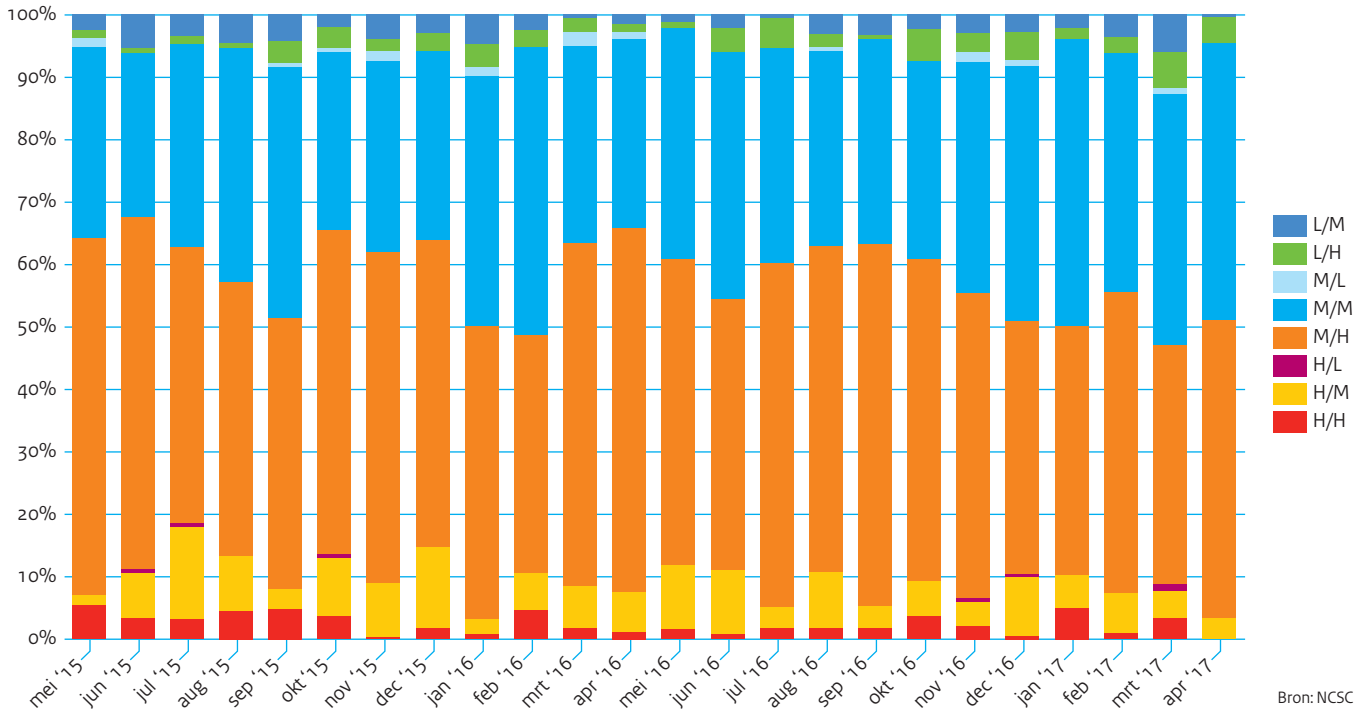
De beveiligingsadviezen van het NCSC worden ingeschaald op twee elementen. Ten eerste stelt men vast wat de kans is dat de kwetsbaarheid misbruikt wordt. Ten tweede bepaalt men de schade die in dat geval optreedt. De inschaling kent dus twee criteria: kans en schade. Voor beide criteria wordt, op basis 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 12 toont de verhoudingen tussen deze niveaus voor alle gepubliceerde adviezen (inclusief updates) per maand voor de afgelopen twee rapportageperiodes.

Figuur 11 **Aantal advisories per kwartaal (2007Q2 – 2017Q1)**



Bron: NCSC

Figuur 12 **Inschaling advisories per maand (mei 2015 – april 2017)**



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 2 getoond. Hierin is te zien dat beveiligingsadviezen die te maken hebben met denial-of-service (DoS) nog altijd het grootste aandeel hebben (61 procent). Hierna volgen het uitvoeren van willekeurige code met gebruikersrechten (42 procent), toegang tot gevoelige gegevens (32 procent), het verhogen van gebruikersrechten (19 procent) en het omzeilen van een beveiligingsmaatregel (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 totaal percentage van meer dan 100 procent.

Tabel 2 **Schadeomschrijving in beveiligingsadviezen CSBN 2015 tot en met CSBN 2017**

Schadeomschrijving	2015	2016	2017
Denial-of-Service (DoS)	51%	56%	61%
Remote code execution (gebruikersrechten)	29%	37%	42%
Toegang tot gevoelige gegevens	26%	32%	32%
Verhoogde gebruikersrechten	14%	21%	19%
Omzeilen van beveiligingsmaatregelen	19%	25%	17%
Toegang tot systeemgegevens	9%	13%	13%
Manipulatie van gegevens	5%	8%	10%
Cross-Site Scripting (XSS)	6%	9%	8%
Remote code execution (admin/rootrechten)	4%	6%	7%
Spoofing	2%	5%	5%
Omzeilen van authenticatie	4%	5%	3%
Cross-Site Request Forgery (XSRF)	1%	2%	2%
SQL-injectie	1%	2%	1%

Cybersecurityincidenten geregistreerd bij het NCSC

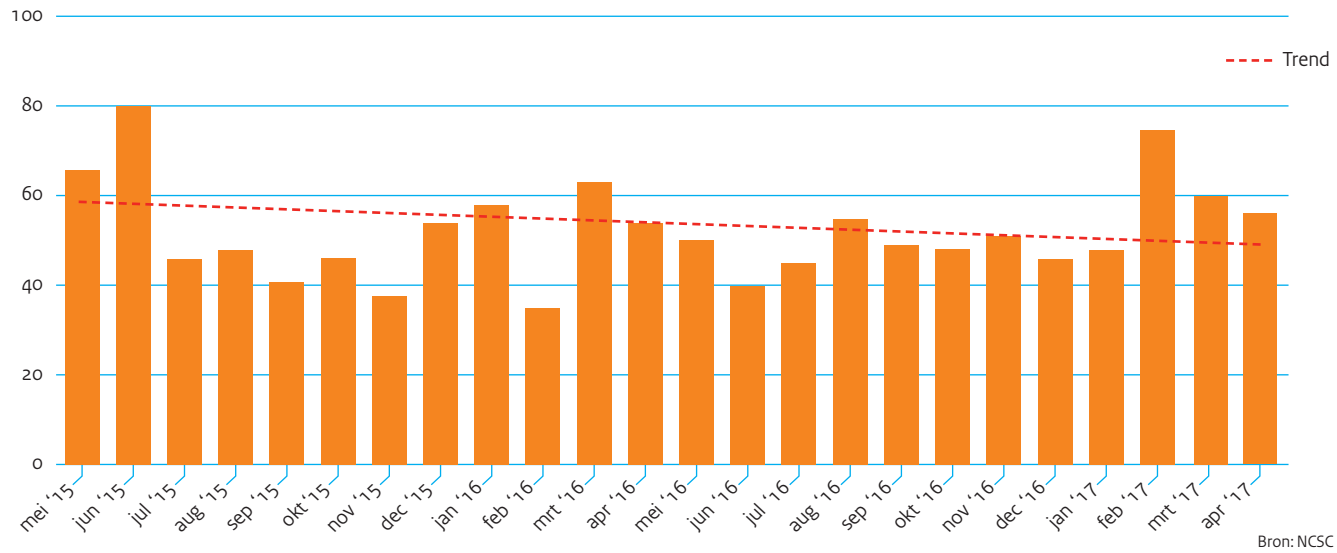
Het NCSC ondersteunt overheden en organisaties in vitale sectoren bij het afhandelen van incidenten op het gebied van ICT-veiligheid. In die rol worden bij het NCSC incidenten en kwetsbaarheden gemeld en worden deze ook door het NCSC zelf geïdentificeerd, bijvoorbeeld op basis van diverse detectiemechanismen.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

Aantallen afgehandelde incidenten

Het aantal afgehandelde incidenten per maand (exclusief geautomatiseerde controles) voor de laatste twee rapportageperiodes wordt in figuur 13 getoond. In de vorige rapportageperiode waren er in totaal 629 incidenten gemeld: gemiddeld 52 per maand. In deze rapportageperiode zijn er 623 incidenten gemeld: ongeveer 52 per maand. In grote lijnen, blijft het aantal (gemelde) incidenten constant.

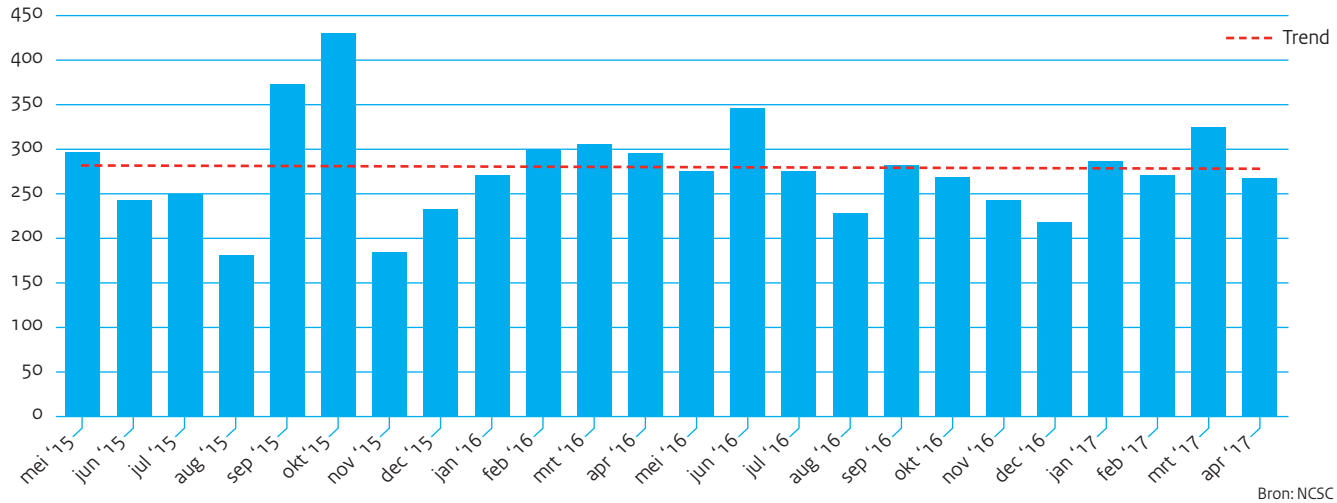
Figuur 14 toont de resultaten van geautomatiseerde controles voor de laatste twee rapportageperiodes. Hieruit blijkt dat er in de afgelopen rapportageperiode gemiddeld 275 incidentenmeldingen per maand zijn op basis van deze automatisering. In de vorige rapportageperiode waren er gemiddeld 280 meldingen per maand.

Figuur 13 **Afgehandelde incidenten (exclusief geautomatiseerde controles)**



Bron: NCSC

Figuur 14 **Geautomatiseerde controles**



Bron: NCSC

Een melding kan meerdere geïnfecteerde systemen binnen een organisatie betreffen.

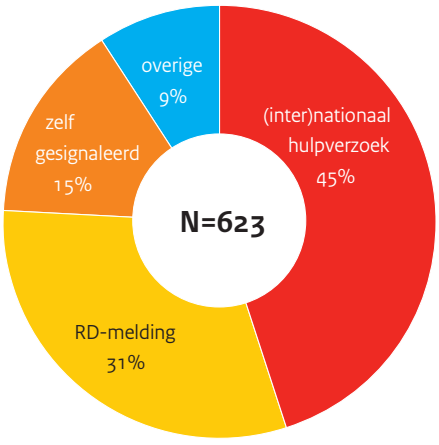
Verdeling incidenten per melding, categorie en afhandeling

De verdeling van incidenten naar meldingstype wordt in figuur 15 getoond. Dit geeft aan hoe een incident bij het NCSC gemeld is. Het merendeel van de incidentmeldingen (45 procent) komt van buitenaf: van nationale of internationale organisaties. Bij 31 procent van alle incidenten komt de melding binnen via responsible disclosure. In 15 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 de overige 9 procent van de meldingen was er sprake van diverse andere meldingen of informatie die ter kennisgeving is aangenomen.

Vergeleken met de vorige rapportageperiode is het percentage RD-meldingen sterk gestegen, van 18 procent naar 31 procent. Een mogelijke verklaring voor het toenemende aantal is de uitbreiding van de rol van het NCSC als RD-meldloket van de Rijksoverheid. Het percentage (inter)nationale hulpverzoeken is echter afgenomen sinds de vorige rapportage periode: van 57 procent naar 45 procent.

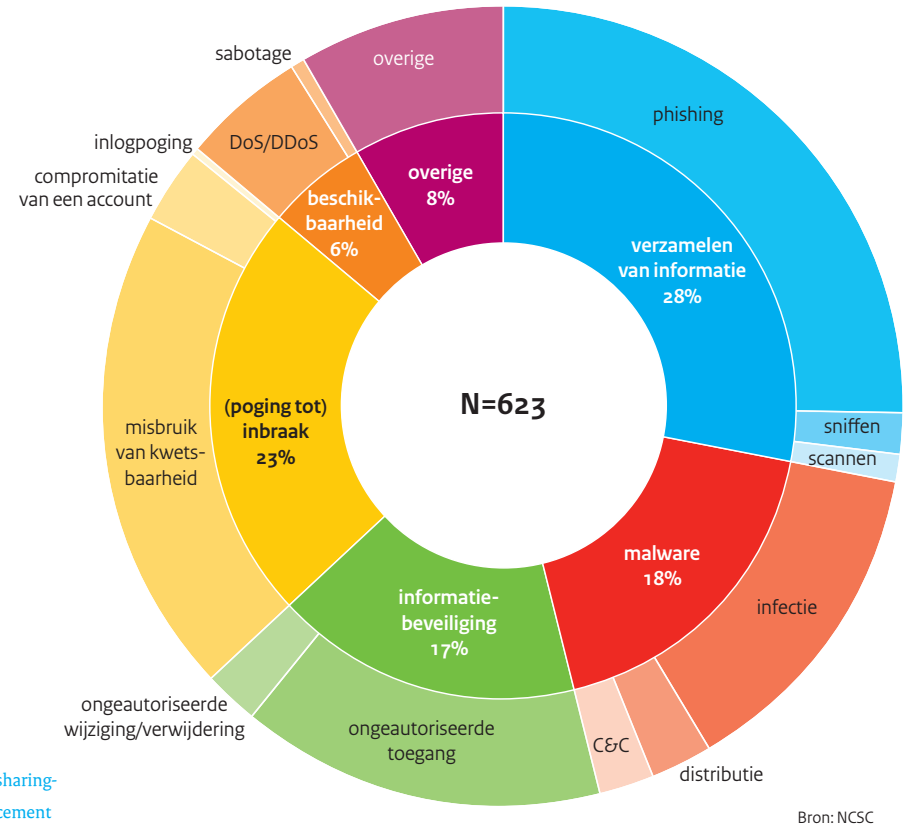
De verdeling incidenten per categorie wordt in figuur 16 getoond. Voor deze verdeling heeft het NCSC gebruikgemaakt van het door CERT.PT en ENISA voorgestelde incidententaxonomie.[v] In de binnenste ring worden de hoofdcategorieën getoond terwijl de subcategorieën in de buitenste ring getoond worden. Hieruit blijkt dat incidenten waarbij er sprake is van informatieverzameling voor meer dan een kwart (26 procent) van alle incidenten heeft gezorgd. Het overgrote merendeel hiervan betreft phishing, hieronder valt ook e-mailfraude. Incidenten waarbij er sprake is van malware hebben voor 18 procent van alle incidenten gezorgd. Het merendeel hiervan heeft met malwarebesmetting te maken. In 17 procent van alle incidenten was er sprake van ongeautoriseerde toegang of misbruik van een kwetsbaarheid. (Poging tot) inbraak zorgt voor 16 procent van alle incidenten. Hierbij gaat het voornamelijk om compromittatie van een account. Slechts 6 procent van alle incidenten had te maken met beschikbaarheid. Bijna al deze incidenten hadden te maken met Denial-of-Service (DoS)-aanvallen of -dreigingen. Het resterende deel (8 procent) heeft te maken met diverse incidenten waaronder het versturen van spam of fraude.

Figuur 15 **Afgehandelde incidenten per meldingstype**



Bron: NCSC

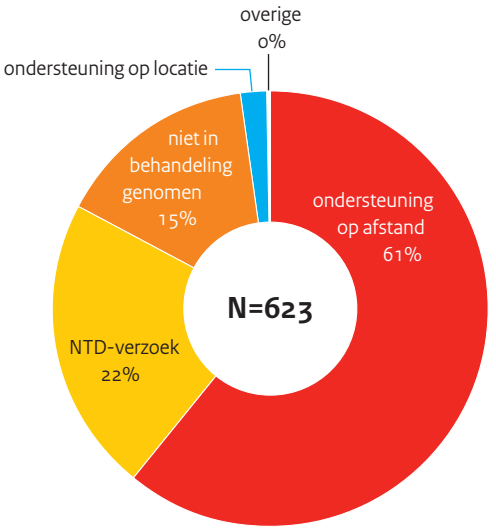
Figuur 16 **Afgehandelde incidenten per categorie**



Bron: NCSC

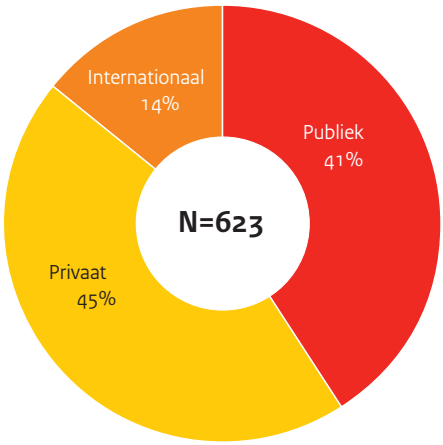
v https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

Figuur 17 **Afgehandelde incidenten per afhandeling**



Bron: NCSC

Figuur 18 **Afgehandelde incidenten per maand per type organisatie**



Bron: NCSC

Vergeleken met de verdeling van incidenten in de vorige rapportageperiode, zien we een toename in misbruik van kwetsbaarheden die ten kosten gaat van malware-incidenten. De toename kan deels worden verklaard door het grote aantal RD-meldingen die binnen deze categorie vallen. Verder worden steeds meer malwaremeldingen geautomatiseerd waardoor ze niet meer worden meegeteld als incidenten maar als geautomatiseerde controles.

De verdeling incidenten per afhandeling wordt in figuur 17 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 61 procent van alle incidenten levert het NCSC ondersteuning op afstand. Bij 22 procent van alle incidenten heeft het NCSC een 'notice-and-take-down' (NTD)-verzoek uitgevoerd. Dit gebeurt bijvoorbeeld als een malafide website 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. In enkele gevallen (2 procent) heeft het NCSC ondersteuning op locatie geleverd. Deze verhoudingen zijn in grote lijnen hetzelfde als in de vorige rapportageperiode.

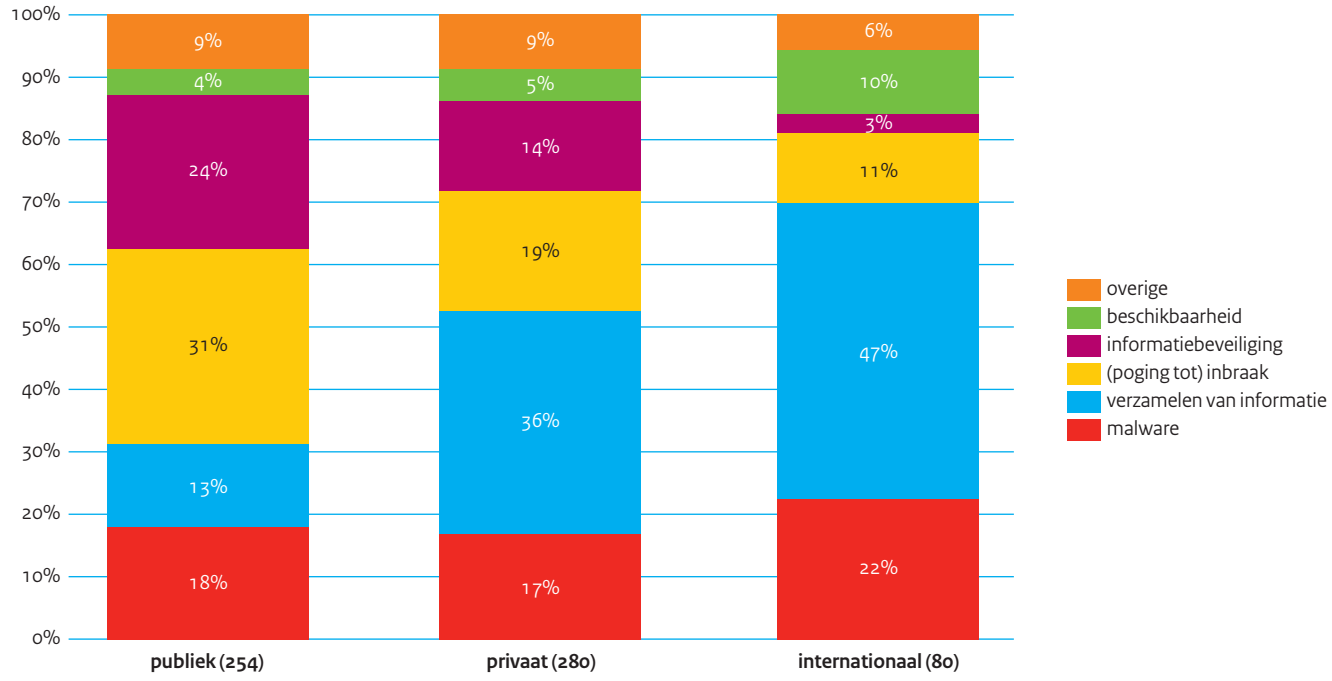
Verdeling incidenten tussen overheid en vitale sectoren

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 18 is te zien wat de verdeling is van het aantal afgehandelde incidenten tussen publieke, private en internationale partijen. In totaal was bij ongeveer 41 procent van de incidenten een publieke organisatie betrokken. Bij 45 procent ging het om een private organisatie. De resterende 14 procent betrof een internationale partij. Een voorbeeld hiervan is het ontvangen van een malwarerapport van de nationale CSIRT-organisatie van een ander land. Ook kan een buitenlandse organisatie het NCSC vragen om een in Nederland gehoste malafide website offline te halen.

Figuur 19 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, ongeacht het type organisatie, is er sprake van malware. Bij incidenten die onder de categorie verzamelen van informatie vallen, is het verschil groter. In 47 procent van alle gevallen waar er een internationale partij betrokken is, gaat het om deze categorie. In de praktijk heeft het merendeel van incidenten uit deze categorie met phishingcampagnes te maken. Uit deze figuur blijkt verder dat (poging tot) inbraak vaker voorkomt (31 procent) bij incidenten in de publieke sector dan bij incidenten waarbij een private (19 procent) of internationale partij (11 procent) betrokken is.

Figuur 19 Incidentencategorieën per type organisatie



Bron: NCSC

Een dergelijke verdeling is ook te zien bij incidenten die met 'informatiebeveiliging' te maken hebben. Zulke incidenten hebben vaak te maken met ongeautoriseerde toegang tot gevoelige informatie of systemen. Een voorbeeld hiervan is het melden van een websitekwetsbaarheid die een aanvaller in staat zou kunnen stellen om een klantenbestand in te zien. Bij incidenten waar er sprake is van een aanval op de beschikbaarheid van een organisatie is er een duidelijker verschil tussen internationale organisaties (10 procent) en de rest (4 tot 5 procent).

Bijlage 2 Sectoraal beeld cybersecurity

Bij het opstellen van het CSBN zijn er gesprekken gevoerd met vertegenwoordigers van Nederlandse organisaties binnen de vitale infrastructuur en andere sectoren. Deze gesprekken hebben geholpen de analyses in dit CSBN te richten en inzichten te onderbouwen. Deze bijlage geeft het beeld weer dat deze vertegenwoordigers schetsten tijdens de gesprekken.

Sector	Manifestaties	Dreigingen: actoren
Drinkwatervoorziening	De drinkwatersector heeft het afgelopen jaar te maken gehad met ransomwarebesmettingen en phishingaanvallen in de kantoorautomatiseringsomgeving.	De drinkwatersector neemt vooral de dreiging van beroepscriminelen waar, die gericht zijn op financieel gewin.
Energie	Het afgelopen jaar heeft de sector veel te maken gehad met ransomwarebesmettingen. Daarnaast zijn datalekken opgetreden.	Beroepscriminelen vormden de belangrijkste dreiging.
Financiële sector	De sector heeft primair te maken gehad met fraude met opgestuurde passen. Beperkt hebben banken last gehad van succesvolle phishingaanvallen. DDoS-aanvallen komen voor, maar raken de sector niet hard.	Beroepscriminelen zijn voor de sector de belangrijkste dreiging, vanwege het financieel gewin dat zij nastreven. Mogelijk vormen ook andere actoren een dreiging, zoals scriptkiddies in geval van DDoS-aanvallen, maar het is onduidelijk door wie die aanvallen uitgevoerd worden.

Dreigingen: middelen	Weerbaarheid	Belangen
Bij een aantal cybercampagnes zijn (vertrouwde) e-mailadressen van leveranciers misbruikt om gebruikers gegevens afhandig te maken (phishing) of te besmetten met ransomware.	Slechte kennis van security bij leveranciers leidt soms tot een verminderde weerbaarheid. Grote (cloud)leveranciers kunnen het risico verkleinen mits voldoende kennis aanwezig is. Op technisch vlak worden meer maatregelen genomen en er is meer aandacht voor detectie en preventie.	De drinkwatervoorziening is van groot belang voor de volksgezondheid en voor het functioneren van de samenleving. Uitval leidt tot sociaal-maatschappelijke ontwrichting. Deze belangen zijn stabiel.
De energiesector heeft veel te maken met pogingen tot CxO-fraude, verspreiding van ransomware en phishingaanvallen. Daarnaast ziet de sector de ontwikkeling van ransomware voor industriële systemen (zoals PLC's) als (toekomstige) dreiging.	De afhankelijkheid van leveranciers wordt als risico gezien, het gevoel bestaat dat de weerbaarheid daardoor lager is. Gezamenlijk wordt er gewerkt aan beleid voor beveiliging van industriële systemen, zoals monitoring en netwerksegmentering.	Ontwikkelingen op het gebied van big data (binnen en buiten de energiesector) hebben als belang brede beschikbaarheid van data voor analyse, wat vaak strijdig is met andere belangen, zoals die van de personen waarvan data verzameld worden.
Ransomware wordt gedetecteerd, dit lijkt niet specifiek gericht op de financiële sector. Daarnaast komt phishing gericht op informatieverzameling veel voor.	De mogelijkheid voor aanvallers om sms-berichten voor transacties af te vangen worden gezien als kwetsbaarheid, net als de mogelijkheid overlay-apps in te zetten om gegevens van gebruikers af te vangen en mogelijk kunnen manipuleren. Daarnaast kunnen verschillende verwachtingen tussen organisaties en leveranciers zorgen voor een lagere weerbaarheid. Organisaties nemen zelf meer maatregelen, zoals versterkte monitoring, vaker gebruik van het vierogenprincipe en deelname aan de veilige e-mailcoalitie.	De PSD2-richtlijn, waarbij instellingen op verzoek van klanten gegevens moeten gaan delen met derde partijen, is een ontwikkeling die mogelijkheden biedt, maar hierbij worden ook risico's onderkend: het is in het belang van de instelling dat de gegevens ook bij de derde partij veilig zijn. Incidenten kunnen negatief afstralen op de instellingen.

Sector	Manifestaties	Dreigingen: actoren
Keren en beheren oppervlaktewater	De sector heeft te maken gehad met ransomwarebesmettingen bij enkele organisaties, spearphishing op basis van het LinkedIn-datalek, CxO-fraude en een beperkt aantal datalekken.	Naast beroepscriminelen vormen ook ontevreden medewerkers soms een dreiging.
Managed Service Providers	Het afgelopen jaar zijn veel gevallen van CxO-fraude/factuurfraude waargenomen. DDoS-aanvallen op klanten van de sector richten zich naast banken meer op de detailhandel.	Beroepscriminelen zijn aan het professionaliseren. Deze groep valt het meest op door het motief financieel gewin.
Nucleair	Er is een toename zichtbaar in phishingaanvallen. Daarnaast heeft de sector te maken gehad met ransomwarebesmettingen en valse facturen.	Statelijke actoren, beroepscriminelen en interne actoren vormen een dreiging voor de sector.
Rijksoverheid	De sector kampt met DDoS-aanvallen, phishingaanvallen en ransomwarebesmettingen.	Statelijke actoren en beroepscriminelen zijn belangrijke dreigingen voor de Rijksoverheid. Daarnaast vormen interne actoren een (vaak onbewuste) dreiging.
Telecom	De telecomsector blijft te maken hebben met DDoS-aanvallen en CxO-fraude. Daarnaast hebben stroomstoringen ervoor gezorgd dat verstoringen in de dienstverlening zijn opgetreden.	De belangrijkste dreigingen voor de sector worden gevormd door beroepscriminelen, statelijke actoren en frauderende medewerkers van de eigen organisaties of resellers.

Dreigingen: middelen	Weerbaarheid	Belangen
De sector ziet de dreiging van specifieke ransomwarevarianten, malware specifiek voor embedded devices en misbruik van andere partijen als stepping-stone om toegang te verkrijgen.	Er is een sterke afhankelijkheid van andere partijen, wat de invloed op de weerbaarheid kan beperken. Koppelingen van kantoorautomatisering aan procesautomatisering zorgen voor nieuwe uitdagingen. Binnen de keten is een sectorale CERT opgericht. Op technisch vlak wordt er microsegmentering toegepast en worden maatregelen genomen op het gebied van asset management en whitelisting.	Vergaande digitalisering en de noodzaak directer te communiceren met burgers zorgt voor uitdagingen. Koppelingen tussen procesautomatisering en kantoorautomatisering vraagt om gedegen maatregelen.
Bankwebsites worden nagebouwd om phishingacties te laten slagen. Middelen zijn gemakkelijk beschikbaar voor onder andere hacktivisten, deze middelen zijn goedkoper en toegankelijker geworden. Er zijn veel partijen die kleine DDoS-aanvallen kunnen uitvoeren, en een aantal partijen dat grote aanvallen kan uitvoeren.	Het gebruik van consumentendiensten voor zakelijke doeleinden,zich manifesterend in de vorm van schaduw-ict, zorgt voor situaties in het bedrijfsleven die niet ondersteund worden en derhalve niet het juiste niveau van beveiliging hebben. Het afhandelen van aanvallen met bepaalde technieken, zoals ransomware en DDoS-aanvallen, is grotendeels business as usual geworden.	Privacyrichtlijnen zorgen voor extra aandacht voor beveiliging bij klanten.
CxO-fraude, valse facturen en ransomware worden gezien als dreiging.	De toenemende wens op afstand te werken en het gebruik van schaduw-ict zorgt soms voor een lage weerbaarheid. Aanscherpen van maatregelen, awareness-sessies en netwerksegmentatie wordt toegepast om de weerbaarheid te vergroten.	Gezien de externe veiligheidsaspecten binnen de sector is nucleaire veiligheid voor de sector van groot belang. ICT is ondersteunend aan het primaire proces.
Er komt veel CxO-fraude voor en phishing op basis van gelekte informatie. Spearphishingaanvallen worden gedaan op basis van goede profielen.	Het patchen van middleware blijft een uitdaging, net als bij appliances zijn kwetsbaarheden hierin vaak onzichtbaar. Https-verkeer zorgt ervoor dat maatregelen genomen moeten worden op endpoints. Privacy weegt soms zwaarder dan beveiliging. Monitoring wordt uitgebreid, waardoor voorheen onbekende problemen duidelijk worden en opgelost kunnen worden.	De afhankelijk van digitale middelen blijft groeien. Ketenafhankelijkheden zorgen ervoor dat derde partijen invulling moeten geven aan beveiligingseisen.
Naast bestaande middelen wordt het internet der dingen gezien als mogelijk middel voor dreigingen. Mensgerichte aanvallen (bijv. door middel van phishing) worden ook steeds meer gezien.	De mens vormt een grote kwetsbaarheid, met name bij phishing en CxO-fraude. De opzet van het SS7-protocol zou de integriteit van het netwerk in gevaar kunnen brengen. Organisaties doen aan kennisdeling op het gebied van cybersecurity. Daarnaast wordt er samengewerkt op het gebied van oefeningen.	Over-the-topdiensten zijn afhankelijk van netwerken van de organisaties.

Sector	Manifestaties	Dreigingen: actoren
Transport (haven, luchtvaart, spoor)	De transportsector heeft te maken gehad met incidenten waarbij bankgegevens gewijzigd zijn, mogelijk na het hacken van een mailserver van een leverancier. Aanvallers hebben zich uitgegeven voor organisaties en daarmee mogelijk geld gestolen. Namen en andere gegevens van medewerkers zijn misbruikt om transacties uit te voeren.	Beroepscriminelen vormen de belangrijkste dreiging voor de sector. Daarnaast vormen politiek gemotiveerde activisten, statelijke actoren en medewerkers een dreiging.
Verzekeraars	Het afgelopen jaar is een sterke toename geconstateerd van ransomware die via (phishing-)e-mail binnenkomt, afkomstig van criminelen. Door het sterke informatieverwerkende karakter is de sector kwetsbaar voor datalekken. Deze worden primair veroorzaakt door onbewust handelen van gebruikers. Daarnaast is de sector beperkt getroffen door DDoS-aanvallen.	De belangrijkste actoren voor verzekeraars zijn beroepscriminelen, die het afgelopen jaar meer uit zijn op financieel gewin dan op vernieling. Menselijke fouten van medewerkers komen voor. Daarnaast vormen fouten van ketenpartners en softwareleveranciers een dreiging.
Zorg	De zorgsector heeft veel te maken met ransomwarebesmettingen, social engineering via telefoon en phishing-e-mails, en malwarebesmettingen via drive-by downloads.	Beroepscriminelen worden gezien als de grootste dreiging. Interne medewerkers blijven een belangrijke groep vormen vanwege de mogelijkheid dat zij (onbewust) informatie lekken.

Dreigingen: middelen	Weerbaarheid	Belangen
Het afgelopen jaar zijn veel aanvallen waargenomen met (spear)phishing met gebruik van gegevens uit datalekken bij derde partijen, pogingen tot defacements, CxO-fraude en ransomware.	De verwevenheid van werk en privé zorgt voor kwetsbaarheden. Daarnaast zijn organisaties sterk afhankelijk van leveranciers voor industriële systemen en IoT: het is onduidelijk hoe het gesteld is met de veiligheid hiervan. De sector neemt veel maatregelen om incidenten te voorkomen, zoals werken aan het tegengaan van phishing uit naam van de organisaties, uit voorzorg blokkeren van online advertenties en coalitievorming richting leveranciers om veiligheid te verbeteren.	Privacyrichtlijnen zorgen aan de ene kant voor aandacht voor cybersecurity, maar leggen het tekort aan resources voor het oplossen van problemen bloot.
De verzekeraars hadden het afgelopen jaar te maken met fraudegevallen, ransomware, phishing, DDoS-aanvallen en malvertising.	In de verzekeringssector blijft schaduw-ict een probleem: clouddiensten worden aangeschaft door individuele medewerkers om eigen werkprocessen te versnellen. Doordat gegevens buiten beheer van de organisatie komen, is vertrouwelijkheid een aandachtspunt. Borging van cybersecurity in agile werkprocessen wordt als uitdaging ervaren.	Binnen de sector zorgt het gebruik van portalen voor informatie-uitwisseling en communicatie voor uitdagingen. Hierbij moet voortdurend het belang tussen klantgemak en veiligheid gemaakt worden. Big data is een uitdaging: het koppelen van informatiebronnen levert efficiënte processen op, waarbij rekening gehouden moet worden met de (aangescherpte) privacywetgeving.
Er wordt de afgelopen tijd meer ransomware waargenomen, zowel gericht als ongericht. Daarnaast komt phishing vaak voor, veelal op basis van publiek bekende gegevens (bijvoorbeeld van openbare websites of uit datasets van eerdere hacks van derde partijen). Er zijn gevallen bekend van pogingen tot CxO-fraude, op basis van bekende gegevens.	De mens blijft een zwakke schakel. Het kunnen achterhalen van de afzender van e-mails is nog steeds niet gemakkelijk mogelijk, wat de organisaties kwetsbaar maakt. Er is weinig grip op veiligheid van e-healthsystemen, hiervoor is men afhankelijk van leveranciers. Ook in geval van clouddiensten bestaat er een grote afhankelijk van de leveranciers. Om de weerbaarheid te vergroten is gestart met Zorg-CERT. Sommige organisaties nemen technische maatregelen zoals het blokkeren van privé-webmail om besmettingen via die weg te voorkomen. Er wordt deelgenomen aan gezamenlijke oefeningen, er worden systemen opgezet om veilig bestanden te delen tussen organisaties.	De zorgsector werkt veel samen, de laatste tijd onder andere met gemeenten. Gemeenten hebben veel zorgtaken gekregen waarvoor zij allerlei informatie opvragen. Soms ontbreekt een wettelijke grondslag voor het opvragen en verwerken van die informatie.

Bijlage 3 Afkortingen- en begrippenlijst

0-day	Zie Zero-daykwetsbaarheid.
Aanval	Het CSBN hanteert als definitie van een digitale aanval een reeks handelingen die inbreuk maakt op informatiesystemen, waarbij de beschikbaarheid, integriteit of vertrouwelijkheid van de informatie wordt aangetast.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
Authenticatie	Authenticatie is het nagaan of een bewijs van identiteit van een gebruiker, computer of applicatie overeenkomt met vooraf vastgelegde echtheidskenmerken.
BGP-hijack	Border Gateway Protocol is een protocol waarmee netwerkapparatuur aan elkaar kan mededelen welke adressen en adresblokken via hen bereikbaar zijn. Een BGP-hijack is een aanvalstechniek waarbij internetverkeer wordt omgeleid door valse BGP-berichten aan naburige netwerkapparatuur te communiceren.
Bitcoin	Munteenheid, zie cryptocurrency.
Bot/Botnet	Een bot is een geïnfecteerde computer die op afstand, met kwade bedoelingen, bestuurd kan worden. Een botnet is een verzameling van dergelijke geïnfecteerde computers die centraal bestuurd kan worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
Certificaat	Een certificaat is een bestand dat fungeert als digitale identificatie van een persoon of systeem. Het bevat ook PKI-sleutels om gegevens tijdens transport te versleutelen. Een bekende toepassing van certificaten zijn websites die met https beveiligd zijn.
Certificaatautoriteit	Een certificaatautoriteit (CA) in een PKI-stelsel is een organisatorisch verband dat wordt vertrouwd om certificaten te maken (genereren), toe te wijzen en in te trekken.
Cloud	Een op internet (de 'wolk') gebaseerd model voor systeemarchitectuur, waarbij software en opslagruimte worden aangeboden als online dienst.
Cryptocurrency	Verzamelnaam voor digitale munteenheden die cryptografische berekeningen gebruiken als echtheidskenmerk en voor transacties. De bekendste en meest gebruikte cryptocurrency is de bitcoin.
CxO-fraude	Vorm van fraude waarbij een crimineel zich voordoet als directeur (CEO of CFO) van een organisatie, specifiek gericht op een financieel medewerker van die organisatie, om een malafide transactie buiten de procedures om te laten plaatsvinden.
Cybercrime	Vorm van criminaliteit gericht op een ICT-systeem of de informatie die door ICT wordt verwerkt.

Cybercrime-as-a-service	Cybercrime-as-a-service is een werkwijze in de ondergrondse economie waarbij criminelen zonder technische kennis gebruik kunnen maken van (betaalde) diensten van anderen om cybercrime te plegen.
Cybercrimineel	Actoren die beroepsmatig cybercrime plegen met hoofdzakelijk geldelijk gewin als doel. Het CSBN onderscheidt de volgende groepen cybercriminelen: • in enge zin, zij die zelf aanvallen plegen (of daarmee dreigen) om geld te verdienen; • criminele digitale dienstverleners, zij die diensten en tools aanbieden waardoor of waarmee anderen digitale aanvallen kunnen uitvoeren; • handelaren in of dienstverleners voor gestolen informatie; • criminelen die digitale aanvallen gebruiken voor traditionele criminaliteit.
Cyberonderzoeker	Actor die op zoek gaat naar kwetsbaarheden en/of inbreekt in ICT-omgevingen om de (te) zwakke beveiliging ervan aan de kaak te stellen.
Cybersecurity	Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.
DANE	DNS-based Authentication of Named Entities is een protocol waarmee certificaten kunnen worden verbonden aan domeinnamen met behulp van DNSSEC
Datalek	Het opzettelijk of onopzettelijk naar buiten komen van vertrouwelijke gegevens.
DDoS	Distributed Denial of Service is een vorm van DoS waarbij een bepaalde dienst (bijvoorbeeld een website) onbereikbaar 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.
DigiD	De digitale identiteit van burgers, waarmee ze zich identificeren en authenticeren op websites van de overheid. Zo weten overheidsinstellingen dat ze echt met een bepaalde burger te maken hebben.
DKIM	DomainKeys Identified Mail is een protocol om legitieme e-mail door de verzendende mailserver digitaal te laten ondertekenen. De eigenaar van het verzendende domein publiceert legitieme 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 (DNS) 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'.
DNSSEC	DNS Security Extensions (DNSSEC) is een uitbreiding op DNS met een extra authenticiteits- en integriteitscontrole.
DoS	Denial of Service is de benaming voor een type aanval die een bepaalde dienst (bijvoorbeeld een website) onbereikbaar maakt voor de gebruikelijke afnemers. Bij websites wordt meestal een DDoS-aanval uitgevoerd.

Dreiging	Het Cybersecuritybeeld Nederland definieert doel en dreiging als volgt: • Het hogere doel (intentie) kan zijn het verstevigen van de concurrentiepositie; politiek/landelijk gewin, maatschappelijke ontwrichting of levensbedreiging. • Dreigingen in het beeld zijn onder andere ingedeeld als: digitale spionage, digitale sabotage, publicatie van vertrouwelijke gegevens, digitale verstoring, cybercrime en indirecte verstoringen.
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
Exploit	Software, gegevens of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om ongewenste functies en/of gedrag te veroorzaken.
Exploitkit	Hulpmiddel van een actor 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 computersystemen. 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: personen of groepen die uit ideologische motieven digitale aanvallen van activistische aard plegen.
ICANN	De Internet Corporation for Assigned Names and Numbers (ICANN) is een organisatie die beheer en onderhoud uitvoert op enkele databases voor de indeling van naamruimte op het internet.
ICS	Industriële controlesystemen zijn meet- en regelsystemen, bijvoorbeeld voor de aansturing van industriële processen of gebouwbeheersystemen. ICS'en verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten.
Identiteitsfraude	Het opzettelijk misbruik maken van de identiteitsgegevens van iemand anders om daarmee fraude te plegen.
Incident	Een incident is een ICT-verstoring in de dienstverlening waardoor de reguliere beschikbaarheid van de dienstverlening geheel of gedeeltelijk verdwijnt en/of het ongeoorloofd openbaren, verkrijgen en/of wijzigen van informatie.
Informatiebeveiliging	Het proces van vaststellen van de vereiste kwaliteit van informatie(systemen) in termen van vertrouwelijkheid, beschikbaarheid, integriteit, onweerlegbaarheid en controleerbaarheid alsook het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende (fysieke, organisatorische en logische) beveiligingsmaatregelen.
Integriteit	Een kwaliteitskenmerk voor gegevens, een object of dienst in het kader van de (informatie)beveiliging. Het is een synoniem voor betrouwbaarheid. Een betrouwbaar gegeven is juist (rechtmatigheid), volledig (niet te veel en niet te weinig), tijdig (op tijd) en geautoriseerd (gemuteerd door een persoon die gerechtigd is de mutatie aan te brengen).
Interne actor	Individueel persoon of groep in een organisatie die daar van binnenuit cybersecurityincidenten veroorzaakt.
IoT	Het internet of things (IoT) is een fenomeen waarbij het internet niet alleen wordt gebruikt om gebruikers toegang te bieden tot websites, e-mail en dergelijke, maar om apparaten aan te sluiten die het internet gebruiken voor functionele communicatie.

Ip	Het internetprotocol (ip) zorgt voor adressering van datapakketten, zodat ze bij het beoogde doel aankomen.
Isac	Een Information Sharing and Analysis Centre (isac) is een samenwerkingsverband tussen organisaties voor het uitwisselen van (dreigings)informatie en gezamenlijke weerbaarheidsverhoging. Het NCSC faciliteert meerdere isacs voor organisaties in de vitale infrastructuur in Nederland.
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.
Malvertising	Het verspreiden van malware door die aan een advertentiebemiddelaar aan te bieden, zodat grote groepen gebruikers worden besmet via legitieme websites.
Malware	Samentrekking van malicious software. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden.
Middel	Een techniek of computerprogramma waarmee een aanvaller misbruik kan maken van bestaande kwetsbaarheden of deze kan vergroten.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NDN	Het Nationaal Detectie Netwerk is een uitwisselingsplatform waarop aangesloten organisaties indicatoren van misbruik met elkaar uitwisselen. De deelnemers kunnen deze indicatoren gebruiken om dreigingen op hun eigen netwerken te signaleren.
Patch	Een patch (letterlijk: pleister) kan bestaan uit reparatiesoftware of kan wijzigingen bevatten die direct in een programma worden doorgevoerd om dat programma te repareren of te verbeteren.
Phishing	Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan worden misbruikt voor bijvoorbeeld creditcardfraude, maar ook voor identiteitsdiefstal.
PKI	Een Public Key Infrastructure (PKI) is een verzameling organisatorische en technische middelen waarmee iemand op een betrouwbare manier een aantal zaken kan regelen, zoals het versleutelen en ondertekenen van informatie en het vaststellen van de identiteit van een andere partij.
Ransomware	Type malware dat systemen en/of informatie daarop blokkeert en alleen tegen betaling van losgeld weer toegankelijk maakt.
RAT	Een Remote Access Tool (soms Remote Access Trojan) wordt gebruikt voor het verkrijgen van toegang tot de computer van een doelwit om die op afstand te kunnen bedienen.
Responsible disclosure	Praktijk van het verantwoord 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.
Scriptkiddie	Actor met beperkte kennis die hulpmiddelen gebruikt die door anderen zijn bedacht en ontwikkeld, voor digitale aanvallen van baldadige aard.
SIDN	Stichting Internet Domeinregistratie Nederland

Spearphishing	Spearphishing is een variant van phishing die zich richt op één persoon, of een zeer beperkte groep personen, 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.
SQL-injectie	Aanvalstechniek waarmee de aanvaller de communicatie tussen een applicatie en de achterliggende database kan beïnvloeden. Het doel is om gegevens in de database te manipuleren of te stelen.
STARTTLS	STARTTLS is een methode om TLS-encryptie toe te voegen aan een bestaand netwerkprotocol, met behoud van terugwaartse compatibiliteit.
Statelijke actor	Er is sprake van een statelijke actor als de actor handelt uit naam van een nationale overheid.
SWIFT	De Society for Worldwide Interbank Financial Telecommunication is een organisatie die internationaal betalingsverkeer faciliteert.
Terrorist	Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolking(sgroepen) angst wil aanjagen of politieke besluitvorming probeert te beïnvloeden, door geweld tegen mensen te gebruiken of ontwrichtende schade aan te richten.
THTC	Team High Tech Crime (politie)
TLS	Transport Layer Security is een protocol voor het opzetten van een beveiligde verbinding tussen twee computersystemen. TLS vormt de basis van het https-protocol.
Tweefactorauthenticatie	Een manier van authentiseren waarvoor twee onafhankelijke bewijzen van identiteit zijn vereist.
Usb	Universal Serial Bus (usb) is een specificatie van een standaard van de communicatie tussen een apparaat, in veel gevallen een computer, en randapparatuur.
Usb-stick	Draagbaar opslagmedium dat via een usb-aansluiting aan computers kan worden gekoppeld.
Vertrouwelijkheid	Een kwaliteitskenmerk van gegevens in het kader van de informatiebeveiliging. Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die ertoe gerechtigd is. Dit wordt vastgesteld door de eigenaar van de gegevens.
Wateringhole	Een wateringhole-aanval is gericht op een plek waar veel beoogde slachtoffers samenkomen. De aanvaller verspreidt zijn exploit of malware via een website die zij regelmatig bezoeken door misbruik te maken van een kwetsbaarheid in deze website of in het contentmanagementsysteem van de website.
Webapplicatie	Het geheel van software, databases en systemen dat betrokken is bij het correct functioneren van een website. De website is het zichtbare gedeelte.
Weerbaarheid	Het vermogen van personen, organisaties of samenlevingen om weerstand te bieden aan negatieve invloeden op de beschikbaarheid, vertrouwelijkheid en/of integriteit van (informatie)systemen en digitale informatie.
Zero-daykwetsbaarheid	Een zero-daykwetsbaarheid is een kwetsbaarheid waarvoor nog geen patch beschikbaar is, omdat de maker van de kwetsbare software nog geen tijd heeft gehad om een patch te maken.

Bijlage 4 Bronnen en referenties

1 https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html, geraadpleegd op 12 mei 2017.
2 http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/, geraadpleegd op 22 maart 2017.
3 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm, geraadpleegd op 26 april 2017
4 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, geraadpleegd op 27 februari 2017.
5 https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html, geraadpleegd op 27 februari 2017.
6 https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html, geraadpleegd op 22 maart 2017.
7 https://www.dni.gov/files/documents/ICA_2017_01.pdf, geraadpleegd op 22 maart 2017
8 http://edition.cnn.com/2017/01/10/politics/comey-republicans-hacked-russia/, geraadpleegd op 19 april 2017.
9 https://www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity, geraadpleegd op 22 maart 2017.
10 http://www.reuters.com/article/us-usa-election-hack-russia-idUSKCN0Z02EK, geraadpleegd 22 maart 2017.
11 https://www.usnews.com/news/world/articles/2016-12-15/russian-officials-deny-vladimir-putins-involvement-in-election-hacking, geraadpleegd op 22 maart 2017.
12 https://guccifer2.wordpress.com/2017/01/12/fake-evidence/, geraadpleegd op 22 maart 2017.
13 https://motherboard.vice.com/en_us/article/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts, geraadpleegd op 20 maart 2017.
14 https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign, geraadpleegd op 20 maart 2017.
15 http://nos.nl/artikel/2111102-russische-hackers-maken-data-democraten-buit.html, geraadpleegd op 19 augustus 2016.
16 http://www.darkreading.com/attacks-breaches/russian-hackers-breach-democrats-to-steal-data-on-trump/d/d-id/1325909, geraadpleegd op 19 augustus 2016.
17 https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cfoo6cb4-316e-11e6-8ff7-7b6c1998b7ao_story.html?hpid=hp_hp-banner-main_dnc-hackers-1145a-banner%3Ahomepage%2Fstory, geraadpleegd op 26 april 2017
18 http://www.nu.nl/internet/4278512/hacker-guccifer-20-claimt-verantwoordelijkeid-hack-democratische-partij.html, geraadpleegd op 19 augustus 2016.
19 http://www.usatoday.com/story/news/politics/2017/03/21/dnc-cyber-attack-russia-highlighted-delayed-response-fbi-chief-says/99455634/, geraadpleegd op 22 maart 2017.
20 https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html, geraadpleegd op 22 maart 2017.
21 https://www.nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html, geraadpleegd op 22 maart 2017.
22 http://www.rtlnieuws.nl/nederland/politiek/rtl-nieuws-toont-aan-zo-makkelijk-is-het-hacken-van-politici, geraadpleegd op 22 februari 2017.
23 https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezichthouders-acm-en-ap-treden-op-tegen-stemwijzernl, geraadpleegd op 27 februari 2017.
24 https://blog.fox-it.com/2017/03/23/turkish-hacktivists-targeting-the-netherlands-high-noise-low-impact/, geraadpleegd op 19 april 2017.
25 https://en.blog.nic.cz/2016/09/01/telnet-is-not-dead-at-least-not-on-smart-devices/, geraadpleegd 1 maart 2017.
26 https://www.bostonglobe.com/business/2016/09/23/cybercrooks-akamai/qOAhvHoohJcmkxIwg5ChKO/story.html, geraadpleegd 1 maart 2017.
27 https://www.ovh.com/us/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac, geraadpleegd op 18 april 2017.
28 https://www.datanyze.com/market-share/dns/Alexa%20top%201K/Alexa%20top%201M, geraadpleegd op 17 maart 2017.

29 Presentatie “Dyn, DDoS, and DNS”, door Andrew Sullivan (Dyn) op ICANN57. Slides & recording op https://schedule.icann.org/event/9npq/tech-day-part-2, geraadpleegd op 17 maart 2017.
30 http://ics.sans.org/blog/2016/12/20/how-do-you-say-ground-hog-day-in-ukrainian, geraadpleegd op 22 maart 2017.
31 http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA, geraadpleegd op 24 maart 2017
32 https://www.slideshare.net/MarinaKrotofil/new-wave-of-attacks-in-ukraine-2016, geraadpleegd op 2 april 2017
33 https://motherboard.vice.com/read/ukrainian-power-station-hacking-december-2016-report, geraadpleegd 22 maart 2017.
34 http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC, geraadpleegd op 22 maart 2017.
35 http://uawire.org/news/ukrenergo-claims-that-blackouts-in-kyiv-could-have-been-caused-by-hackers, geraadpleegd op 8 juni 2017.
36 https://securingtomorrow.mcafee.com/business/shamoon-returns-bigger-badder/, geraadpleegd op 18 mei 2017.
37 Bron: AIVD en MIVD
38 http://www.volkskrant.nl/buitenland/nederlands-duits-defensiebedrijf-gehackt-door-chinezen~a4320398/, geraadpleegd op 4 juli 2016.
39 http://www.reuters.com/article/us-thyssenkrupp-cyber-idUSKBN13XoVW, geraadpleegd op 2 april 2017
40 https://blog.linkedin.com/2016/05/18/protecting-our-members, geraadpleegd op 17 maart 2017.
41 https://blog.fox-it.com/2016/06/07/linkedin-information-used-to-spread-banking-malware-in-the-netherlands/, geraadpleegd op 2 maart 2017.
42 https://www.ncsc.nl/actueel/nieuwsberichten/65-miljoen-wachtwoorden-gelekt.html#ophef, geraadpleegd op 7 juni 2012.
43 https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, geraadpleegd op 2 maart 2017.
44 https://support.apple.com/en-us/HT207130, geraadpleegd op 2 maart 2017.
45 https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws, geraadpleegd 17 maart 2017.
46 https://www.consumentenbond.nl/nieuws/2016/pratende-pop-cayla-slecht-beveiligd, geraadpleegd op 17 maart 2017.
47 https://www.nvb.nl/media/document/000254_od15799-nvb-factsheet-veiligheid-en-fraude-06-06.pdf, geraadpleegd 3 maart 2017.
48 https://twitter.com/KeesVee/status/846613127559106560, geraadpleegd op 27 maart 2017
49 http://nos.nl/artikel/2165391-software-die-computers-gijzelt-aangetroffen-in-tweede-kamer.html, geraadpleegd op 28 maart 2017
50 https://www.fraudehelpdesk.nl/nieuws/ceo-fraudeurs-richten-pijlen-op-nederlandse-bedrijfsleven/, geraadpleegd op 22 maart 2017.
51 Input Fraudehelpdesk voor NCSC Sectoraal Dreigingsbeeld Energiesector kwartaal 4.
52 https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m, geraadpleegd op 20 februari 2017.
53 https://baesystemsai.blogspot.nl/2017/02/lazarus-watering-hole-attacks.html, geraadpleegd op 22 februari 2017.
54 http://www.reuters.com/article/us-italy-cybercrime-idUSKBN14U1K2?il=0, geraadpleegd op 3 maart 2017.
55 https://blog.kaspersky.com/eyepyramid-spyware/13838/, geraadpleegd op 3 maart 2017.
56 http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/, geraadpleegd op 3 maart 2017.
57 https://www.theregister.co.uk/2016/09/07/st_jude_sues_over_hacking_claim/, geraadpleegd op 3 maart 2017.
58 https://threatpost.com/fda-demands-st-jude-take-action-on-medical-device-security/124972/, geraadpleegd op 12 mei 2017.
59 https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2017/ucm552687.htm, geraadpleegd op 12 mei 2017.
60 https://autoriteitpersoonsgegevens.nl/nl/nieuws/1-jaar-meldplicht-datalekken, geraadpleegd 27 februari 2017.
61 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/overzicht_meldingen_datalekken_q1_2017.pdf, geraadpleegd op 12 mei 2017.
62 https://investor.yahoo.net/releasedetail.cfm?ReleaseID=990570, geraadpleegd op 27 februari 2017.
63 https://investor.yahoo.net/releasedetail.cfm?ReleaseID=1004285, geraadpleegd op 27 februari 2017.
64 https://nakedsecurity.sophos.com/2016/12/15/yahoo-breach-ive-closed-my-account-because-it-uses-md5-to-hash-my-password/, geraadpleegd op 27 februari 2017.
65 https://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement, geraadpleegd op 27 februari 2017.
66 http://www.reuters.com/article/us-yahoo-sec-probe-idUSKBN15709O, geraadpleegd op 22 maart 2017.
67 https://www.security.nl/posting/485082/Energiedata+2+miljoen+Nederlandse+huishoudens+gestolen, geraadpleegd 27 februari 2017.
68 https://tweakers.net/nieuws/117829/ook-burgerservicenummers-asml-medewerkers-liggen-op-straat.html, geraadpleegd 27 februari 2017.
69 http://www.nporadio1.nl/onderzoek/2913-autoriteit-persoonsgegevens-wil-strenger-optreden-tegen-datalekken, geraadpleegd 27 februari 2017.
70 http://webwereld.nl/security/97134-bankrovers--kijk-daar--russen, geraadpleegd op 19 mei 2017.
71 https://www.security.nl/posting/479242/Ransomwaremaker+zet+decryptiesleutels+concurrent+online, geraadpleegd op 19 mei 2017.
72 http://www.dutchcowboys.nl/cybercrime/nieuwe-ransomware-laat-slachtoffers-vrij-als-ze-andere-vinden, geraadpleegd op 19 mei 2017.
73 http://www.itpro.co.uk/security/26993/ransomware-is-the-most-profitable-cybercrime, geraadpleegd op 19 mei 2017.
74 https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIMoYoHvmc5g/pubhtml, geraadpleegd op 19 mei 2017.
75 https://www.wired.com/2017/02/ransomware-turns-big-targets-even-bigger-fallout/, geraadpleegd op 19 mei 2017.
76 http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/, geraadpleegd op 19 mei 2017.
77 https://krebsonsecurity.com/2016/11/computer-virus-cripples-uk-hospital-system/, geraadpleegd op 19 mei 2017.

78 http://www.csoonline.com/article/3099852/security/health-care-organizations-114-times-more-likely-to-be-ransomware-victims-than-financial-firms.html, geraadpleegd op 19 mei 2017.
79 http://www.sfexaminer.com/hacked-appears-muni-stations-fare-payment-system-crashes/, geraadpleegd op 19 mei 2017.
80 https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/#more-37060, geraadpleegd op 19 mei 2017.
81 https://motherboard.vice.com/en_us/article/luxury-hotel-goes-analog-to-fight-ransomware-attacks, geraadpleegd op 19 mei 2017.
82 http://www.securityweek.com/simulation-shows-threat-ransomware-attacks-ics, geraadpleegd op 19 mei 2017.
83 Bron: politie (THTC).
84 https://yourcommunity.tescobank.com/t5/News/Message-for-Current-Account-customers/td-p/6599, geraadpleegd op 19 mei 2017.
85 http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q?il=0, geraadpleegd op 19 mei 2017.
86 https://tweakers.net/nieuws/111301/bankaanval-swift-netwerk-gelieerd-aan-sony-hack.html, geraadpleegd op 19 mei 2017.
87 https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0, geraadpleegd op 19 mei 2017.
88 https://www.swift.com/insights/press-releases/swift-introduces-mandatory-customer-security-requirements-and-an-associated-assurance-framework, geraadpleegd op 3 maart 2017.
89 https://www.swift.com/news-events/news/swift-launches-new-anti-fraud-payment-control-service-for-customers, geraadpleegd op 19 mei 2017.
90 https://www.theregister.co.uk/2016/11/29/liechtenstein_bank_breaches/, geraadpleegd op 19 mei 2017.
91 Volgens het ministerie van Buitenlandse Zaken waren in Saoedi-Arabië ruim 9000 computers geïnfecteerd.
92 Zie bijvoorbeeld 'Western Countries | Understanding pro-IS hacking capabilities', Risk Advisory, September 27 2016 (https://news.riskadvisory.net/2016/27/western-countries-understanding-pro-is-hacking-capabilities/), geraadpleegd op 19 mei 2017.
93 'United Cyber Caliphate Maken Threats in "Message to America," Claims DDoS Attacks', Site Intelligence Group, 27 december 2016.
94 'Pro-IS Hacking Group CCTA Identifies German Pilot to Kill', Site Intelligence Group, 14 maart 2017.
95 Zie hiervoor bijvoorbeeld 'Western Countries | Understanding pro-IS hacking capabilities', Risk Advisory, September 27 2016 (https://news.riskadvisory.net/2016/27/western-countries-understanding-pro-is-hacking-capabilities/), geraadpleegd op 19 mei 2017.
96 'UCC Announces Merger with Cyber Kahilafah, Claims "Kill Lists" arte Forthcoming', Site Intelligence Group, 24 December 2016.
97 'UCC Calls on Muslim Hackers to Join its Ranks Against "Disbelievers"', Site Intelligence Group, 10 March 2017.
98 'Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes', ICSR & EY, London, 2017.
99 'Don't panic over cyber-terrorism: Daesh-bags still at script kiddie level', The Register, 16 februari 2017.
100 http://nos.nl/artikel/2163055-turkse-hack-was-waarschijnlijk-online-vandalisme.html, geraadpleegd op 19 mei 2017.
101 http://www.elsevier.nl/nederland/achtergrond/2017/03/turkse-hackers-openen-aanval-op-nederlandse-sites-470305/, geraadpleegd op 19 mei 2017.
102 http://tuoitrenews.vn/society/36243/alleged-chinese-hackers-compromise-hanoi-airport-system-vietnam-airlines-website, geraadpleegd op 19 mei 2017.
103 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, geraadpleegd op 19 mei 2017.
104 http://www.cbsnews.com/news/new-world-hackers-claims-responsibility-internet-disruption-cyberattack/, geraadpleegd op 19 mei 2017.
105 https://www.theregister.co.uk/2017/03/28/congress_approves_sale_of_internet_histories/, geraadpleegd op 2 april 2017
106 'Consumentenbond hekelt beveiliging gezondheidswebsites', Security.nl, 20 januari 2017, 'Autoriteit Persoonsgegevens tikt stemwijzers op de vingers', Security.nl, 17 februari 2017, 'Smart-tv's Sony en Panasonic volgen standaard kijkgedrag', Security.nl, 19 december 2017, 'AP wijst fabrikant Philips smart-tv's op privacyregels bij reclame', Security.nl, 26 januari 2017, 'Toezichthouders willen opheldering WhatsApp over datadelen', Security.nl, 19 december 2016, , 'Franse privacywaakhond heeft kritiek op Windows 10', NOS.nl, 21 juli 2016.
107 http://nos.nl/artikel/2133893-internet-der-dingen-wachten-tot-er-een-ramp-gebeurt.html, geraadpleegd op 19 mei 2017.
108 http://www.networkworld.com/article/3118759/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html, geraadpleegd op 19 mei 2017.
109 https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, geraadpleegd op 19 mei 2017.
110 http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html, geraadpleegd op 19 mei 2017.
111 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, geraadpleegd op 19 mei 2017.
112 https://www.grahamcluley.com/nyadrop-exploiting-iot-insecurity-infect-devices-malware/, geraadpleegd op 19 mei 2017.
113 https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/, geraadpleegd op 19 mei 2017.
114 https://www.theregister.co.uk/2016/10/13/sshowdown_botnet/, geraadpleegd op 19 mei 2017.
115 https://www.ietf.org/blog/2016/07/patching-the-internet-of-things-iot-software-update-workshop-2016/, geraadpleegd op 19 mei 2017.
116 https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/neustar-2017-worldwide-ddos-attacks-cyber-insights-research-report.pdf, geraadpleegd op 12 mei 2017
117 http://www.securityweek.com/iot-botnets-fuel-ddos-attacks-growth-report, geraadpleegd op 12 mei 2017
118 http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/, geraadpleegd op 12 mei 2017
119 https://www.bleepingcomputer.com/news/security/turkish-hackers-are-playing-a-ddos-for-points-game/, geraadpleegd op 19 mei 2017.
120 http://www.itpro.co.uk/security/26993/ransomware-is-the-most-profitable-cybercrime, geraadpleegd op 19 mei 2017.

121 http://www.emerce.nl/nieuws/ransomware-vorig-jaar-flink-gestegen, geraadpleegd op 19 mei 2017.
122 https://www.security.nl/posting/469515/Ransomware+vraagt+losgeld+in+iTunes-cadeaubonnen, geraadpleegd op 19 mei 2017.
123 https://www.bleepingcomputer.com/news/security/decrypted-alpha-ransomware-accepts-itunes-gift-cards-as-payment/, geraadpleegd op 6 maart 2017
124 http://www.csoonline.com/article/3099852/security/health-care-organizations-114-times-more-likely-to-be-ransomware-victims-than-financial-firms.html, geraadpleegd op 19 mei 2017.
125 Bron: input vanuit de zorg-isac.
126 http://www.faronics.com/news/blog/server-side-ransomware-rise-heres-beat/, geraadpleegd op 19 mei 2017.
127 https://www.security.nl/posting/499094/MongoDB+waarschuwt+voor+aanvallers+die+databases+gijzelen
128 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-satan-offered-as-ransomware-as-a-service, geraadpleegd op 2 april 2017
129 https://www.recordedfuture.com/karmen-ransomware-variant/, geraadpleegd op 28 april 2017
130 Bron: THTC.
131 Bron: MSS 2016, NLO, NOM, SKO en VINEX
132 http://www.adformatie.nl/sites/default/files/MSS_2016_Rapportage_infographic.pdf, geraadpleegd op 6 maart 2017
133 Bron: politie en Fox-IT.
134 https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv/, geraadpleegd op 19 mei 2017.
135 https://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/, geraadpleegd op 19 mei 2017.
136 https://www.wired.com/2016/12/popcorn-time-ransomware/, geraadpleegd op 19 mei 2017.
137 https://blogs.forcepoint.com/security-labs/merry-cryptmas-cryptxxx-ransomware-offers-christmas-discount, geraadpleegd op 19 mei 2017.
138 https://blog.barkly.com/ransomware-statistics-2016, geraadpleegd op 19 mei 2017.
139 http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704, geraadpleegd op 19 mei 2017.
140 https://www.bnr.nl/nieuws/economie/10305706/phishing-meldingen-overspoelen-fraudehelpdesk, geraadpleegd op 19 mei 2017.
141 https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html, geraadpleegd op 12 mei 2017.
142 https://www.ncsc.nl/actueel/nieuwsberichten/ceo-fraudeurs-richten-pijlen-op-nederlandse-bedrijfsleven.html, geraadpleegd op 19 mei 2017.
143 https://www.nvb.nl/nieuws/2178/fraude-betalingsverkeer-wederom-fors-lager.html, geraadpleegd op 2 april 2017
144 https://www.betaalvereniging.nl/nieuws/fraude-betalingsverkeer-wederom-fors-lager/, geraadpleegd op 15 mei 2017.
145 http://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT, geraadpleegd op 19 mei 2017.
146 http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q?il=0, geraadpleegd op 19 mei 2017.
147 https://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/, geraadpleegd op 22 december 2016
148 https://www.fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html, geraadpleegd op 16 januari 2017
149 https://www.riskiq.com/infographic/riskiqs-2016-malvertising-report/, geraadpleegd op 7 mei 2017
150 https://pagefair.com/downloads/2016/05/2015_report-the_cost_of_ad_blocking.pdf, geraadpleegd op 7 mei 2017
151 https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf, geraadpleegd op 7 mei 2017
152 http://www.nu.nl/internet/4307673/hackersgroep-claimt-nsa-spionagesoftware-hebben-gestolen.html, geraadpleegd op 19 augustus 2016.
153 http://nos.nl/artikel/2126368-de-nsa-is-mogelijk-gehackt-maar-door-wie.html, geraadpleegd op 19 augustus 2016.
154 http://arstechnica.com/security/2017/01/nsa-leaking-shadow-brokers-lob-molotov-cocktail-before-exiting-world-stage/, geraadpleegd op 22 maart 2017.
155 https://wikileaks.org/vault7/darkmatter/, geraadpleegd op 24 maart 2017.
156 https://www.security.nl/posting/506475/WikiLeaks+onthult+hackingtools%2C+informatie+en+malware+van+CIA, geraadpleegd op 22 maart 2017.
157 http://www.usatoday.com/story/news/world/2017/03/09/wikileaks-provide-tech-firms-access-cia-hacking-tools-assange/98946128/, geraadpleegd 22 maart 2017.
158 https://arstechnica.com/security/2017/04/10000-windows-computers-may-be-infected-by-advanced-nsa-backdoor/, geraadpleegd op 13 mei 2017.
159 https://arstechnica.com/security/2017/04/purported-shadow-brokers-odays-were-in-fact-killed-by-mysterious-patch/, geraadpleegd op 13 mei 2017.
160 https://www.theregister.co.uk/2017/05/12/spain_ransomware_outbreak/, geraadpleegd op 13 mei 2017.
161 https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/, geraadpleegd op 13 mei 2017.
162 http://www.bbc.com/news/health-39906019, geraadpleegd op 13 mei 2017.
163 https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC.pdf
164 https://www.forbes.com/sites/davelewis/2014/10/29/internet-of-things-security-vs-time-to-market/#5923ffe215c4

165 https://www.arxan.com/wp-content/uploads/2017/01/2017_Security_IoT_Mobile_Study.pdf
166 Bron: input vanuit de energie-, insurance- en msp-isacs.
167 Bron: input vanuit alle isacs.
168 https://www.security.nl/posting/484543/Chrome+gaat+http-websites+als+%22niet+veilig%22+weergeven, geraadpleegd op 22 februari 2017.
169 https://www.security.nl/posting/500740/Firefox+gaat+alle+http-websites+als+onveilig+weergeven, geraadpleegd op 22 februari 2017.
170 https://pages.nist.gov/800-63-3/, geraadpleegd op 22 februari 2017.
171 https://www.vvdveen.com/publications/BAndroid.pdf, geraadpleegd op 12 mei 2017
172 https://zoek.officielebekendmakingen.nl/kst-798314.pdf, geraadpleegd op 23 februari 2017.
173 https://www.logius.nl/diensten/digid/ontwikkelingen/, geraadpleegd op 24 februari 2017.
174 https://www.idensys.nl/over-idensys-en-het-stelsel/, geraadpleegd op 24 februari 2017 en https://www.digitaleoverheid.nl/dossiers/identificatie-en-authenticatie/, geraadpleegd op 2 mei 2017.
175 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, geraadpleegd op 24 februari 2017.
176 http://www.japantimes.co.jp/news/2016/12/01/business/tech/1-3-million-connected-devices-around-world-infected-viruses-study/, https://www.security.nl/posting/489469/Bijna+500_000+IoT-apparaten+besmet+door+Mirai-malware, https://telekomhilft.telekom.de/t5/Telefonie-Internet/Probleme-an-Telekom-Anschluessen/m-p/2294533#M694126, geraadpleegd op 24 februari 2017.
177 https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/statement-vice-president-ansip-press-conference-mid-term-review-digital-single-market-strategy_en, geraadpleegd op 12 mei 2017
178 https://www.security.nl/posting/493278/D66+wil+verkoopverbod+onveilige+Internet+of+Things-apparaten, geraadpleegd op 24 februari 2017.
179 WODC, J.J. van Berkel, R.L.D. Pool, M. Harbers, J.J. Oerlemans, M.S. Bargh en S.W. van den Braak , (Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen, 2017 (te verschijnen).
180 http://blog.checkpoint.com/2016/08/07/quadrooter/, geraadpleegd op 24 februari 2017.
181 https://www.ncsc.gov.uk/advisory-quadrooter-vulnerability-affecting-android, geraadpleegd op 8 juni 2017.
182 https://www.vusec.net/projects/dedup-est-machina/, geraadpleegd op 24 februari 2017.
183 https://www.vusec.net/projects/flip-feng-shui/, geraadpleegd op 24 februari 2017.
184 https://www.vusec.net/projects/anc/, geraadpleegd op 24 februari 2017.
185 https://www.forumstandaardisatie.nl/nieuws/nederland-zorgt-voor-veilig-e-mailverkeer, geraadpleegd op 24 februari 2017.
186 https://www.forumstandaardisatie.nl/atom/136, geraadpleegd op 24 februari 2017.
187 https://www.forumstandaardisatie.nl/thema/iv-meting, geraadpleegd op 23 mei 2017.
188 https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html, geraadpleegd op 19 mei 2017.
189 https://letsencrypt.org/2017/01/06/le-2016-in-review.html, geraadpleegd op 24 februari 2017.
190 http://www.nu.nl/internet/4399254/plasterk-wil-toch-beveiligde-verbinding-verplichten-alle-overheidssites.html, geraadpleegd op 24 februari 2017.
191 https://www.security.nl/posting/499791/Onderzoeker+waarschuwt+voor+backdoor+in+WhatsApp, geraadpleegd op 24 februari 2017.
192 https://whispersystems.org/blog/there-is-no-whatsapp-backdoor/, geraadpleegd op 22 maart 2017.
193 https://blog.mozilla.org/security/2016/10/24/distrusting-new-wosign-and-startcom-certificates/, geraadpleegd op 3 maart 2017.
194 https://support.apple.com/en-us/HT204132, geraadpleegd op 3 maart 2017.
195 https://security.googleblog.com/2016/10/distrusting-wosign-and-startcom.html, geraadpleegd op 3 maart 2017.
196 https://www.ncsc.nl/actueel/factsheets/factsheet-postkwantumcryptografie.html, geraadpleegd op 12 mei 2017.
197 Bron: input vanuit de energie-, insurance-, transport-, water- en zorg-isacs.
198 Bron: input vanuit de energie-, insurance-, transport- en water-isacs.
199 De economische en maatschappelijke noodzaak van meer cybersecurity, http://www.mailswitch.nl/files/Px187NDcwMDM5MCowLTQ3NTI3MzcyMw==.pdf, geraadpleegd op 24 februari 2017.
200 Rathenau Instituut, Een nooit gelopen race, https://www.rathenau.nl/nl/publicatie/een-nooit-gelopen-race, geraadpleegd op 22 maart 2017.
201 http://rekenkamer.nl/Nieuws_overzicht/Persberichten/2017/05/Te_weinig_bekend_van_resultaten_rijksbeleid_knelpunten_bij_personeel_en_ICT_nog_zorgen_over_Belastingdienst, geraadpleegd op 29 mei 2017.
202 http://www.volkskrant.nl/binnenland/burgemeester-aboutaleb-loopt-onnodig-groot-veiligheidsrisico~a4483405/, geraadpleegd op 29 mei 2017.
203 https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar, geraadpleegd op 28 april 2017.
204 https://www.cybersecurityraad.nl/binaries/20170405_CSR_Handreiking2017_CompleetDEFweb_tcm56-253718.pdf, geraadpleegd op 12 mei 2017.
205 https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections, geraadpleegd op 22 maart 2017.

206 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z01527&did=2017D03236, geraadpleegd op 22 maart 2017.
207 Bron: input vanuit de msp-isac.
208 ENISA Threat Landscape Report 2016, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016, geraadpleegd op 21 februari 2017.
209 Ponemon Institute: The Rise of Ransomware, https://www.carbonite.com/globalassets/files-white-papers/ransomware-report.pdf, geraadpleegd op 21 februari 2017.
210 https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie, geraadpleegd op 24 april 2017.
211 https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/prive/aangifte_doen/praktische_informatie/belastingdienst_en_de_berichtenbox/belastingdienst_en_de_berichtenbox, geraadpleegd op 20 februari 2017.
212 https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2017, geraadpleegd op 12 mei 2017.
213 www.netbeheernederland.nl/smartgrids/, geraadpleegd op 20 februari 2017.
214 https://www.technischweekblad.nl/nieuws/slimme-aardappelen-voor-precisielandbouw/item9986?PageSpeed=noscript, geraadpleegd op 20 februari 2017.
215 https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf, geraadpleegd op 20 februari 2017.
216 http://www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/dnbulletin-2017/dnb352209.jsp, geraadpleegd op 20 februari 2017.
217 https://www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-6juli2016-Risicorapportage-cyberveiligheid-economie.pdf, geraadpleegd op 20 februari 2017.
218 https://www.consumentenbond.nl/nieuws/2016/bodemprocedure-tegen-samsung-van-start, geraadpleegd op 20 februari 2017.
219 https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications, geraadpleegd op 24 april 2017.
220 http://europa.eu/rapid/press-release_IP-17-16_en.htm, geraadpleegd op 22 februari 2017.
221 Zie CSBN 2016, p. 83 over het ongelijke speelveld dat de telecommunicatiesector signaleerde.
222 https://www.mobileworldlive.com/featured-content/home-banner/facebook-vodafone-in-opposition-over-e-privacy-directive/, geraadpleegd op 24 april 2017.
223 https://tweakers.net/nieuws/122729/amerikaanse-senaat-stemt-in-met-verkoop-browsegeschiedenis-door-providers.html, geraadpleegd op 28 maart 2017.
224 http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910, geraadpleegd op 24 april 2017.
225 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679, geraadpleegd op 24 april 2017.
226 https://www.ntia.doc.gov/other-publication/2016/q-and-iana-stewardship-transition-0, geraadpleegd op 24 april 2017.
227 Dit betreft de rapporten de rapporten 'Het internet, een onbegrensde ruimte met beperkte staatsmacht' van de AIV en 'De publieke kern van het internet: naar een buitenlands internetbeleid' van de WRR.
https://www.rijksoverheid.nl/documenten/kamerstukken/2016/08/22/kabinetsreactie-met-kabinetsreactie-het-internet-een-wereldwijde-vrije-ruimte-met-begrensde-staatsmacht-en-het-advies-de-publieke-kern-van-het-internet-naar-een-buitenlands-internetbeleid, geraadpleegd op 22 februari 2017.
228 https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/, geraadpleegd op 24 april 2017.
229 https://www.rijksoverheid.nl/actueel/nieuws/2017/02/12/koenders-lanceert-internationale-cyberstrategie, geraadpleegd op 24 april 2017.
230 https://www.internetconsultatie.nl/telecommunicatie, geraadpleegd op 28 februari 2017.
231 https://www.nrc.nl/nieuws/2017/01/24/overheid-eist-invloed-bij-cyberbeveiliger-fox-it-6382806-a1542772?utm_source=SIM&utm_medium=email&utm_campaign=Gesprekstof&utm_content=&utm_term=20170125, geraadpleegd op 28 februari 2017.
232 https://fd.nl/economie-politiek/1190995/dijsselbloem-elf-van-25-aex-bedrijven-zijn-onvoldoende-beschermd-tegen-buitenlandse-overnames, geraadpleegd op 24 april 2017.
233 https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html, geraadpleegd op 24 april 2017.
234 http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en, geraadpleegd op 28 februari 2017.
235 Zie ook het AIV/CAVV rapport "Digitale oorlogsvoering" uit 2011, http://aiv-advies.nl/download/9fc55422-c96d-4563-9279-f434803coafd.pdf, geraadpleegd op 24 april 2017.
236 https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html, geraadpleegd op 28 februari 2017.
237 https://www.security.nl/posting/505252/Google+onthult+ongepatcht+lek+in+Internet+Explorer+en+Edge, geraadpleegd op 28 februari 2017.
238 https://googleprojectzero.blogspot.nl/2015/02/feedback-and-data-driven-updates-to.html, geraadpleegd op 28 februari 2017.
239 https://techcrunch.com/2017/03/07/is-signal-app-safe-wikileaks/, geraadpleegd op 21 maart 2017.
240 Zie CSBN 2015.

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

Meer informatie
www.nctv.nl
info@nctv.minvenj.nl
@nctv_nl

Juni 2017