Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Cybersecuritybeeld Nederland
CSBN 2016

Cybersecuritybeeld Nederland

CSBN 2016

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 Directie Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

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.

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
- MIVD
- DefCERT
- AIVD
- Politie (Team High Tech Crime)
- Openbaar Ministerie
- Vertegenwoordigers van organisaties in de vitale infrastructuur, leden van de isacs en andere NCSC-partners
- NCTV
- Nationale Beheersorganisatie Internet Providers
- Platform Internetstandaarden
- Bits of Freedom
- Consumentenbond
- 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 beeld.

Inhoud

Beroepscriminelen hebben zich ontwikkeld tot geavanceerde actoren en voeren langdurige en hoogwaardige operaties uit

Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk

Ransomware is gemeengoed en is nog geavanceerder geworden

Advertentienetwerken zijn nog niet in staat gebleken malvertising het hoofd te bieden

Samenvatting

Het Cybersecuritybeeld Nederland (CSBN) 2016 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 2015 tot en met april 2016. Het CSBN wordt jaarlijks door het Nationaal Cyber Security Centrum gepubliceerd en komt tot stand in samenwerking met publieke en private partners.

Statelijke actoren en beroepscriminelen vormden het afgelopen jaar de grootste dreiging voor Nederland op het gebied van cybersecurity. Het afgelopen jaar hebben zij veel incidenten veroorzaakt, of hebben pogingen daartoe gedaan. Ook de dreiging die van deze groepen uitgaat is groot, en is in het afgelopen jaar gegroeid.

Criminelen hebben zich het afgelopen jaar massaal toegelegd op ransomware en de organisatiegraad van criminele campagnes wordt steeds hoger. Organisaties in de samenleving hebben zeer regelmatig te maken met computers en gegevens die ontoegankelijk zijn gemaakt door ransomware. Voor criminelen zijn campagnes met ransomware eenvoudig uit te voeren. Criminelen houden rekening met de koopkracht van slachtoffers: bij besmettingen van (grote) organisaties wordt soms meer losgeld geëist. Daarmee is ransomware de afgelopen jaren gegroeid tot het middel bij uitstek voor beroepscriminelen om geld te verdienen. De klassieke maatregelen van reguliere back-ups en netwerksegmentering kunnen de impact van ransomware-aanvallen beperken. Naast korte acties gericht op snel geld verdienen breiden beroepscriminelen hun methoden uit: **beroepscriminelen hebben zich ontwikkeld tot geavanceerde actoren en voeren langdurige en hoogwaardige operaties uit.** Het afgelopen jaar zijn meerdere langlopende campagnes waargenomen, waarbij gebruik wordt gemaakt van geavanceerde vormen van spearphishing. Hierbij zijn zowel de investeringen als de opbrengsten van de campagnes groter geworden. In het verleden was deze manier van werken het domein van statelijke actoren.

Statelijke actoren hebben het afgelopen jaar veel digitale spionage uitgevoerd op de Nederlandse topsectoren. **Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk.** Naast economische spionage verzamelen buitenlandse inlichtingendiensten actief politieke inlichtingen via digitale weg. De Nederlandse overheid wordt structureel digitaal aangevallen. **Politieke spionage ondermijnt politiek en bestuur en vormt daarmee een bedreiging voor de democratische rechtsorde.** In het buitenland zijn er manifestaties waargenomen van statelijke actoren die sabotage en andere (militaire) cybercapaciteiten hebben ingezet. De dreiging ervan voor Nederland is gestegen. Statelijke actoren hebben, in het buitenland, vaker digitale aanvallen ingezet om hun strategische doeleinden te bereiken, conflicten te beïnvloeden en in enkele gevallen een gewapende strijd te ondersteunen. Genomen cybersecuritymaatregelen kunnen ook beschermen tegen een digitale component van hybride aanvallen.

Encryptie heeft het afgelopen jaar veel aandacht gekregen. Belangen van partijen staan soms recht tegenover elkaar. In de discussie over relevantie van encryptie moeten de belangen van opsporing en nationale veiligheid worden afgewogen tegen de veiligheid van het internet en de privacy van zijn gebruikers. In Nederland heeft het kabinet zijn standpunt over encryptie naar buiten gebracht. Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie. Het kabinet heeft zijn standpunt over encryptie naar de Tweede Kamer gestuurd. **Het kabinet is van mening dat het momenteel niet wenselijk is om wettelijke maatregelen te nemen om ontwikkeling, beschikbaarheid of het gebruik van encryptie te beperken.**

Van terroristen en hacktivisten gaat op het gebied van cybersecurity minder dreiging uit dan van statelijke actoren en beroepscriminelen, maar deze actoren hebben zich het afgelopen jaar wel ontwikkeld. Terroristen hebben de afgelopen periode geen aanslag gepleegd met digitale middelen. Wel genereren zij veel media-aandacht met kleinschalige digitale aanvallen waar weinig kennis of vaardigheden voor nodig zijn. Hacktivisten hebben zich het afgelopen jaar vooral gericht op het online plaatsen van gevoelige bedrijfsinformatie en persoonlijke gegevens.

Cybervandalen en scriptkiddies vormen een groeiende dreiging. Zij kunnen met laagdrempelige hulpmiddelen en tegen lage kosten digitale aanvallen uitvoeren. Denk hierbij aan booterservices voor het uitvoeren van DDoS-aanvallen; het zijn vormen van cybercrime-as-a-service. Deze criminele bedrijfstak heeft zich het afgelopen jaar uitgebreid. Standaardoplossingen worden online aangeboden en continu verbeterd. Kant-en-klare exploitkits worden verhandeld op ondergrondse marktplaatsen. Malware wordt hierbij als dienstverlening aangeboden, inclusief een helpdesk die dag en nacht bereikbaar is. Op mobiele apparaten groeit de hoeveelheid malware sterk. Deze apparaten vormen een interessant doelwit omdat er steeds meer (financiële) activiteiten mee plaatsvinden. Kwetsbaarheden blijven vaak aanwezig omdat updates niet worden geïnstalleerd of omdat er soms geen updates beschikbaar zijn wanneer apparaten een aantal jaar oud zijn.

Net als vorig jaar zijn er het afgelopen jaar veel DDoS-aanvallen waargenomen. Deze aanvallen worden voornamelijk uitgevoerd door criminelen, hacktivisten, cybervandalen en scriptkiddies. Naast het uitvoeren van deze aanvallen en daarmee het platleggen van websites, infrastructuren en systemen worden DDoS-aanvallen ook gebruikt voor afpersing. Vaak zijn dit loze dreigementen gebleken. **Veel organisaties hebben het afgelopen jaar, collectief of op organisatiebasis, maatregelen getroffen tegen DDoS-aanvallen.** Deze maatregelen zijn voor veel aanvallen effectief, maar vereisen investeringen. Private partijen werken collectief aan verschillende initiatieven om DDoS-bescherming eenvoudiger en goedkoper uit te voeren door samen te werken.

Ketenafhankelijkheden en connectiviteit van industriële controlesystemen maken dat de vitale processen in Nederland kwetsbaar zijn. Ketens zijn zo sterk als de zwakste schakel. De vermenging van industriële controlesystemen en kantoorautomatisering brengt naast veel voordelen ook kwetsbaarheden in deze keten met zich mee.

Het mkb neemt, ten opzichte van grotere bedrijven, relatief weinig maatregelen op het gebied van cybersecurity. Dit terwijl een groot deel van de Nederlandse economie wordt gevormd door bedrijven uit het mkb. Lage weerbaarheid van het mkb op het gebied van cybersecurity kan negatieve impact hebben op de Nederlandse economie.

Het up-to-date houden van apparaten en software blijft een uitdaging. Organisaties zijn kwetsbaar omdat updates niet tijdig op systemen worden geïnstalleerd. In organisaties met industriële controlesystemen zijn systemen vaak kwetsbaar en worden updates niet regelmatig uitgevoerd. In deze situaties bestaat de zorg dat updaten kan leiden tot productiviteitsverlies. **Er is in Nederland verbetering mogelijk op het gebied van beschermingsmaatregelen:** bedrijven hebben vaak geen goed beeld van benodigde maatregelen.

Advertentienetwerken zijn nog niet in staat gebleken malvertising het hoofd te bieden. Deze methode van verspreiding van malware blijft populair en is een groeiend probleem dat niet eenvoudig op te lossen is: de manier waarop advertenties realtime worden ingekocht en aan de gebruiker worden gepresenteerd, gebeurt buiten het zicht van website-eigenaren. Advertentienetwerken controleren de inhoud van advertenties momenteel niet volledig. Gecombineerd met het feit dat veel systemen niet voorzien zijn van de laatste updates zorgt dit voor een groot aanvalsoppervlak. **Effectieve bescherming tegen malvertising zonder het verdienmodel van websites te raken vereist fundamentele maatregelen in de manier waarop advertentienetwerken werken.**

De afgelopen jaren hebben verschillende partijen hard gewerkt aan het verminderen van het aantal malafide websites die in Nederland worden gehost. **Hostingproviders, wetenschap en politie hebben het afgelopen jaar samengewerkt aan het terugdringen van zogenaamde bad hosting in Nederland.** Verbetering is zichtbaar, maar er bestaan nog steeds partijen die zich inlaten met bad hosting.

Naast technische kwetsbaarheden, de achilleshiel van digitale veiligheid, blijft ook de mens kwetsbaar. Kwaadwillenden blijven hun pogingen om gebruikers aan te zetten tot actie verbeteren. **Social engineering is nog altijd populair en vooral succesvol wanneer het gaat om gerichte activiteiten via spearphishing. Het overbrengen van generieke vaardigheden om dreigingen te kunnen herkennen en ernaar te handelen is lastig. Campagnes slagen er niet in deze vaardigheid over te brengen.** Campagnes voor het verhogen van het beveiligingsbewustzijn werken vooral wanneer zij gericht zijn op een afgebakend probleem, zoals het regelen van bankzaken via internet.

Het afgelopen jaar is het **Coordinated Vulnerability Disclosure Manifesto** opgesteld. Ondertekenaars van dit manifest onderschrijven het belang van het vulnerability-disclosureproces (responsible disclosure) en waarderen de interactie met onderzoekers en de hackercommunity. In mei 2016 is het manifest door 29 partijen uit binnen- en buitenland ondertekend tijdens de hoogambtelijke bijeenkomst, georganiseerd tijdens het Nederlandse EU-voorzitterschap.

Internetproviders in Nederland zijn het Dutch Continuity Board (DCB) gestart, waarmee gewerkt wordt aan maatregelen om de impact van DDoS-aanvallen op Nederlandse kritieke infrastructuur te beperken en diensten bij verstoring zo snel mogelijk weer beschikbaar te maken. De overheid heeft het afgelopen jaar maatregelen getroffen om digitaal veiliger te worden en om Nederland digitaal veiliger te maken. De Rijksoverheid heeft maatregelen genomen waardoor ontvangers meer zekerheid krijgen over de afzender van e-mail van de overheid. **Het Platform Internetstandaarden heeft de website internet.nl gelanceerd, waarmee gebruikers kunnen controleren of internetverbindingen, websites en e-mail werken met moderne (beveiligings)standaarden.** Ook is de nieuwe Wet bescherming persoonsgegevens op 1 januari 2016 van kracht geworden. **Met de nieuwe wet is de meldplicht datalekken in werking getreden.** Hiermee is iedereen verplicht mogelijke incidenten met persoonsgegevens te melden bij de Autoriteit Persoonsgegevens. De boetes die kunnen worden opgelegd, kunnen het nemen van maatregelen tegen het lekken van deze gegevens aanmoedigen.

Kernbevindingen

De samenvatting geeft een beknopt volledig beeld van belangen, dreigingen en weerbaarheid op het gebied van cybersecurity. Daarnaast zijn opvallende observaties uit de rapportageperiode gevat in vier kernbevindingen. Deze kernbevindingen worden hieronder beschreven.

Beroepscriminelen hebben zich ontwikkeld tot geavanceerde actoren en voeren langdurige en hoogwaardige operaties uit

Campagnes van beroepscriminelen worden steeds geavanceerder. In het verleden waren de digitale aanvallen en bijbehorende campagnes van criminelen vaak van korte duur en gericht op snel geld verdienen door veel partijen te benadelen. Criminelen hebben het afgelopen jaar een aantal campagnes uitgevoerd waarvoor hoge investeringen zijn gedaan en waaruit een hoge organisatiegraad blijkt. Bovendien wordt spearphishing door criminelen steeds verfijnder en daarmee geloofwaardiger. Spearphishing is zo steeds lastiger te bestrijden met beveiligingsbewustzijn. Langdurige campagnes met grote investeringen en geavanceerde spearphishing waren in het verleden het terrein van statelijke actoren.

Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk

Het afgelopen jaar zijn veel digitale aanvallen waargenomen op bedrijven in Nederland, waarbij het motief economische spionage was. Spionage met een economisch oogmerk is schadelijk voor de concurrentiepositie van Nederland. Deze aanvallen richtten zich op het verkrijgen van technologie die zijn marktwaarde soms nog moet bewijzen. Twee derde van de getroffen bedrijven had deze aanvallen niet zelf waargenomen.

Ransomware is gemeengoed en is nog geavanceerder geworden

Het gebruik van ransomware door criminelen is het afgelopen jaar gemeengoed geworden. Besmettingen zijn aan de orde van de dag en raken de gehele samenleving. Waar in het verleden dezelfde prijs betaald moest worden per besmetting, wordt nu een prijs bepaald aan de hand van het type getroffen organisatie. Bovendien is de malware zelf verfijnder: naast bestanden op de lokale schijf worden tegenwoordig ook databases, back-ups en bestanden op netwerkschijven versleuteld.

Advertentienetwerken zijn nog niet in staat gebleken malvertising het hoofd te bieden

Het verspreiden van malware via advertenties op grote websites is een probleem. De advertentienetwerken zijn nog niet in staat gebleken dit probleem het hoofd te bieden. Het brede bereik van advertentienetwerken zorgt, samen met het grote aantal systemen waarop de laatste updates ontbreken, voor een groot aanvalsoppervlak. Beheerders van deze websites en de advertentienetwerken zelf hebben geen volledige controle over de advertenties. Dit zorgt ervoor dat malware zich kan verspreiden. Het volledig blokkeren van advertenties in de browser raakt aan het verdienmodel van website-eigenaren. Om gebruikers te beschermen tegen malvertising zonder alle advertenties te blokkeren zijn fundamentele wijzigingen nodig in de manier waarop deze netwerken werken.

Inzicht in dreigingen en actoren

Tabel 1 geeft inzicht in de dreigingen die de verschillende actoren vormden over de periode mei 2015 tot en met april 2016 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 2015 gegroeid of gekrompen zijn, worden aangegeven met een pijl. De dreiging die uitgaat van cybervandalen en scriptkiddies is gegroeid waar het gaat om verstoring van ICT. Zij hebben veel middelen tot hun beschikking om relatief eenvoudig onder andere DDoS-aanvallen uit te voeren. Diefstal van informatie door deze actoren is een beperkte dreiging voor alle doelwitten. De dreiging van diefstal en publicatie van verkregen gegevens door hacktivisten is gegroeid, terwijl deze dreiging door interne actoren is gekrompen ten opzichte van vorig jaar.

Tabel 1 **Dreigingsmatrix**

	Doelwitten		
Bron van Dreiging	**Overheden**	**Private organisaties**	**Burgers**
Beroepscriminelen	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie	Diefstal en publicatie of verkoop van informatie
	Manipulatie van informatie	Manipulatie van informatie	Manipulatie van informatie
	Verstoring van ICT	Verstoring van ICT	Verstoring van ICT
	Overname van ICT	Overname van ICT	Overname van ICT
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Offensieve cybercapaciteiten	Offensieve cybercapaciteiten	
Terroristen	Verstoring/overname van ICT	Verstoring/overname van ICT	
Cybervandalen en scriptkiddies	Diefstal van informatie	Diefstal van informatie	Diefstal van informatie ↘
	Verstoring van ICT ↗	Verstoring van ICT ↗	
Hacktivisten	Diefstal en publicatie van verkregen informatie ↗	Diefstal en publicatie van verkregen informatie ↗	
	Defacement	Defacement	
	Verstoring van ICT	Verstoring van ICT	
	Overname van ICT	Overname van ICT	
Interne actoren	Diefstal en publicatie of verkoop van verkregen informatie ↘	Diefstal en publicatie of verkoop van verkregen informatie ↘	
	Verstoring van ICT	Verstoring van ICT	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private Organisaties		Diefstal van informatie (bedrijfs-spionage)	Commercieel gebruik, misbruik of 'doorverkopen' van gegevens
Geen actor	Uitval van ICT	Uitval van ICT	Uitval van ICT

↘ ↗ *Verandering ten opzichte van CSBN 2015*			
	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 manifestaties van de dreiging voorgedaan in de rapportageperiode*	*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.*	*Er zijn duidelijke ontwikkelingen die de dreiging opportuun maken.* *OF* *Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft.* *OF* *Incidenten hebben zich voorgedaan in Nederland.*

Inleiding

Jaarlijks publiceert het Nationaal Cyber Security Centrum het Cybersecuritybeeld Nederland. Het CSBN komt tot stand in nauwe samenwerking met een groot aantal partijen, zowel publieke (politie, inlichtingen- en veiligheidsdiensten en het Openbaar Ministerie) en wetenschappelijke organisaties, als private (bedrijven in de vitale processen en partijen vertegenwoordigd in de isacs).

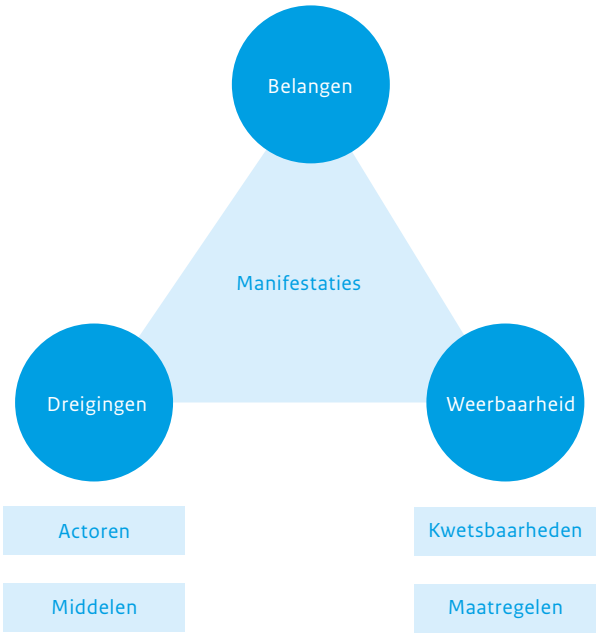
Het CSBN 2016 biedt inzicht in de belangen, dreigingen en weerbaarheid en daarmee samenhangende ontwikkelingen op het gebied van cybersecurity. Het richt zich primair op Nederland over de periode mei 2015 tot en met april 2016. Het is bedoeld voor beleidsmakers bij de overheid en bij de vitale processen, met als doel de digitale weerbaarheid van Nederland te versterken of lopende cybersecurityprogramma's te verbeteren.

Het CSBN is een feitelijke beschrijving met duiding op basis van de inzichten en de expertise van overheidsdiensten en organisaties in vitale processen zelf. Het beschrijft ontwikkelingen in kwalitatieve vorm en geeft, daar waar in betrouwbare vorm beschikbaar, een kwantitatieve onderbouwing en/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 de vorige edities niet of nauwelijks zijn veranderd, zijn niet of beknopt beschreven.

Leeswijzer

De hoofdvragen van het CSBN 2016 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 en weerbaarheid staat model voor de hoofdstukindeling van het CSBN.



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

De dreigingen vallen uiteen in hoofdstukken over actoren en middelen. De capaciteiten, kenmerken en methoden van actoren worden beschreven in hoofdstuk 2. Hoofdstuk 3 beschrijft de middelen die deze actoren gebruiken en de ontwikkelingen daarvan.

De weerbaarheid van Nederland kan de kans dat een dreiging zich manifesteert en de impact van manifestaties beperken. In hoofdstuk 4 is de kwetsbaarheid beschreven, hoofdstuk 5 beschrijft de maatregelen die genomen zijn om die kwetsbaarheden te beperken en weerstand en veerkracht te versterken.

Hoofdstuk 6 gaat in op de Nederlandse belangen en legt de nadruk op de veranderingen in deze belangen het afgelopen jaar, en wat daarvan de impact op cybersecurity is. De bijlagen bieden een overzicht van de door het NCSC afgehandelde incidenten, een beeld van cybersecurity binnen de verschillende sectoren en lichten de gebruikte afkortingen toe.

Ransomware is gemeengoed en besmettingen zijn aan de orde van de dag

1 Manifestaties

Het aantal infecties met ransomware is sinds de vorige rapportageperiode aanzienlijk gestegen. Digitale spionage is ongeëvenaard succesvol en vormt een significante bedreiging voor de nationale veiligheid. Per 1 januari 2016 is de meldplicht datalekken van kracht. De Autoriteit Persoonsgegevens ontving in het eerste kwartaal van 2016 ruim duizend meldingen van datalekken.

Activiteiten gericht op geldelijk gewin

Ransomware is gemeengoed en nog geavanceerder geworden

Ransomware[1] heeft sinds de vorige rapportageperiode een grote vlucht genomen. Organisaties en personen de gehele maatschappij hebben veel te maken met computers en gegevens die ontoegankelijk zijn gemaakt door zulke malware.

Het aantal ransomware-infecties is aanzienlijk gestegen, volgens de vertegenwoordigers uit verschillende sectoren die voor dit CSBN zijn geïnterviewd. Zo wordt de energiesector meerdere keren per maand geconfronteerd met infecties. Deze leiden slechts tot beperkte verstoringen van de kantoorautomatisering en bereiken de procesautomatisering niet. Ook de zorgsector en telecomsector worden geconfronteerd met buitengewone stijgingen in het aantal besmettingen. Managed service providers, die vaak de automatisering voor andere sectoren leveren, stellen vast dat een meerderheid van hun klanten te maken heeft met meer dan één besmetting per jaar.

De politie heeft tijdens de rapportageperiode 124 meldingen en aangiftes ontvangen van besmettingen met ransomware. Bij tenminste 35 van deze meldingen en aangiftes ging het specifiek om cryptoware. Deze aantallen zijn waarschijnlijk slechts een fractie van het totaal aantal incidenten met ransomware. Problemen bij het opnemen van aangiftes, inconsistentie bij de registratie en onbekendheid met de mogelijkheid van melden en aangifte doen, zorgen dat lang niet alle incidenten in deze statistieken terug te vinden zijn. Cijfers van het CBS onderbouwen dit: 11 procent van de Nederlanders was in 2015 slachtoffer van cybercrime; slechts in een klein deel van de gevallen werd aangifte gedaan.[2]

Verschillende sectoren geven aan dat de wijze van infectie met ransomware verandert. Eerder ging het slechts om ongerichte besmettingen. Nu geven de energiesector, organisaties die water keren en beheren en de managed service providers aan dat ze regelmatig geconfronteerd worden met op de persoon of organisatie gerichte phishing-e-mails waarmee aanvallers proberen ransomware te installeren. Andere sectoren, vooral de bancaire sector, zien juist weinig gerichte phishing om ransomwarebesmettingen te bewerkstelligen.

Organisaties merken dat infecties met ransomware nog steeds in belangrijke mate plaatsvinden doordat werknemers hun privé-e-mail op hun werkplek lezen. Hiervoor gebruiken werknemers de webmailfunctionaliteit van hun privé-e-mail. In zo'n e-mail zijn dan bijvoorbeeld links opgenomen naar een website die de computer van de werknemer infecteert.

Verschillende sectoren hebben uiteenlopende ervaringen met de verstorende werking van ransomware. De managed service providers en de energiesector zien infecties met ransomware inmiddels als 'business as usual'. Back-ups zetten zij routinematig terug. Dat leidt tot beperkte verstoringen voor de organisatie. De verzekeringssector geeft aan ransomwarebesmettingen juist als erg verstorend voor de organisatie te ervaren.

Ook de aard van de ransomware waarmee infecties plaatsvinden, is de afgelopen periode veranderd. In deze rapportageperiode zijn manifestaties waargenomen waarbij back-ups en netwerkschijven werden versleuteld. Waar ransomware in eerste instantie de bestanden op de computer van de eindgebruiker versleutelde, zoekt deze nu verder in het netwerk. Voor de gebruiker toegankelijke netwerkschijven worden ook versleuteld, zodat de gevolgen van een infectie voor veel grotere delen van de organisatie voelbaar zijn.

In het buitenland werd de dienstverlening van ziekenhuizen enkele keren onderbroken door ransomware-infecties. In Nederland is dit voor zover bekend nog niet gebeurd.

Een ziekenhuis in het Duitse Neuss werd slachtoffer van ransomware die patiëntgegevens versleutelde, zo werd in februari 2016 bekend.[3] De malware, 'gewone' consumentenransomware, werd verspreid via een e-mailbijlage. Operaties moesten worden uitgesteld en de e-mailcommunicatie werd opgeschort. De Duitse nieuwswebsite RP Online stelt dat vijf andere Duitse ziekenhuizen voor zich hebben gehouden dat zij dezelfde besmetting opliepen.

In het Hollywood Presbyterian Medical Center in Los Angeles verstoorde ransomware in februari 2016 de werking van het computernetwerk.[4] Het ziekenhuis stelt dat er geen toegang is verkregen tot patiëntgegevens. CT-scanners, laboratoriumrobots en medicijnverstrekkende machines zijn wel gesaboteerd. Het ziekenhuis betaalde uiteindelijk het losgeld, 17.000 dollar.[5]

Het lukt lang niet altijd om de daders van een ransomware-besmetting te vinden. In september 2015 slaagde de Nederlandse politie er, in samenwerking met Kaspersky, toch in om twee verdachten van 18 en 22 jaar aan te houden in Amersfoort. Zij zouden wereldwijd tienduizenden computers hebben besmet met Coinvault-ransomware.[6]

Toename van malvertising voedt discussie over noodzaak adblockers

Ook dit jaar kwam het regelmatig voor dat bezoekers van reguliere websites geconfronteerd werden met malware in de getoonde advertenties. Dit komt niet alleen voor in obscure hoeken van het internet, maar ook op zeer populaire Nederlandse websites. De werkwijze bij deze aanvallen suggereert dat de daders meestal criminelen zijn.

In juni 2015 ontdekte Fox-IT dat een aantal nieuwswebsites, waaronder de website van De Telegraaf, malware verspreidden via de getoonde advertenties. De besmette advertenties[7] kwamen van de advertentienetwerken Rubicon en AppNexus. Deze advertenties probeerden met de Angler-exploitkit bezoekers van de websites te infecteren met malware.

Ook in april 2016 detecteerde Fox-IT een malvertisingcampagne op Nederlandse websites. Dit keer ging het om minimaal 288 verschillende websites, waaronder zeer populaire websites als Nu.nl, Buienradar en Marktplaats.[8] Ook in dit geval gebruikten de aanvallers de Angler-exploitkit om gebruikers met malware te infecteren.

Malvertising op populaire Nederlandse websites draagt bij aan de discussie over of het wenselijk is om advertenties te blokkeren via een adblocker. Het groeiende gebruik van adblockers leidde tot het ontstaan van aanbieders van anti-adblockdiensten voor website-eigenaren. Ironisch genoeg werd juist PageFair, een anti-adblock-dienst, in november 2015 gebruikt voor een malvertisingcampagne. Ruim vijfhonderd websites die van deze dienst gebruikmaken, boden anderhalf uur lang malware aan bij het tonen van advertenties.[9]

Innovatieve criminelen stelen financiële middelen en goederen

Banken zijn weerbaarder geworden tegen banking-malware, zo merkt de politie. Man-in-the-browser-aanvallen gericht op eindgebruikers werken niet meer zo goed, mede dankzij fraude-detectie door de banken. Logischerwijs zijn cybercriminelen daarom op zoek gegaan naar andere werkwijzen, middelen en doelwitten. Dit zou kunnen verklaren waarom het gebruik van banking-trojans blijft afnemen en het gebruik van ransomware en RAT's (Remote Access Tools) blijft toenemen. Een voorbeeld zijn aanvallen op banksystemen zelf in plaats van op de rekening-houders. Dit gebeurde bijvoorbeeld bij Carbanak[10] en bij aanvallen op buitenlandse banken waarbij aanvallers toegang verkregen tot systemen waarmee transacties op het SWIFT-netwerk worden ingelegd.

RAT's zijn zeer populair onder criminelen. De politie ontving tijdens de rapportageperiode veertig meldingen en aangiften van incidenten met RAT's. Dat is opmerkelijk, want het inzetten van een RAT is erg arbeidsintensief voor een crimineel.[11] Criminelen gebruiken RAT's om binnen computernetwerken van organisaties te zoeken naar waardevolle systemen en informatie. Ook zijn er online marktplaatsen waar deze activiteiten voor iedereen als dienst in te kopen zijn.

Phishingcampagnes waarbij gebruikers wordt gevraagd om wachtwoorden in te vullen of een bedrag over te maken, komen nog steeds vaak voor. In november 2015 deed een aanvaller zich bijvoorbeeld voor als het Centraal Justitieel Incassobureau (CJIB).[12] De aanvaller verstuurde nepboetes aan personen en manipuleerde hen om zo snel mogelijk te betalen. Slachtoffers dachten geld over te maken naar het CJIB, maar maakten het over naar de crimineel.

Meerdere organisaties worden geconfronteerd met veel gerichtere en geavanceerde social-engineering-aanvallen. Managed service providers geven aan dat hun klanten zeer regelmatig worden geconfronteerd met complexe en in hoge mate gerichte phishing-aanvallen. De succesratio van zulke aanvallen is vrij hoog. Vertegenwoordigers van multinationals en de transportsector vullen aan dat zij een grote stijging zien van het aantal gespoofte e-mails. Hieronder vallen e-mails waarin de aanvaller zich voordoet als de CEO of CFO van het bedrijf. Deze vorm van fraude staat ook wel bekend als CEO-fraude of CFO-fraude. De aanvaller probeert op die manier grote transacties naar zijn rekening te autoriseren.

De transportsector geeft verder aan dat ze waarnemen dat hun personeelsleden door criminele organisaties worden geronseld om informatie uit interne ICT-systemen te verstrekken. Als zij bijvoorbeeld laten weten waar een container vol dure smartphones staat, is het voor de andere criminelen veel eenvoudiger om hun slag te slaan.

In februari 2016 ontvreemdden onbekenden 81 miljoen dollar van de centrale bank van Bangladesh door hun systemen te hacken.[13] Zij zouden toegang verkregen hebben tot het systeem bij de bank om SWIFT-transacties in te leggen. Dit systeem wordt gebruik voor het internationale interbancaire betalingsverkeer. Informatiebeveiligingsbedrijf BAE Systems stelt te hebben ontdekt welke malware is gebruikt bij de aanval.[14] Deze malware zou specifiek de SWIFT Alliance softwaresuite, die door de Bangladesh Bank gebruikt wordt, als doelwit hebben. Reuters meldt dat ook de Tien Phong Bank uit Vietnam eerder tevergeefs doelwit was van de zelfde aanvallers. Daarnaast is de Ecuadoraanse Banco del Austro op dezelfde wijze[15] het slachtoffer geworden.[16]

Bank en managed service provider slaan geavanceerde phishingaanval af [17]

Een Nederlandse bank is in de afgelopen periode geconfronteerd met een zeer vasthoudende en toegewijde phisher. Met behulp van fysieke onderschepping wist deze aanvaller een beperkt aantal (minder dan tien) tokens te verkrijgen van zakelijke klanten van de bank. Zulke tokens worden gebruikt voor het autoriseren van bankoverschrijvingen. Als de aanval geslaagd was, had dit tot aanzienlijke schade kunnen leiden. De bank en de managed service provider waren samen in staat de aanval te ontdekken en de tokens te blokkeren voordat de aanvaller ze kon misbruiken.

Activiteiten gericht op verwerven van informatie

Digitale spionage is ongeëvenaard succesvol

Digitale spionage is vanuit historisch perspectief ongeëvenaard succesvol en vormt een significante bedreiging voor de nationale veiligheid. Volgens de AIVD en MIVD zijn de waargenomen aanvallen slechts het topje van de ijsberg. Het totale aantal gevallen van digitale spionage is vele malen groter. In het afgelopen jaar hebben de inlichtingendiensten veel digitale spionage waargenomen op Nederlandse bedrijven binnen de defensie-industrie en topsectoren als high-tech, chemie, energie, life sciences & health en de watersector. Hierbij is vastgesteld dat de aanvallers op zoek waren naar zeer specialistische technologie en soms zelfs experimentele technologie die zijn marktwaarde nog moet bewijzen.

Dit getuigt van structurele en gedetailleerde aandacht voor innovatie-initiatieven in Nederland. Deze technologieën zijn essentieel voor het huidige en toekomstige verdienmodel van de getroffen bedrijven. Dit illustreert de structurele en omvangrijke digitale spionagedreiging tegen het innovatie- en concurrentievermogen van het Nederlandse bedrijfsleven. Nederlandse inspanningen op het gebied van onderzoek en ontwikkeling zijn een gewild doelwit voor digitale spionage door statelijke actoren. Hiermee kunnen zij hun economieën draaiende houden, maar ook de krijgsmacht versneld moderniseren.

De omvang van de economische schade door digitale spionage op de Nederlandse bedrijven is moeilijk vast te stellen. Ook blijkt dat circa twee derde van de getroffen bedrijven, tot het moment van notificatie door inlichtingendiensten, niet op de hoogte was van deze aanvallen.[18]

Op woensdag 15 juni 2016 publiceerde de Volkskrant een artikel[19] 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.

Statelijke actoren, met name buitenlandse inlichtingendiensten, verzamelen actief digitaal politieke inlichtingen in Nederland. Politieke spionage ondermijnt het gezag van politiek en bestuur en vormt daarmee een bedreiging van de democratische rechtsorde. De Nederlandse overheid wordt structureel digitaal aangevallen. Het doel van de aanvallen is om informatie te bemachtigen over politieke besluitvorming en stellingname, de ontwikkeling en inhoud van politiek-economische plannen, agendapunten van politieke bijeenkomsten en Nederlandse standpunten en tactieken over onderhandelingen op verschillende terreinen.

Naast de Nederlandse overheid worden ook politieke of etnische minderheden in Nederland het slachtoffer van digitale aanvallen. Deze aanvallen worden uitgevoerd door buitenlandse inlichtingendiensten, zoals inlichtingendiensten uit hun land van herkomst. Zeker als deze minderheden in de ogen van hun land van herkomst een bedreiging vormen voor de stabiliteit en legitimiteit van het regime.

Nederland als digitale doorvoerhaven voor statelijke actoren

Nederland beschikt over veel bandbreedte, een van 's werelds grootste internetknooppunten en tal van mogelijkheden voor het huren van servers. Hierdoor is Nederland een voor de hand liggende doorvoerhaven voor digitale aanvallen en speelt het een belangrijke rol in de uitvoering en verspreiding hiervan.

Het afgelopen jaar waren meerdere bedrijven en overheidsinstanties in diverse landen in Europa, het Midden-Oosten, Azië en Noord-Amerika doelwit van digitale spionageaanvallen die onder meer via Nederland liepen.[20] Deze aanvallen richtten zich op politiek-strategische, militair-strategische en economische informatie. Hierdoor spelen Nederlandse ICT-systemen onbewust een rol bij inperking van burgerlijke vrijheden, ontwijking van exportrestricties, schending van intellectuele-eigendomsrechten en diefstal van vertrouwelijke overheidsinformatie.

Onder de slachtoffers bevinden zich (samenwerkingsverbanden tussen) overheidsinstellingen, ministeries en de (defensie-) industrie. Het gaat om digitale aanvallen op kantooromgevingen, mobiele platformen en industriële controlesystemen.

Diefstal van informatie manifesteert zich groot buiten Nederland

Het afgelopen jaar stond in het teken van een aantal gerichte hacks waarbij grote hoeveelheden persoonsgegevens zijn buitgemaakt. Al deze incidenten deden zich voor buiten Nederland. Dat betekent niet dat de Nederlandse samenleving immuun is voor dit soort aanvallen. De zorgsector geeft bijvoorbeeld aan een duidelijke toename te zien in phishing naar inloggegevens. Ze hebben aanwijzingen dat het doel van deze aanvallen financieel van aard is.

Het is nog maar de vraag welk deel van de datalekken zichtbaar is voor de buitenwereld. Angst voor reputatieschade kan organisaties ertoe brengen ontdekte datalekken geheim te houden. De meldplicht datalekken vereist sinds januari 2016 dat alle datalekken van persoonsgegevens gemeld worden bij de Autoriteit Persoonsgegevens. De AP betwijfelt echter of alle lekken wel gemeld worden.[21]

In juni 2015 liet het Amerikaanse Office of Personnel Management (OPM) weten dat het slachtoffer is geworden van een hack. Bij de hack zouden de gegevens van vier miljoen overheidsmedewerkers zijn buitgemaakt.[22] Later die maand werd bekend dat de gegevens van 21,5 miljoen medewerkers en sollicitanten zijn buitgemaakt. Het gaat onder meer om informatie uit veiligheidsonderzoeken van Amerikaans overheidspersoneel. De aanvaller kan zulke gegevens misbruiken voor contraspionage en het onder druk zetten of chanteren van overheidsmedewerkers. Er werd gespeculeerd over de betrokkenheid van China bij de hack, maar de Chinese overheid heeft gezegd dat zij niet verantwoordelijk is voor de aanval.[23] Later heeft de Chinese overheid een aantal hackers gearresteerd die volgens hen de hack hebben gepleegd.[24]

Bij de hack op Ashley Madison, een website voor mensen die een affaire zoeken, werden de persoonsgegevens van meer dan dertig miljoen mensen buitgemaakt.[25] De hackers eisten dat de website zou worden opgeheven en dreigden met publicatie van de gebruikersgegevens. Toen de website niet offline werd gehaald, publiceerden de hackers de gegevens van de 32 miljoen gebruikers, voornamelijk mannen.[26] Vermoedelijk andere aanvallers gebruikten de gegevens in deze dataset vervolgens om betrokkenen te chanteren.[27] Volgens de politie van Toronto heeft de hack twee gebruikers van de website zelfs tot zelfmoord gedreven.[28]

De hack op Ashley Madison was niet het enige ideologisch gemotiveerde lek tijdens deze periode. Van het Italiaanse bedrijf Hacking Team werden na een hack honderden gigabytes aan interne bedrijfsgegevens openbaar gemaakt via BitTorrent en Twitter.[29] Reporters Without Borders heeft Hacking Team in 2012 uitgeroepen tot 'vijand van het internet', omdat het hulpmiddelen zou leveren aan autoritaire regimes om hun bevolking te onderdrukken. De gelekte gegevens zijn breed opgevat als een bevestiging van de eerdere vermoedens over de controversiële klantenkring van Hacking Team. Inmiddels heeft de Italiaanse overheid de brede licentie van Hacking Team voor het exporteren van hun producten ingetrokken.[30]

In juni 2016 verschenen er berichten in de media[31] 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 partijbestuur (het Democratic National Committee). De hackers zouden e-mail- en chatverkeer van de Democraten hebben kunnen lezen. Een beveiligingsbedrijf relateerde de gevonden malware aan twee Russische actoren.[32] Later werd de hack ook geclaimd door een onbekende persoon. Deze probeerde door middel van het vrijgeven van meerdere documenten uit de hack de verantwoordelijkheid op te eisen.[33]

In augustus 2016 beweerden onbekende hackers die zichzelf the Shadow Brokers noemen een Amerikaanse spionagecampagne te hebben gecompromitteerd. Zij zouden door middel van een hack spionagemalware gestolen hebben.[34] Deze malware, hackerstools 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 aangeboden via een publieke veiling.[35] De reeds gepubliceerde bestanden bevatten spionagemalware; hulpmiddelen om verschillende firewalls aan te kunnen vallen (waaronder die van Cisco, Fortigate en Juniper).

Activiteiten gericht op verstoring

DDoS-aanvallen afweren is kostbaar maar steeds effectiever

Ook deze periode waren organisaties frequent het doelwit van DDoS-aanvallen. De managed service providers en organisaties uit de Rijksoverheid zeggen dat het steeds beter mogelijk is om effectieve maatregelen te treffen tegen DDoS-aanvallen van reguliere omvang. Wel zijn de mogelijke maatregelen kostbaar. Dat maakt het online zakendoen duurder. Ook is het onduidelijk hoe lang de wedloop tussen aanvallers en verdedigers in het voordeel van de (kapitaalkrachtige) verdedigers uit zal vallen.

Talloze Nederlandse organisaties zijn in deze periode online onbereikbaar geweest door DDoS-aanvallen. De politie heeft tijdens de rapportageperiode 150 meldingen en aangiften van DDoS-incidenten ontvangen. Scholen zijn regelmatig het slachtoffer van een aanval.[36] De aanval is daarbij meestal gericht tegen een willekeurige pc op de school waarop een scholier actief is, maar raakt de router en internetverbinding van de school.[37] Ook individuele eindgebruikers worden geraakt, bijvoorbeeld on-line gamers die het door hun concurrenten op die wijze onmogelijk wordt gemaakt om de game te spelen. De internetprovider van de gamer kan daar veel last van ondervinden.[38] Deze aanvallen zijn vaak gericht op het verstoren van een enkele verbinding, maar kunnen een uitwerking hebben op alle verbindingen van een provider.

De DNS-servers van internetprovider Ziggo waren op twee opeenvolgende avonden in augustus 2015 het doelwit van een DDoS-aanval. Hierdoor konden bijna twee miljoen Nederlanders tijdelijk geen internet gebruiken. In oktober arresteerde de politie vijf jongens in verband met de DDoS-aanvallen.[39] Vier van hen waren jonger dan achttien, de vijfde was 21 jaar oud.

Het komt regelmatig voor dat Nederlandse organisaties worden afgeperst met DDoS-aanvallen. De aanvaller voert een kleine DDoS-aanval uit en meldt zijn intentie om later een veel grotere aanval uit te voeren. Alleen als de organisatie betaalt, zal de aanval uitblijven. Een bekende groepering die op deze manier afperst is DD4BC (DDoS for bitcoin). In geen van de bij het NCSC bekende Nederlandse gevallen tijdens de rapportageperiode leidde het uitblijven van betaling tot een grotere aanval na de deadline. Managed service providers geven aan dat ze wekelijks te maken hebben met pogingen tot afpersing van hun klanten met DDoS-aanvallen.

Digitale sabotage en beïnvloeding

In Nederland zijn er geen incidenten geweest waarbij statelijke actoren succesvol sabotage uitvoerden. De transportsector geeft wel aan dat er regelmatig incidenten plaatsvinden waarbij ontevreden of net ontslagen medewerkers hun ICT-autorisaties misbruiken om flinke schade aan te richten.

In het buitenland vonden ernstigere vormen van sabotage-aanvallen plaats. De effectiefste was ongetwijfeld de aanval op Oekraïense elektriciteitsbedrijven, waardoor tussen de 700.000 en 1,4 miljoen mensen zonder stroom kwamen te zitten. De daders zijn door een hack binnengedrongen in de systemen van de elektriciteitsbedrijven, waarna ze de werking van het systeem konden dwarsbomen. Na ongeveer zes uur was de stroomvoorziening weer hersteld.

Inlichtingendiensten constateren dat statelijke actoren steeds vaker digitale middelen inzetten om hun strategische doeleinden te bereiken, (internationale) conflicten te beslechten en in sommige gevallen een gewapende strijd te ondersteunen. Voorbeelden van deze trend zijn de conflicten in Oekraïne en Syrië, waarbij dergelijke middelen met regelmaat zijn gebruikt.
Naast in digitale spionage is dit ook terug te zien in digitale sabotage en activiteiten om de publieke opinie te beïnvloeden. Het inzetten van digitale spionage, sabotage of beïnvloeding met deze doeleinden is kosteneffectief. Bovendien biedt het internet mogelijkheden om dergelijke operaties relatief anoniem te doen. Dat bemoeilijkt attributie.

Defacements worden veel gebruikt voor propaganda

Nog altijd worden dagelijks veel websites gedefaced. Daarvoor wordt een kwetsbaarheid in de webapplicatie gebruikt om de inhoud aan te passen die een bezoeker ziet. Over het algemeen is een defacement geen teken dat de kernprocessen van een organisatie digitaal gevaar lopen.

Defacements worden meestal uitgevoerd met een ideologisch motief, of om bepaalde vaardigheden te tonen of op te scheppen. Ideologische defacements worden bijvoorbeeld regelmatig uitgevoerd door sympathisanten van ISIS. Dergelijke aanvallen worden niet gezien als terroristische activiteiten op zich, maar slechts als propaganda. Het zijn natuurlijk wel strafbare feiten.

Manifestaties met onbedoelde schade

Uitval van ICT kan grootschalige invloed hebben

Ook zonder dat mensen systemen aanvallen, kan de werking ervan tekortschieten. Dit gebeurt bijvoorbeeld wanneer een systeem overbelast raakt of een beheerder zich vergist.

In mei 2015 was er een korte storing bij de Amsterdam Internet Exchange (AMS-IX). Hierdoor waren diverse websites en andere diensten die afhankelijk zijn van doorgifte via de AMS-IX tijdelijk niet of slecht bereikbaar. Omdat AMS-IX een van de grootste internetknooppunten ter wereld is waren de gevolgen niet alleen in Nederland merkbaar maar ook daarbuiten.

De storing is veroorzaakt door een menselijke configuratiefout tijdens onderhoudswerkzaamheden.[40]

Ook bij software op nieuwe plaatsen, zoals in thermostaten, kunnen zich storingen voordoen. Dat gebeurt meestal bij apparaten uit het internet der dingen. De slimme thermostaat Nest van Google had in januari 2016 last van een storing.[41] De besturing van de individuele thermostaten bleek afhankelijk van de goede werking van de systemen van Google. Door de storing in deze systemen kon geen enkele Nest-gebruiker de thermostaat bedienen.

Tijdens de aanslagen in Brussel van maart 2016 wilden zoveel mensen bellen en sms'en dat het mobieletelefonienetwerk overbelast raakte. De autoriteiten adviseerden mensen sms of datadiensten te gebruiken en niet te bellen.[42] Ze hoopten dat het netwerk daardoor beschikbaar zou blijven. Het communicatiesysteem van de Belgische politie had ook last van de storing. Agenten besloten daarom tijdelijk gebruik te maken van WhatsApp.[43]

Datalekken ontstaan vaak door vergissingen

Sinds 1 januari 2016 is in Nederland de meldplicht datalekken van kracht. In het kader van de Telecommunicatiewet bestond er voor telecombedrijven al eerder een meldplicht bij de Autoriteit Consument en Markt. De Autoriteit Persoonsgegevens kreeg in het eerste kwartaal van 2016 ruim duizend meldingen van datalekken. Bijna 90 procent van deze meldingen werd gedaan in het kader van de recent gewijzigde Wet bescherming persoonsgegevens. Organisaties zouden deze datalekken dus voor 2016 niet hebben hoeven melden.[44]

Door diverse beveiligingsproblemen konden deze periode de klantenbestanden worden gecompromitteerd van onder andere IT-dienstverlener Invers,[45] huishoudketen Brabantia[46] en twee Nederlandse ziekenhuizen.[47]

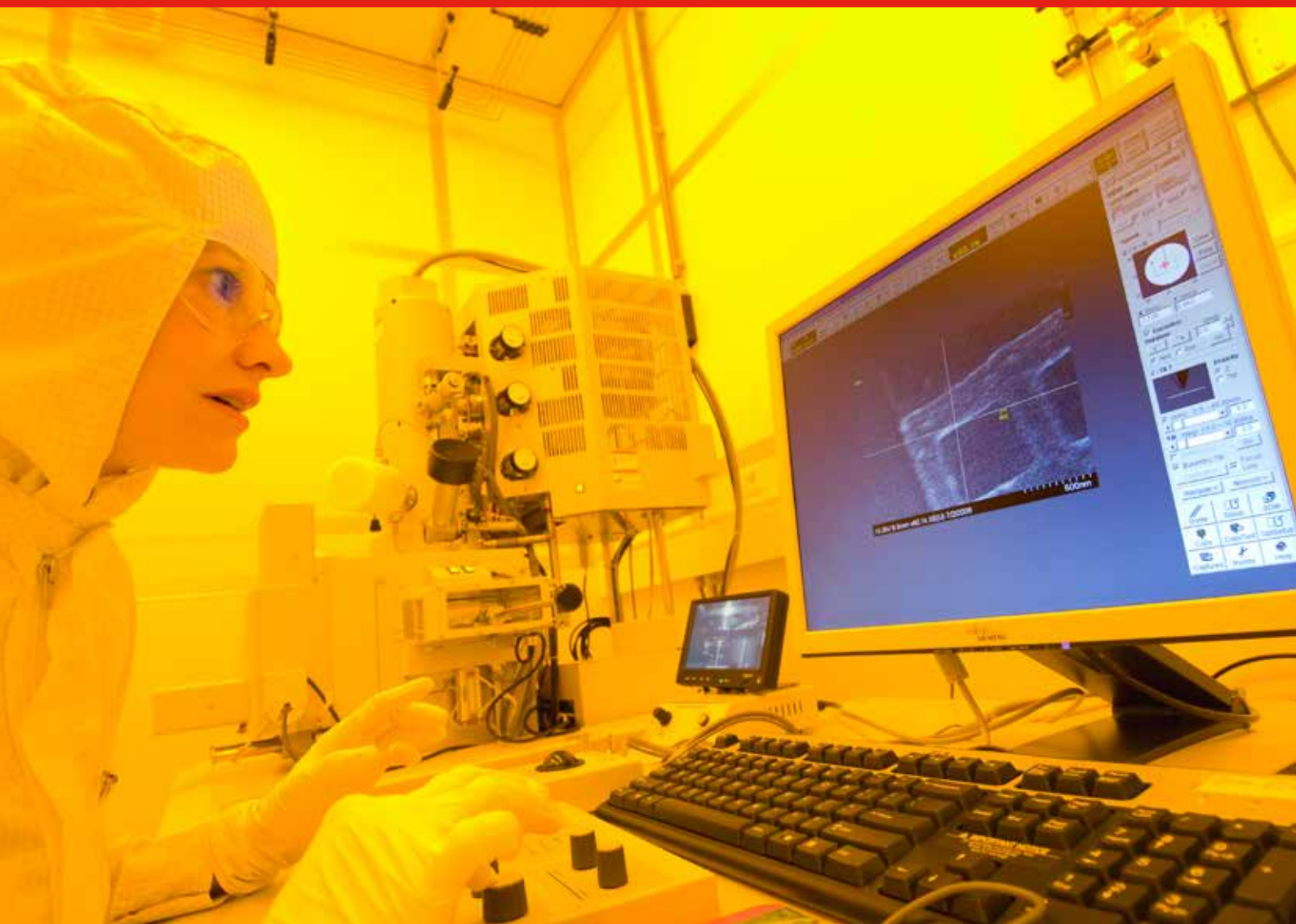
Menselijke fouten en onzorgvuldigheid speelden deze periode ook een rol in gemeentes en de zorgsector. Privégegevens van duizenden inwoners uit Oegstgeest en Rotterdam waren een tijd voor iedereen toegankelijk; een medewerker van de gemeente Rotterdam had vertrouwelijke informatie aan een privécomputer gekoppeld.[48] Een oud-medewerker van een door Oegstgeest gecontracteerde applicatieleverancier had vertrouwelijke informatie op zijn laptop opgeslagen.[49] In december werd een onbeveiligde externe harde schijf ontvreemd van een onderzoeker van het Antoni van Leeuwenhoek ziekenhuis. Hierop stonden patiëntgegevens en medische gegevens.[50]

De zorgsector geeft aan dat datalekken daar aan de orde van de dag zijn. Daarbij gaat het niet alleen om kwaadaardige inbreuken zoals diefstal van apparatuur, maar ook om vergissingen. Een arts stuurt dan bijvoorbeeld een medisch dossier van een patiënt per ongeluk naar een andere patiënt.
Organisaties uit de Rijksoverheid geven zelfs aan dat datalekken meestal het gevolg zijn van menselijke fouten en niet van hackers. Voorbeelden die zij noemen zijn typefouten in een e-mailadres of het bijsluiten van lijsten persoonsgegevens die niet gedeeld mogen worden in e-mails.

Noten

1 In dit rapport wordt cryptoware, tenzij expliciet beschreven, geschaard onder de verzamelnaam ransomware.
2 http://download.cbs.nl/pdf/veiligheidsmonitor-2015.pdf
3 https://www.security.nl/posting/460845/E-mail+besmet+computers+Duits+ziekenhuis+met+ransomware, geraadpleegd op 4 juli 2016.
4 http://www.theregister.co.uk/2016/02/15/ransomware_scum_tear_up_tinsel_town_hospital_demand_record_36m/, geraadpleegd op 4 juli 2016.
5 http://venturebeat.com/2016/02/17/los-angeles-hospital-paid-hackers-17000-ransom-in-bitcoins/, geraadpleegd op 4 juli 2016.
6 https://www.politie.nl/nieuws/2015/september/16/11-cybercriminelen-aangehouden.html, geraadpleegd op 4 juli 2016.
7 https://blog.fox-it.com/2015/06/15/large-malvertising-campaign-targeting-the-netherlands/, geraadpleegd op 4 juli 2016.
8 https://blog.fox-it.com/2016/04/11/large-malvertising-campaign-hits-popular-dutch-websites/, geraadpleegd op 4 juli 2016.
9 Bron: https://blog.pagefair.com/2015/halloween-security-breach/, geraadpleegd op 4 juli 2016.
10 Zie CSBN 2015 voor een uitvoeriger beschrijving van Carbanak.
11 Bron: politie.
12 https://www.security.nl/posting/450641/Politie+waarschuwt+voor+nepmails+van+CJIB, geraadpleegd op 4 juli 2016.
13 http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCNoXI1UO, geraadpleegd op 4 juli 2016.
14 http://baesystemsai.blogspot.nl/2016/04/two-bytes-to-951m.html, geraadpleegd op 4 juli 2016.
15 http://www.reuters.com/article/us-vietnam-cybercrime-idUSKCNoY60EN, geraadpleegd op 4 juli 2016.
16 http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCNoYBoDD, geraadpleegd op 4 juli 2016.
17 Bron: de betrokken managed service provider.
18 Bron: AIVD en MIVD.
19 http://www.volkskrant.nl/buitenland/nederlands-duits-defensiebedrijf-gehackt-door-chinezen~a4320398/, geraadpleegd op 4 juli 2016.
20 Bron: AIVD en MIVD.
21 http://nos.nl/artikel/2104842-privacywaakhond-datalekken-worden-niet-gemeld.html
22 https://www.opm.gov/cybersecurity/cybersecurity-incidents/, geraadpleegd op 11 juli 2016.
23 http://www.welivesecurity.com/2015/12/03/opm-data-breach-not-state-sponsored-says-china/, geraadpleegd op 11 juli 2016.
24 https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html, geraadpleegd op 11 juli 2016.
25 http://nos.nl/artikel/2047968-gegevens-miljoenen-vreemdgangers-gehackt.html, geraadpleegd op 11 juli 2016.
26 http://nos.nl/op3/artikel/2052728-hackers-zetten-32-miljoen-vreemdgangers-online.html, geraadpleegd op 11 juli 2016.
27 http://www.zdnet.be/nieuws/171086/hackers-chanteren-ashley-madison-gebruikers/, geraadpleegd op 11 juli 2016.
28 http://www.volkskrant.nl/buitenland/-twee-zelfmoorden-na-hack-ashley-madison~a4128352/, geraadpleegd op 11 juli 2016.
29 https://www.security.nl/posting/434642/Italiaanse+spyware-ontwikkelaar+HackingTeam+gehackt, geraadpleegd op 11 juli 2016.
30 https://nakedsecurity.sophos.com/2016/04/08/hacking-team-loses-global-license-to-sell-spyware/ , geraadpleegd op 11 juli 2016.
31 http://nos.nl/artikel/2111102-russische-hackers-maken-data-democraten-buit.html, geraadpleegd op 19 augustus 2016.
32 http://www.darkreading.com/attacks-breaches/russian-hackers-breach-democrats-to-steal-data-on-trump/d/d-id/1325909, geraadpleegd op 19 augustus 2016.
33 http://www.nu.nl/internet/4278512/hacker-guccifer-20-claimt-verantwoordelijkeid-hack-democratische-partij.html, geraadpleegd op 19 augustus 2016.
34 http://www.nu.nl/internet/4307673/hackersgroep-claimt-nsa-spionagesoftware-hebben-gestolen.html, geraadpleegd op 19 augustus 2016.
35 http://nos.nl/artikel/2126368-de-nsa-is-mogelijk-gehackt-maar-door-wie.html, geraadpleegd op 19 augustus 2016.
36 http://nos.nl/artikel/2073898-ddos-aanvallen-treffen-scholen-we-haalden-de-boeken-weer-uit-de-kast.html, geraadpleegd op 4 juli 2016.
37 Bron: interview met Michel van Eeten.
38 Bron: politie.
39 https://www.politie.nl/nieuws/2015/oktober/7/11-vijf-jongeren-aangehouden-na-aanvallen-op-ziggo.html, geraadpleegd op 4 juli 2016.
40 https://ams-ix.net/newsitems/194, geraadpleegd op 4 juli 2016.
41 http://tweakers.net/nieuws/107255/nest-kampte-met-grote-storing-wereldwijd.html, geraadpleegd op 4 juli 2016.
42 https://twitter.com/CrisiscenterBE/status/712207222718259200, geraadpleegd op 4 juli 2016.
43 http://www.nieuwsblad.be/cnt/dmf20160326_02205315, geraadpleegd op 4 juli 2016.
44 Bron: Autoriteit Persoonsgegevens.
45 http://www.telegraaf.nl/binnenland/24934680/Invers_lekt_gegevens.html, geraadpleegd op 4 juli 2016.
46 http://www.brabantia.com/nl/statement-beveiligingsincident, geraadpleegd op 4 juli 2016.
47 https://www.security.nl/posting/458824/Datalek+bij+drie+ziekenhuizen+treft+ruim+158_000+pati%C3%ABnten, geraadpleegd op 4 juli 2016.
48 http://www.rotterdam.nl/persoonsgegevens, geraadpleegd op 4 juli 2016.
49 https://www.oegstgeest.nl/fileadmin/redacteuren/20160309_Vragen_en_antwoorden_DEF_tbv_website.pdf, geraadpleegd op 4 juli 2016.
50 http://www.avl.nl/topmenu/over-avl/nieuws/persbericht-externe-harde-schijf-onderzoeker-antoni-van-leeuwenhoek-ontvreemd/, geraadpleegd op 4 juli 2016.

Beroepscriminelen hebben hun vaardigheden ontwikkeld en zijn in staat geavanceerde campagnes uit te voeren



2 Dreigingen: Actoren

Beroepscriminelen en statelijke actoren vormen nog steeds de grootste dreiging voor de Nederlandse digitale veiligheid. De aanvalsvectoren van deze partijen bleven in de afgelopen periode op hoofdlijnen vaak hetzelfde ten opzichte van voorgaande jaren. In de toekomst blijven criminelen ransomware als verdienmodel verder uitbreiden en gerichter inzetten. Het gericht verzamelen van persoonlijke gegevens zonder toestemming van de eigenaar is voor verschillende actoren een steeds aantrekkelijker scenario. Ook wordt het voor kwaadwillenden (zonder specifieke kennis en vaardigheden) steeds eenvoudiger digitale aanvallen uit te voeren. Zij kunnen hierbij gebruikmaken van laagdrempelige hulpmiddelen en betaalbare vormen van cybercrime-as-a-service.

Dit hoofdstuk gaat in op actoren die de betrouwbaarheid en de beveiliging van informatie(systemen) aantasten, hun capaciteiten en de ontwikkelingen op dit vlak.

Beroepscriminelen

Criminele actoren vormen op diverse manieren een grote dreiging voor de Nederlandse digitale veiligheid. Zij hebben grote impact op zowel particulieren als organisaties en de Nederlandse overheid. Het doel van beroepscriminelen is financieel gewin. Dit verkrijgen zij door het plegen van digitale aanvallen of door het dreigen met digitale aanvallen (afpersing).

De afgelopen periode hebben criminelen laten zien in staat te zijn tot geavanceerde campagnes die een hoge organisatiegraad vereisen. Campagnes als Carbanak en de aanvallen op banken met als doel het verkrijgen van toegang tot systemen waarmee SWIFT- transacties ingelegd worden, laten zien dat beroepscriminelen zich tegenwoordig ook richten op een aanpak waarin een langdurige en grootschalige campagne opgezet wordt. Met dergelijke campagnes verdienen criminelen op de middellange termijn meer geld dan met kortere acties. In het verleden werden activiteiten met een dergelijke organisatiegraad alleen gezien bij statelijke actoren.

In april 2016 haalden de politie en het OM een groot versleuteld communicatienetwerk uit de lucht en namen computers in beslag van het bedrijf dat telefoons en bijbehorende dienstverlening leverde om versleuteld via berichten te kunnen communiceren, zogenaamde PGP-telefoons.[51] Deze telefoons zijn door de politie vaak aangetroffen bij opsporingsonderzoeken naar drugshandel en liquidaties. Dit laat zien dat beroepscriminelen technische geavanceerde middelen inzetten om communicatie te beschermen.

Criminelen worden doelbewuster in afpersing

Ook de acties van criminelen worden voor slachtoffers steeds ingrijpender.[52] Criminelen leggen zich bijvoorbeeld steeds vaker toe op digitale afpersing. Ransomware is hiervan het meest voor de hand liggende voorbeeld. Het gebruik van ransomware door criminelen heeft in de vorige rapportageperiode een vlucht genomen in populariteit en heeft zich deze periode onverminderd voortgezet. De digitale aanvalsmethoden voor ransomware worden verfijnder en tactieken om de ransomware op het systeem van het slachtoffer te krijgen worden geraffineerder.

Hoewel de politie de afgelopen periode meer gerichte aanvallen heeft waargenomen, gebruiken criminelen ransomware in Nederland tot nu toe vooral ongericht. Dit betekent dat zij zich niet richten op het versleutelen en het afpersen van specifieke systemen. Zowel particulieren als organisaties worden door deze vorm van afpersing getroffen. Er zijn echter aanwijzingen dat

criminelen ransomware vaker gericht op organisaties inzetten.[53] Soms gebruiken zij hiervoor een aangepaste (hogere) losgeldeis en richten zij zich op kwetsbare doelen die van belang zijn voor de continuïteit, zoals ziekenhuizen en zorginstellingen.[54] Dit is bijvoorbeeld het geval geweest bij een Amerikaans ziekenhuis, dat 40 bitcoins (17.000 USD) aan de aanvallers betaald heeft om de systemen zo snel mogelijk weer operationeel te krijgen.[55] Dit was niet alleen zorgelijk omdat de gegevens van patiënten versleuteld waren, ook medische apparatuur functioneerde niet meer als gevolg van deze aanval.[56]

Criminelen buiten het succesvolle gebruik van ransomware verder uit door de diversiteit van hun doelwitten uit te breiden. Het voorbeeld van het Amerikaanse ziekenhuis laat ook zien dat criminelen daarbij niet alleen standaardsystemen treffen. Ook systemen zoals medische apparatuur, databases[57] en zelfs back-up-bestanden[58] kunnen kwetsbaar zijn voor deze aanvallen.

Naast ransomware werden Nederlandse organisaties de afgelopen periode vaker slachtoffer van DDoS-afpersingscampagnes. In deze campagnes worden DDoS-aanvallen door criminelen gebruikt als deel van een afpersingsscenario. Via e-mail dreigen criminelen met een DDoS-aanval tenzij er bitcoins aan de verzender worden betaald. Niet altijd worden de DDoS-aanvallen ook daadwerkelijk uitgevoerd.[59] DD4BC[60] en het Armada Collectief[61] zijn bekende criminele groeperingen die deze werkwijze hanteren, hoewel er ook aanwijzingen zijn dat andere criminelen van deze namen gebruik maken om het dreigement van een DDoS-aanval kracht bij te zetten.[62 63]

Verder werd in de rapportageperiode ook waargenomen dat criminelen particulieren afpersen met uit digitale aanvallen gestolen data. Dit is bijvoorbeeld gebeurd na de hack op het klantenbestand van de site Ashley Madison.[64] Personen uit het klantenbestand werden vervolgens door de criminelen benaderd.[65] Ook worden soms organisaties afgeperst met gestolen data afkomstig uit digitale aanvallen.[66] In de afgelopen periode dreigde de criminele groep Rex Mundi bijvoorbeeld de klantenbestanden van verschillende Nederlandse en Belgische organisaties online te zetten als de betreffende organisaties niet zouden betalen.[67 68]

Bestaande verdienmodellen blijven in zwang onder criminelen

Terwijl er een groep beroepscriminelen ontstaat die met een hoge organisatiegraad geavanceerde campagnes uitvoert, blijven bestaande verdienmodellen in gebruik.[69] Dit is zowel bij ransomware waar te nemen als ook bij andere soorten criminele malware, zoals banking malware. Het gebruik van deze laatste vorm van malware neemt in Nederland af.[70]

Soms wordt broncode van malware (bedoeld of onbedoeld) openbaar, waardoor het voor criminelen mogelijk wordt deze naar eigen wens aan te passen. Het gevolg is dat er snel meerdere versies van de originele malware verschijnen.[71 72] Daarbij komt het vaker voor dat criminelen hun malware specifiek kunnen aanpassen voor gerichte aanvallen: zij modelleren hun aanvallen dus vaker naar hun beoogde slachtoffer.[73]

Het niveau van expertise en vaardigheden van criminelen loopt sterk uiteen. Er zijn specialisten die worden gekenmerkt door een hoge mate van professionaliteit en innoverend vermogen. Door de professionele dienstensector die er afgelopen jaren voor digitale criminaliteit is ontstaan, is er ook een steeds groter wordende groep criminelen actief met een relatief laag niveau van expertise en vaardigheden.[74] Het CSBN 2015 en 2014 stelden al dat het voor een crimineel al lang niet meer nodig is om digitale vaardigheden te bezitten om gebruik te kunnen maken van digitale aanvallen.

Dat cybercrime-as-a-service steeds professioneler en klantvriendelijker wordt, is de afgelopen periode nogmaals duidelijk geworden door het verschijnen van verschillende soorten ransomware-as-a-service,[75 76] instructievideo's voor malware op YouTube[77] en code voor ransomware op GitHub.[78] Dit draagt bij aan het gebruikersgemak waarmee criminelen zonder specifieke kennis en vaardigheden malware en ransomware kunnen inzetten tegen hun slachtoffers.

Opsporing van criminelen blijft een uitdaging

Nederlandse hosting blijft onverminderd populair onder cybercriminelen. In 2015 hebben de politie en het Openbaar Ministerie het aantal ip-adressen waar zij op basis van internationale rechtshulpverzoeken op moet acteren zien groeien van 214 in 2014 naar 383 in 2015.[79] Ook winnen uiteenlopende anonimiseringstechnieken bij criminelen aan populariteit. Hierbij proberen zij criminele activiteiten, communicatie en geldstromen buiten het zicht van opsporingsdiensten te houden. Criminele fora worden vaak achter proxies en DDoS-beschermingsdiensten geplaatst, om de daadwerkelijke locatie van servers te verbergen.[80] De politie constateert dat command & control-servers die gebruikt worden bij bijvoorbeeld ransomware-campagnes in het Tor-netwerk geplaatst worden om niet vindbaar te zijn. Daarnaast wordt het gebruik van zogenoemde bitcoinmixers steeds populairder: diensten die bitcoin-tegoeden door wisselen proberen verder te anonimiseren. Zo wordt verhinderd dat de sporen van het virtuele geld, de zenders en de ontvangers van transacties, nog te achterhalen zijn.

In aanvulling daarop kunnen via advertenties op ondergrondse marktplaatsen illegale bitcoinwisselaars worden ingeschakeld om tegen een hoog tarief (8 tot12 procent in plaats van ongeveer 0,5 procent bij bonafide wisselaars) anoniem geld te kunnen opnemen op een afgesproken tijd en plaats. In januari 2016 heeft de FIOD een crimineel netwerk met meerdere bitcoinwisselaars ontmanteld. In maart 2016 heeft de politie ook een bitcoinwisselaar aangehouden voor het op die manier witwassen van waarschijnlijk miljoenen euro's aan bitcoins.

Er is duidelijk een grote, wereldwijde, anonieme markt voor digitale criminaliteit is. Toch neemt de politie daarnaast ook steeds vaker lokaal gevormde, fysieke samenwerkingsverbanden waar. In plaats dat zij alleen op afstand via (anonieme) digitale kanalen

contact met elkaar hebben, ontmoeten en kennen criminelen elkaar bij sommige gerichte operaties wel degelijk. Een bekend voorbeeld is de Dyre-malwarecampagne waarvoor een crimineel samenwerkingsverband bij elkaar ondergebracht was in een kantoorpand in Rusland.[81]

Marktplaatsen voor cybercrime-as-a-service

Standaardoplossingen voor het uitvoeren van cybercrime worden continu doorontwikkeld en doorverkocht. Dit doorverkopen wordt ook wel commodificatie genoemd. Campagnes of operaties worden vaak door gelegenheidscoalities van specialisten uitgevoerd.[82] Grotere en kundige coalities houden daarbij zoveel mogelijk grip op de volledige operatie.[83]

Ondergrondse marktplaatsen worden nog steeds gebruikt om middelen voor het plegen van cybercrime uit te wisselen of te verhandelen.[84] Er wordt gebruikgemaakt van hidden services, om zo opsporing te bemoeilijken.

Diensten die worden aangeboden zijn onder andere kant-en-klare malware, gestolen creditcardgegevens, socialemedia- en e-mailaccountgegevens, DDoS-aanvallen (DDoS-as-a-service), RAT's en online handleidingen voor het plegen van cybercrime.

Betrouwbaarheid en kwaliteit wordt als competitief voordeel gezien. Zo zijn er dienstenaanbieders met een helpdesk die ondersteuning bieden tijdens kantooruren of zelfs 24 uur per dag.[85] Zij geven de garantie dat de geleverde gegevens of producten aan de verwachtingen voldoen. Om oplichting te voorkomen worden er eveneens vertrouwde tussenpersonen ingezet die het geld pas vrijgeven aan de verkoper wanneer de klant heeft aangegeven tevreden te zijn.[86]

De Angler-exploitkit hanteert mogelijk een model waarbij de gebruiker betaalt per succesvolle malware-installatie.[87] Andere exploitkits, zoals Sweet Orange, lijken zowel een abonnementsdienst aan te bieden als de mogelijkheid om de kit voor onbeperkte tijd te kopen.[88] Exploitkits worden soms ook onder voorwaarden verkocht, bijvoorbeeld dat ze alleen voor gerichte aanvallen gebruikt mogen worden en niet voor brede phishingaanvallen.[89] Een andere voorwaarde is dat ze niet ingezet mogen worden in landen waar de dienstverlener onder de radar wil blijven.[90] Ook kan de dienstverlener een deel van de opbrengst eisen, zoals 30 procent bij CTB-locker.[91]

Statelijke actoren

De grootste dreiging in het digitale domein voor de nationale veiligheid komt van statelijke actoren, in het bijzonder van buitenlandse inlichtingendiensten.[92] De Nederlandse overheid, nationale veiligheid en economie worden bedreigd door activiteiten van deze statelijke actoren. Digitale aanvallen zijn inmiddels een volwaardig alternatief voor conventionele (spionage)middelen vanwege de lage kosten, de beperkte afbreukrisico's en de hoge opbrengsten (in hoeveelheid informatie).

De werkwijze neemt in complexiteit toe, aanvallers worden vindingrijker en ontwikkelen steeds betere methodes om het probleem van onderkenning en attributie te voorkomen. De Nederlandse inlichtingen- en veiligheidsdiensten namen in de afgelopen periode structureel omvangrijke spionageaanvallen waar gericht tegen Nederlandse overheidsinstellingen, wetenschappelijke instituten en bedrijven uit topsectoren. Staten benutten ook het militaire potentieel van het digitale domein door offensieve cyberactiviteiten in te zetten. Dit is nog niet specifiek in Nederland waargenomen.[93]

Staten investeren in offensieve cybercapaciteiten

Staten investeren net als voorgaande jaren fors in het ontwikkelen van hun offensieve digitale capaciteiten.[94] Het zijn vaak inlichtingendiensten die deze capaciteiten herbergen en heimelijk inzetten. Staten hebben in toenemende mate digitale aanvallen ingezet om hun strategische doelen te bereiken, (internationale) conflicten te beïnvloeden en in enkele gevallen een gewapende strijd te ondersteunen.

De militaire inzet van digitale capaciteiten, digitale aanvallen met als doel sabotage en manipulatie van beeldvorming, is in toenemende mate een aanvulling op conventionele middelen. Hoewel de manifestatie van dergelijke aanvallen nauwelijks in openbare bronnen verschijnt, moet worden geconstateerd dat sommige staten voorbereidende handelingen verrichten voor het verzamelen van informatie, het beïnvloeden van de draagkracht voor politieke en militaire operaties of het in stand houden van een infrastructuur voor toekomstige operaties. Dit is nog niet waargenomen in Nederland. Zorgwekkend hierbij zijn verkenningen op vitale infrastructuur, het installeren van malware om zich toegang te verschaffen voor toekomstige operaties of investeringen in hackerscollectieven die dergelijke handelingen mogelijk maken.

Staten organiseren hun cybercapaciteiten

De organisatiegraad achter digitale aanvallen van buitenlandse statelijke actoren is vaak groot; de taakverdeling en specialisatie ontwikkelt zich. De Nederlandse inlichtingen- en veiligheidsdiensten hebben bij verschillende aanvallen waargenomen dat diverse actorgroepen betrokken zijn bij de uitvoering van digitale aanvallen. Zo is bij herhaling vastgesteld dat de verschillende fasen van een digitale aanval bij diverse derde partijen zijn belegd. Deze partijen specialiseren zich in behoeftestelling, toolontwikkeling, uitvoering of infrastructuurbeheer.

Ook wordt infiltratie enerzijds en exploratie en exfiltratie anderzijds bij verschillende groepen belegd, ook bij private partijen. De Nederlandse inlichtingen- en veiligheidsdiensten stelden diverse malen vast dat medewerkers van ogenschijnlijk private ICT-bedrijven digitale aanvallen uitvoeren of infrastructuur aanschaffen en beheren in opdracht van buitenlandse overheden. Deze

activiteiten richten zich op Nederlandse overheidsinstellingen, wetenschappelijke instituten en bedrijven uit topsectoren. Deze segmentatie in de opzet en uitvoering van digitale spionage werkt de specialisatie en continuïteit (in de vorm van slagkracht) van digitale aanvallen in de hand.

Terroristen

Van terroristen is op digitaal gebied nog geen concrete dreiging tegen de nationale veiligheid waargenomen. Zij hebben tot nu toe nooit een (dodelijke) aanslag gepleegd met digitale middelen. Wel veroorzaken zij nog altijd maatschappelijke onrust met kleinschalige digitale aanvallen waar weinig kennis of vaardigheden voor nodig zijn. Dit soort aanvallen nam in de afgelopen periode toe.

Geavanceerde digitale capaciteiten van jihadisten manifesteren zich nog niet

De meeste dreiging van terroristen gaat op dit moment uit van jihadisten en ISIS-sympathisanten. Hoewel er in de vorige rapportageperiode werd vastgesteld dat de capaciteiten van jihadisten op digitaal gebied groeiende zijn, heeft zich dat tot nu toe nog niet gemanifesteerd in grootschalige of technisch geavanceerde aanvallen met een terroristisch of jihadistisch motief.

Jihadisten concentreren zich vooral op het verbergen en versleutelen van hun communicatiekanalen. Zij wijzen hun medestanders namelijk vaak op het belang van veiligheidsbewustzijn. Ook ontwikkelen zij nieuwe applicaties en nieuwsfora[95 96 97] om hun boodschap verder te verspreiden. Hierbij lijken zij naar een balans te zoeken tussen veiligheid en rekrutering: in plaats van het volledig verplaatsen van hun communicatie naar ondergrondse kanalen,[98] hebben jihadisten er voor rekruterings- en propagandadoeleinden baat bij dat hun boodschap in enige mate toegankelijk blijft voor geïnteresseerden.[99 100]

Jihadisten claimen geregeld dat het hen gelukt is om via digitale aanvallen gevoelige data te verkrijgen. De gegevens die zij vervolgens openbaar maken, zijn echter in de meeste gevallen nog steeds op het internet terug te vinden,[101] of zijn het resultaat van eenvoudige hacks waar weinig capaciteit en middelen voor nodig zijn.[102] Het gaat hier vooral om gegevens van Amerikaanse soldaten en overheidsmedewerkers,[103 104] maar de afgelopen rapportageperiode publiceerden zij ook lijsten van Europese overheidsmedewerkers,[105 106] waaronder verouderde gegevens over Nederlanders.[107] Jihadisten publiceren vooral gegevens van overheidsmedewerkers met de oproep aan aanhangers deze informatie voor aanslagen te gebruiken. Tot nu toe is het niet voorgekomen dat jihadisten gepubliceerde persoonlijke gegevens gebruikt hebben voor het plegen van aanslagen.

Hoewel jihadisten de financiële middelen en de intentie hebben om digitale aanvallen te plegen, blijkt uit hun eerder uitgevoerde aanvallen dat deze nog niet technisch geavanceerd zijn en weinig kennis en mankracht vergen. Jihadisten proberen externe partijen aan te trekken om kennis en capaciteit op het gebied van digitale aanvallen te vergroten.[108]

Incidenten of aanslagen vormen vaak een katalysator voor online defacements vanuit verschillende partijen, zoals de digitale reacties op de aanslagen in Parijs door zowel sympathisanten van ISIS als aanhangers van Anonymous. Bij conflicten als die in Oekraïne en de aanslagen in Parijs is zichtbaar dat ISIS-sympathisanten zich vaker richten op defacements, DDoS-aanvallen en hacks van socialemedia-accounts.

De namen 'Caliphate Cyber Army'[109 110] en 'Islamic Cyber Army'[111 112] lijken de afgelopen periode prominenter naar voren te komen bij digitale aanvallen. Soms worden deze namen door elkaar heen gebruikt.[113] Ook hebben enkele namen die geassocieerd worden met jihadistische digitale aanvallen, aangekondigd zich te verenigen.[114] Het is niet bekend welke identiteit(en) er achter deze namen schuilgaan en of ze door dezelfde personen gebruikt worden of inwisselbaar zijn. Ook is het niet bekend hoeveel personen erachter schuilgaan, zodat conclusies over de eventuele impact van deze fusies momenteel niet mogelijk zijn. In juni 2016 verschenen mediaberichten waarin gemeld werd dat aanvallen uitgevoerd uit naam van Cyber Caliphate en ISIS, uitgevoerd waren door partijen gelieerd aan Rusland.[115]

Hacktivisten

Hacktivisme neemt toe tijdens internationale conflicten

Hacktivisten claimen digitale aanvallen te plegen uit ideologisch motief. Zowel hun motieven als capaciteiten kunnen zeer divers zijn. In veel gevallen voeren hacktivisten DDoS-aanvallen uit op overheidsdoelen,[116 117] media[118 119] en organisaties.[120 121] Het aantal digitale aanvallen van hacktivisten neemt toe tijdens internationale conflicten en aanslagen. Deze activiteiten hebben tot nu toe geen grote gevolgen gehad voor de nationale veiligheid. Het is mogelijk dat digitale aanvallen en publicaties door hacktivisten in de toekomst media-aandacht genereren.

Hacktivisten richtten zich de afgelopen periode meer op doxing. Een voorbeeld van doxing is het openbaar maken van Ku Klux Klan-accounts door hacktivisten.[122 123] Ook werden de namen en inloggegevens van een Israëlische defensie-organisatie gehackt en op het internet vrijgegeven.[124] In Nederland kwam doxing door hacktivisten nog niet vaak voor.

Capaciteiten van hacktivisten lopen uiteen

De capaciteiten van hacktivisten lopen zeer sterk uiteen. Soms wordt gebruik gemaakt van aanvalstechnieken waarvoor weinig kennis en vaardigheden nodig zijn. Soms zijn de digitale aanvallen geavanceerder van aard, zoals bij het compromitteren van gevoelige bedrijfsgegevens.[125 126] Ook zijn in de afgelopen periode

gevallen van sabotage door hacktivisten onderkend: in februari werd bekend dat onbekende personen een drone van de NASA hackten en geprobeerd hebben om deze in zee te laten neerstorten.[127]

Hacktivisten zijn actiever tijdens internationale conflicten en aanslagen. Hacktivisten kondigen na aanslagen vaak digitale aanvallen aan tegen sympathisanten van ISIS.[128][129] Na de aanslagen in Parijs en Brussel leidde dit tot een toename van defacements en DDoS-aanvallen op diverse sites, uitgevoerd door zowel hacktivistische personen en groeperingen die gebruik maken van de naam Anonymous als jihadistische sympathisanten.[130][131] Voor Nederland hadden deze aanvallen slechts een beperkte impact.

Anonymous als digitale dreiging

Anonymous is een losse en ongeorganiseerde verzameling individuen met verschillende belangen, die voor hun digitale activiteiten gebruik maken van de naam 'Anonymous'. Anonymous wordt meestal geassocieerd met digitale activiteiten met een activistisch karakter. Ze roepen vaak op tot digitale aanvallen op verschillende organisaties en instanties.[132][133] Ook maken personen onder de naam Anonymous wel eens bedrijfs- of persoonsgegevens openbaar en roepen zij soms op tot fysiek protest.[134][135]

Toch kan de naam Anonymous niet altijd in verband worden gebracht met hacktivisme. Personen die zich met Anonymous associëren doen dit vaak vanuit verschillende motieven. Hierdoor variëren hun doelstellingen aanzienlijk en kennen zij een grote verscheidenheid aan doelwitten. Waar sommige personen daadwerkelijk ideologisch gemotiveerd zijn, voeren anderen slechts acties uit 'voor de lol'.

Omdat het iedereen vrij staat om zich Anonymous te noemen wordt de naam gebruikt door partijen en personen die zonder ideologische motieven digitale aanvallen plegen.[136] Dit is het afgelopen jaar het geval geweest bij de DDoS-aanval op Ziggo[137] en vermoedelijk bij de aanval op de Volkskrant.[138] In de media leeft vaak het onjuiste beeld dat Anonymous een vaste groepering is die digitale aanvallen uitvoert met eenduidige doelstellingen. Dit beeld duikt vooral op als personen uit naam van Anonymous bijvoorbeeld aankondigen om socialemedia-accounts en websites van pro-jihadistische partijen te deactiveren.

De impact van de digitale aanvallen die uitgevoerd worden onder de noemer Anonymous verschillen evenzeer als de motieven en doelwitten. Soms komt het voor dat aanvallers erin slagen sites een tijd offline te krijgen. Ook het openbaar maken van persoonsgegevens veroorzaakt geregeld overlast voor organisaties en overheden. De impact van het deactiveren van socialemedia-accounts en websites van pro-jihadistische partijen is waarschijnlijk niet bijzonder groot: vaak maken personen nadat zij gedeactiveerd zijn, gewoon een ander account aan.

Cybervandalen en scriptkiddies

Toenemende dreiging door betere beschikbaarheid van middelen

De dreiging vanuit cybervandalen en scriptkiddies neemt toe. De reden voor deze toename is de groeiende beschikbaarheid van laagdrempelige hulpmiddelen voor digitale aanvallen. Cybervandalen en scriptkiddies plegen digitale aanvallen uit baldadigheid, voor de uitdaging of om de eigen capaciteiten aan te tonen. De politie constateert bovendien dat verdachte cybervandalen en scriptkiddies vaak minderjarig zijn. De jonge verdachten en hun ouders zijn zich vaak niet bewust van de aangerichte schade en de consequenties.[139] Cybervandalen hebben een variërend kennisniveau. Het kennisniveau van scriptkiddies is doorgaans laag. Beiden voeren zowel gerichte als ongerichte aanvallen uit.

Cybervandalen en scriptkiddies voeren steeds makkelijker DDoS-aanvallen uit door gebruik te maken van zogenoemde booterservices, die het uitvoeren van DDoS-aanvallen mogelijk maken via een website (DDoS-as-a-service). Deze services zijn op het internet gemakkelijk te vinden en zijn eenvoudig in gebruik. Zelfs met weinig geld[140] en kennis is hierdoor een effectieve aanval uit te voeren. Voorbeelden van dit soort aanvallen zijn de DDoS-aanvallen op Ziggo[141] en de Volkskrant.[142]

Een voorbeeld van gerichte aanvallen door cybervandalen en scriptkiddies waren de hacks door de groep 'Crackas with attitude' van de Amerikaanse hoofden van inlichtingendiensten John Brennan[143] en James Clapper[144]. Na deze hacks werden de gegevens van CIA- en FBI-medewerkers op het internet gepubliceerd. Later werd een 16-jarige Brit voor beide hacks gearresteerd.[145][146] Verder zijn onlinegamingplatformen nog altijd even populaire doelwitten,[147] vooral tijdens de kerstvakantie.[148][149][150]

Attributie van vooral DDoS-aanvallen en defacements blijft moeilijk

Het onderscheid tussen cybervandalen, scriptkiddies, ISIS-sympathisanten en hacktivisten is niet altijd eenvoudig te maken. Vooral bij DDoS-aanvallen en defacements wordt de verantwoordelijkheid van een aanval wel eens opgeëist door een specifieke partij. Toch hoeven de opgegeven redenen niet altijd de echte motivatie achter de aanval te zijn. Een bekend voorbeeld is de aanval op de website van Malaysia Airlines in de vorige rapportageperiode, waar scriptkiddies verwezen naar ISIS.[151] Dit jaar zagen we bij de DDoS-aanvallen op Ziggo en de Volkskrant verwijzingen naar Anonymous, een naam die doorgaans met hacktivisme geassocieerd wordt.[152] Ook werd er een zware DDoS-aanval op de BBC uitgevoerd door een partij die zich naar eigen zeggen bezighoudt met anti-jihadistische activiteiten.[153]

Eenzelfde aanval wordt vaak door meerdere personen of partijen op verschillende fora geclaimd.[154][155] De werkelijke reden voor de aanval blijft dan onduidelijk.

Interne actoren

Dreiging vanuit interne actoren blijft stabiel

Er is geen indicatie dat de dreiging door interne actoren deze periode is veranderd ten opzichte van vorige jaren. Deze dreiging kan afkomstig zijn van kwaadwillende medewerkers die, uit financiële, politieke of persoonlijke motieven, bewust systemen manipuleren of gegevens lekken. Dreiging door interne actoren kan echter ook afkomstig zijn van onbewuste acties en onzorgvuldigheid.

Hoewel in de afgelopen periode in het buitenland enkele berichten gepubliceerd werden over moedwillige acties door interne actoren,[156] [157] viel dit in Nederland mee. In augustus vorig jaar werd een medewerker van een supermarktketen veroordeeld omdat hij bijna honderd bedrijfslaptops geïnfecteerd had.[158]

De grootste interne dreiging in Nederlandse organisaties was echter het gevolg van onoplettendheid en menselijke fouten. Dit varieerde van medewerkers die (onbeveiligde) gegevensdragers kwijtraakten tot instellingsfouten waarbij klantgegevens via het internet te bereiken waren. De Indiase visumverstrekker BSL liet bijvoorbeeld de gegevens van Nederlandse aanvragers uitlekken door een eenvoudige programmeerfout.[159] Een Nederlandse telecomwinkel liet onbedoeld inloggegevens van klantenbestanden op een scherm staan, dat vervolgens eenvoudig voor een onderzoeker in te zien was.[160] Via een SQL-lek bleek dat het merendeel van de medewerkers van een Europese ruimtevaartorganisatie zeer zwakke wachtwoorden gebruikten van soms maar drie tekens lang.[161]

Cyberonderzoekers

Cyberonderzoekers zoeken kwetsbaarheden in ICT-omgevingen om (te) zwakke beveiliging aan de kaak te stellen. Zij gebruiken vaak de media om hun bevindingen te publiceren en de bewustwording over cybersecurity te vergroten. Publiciteit over de kwetsbaarheden kan organisaties (tijdelijk) kwetsbaar maken omdat kwaadwillenden kunnen profiteren van de onderzoeksbevindingen. De afgelopen rapportageperiode is er in Nederland geen significante dreiging door Nederlandse publicaties over kwetsbaarheden waargenomen.

Op publiek en privaat gebied zijn er de afgelopen jaren verschillende afspraken gemaakt om cyberonderzoekers eenvoudiger hun onderzoeksresultaten te laten delen, zonder dat dit ten koste gaat van de veiligheid van organisaties. Een resultaat van deze afspraken is de leidraad die organisaties helpt om te komen tot een praktijk van responsible disclosure, om melders te faciliteren en tot een snelle oplossing van kwetsbaarheden te komen.[162]

Bugbounty-programma wint aan populariteit

Ook valt er onder organisaties een trend waar te nemen van het invoeren van zogenoemde bugbounty's. Dit zijn beloningen die onder bepaalde voorwaarden uitgeloofd worden aan onderzoekers die beveiligingsproblemen blootleggen. Dit jaar sloten bijvoorbeeld het Pentagon[163] en General Motors[164] zich aan bij het bugbounty-programma.[165] In Nederland maken al diverse bedrijven gebruik van bugbounty's, zoals diverse Nederlandse banken[166] [167] [168], Fox-IT[169] en Gamma[170].

Hoewel cyberonderzoekers nog steeds onderzoeksresultaten kunnen publiceren waarvan kwaadwillenden kunnen profiteren, kunnen zowel de leidraad om te komen tot een praktijk van responsible disclosure als het bugbounty-programma ertoe bijdragen dat de dreiging vanuit onderzoekspublicaties geleidelijk afneemt.

Private organisaties

Dreiging door private organisaties kan drie vormen aannemen: organisaties kunnen de vertrouwelijkheid van systemen aantasten voor financieel gewin, organisaties kunnen digitale aanvallen uitvoeren om hun concurrentiepositie te verbeteren en organisaties kunnen de data die zij verzamelen over hun klanten commercieel gebruiken of verkopen aan derden. Het uitvoeren van digitale aanvallen om de eigen concurrentiepositie te verbeteren valt meestal onder de noemer bedrijfsspionage. Er is geen indicatie dat de dreiging vanuit private partijen is veranderd ten opzichte van de vorige rapportageperiode.

In het buitenland zijn de afgelopen periode enkele gevallen van bedrijfsspionage waargenomen. In Amerika heeft bijvoorbeeld een aanbieder van linnengoed bekend dat medewerkers van het bedrijf een concurrent hebben gehackt voor financieel gewin.[171] Ook bekende een medewerker van een Amerikaans honkbalteam een database van een rivaliserend team gehackt te hebben.[172] Verder bleek uit de gelekte documenten van de gecompromitteerde datingsite Ashley Madison dat de bedrijfsleiding een concurrerende datingssite kon infiltreren.[173] In Nederland zijn tot nu toe geen vergelijkbare gevallen bekend.

Tabel 2 Actoren en hun intenties

Actor	Intenties
Beroepscriminelen	Geldelijk gewin (direct of indirect)
Statelijke actoren	Geopolitieke (of interne) machtspositie verbeteren
Terroristen	Maatschappelijke verandering veroorzaken, bevolking ernstige vrees aanjagen of politieke besluitvorming beïnvloeden
Cybervandalen en scriptkiddies	Aantonen van kwetsbaarheden, hacken omdat het kan, baldadigheid, zoeken van uitdaging
Hacktivisten	Ideologische motieven
Interne actoren	Wraak, geldelijk gewin, ideologische motieven (mogelijk 'aangestuurd')
Cyberonderzoekers	Aantonen zwakheden, eigen profilering
Private organisaties	Verkrijgen waardevolle informatie

Persoonsgegevens zijn een steeds aantrekkelijker doelwit voor diverse actoren

De afgelopen maanden zijn er diverse berichten in de internationale media verschenen over diefstal en/of publicatie van persoonsgegevens. Vaak gaat het hier om gegevens uit openbare bronnen die op het internet terug te vinden zijn, maar ook gegevens uit afgeschermde databases vormen voor kwaadwillenden een aantrekkelijk doelwit. Het gericht verzamelen en vervolgens op het internet plaatsen van persoonlijke gegevens zonder toestemming van de eigenaar staat ook wel bekend als 'doxing'. Hoewel niet alle verzamelde gegevens altijd online worden vrijgegeven, vormen persoonsgegevens een aantrekkelijk doelwit voor verschillende actoren.

- Statelijke actoren richten zich doorgaans op persoonlijke gegevens van overheidsmedewerkers voor vermoedelijk spionagedoeleinden. In de media overheerst het beeld dat een statelijke actor bijvoorbeeld verantwoordelijk is voor de hack op het Amerikaanse Office of Personnel Management (OPM), waarbij de persoonsgegevens van meer dan 21 miljoen overheidsmedewerkers zouden zijn buitgemaakt.[174] De gestolen gegevens zijn nooit online openbaar gemaakt. Het is op dit moment dan ook niet bekend hoe deze gegevens precies misbruikt worden.
- Criminelen verzamelen gegevens om deze te misbruiken voor financieel gewin. Hierbij zijn niet alleen persoons- en betaalgegevens een gewild product, maar ook medische gegevens en accountgegevens. Een eerder genoemd voorbeeld is de hack op Ashley Madison.[175]
- Jihadistische groeperingen claimen geregeld gevoelige gegevens en persoonsgegevens uit overheidssystemen gestolen te hebben en publiceren deze vervolgens op het internet. Vaak gaat het hierbij echter om openbaar verkrijgbare informatie, die jihadistische aanhangers waarschijnlijk in het bezit gekregen hebben door gerichte zoekopdrachten naar overheidsdata op het internet.
- Hacktivisten stelen en publiceren persoons- en bedrijfsinformatie om ideologische redenen. Hoewel het moeilijk is om de daadwerkelijke motieven te achterhalen, gaat het publiceren van gevoelige bedrijfsgegevens of persoonsgegevens vaak vergezeld met een ideologische verantwoording. Het is daarbij niet zeker of deze claim ook de daadwerkelijke reden was van de datadiefstal.

Conclusie en vooruitblik

Criminelen en statelijke actoren vormen nog altijd de grootste digitale dreiging voor de nationale veiligheid. Digitale aanvallen van deze actoren zijn het meest geraffineerd en hebben doorgaans de grootste impact op het slachtoffer en de maatschappij.

Bij statelijke actoren is er sprake van een zich ontwikkelende taakverdeling en specialisatie. De werkwijze neemt in complexiteit toe, aanvallers worden vindingrijker en ontwikkelen steeds betere methodes om het probleem van onderkenning en attributie te voorkomen.
De verdienmodellen van criminelen blijven succesvol en zijn het afgelopen jaar populair gebleken. Ransomware wordt in de toekomst verder uitgebreid en gerichter ingezet. Hierbij zijn ziekenhuizen en zorginstellingen een populair doelwit.

Naast het doorontwikkelen van bestaande businessmodellen modelleren criminelen hun aanvallen vaker naar hun beoogde slachtoffer. Het afgelopen jaar is een aantal grote campagnes waargenomen waaruit blijkt dat beroepscriminelen hun werkveld uitbreiden. Professionele groepen beroepscriminelen hebben een hoge organisatiegraad en voeren geavanceerde campagnes uit. De investeringen bij dergelijke campagnes zijn hoog, maar dit lijkt zich uit te betalen: de opbrengsten van de bekende gevallen zijn hoog.

Jihadisten genereren nog altijd veel media-aandacht met kleinschalige digitale aanvallen waarvoor weinig kennis of vaardigheden nodig zijn. Hoewel de digitale capaciteiten van jihadisten nog altijd groeien, hebben zij tot nu toe geen aanslag gepleegd met digitale middelen. De verwachting is dat (kleinschalige) aanvallen vanuit jihadistisch motief in aantal toenemen en dat jihadisten zich meer gaan toeleggen op het publiceren van persoonsgegevens.

Hacktivisten richtten zich de afgelopen periode meer op het publiceren van gevoelige bedrijfsinformatie of persoonlijke gegevens (zonder toestemming van de eigenaar). Diefstal en/of publicatie van persoonsgegevens zijn echter niet alleen aantrekkelijk voor hacktivisten. Ook cybervandalen, scriptkiddies, criminelen, jihadisten en statelijke actoren richten zich om uiteenlopende redenen op het buitmaken van deze gegevens. Deze trend zet zich in de toekomst door.

De dreiging vanuit cybervandalen en scriptkiddies neemt toe. De reden voor deze toename is hoofdzakelijk de groei van laagdrempelige hulpmiddelen voor digitale aanvallen. Ook de beschikbaarheid en betaalbaarheid van cybercrime-as-a-service spelen mee. Hierdoor zijn steeds meer personen in staat om deze aanvallen uit te voeren. De verwachting is dat vooral DDoS-aanvallen in aantal toenemen.

Op het gebied van interne actoren en private organisaties is er geen indicatie dat de dreiging is veranderd ten opzichte van de vorige rapportageperiode. Ook zijn bij deze actoren geen nieuwe trends of fenomenen waargenomen waarvan dreiging uitgaat. Dreiging vanuit cyberonderzoekers neemt door een aantal trends waarschijnlijk verder af.

Noten

51 1. https://www.om.nl/vaste-onderdelen/zoeken/@94086/groot-crimineel/, geraadpleegd op 13 juli 2016.
2. http://www.nrc.nl/next/2016/04/21/informatieschat-op-criminele-gsms-1614033, geraadpleegd op 13 juli 2016.

52 https://www.europol.europa.eu/latest_news/iocta-2015-europol-annual-report-cybercrime-threat-landscape-published

53 1. http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/, geraadpleegd op 4 juli 2016.
2. http://blog.trendmicro.com/trendlabs-security-intelligence/businesses-held-for-ransom-torrentlocker-and-cryptowall-change-tactics/, geraadpleegd op 4 juli 2016.
3. Bron: Fox-IT.

54 1. https://www.technologyreview.com/s/600838/hollywood-hospitals-run-in-with-ransomware-is-part-of-an-alarming-trend-in-cybercrime/, geraadpleegd op 4 juli 2016.
2. http://arstechnica.com/security/2016/03/kentucky-hospital-hit-by-ransomware-attack/, geraadpleegd op 4 juli 2016.

55 https://www.security.nl/posting/461521/Amerikaans+ziekenhuis+betaalt+17_000+dollar+aan+ransomware, geraadpleegd op 4 juli 2016.

56 http://www.theregister.co.uk/2016/02/15/ransomware_scum_tear_up_tinsel_town_hospital_demand_record_36m/, geraadpleegd op 4 juli 2016.

57 http://www.securityweek.com/cybercriminals-encrypt-website-databases-%E2%80%9Cransomweb%E2%80%9D-attacks, geraadpleegd op 4 juli 2016.

58 https://www.security.nl/posting/464735/FBI+waarschuwt+voor+ransomware-aanval+die+back-ups+wist, geraadpleegd op 4 juli 2016.

59 http://securityaffairs.co/wordpress/41775/cyber-crime/protonmail-paid-ransom-ddos.html, geraadpleegd op 4 juli 2016.

60 1. http://www.computerweekly.com/news/4500246707/DD4B-cyber-extortion-gang-targets-key-European-sectors, geraadpleegd op 4 juli 2016.
2. https://blogs.akamai.com/2015/05/dd4bc-escalates-attacks.html, geraadpleegd op 4 juli 2016.

61 https://blogs.akamai.com/2015/11/operation-profile-armada-collective.html, geraadpleegd op 4 juli 2016.

62 http://news.softpedia.com/news/unknown-copycat-using-armada-collective-name-for-ddos-for-bitcoin-extortions-497297.shtml, geraadpleegd op 4 juli 2016.

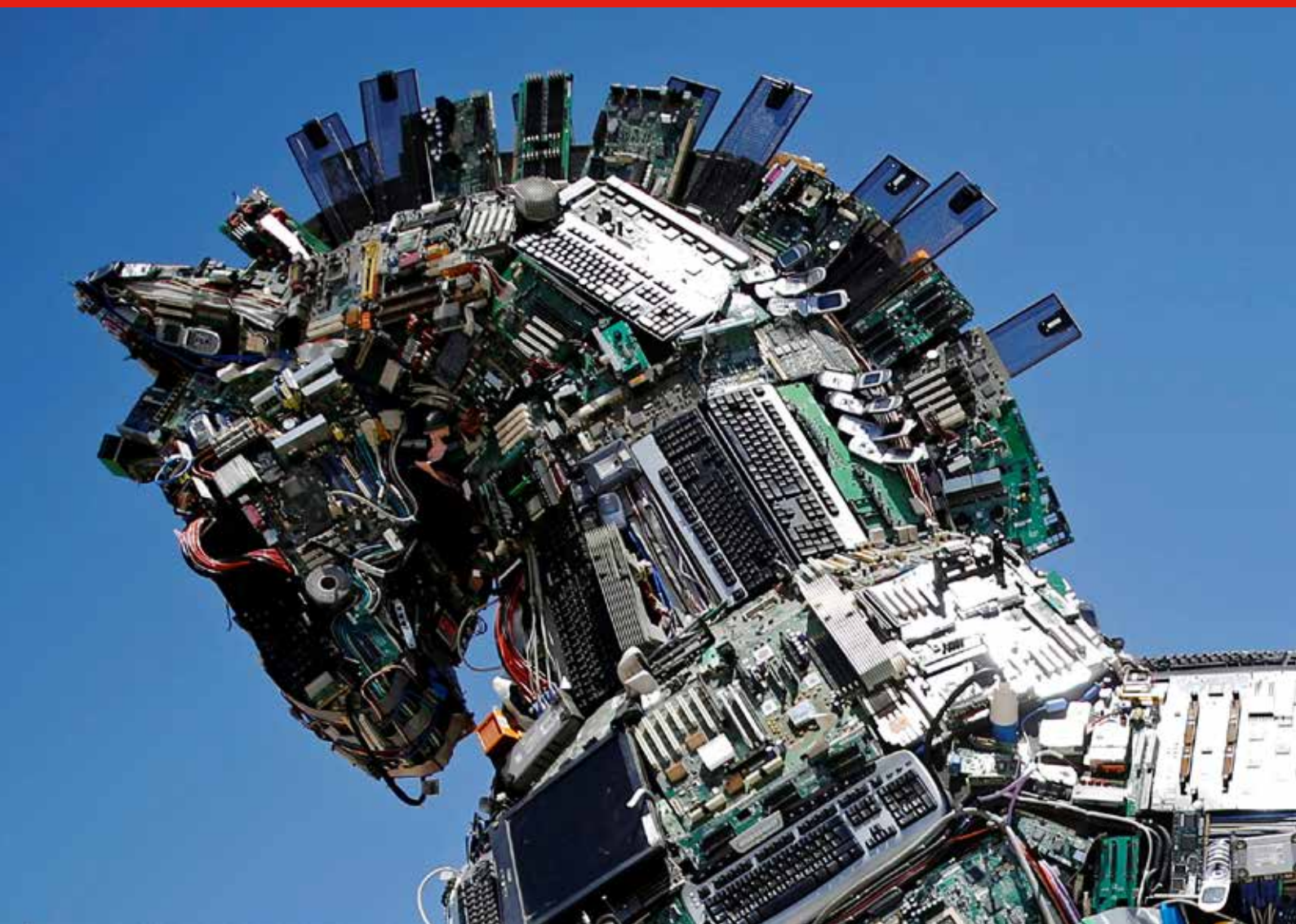
63 http://www.securityweek.com/dd4bc-armada-collective-inspire-cyber-extortion-copycats, geraadpleegd op 4 juli 2016.

64 Zie voor nadere uitleg over de hack op Ashley Madison in hoofdstuk 1.
65 http://www.zdnet.be/nieuws/171086/hackers-chanteren-ashley-madison-gebruikers/, geraadpleegd op 4 juli 2016.
66 http://tweakers.net/nieuws/104536/hackers-zetten-inloggegevens-van-bitdefender-klanten-online.html, geraadpleegd op 4 juli 2016.
67 http://tweakers.net/nieuws/104290/rex-mundi-heeft-financiele-gegevens-duizenden-belgen-buitgemaakt.html, geraadpleegd op 4 juli 2016.
68 http://nos.nl/op3/artikel/2011495-hacker-s-rex-mundi-al-drie-jaar-een-etterende-wond.html, geraadpleegd op 4 juli 2016.
69 http://www.csoonline.com/article/2931535/data-breach/check-point-reports-explosion-in-unrecognizeable-malware.html, geraadpleegd op 4 juli 2016.
70 Bron: politie.
71 https://www.security.nl/posting/434682/Bouwdoos+van+malware+die+Nederlandse+banken+aanviel+gelekt?channel=rss, geraadpleegd op 4 juli 2016.
72 https://securityintelligence.com/tinba-worlds-smallest-malware-has-big-bag-of-nasty-tricks/, geraadpleegd op 4 juli 2016.
73 Bron: politie.
74 Bron: politie.
75 Bron: politie.
76 http://arstechnica.com/security/2016/01/researchers-uncover-javascript-based-ransomware-as-service/, geraadpleegd op 4 juli 2016.
77 https://www.security.nl/posting/438203/Organisatie+luidt+noodklok+over+malware-video%27s+op+YouTube, geraadpleegd op 4 juli 2016.
78 http://feeds.webwereld.nl/~r/Webwereld/~3/AzkSM1zMpUo/88019-open-source-ransomware-vrijelijk-beschikbaar-op-github, geraadpleegd op 4 juli 2016.
79 Bron: politie.
80 Bron: politie.
81 http://tweakers.net/nieuws/108009/verspreiding-financiele-dyre-malware-gestopt-door-russische-autoriteiten.html, geraadpleegd op 4 juli 2016.
82 Bron: politie.
83 Bron: interview met Michel van Eeten.
84 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report, geraadpleegd op 4 juli 2016.
85 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report, geraadpleegd op 4 juli 2016.
86 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report, geraadpleegd op 4 juli 2016.
87 Bron: politie en https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/, geraadpleegd op 4 juli 2016.
88 http://www.drchaos.com/sweet-orange-web-exploit-kit/, geraadpleegd op 4 juli 2016.
89 http://news.softpedia.com/news/New-MS-Word-Exploit-Kit-Adds-Statistics-Tool-to-Track-Success-of-the-Campaign-477568.shtml, geraadpleegd op 4 juli 2016.
90 Bron: politie.
91 Bron: politie.
92 Bron: AIVD en MIVD.
93 Bron: AIVD en MIVD.
94 Bron: AIVD en MIVD.
95 http://www.nytimes.com/2016/01/15/world/middleeast/a-news-agency-with-scoops-directly-from-isis-and-a-veneer-of-objectivity.html?_r=0, geraadpleegd op 4 juli 2016.
96 http://www.mirror.co.uk/news/technology-science/technology/hidden-isis-android-app-lets-6203483, geraadpleegd op 4 juli 2016.
97 http://securityaffairs.co/wordpress/24978/cyber-crime/al-qaeda-encryption-tools.html, geraadpleegd op 4 juli 2016.
98 http://www.csoonline.com/article/3004648/security-awareness/after-paris-isis-moves-propaganda-machine-to-darknet.html, geraadpleegd op 4 juli 2016.
99 http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085, geraadpleegd op 4 juli 2016.
100 https://www.security.nl/posting/466258/Onderzoek%3A+terroristen+nauwelijks+aanwezig+op+Tor-netwerk, geraadpleegd op 4 juli 2016.
101 http://www.thedailybeast.com/articles/2015/03/23/isis-hackers-googled-their-hit-list-troops-names-were-already-on-public-websites.html, geraadpleegd op 4 juli 2016.
102 http://www.databreaches.net/feds-charge-ardit-ferizi-aka-th3dir3ctory-with-creating-hit-list-of-american-military-govt-employees-for-isis/, geraadpleegd op 4 juli 2016.
103 http://www.nu.nl/internet/4106100/zet-informatie-1400-amerikaanse-militairen-en-ambtenaren-online.html, geraadpleegd op 4 juli 2016.
104 http://www.databreaches.net/jihadist-leaks-addresses-of-army-sgt-dillard-johnson-navy-seal-rob-oneill/, geraadpleegd op 4 juli 2016.
105 http://www.ubergizmo.com/2015/12/islamic-cyber-army-responds-to-isis-day-of-trolling/, geraadpleegd op 4 juli 2016.
106 https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-6-1-15-ishd-calls-for-attacks-on-10-italian-army-personnel.html, geraadpleegd op 4 juli 2016.
107 http://www.telegraaf.nl/binnenland/26069079/__74_Nederlanders_op_dodenlijst_IS__.html
108 Bron: AIVD en MIVD.
109 https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&tagId=787&Itemid=1355, geraadpleegd op 4 juli 2016.
110 http://www.washingtontimes.com/news/2016/mar/15/islamic-state-hackers-post-kill-list-minnesota-cop/, geraadpleegd op 4 juli 2016.

111 http://www.techworm.net/2015/09/isis-affiliates-to-launch-cyber-attacks-on-united-states-to-celebrate-911.html, geraadpleegd op 4 juli 2016.
112 http://abcnews.go.com/US/fbi-warns-isis-inspired-cyber-attacks-911-anniversary/story?id=33684413, geraadpleegd op 4 juli 2016.
113 SITE Intel Group, Pro-IS Hackers Forward Purported Info of Military Personnel Prominent Government Figures, 21-11-2015
114 http://www.ibtimes.co.uk/isis-cyber-army-grows-strength-caliphate-hacking-groups-merge-telegram-1553326, geraadpleegd op 4 juli 2016.
115 http://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/, geraadpleegd op 4 juli 2016.
116 http://www.nu.nl/internet/4173614/anonymous-hackt-ijslandse-overheidswebsites-walvisvangst.html, geraadpleegd op 4 juli 2016.
117 http://spd.rss.ac/aHRocDovL25ld3Muc29mdHBlZGlhLmNvbS9uZXdzL2Fub255bW91cy10YWNrcy11cy1kZXBhcnRtZW50LW9mLWFncmljdWxodXJlLXR-vLXByb3Rlc3QtYWdhaW5zdC1tb25zYW50obyooOTU4NTUuc2hobWw, geraadpleegd op 4 juli 2016.
118 http://www.rcfp.org/browse-media-law-resources/news/online-attacks-against-media-websites-are-increasing-and-costly, geraadpleegd op 4 juli 2016.
119 https://www.hackread.com/anonymous-ddos-zimbabwe-herald-website/, geraadpleegd op 4 juli 2016.
120 http://www.scmagazineuk.com/anonymous-attacks-two-japanese-airports/article/447817/, geraadpleegd op 4 juli 2016.
121 http://www.bbc.com/news/technology-35306206, geraadpleegd op 4 juli 2016.
122 http://www.ibtimes.co.uk/anonymous-hackers-threaten-reveal-identities-1000-ku-klux-klan-members-opkkk-1525758, geraadpleegd op 4 juli 2016.
123 http://www.nu.nl:80/internet/4157261/anonymous-begint-met-publiceren-namen-ku-klux-klanleden.html, geraadpleegd op 4 juli 2016.
124 https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/anonsec-allegedly-hacks-israel-missile-defense-association.html, geraadpleegd op 4 juli 2016.
125 http://tweakers.net/nieuws/109245/hackers-stelen-gegevens-van-anti-ddos-dienstverlener-staminus.html, geraadpleegd op 4 juli 2016.
126 https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim, geraadpleegd op 4 juli 2016.
127 http://www.ibtimes.co.uk/nasa-hack-anonsec-attempts-crash-222m-drone-releases-secret-flight-videos-employee-data-1541254, geraadpleegd op 4 juli 2016.
128 http://news.softpedia.com/news/anonymous-announces-payback-for-the-isis-paris-attacks-496184.shtml, geraadpleegd op 4 juli 2016.
129 http://www.independent.co.uk/life-style/gadgets-and-tech/news/paris-attacks-anonymous-launches-its-biggest-operation-ever-against-isis-promises-to-hunt-down-a6735811.html, geraadpleegd op 4 juli 2016.
130 http://www.eteknix.com/major-isis-messaging-forum-taken-anonymous/, geraadpleegd op 4 juli 2016.
131 http://www.zdnet.com/article/isis-supporter-cyber-caliphate-takes-over-54000-twitter-accounts/#ftag=RSSbaffb68, geraadpleegd op 4 juli 2016.
132 http://www.rtlz.nl/tech/anonymous-haalt-website-trump-offline-verspreid-geen-haat, geraadpleegd op 4 juli 2016.
133 http://grapevine.is/news/2015/11/28/anonymous-shuts-down-almost-all-icelandic-govt-websites-for-13-hours/, geraadpleegd op 4 juli 2016.
134 http://nos.nl/artikel/279137-anonymous-verklaart-de-oorlog-aan-wall-street.html, geraadpleegd op 4 juli 2016.
135 http://edition.cnn.com/2015/11/06/europe/uk-anonymous-london-march/, geraadpleegd op 4 juli 2016.
136 http://news.softpedia.com/news/anonymous-hacks-european-space-agency-just-for-fun-497551.shtml, geraadpleegd op 4 juli 2016.
137 http://nos.nl/artikel/2052851-weer-urenlange-storing-bij-ziggo-door-ddos-aanval.html, geraadpleegd op 4 juli 2016.
138 http://www.volkskrant.nl/tech/volkskrant-nl-kort-uit-de-lucht-door-ddos-aanval~a4125596/, geraadpleegd op 4 juli 2016.
139 Bron: politie.
140 Zie voor prijzen op ondergrondse marktplaatsen tabel 2.
141 http://www.volkskrant.nl/economie/ddos-aanval-op-ziggo-klanten-blijkt-letterlijk-kinderspel~a4158438/, geraadpleegd op 4 juli 2016.
142 http://www.volkskrant.nl/tech/volkskrant-nl-kort-uit-de-lucht-door-ddos-aanval~a4125596/, geraadpleegd op 4 juli 2016.
143 https://www.theguardian.com/technology/2015/oct/19/cia-director-john-brennan-email-hack-high-school-students, geraadpleegd op 4 juli 2016.
144 http://www.theguardian.com/us-news/2016/jan/13/hacker-breaks-into-personal-email-of-us-director-of-national-intelligence, geraadpleegd op 12 juli 2016.
145 https://www.washingtonpost.com/world/national-security/british-teen-arrested-in-hacking-of-top-us-intelligence-officials/2016/02/12/7b87351e-d1a5-11e5-b2bc-988409ee911b_story.html, geraadpleegd op 12 juli 2016.
146 http://www.nu.nl/internet/4213760/britse-politie-arresteert-tiener-fbi-hack.html, geraadpleegd op 12 juli 2016.
147 http://tweakers.net/nieuws/104593/dota-2-gametoernooi-tijdelijk-stilgelegd-vanwege-ddos-aanval.html, geraadpleegd op 12 juli 2016.
148 http://news.softpedia.com/news/phantom-squad-starts-christmas-ddos-attacks-by-taking-down-ea-servers-498078.shtml, geraadpleegd op 12 juli 2016.
149 http://www.csmonitor.com/World/Passcode/2015/1224/Lizard-Squad-plans-Christmas-Day-encore-with-Xbox-PlayStation-attacks, geraadpleegd op 12 juli 2016.
150 http://www.engadget.com/2015/12/30/steams-christmas-privacy-issues-affected-34-000-users/, geraadpleegd op 12 juli 2016.
151 http://www.bloomberg.com/news/articles/2015-01-26/malaysia-air-website-hacked-with-phrase-isis-will-prevail-, geraadpleegd op 12 juli 2016.
152 http://www.ad.nl/ad/nl/1012/Nederland/article/detail/4125550/2015/08/20/De-Volkskrant-getroffen-door-hackeraanval.dhtml, geraadpleegd op 12 juli 2016.
153 http://www.bignewsnetwork.com/news/239915393/anti-isis-hackers-say-they-took-down-bbc-website-during-testing, geraadpleegd op 12 juli 2016.
154 http://www.emerce.nl/nieuws/alleen-nederlanders-achter-aanval-ziggo, geraadpleegd op 12 juli 2016.
155 http://www.techworm.net/2015/12/hacking-group-skidnp-takes-down-phantom-squads-website.html, geraadpleegd op 12 juli 2016.

156 https://www.security.nl/posting/462079/Ontslagen+systeembeheerder+saboteert+fabriek, geraadpleegd op 12 juli 2016.
157 http://www.newsobserver.com/news/business/article32944404.html, geraadpleegd op 12 juli 2016.
158 https://www.security.nl/posting/440098/Jumbo-medewerker+hackte+bijna+honderd+bedrijfslaptops, geraadpleegd op 4 juli 2016.
159 http://tweakers.net/nieuws/104706/indiase-visumverstrekker-bls-liet-gegevens-nederlandse-aanvragers-uitlekken.html, geraadpleegd op 4 juli 2016.
160 http://sijmen.ruwhof.net/weblog/608-personal-data-of-dutch-telecom-providers-extremely-poorly-protected-how-i-could-access-12-million-records, geraadpleegd op 4 juli 2016.
161 http://webwereld.nl/security/90837-esa-wachtwoorden-zo-simpel-als-123, geraadpleegd op 4 juli 2016.
162 https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html
163 http://www.wired.co.uk/news/archive/2016-03/02/hack-the-pentagon-bug-bounty, geraadpleegd op 4 juli 2016.
164 https://hackerone.com/gm
165 https://hackerone.com/internet-bug-bounty
166 https://hackerone.com/abnamro
167 https://hackerone.com/dnb_nl
168 https://hackerone.com/ing
169 https://hackerone.com/foxit
170 https://hackerone.com/gammanl
171 https://www.security.nl/posting/453200/IT-directeur+Amerikaans+bedrijf+hackte+server+concurrent, geraadpleegd op 4 juli 2016.
172 https://nakedsecurity.sophos.com/2016/01/12/ex-cardinals-exec-yes-i-hacked-rival-astros-database/, geraadpleegd op 4 juli 2016.
173 http://krebsonsecurity.com/2015/08/leaked-ashleymadison-emails-suggest-execs-hacked-competitors/, geraadpleegd op 4 juli 2016.
174 https://www.washingtonpost.com/news/the-switch/wp/2015/07/15/the-opm-breach-exposed-more-than-a-million-fingerprints-heres-why-that-terrible-news/, geraadpleegd op 4 juli 2016.
175 http://www.zdnet.be/nieuws/171086/hackers-chanteren-ashley-madison-gebruikers/, geraadpleegd op 4 juli 2016. http://www.zdnet.be/nieuws/171086/hackers-chanteren-ashley-madison-gebruikers/, geraadpleegd op 4 juli 2016.

Advertentienetwerken zijn nog niet in staat gebleken malvertising het hoofd te bieden



3 Dreigingen: Middelen

Actoren blijven de effectiviteit van bestaande middelen vergroten. Zo zetten makers van ransomware slachtoffers steeds meer onder druk. Malware en communicatie door malware kan steeds beter worden verborgen. Ook de hoeveelheid nieuwe malware voor mobiele platformen neemt toe. Actoren proberen vertrouwde bronnen en advertentienetwerken te infecteren, om zo malware te kunnen verspreiden. De ontwikkeling van kant-en-klaarmiddelen en cybercrime-as-a-service zet door.

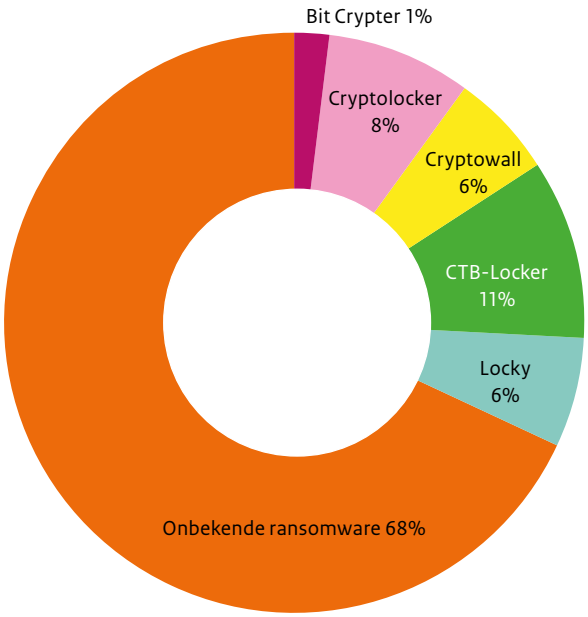
Actoren gebruiken bij digitale aanvallen middelen om kwetsbaarheden te misbruiken of vergroten. Dit hoofdstuk gaat in op de gebruikte middelen en gehanteerde methoden.

Malware

Ransomware blijft een groot probleem

In het CSBN 2015 werd ransomware al aangeduid als groeiend probleem. De verdere ontwikkeling en verspreiding van ransomware zet zich voort. Nieuwe varianten van ransomware verschijnen frequent en de opbrengsten die criminelen weten te realiseren zijn hoog. In bijna alle gevallen worden alle bestanden van het slachtoffer versleuteld en daarmee ontoegankelijk gemaakt. Alleen tegen betaling wordt de versleuteling ongedaan gemaakt. In uitzonderlijke gevallen hebben slachtoffers geluk. Soms kan de sleutel achterhaald worden door een implementatiefout in de versleuteling of door het oprollen van de infrastructuur van de cryptoware. Dan kunnen de bestanden kosteloos worden ontsleuteld. Ook in Nederland blijken ontwikkelaars van cryptoware actief. Zo werden twee Nederlanders opgepakt die verdacht werden van het maken en verspreiden van de Coinvault-cryptoware.[176]

Figuur 1 **Aangiftes ransomware in Nederland**



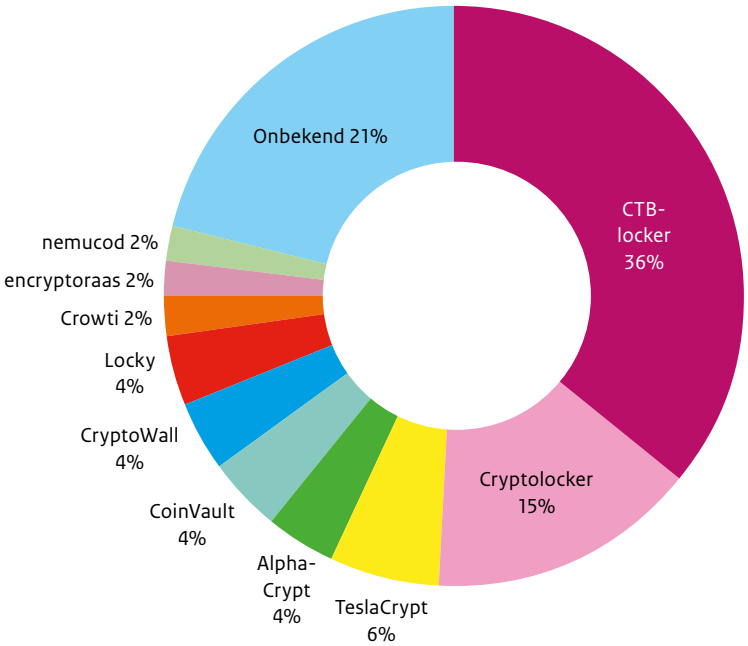
Bron: politie.

Ransomware treft steeds meer platformen die hier voorheen geen last van hadden. Bijvoorbeeld Mac OS X, dat nu is getroffen door de KeRanger-ransomware.[177] Nu steeds meer alledaagse apparaten uitgerust worden met processoren en connectiviteit neemt het risico van een ransomware-infectie op dergelijke apparaten toe. Zo neemt het aantal ransomware-infecties op Android toe.[178] Symantec heeft een proof-of-concept uitgevoerd met ransomware die een smartwatch kon infecteren via de smartphone waarop deze was aangesloten.[179] Ook is er een proof-of-concept uitgebracht van ransomware die smart-tv's kan besmetten.[180]

Ransomware wordt niet alleen tegen systemen van eindgebruikers ingezet, maar ook direct tegen servers. Dat gebeurt door kwetsbaarheden op die servers te misbruiken.[181] Via deze weg kan de server zelf gegijzeld worden. Ook kan de server gebruikt worden om voet aan de grond te krijgen binnen het netwerk van de organisatie. Van daaruit kan verder actie ondernomen worden.[182] Zo kan de aanvaller verkennen welke (netwerk-)schijven of bestanden het waardevolst zijn. Deze kunnen later te versleuteld worden. Dan kan een zo hoog mogelijke losgeldsom worden gevraagd.[183]

Net als in eerdere jaren is ook het afgelopen jaar ransomware aangetroffen die back-upbestanden,[184] netwerkschijven en databases versleutelde. Ook is er gedreigd met het publiceren van persoonlijke gegevens als er niet betaald zou worden.[185] Het is onduidelijk of dit ook daadwerkelijk is gebeurd.

Figuur 2 **Bij het NCSC gemelde ransomwarebesmettingen**



Bron: NCSC. Periode januari 2015 tot en met april 2016.

Verspreiding van malware door vertrouwde bronnen te infecteren

Als gebruikers van mobiele apparaten uitsluitend software uit legitieme bronnen installeren, zoals de appstores van Apple, Google en Microsoft, lopen zij een kleinere kans op een virus- of malwareinfectie. Hoewel er controles uitgevoerd worden, blijven appstores niet vrij van malware. Actoren proberen malware te verspreiden door gebruik te maken van het vertrouwen dat gebruikers hebben in deze kanalen.

Een watering hole-aanval is een voorbeeld van een dergelijke strategie. Er zijn meerdere werkwijzen om legitieme software te infecteren met malware. Allereerst kan de website van de software-leverancier gecompromitteerd worden. De malware wordt in de op de website aangeboden software verwerkt en vervolgens zo door gebruikers gedownload. Voorbeelden zijn de websites van Linux Mint[186] en Transmission[187]. Beiden raakten gecompromitteerd, waarna de software met malware werd verspreid. In sommige gevallen wordt daarbij de software digitaal ondertekend met buitgemaakt geheim sleutelmateriaal. Hierdoor wordt de software vertrouwd door het besturingssysteem.[188]

Een andere werkwijze is het infecteren van ontwikkelomgevingen (integrated development environments, IDE) en compilers, waarmee programma's en apps gemaakt kunnen worden en programmacode omgezet kan worden in systeeminstructies. In China zijn geïnfecteerde exemplaren van de Xcode IDE van Apple verspreid. Deze versie staat bekend als XcodeGhost. Alle daarmee ontwikkelde legitieme apps kregen automatisch malware meegeleverd. Zo konden ze geïnfecteerd in de Apple App Store belanden.[189] Uiteindelijk ging het om vele tientallen apps die wereldwijd in totaal door honderden miljoenen mensen werden gebruikt.[190] Ruim 36.000 Nederlanders zouden geraakt zijn door een van de malafide apps.[191]

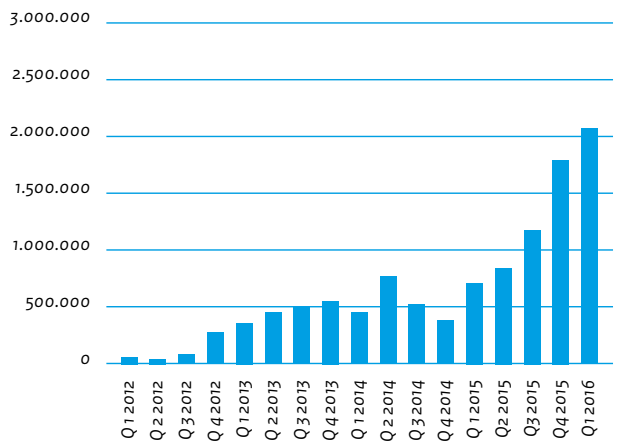
Ten slotte is het ook mogelijk dat nieuwe apparatuur al van malware is voorzien. Dit is een fenomeen dat al sinds jaren bestaat en zich nog steeds voordoet.[192] De besmetting kan zich bij de fabrikant zelf voordoen, of worden veroorzaakt door doorverkopers die doelbewust apparatuur van malware voorzien. Deze ontwikkeling was vooral zichtbaar bij Androidtelefoons en -tablets uit China.[193] Met name replicaproducten hebben een verhoogd risico op malware-infectie.

De hoeveelheid malware voor mobiele platformen neemt toe

Mobiele apparaten, zoals smartphones en tablets, nemen een steeds centralere positie in het dagelijks leven van gebruikers in. Steeds meer (financiële) activiteiten worden ermee uitgevoerd. Veel fabrikanten van mobiele apparatuur voorzien deze vaak maar voor een beperkte periode van updates. Hierdoor worden grote groepen gebruikers kwetsbaar voor nieuw gevonden kwetsbaarheden.

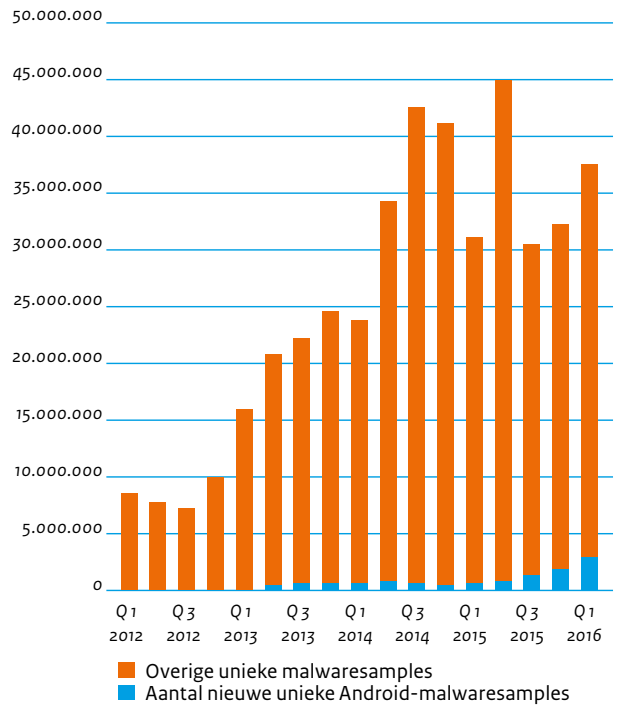
Uit de cijfers van AV-Test blijkt dat het aantal nieuwe Android-malwaresamples meer dan verdriedubbeld is in de periode januari 2015 tot en met maart 2016. Ook het aandeel van nieuwe Android-malware in het totaal aan nieuwe malware is meer dan verdriedubbeld en komt daarmee op 6,8 procent. Dit toont aan dat de mobiele platformen een steeds aantrekkelijker doelwit voor malware worden. De groei van het aantal unieke malwaresamples voor alle platformen, inclusief mobiele platformen, fluctueert sterk in 2015. Zo is er een sterke groei van het aantal unieke malwaresamples in het tweede kwartaal van 2015 te zien.

Figuur 3 **Aantal nieuwe unieke Android-malwaresamples**



Bron: AV-Test.

Figuur 4 **Aantal nieuwe unieke malwaresamples**



Bron: AV-Test.

Vooralsnog lijkt het erop dat infectie van mobiele apparaten vooral plaatsvindt via malafide apps in de alternatieve appstores, infectie van gejailbreakte toestellen en infectie van ontwikkelomgevingen (zoals bij XcodeGhost). Het is niet bekend hoe de meeste besmettingen plaatsvinden. Een oorzaak van infectie kan ook in de relationele sfeer liggen. Bekenden installeren dan spyware op het apparaat van het slachtoffer.[194]

Hoeveelheid malware voor iOS relatief laag, maar groeit gestaag

iOS-systemen blijven over het algemeen weerbaar tegen malware, maar het aantal gebruikte aanvalsvectoren en de hoeveelheid malware gericht op deze systemen neemt toe.[195] Het grootste risico wordt gelopen wanneer een iOS-systeem door de gebruiker is gejailbreakt. Hierdoor worden er apps vanuit een niet-vertrouwde bron toegestaan. Ook niet-gejailbreakte iOS-systemen zijn in het verleden kwetsbaar gebleken. Deze ontwikkeling zet zich door.

Eerder in dit hoofdstuk kwam de inzet van een gecompromitteerde versie van Xcode aan de orde. Hiermee ontwikkelde apps kregen malware meegeleverd die uiteindelijk in de Apple App Store belandden. Een andere zaak waarbij malware meegeleverd werd met iOS-apps was een advertentie-library die in veel iOS-apps werd gebruikt. Deze maakte het mogelijk om gevoelige informatie van het iOS-systeem te verkrijgen.[196]

Daarnaast wordt er misbruik gemaakt van de mogelijkheid voor bedrijven om applicaties buiten de Apple App Store op iOS-systemen te installeren (enterprise provisioning). Deze apps worden vaak ondertekend met gestolen digitale certificaten of certificaten van minder betrouwbare ontwikkelaars. Voor besmetting is het noodzakelijk dat de gebruiker instemt met de installatie van de applicatie en het iOS-systeem aansluit aan een computer.

Een andere gehanteerde methode is het verleiden van gebruikers om een profiel voor mobile device management te installeren op een iOS-systeem. Een dergelijk profiel maakt het binnen bedrijfsomgevingen mogelijk om iOS-systemen op afstand te beheren. Aanvallers die er in slagen de gebruiker een dergelijk profiel te laten installeren, kunnen netwerkverkeer echter omleiden naar een systeem dat onder controle staat van de aanvaller. Deze kan dan op afstand applicaties installeren.[197]

Een nieuwe ontwikkeling is dat malware actief gebruik maakt van kwetsbaarheden in iOS om zichzelf te installeren zonder dat hiervoor een expliciete actie van de gebruiker op het iOS-systeem vereist is. Een voorbeeld is de AceDeceiver-malware. Hierbij is overigens nog steeds een USB-verbinding met een geïnfecteerde computer noodzakelijk voor besmetting van het iOS-systeem.[198]

Bij Android malware is het gebruik van overlays een vaker voorkomend middel om inloggegevens van gebruikers af te vangen.[199] Gebruikers denken de legitieme app te gebruiken, maar de malware vangt de scherminvoer van de gebruiker af.

Tools

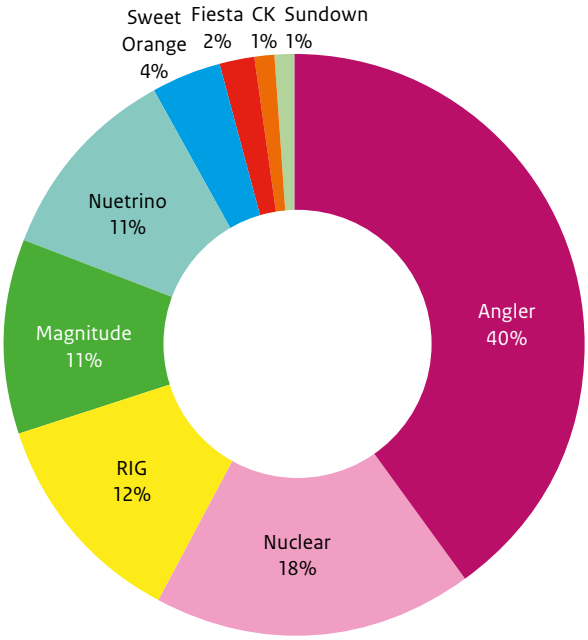
Exploitkits worden doorontwikkeld

Er zijn softwareontwikkelaars die kant-en-klare en gebruiksvriendelijke exploitkits aanbieden om gebruikers met malware te besmetten, zoals de Angler-exploitkit. Een ander bekende exploitkit is BlackEnergy. Deze wordt in verband gebracht met verstoringen bij Oekraïense energiecentrales.[200] Er zijn niet alleen exploitkits voor reguliere computers, maar ook voor apparaten zoals routers.[201] Exploits voor het misbruiken van kwetsbaarheden kunnen al meegeleverd zijn met de exploitkit, maar nieuwe exploits kunnen ook van een derde partij aangekocht worden. 86 procent van de exploits die binnen exploitkits wordt gebruikt, maakt misbruik van een lek in Flash Player.[202]

Exploits voor kwetsbaarheden worden verhandeld op het internet, zowel op ondergrondse fora[203] als door commerciële bedrijven.[204] In het bijzonder zogenoemde zero-daykwetsbaarheden, kwetsbaarheden waarvan het publiek nog niet op de hoogte is, worden voor grote bedragen verhandeld.

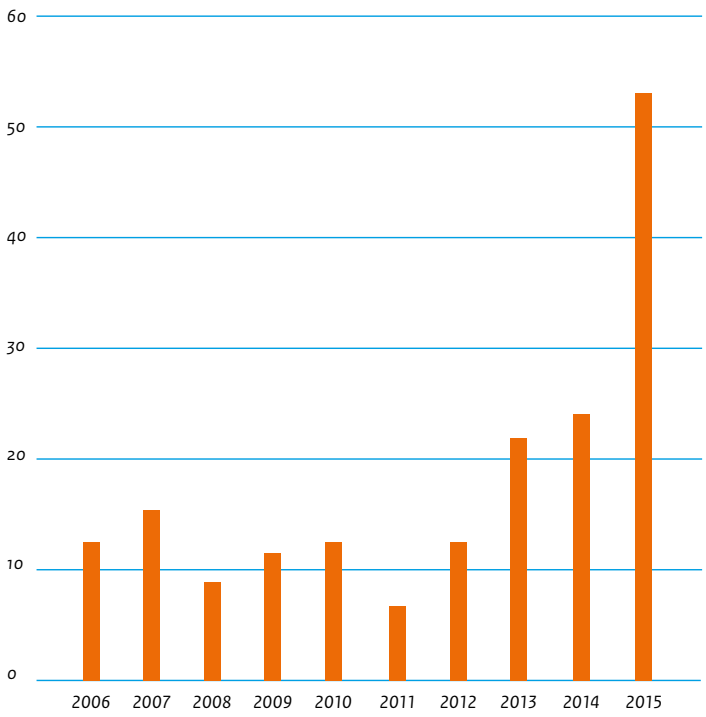
Het aantal gepubliceerde zero-daykwetsbaarheden in 2015 nam sterk toe.[205] Hiervoor is geen eenduidige verklaring. Wanneer misbruik van zero-days wordt gedetecteerd en dat bekend wordt, komt er in de meeste gevallen een update beschikbaar. Van de 54 bekende zero-days in 2015 betroffen vier Android, tien Adobe Flash Player, zes Microsoft Windows, twee Internet Explorer, twee Microsoft Office en tien software voor industriële controlesystemen. De overige zero-days waren voor andere software.[206]

Figuur 5 **Aandeel diverse exploitkits in 2015**



Bron: Trustwave.

Figuur 6 **Totaal aantal bekend geworden zero-dayexploits per jaar**



Bron: Symantec.

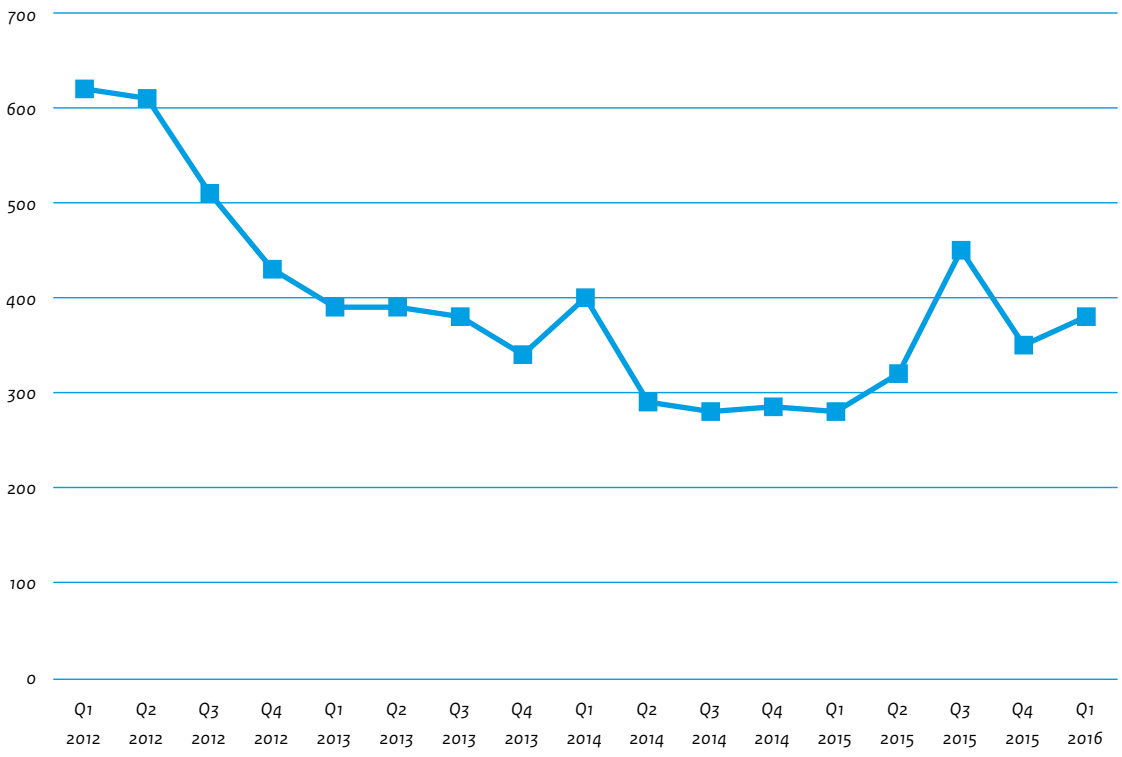
Naast de eerdergenoemde partijen zijn er partijen die zich bijvoorbeeld richten op het ontwikkelen van ransomware of een banking trojan om slachtoffers geld afhandig te maken. Andere bekende alternatieven zijn RAT's. Hiermee kan onder andere informatie van het systeem van het slachtoffer worden ontvreemd.

Het aantal gepubliceerde exploits per kwartaal bleef na een sterke daling in 2012 constant. In 2015 is echter weer een stijgende lijn waarneembaar.

Remote access tools blijven een geliefd middel voor cybercrime

RAT's blijven vanwege hun brede toepasbaarheid een geliefd instrument om verschillende soorten van criminaliteit mogelijk te maken. Aangezien de aanvaller praktisch alle functies overneemt die de gewone gebruiker ook op het systeem ter beschikking staan, zijn er veel aanvalsmogelijkheden. De ontwikkeling van RAT's zet zich door. Zo zijn er RAT's die zonder aanpassing op verschillende besturingssystemen werken.[207] Een RAT is al vanaf 5 dollar te koop op ondergrondse markplaatsen.[208] RAT's zijn het afgelopen jaar wederom een laagdrempelig en veelzijdig middel voor actoren gebleken.

Figuur 7 **Aantal gepubliceerde exploits per kwartaal**



Bron: Exploit-DB.

Denial-of-serviceaanvallen

Aanvallers blijven nieuwe amplificatiemethoden ontdekken

Aanvallers blijven nieuwe methodes ontdekken om een DDoS-aanval zo effectief mogelijk te laten zijn door de hoeveelheid naar het slachtoffer verstuurde data te vergroten. De belangrijkste methode hierbij is amplificatie. Hierbij sturen aanvallers een klein verzoek naar een dienst, met een vervalst afzenderadres dat gelijk is aan het adres van het slachtoffer. Daarna volgt een groot antwoord. De benodigde mate van kennis en vaardigheden voor een aanvaller is in beginsel beperkt. Dat komt door het aanbod van laagdrempelige websites (booterservices) die DDoS-as-a-service aanbieden.[209] Deze trend uit het vorige CSBN zet door.

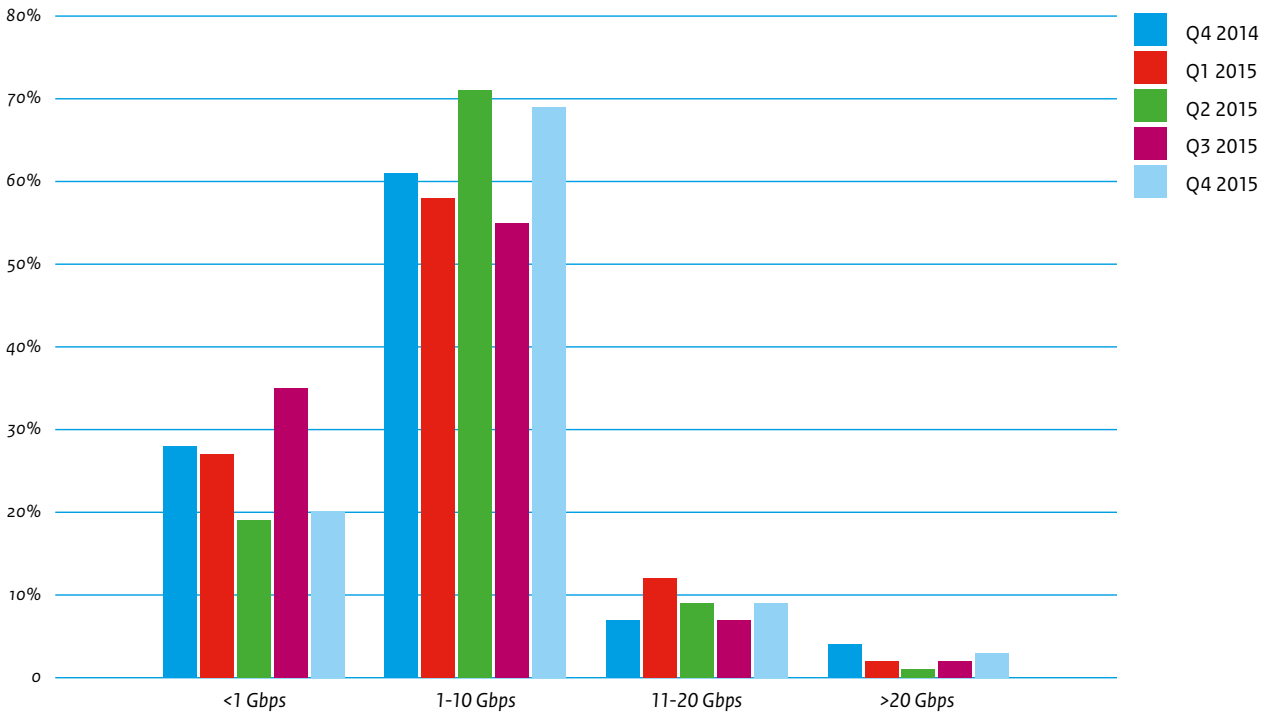
Ook het afgelopen jaar bleven aanvallers zoeken naar nieuwe vormen van amplificatie. Er zijn amplificatieaanvallen gezien door misbruik van NetBIOS, RPC, Sentinel[210], RPC Portmapper[211], DNSSEC[212], TFTP[213], Bittorrent[214]en RIPv1[215]. Hieruit blijkt dat zeer verschillende netwerkdiensten en bijbehorende protocollen voor misbruik vatbaar zijn. Hieronder vallen diensten voor bestandsoverdracht, voor domeinnamen en voor routering. Veel van de misbruikte protocollen zijn niet nieuw. Aanvallers hebben in deze oude protocollen eerder onbekende mogelijkheden gevonden om ze te misbruiken voor amplificatieaanvallen.

Op het internet aangesloten apparatuur, zoals routers, ip-camera's, netwerkhardeschijven en netwerkprinters worden ook misbruikt om DDoS-aanvallen uit te voeren.[216] Deze apparaten worden vaak overgenomen, doordat het managementsysteem bereikbaar is via het internet en een sterk wachtwoord ontbreekt. Tegelijkertijd kan ook het feit dat een dienst op een dergelijk apparaat via het internet beschikbaar is, misbruikt worden om een aanval uit te voeren. Met uitbreiding van het aantal op het internet aangesloten (onbeheerde) apparaten zal deze problematiek waarschijnlijk toenemen.

Omvang, volume en duur van DDoS-aanvallen breken opnieuw records

Uit rapportages van DDoS-aanvallen wereldwijd blijkt dat er weer records zijn gebroken. De grootste gerapporteerde aanvallen betroffen 500 gigabit per seconde.[217] Aanvallen van deze omvang blijven echter uitzonderlijk. Naast de omvang van de aanval uitgedrukt in gigabit per seconde en de duur van de aanval, is het volume – het aantal pakketten dat per seconde wordt verzonden – relevant voor de impact van de aanval.[218] Het verwerken van grote aantallen pakketten heeft soms een grotere impact op routers en andere netwerkapparatuur dan het verwerken van een aanval die groot is in omvang en waarvoor veel bandbreedte vereist is. Aanvallen met veel pakketten per seconde spreken meer geheugen aan in netwerkapparatuur. Hierdoor worden andere verbindingen niet of met vertraging opgezet. Het volume van DDoS-aanvallen wordt uitgedrukt in miljoenen pakketten per seconde.

Figuur 8 **Omvang van DDoS-aanvallen**



Bron: Nationale anti-DDoS Wasstraat (NaWas) van de Stichting Nationale Beheersorganisatie Internet Providers (NBIP).

Uit cijfers van de Nationale anti-DDoS Wasstraat (NaWas) van de Stichting Nationale Beheersorganisatie Internet Providers (NBIP) blijkt dat qua omvang van de aanvallen, op bij hen aangesloten partijen, de relatieve verdeling op hoofdlijnen gelijk blijft. Het 1-10 Gbps bereik blijft het merendeel uitmaken. Aanvallen van meer dan 20 Gbps blijven een uitzondering.

De meeste aanvallen op deelnemers van de NaWas blijven van korte duur, minder dan een kwartier. In ongeveer 10 procent van de gevallen gaat het om aanvallen van langer dan een uur. Over het volume van de aanvallen op deelnemers van de NaWas zijn geen gegevens bekend.

Obfuscatie: het verbergen van criminele activiteit

Malware kan steeds beter worden verborgen

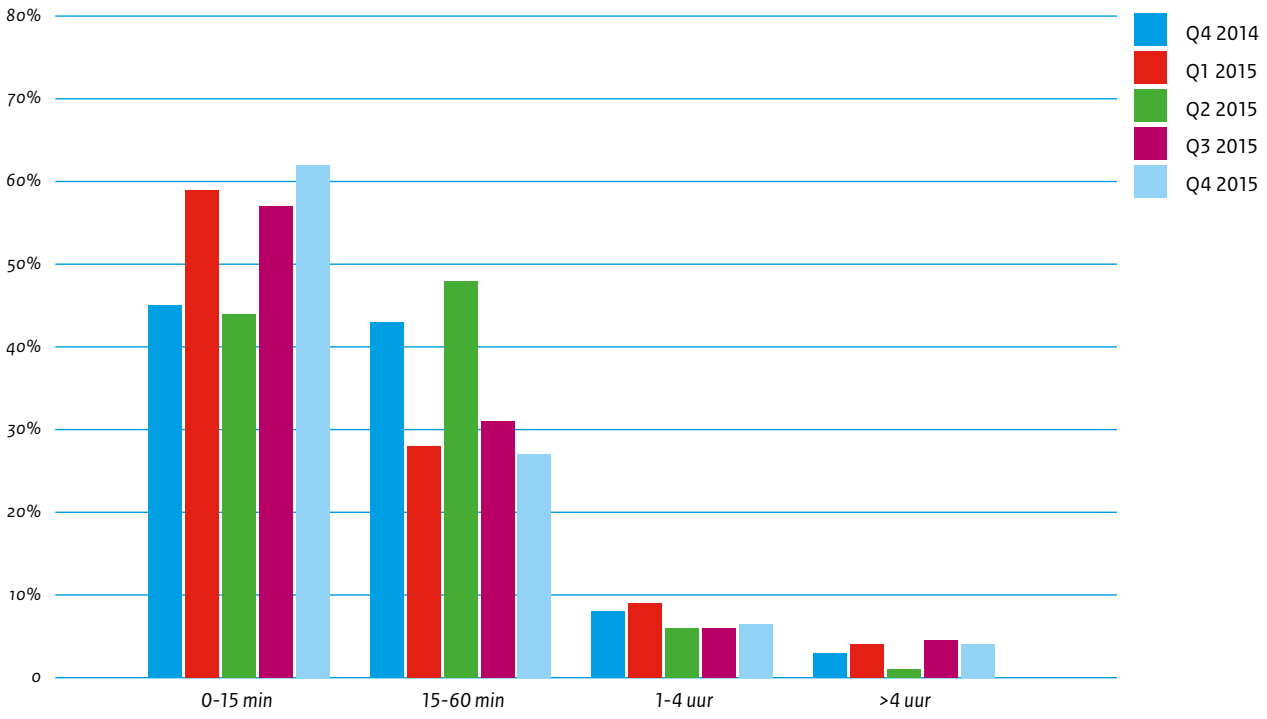
Aanvallers die met malware informatie van het systeem van het slachtoffer buit willen maken, hebben een belang bij het verborgen houden van deze malware. Dat geldt ook voor het wissen van alle sporen als de malware alsnog wordt gedetecteerd. Om dit doel te bereiken worden diverse technieken ingezet.

De USBthief-malware werkt alleen vanaf een usb-stick waar het oorspronkelijk op is geplaatst. Deze malware laat geen sporen achter op het gecompromitteerde systeem.[219] De malware is versleuteld met het hardwareID en de schijfeigenschappen van de usb-stick. Hierdoor is het in principe niet leesbaar zonder deze usb-stick. Ook zijn de bestandsnamen van de malwarebestanden per usb-stick uniek. Dit bemoeilijkt zowel detectie als onderzoek door onderzoekers.

De Cherry Picker-malware, speciaal ontwikkeld voor kassasystemen, is uitgerust met specifieke cleaner activiteiten. Dat maakt het mogelijk om alle sporen van de malware uit te wissen zodra het doel van de malware – het verzamelen van kaartinformatie – bereikt is.[220] Naast deze subtiele aanpak is er ook malware die ervoor kiest om, bij detectie, de gehele harde schijf en daarmee alle sporen te wissen.[221] Een alternatieve strategie wordt door de makers van de Duqu 2.0-malware gevolgd. Hierbij wordt detectie en het achterlaten van sporen voorkomen door de malware uitsluitend in het werkgeheugen van het systeem aanwezig te laten zijn en geen wijzigingen op het systeem door te voeren.[222]

Veelgebruikte firmware vormt een interessant doelwit voor aanvallen, zoals de firmware van routers. Gerichte aanvallen op firmware van (rand)apparatuur lijken nu vooral ingezet te worden door geavanceerde criminele partijen en statelijke actoren. Hierbij is het voor de aanvaller belangrijk dat de infectie niet wordt opgemerkt en na een herinstallatie blijft bestaan. Het is echter goed voorstelbaar dat deze techniek ook voor andere groepen beschikbaar komt.[223]

Figuur 9 **Duur van DDoS-aanvallen**



Bron: Nationale anti-DDoS Wasstraat (NaWas) van de Stichting Nationale Beheersorganisatie Internet Providers (NBIP).

Malware-infecties van firmware

Firmware is software die in het geheugen van specifieke hardware ingeladen is en deze direct aanstuurt, vergelijkbaar met een besturingssysteem bij computers. Deze apparatuur, de hardware, en de daarop ingeladen firmware zijn nauw met elkaar verbonden. Een voorbeeld is firmware voor harde schijven die het daadwerkelijk wegschrijven van gegevens op de magnetische schijf voor zijn rekening neemt. Andere voorbeelden zijn firmware voor videokaarten, smartphones, smartwatches, smart-tv's, routers, ip-camera's en muizen. In het verleden kon firmware vaak maar eenmalig door de fabrikant bij productie ingeladen worden. Tegenwoordig is het vaker mogelijk om firmware op een later moment te updaten. Apparatuur bevat steeds krachtigere processoren en grote hoeveelheden geheugen, waardoor het vaker mogelijk wordt om (delen van) volwaardige besturingssystemen, in het bijzonder Linux, als basis voor de firmware te gebruiken. Hierdoor vervaagt het onderscheid tussen besturingssysteem en firmware en kunnen bekende kwetsbaarheden in een besturingssysteem ook gevolgen hebben voor veel andersoortige apparaten dan computers. Zo kan malware die oorspronkelijk voor gewone computers geschreven is ook die andersoortige apparaten infecteren. De gebruiker verwacht dit vaak niet. Denk hierbij bijvoorbeeld aan auto's[224] of industriële systemen.

Misbruik van bonafide diensten blijft populair

In het vorige CSBN werd misbruik van diensten als Dropbox, Pinterest en Google Docs voor malafide doeleinden al onder de aandacht gebracht. Het misbruiken van deze diensten is aantrekkelijk, omdat verkeer van en naar de diensten vaak standaard versleuteld wordt verstuurd. Ook is communicatie met de diensten op zichzelf niet verdacht. Bedrijven en organisaties blokkeren dit verkeer vaak niet op voorhand.

Ook de afgelopen periode is dit waargenomen. Geavanceerde criminele partijen blijken deze techniek toe te passen. Zo maakt HAMERTOSS, de backdoor van een groep die APT29 wordt genoemd, gebruik van Twitter om legitiem verkeer na te bootsen en voor command-and-control-aansturing (C2) om de malware aan te sturen.[225] Ook Twitter Direct Messages kunnen worden gebruikt om met malware geïnfecteerde systemen aan te sturen.[226] Twee Android-malwarefamilies (OpFake en Marry) maakten gebruik van Facebook als C2-infrastructuur.[227] Daarnaast zet de vermeende Chinese groep admin@338 Dropbox-accounts in als C2-infrastructuur[228] en maakte de Dridex-malware misbruik van Pastebin voor de opslag van malafide VBScript die het in het aanvalsproces gebruikt.[229]

Het gebruik van bonafide diensten heeft voor aanvallers als voordeel dat gebruikers met een vertrouwde domeinnaam communiceren. Zo zijn er via Google Drive phishingaanvallen uitgevoerd op Google-accounts. Dat gebeurde door op een Google Drive-pagina een inlogpagina van Google na te maken.[230] Slachtoffers communiceerden zo met een echt Google-adres (googledrive.com) en vermoedden geen phishing. Ook technische maatregelen kunnen op die manier omzeild worden. Zo omzeilde een onderzoeker beperkingen in de Noscript-extensie van Firefox door de aanvalscode te hosten in de Google Cloud. Het googleapis.com-domein is standaard gewhitelist in deze extensie.[231]

Ook maken aanvallers misbruik van bekende certificaatinstanties om op legitieme wijze een certificaat voor hun malafide dienst te verkrijgen, bijvoorbeeld voor een phishingwebsite.[232][233] Zo zijn certificaten van het Let's Encrypt-initiatief, dat als doel heeft om zoveel mogelijk dataverbindingen te beveiligen, ook al gebruikt voor het beveiligen van een phishingwebsite.[234]

Ten slotte maakt de TURLA-groep clandestien gebruik van satellietcommunicatie om de locatie van C2-servers te maskeren en data te exfiltreren. Veel satellietcommunicatie wordt onversleuteld verzonden en kan in een erg groot gebied ontvangen worden. Dit maakt het voor een kwaadwillende mogelijk om op dit signaal mee te liften en zo gegevens te ontvangen, zonder dat achterhaald kan worden waar de kwaadwillende ontvanger zich precies bevindt. Dit maakt het zeer lastig om de C2-infrastructuur in kaart te brengen en de daders te vinden.[235]

Opsporingsdiensten stellen dat de huidige bijzondere opsporingsbevoegdheden, zoals het aftappen en opnemen van communicatie, nauwelijks meer effectief zijn door versleuteling. Om die reden bevat het wetsvoorstel Computercriminaliteit III de bevoegdheid om, als er sprake is van een misdrijf, onder bepaalde voorwaarden geautomatiseerde werken op afstand binnen te dringen.

Aanvalsvectoren

Malvertising blijft een gevaar voor internetgebruikers

Criminelen blijven malafide advertenties (malvertising) inzetten om internetgebruikers te besmetten met malware. Veel websites gebruiken advertentienetwerken als tussenpersoon voor het samenbrengen van vraag en aanbod van adverteerders en de websites, evenals het daadwerkelijk tonen van de advertentie. Door het brede bereik van deze advertentienetwerken vormen ze een voor criminelen interessant kanaal om malware te verspreiden. Gebruikers met niet bijgewerkte software zijn daarbij vooral het doelwit.

Meerdere malen zijn advertentienetwerken door malafide advertenties getroffen. Hierdoor verstuurden websites met een wereldwijd publiek malware naar hun bezoekers.[236] Deze websites hebben bij elkaar ruim twee miljard bezoekers per maand en bieden een groot aanvalsoppervlak. Ook populaire Nederlandse websites zijn getroffen.[237]

Via real-time-bidding-advertentienetwerken worden advertenties aan specifieke gebruikers(groepen) getoond.[238] Ook in de afgelopen rapportageperiode is deze methode gebruikt. Hierbij zijn aanvullende technieken ingezet, zoals fingerprinting.[239] Hiermee

wordt eerst het systeem van het mogelijke slachtoffer in kaart gebracht. Pas na een afweging wordt (een specifieke vorm van) malware aangeboden. Op deze wijze wordt alleen malware aan kwetsbare systemen aangeboden. Daarnaast wordt bijvoorbeeld ook alleen malware afgeleverd op computers met een ip-adres van een internetprovider voor consumenten. Ook kan op basis van de netwerkpakketjes vastgesteld worden welk besturingssysteem het mogelijke slachtoffer gebruikt.[240]

Al deze technieken samen maken het kostenefficiënter voor de aanvallers om een dergelijke campagne uit te voeren. Daarnaast wordt het lastiger voor onderzoekers en advertentienetwerken om actuele malwarecampagnes te achterhalen. De malware wordt bijvoorbeeld niet aan Linuxmachines en loksystemen, zogenoemde honeypots, aangeboden.

Bescherming tegen malvertising is niet eenvoudig. Het verspreiden van malware via de advertenties is mogelijk doordat advertenties door grote websites worden ingekocht bij advertentienetwerken. Deze netwerken verkopen de advertentieruimte real-time en kunnen deze vanwege de opzet van het advertentiesysteem niet controleren op malware. Wanneer malware zijn weg vindt naar de advertenties, kunnen systemen besmet worden die niet volledig geüpdatet zijn. Het up-to-date houden van systemen is dus een methode om besmetting door malvertising tegen te gaan. Een andere maatregel is het gebruik van adblockers. Deze software blokkeert de advertenties in zijn geheel. Hieraan kleven andere nadelen: de gebruiker krijgt geen advertenties meer te zien, daarmee wordt het verdienmodel van websites geraakt.

Javascript ingezet voor malafide doeleinden

Populaire Javascriptbibliotheken bieden aanvallers veel mogelijkheden. Alle moderne en veelgebruikte webbrowsers ondersteunen Javascript. Zo ontstaat een groot aanvalsoppervlak bij veel gebruikers. Tegelijkertijd is het een krachtige tool om rijke functionaliteiten aan websites toe te voegen. Het simpelweg uitzetten van ondersteuning voor Javascript is daarom geen oplossing.

Cloudflare beschreef een voorbeeld waarbij Javascriptbibliotheken[241] en Javascript in advertentienetwerken[242] werden ingezet voor het uitvoeren van DDoS-aanvallen. De afgelopen periode zien we dat Javascript op diverse andere manieren voor malafide doeleinden kan worden ingezet. Zo trachtten criminelen de systemen van gebruikers te infecteren via Javascript-bijlagen bij e-mail.[243] Op Github verscheen een volledig Javascript-gebaseerde bot die via Twitter kan worden aangestuurd.[244] Daarnaast blijken criminelen Javascript ook als dropper in te zetten.[245] Javascript is daarnaast ingezet om de identiteit van Chinese Tor- en VPN-gebruikers te achterhalen.[246] Ook is het gebruikt om de router van gebruikers aan te vallen en bijvoorbeeld de DNS-instellingen te veranderen. Hierdoor wordt verkeer onderschept en worden slachtoffers richting phishingsites gestuurd.[247]

Gebruik van gestolen sleutelmateriaal

Digitale certificaten hebben onder andere als doel om de eindgebruiker te helpen om de authenticiteit van een bron of dienst vast te stellen. Wanneer een dienst op een juiste wijze gebruik maakt van een vertrouwd certificaat, geeft de applicatie aan de eindgebruiker geen waarschuwingen: de verbinding is immers vertrouwd. Voor de gebruiker kan het eerder vertrouwen wekken, zoals bij een groene adresbalk in de browser als het certificaat voor de website correct is en uitgegeven is door een vertrouwde instantie.

Criminelen trachten dit vertrouwen in certificaten uit te buiten om hun malafide activiteiten extra vertrouwd over te laten komen. In sommige gevallen maken de criminelen hierbij misbruik van gestolen sleutelmateriaal om bijvoorbeeld malware digitaal te ondertekenen.[248][249][250] Naar verluidt verkopen criminelen dergelijke sleutels ook op het dark web voor prijzen tussen de 600 en 900 dollar.[251]

Toename in misbruik van open bronnen en sociale media

In de afgelopen rapportageperiode is open informatie vaker misbruikt. Daarbij gaat het om informatie uit eerdere incidenten en om doxing. Dit was bijvoorbeeld het geval bij het online plaatsen van de gegevens van 1.400 Amerikaanse militairen en ambtenaren.[252]

Criminelen zijn niet alleen geïnteresseerd in informatie op sociale media. Ze willen deze media ook misbruiken. Zo richt de Mooseworm zich op (thuis)routers om in te kunnen breken op communicatie met sociale netwerken. Zo kunnen likes, views en volgers worden gegenereerd voor accounts op deze netwerken.[253] Mogelijk kan hiermee geld verdiend worden.

(Spear-)phishing blijft populair

Phishingcampagnes blijven een populair middel om gegevens van slachtoffers buit te maken of om systemen te besmetten met malware. Phishing- en spearphishing-e-mails worden steeds beter en overtuigender. Zo maken ze gebruik van buitgemaakte naam- en adresgegevens om gepersonaliseerde phishing-e-mails te sturen.[254] Voor ontvangers is phishing-e-mail vaak niet meer te onderscheiden van legitieme e-mail van een organisatie. De namen en logo's van veel bekende grote Nederlandse bedrijven worden misbruikt om gebruikers te misleiden.[255] Ook wordt er qua toon aangesloten bij gangbare communicatie van het betreffende bedrijf in de gegeven periode.[256] In bepaalde gevallen werd de communicatiestijl van het bedrijf tijdens de presentatie van kwartaalcijfers door criminelen geanalyseerd en gekopieerd om een zo realistisch mogelijke phishing-e-mail op te stellen. Het moment van presentatie van deze cijfers werd bovendien door de criminelen aangegrepen om hun phishingcampagne uit te voeren.

Conclusie en vooruitblik

Ransomware ontwikkelt zich verder en blijft een interessant middel voor financieel gewin. Ook wordt het steeds gerichter ingezet. Zo wordt er gefilterd op het besturingssysteem waar de gebruiker mee werkt, evenals zijn locatie, ip-adres en softwareversies. Op deze wijze proberen actoren ook ontdekking door informatiebeveiligingsonderzoekers te voorkomen.

De hoeveelheid malware op mobiele apparaten neemt sterk toe. Het is de verwachting dat deze trend zich voortzet. Mobiele apparaten worden steeds belangrijker in het dagelijks leven en steeds meer (financiële) activiteiten vinden ermee plaats. Hierdoor wordt het een steeds interessanter doelwit. Ook andere alledaagse apparaten kunnen in het toekomst dienen als aanvalsvector voor bijvoorbeeld ransomware.

Actoren proberen vertrouwde softwarebronnen, zoals appstores, te besmetten. Zo kunnen ze malware verspreiden of kunnen ze ongeautoriseerd toegang krijgen tot het systeem dat hierdoor geraakt is. Het bewaken van de integriteit van de gehele productketen is noodzakelijk om de integriteit van software en producten te bewaren en infecties te voorkomen.

Malware kan steeds beter worden verborgen en meer gericht worden aangeboden om zo (vroegtijdige) detectie te voorkomen en om voet aan de grond te houden op het systeem. Actoren blijven hierdoor zoveel mogelijk onder de radar. De investeringen om kwetsbaarheden in bijvoorbeeld de firmware van (rand-)apparatuur te misbruiken lijken momenteel nog hoog. Hierdoor is het niet waarschijnlijk dat er op grote schaal misbruik van wordt gemaakt. Wel biedt het mogelijkheden voor zeer gerichte aanvallen op waardevolle doelen.
Malvertising via advertentienetwerken blijft een effectieve methode om malware met behulp van exploitkits te verspreiden. In de afgelopen periode raakte dit ook populaire Nederlandse websites. Omdat de methode zo aantrekkelijk is voor aanvallers is het de verwachting dat deze aanvalsmethode ook in de komende tijd ingezet blijft worden.

Nieuwe amplificatiemethoden gaan de effectiviteit van DDoS-aanvallen verder vergroten. Gezien het grote aantal te misbruiken diensten en protocollen is het de verwachting dat deze trend zich ook in de toekomst doorzet. De drempel voor het uitvoeren van DDoS-aanvallen blijft laag, waardoor bijvoorbeeld jongeren ze inzetten tegen scholen.

Tot slot blijft Javascript ingezet worden voor malafide doeleinden. Het wordt namelijk door alle moderne en veelgebruikte browsers ondersteund en bovendien op het systeem van de gebruiker uitgevoerd. Javascript biedt zo de mogelijkheid om het systeem van de gebruiker direct in te zetten, bijvoorbeeld voor een DDoS-aanval. Daarnaast biedt het de mogelijkheid om het systeem van de gebruiker te verkennen, voordat er echt kwaadaardige code wordt gestuurd. Het is de verwachting dat het aantal methoden waar Javascript kwaadaardig kan worden ingezet verder toeneemt.

Noten

176 https://www.politie.nl/nieuws/2015/september/16/11-cybercriminelen-aangehouden.html, geraadpleegd op 5 juli 2016.

177 http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/. Eerder waren er al voor de Mac ransomwareversies die uitsluitend de browser blokkeerden en niet het hele systeem zelf. Door middel van oplichting wordt vervolgens geprobeerd om geld los te krijgen. https://blog.malwarebytes.org/exploits-2/2013/07/qa-about-the-latest-html-ransomware-affecting-mac-os-x-users/.

178 Bron: politie en http://www.welivesecurity.com/wp-content/uploads/2016/02/Rise_of_Android_Ransomware.pdf, geraadpleegd op 5 juli 2016.

179 http://www.symantec.com/connect/blogs/dawn-ransomwear-how-ransomware-could-move-wearable-devices, geraadpleegd op 5 juli 2016.

180 https://securityledger.com/2015/11/ransomware-works-on-smart-tvs-too/, geraadpleegd op 5 juli 2016.

181 http://www.cio.com/article/3052553/server-software-poses-soft-target-for-ransomware.html#tk.rss_security, geraadpleegd op 5 juli 2016. Zie ook de al in CSBN 2015 gesignaleerde Ransomweb die de database van een gecompromitteerde webserver versleuteld. https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html, geraadpleegd op 5 juli 2016.

182 http://blog.talosintel.com/2016/04/jboss-backdoor.html, http://blog.talosintel.com/2016/03/samsam-ransomware.html, geraadpleegd op 5 juli 2016.

183 Bron: politie.

184 https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/, geraadpleegd op 5 juli 2016.

185 https://www.secureworldexpo.com/new-ransomware-threatens-publish-personal-information, geraadpleegd op 5 juli 2016.

186 http://blog.linuxmint.com/?p=2994, geraadpleegd op 5 juli 2016.

187 http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/, geraadpleegd op 5 juli 2016.

188 http://www.computerworld.com/article/3044728/security/cyberespionage-groups-are-stealing-digital-certificates-to-sign-malware.html, geraadpleegd op 5 juli 2016.

189 https://blog.malwarebytes.org/mac/2015/09/xcodeghost-malware-infiltrates-app-store/, geraadpleegd op 5 juli 2016.http://researchcenter.paloalto-networks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/, geraadpleegd op 5 juli 2016.

190 http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/, geraadpleegd op 5 juli 2016.

191 http://www.rtlz.nl/tech/36000-nederlanders-downloadden-malware-app-app-store, geraadpleegd op 5 juli 2016.

192 https://www.sophos.com/en-us/press-office/press-releases/2006/10/ipod-ships-with-virus.aspx, https://www.sophos.com/fr-fr/press-office/press-releases/2007/01/tomtom.aspx, geraadpleegd op 5 juli 2016.

193 https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_US.pdf, http://www.ibtimes.co.uk/amazon-selling-least-30-brands-cheap-chinese-android-tablets-infected-cloudsota-malware-1528442, geraadpleegd op 5 juli 2016.

194 Bron: politie.

195 https://www.theiphonewiki.com/wiki/Malware_for_iOS, https://blog.fortinet.com/post/ios-malware-does-exist, geraadpleegd op 5 juli 2016.

196 https://www.fireeye.com/blog/threat-research/2015/11/ibackdoor_high-risk.html, geraadpleegd op 5 juli 2016.

197 http://www.theverge.com/2016/3/31/11336542/apple-corporate-iphone-security-sidestepper-attack-malware, geraadpleegd op 5 juli 2016.

198 http://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/, geraadpleegd op 5 juli 2016.

199 https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/, geraadpleegd op 5 juli 2016.

200 https://tweakers.net/nieuws/107138/stroomstoring-in-oekraine-werd-veroorzaakt-door-gerichte-inzet-malware.html

201 https://github.com/reverse-shell/routersploit, geraadpleegd op 5 juli 2016.

202 https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf

203 http://www.wired.com/2015/04/therealdeal-zero-day-exploits/, geraadpleegd op 5 juli 2016.

204 http://betanews.com/2015/11/20/zerodium-reveals-price-list-for-zero-day-exploits/, geraadpleegd op 5 juli 2016.

205 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

206 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

207 https://www.security.nl/posting/460316/Java-backdoor+besmet+440_000+computers+wereldwijd, geraadpleegd op 5 juli 2016.

208 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report, geraadpleegd op 5 juli 2016.

209 Zie ook CSBN 2015.

210 https://blogs.akamai.com/2015/10/netbios-rpc-portmap-and-sentinel-reflection-ddos-attacks.html, geraadpleegd op 5 juli 2016.

211 http://blog.level3.com/security/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/, geraadpleegd op 5 juli 2016.

212 https://www.stateoftheinternet.com/downloads/pdfs/2016-state-of-the-internet-threat-advisory-dnssec-ddos-amplification-attacks.pdf

213 http://researchrepository.napier.ac.uk/8746/, geraadpleegd op 5 juli 2016.

214 http://arstechnica.com/security/2015/08/how-bittorrent-could-let-lone-ddos-attackers-bring-down-big-sites/, geraadpleegd op 5 juli 2016.

215 https://blogs.akamai.com/2015/07/ripv1-reflection-ddos-making-a-comeback.html, geraadpleegd op 5 juli 2016.

216 http://www.computerworld.com/article/2921559/malware-vulnerabilities/malware-infected-home-routers-used-to-launch-ddos-attacks.html, http://www.computerworld.com/article/2996079/internet-of-things/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html, geraadpleegd op 5 juli 2016.

217 https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf

218 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/2015-q3-cloud-security-report.pdf

219 http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/, geraadpleegd op 5 juli 2016.

220 https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/, geraadpleegd op 5 juli 2016.

221 http://blogs.cisco.com/security/talos/rombertik, geraadpleegd op 5 juli 2016.

222 https://cdn.securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

223 Virustotal.com, een website die bestanden analyseert om te detecteren of het om malware gaat, biedt sinds 2016 ook de mogelijkheid om firmware te controleren. http://blog.virustotal.com/2016/01/putting-spotlight-on-firmware-malware_27.html.

224 http://money.cnn.com/2015/08/06/technology/tesla-hack/index.html, geraadpleegd op 5 juli 2016.

225 https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html, geraadpleegd op 5 juli 2016.

226 https://github.com/PaulSec/twittor, geraadpleegd op 5 juli 2016.

227 http://news.softpedia.com/news/two-mobile-banking-trojans-used-facebook-parse-as-c-c-server-497597.shtml, geraadpleegd op 5 juli 2016.

228 http://news.softpedia.com/news/malware-that-hides-c-c-server-on-dropbox-detected-in-the-wild-496951.shtml, geraadpleegd op 5 juli 2016.

229 https://blog.gdatasoftware.com/2015/06/24285-new-dridex-infection-vector-identified, geraadpleegd op 5 juli 2016.

230 https://www.elastica.net/2015/07/elastica-cloud-threat-labs-discovered-latest-google-drive-phishing-campaign/, geraadpleegd op 5 juli 2016.

231 http://labs.detectify.com/2015/06/30/using-google-cloud-to-bypass-noscript/, geraadpleegd op 5 juli 2016.

232 http://news.netcraft.com/archives/2015/10/12/certificate-authorities-issue-hundreds-of-deceptive-ssl-certificates-to-fraudsters.html, geraadpleegd op 5 juli 2016.

233 http://news.netcraft.com/archives/2015/10/13/fraudsters-use-paypal-office-com-ov-certificate-for-phishing.html, geraadpleegd op 5 juli 2016.

234 http://www.infoworld.com/article/3019926/security/cyber-criminals-abusing-free-lets-encrypt-certificates.html , geraadpleegd op 5 juli 2016.

235 https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/ , geraadpleegd op 5 juli 2016.

236 https://www.security.nl/posting/464560/Advertenties+op+populaire+websites+verspreiden+ransomware , geraadpleegd op 5 juli 2016.

237 https://blog.fox-it.com/2016/04/11/large-malvertising-campaign-hits-popular-dutch-websites/, geraadpleegd op 5 juli 2016.
238 Zie ook CSBN 2015.
239 https://blog.malwarebytes.org/threat-analysis/2016/03/ofp/, geraadpleegd op 5 juli 2016.
240 http://www.pcworld.com/article/3030419/security/the-neutrino-exploit-kit-has-a-new-way-to-detect-security-researchers.html, geraadpleegd op 5 juli 2016.
241 https://blog.cloudflare.com/an-introduction-to-javascript-based-ddos/, geraadpleegd op 5 juli 2016.
242 https://blog.cloudflare.com/mobile-ad-networks-as-ddos-vectors/, geraadpleegd op 5 juli 2016.
243 https://www.trustwave.com/Resources/SpiderLabs-Blog/Cryptowall-and-phishing-delivered-through-JavaScript-Attachments/, https://blogs.technet.microsoft.com/mmpc/2016/04/18/javascript-toting-spam-emails-what-should-you-know-and-how-to-avoid-them/, geraadpleegd op 5 juli 2016.
244 https://github.com/Plazmaz/JSBN, geraadpleegd op 5 juli 2016.
245 http://labs.bromium.com/2015/06/12/oh-look-javascript-droppers/, geraadpleegd op 5 juli 2016.
246 https://www.alienvault.com/open-threat-exchange/blog/watering-holes-exploiting-jsonp-hijacking-to-track-users-in-china, geraadpleegd op 5 juli 2016.
247 http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-devices-used-to-execute-dns-malware-against-home-routers/, geraadpleegd op 5 juli 2016.
248 http://www.theregister.co.uk/2015/06/15/duqu2_stolen_foxconn_cert/, geraadpleegd op 5 juli 2016.
249 http://research.zscaler.com/2016/01/yet-another-signed-malware-spymel.html, geraadpleegd op 5 juli 2016.
250 https://securityintelligence.com/certificates-as-a-service-code-signing-certs-become-popular-cybercrime-commodity/, geraadpleegd op 5 juli 2016.
251 http://www.theregister.co.uk/2015/11/04/code_signing_malware/, geraadpleegd op 5 juli 2016.
252 http://www.theguardian.com/world/2015/aug/13/isis-hacking-division-releases-details-of-1400-americans-and-urges-attacks, geraadpleegd op 5 juli 2016.
253 http://www.welivesecurity.com/2015/05/26/dissecting-linuxmoose/ , geraadpleegd op 5 juli 2016.
254 http://www.bbc.co.uk/news/technology-35996408, geraadpleegd op 5 juli 2016.
255 Zie voor een recent overzicht https://www.fraudehelpdesk.nl/sub-vragen/phishingmails/, geraadpleegd op 5 juli 2016.
256 Bron: interviews met diverse sectoren.

Beveiligingsbewustzijn van gebruikers kan de ontwikkeling van social engineering niet bijhouden

4 Weerbaarheid: Kwetsbaarheden

Kwetsbaarheden in software vormen de achilleshiel van digitale veiligheid. Het up-to-date houden van alle systemen is een uitdaging voor zowel organisaties als thuisgebruikers. Tegelijk blijven de toepassingen van ICT groeien en hebben softwarekwetsbaarheden impact op de fysieke veiligheid van gebruikers en openbare ruimte, bijvoorbeeld bij kwetsbaarheden in software in auto's.

Een kwetsbaarheid is een eigenschap van ICT, een organisatie of gebruiker die actoren kunnen misbruiken om hun doelen te bereiken of die door een natuurlijke of technische gebeurtenis kan leiden tot verstoringen. Dit hoofdstuk gaat in op de ontwikkelingen op het gebied van kwetsbaarheden.

Organisatorische ontwikkelingen

Gebrek aan controleerbaarheid van de keten maakt ICT kwetsbaar

De softwareindustrie lijkt steeds meer op een assemblage-industrie,[257] met als gevolg veel hergebruik van bestaande componenten. Net als in de keten van bijvoorbeeld vliegtuigbouw is het wenselijk om een aantal zaken exact na te kunnen gaan: waar een onderdeel vandaan komt, dat het een origineel onderdeel is (zonder aanpassingen), waar het onderdeel in gebruikt wordt en wat de staat van onderhoud is.

In de rapportageperiode hebben diverse incidenten plaatsgevonden waarbij deze keten kwetsbaar bleek. Een wijziging in de JavaScriptbibliotheek NPM (die door veel webapplicaties wordt gebruikt) verwijderde functionaliteit waar veel van die applicaties afhankelijk van waren. Dit leidde tot het plotseling niet meer werken van die applicaties.[258]

In augustus 2015 zijn er kwetsbaarheden in voorgeïnstalleerde software op Lenovoproducten aangetroffen.[259] Lenovo maakte hierbij gebruik van aangepaste firmware die een schone Windows-installatie voorzag van de Lenovo-tools. Na de vondst van een kwetsbaarheid besloot Lenovo dit mechanisme te verwijderen. De Taiwanese fabrikant D-Link lekte per ongeluk een code-signing-sleutel online uit. Daardoor konden kwaadwillenden software van een legitieme D-Link ondertekening voorzien.[260]

Verder bleek ook nog een aangepaste firmware met een backdoor voor een aantal Cisco-routers in omloop.[261] Ook Juniper maakte bekend dat er bij een interne audit twee ernstige problemen in ScreenOS aan het licht waren gekomen. Deze problemen zouden zijn geïntroduceerd door "ongeautoriseerde code" in ScreenOS waarvan het bedrijf niet op de hoogte was.[262] Netwerkapparatuur van deze fabrikanten wordt bijna overal ter wereld gebruikt; aanvallers kunnen hiermee potentieel veel schade aanrichten.

Security is geen kerncompetentie van softwareontwikkelaars

Bij mbo- en hbo-opleidingen voor softwareontwikkeling wordt weinig aandacht besteed aan softwarebeveiliging.[263] Netwerk- en platformbeveiliging zijn volwassen beroepscompetenties; daarvan wordt een basiskennisniveau verondersteld onder ICT-specialisten die opgeleid worden tot softwareontwikkelaar. Softwarebeveiliging daarentegen blijft als onderwerp beperkt tot wo-niveau, specifieke opleidingen of keuzevakken die ICT-studenten alleen volgen als zij daar zelf belangstelling voor hebben.

Omdat dit fenomeen wereldwijd aan de orde is bestaat er geen algemeen aanvaarde norm die ontwikkelaars motiveert hier aandacht voor te hebben. Ontwikkelorganisaties concentreren

zich vooral op functionaliteit en snelheid. Deze impasse leidt ertoe dat software bij voltooiing vele kwetsbaarheden bevat die achteraf pas ontdekt en verholpen kunnen worden.

Connectiviteit van industriële controlesystemen neemt toe

Industriële controlesystemen (ICS)[264] worden vaker verbonden met ICT-netwerken en daarmee (direct of indirect) met het internet. ICT-netwerken kennen echter vaak een ander, meestal lager vertrouwensniveau met bijbehorende beveiligingsmaatregelen dan voor de gekoppelde ICS is vastgesteld. Dit kan leiden tot situaties waarin deze systemen kwetsbaar zijn voor aanvallen.

Up-to-date houden van alle apparaten en software is een uitdaging

Veel datalekken bij bedrijven zijn mogelijk door kwetsbaarheden die al langer dan een jaar bekend zijn, maar nog niet verholpen door de getroffen organisatie.[265] Veel organisaties investeren daarom in een gedegen updatebeleid, hoewel een deel nog achterblijft. Om software op werkplek-pc's en servers te updaten bieden ontwikkelaars van besturingssystemen ook steeds meer mogelijkheden.[266] [267]

Veel organisaties gebruiken legacysystemen, verouderde systemen waarvoor geen updates meer worden uitgegeven. Het is niet altijd mogelijk om deze systemen te moderniseren of er een apart netwerk voor in te richten. Daardoor blijven ze kwetsbaar.[268] Andere apparaten dan computers zijn ook niet altijd voorzien van een eenvoudig updatemechanisme. Organisaties die via een bring-your-own-devicebeleid toestaan dat medewerkers eigen smartphones en tablets gebruiken om bedrijfsnetwerken en -informatie benaderen, kunnen niet controleren of gebruikers updates installeren op die (eigen) apparaten. Dit bemoeilijkt de beheersing van kwetsbaarheden.

Kwetsbaarheid voor geavanceerde dreigingen onbekend

Tijdens onderzoeken constateren de inlichtingendiensten dat de beschermingsmaatregelen van veel bedrijven slechts bestaan uit de inzet van commerciële antivirusproducten. Veel bedrijven realiseren zich niet dat aanvallen van geavanceerde dreigingen, zoals statelijke actoren, verdergaan dan de inzet van al bekende malware. Deze statelijke actoren plegen vaker aanvallen waarbij er geen gebruik wordt gemaakt van bestanden die op zichzelf kwaadaardig zijn,[269] maar door middel van scans vinden deze actoren kwetsbaarheden in systemen die vervolgens worden uitgebuit.

Een andere trend is dat buitenlandse actoren zich steeds vaker richten op sociale netwerken of de thuisomgeving van hun doelwitten. Waar ze eerder conventionele methoden voor bijvoorbeeld afluisteren en volgen gebruikten, richten buitenlandse actoren zich nu meer op digitale middelen. De afgelopen jaren is geïnvesteerd in detectie binnen overheids- en bedrijfsnetwerken, bijvoorbeeld met het Nationaal Detectie Netwerk (NDN). Inlichtingendiensten hebben waargenomen dat mede hierdoor aanvallers zich zijn gaan richten op netwerken die minder goed beveiligd zijn, zoals de thuisomgeving. Vooral infectie van mobiele apparaten is populair; dit biedt toegang tot verschillende applicaties, maar de telefoon zelf kan ook fungeren als een op afstand bedienbare microfoon of camera. In intergouvernementele instellingen zijn diverse hoge ambtenaren slachtoffer geweest van dergelijke infecties.[270]

Hoogpublicitaire kwetsbaarheden worden gemeengoed

De eerder geconstateerde trend van publiciteitscampagnes rondom technische kwetsbaarheden[271] zet zich voort.[272] Onderzoekers maken een afweging tussen het creëren van voldoende bewustzijn voor een ernstige kwetsbaarheid enerzijds en het gevaar van het overdrijven van een alledaagse kwetsbaarheid anderzijds.

Het overdrijven van kwetsbaarheden kan leiden tot het Cry Wolf-effect.[273] Door een teveel aan loze waarschuwingen kan de aandacht verslappen en is men niet meer alert wanneer er daadwerkelijk iets ernstigs aan de hand is. Badlock (zie kader) lijkt dit risico breder onder de aandacht te hebben gebracht. De ergernis die daardoor is ontstaan, geeft mogelijk aanleiding tot heroverweging van de marketingstrategie die sommige beveiligingsonderzoekers toepassen.

Badlock blijkt mee te vallen

Op 23 maart 2016 werd de Badlock-kwetsbaarheid vooraangekondigd voor publicatie op 12 april.[274] De kwetsbaarheid kreeg een naam, logo en website, maar er werden nog geen details over de aard en ernst van de kwetsbaarheid gepresenteerd. Er werd slechts vermeld dat de kwetsbaarheid in SMB zat, een protocol om onder andere bestanden via een lokaal netwerk te delen dat gebruikt wordt in Microsoft Windows en de opensourcesoftware Samba.

Systeembeheerders hielden rekening met een ernstige kwetsbaarheid die onmiddellijk gepatcht moest worden op het moment van bekendmaking.[275] Na bekendmaking van de details en publicatie van de updates waren beveiligingsonderzoekers verbaasd: er ontstond kritiek op de hype die was gecreëerd en de kwetsbaarheid werd omgedoopt tot Sadlock.[276] Hoewel werd onderkend dat het nog steeds een kwetsbaarheid was die serieus moest worden genomen,[277] hekelden deskundigen de onnodige inzet van mankracht en de aandacht die dit afleidde van andere, ernstigere kwetsbaarheden.[278]

Ontwikkelingen aan de gebruikerszijde

Mobiele apparaten zijn vaak niet voorzien van de laatste updates

De markt voor smartphones en tablets is zeer innovatief en concurrerend. Fabrikanten brengen daarom soms meerdere keren per jaar nieuwe modellen uit om voorop te blijven. Dit leidt tot een grote hoeveelheid verschillende apparaten, waarop afhankelijk van het moment van uitkomen verschillende versies van besturingssystemen draaien.

Vanwege de korte periode waarin fabrikanten deze apparaten leveren, twee jaar is gangbaar, publiceren veel fabrikanten al snel geen updates voor een bepaald ouder toestel. Gebruikers van oude apparaten kunnen daardoor geen updates meer installeren. Softwarekwetsbaarheden worden dan niet verholpen op die apparaten.

Tegelijkertijd is er een verschuiving van het internetgebruik onder thuisgebruikers zichtbaar. Oorspronkelijk was de pc of laptop het aangewezen apparaat in een huishouden om te gebruiken voor internettoegang, maar inmiddels is die rol overgenomen door tablets, smartphones en smart-tv's.[279] Het belang van het up-to-date houden van deze andere apparaten is daarmee nog groter geworden.

Bewustzijn van gebruikers kan ontwikkeling van social engineering niet bijhouden

Cybercriminelen blijven hun pogingen om gebruikers tot acties over te halen verbeteren. Gebruikers trappen in phishing-e-mail en telefonische scams, hoewel het percentage bij algemene phishingcampagnes laag blijft. Wanneer social engineering specifiek wordt gericht op individuele sectoren, organisaties of personen, stijgt dit percentage aanzienlijk.[280] Door gerichtere informatie wordt meer vertrouwen gewonnen van de geadresseerde waardoor één slachtoffer binnen een organisatie vaak al voldoende is voor een aanvaller om zijn doel te bereiken.

Bewustwordingscampagnes voor eindgebruikers hebben voornamelijk effect wanneer zij gericht zijn op gedragsverandering in een specifieke situatie. Zo is de campagne van de Nederlandse banken (Hang op, klik weg, bel uw bank) succesvol. Deze campagne draagt aantoonbaar bij aan gedragsverandering.[281] Campagnes die generiek opgezet zijn en gericht zijn op herkenning van dreigingen zoals phishing en social engineering in brede zin, zijn minder effectief.

In deze rapportageperiode is sprake van een toename aan telefonische oplichters die slachtoffers proberen te overtuigen dat zij een probleem hebben met hun computer. Vervolgens worden ze overgehaald om bepaalde software te installeren. Dit betreft vaak malware waarmee de oplichter de controle over de computer kan overnemen, zoals RAT's.

In eerste instantie deden oplichters zich voornamelijk voor als medewerkers van Microsoft.[282] Nadat daar veel waarschuwingen voor werden gegeven, werden ook de namen van andere organisaties hiervoor misbruikt. In veel gevallen ging het om de naam van telecom- of internetproviders. Soms werd ook gesproken uit naam van een overheidspartij.[283]

Internet der dingen rukt op en maakt gebruikers fysiek kwetsbaar

Het internet der dingen is geen toekomstvoorspelling meer. Vele soorten toepassingen en apparaten zijn met internet verbonden. Fabrikanten lijken onvoldoende bewust van de risico's hiervan of missen de technische mogelijkheden. Dat leidt ertoe dat er producten op de markt komen die nog diverse softwarekwetsbaarheden bevatten.

Autofabrikanten ervaren nu de problematiek van het verhelpen van softwarekwetsbaarheden. In de zomer van 2015 zijn auto's van Ford, Range Rover, Toyota, Chrysler, Tesla en Chevrolet kwetsbaar gebleken.[284] Sommige modellen konden niet automatisch geüpdatet worden. In sommige gevallen waren kostbare terugroepacties noodzakelijk. Chrysler bracht in september een update op usb-stick uit en stuurde deze per post aan de autobezitters.[285]

Deze en andere kwetsbaarheden in boordcomputers van auto's zijn rechtstreeks van invloed op de verkeersveiligheid. Onderzoekers hebben onder meer aangetoond de remmen van een auto op afstand te kunnen bedienen. Dit kan inzittenden in levensgevaar brengen wanneer dit bijvoorbeeld op de snelweg gebeurt.[286]

Veel kwetsbaarheden kunnen worden voorkomen als security de juiste aandacht krijgt in de softwareontwikkelingscyclus. Het blijft echter ook noodzakelijk om voor latere kwetsbaarheden een goed en veilig updatemechanisme te hebben. Een terugroepactie kan aanzienlijk in de kosten lopen. Bij het versturen van een usb-stick met een software-update is geen zekerheid of alle gebruikers die ook toepassen. Bovendien kunnen criminelen hier misbruik van maken. Als de update niet digitaal ondertekend is en daar niet op wordt gecontroleerd, kan een crimineel een kwaadaardige update op dezelfde manier aan (gerichte) slachtoffers aanbieden.

Technische ontwikkelingen

TLS blijft speelbal van kwetsbaarheden en maatregelen

Transport Layer Security (TLS) wordt veel gebruikt in beveiligde verbindingen op internet. Het bekendste gebruik ervan is https, om websiteverkeer over een beveiligde verbinding te laten verlopen. Dit alomtegenwoordige gebruik maakt het voor beveiligingsonderzoekers prestigieus om kwetsbaarheden in TLS te ontdekken.

De rapportageperiode kende opnieuw diverse nieuwe kwetsbaarheden en aanvalsmethoden in TLS-toepassingen. Vooral de Drown-kwetsbaarheid baarde in maart 2016 enig opzien.[287] Hierbij wordt misbruik gemaakt van een server die naast TLS ook het verouderde SSLv2 aanbiedt. Hoewel al jaren wordt aanbevolen SSLv2 uit te schakelen, bleken nog diverse websites kwetsbaar voor deze aanvalsmethode.[288] De kans dat aanvallen op basis van Drown zich daadwerkelijk manifesteren is echter beperkt vanwege de complexiteit van de kwetsbaarheid.

Adobe Flash Player zorgt voor veel kwetsbaarheden, voorlopig niet opgelost

In 2015 zijn meer dan 330 kwetsbaarheden verholpen in Adobe Flash Player, waaronder acht zero-daykwetsbaarheden.[289] De top tien van meestgebruikte kwetsbaarheden door exploitkits wordt geheel ingenomen door Flash Player.[290] Mede door de komst van html5, waarmee veel functies die voorheen in Flash werden ontwikkeld zonder plug-in beschikbaar zijn geworden in moderne browsers, lijkt het bestaansrecht van Flash Player voor het afspelen van media te verminderen. Het gebruik van Flash Player voor online games, onder andere via Facebook, is echter nog populair door het ontbreken van alternatieven.

Op websites neemt het gebruik van Flash af.[291] Populaire websites zoals Facebook[292] en YouTube[293] zijn overgeschakeld op html5 om video's af te spelen. Ook Adobe zelf richt zich niet langer op het doorontwikkelen van Flash.[294] De verwachting is dat wanneer grote browsers Flash Player niet meer als plug-in aanbieden, de marktpenetratiegraad verder afneemt. Flash zal voorlopig echter nog niet verdwijnen. Onder andere online games en legacysoftware vertrouwen nog op Flash.

Malware wordt verborgen in videokaarten en firmware

Detectie van malware kan bemoeilijkt worden door delen van de malware niet in het normale geheugen van een computer te laten uitvoeren, maar in de firmware van randapparatuur en onderdelen binnen een computer. De technieken hiervoor zijn geavanceerd en zijn voornamelijk in de context van academisch onderzoek aangetoond. Zo kan malware gedeeltelijk in de videokaart van een computersysteem worden uitgevoerd, om zo detectie te voorkomen.[295]

Daarnaast zijn onderzoekers erin geslaagd om malware in de firmware van een lte-modem[296], een SSD[297] en een harde schijf[298] te installeren. Hierdoor kan een malware-infectie ook na herinstallatie van het besturingssysteem voortduren. Op eenzelfde wijze kan er misbruik gemaakt worden van kwetsbaarheden in de firmware van standaardcomputers, zoals de BIOS[299] of de opvolger ervan, UEFI.[300] Ten slotte kan firmware van routers geïnfecteerd worden, zodat de malware niet na een herstart verdwijnt.[301] Bestaande maatregelen zijn veelal niet in staat deze verborgen malware te detecteren.

Via Javascript uitlezen van geheugen: rowhammering

Onderzoekers hebben een proof-of-concept ontwikkeld voor een methode om met Javascript het DRAM-geheugen van een computer te kunnen manipuleren.[302] Hiervoor wordt gebruikt gemaakt van de rowhammering-aanvalstechniek, waarmee sandboxing en andere beveiligingsmechanismen omzeild kunnen worden. In mei 2016 lieten onderzoekers van de Vrije Universiteit zien[303] dat deze techniek op Windows 8.1 en hoger gebruikt kan worden om zeer gericht geheugenblokken aan te passen. Met deze techniek is het dan mogelijk om op afstand toegang te krijgen tot het systeem.

Conclusie en vooruitblik

Nederland is kwetsbaar voor digitale aanvallen. Van software is de herkomst en het veiligheidsniveau niet altijd goed te achterhalen. Vaak is software onbewust onveilig ontwikkeld. Daardoor bevat het talloze kwetsbaarheden, terwijl steeds meer apparaten van software worden voorzien en met internet worden verbonden. Kwetsbaarheden in oudere software worden niet altijd verholpen en dat stelt organisaties voor uitdagingen.

Grote publiciteitscampagnes voor specifieke kwetsbaarheden scheppen meer bewustzijn, maar leiden de aandacht af en geven een vertekend beeld van de aanzienlijke hoeveelheid kwetsbaarheden die jaarlijks verholpen moet worden. Door de hypes die gecreëerd zijn rondom deze hoogpublicitaire kwetsbaarheden, kan deze trend op termijn weer afnemen.

Eindgebruikers hebben moeite met het herkennen van valse e-mail en andere vormen van social engineering. Misbruik hiervan zal blijven toenemen en bewustwordingscampagnes alleen kunnen dit niet meer oplossen. Aanvullende maatregelen zijn nodig om gebruikers in staat te stellen zich te weren tegen aanvallen door middel van social engineering.

De totale kwetsbaarheid van Nederland blijft toenemen. Dit heeft te maken met de toenemende koppeling van systemen met het internet, in combinatie met de beperkte mogelijkheden van softwareontwikkelaars om veilige software te ontwikkelen. Omdat software doordringt in steeds meer apparaten als onderdeel van het internet der dingen, gaat misbruik van softwarekwetsbaarheden impact hebben op de fysieke veiligheid van gebruikers.

Noten

257 https://vimeo.com/111043298, geraadpleegd op 13 april 2016.
258 http://www.theregister.co.uk/2016/03/23/npm_left_pad_chaos/, geraadpleegd op 26 mei 2016.
259 http://www.theregister.co.uk/2015/08/12/lenovo_firmware_nasty/, geraadpleegd op 13 april 2016.
260 http://www.theregister.co.uk/2015/09/18/d_link_code_signing_key_leak/, geraadpleegd op 13 april 2016.
261 https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html, geraadpleegd op 13 april 2016.
262 http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST, geraadpleegd op 13 april 2016.
263 Gebaseerd op een inventarisatie van competentielijsten voor ICT-opleidingen op mbo- en hbo-niveau in Nederland.
264 Hieronder worden ook begrepen: procescontrolesystemen, operationele technologie en SCADA-systemen.
265 Verizon 2016 Data Breach Investigations Report, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf, geraadpleegd 28 april 2016.
266 Microsoft Windows Update for Business, https://blogs.windows.com/windowsexperience/2015/05/04/announcing-windows-update-for-business/, geraadpleegd op 11 april 2016.
267 http://www.itwire.com/business-it-news/open-source/67655-linux-40-released-includes-live-patching, geraadpleegd op 11 april 2016.
268 Bron: input aan het NCSC vanuit de vitale infrastructuur, zie bijlage 2.
269 Een (niet statelijk) voorbeeld hiervan is de dreiging “The PantomPantomPhantom Menace”.
270 Bron: AIVD en MIVD.
271 Cybersecuritybeeld Nederland 2015, https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecurity-beeld-nederland-5/1/CSBN5.pdf, geraadpleegd op 12 april 2016.
272 https://www.security.nl/posting/465541/Update+voor+ernstig+lek+in+Samba+en+Windows+aangekondigd, geraadpleegd op 15 april 2016.
273 https://www.wodc.nl/onderzoeksdatabase/2056a-cry-wolf.aspx, geraadpleegd op 25 mei 2016.
274 Badlock: “On April 12th, 2016, a crucial security bug in Windows and Samba will be disclosed. We call it: Badlock.”, http://badlock.org/, geraadpleegd op 12 april 2016.
275 https://nakedsecurity.sophos.com/2016/04/12/badlock-revealed-probably-not-as-bad-as-you-thought/, geraadpleegd op 15 april 2016.
276 https://sadlock.org/, geraadpleegd op 15 april 2016.
277 https://labsblog.f-secure.com/2016/04/14/badlock-a-lateral-concern/, geraadpleegd op 15 april 2016.
278 https://www.trustwave.com/Resources/SpiderLabs-Blog/Microsoft-Patch-Tuesday,-April-2016/, geraadpleegd op 15 april 2016.
279 http://www.eenvoudigallesonline.nl/gebruik-van-mobiele-apparaten-in-nederland-de-cijfers/, geraadpleegd op 18 april 2016.
280 Bron: input aan het NCSC vanuit de vitale infrastructuur, zie bijlage 2.
281 Bron: Betaalvereniging Nederland.
282 https://www.fraudehelpdesk.nl/zoeken/antwoord/?antwoord_id=241&zoekopdracht=microsoft, geraadpleegd op 18 april 2016.
283 https://www.ncsc.nl/actueel/nieuwsberichten/wees-alert-op-social-engineering.html, geraadpleegd op 18 april 2016.
284 F-Secure Threat Report 2015, https://www.f-secure.com/documents/996508/1030743/Threat_Report_2015.pdf, geraadpleegd op 12 april 2016.
285 http://www.wired.com/2015/09/chrysler-gets-flak-patching-hack-via-mailed-usb/, geraadpleegd op 12 april 2016.
286 http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/, geraadpleegd op 12 april 2016.
287 https://www.security.nl/posting/462943/Ernstige+kwetsbaarheid+in+ssl+raakt+33%25+https-servers, geraadpleegd op 18 april 2016.
288 http://www.rtlnieuws.nl/nieuws/binnenland/beveiliging-tientallen-gemeentesites-lek-persoonsgegevens-niet-veilig, geraadpleegd op 18 april 2016.
289 Common Vulnerabilities and Exposures, https://cve.mitre.org/, geraadpleegd op 7 januari 2016.
290 NTT Group Global Threat Intelligence Report, https://www.solutionary.com/_assets/pdf/research/2016-gtir.pdf, geraadpleegd op 26 april 2016.
291 http://w3techs.com/technologies/details/cp-flash/all/all, geraadpleegd op 28 april 2016.
292 https://code.facebook.com/posts/159906447698921/why-we-chose-to-move-to-html5-video/, geraadpleegd op 11 april 2016.
293 http://youtube-eng.blogspot.com/2015/01/youtube-now-defaults-to-html5_27.html, geraadpleegd op 11 april 2016.
294 Welcome Adobe Animate CC, http://blogs.adobe.com/animate/welcome-adobe-animate-cc-a-new-era-for-flash-professional/, geraadpleegd op 11 april 2016.
295 http://www.securityweek.com/gpu-malware-not-difficult-detect-intel-security, geraadpleegd op 5 juli 2016.
296 http://www.fiercecio.com/story/security-researchers-hide-malware-firmware-lte-modem/2015-08-10, geraadpleegd op 5 juli 2016.
297 https://www.computable.nl/artikel/nieuws/security/5408780/250449/hackinggroep-herprogrammeert-ssd-firmware.html, geraadpleegd op 5 juli 2016.
298 http://arstechnica.com/information-technology/2015/02/how-hackers-could-attack-hard-drives-to-create-a-pervasive-backdoor/, geraadpleegd op 5 juli 2016.
299 http://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/, geraadpleegd op 5 juli 2016.
300 www.computerworld.com/article/2948177/malware-vulnerabilities/hacking-teams-malware-uses-uefi-rootkit-to-survive-os-reinstalls.html, http://www.securityweek.com/researchers-find-several-uefi-vulnerabilities, geraadpleegd op 5 juli 2016.
301 http://news.softpedia.com/news/cisco-routers-infected-with-boot-resistant-malware-491835.shtml, geraadpleegd op 5 juli 2016.
302 Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript, http://arxiv.org/pdf/1507.06955v1.pdf

Centralisatie van ICT-diensten maakt beveiligen eenvoudiger maar data ook vatbaarder voor spionage

5 Weerbaarheid: Maatregelen

Bewust inzetten van technische en niet-technische maatregelen zorgt voor een sterkere verdedigingspositie. De mens is een belangrijke schakel in de beveiliging, maar awareness lijkt op zijn top. Cybersecurity heeft duidelijk zijn plek op de bestuurlijke agenda gevonden. Dat is te zien aan vele nationale en internationale maatregelen.

Dit hoofdstuk gaat in op maatregelen die de weerstand en veerkracht van individuen, organisaties en de samenleving versterken en menselijke en technische kwetsbaarheden beperken. Maatregelen kunnen preventief of reactief zijn en gericht op de mens of systemen (techniek).

De mens

Zorgen over statelijke actoren groeien

Na de onthullingen van Snowden en de aanval op Sony Pictures maken steeds meer mensen zich druk om aanvallen door statelijke actoren. Grote partijen als Facebook, Google en anderen waarschuwen gebruikers voortaan als zij vermoeden dat een gebruiker doelwit is van een statelijke actor.[304]

In oktober 2015 verklaarde het Europese Hof van Justitie het Safe Harbour-raamwerk ongeldig. Dit gebeurde na een jarenlange procedure tegen Facebook door een groep gebruikers onder leiding van de Oostenrijker Max Schrems. Zij betoogden dat de onthullingen van Snowden aantoonden dat persoonsgegevens van buitenlanders in de Verenigde Staten onvoldoende beschermd waren. Dit zou aantonen dat de afspraken uit het Safe Harbour-raamwerk niet nageleefd werden. Het Safe Harbour-raamwerk vormde tot dat moment de basis voor de meeste gegevensuitwisseling tussen de Europese Unie en de Verenigde Staten. Op 12 juli 2016 heeft de Europese Commissie het EU-U.S. Privacy Shield aangenomen.[305]

Deze overeenkomst tussen de EU en de VS is de opvolger van het Safe Harbour-raamwerk en heeft als doel het zorgen voor goede bescherming van in de VS opgeslagen persoonsgegevens van personen in de EU. Met Privacy Shield geeft de commissie invulling aan de eisen die het Europese Hof van Justitie bij het ongeldig verklaren van het Safe Harbour-raamwerk heeft gesteld aan de opslag van persoonsgegevens. Voorbeelden van deze eisen zijn verplichtingen voor bedrijven die gegevens verwerken, waarborgen over de toegang van Amerikaanse opsporingsdiensten tot persoonsgegevens, de mogelijkheid van arbitrage en jaarlijkse monitoring van de werking van Privacy Shield.

Bewustwordingscampagnes hebben wisselend effect

Afgelopen jaar was er door verschillende campagnes opnieuw veel aandacht voor awareness: Europese Cyber Security Month, Alert Online , 'Hang op, klik weg, bel uw bank' en Safer Internet Day. Het Verizon Data Breach Investigations Report laat zien dat awareness alleen zeker niet voldoende is. Volgens geaggregeerd onderzoek wordt 30 procent van de phishing-e-mails geopend, 12 procent opent ook nog de attachment. Dit gebeurt ook nog eens erg snel, gemiddeld klikt een ontvanger binnen vier minuten na het verzenden op een attachment.[306]

Tekort aan cybersecurityprofessionals dreigt

De vraag naar cybersecurityprofessionals blijft groot. De Cyber Security Raad (CSR) signaleerde dat een groot tekort aan cybersecurityprofessionals dreigt. Ook constateerde de CSR dat er in het algemene onderwijs meer aandacht voor cybersecurity zou moeten zijn. De CSR gaf hierover een advies aan de staatssecretaris van Veiligheid en Justitie.[307]

Belastingdienst

De Belastingdienst heeft een Security Operations Center (soc). Dit soc is verantwoordelijk voor het signaleren en opsporen van kwetsbaarheden in de operationele infrastructuur, het duiden van cyberdreigingen en het adviseren van tegenmaatregelen om bestaande risico's op te heffen. Tijdens calamiteiten fungeert het soc als het Computer Emergency Response Team van de Belastingdienst.[308] In de rapportageperiode:

- zijn in de kantoor- en datacenteromgeving van de Belastingdienst (ruim 35.000 werkplekken en 5.600 servers) diverse meldingen afgegeven vanuit het internet. Het gaat om circa 3.300 meldingen van virussen, veertig meldingen van en hack- en cracktools en ruim 4700 meldingen van het tegenhouden van kwaadaardige software;
- heeft de eerstelijnsbescherming (firewalls) bijna drie miljard aanvallen en de tweedelijnsbescherming (intrusion prevention-faciliteit) ruim 2,2 miljoen aanvallen tegengehouden;
- is er een significante toename te zien ten aanzien van de hoeveelheid binnenkomende spam-e-mails tijdens het tweede half jaar van 2015. Deze toename heeft zich doorgezet in de eerste helft van 2016;
- zijn een groot aantal DDoS-aanvallen waargenomen. Geen van deze aanvallen leidde tot onbeschikbaarheid van de informatiesystemen. De grootste aanval was 16 Gbit/s en vond plaats in april 2016. Er zijn 97 security-incidenten geregistreerd waarvan vier incidenten van de hoogste prioriteit. Het soc onderzocht al deze security-incidenten en loste ze samen met de betreffende platformteams op;
- zijn 15 responsible-disclosuremeldingen gedaan, waarvan 12 terechte. Al deze meldingen zijn opgelost.[309] In totaal reikte de Belastingdienst zes bokalen uit. Twee van deze security incidenten of kwetsbaarheden leidden tot een mogelijke inbreuk op de integriteit en vertrouwelijkheid van de door de Belastingdienst beheerde gegevens. Deze incidenten zijn gemeld conform de wet over de meldplicht voor datalekken;
- zijn ruim 7.100 meldingen ontvangen van valse Belastingdienst-e-mails. De Belastingdienst deed in deze rapportageperiode meerdere aangiften tegen deze phishingcampagnes bij de politie;
- zijn er in samenwerking met het NCSC en de politie 32 phishing-websites ontmanteld. Hiervan waren er vijftien valse DigiD-websites.

De techniek

De mens wordt vaak aangeduid als de zwakste schakel in de cybersecurityketen, maar de techniek is onmisbaar voor het borgen van cybersecurity. Om veilig te blijven moet een bewuste gebruiker ook ondersteund worden door de juiste, veilige software. Deze paragraaf gaat in op de belangrijkste ontwikkelingen op dit gebied in de afgelopen periode.

Om langdurige problemen met legacysoftware te voorkomen heeft Microsoft met Windows 10 een andere strategie ingezet. Gebruikers van eerdere versies van Windows krijgen automatisch melding dat Windows 10 gratis beschikbaar is. Bovendien is de standaardinstelling van Windows 10 dat updates automatisch geïnstalleerd worden. Statistieken laten zien dat de adoptie van Windows 10 sneller ging dan bij eerdere versies van Windows, maar Windows 7 blijft nog steeds veruit het populairst.[310]

In 2015 waren er enkele incidenten[311] [312] met voorgeïnstalleerde software op Windows-machines die verkeer afluisterde of zelfs aanpaste. Microsoft kondigde in december 2015 aan software te blokkeren die man-in-the-middle-technieken gebruikt om advertenties te tonen.[313] Deze maatregel startte op 31 maart 2016.

Adoptie van standaarden neemt toe

De adoptie van DNSSEC in Nederland en binnen de Rijksoverheid laat nog steeds een stijgende trend zien. In augustus 2015 beschikte 44 procent van de .nl-domeinen over DNSSEC. Binnen de Rijksoverheid was dit in de zomer van 2015 nog 28 procent.[314]

Sinds de lancering van internet.nl zijn in de periode mei 2015 tot en met april 2016 veel tests uitgevoerd. Er zijn bijna 10.000 unieke .nl-domeinen getest. Hiervan had slechts 12 procent een perfecte score op de TLS-test. Van de 2263 geteste .nl-e-mailservers gebruikt 59 procent SPF, 47 procent DKIM en 18 procent DMARC. Slechts 13 procent gebruikt alle drie de maatregelen.

Uit gesprekken met de verschillende sectoren blijkt dat de meeste bedrijven erkennen dat digitale beveiligingsmaatregelen nodig zijn. Gemiddeld genomen zijn de basale technische maatregelen ook getroffen. Het is niet altijd bekend dat deze maatregelen onvoldoende kunnen zijn tegen gerichte aanvallen.[315]

Bescherming tegen malvertising door adblockers en patching

In een eerder hoofdstuk kwam al aan bod dat een significant deel van de malware-infecties gebeurt door malvertising. De Autoriteit Consument en Markt (ACM) heeft de online advertentie-industrie in Nederland gewezen op dit risico. De ACM geeft verder aan dat wanneer het risico te groot wordt, een mogelijk toekomstig advies is om adblockers te gebruiken om eindgebruikers zo te beschermen.

Naast adblockers biedt ook het updaten van systemen bescherming tegen malvertising. Malafide advertenties gebruiken kwetsbaarheden in software om systemen te besmetten. Als systemen voorzien zijn van de laatste updates, kunnen malafide advertenties, die gebruikmaken van bekende kwetsbaarheden, deze systemen niet meer besmetten.

Het grootschalig gebruik van adblockers kan impact hebben op het verdienmodel van diverse websites. Sinds de opkomst van de pop-upadvertenties in de jaren 90 zijn adblockers beschikbaar. Vooral de meer technisch onderlegde gebruikers thuis gebruikten deze adblockers. Hiermee zorgden ze voor visueel rustigere pagina's en wilden ze privacy-onvriendelijk gedrag van de advertentie-industrie tegengaan.

Binnen de geraadpleegde sectoren installeert een klein aantal bedrijven al adblockers om veiligheidsredenen. Een aantal andere bedrijven deed dit niet standaard, zeker op de securityafdelingen niet. Wel adviseerden zij sterk om zelf adblockers te installeren.

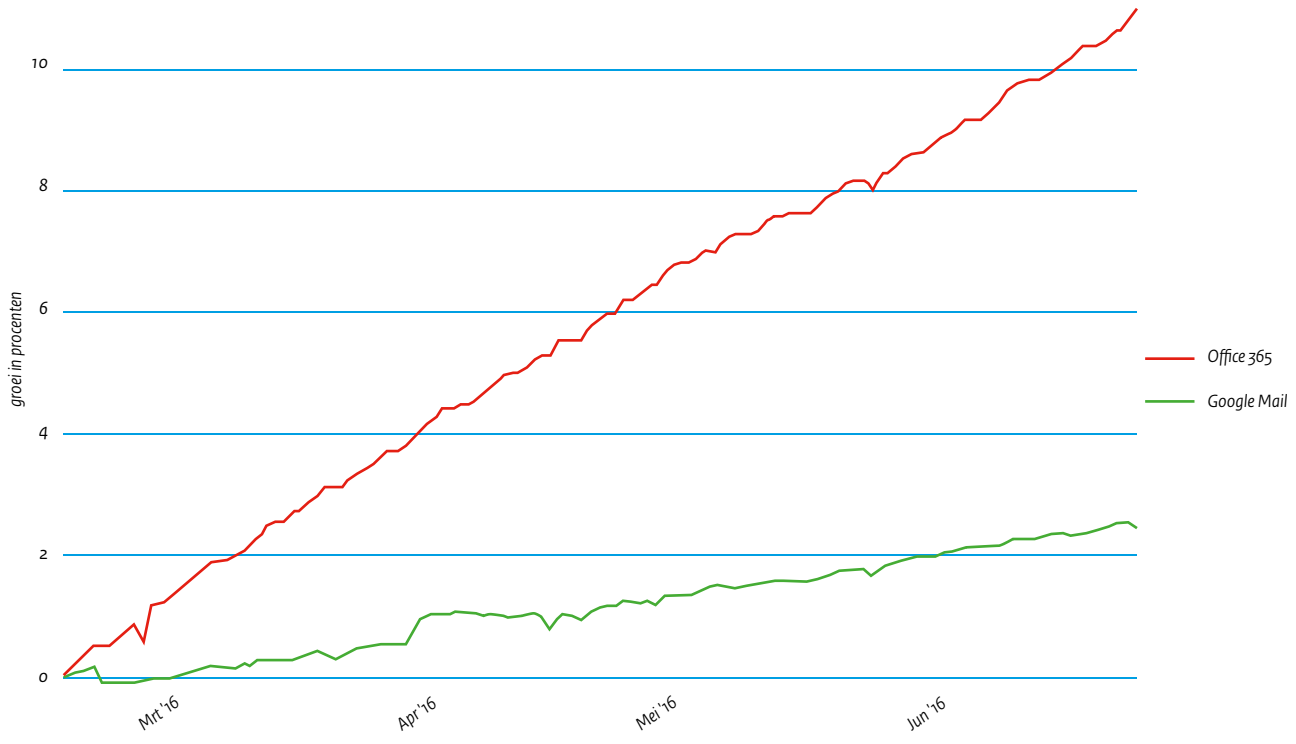
Centralisatie van ICT-diensten maakt beveiligen eenvoudiger maar data ook vatbaarder voor spionage

Het uitbesteden van ICT-diensten, bijvoorbeeld door het gebruik van clouddiensten, is een trend die al langer aan de gang is. E-mail is hiervan een voorbeeld. E-mail is voor organisaties in het midden- en kleinbedrijf complex om zelf te beheren. Alternatieven in de cloud zijn dan aantrekkelijk, vanwege lage kosten en beperkt beheer. Een grote en ervaren aanbieder kan e-mail vaak beter en veiliger aanbieden dan een eigen ICT-beheerafdeling. Onderstaande observaties over uitbesteding van e-mail gaan ook op voor veel andere, uitbesteedbare ICT-diensten.

E-mail uitbesteden komt steeds vaker voor, zowel direct bij clouddienstverleners als via fullserviceproviders. Een clouddienstverlener beheert wel de e-mail, maar vraagt de domeinnaamhouder zijn DNS-instellingen zo in te richten dat de e-mail bij de clouddienstverlener terechtkomt. Een fullserviceprovider verkoopt de dienstverlening van een cloudprovider, maar beheert daarnaast ook de DNS-zone voor de klant.

Figuur 10 laat zien hoe de groei van twee clouddienstverleners in een periode van vier maanden is verlopen voor .nl-domeinnamen.[316] Tijdens deze periode bleef het aantal .nl-domeinnamen nagenoeg gelijk. Dit wekt het beeld dat organisaties hun e-mail steeds vaker uitbesteden aan clouddienstverleners. Deze centralisatie is voor .nl-domeinnamen aanzienlijk. 30 procent van de .nl-domeinnaamhouders laat e-mail afhandelen door een van de tien populairste e-mailafhandelaars.[317] Voor .com-domeinnamen is deze centralisatie nog sterker: daar wordt voor 50 procent van de domeinnamen de e-mail afgehandeld door een van de tien populairste e-mailafhandelaars. Omdat kleine organisaties hier even zwaar worden meegeteld als grote, zijn deze statistieken waarschijnlijk vooral representatief voor het mkb.[318]

Figuur 10 **Groei van clouddienstverleners**

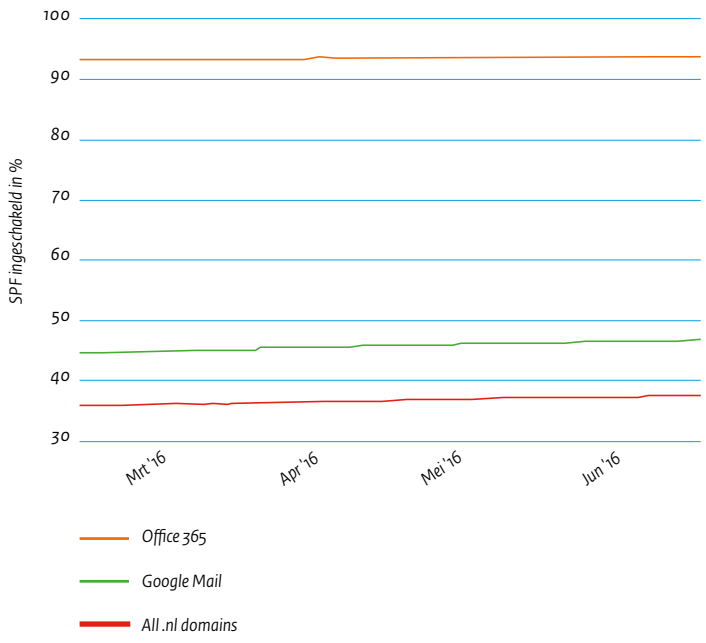


Bron: OpenINTEL.

Nieuwe beveiligingsstandaarden voor e-mail worden eenvoudiger overgenomen als organisaties hun e-mail uitbesteden. Fullserviceproviders kunnen bijvoorbeeld SPF in één keer voor al hun klanten inschakelen. Voor hen is het toepassen van de standaard een eenmalige investering en een verkoopargument. Ook clouddienstverleners maken het hun klanten gemakkelijk, met kant-en-klare instructies voor het instellen van standaarden als SPF. Het uitbesteden van e-mail aan een clouddienstverlener, eventueel via een fullserviceprovider, lijkt een grotere adoptie van SPF op te leveren. In figuur 11 is te zien dat de klanten van clouddienstverleners Microsoft en Google een aanzienlijk hogere SPF-toepassing laten zien dan de rest van de .nl-domeinnaamhouders.

Centralisatie van e-mail heeft ook nadelen. Al in het jaarverslag van 2015 vermeldde de AIVD dat het gebruik van clouddiensten een aanvullend risico op spionage met zich meebrengt. Dit risico geldt ook voor fullserviceproviders. Daarnaast hebben kwetsbaarheden in de software van clouddienstverleners en fullserviceproviders direct grotere gevolgen, omdat meer klanten afhankelijk zijn van de veiligheid van de dienst. In januari 2016 vonden twee onderzoekers een kwetsbaarheid in Microsoft Office 365. Deze stelde hen in staat in te loggen op accounts van andere organisaties.[319] Deze kwetsbaarheid werd bij Microsoft gemeld en binnen enkele uren gerepareerd. Als de onderzoekers de kwetsbaarheid echter hadden achtergehouden, dan konden ze toegang krijgen tot veel gevoelige informatie bij allerlei organisaties.

Figuur 11 **Toepassing van SPF op .nl-domeinnamen**



Bron: OpenINTEL.

Maatregelen tegen DDoS-aanvallen

DDoS-aanvallen zijn onderdeel geworden van de algemene dreiging, zoals eerder al beschreven. Wel kunnen verschillende maatregelen DDoS-aanvallen voorkomen, of de effecten ervan tegengaan.

Door routers in netwerken op de juiste manier in te stellen, kunnen DDoS-aanvallen worden voorkomen. Pakketten met vervalste afzenders worden zo tegengehouden.[327] Deze pakketten vormen de bron van veel verschillende vormen van aanvallen. Helaas werkt het filteren hiervan alleen effectief als bijna alle netwerken dit instellen.

Om de nadelige effecten van DDoS-aanvallen tegen te gaan, zijn het afgelopen jaar twee verschillende initiatieven opgezet in Nederland: het Trusted Network Initiative (TNI)[328] en een samenwerking van de internetproviders, Dutch Continuity Board (DCB). Het doel van beide initiatieven is om de impact van een DDoS-aanval op Nederlandse kritieke infrastructuur te minimaliseren. Hierdoor kunnen diensten zo snel mogelijk weer beschikbaar worden gemaakt voor Nederlandse gebruikers. De meeste leden van TNI besloten uiteindelijk aan te haken bij DCB. Het DCB-project wil eind 2016 operationeel zijn.

Is er sprake van een tweede crypto-oorlog?

Het publieke debat over encryptie is nog niet voorbij. In september 2015 probeerde de Amerikaanse overheid bedrijven over te halen om samen te werken op het gebied van encryptie en decryptie, om zo opsporing niet in de weg te zitten.[320] Dit werd in eerste instantie niet goed ontvangen.

In maart 2016 escaleerde deze discussie: de FBI probeerde met een rechtszaak de hulp van Apple af te dwingen om toegang te krijgen tot een telefoon van een Amerikaanse terrorist.[321] Apple was het hier niet mee eens en gaf aan dat de methode toegang zou geven tot bijna alle iPhones. Daarom ging Apple in hoger beroep en publiceerde het bedrijf een open brief.[322] In het publieke debat kreeg Apple al snel steun van veel grote technologiebedrijven. Uiteindelijk trok de FBI de zaak in omdat op een andere manier toegang was verkregen tot de telefoon.

Tijdens dit debat in de VS schakelde WhatsApp end-to-end-encryptie in voor alle gebruikers.[323] Hiermee is de inhoud van de berichten in principe alleen nog voor de zender en ontvangers toegankelijk. WhatsApp is niet de eerste berichten-app die dit aanbiedt, maar wel de grootste, met wereldwijd meer dan een miljard gebruikers.

De Autoriteit Persoonsgegevens publiceerde een advies voor fysiotherapeuten die op hun website een invulformulier gebruiken. Mochten daar gevoelige gegevens (BSN of medische gegevens) worden ingevuld, dan moet de gehele website gebruikmaken van TLS.

Vergelijkbaar besloot de Amerikaanse overheid in juni 2015 alle overheidswebsites over te schakelen op https.[324] De uitleg geeft aan dat webverkeer centraal onderdeel is geworden van ons leven. Niet-gevoelig verkeer bestaat niet op het internet. Daarom zou de overheid niet afhankelijk moeten zijn van de goede intentie van netwerkbeheerders.

De start van Let's Encrypt hielp de adoptie van https en encryptie verder vooruit. Deze gratis en toegankelijke webcertificaatdienst werd eind 2015 publiek beschikbaar. Inmiddels zijn al meer dan 2 miljoen certificaten uitgegeven door Let's Encrypt.

In januari bracht het kabinet haar standpunt over encryptie naar buiten.[325] Daarin werd duidelijk dat de Nederlandse overheid achter encryptie staat. Ook is de overheid tegen wettelijke maatregelen ten aanzien van de ontwikkeling, beschikbaarheid of het gebruik van encryptiealgoritmen. De Franse overheid volgde in januari 2016 het Nederlandse standpunt en nam eenzelfde standpunt in.

De Nederlandse overheid draagt ook voor de implementatie van encryptie haar steentje bij door een gift van 500.000 euro aan encryptieprojecten (zoals OpenSSL, LibreSSL en PolarSSL).[326]

Nederlandse ontwikkelingen

Digitale veiligheid staat duidelijk zichtbaar op de Nederlandse beleidsagenda. Een aantal lopende initiatieven werd het afgelopen jaar zichtbaarder, zoals Idensys en MijnOverheid.

De ontwikkelingen rond Idensys (voorheen het eID-stelsel) krijgen duidelijker vorm. In juli 2015 kwam de Privacy Impact Assessment van Idensys uit. Daarin staat een aantal aanbevelingen.[329] Eind 2015 is dit verder uitgewerkt en startten enkele publieke en private partijen met een pilot.[330]

De Nederlandse banken hebben gezamenlijk ook een vergelijkbare dienst opgezet: iDIN.[331] Hiermee kunnen klanten hun inlogmethode van de bank gebruiken bij andere instellingen om zich te identificeren. Op dit moment loopt er een pilot bij de Belastingdienst met deze dienst.

De overheid probeert steeds meer digitaal te communiceren met burgers. Om dit te faciliteren is het project MijnOverheid opgezet. Een centrale website, mijnoverheid.nl, geeft toegang tot het berichtenverkeer met verschillende overheidsinstanties. In november 2015 is de wettelijke basis gelegd voor elektronisch berichtenverkeer van de Belastingdienst via deze website. Steeds meer overheidsinstanties zijn aangesloten bij de Digitale Berichtenbox: in april 2016 al 119 gemeenten, 23 pensioenfondsen en 28 andere overheidsinstanties.

Het Nationaal Detectie Netwerk (NDN) werd vorig jaar al genoemd als belangrijk samenwerkingsverband van het NCSC en andere partijen om dreigingsinformatie uit te wisselen. De pilots zijn eind 2015 positief geëvalueerd. Het netwerk wordt in 2016 verder uitgebreid en opgenomen in de standaarddienstverlening van het NCSC.

De Nederlandse energiesector werkte het afgelopen jaar aan een risicoanalyse van de ketenafhankelijkheden in de energiesector. Deze analyse maakte de kwetsbaarheid van systemen door deze afhankelijkheden inzichtelijk.[332]

Platform Internetstandaarden spoort aan op toepassen standaarden

Platform Internetstandaarden, een samenwerkingsverband van de Internetgemeenschap en de Nederlandse overheid, lanceerde in april 2015 de website internet.nl. Deze website controleert of een internetverbinding, e-mail- of webserver voldoet aan moderne internetstandaarden. De website internet.nl kan een server testen op de verbindingsbeveiliging van zowel het web- als het e-mailverkeer. Ook geeft de site aan in hoeverre dit voldoet aan de pas-toe-of-leg-uitlijst van het Forum Standaardisatie.

De website blijkt een effectief middel om partijen te helpen hun gebruik van moderne internetstandaarden te verbeteren. Van alle websites die door bezoekers van internet.nl meermaals zijn getest, verbeterde bijna vijftig procent de score tussen de eerste en de recentste test.

In juni 2015 kwamen er nieuwe beveiligingseisen voor e-mailverkeer bij: naast DKIM (DomainKeys Identified Mail) werden SPF (Sender Protection Framework) en DMARC (Domain-based Message Authentication Reporting and Conformance) toegevoegd aan de pas-toe-of-leg-uitlijst. Deze moeten e-mail veiliger maken en spam en phishing tegengaan. Voor grotere organisaties is het niet gemakkelijk om deze standaarden in te voeren, de NCSC-factsheet Bescherm domeinnamen tegen phishing[333] kan hierbij helpen.

Bovenstaande maatregelen helpen de afzender van e-mails te authentiseren. Om ook de integriteit en vertrouwelijkheid te garanderen is meer nodig. Hiervoor wordt traditioneel STARTTLS gebruikt, dat ook door meer dan 90 procent van de e-mailservers gebruikt wordt. STARTTLS is hier alleen een effectieve maatregel tegen een passieve, afluisterende aanvaller. In oktober 2015 is daarom de combinatie van STARTTLS met DANE gestandaardiseerd.[334] Deze combinatie beveiligt ook tegen andere mogelijke aanvallen. In februari 2016 is voorgesteld om dit ook toe te voegen aan de pas-toe-of-leg-uitlijst.

Consumentenbond spande een kort geding aan tegen Samsung

In Nederland startte de Consumentenbond de campagne 'Updaten!'. Hierbij willen ze fabrikanten aanpakken die Androidtelefoons gebrekkig updaten. In een eerste actie klaagde de Consumentenbond Samsung hierover aan. De Consumentenbond argumenteerde in een kort geding dat Samsung minstens twee jaar na aanschaf nog zorgplicht heeft en updates beschikbaar moet stellen. De rechter gaf in deze procedure aan geen spoedeisend belang te zien en daarom geen verdere procedure te starten. De Consumentenbond vindt de situatie rondom het updatebeleid van Android door verschillende fabrikanten nog steeds zorgelijk.[335]

Nederland Schoon vergroot bewustzijn over bad hosting

Nederlandse hosting blijft onverminderd populair onder beroepscriminelen.[336] Veel hostingproviders geven aan dat ze geen zicht hebben op de feitelijke gebruikers van hun infrastructuur, omdat deze een model van reselling hanteren. Sommige van hun resellers faciliteren criminele activiteiten door tegen relatief hoge prijzen zo anoniem mogelijke hosting aan te bieden.

Om hostingproviders bewust te maken van de malafide activiteiten van hun klanten op hun infrastructuur zijn in het kader van het project Nederland Schoon door de TU Delft metingen verricht naar bad hosting in Nederland.[337] De metingen zijn onder meer gebaseerd op publieke en private gegevens, zoals van het Meldpunt Kinderporno en van het Landelijk International Rechtshulpcentrum (LIRC). Ze zijn verder genormaliseerd naar de grootte van de hostingprovider. Op basis hiervan is een inschatting gemaakt van de 'badness' van alle Nederlandse hosting providers.

Medio 2015 gingen het OM, de politie en de ACM gesprekken aan met de top 10 badhostingproviders. Dit was om hen te wijzen op hun faciliterende rol in digitale criminaliteit en op maatregelen die zij daartegen kunnen nemen. Uit een tweede ronde van metingen blijkt dat sommige hosters verbeterden. Enkele providers blijven slecht scoren in termen van bad hosting of verslechterden zelfs. Samen met andere indicatoren, zoals het gebrek aan samenwerking met de overheid en de afwezigheid van preventieve maatregelen, geven de resultaten van Nederland Schoon inzicht in welke providers extra aandacht moeten krijgen. De politie en het OM gaan in de nabije toekomst juist inzetten op de aanpak van deze bad hosts. Het uiteindelijke doel van het project Nederland Schoon is echter een gedragsverandering bij hostingproviders. Hierbij zorgt de branche door zelfregulering voor opschoning van de hostinginfrastructuur.

Meldplichten

Op 1 januari 2016 ging de nieuwe Wet Bescherming Persoonsgegevens van kracht. Hiermee kreeg de toezichthouder ook een nieuwe naam: Autoriteit Persoonsgegevens. De wet regelt ook dat er meer bevoegdheden zijn, waaronder het uitdelen van boetes bij overtredingen van de wet. Nederland gaf met deze wet invulling aan de EU General Data Protection Regulation.

Volgens de nieuwe Wet Bescherming Persoonsgegevens moeten bedrijven na 1 januari incidenten melden waarbij persoonsgegevens mogelijk gelekt zijn. In de eerste week van januari werden er al twintig meldingen gedaan bij de nieuwe Autoriteit Persoonsgegevens; in april waren er in totaal al duizend meldingen gedaan.

De meldplicht datalekken is echter iets anders dan de meldplicht uit het wetsvoorstel gegevensverwerking en meldplicht cybersecurity. Deze laatste meldplicht geldt voor organisaties uit de vitale infrastructuur. Meldingen over beveiligingsincidenten moeten bij het NCSC worden gedaan. Deze meldplicht is onderdeel van een groter wetsvoorstel rondom de taken van het NCSC, en ligt nog ter behandeling bij de Tweede Kamer.

Internationale ontwikkelingen

Regulering

In de zomer van 2015 werd in de VS een consultatie gehouden over de praktische uitwerking van exportregulering rondom 'intrusion software'. In 2013 zijn technologie en middelen rondom intrusion software toegevoegd aan de Wassenaar Arrangement-lijst van dual-use-goederen. In de deelnemende landen moet daarom een exportvergunning aangevraagd worden voor het uitvoeren van technologie, software en middelen voor het toegang krijgen tot andere computers. De securitysector in de Verenigde Staten reageerde massaal op de consultatie. Ze gaven aan dat de huidige definities van intrusion software zeer problematisch waren.[338] Microsoft gaf bijvoorbeeld aan dat het bedrijf bij deze regulering naar verwachting honderdduizenden licentieaanvragen per jaar moet doen. De Amerikaanse overheid kreeg de opdracht opnieuw te gaan onderhandelen over de toevoeging.[339] Deze exportregulering is al sinds eind 2013 van kracht in Europa en ook op de afgelopen NCSC One Conference bediscussieerd.

Asus liet in Amerika zien dat fabrikanten toch enige mate van verantwoordelijkheid hebben voor veilige software. In februari 2016 trof de fabrikant een schikking met de FTC over gebrekkige beveiliging in software voor wifirouters.[340] Asus heeft toegezegd de komende twintig jaar onafhankelijke security-audits te laten uitvoeren.

Samenwerking

De VS en China sloten in september 2015 een digitaal niet-aanvalsverdrag. Het verdrag houdt in dat de overheden zich niet zullen mengen in economische spionage naar elkaar. Het verdrag zegt verder niets over traditionele vormen van spionage.

De Europese Richtlijn voor netwerk- en informatiebeveiliging (NIB) is op 6 juli 2016 aangenomen door het Europees Parlement. Lidstaten hebben 21 maanden om de richtlijn te implementeren (plus aanvullend zes maanden om aanbieders van essentiële diensten aan te wijzen). De richtlijn verplicht lidstaten allereerst om nationale cybersecuritycapaciteit op orde te hebben, ten tweede om samenwerking (nationaal en in de EU) te verstevigen en tot slot om beveiligings- en meldingseisen voor aanbieders van essentiële diensten in te richten.

Responsible of coordinated vulnerability disclosure

Een van de speerpunten van het Global Forum on Cyber Expertise is het verder uitdragen van responsible disclosure. Dit stond ook bij het Europees Voorzitterschap hoog op de agenda. Nationaal en internationaal zijn er verschillende belangrijke ontwikkelingen op dit gebied. Een eerste ontwikkeling is dat internationaal vooral de term 'coordinated vulnerability disclosure' wordt gebruikt. De term 'responsible' wordt vaak gezien als een waardeoordeel, vooral naar de ontdekker toe. 'Coordinated' probeert aan te geven dat dit een gelijkwaardig proces is voor beide partijen.

In de VS zijn verschillende multi-stakeholdersbijeenkomsten georganiseerd over mogelijke regelgeving rondom vulnerability-disclosure. De NTIA organiseert deze bijeenkomsten samen met vertegenwoordigers van de industrie, onderzoekers en de overheid. Deze hebben zich georganiseerd rond vier thema's: bewustzijn en adoptie, multi-vendor-disclosure, economie en incentives en ten slotte veiligheid en disclosure.

In steeds meer sectoren wordt het gebruikelijk om een vulnerability-disclosureprogramma te hebben. Na de ervaring met het Jeep-incident[345] kondigde General Motors voor alle producten een algemeen vulnerability-disclosureprogramma aan. Verschillende luchtvaartmaatschappijen starten ook met disclosureprogramma's en loven airmiles uit als beloning voor het melden van kwetsbaarheden.

De praktijk rond vulnerability-disclosure professionaliseert ook steeds meer. Meerdere bedrijven bieden hulp aan bij het opzetten of onderhouden van een vulnerability-disclosureprogramma. Ook wordt het steeds gebruikelijker dat er financiële beloningen worden uitgekeerd voor meldingen. Google alleen al keerde meer dan twee miljoen dollar uit in 2015.[346]

In april 2016 stelde de Internationale Standaardisatie Organisatie (ISO) het document over vulnerability-disclosure (ISO 29147) openbaar beschikbaar.[347] Op dit moment wordt ook gewerkt aan herziening van deze standaard uit 2014, om nieuwe inzichten op het gebied van vulnerability-disclosure te verwerken.

Rabobank en het CIO Platform Nederland hebben een Coordinated Vulnerability Disclosure Manifesto opgesteld. Ondertekenaars van dit manifest onderschrijven het belang van het vulnerability-disclosureproces en waarderen de interactie met onderzoekers en de hackergemeenschap. In mei 2016 is dit manifest gepubliceerd. 29 bedrijven binnen en buiten Nederland ondertekenden het al.[348]

Bestrijding van cybercrime

In het afgelopen jaar zijn enkele grote operaties geweest tegen cybercriminelen in Nederland, maar ook een aantal grote operaties daarbuiten.

In het voorjaar van 2015 hield de politie twee verdachten aan. Zij verstuurden spam met als onderwerp 'foutieve factuur' naar midden- en kleinbedrijven. Op die manier wisten ze RAT's te installeren en kregen ze toegang tot de internetbankieraccounts van de bedrijven. Naar aanleiding van dit onderzoek publiceerden het OM en de politie, in samenwerking met het NCSC, MKB Nederland, ECP en Betaalvereniging Nederland, in mei 2016 een informatieblad voor het mkb.

Een aantal leden van de Lizard Squad is het afgelopen jaar veroordeeld. De 17-jarige 'obnoxious' werd in mei 2015 veroordeeld, met name voor zijn swatting-activiteiten.[341] In Noorwegen werd de eveneens 17-jarige 'zeekill' veroordeeld voor meer dan 50.000 vergrijpen.[342]

In juni 2015 werd een grootschalig internationaal opsporingsonderzoek naar mobiele-bankier-malware afgerond. Hierbij werd een belangrijk netwerk van cybercriminelen opgerold. Zo konden wereldwijd in totaal zestig verdachten aangehouden worden, waarvan ongeveer veertig in Nederland. Vier hoofdverdachten kregen in Nederland gevangenisstraffen van 24 tot 39 maanden. Ook een deel van de gebruikte infrastructuur stond in Nederland en werd ontmanteld.

Het cybercrime-forum Darkode is in juli 2015 offline gehaald door een grote internationale operatie.[343] De FBI werkte voor de operatie Shrouded Horizon samen met Europol. Er werden acties ondernomen in 20 landen waarbij 70 mensen zijn gearresteerd. Ziggo werd in augustus 2015 twee avonden lang getroffen door grote DDoS-aanvallen. Hierbij ontstond een storing in het netwerk van Ziggo, waardoor ongeveer 1,8 miljoen klanten van de provider zonder internet zaten. In videoboodschappen op YouTube werd gedreigd met nieuwe aanvallen op Ziggo. Ook KPN was het doelwit van DDoS-aanvallen. Tijdens het politieonderzoek werd de DDoS-aanval anoniem op internet opgeëist. De indruk ontstond dat de jongens wilden laten zien dat zij tot grote dingen in staat zijn, zoals het platleggen van de internetprovider. Er zijn vijf verdachten aangehouden. Vier van hen waren minderjarig (in de leeftijd van 14-17 jaar).

In het vorige CSBN is al beschreven hoe de politie er in april 2015 in slaagde een reeks veiliggestelde decryptiesleutels te verstrekken aan ransomwareslachtoffers. Door samenwerking met antivirusbedrijf Kaspersky kreeg de politie vervolgens zicht op verdachten achter deze criminele activiteiten. In september konden in Amersfoort twee mannen (18 en 22 jaar) worden aangehouden. In oktober 2015 werden twee Nederlandse verdachten aangehouden. Zij maakten vele slachtoffers door steeds voor een korte periode (maximaal enkele dagen) nep-webshops online te zetten en daar gewilde spullen (zoals telefoons en bakfietsen) te verkopen die nooit geleverd werden.

In januari 2016 maakte Europol bekend dat ze een geslaagde operatie hadden uitgevoerd tegen de DD4BC-groep. Deze groep was het afgelopen jaar erg actief in het chanteren van bedrijven met DDoS-aanvallen. Deze groep bedreigde duizenden bedrijven. Hierbij werd vaak geen aangifte gedaan.

In het vorige CSBN werd AbuseHub al genoemd. Dit is een samenwerking tussen de verschillende internetproviders om informatie uit te wisselen en zo cybercrime tegen te gaan. Sinds januari dit jaar is dit initiatief verder uitgebreid met hostingproviders. Via dit platform kunnen beveiligingsrisico's en gesignaleerd misbruik automatisch worden doorgegeven aan de klanten zonder tussenkomst van de hostingpartijen. Het doel is om het cybercriminelen zo moeilijk mogelijk te maken.

In Nederland trad de FIOD ook op om daders achter een phishingoperatie te arresteren. In januari 2016 werd hiervoor een 23-jarige man aangehouden in Almere. Hij wordt er onder andere van verdacht phishing-e-mails te hebben gestuurd namens de directeur-generaal van de Belastingdienst.[344]

Op sociale media verscheen dinsdag 29 maart en woensdag 30 maart 2016 berichtgeving dat de site van de Belastingdienst plat zou worden gelegd. Hierdoor zouden veel mensen hun belastingaangifte niet op tijd kunnen indienen. Het cybercrimeteam van de Eenheid Midden-Nederland van de politie hield in samenwerking met het Team High Tech Crime van de Landelijke Eenheid een 17-jarige verdachte aan. Hij dreigde om de website van de belastingdienst via een DDoS-aanval plat te leggen.
In april 2016 stelde de politie de netwerkinfrastructuur van een bedrijf veilig. De eigenaar werd aangehouden voor witwassen. Het bedrijf verkocht voor gemiddeld 1.500 euro BlackBerry's met PGP-software om berichten te versleutelen. Hierbij bedroegen de abonnementskosten gemiddeld 3.000 euro per jaar. Deze telefoons zijn niet geschikt om te bellen, maar alleen om berichten te versturen. De politie en het OM vermoeden dat het grootste deel van de gebruikers de telefoons inzet om zware en georganiseerde criminaliteit af te schermen.

Conclusie en vooruitblik

Cybersecurity heeft duidelijk zijn plek gevonden op de bestuurlijke agenda. Het afgelopen jaar leidde dit tot verschillende maatregelen gericht op de mens, de techniek en organisaties. De vraag naar cybersecurityprofessionals blijft onverminderd groot. Dit kan in de toekomst leiden tot problemen.

De klassieke technische maatregelen als back-ups en netwerksegmentering bewijzen opnieuw hun waarde doordat ze de impact van ransomware-aanvallen beperken. Nieuwe maatregelen die zijn toegevoegd aan de pas-toe-of-leg-uitlijst krijgen ook meer aandacht omdat het mogelijk is ze eenvoudig te testen met de website internet.nl.

Maatregelen rond encryptie waren het afgelopen jaar een duidelijk onderdeel van het publieke debat. Er zijn maatregelen genomen om encryptie beter toe te passen, zoals nieuwe verplichtingen rondom TLS. Daarnaast maakt Let's Encrypt certificaten toegankelijker. Tegelijkertijd maakt dit het spanningsveld tussen de belangen van veiligheid en opsporing ook duidelijker. Dat leidde tot een internationale discussie. Nederland sprak als eerste land uit dat het voorstander is van encryptie. Het neemt geen maatregelen om ontwikkeling, beschikbaarheid of gebruik van encryptiealgoritmen te beperken.

Vulnerability-disclosure kreeg het afgelopen jaar veel aandacht. Steeds meer organisaties voeren het in. Ook internationaal wordt deze praktijk steeds geaccepteerder. Meer en meer bedrijven spreken zich ook publiekelijk uit als voorstander.

Noten

303 http://www.cs.vu.nl/~kaveh/pubs/pdf/dedup-sp16.pdf

304 http://www.securityweek.com/microsoft-warn-users-state-sponsored-attacks, geraadpleegd op 5 juli 2016.

305 http://europa.eu/rapid/press-release_IP-16-2461_en.htm, geraadpleegd 3 augustus 2016.

306 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, geraadpleegd op 5 juli 2016.

307 http://cybersecurityraad.nl/assets/csr_advies_cybersecurity_in_onderwijs_en_bedrijfsleven-vdef.pdf

308 Verder heeft het soc de taak om fraude-indicaties af te geven aan de anti-fraudeteams binnen de Belastingdienst. Middels het afgeven van deze indicaties is er voor vele miljoenen euro's aan mogelijk frauduleuze transacties tegen gehouden.

309 De Belastingdienst hanteert sinds 18 februari 2014 een responsible-disclosureprocedure, deze is op internet gepubliceerd, zie www.belastingdienst.nl/security.

310 http://gs.statcounter.com/#desktop-os-ww-monthly-201503-201603

311 https://blog.hboeck.de/archives/865-Software-Privdog-worse-than-Superfish.html, geraadpleegd op 5 juli 2016.

312 http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/23/response-to-concerns-regarding-edellroot-certificate, geraadpleegd op 5 juli 2016.

313 https://blogs.technet.microsoft.com/mmpc/2015/12/21/keeping-browsing-experience-in-users-hands/, geraadpleegd op 5 juli 2016.

314 https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/Monitor_OSb_2015_Definitief.pdf

315 https://www.aivd.nl/actueel/nieuws/2016/04/21/aivd-jaarverslag-breed-palet-aan-dreigingen-voor-nederland, geraadpleegd op 5 juli 2016.

316 De meting voor.nl-domeinnamen is pas uitgevoerd vanaf begin 2016. Daarom zijn enkele maanden buiten de rapportageperiode in de grafiek opgenomen, om zo meer inzicht te verschaffen.

317 Deze top 10 is bepaald aan de hand van de MX-records van de onderzochte domeinnamen. Het is denkbaar dat meerdere van deze leveranciers standaard e-mailafhandeling aan de domeinnaam koppelen, zonder daarvoor ook e-mailboxen beschikbaar te stellen.

318 De gegevens in deze paragraaf komen uit onderzoek dat onderdeel is van OpenINTEL (http://www.openintel.nl/), een gezamenlijk project van SURFnet, de Universiteit Twente en SIDN.

319 https://bratec.si/security/2016/04/27/road-to-hell-paved-with-saml-assertions.html, geraadpleegd op 5 juli 2016.

320 http://motherboard.vice.com/read/the-white-house-thinks-it-can-make-a-deal-with-companies-to-break-encryption, geraadpleegd op 5 juli 2016.

321 https://assets.documentcloud.org/documents/2714001/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf, geraadpleegd op 5 juli 2016.

322 http://www.apple.com/customer-letter/, geraadpleegd op 5 juli 2016.

323 https://blog.whatsapp.com/10000618/end-to-end-encryption, geraadpleegd op 5 juli 2016.

324 https://https.cio.gov/

325 https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie, geraadpleegd op 5 juli 2016.

326 https://www.tweedekamer.nl/kamerstukken/amendementen/detail?id=2015Z23825&did=2015D48058, geraadpleegd op 5 juli 2016.

327 http://www.routingmanifesto.org/

328 https://tn-init.nl/

329 https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/pia/310715_Managementsamenvatting_van_de_finale_versie_van_de_PIA.pdf

330 https://www.rijksoverheid.nl/documenten/kamerstukken/2016/02/17/kamerbrief-over-verzoek-overzicht-lopende-pilots-e-id-met-vermelding-van-deelnemende-partijen, geraadpleegd op 5 juli 2016.

331 http://www.betaalvereniging.nl/giraal-en-online-betalen/idin/, geraadpleegd op 5 juli 2016.
332 https://www.cybersecurityraad.nl/actueel/digitale-ketenveiligheid-krijgt-veel-te-weinig-aandacht.aspx, geraadpleegd op 13 juli 2016.
333 https://www.ncsc.nl/actueel/factsheets/factsheet-bescherm-domeinnamen-tegen-phishing.html
334 https://tools.ietf.org/html/rfc7672, geraadpleegd op 5 juli 2016.
335 http://www.consumentenbond.nl/campagnes/updaten/updates-naar-android6/, geraadpleegd op 5 juli 2016.
336 Bron: politie.
337 Bron: politie.
338 https://threatpost.com/security-researchers-sound-off-on-proposed-us-wassenaar-rules/113023/, geraadpleegd op 5 juli 2016.
339 https://langevin.house.gov/press-release/white-house-responds-langevin-and-mccaul-wassenaar-concerns, geraadpleegd op 5 juli 2016.
340 https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put, geraadpleegd op 5 juli 2016.
341 "Swatting" betekent het anoniem tippen bij de politie met als resultaat dat een SWAT team een inval doet bij een onschuldig slachtoffer.
342 http://www.dailydot.com/crime/lizard-squad-indicted-julius-kivimaki/, geraadpleegd op 5 juli 2016.
343 http://motherboard.vice.com/read/the-mysterious-disappearance-and-reappearance-of-a-dark-web-hacker-market, geraadpleegd op 5 juli 2016.
344 https://www.security.nl/posting/458110/FIOD+arresteert+man+wegens+phishingmails+Belastingdienst, geraadpleegd op 5 juli 2016.
345 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, geraadpleegd op 5 juli 2016.
346 https://googleonlinesecurity.blogspot.nl/2016/01/google-security-rewards, geraadpleegd op 5 juli 2016.
347 http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip
348 http://www.thegfce.com/news/news/2016/05/12/launch-manifesto-on-responsible-disclosure, geraadpleegd op 5 juli

Het mkb is belangrijk voor de economie, maar is kwetsbaar op digitaal gebied

6 Belangen

Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan. Het voorkomen van schade, ook via digitale weg, is in het belang van Nederland. Het kabinetsstandpunt over encryptie laat zien dat het kabinet de belangen van burgers, bedrijven en overheid vooropstelt. Het ziet geen mogelijkheden om encryptie te verzwakken zonder te raken aan deze belangen. De meldplicht datalekken kan ervoor zorgen dat organisaties meer aandacht besteden aan maatregelen om persoonsgegevens te beschermen. Het economisch belang van het midden- en kleinbedrijf voor Nederland is groot. Op het gebied van cybersecuritymaatregelen blijft deze groep echter achter.

Verstoring van ICT-systemen en inbreuken op de veiligheid ervan schaden de belangen van individuen, organisaties of de samenleving. Dit uit zich in belangen op het gebied van vrijheid, veiligheid en maatschappelijke groei.[349]

Maatschappelijke belangen

Vrijheid

ICT speelt een centrale rol in de samenleving. Fundamentele waarden en rechten staan dus niet meer los van de technische omgeving waarin ze voorkomen. Deze waarden en rechten moeten dan ook worden gewaarborgd in het digitale domein.

Veiligheid

De veiligheid van de samenleving in zijn geheel en van burgers in het bijzonder is voor een deel afhankelijk van ICT. Uitval van diensten en processen die ICT gebruiken, kan grote maatschappelijke gevolgen hebben op het gebied van veiligheid. Ook kan het de veiligheid van burgers aantasten. Vertrouwen in het digitale domein is essentieel voor het waarborgen van de veiligheid.

Maatschappelijke groei

De ontwikkeling van ICT en de innoverende kracht van technologische ontwikkeling zijn een belangrijke stimulans voor groei. Behalve economische groei gaat het ook om maatschappelijke groei. Digitalisering biedt de samenleving nieuwe mogelijkheden, bijvoorbeeld in de vorm van onderwijstoepassingen, mogelijkheden om sociale contacten te onderhouden en verbeterde overheidsvoorzieningen.

Ontwikkelingen van belangen

Belangen blijven vaak stabiel over een langere periode. Toch zijn er ontwikkelingen te zien: het gebruik van digitale middelen verandert. Deze ontwikkelingen richten zich veelal op het effect dat groei van het gebruik van digitale middelen heeft op de bestaande belangen.

Kabinetsstandpunt encryptie: geen maatregelen voor verzwakking encryptie

In januari 2016 stuurde het kabinet zijn standpunt[350] over encryptie aan de Tweede Kamer. Het standpunt van het kabinet is dat het belang van encryptie voor overheid, bedrijven en burgers groot is.

Cryptografie speelt een sleutelrol in de technische beveiliging in het digitale domein en veel cybersecuritymaatregelen in organisaties leunen sterk op de toepassing van encryptie, aldus het kabinet. Het kabinet is van mening dat er momenteel geen zicht is op mogelijkheden om encryptieproducten te verzwakken, zonder daarmee de belangen van overheid, bedrijfsleven en burger te raken. Het introduceren van een technische ingang in encryptieproducten om het voor opsporingsinstanties mogelijk te maken om versleutelde bestanden te kunnen inzien, bijvoorbeeld, zou digitale systemen kwetsbaar kunnen maken voor bijvoorbeeld criminelen, terroristen en statelijke actoren.

De overheid communiceert steeds meer digitaal. Een van de afspraken uit het Regeerakkoord is dat in 2017 alle communicatie tussen burgers en bedrijven en de overheid digitaal mogelijk moet zijn. Ook informatie binnen de overheid is in toenemende mate digitaal. Voor deze zaken zijn de mogelijkheden van encryptie essentieel. Encryptie kan ervoor zorgen dat deze gegevens beschermd zijn tegen kennisneming door derden.

Encryptie stelt bedrijven in staat bedrijfsinformatie veilig te bewaren en versturen. Als zij encryptie kunnen gebruiken, dan versterkt dat de internationale concurrentiepositie van Nederland. Vertrouwen in veilige communicatie en opslag van data is essentieel voor de (toekomstige) groeipotentie van de Nederlandse economie. Deze zit vooral in de digitale economie. De belangen van bedrijven op het gebied van maatschappelijke groei worden hiermee beschermd.

Ten slotte ondersteunt encryptie burgers om zichzelf te beschermen tegen inbreuken op persoonlijke levenssfeer en tegen beperking van vrijheid van meningsuiting. Hiermee kunnen burgers hun belangen op het gebied van vrijheid en veiligheid te beschermen.

Encryptie biedt overheid, bedrijfsleven en burgers voordelen. Tegelijkertijd biedt het kwaadwillenden ook de mogelijkheid hun gedragingen in het digitale domein te verhullen. Daarmee kunnen ze uit het zicht blijven van opsporings-, inlichtingen- en veiligheidsdiensten. Dit raakt aan het veiligheidsbelang. Het kabinet acht het nemen van beperkende wettelijke maatregelen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland op dit moment niet wenselijk.

Meldplicht datalekken

De meldplicht datalekken[351] die op 1 januari 2016 is ingegaan, draagt bij aan de eerbiediging en de bescherming van de persoonlijke levenssfeer. Iedereen die persoonsgegevens verwerkt moet deze beveiligen tegen verlies en onrechtmatige verwerking. Als deze beveiliging faalt, en er een inbreuk is op de beveiliging van persoonsgegevens, dan is er een datalek. Ernstige datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens. In bepaalde gevallen moet het datalek ook gemeld worden aan de betrokkene.

De invoering van de meldplicht datalekken had voor veel bedrijven impact. Zij moesten nadenken over hoe en wanneer de organisatie overgaat tot het melden van een datalek, en in veel gevallen moesten organisaties hun interne werkwijze aanpassen om datalekken, de melding ervan en boetes en mogelijke imagoschade te voorkomen. Dit kan bedrijven aanmoedigen betere maatregelen te nemen om persoonsgegevens te beschermen.

Cybersecurity bij het mkb van belang voor de samenleving

Het mkb vormt een grote groep bedrijven en is goed voor 61 procent van het bruto binnenlands product.[352] Veel vitale processen zijn onderdeel van een keten, waar bedrijven uit het mkb ook vaak onderdeel van uitmaken. Het mkb is dus niet alleen belangrijk voor de economie, maar ook voor de samenleving. Dit terwijl het mkb een lage weerbaarheid heeft op digitaal gebied. Samen met de groeiende dreiging van beroepscriminelen vormt dit een groeiend risico voor het economisch belang van Nederland.

Grote bedrijven en organisaties investeerden de afgelopen jaren vrijwel altijd in meer of mindere mate in cybersecuritymaatregelen. Dit geldt niet voor het mkb. Uit onderzoek van Interpolis blijkt dat ondernemers het risico van digitale dreigingen onderschatten.[353] Een derde van de onderzochte bedrijven besteedt niet regelmatig aandacht aan digitale dreigingen. Veel bedrijven in het mkb kunnen zich geen voorstelling maken bij cybercrime. De beschermingsmaatregelen die ze nemen zijn basaal, zoals het gebruik van virusscanners, firewalls en het versleutelen van wifi-verbindingen. Dit is opvallend, omdat uit onderzoek blijkt dat 74 procent van de bedrijven uit het mkb in grote mate of volledig afhankelijk zegt te zijn van ICT.[354] Hetzelfde onderzoek meldt dat ruim 28 procent van het mkb slachtoffer is geweest van cybercrime.

De afgelopen jaren is er wel aandacht besteed aan digitale veiligheid bij het mkb. De jaarlijkse campagne Alert Online had, om het mkb beter te bereiken, digitaal verantwoord ondernemen als thema.[355] Dit lijkt echter onvoldoende om het mkb, als essentiele partij in de maatschappij en in vitale processen, goed genoeg te beschermen.

Kwaliteitseisen als impliciete verwachting

ICT-systemen en het internet vormen een integraal onderdeel van veel processen binnen de samenleving. De overheid zet in op communicatie met de burger via internet en richt haar dienstverlening in via digitale portalen. Voor het bedrijfsleven is de analoge wereld op sommige punten al langer een gedachte uit het verleden. Dit is niet nieuw, maar de trend zet wel door. Wat opvalt, is dat gebruikers impliciet kwaliteitseisen stellen aan ICT in de breedste zin. Ze verwachten dat ICT-processen bestand zijn tegen verstoringen op het gebied van beschikbaarheid en aantasting van integriteit en vertrouwelijkheid. Deze verwachtingen worden vaak niet uitgesproken. De verwachting en het daadwerkelijke resultaat van genomen maatregelen komen dus niet overeen.

Vanuit traditioneel informatiebeveiligingsoogpunt worden eisen gesteld aan beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen. Dienstverleners op hun beurt voelen de noodzaak van 'goed huisvaderschap' voor de informatie van klanten.[356] Zelfs als contractueel afgesproken beschikbaarheidseisen gehaald worden, maar er toch een verstoring optreedt, wordt de verwachting van klanten gevoeld dat er geen rekening gehouden wordt met hun onuitgesproken eisen. De eis voor 99,9 procent beschikbaarheid kan afgesproken zijn, terwijl tijdens de kerstdagen impliciet verwacht wordt dat dit 100 procent is.

Ook op andere vlakken komt dit voor. Consumenten kennen van hun mobiele aanbieder een bepaalde kwaliteit. Deze verwachten ze ook in het zakelijk gebruik. Speciale abonnementen voor hoge beschikbaarheid en specifieke dienstverlening worden vanwege kostenoverwegingen overgeslagen.[357] Het bedrijfsleven kiest liever voor goedkopere standaardabonnementen voor bijvoorbeeld zakelijk dataverkeer. Door kostenbesparingen en impliciete verwachtingen loopt het bedrijfsleven onnodig risico's.

Het kabinetsstandpunt over encryptie laat zien dat het kabinet de belangen van burgers, bedrijven en overheid voorop stelt. Het ziet geen mogelijkheden om encryptie te verzwakken zonder te raken aan deze belangen. De meldplicht datalekken gaat samen met de mogelijkheid om sancties op te leggen aan organisaties met datalekken. Dit kan deze organisaties stimuleren de beveiliging van deze gegevens op orde te krijgen en te houden.

Het mkb is belangrijk voor Nederland. Veel ketens bevatten bedrijven uit het mkb, zo ook ketens binnen de vitale processen. Qua cybersecuritymaatregelen blijft deze groep achter. Dat betekent een risico voor de vitale processen en daarmee voor de Nederlandse samenleving.

Gebruikers stellen impliciet hoge kwaliteitseisen aan digitale dienstverlening. Zonder dit af te spreken gaan zij ervan uit dat beschikbaarheid, integriteit en vertrouwelijkheid hoog is. Dienstverleners voelen de noodzaak van 'goed huisvaderschap', maar kunnen niet aan alle impliciete verwachtingen voldoen.

Conclusie en vooruitblik

Cybersecurity raakt aan de belangen van individuen, organisaties en de samenleving. Dit zijn belangen op het gebied van vrijheid, veiligheid en maatschappelijke groei. Deze belangen blijven vaak langere tijd stabiel. Het afgelopen jaar is op dit gebied een aantal ontwikkelingen waargenomen.

Noten

349 Nationale Cybersecurity Strategie 2, https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2.

350 https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie, geraadpleegd op 5 juli 2016.

351 https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

352 http://www.staatvanhetmkb.nl/nieuws/kernpublicatie-de-staat-van-het-mkb-2015, geraadpleegd op 5 juli 2016.

353 https://www.interpolis.nl/DocumentenLijst/rapport-mkb-cybersecurity.pdf

354 Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland. https://www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/Cybercrime%20onder%20bedrijven%20definitief%20rapport.pdf

355 https://ecp.nl/actueel///4492/alert-online-maakt-vliegende-start-met-eerste-netwerkbijeenkomst.html, geraadpleegd op 5 juli 2016.

356 Bron: input aan het NCSC vanuit de MSP-isac.

357 Bron: input aan het NCSC vanuit de Telecom-isac.

Bijlagen

Bijlage 1 NCSC-statistieken

Deze bijlage geeft een overzicht van de responsible-disclosuremeldingen, beveiligingsadviezen en incidenten die door het NCSC zijn afgehandeld. Het NCSC registreert en houdt incidenten bij met een registratiesysteem. Dit systeem is de bron voor alle grafieken in deze bijlage. Ook dit jaar is het aantal afgehandelde incidenten en gepubliceerde beveiligingsadviezen groter dan het jaar daarvoor. Dit jaar heeft het NCSC ongeveer 5 procent meer incidenten afgehandeld en 25 procent meer nieuwe beveiligingsadviezen geschreven dan het jaar daarvoor.

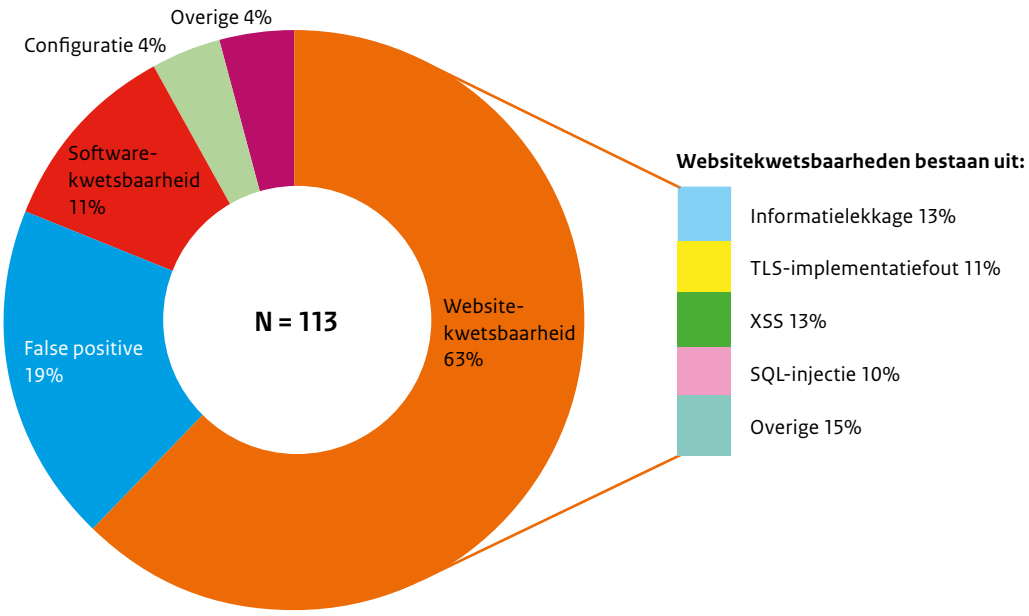
Het NCSC faciliteert het doen en het verwerken van responsible-disclosuremeldingen voor zowel haar eigen infrastructuur als die van de Rijksoverheid en enkele private partijen. Het brengt beveiligingsadviezen voor zijn deelnemers uit en handelt cybersecurityincidenten af. Hierover zijn voor deze rapportageperiode (mei 2015 tot en met april 2016) statistieken berekend die hieronder worden gepresenteerd. Door deze statistieken te vergelijken met eerdere rapportageperiodes worden trends en ontwikkelingen zichtbaar.

Responsible disclosure

In de rapportageperiode heeft het NCSC 113 responsible-disclosure-meldingen ontvangen. Dit zijn zowel meldingen voor eigen systemen als voor andere 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 totale aantal meldingen niet representatief voor het totale aantal kwetsbaarheden. In 19 procent van alle meldingen was er bij nader onderzoek 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 brute-forceaanvallen. Deze gevallen werden geclassificeerd als false positive. Vorig jaar was dit 20 procent van alle meldingen.

Figuur 12 toont de verschillende typen meldingen. De meerderheid (63 procent) van alle meldingen hebben 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 versienummer van een webapplicatie of een configuratiebestand te zien. In 11 procent van alle meldingen is er sprake van een kwetsbaarheid in software (exclusief webservers en -applicaties). Relatief weinig meldingen (4 procent) hebben te maken met configuratiefouten in hard- en software.

Figuur 12 **Typen responsible-disclosuremeldingen**

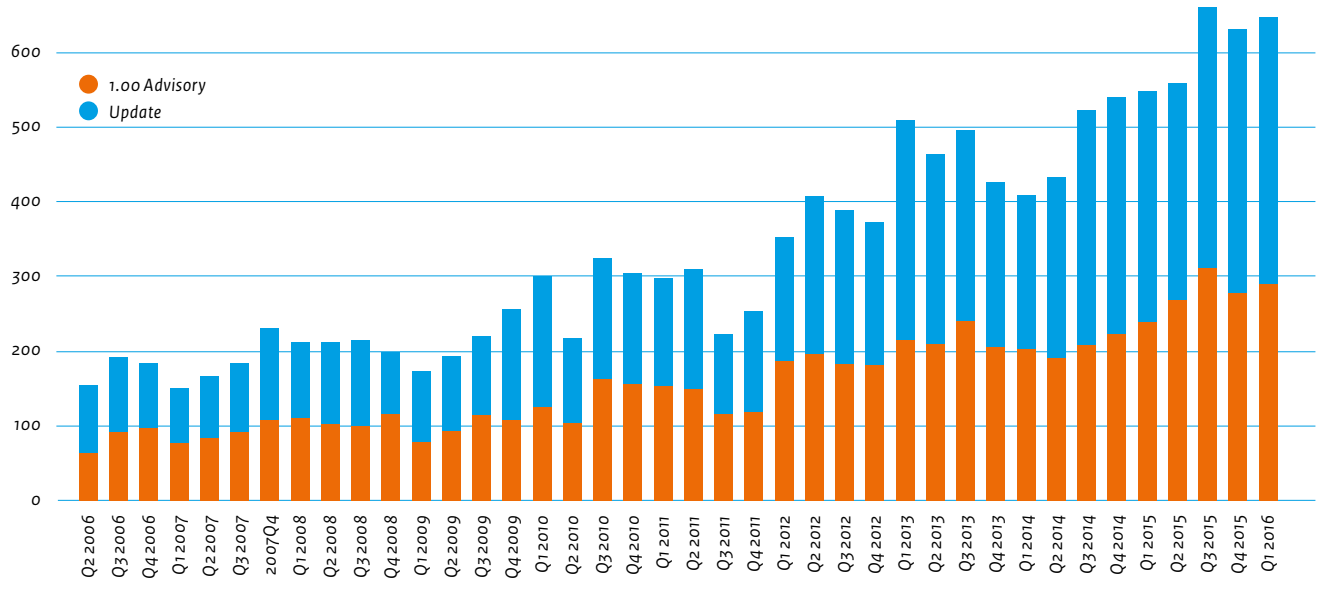


Bron: NCSC.

Beveiligingsadviezen

Het NCSC publiceert beveiligingsadviezen (advisories) naar aanleiding van softwarekwetsbaarheden of geconstateerde dreigingen. Een beveiligingsadvies beschrijft wat er aan de hand is, welke systemen mogelijk getroffen zijn en wat er moet gebeuren om te voorkomen dat een organisatie slachtoffer wordt. Figuur 13 toont het aantal adviezen dat het NCSC heeft gepubliceerd per kwartaal van het tweede kwartaal van 2006 tot en met het eerste kwartaal van 2016. Hierbij wordt onderscheid gemaakt tussen nieuwe advisories (met versienummer 1.00) en updates van bestaande advisories. In totaal heeft het NCSC 1133 beveiligingsadviezen gepubliceerd in de afgelopen rapportageperiode. Dit is ongeveer 25 procent meer dan het jaar daarvoor. Deze toename kan deels verklaard worden door het groeiende aantal deelnemers dat het NCSC bedient. De groei van het aantal deelnemers leidt tot een groei in de lijst van software en systemen waarvoor het NCSC beveiligingsadviezen schrijft.

Figuur 13 **Aantal advisories per kwartaal (2006Q2 - 2016Q1)**



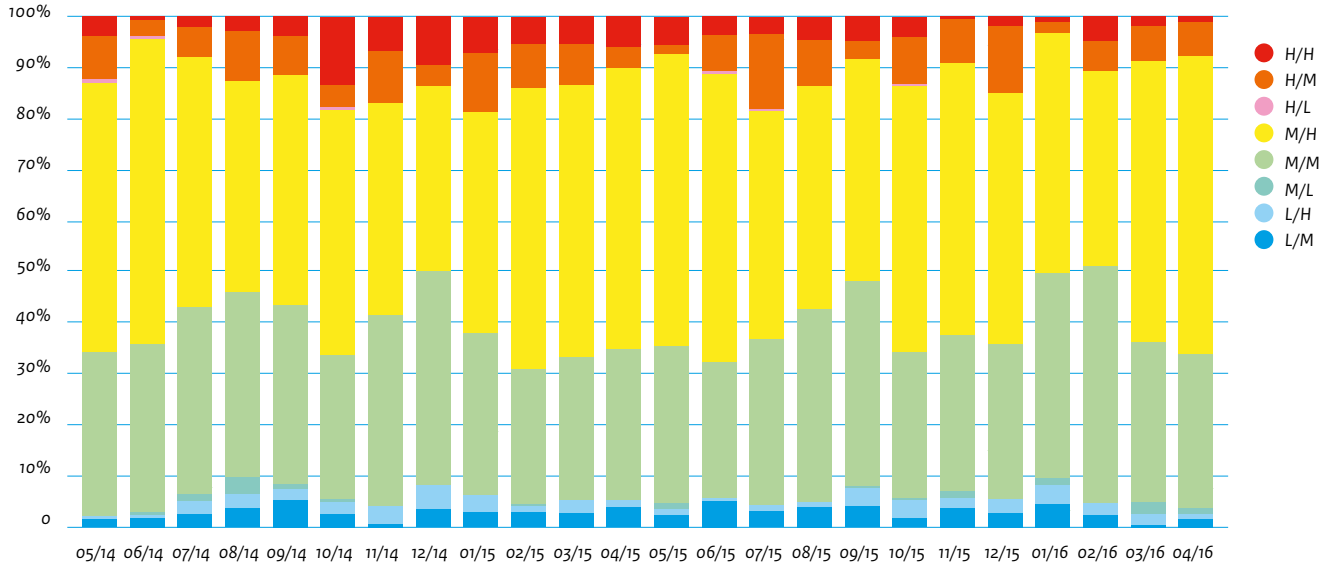
Bron: NCSC.

De beveiligingsadviezen van het NCSC worden ingeschaald op twee elementen. Ten eerste stelt het vast wat de kans is dat de kwetsbaarheid misbruikt wordt. Ten tweede bepaalt het NCSC de schade die optreedt wanneer de kwetsbaarheid misbruikt wordt. 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 14 toont de verhoudingen tussen deze niveaus voor alle gepubliceerde adviezen (inclusief updates) per maand voor de afgelopen twee rapportageperiodes.

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 3 rapportageperiodes wordt het percentage adviezen per schadeomschrijving in tabel 3 getoond. Beveiligingsadviezen die te maken hebben met denial-of-service (DoS) blijken nog altijd het grootste aandeel te hebben (56 procent). Hierna volgen het uitvoeren van willekeurige code met gebruikersrechten (37 procent), toegang tot gevoelige gegevens (32 procent) en het omzeilen van een beveiligingsmaatregel (25 procent). Dit waren ook in de vorige rapportageperiode de meest voorkomende beveiligingsadviezen. Regelmatig zijn bij een advies meerdere schadeomschrijvingen van toepassing.

Figuur 14 **Inschaling advisories in de rapportageperiode**



Bron: NCSC.

Tabel 3 **Percentage beveiligingsadviezen per schadeomschrijving CSBN4 t/m CSBN-2016**

Schadeomschrijving	2014	2015	2016
Denial-of-service (DoS)	46%	51%	56%
Remote code execution (gebruikersrechten)	31%	29%	37%
Toegang tot gevoelige gegevens	24%	26%	32%
Omzeilen van beveiligingsmaatregelen	13%	19%	25%
Verhoogde gebruikersrechten	21%	14%	21%
Toegang tot systeemgegevens	8%	9%	13%
Cross-site scripting (XSS)	11%	6%	9%
Manipulatie van gegevens	6%	5%	8%
Omzeilen van authenticatie	6%	4%	5%
Remote code execution (admin/rootrechten)	4%	4%	6%
Spoofing	4%	2%	5%
Cross-site request forgery (XSRF)	3%	1%	2%
SQL-injectie	2%	1%	2%

Cybersecurityincidenten geregistreerd bij het NCSC

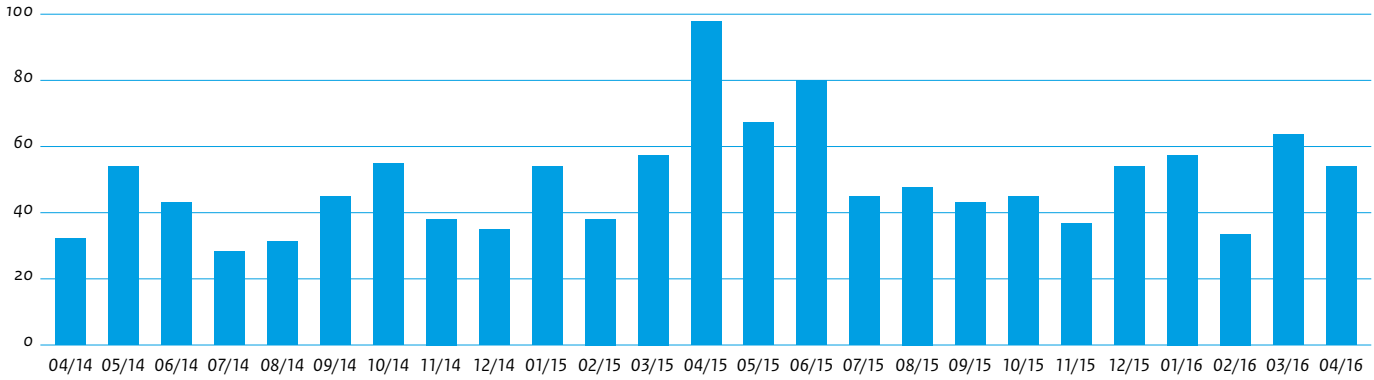
Het NCSC ondersteunt overheden en organisaties in de vitale infrastructuur bij het afhandelen van incidenten op het gebied van ICT-veiligheid. In die rol worden bij het NCSC incidenten en kwetsbaarheden gemeld. Het NCSC identificeert ze zelf ook, bijvoorbeeld op basis van diverse detectiemechanismen. Op verzoek van (inter)nationale partijen ondersteunt het NCSC Nederlandse internetserviceproviders 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

Figuur 15 toont het aantal afgehandelde incidenten per maand (exclusief geautomatiseerde controles) voor de laatste twee rapportageperiodes. In de vorige rapportageperiode waren er in totaal 598 incidenten gemeld: gemiddeld 46 per maand. In deze rapportageperiode zijn er 629 incidenten gemeld: 52 per maand. Dit verschil kan deels verklaard worden door het groeiende aantal deelnemers dat het NCSC bedient.

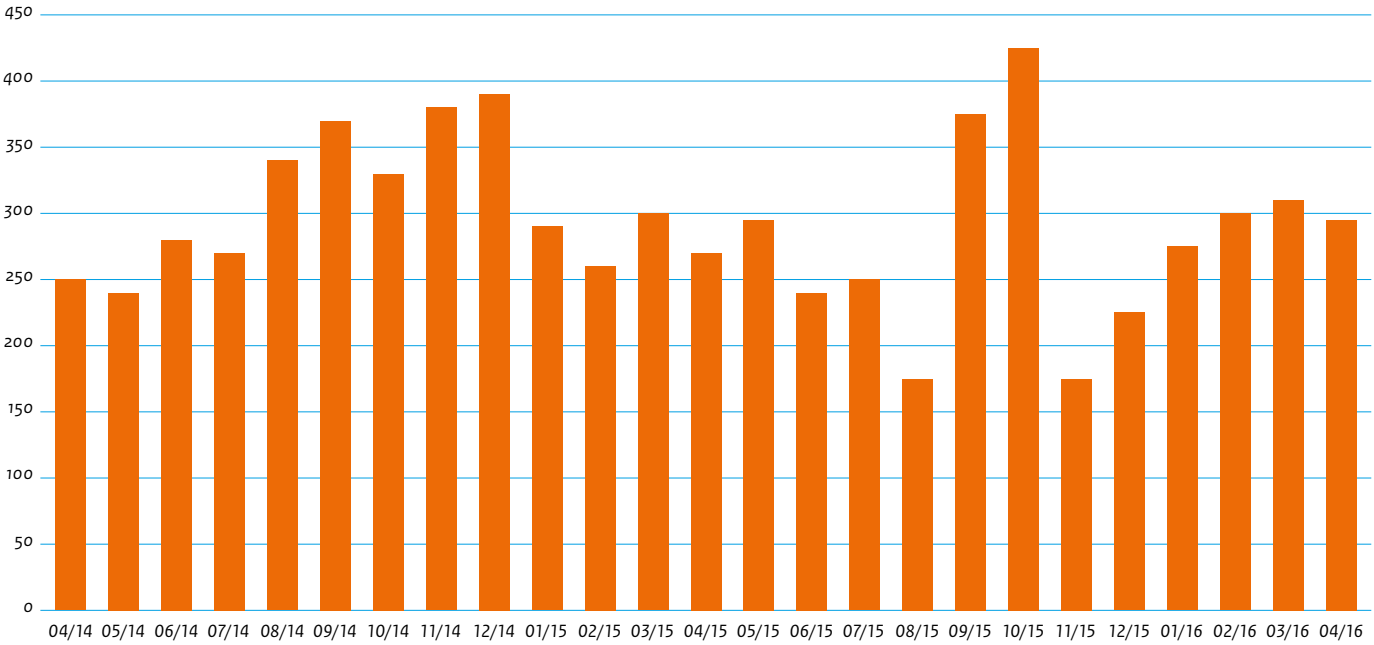
Figuur 16 toont de resultaten van geautomatiseerde controles voor de laatste twee rapportageperiodes. Hieruit blijkt dat er in de afgelopen rapportageperiode gemiddeld 280 incidentenmeldingen per maand zijn op basis van deze automatisering. In de vorige rapportageperiode waren er gemiddeld 300 meldingen per maand.

Figuur 15 **Afgehandelde incidenten (exclusief geautomatiseerde controles)**



Bron: NCSC.

Figuur 16 **Geautomatiseerde controles**



Bron: NCSC.

Een melding kan meerdere geïnfecteerde systemen binnen een organisatie betreffen.

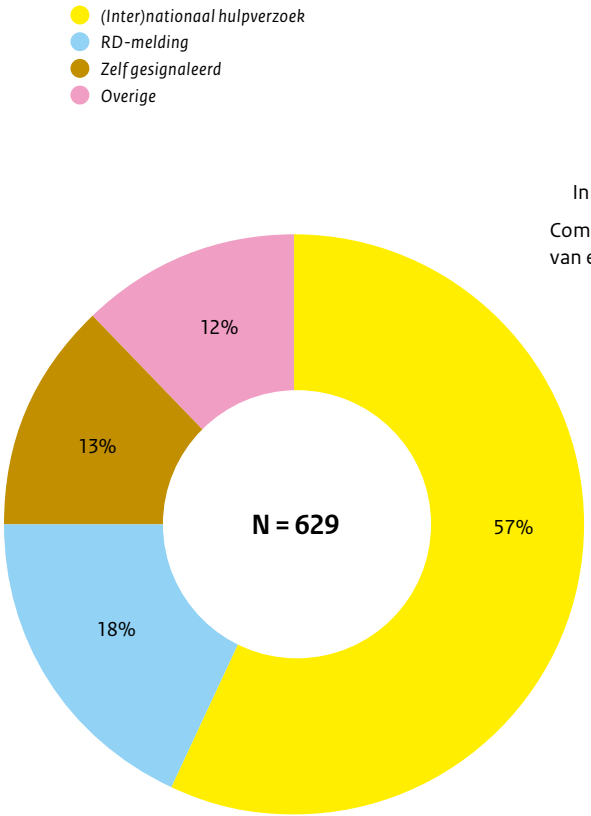
Verdeling incidenten per melding, categorie en afhandeling

Voor de volgende analyses heeft het NCSC gebruikgemaakt van een andere incidententaxonomie dan is gebruikt in voorgaande rapportages. Deze analyses zijn daarom moeilijk te vergelijken met analyses uit andere rapportages. Deze taxonomie is voorgesteld door CERT.PT[358] en wordt aanbevolen door ENISA[359] als een gemeenschappelijke taxonomie voor het internationale netwerk van Computer Security Incident Response Teams (CSIRT's). Door deze taxonomie te hanteren, wordt het makkelijker om de analyses te vergelijken met andere CSIRT's. Een gemeenschappelijke taxonomie maakt het ook mogelijk om incidenteninformatie uit te wisselen met partnerorganisaties voor incidentrespons.

Figuur 17 toont de verdeling van incidenten naar meldingstype. Het merendeel van de incidentmeldingen (57 procent) komt van buitenaf: van nationale of internationale bronnen. Bij 18 procent van alle incidenten komt de melding binnen via responsible disclosure. 13 procent van alle gevallen betreft eigen signalering. Voorbeelden hiervan zijn een waarschuwing uit een eigen detectiemechanisme of een bericht uit een openbare bron. In het overige 12 procent van de meldingen was er sprake van een PKI-meldplichtmelding, informatie die ter kennisgeving is aangenomen, geautomatiseerde meldingen waarbij extra handmatige acties nodig waren of andere diverse meldingen.

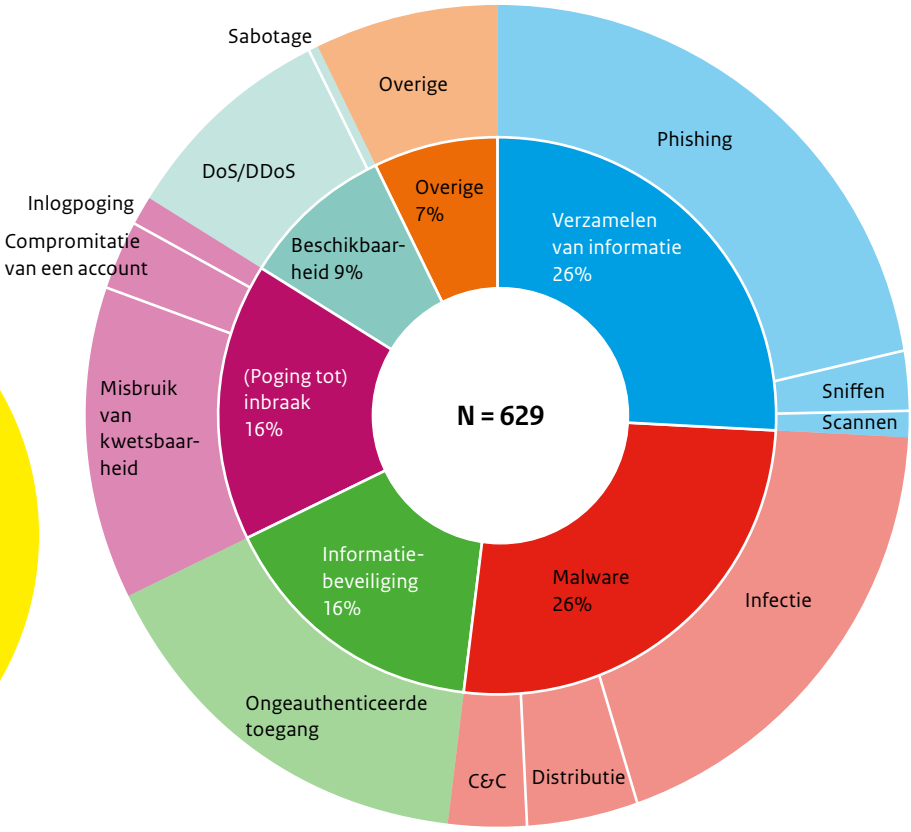
Figuur 18 toont de verdeling incidenten per categorie. In de binnenste ring worden de hoofdcategorieën getoond, terwijl de buitenste ring de subcategorieën duidt. Hieruit blijkt dat incidenten waarbij er sprake is van informatieverzameling voor meer dan een kwart (26 procent) van alle incidenten heeft gezorgd. Het overgrote merendeel hiervan betreft phishing. Malware-incidenten hebben voor 26 procent van alle incidenten gezorgd. Het merendeel hiervan heeft met malwarebesmetting te maken. In 16 procent van alle incidenten was er sprake van ongeautoriseerde toegang. (Poging tot) inbraak zorgt voor 16 procent van alle incidenten. Hierbij gaat het voornamelijk om het misbruik van een kwetsbaarheid. Slechts 9 procent van alle incidenten hadden te maken met beschikbaarheid. Bijna al deze incidenten betreffen Denial-of-Service (DoS) aanvallen of dreigingen. Het resterende deel (7 procent) heeft te maken met diverse incidenten waaronder het versturen van spam of fraude.

Figuur 17 Afgehandelde incidenten per meldingstype



Bron: NCSC.

Figuur 18 Afgehandelde incidenten per categorie



Bron: NCSC.

In figuur19 staat de verdeling incidenten per afhandeling. 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 26 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.

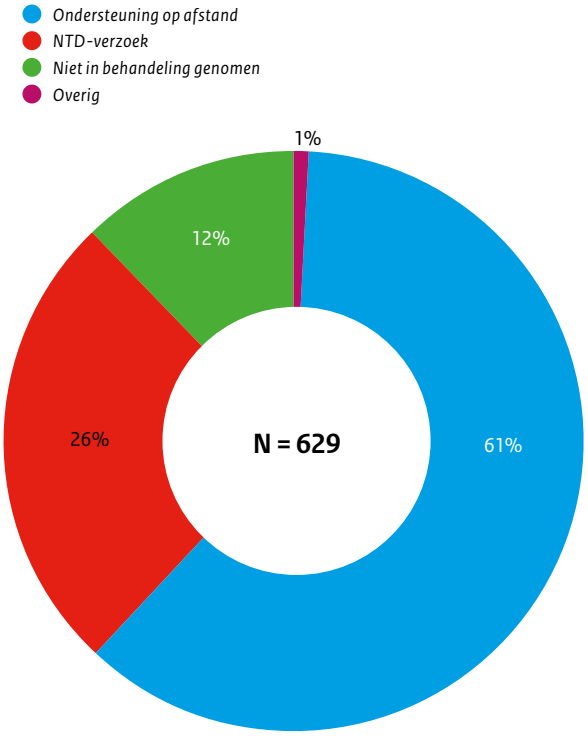
Verdeling incidenten tussen overheid en vitale infrastructuur

Het NCSC ondersteunt zowel de Rijksoverheid als de vitale infrastructuur bij beveiligingsincidenten. Daarnaast treedt het NCSC op als contactpunt voor internationale hulpverzoeken over informatiebeveiliging.

In figuur 20 is te zien wat de verdeling is van het aantal afgehandelde incidenten tussen publieke, private en internationale partijen. In totaal was bij ongeveer 43 procent van de incidenten een publieke organisatie betrokken. Bij 35 procent ging het om een private organisatie. Het resterende 22 procent betrof een internationale partij. In vergelijking met de vorige rapportageperiode heeft het NCSC twee keer zoveel incidenten afgehandeld van 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 malafide website offline te halen die in Nederland wordt gehost.

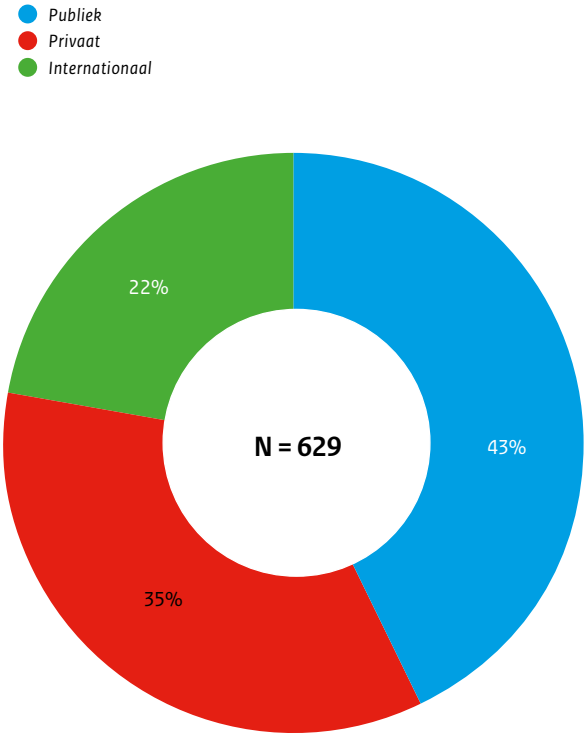
Figuur 21 toont de verdeling tussen incidentcategorieën per type organisatie. Onderaan iedere kolom wordt aangegeven over welk type organisatie de verdeling gaat en hoeveel incidenten daarin worden vertegenwoordigd. Incidenten met malware zijn verantwoordelijk voor ongeveer en kwart van alle incidenten ongeacht het type organisatie. Bij incidenten die onder de categorie 'verzamelen van informatie' vallen, is het verschil nog groter.

Figuur 19 **Afgehandelde incidenten per afhandeling**



Bron: NCSC.

Figuur 20 **Afgehandelde incidenten per type organisatie**



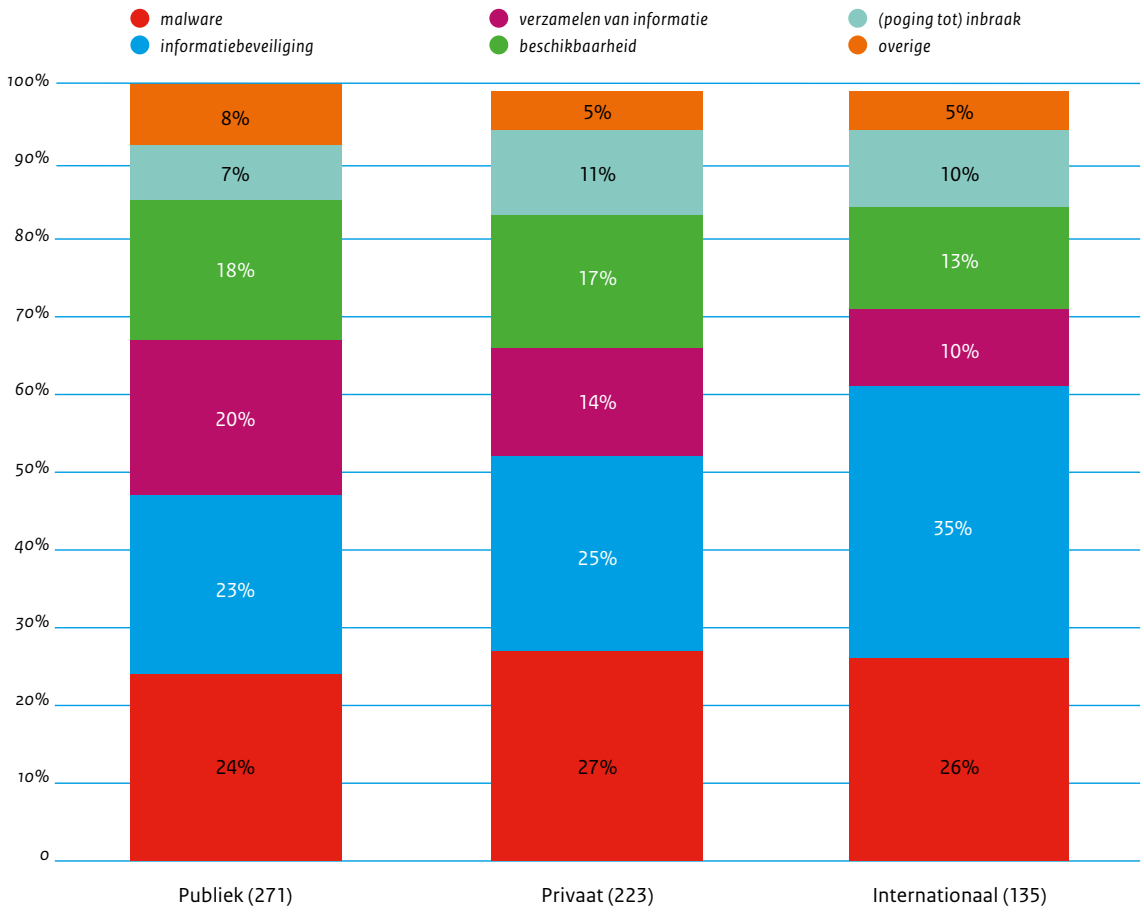
Bron: NCSC.

In 35 procent van alle gevallen waar er een internationale partij betrokken is, gaat het om deze categorie. In de praktijk heeft het merendeel van deze incidenten met phishingcampagnes te maken.

Uit deze figuur blijkt verder dat (poging tot) inbraak vaker voorkomt bij incidenten in de publieke sector (20 procent) dan bij een private partij (14 procent) of internationale partij (10 procent). Een dergelijke verdeling is ook te zien bij incidenten die met 'informatiebeveiliging' te maken hebben. Zulke incidenten betreffen vaak ongeautoriseerde toegang tot gevoelige informatie of systemen.

Een voorbeeld hiervan is het melden van een websitekwetsbaarheid waarmee een aanvaller een klantenbestand in kan zien. Bij incidenten waar er sprake is van een aanval op de beschikbaarheid (availability) van een organisatie is er een duidelijker verschil tussen publieke organisaties (6 procent) en de rest (gemiddeld 11,5 procent).

Figuur 21 **Incidentcategorieën per type organisatie**



Bron: NCSC.

Noten

358 http://www.cncs.gov.pt/home/index.html

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

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	Dreigingen: middelen
Drinkwatervoorziening	Er zijn vooral manifestaties waargenomen van ransomware, phishing en DDoS-aanvallen.	De sector heeft geen beeld van specifieke actoren die een dreiging vormen. Wel worden interne actoren genoemd als belangrijke actor.	Malware, phishing en DDoS-aanvallen op de kantoorautomatisering; malware op de procesautomatisering.
Energie	Er zijn vooral manifestaties waargenomen van ransomware, phishing en DDoS-aanvallen.	De grootste dreiging voor deze sector vormen statelijke actoren en interne actoren.	Er vindt veel (spear)phishing plaats. DDoS-as-a-service, onder andere via booterservices, wordt gezien als middel dat gebruikt wordt.
Financiële instellingen	Er zijn beperkt ransomware-infecties waargenomen. Deze lijken gericht op medewerkers als privépersoon en niet specifiek op de financiële sector. Aanvallen op klanten van banken zijn verschoven van massale aanvallen naar grote groepen (particuliere) klanten naar gerichte aanvallen op (vaak zakelijke) klanten.	Als grootste dreigingen worden criminelen en (in mindere mate) interne actoren gezien.	Er wordt beperkt (spear)phishing waargenomen. Daarnaast wordt malware hergebruikt door verschillende partijen. Criminelen richten zich meer op medewerkers van banken, naast klanten van banken.

Weerbaarheid: kwetsbaarheden	Weerbaarheid: maatregelen	Belangen
De mens blijft een zwakke schakel. Daarnaast wordt afhankelijkheid van derde partijen als kwetsbaarheid gezien.	Er wordt gewerkt aan securityframeworks en het segmenteren van netwerken en afschermen van de segmenten. Geplande vernieuwing van procesautomatiseringssystemen is aan de orde. Er wordt, naast preventie, meer gewerkt aan detectie en respons.	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 grootste kwetsbaarheden worden gezien in de ketenafhankelijkheden.	Er wordt gewerkt aan verdere segmentering van netwerken. Monitoring van netwerken, ook van ICS-netwerk, is in opkomst. Pentesting wordt vaker toegepast.	Er zijn diverse ontwikkelingen in de belangen. Door just-in-time neemt de impact van grote verstoringen toe. Ketenafhankelijkheden nemen toe. De afhankelijkheid van buitenlandse partijen neemt toe, ook door overnames in de cybersecuritysector. Er ontstaat steeds meer behoefte aan informatie-uitwisseling tussen verschillende omgevingen. Deze koppelingen kunnen leiden tot risico's door verschillende beveiligingsmaatregelen.
Waargenomen kwetsbaarheden zijn de mogelijkheid dat veelgebruikte DDoS-mitigatieproviders zelf aangevallen worden en implementatiefouten in reeds jarenlang gebruikte encryptiebibliotheken (Heartbleed, DROWN).	Organisaties hebben door actuele back-ups minder last van de gevolgen van ransomwarebesmettingen dan particulieren. Beschermen tegen DDoS-aanvallen is duur, maar inmiddels business as usual. Banken monitoren steeds beter, ook zijn de oplossingen voor authenticatie steeds vaker what-you-see-is-what-you-sign. Bovendien helpt de samenwerking met het Electronic Crimes Task Force bij opsporing.	Vergaande automatische gegevensuitwisseling en -combinaties verhogen de impact van onjuiste informatie voor de klant. Het belang van goede bescherming groeit door toenemend gebruik van digitale middelen en wegvallen van analoge middelen (zoals loket, telefoon). Veiligheid is niet altijd de aanleiding om een (politiek) besluit te nemen en delft soms het onderspit ten opzichte van kosten en gebruikersgemak.

Sector	Manifestaties	Dreigingen: actoren	Dreigingen: middelen
Managed Service Providers	Door de MSP's zijn manifestaties waargenomen van cryptoware, DDoS-aanvallen, social engineering, (digitaal ondersteunde) factuurfraude en spionage.	Meerdere keren per jaar hebben de MSP's te maken met geavanceerde aanvallen waarvan door sommige organisaties vermoed wordt dat het om statelijke actoren gaat. Daarnaast vormen criminelen, hacktivisten en onderzoekers een dreiging voor de sector.	Cybercrime-as-a-service wordt als dreiging gezien. Reflectie-aanvallen worden veel gezien. Sociale media door organisaties gebruikt voor legitieme doelen worden misbruikt om gegevens te verzamelen over doelen. Booterservices worden gebruikt voor het uitvoeren van DDoS-aanvallen.
Nucleair	Er zijn manifestaties waargenomen van phishing, malware, telefoonfraude, CEO-/CFO-fraude. Deze lijken niet gericht op de sector en manifesteren zich op kantoorautomatiseringssystemen.	Statelijke actoren, criminelen en interne actoren (inclusief leveranciers) vormen een dreiging voor de sector.	Generieke malware in combinatie met het koppelen met systemen van derde partijen vormt een belangrijke dreiging.
Rijksoverheid	De sector kampt met een groeiende hoeveelheid DDoS-aanvallen. Phishing is aan de orde van de dag, cryptowarebesmettingen komen wekelijks voor. Daarnaast komt interne fraude voor.	Statelijke actoren en criminelen zijn belangrijke dreigingen voor de Rijksoverheid. Daarnaast vormen interne actoren een (vaak onbewuste) dreiging.	Voor een breed publiek beschikbare malware wordt actief gebruikt (cybercrime-as-a-service). Actoren professionaliseren verder. Gebruikelijke methoden als e-mail voor (spear) phishing en Tor voor communicatie door malware wordt gezien. Er is regelmatig malware in of bij portable apps gesignaleerd, (onbewust) in gebruik bij interne actoren.
Telecom	De sector had te maken met een kwetsbaarheid in een implementatie van TN69, een protocol voor het op afstand beheren van modems. Daarnaast zijn er veel ransomware-infecties waargenomen. DDoS-aanvallen zijn er veel, maar deze zijn voor het grootste deel van korte duur. Daarnaast heeft de sector last van criminelen die zich uitgeven voor telecombedrijven en via phishing en webwinkels stelen.	De belangrijkste actoren die een dreiging vormen voor de telecomsector zijn statelijke actoren en criminelen.	Actoren lijken veel booterservices te gebruiken voor DDoS-aanvallen. Daarnaast worden veel phishing-e-mails verstuurd om malware te verspreiden.

Weerbaarheid: kwetsbaarheden	Weerbaarheid: maatregelen	Belangen
Kleine partijen zijn kwetsbaar voor DDoS-aanvallen rondom drukke periodes zoals de feestdagen. Standaardbibliotheken, zoals TLS-implementaties, vormen vaak een kwetsbaarheid zonder dat men zich dat realiseert. Het mengen van privégebruik en zakelijk gebruik van mobiele apparaten zorgt voor kwetsbaarheden. Het niet kunnen updaten van mobiele apparaten maakt in korte tijd een grote groep gebruikers kwetsbaar.	Beveiligingsbewustzijn blijft cruciaal. Om dit te verbeteren worden bij diverse organisaties interne phishingtests uitgevoerd. Maatregelen die werken zijn bijvoorbeeld conservatieve maatregelen zoals het niet aan het internet koppelen van beheersinterfaces.	Gebruikers hebben impliciet de verwachting dat sterke maatregelen genomen zijn, terwijl dit niet altijd het geval is. Tegelijkertijd worden door kostendruk meer single points of failure geïntroduceerd. Ketenafhankelijkheden vormen een groeiende uitdaging en zijn niet 1-op-1, maar veel-op-veel. Nederland als digitale mainport kan zorgen voor economische groei, maar zorgt er tegelijkertijd voor dat de dreiging groter is.
Er is een verschuiving zichtbaar door introductie van digitale systemen.	Met de Cyber Design Basis Threat is gewerkt aan het weerbaar maken van de sector tegen de belangrijkste dreigingen. De sector doet aan collegiale toetsing op het gebied van securitymaatregelen.	Gezien de externe veiligheidsaspecten binnen de sector is nucleaire veiligheid voor de sector van groot belang. ICT heeft vooral een rol bij bijvoorbeeld toegangsbeveiligingsmaatregelen. ICT is ondersteunend aan het primaire proces.
Aandacht voor interne (netwerk)monitoring is te beperkt, de aandacht ligt nog teveel op verkeer van en naar buiten. Bovendien wordt logging nog te weinig proactief bekeken, reageren op incidenten is de norm. Door vermenging van zakelijk en privé ontstaan kwetsbaarheden. Er is een gebrek aan cybersecuritykennis bij zowel bestuurders als de politiek. Het staat nog niet op het netvlies. Er bestaan nog steeds single-points-of-failure in software. Organisaties hadden te maken met kwetsbare servers die van buiten bereikbaar waren.	In contracten met leveranciers wordt cybersecurity structureler opgenomen. Netwerkbeveiliging wordt steeds beter ingericht. Er is samenwerking tussen verschillende partijen, onder andere op het gebied van best practices en SOC's. Deze samenwerking wordt gezien als belangrijke ondersteuning voor maatregelen.	De afhankelijkheid van digitale middelen groeit. Een voorbeeld is het gebruik voor transportsystemen. Ook de afhankelijkheid van online kunnen werken groeit, door veel gebruik van op afstand werken. Ketenafhankelijkheden zijn er veel, bijvoorbeeld bij uitbesteding of hosting door andere organisaties binnen of buiten de Rijksoverheid. Verkleinen van het aanvalsoppervlak levert schaalvoordelen op, maar kan ook leiden tot single-points-of-failure.
Technische kwetsbaarheden: legacyapparaten waar geen updates voor verschijnen, lekken in Cisco-routers, het bekend worden van het algoritme voor het berekenen van wifi-sleutels. Bij overbelasting in geval van calamiteiten is er geen eenduidig scenario voor opvang. Secure software development ontbreekt bij leveranciers. De grootte van leveranciers zorgt ervoor dat kleine partijen weinig in te brengen hebben. Ten slotte kampt de sector met een misplaatst gevoel van veiligheid door initiatieven die niet altijd de oplossing bieden die verondersteld wordt.	De telecomsector ziet inzet van methoden om actoren te volgen als goede manier om te kunnen komen tot betere bescherming, net als de inzet van sterke cryptografie voor veilige hard- en software. Publiek-private samenwerking wordt gestimuleerd, mits gekanaliseerd. Op het gebied van malware en DDoS-aanvallen worden diverse beschermingsmaatregelen genomen.	De sector merkt dat er door afnemers meer gestuurd wordt op prijs. Klanten verwachten impliciet perfecte dienstverlening. Groeiend gebruik van mobiele diensten zorgt voor een grotere afhankelijkheid en daarmee groeit de impact van verstoringen op de samenleving. Mobiele aanbieders worden aangesproken op niet goed functioneren van mobiele apparaten die klanten bij een abonnement afnemen. De verantwoordelijkheid van de aanbieders groeit hiermee. Partijen die 'over-the-top-diensten' leveren (zoals bellen en berichten sturen via het datanetwerk) zijn gebonden aan andere of beperktere regelgeving dan telecomaanbieders. Deze partijen hebben veel bewegingsruimte en weinig verplichtingen.

Sector	Manifestaties	Dreigingen: actoren	Dreigingen: middelen
Transport (haven, luchthaven, spoor)	De transportsector had het afgelopen jaar te maken met spionageaanvallen waarbij statelijke actoren gericht zochten naar informatie op netwerken. Er is een aantal manifestaties geweest van malwarebesmetting door een besmette laptop van een leverancier in het netwerk. Algemene dreigingen, zoals ransomware, phishing en DDoS-aanvallen hebben zich ook gemanifesteerd.	Criminelen vormen de belangrijkste dreiging voor de transportsector. Deze groep is gericht op verkrijgen van informatie voor het smokkelen van goederen. Daarnaast vormen statelijke actoren een belangrijke dreiging. Interne actoren vormen ook een belangrijke actor, vooral wanneer zij het doelwit worden van afpersing door criminelen.	De transportsector ziet bij afpersing een verschuiving van het fysieke naar het digitale domein. Chantage, phishing en social engineering gaan steeds meer digitaal. Het doel hierbij is vaak het bemachtigen van toegangspassen of inloggegevens. Waar wifi-netwerken gebruikt worden voor communicatie, bijvoorbeeld in de haven, worden drive-by-aanvallen uitgevoerd.
Verzekeraars	De verzekeringssector heeft ransomware waargenomen waarbij gebruikers die geïnfecteerd werden via phishing-e-mail. Ook hebben zij te maken gehad met (verstorende) DDoS-aanvallen. Daarnaast gebruiken aanvallers digitale middelen ter ondersteuning van verzekeringsfraude.	De belangrijkste actoren voor verzekeraars zijn criminelen, externe actoren in de keten en interne actoren.	Phishing-e-mails zijn aan de orde van de dag, net als e-mail met malwarebijlagen. Het aantal DDoS-aanvallen is afgenomen.
Zorg	De zorgsector heeft manifestaties waargenomen van ransomware en phishing-e-mails gericht op het bemachtigen van inloggegevens. Daarnaast worden veel ongeoorloofde inlogpogingen op diverse systemen geconstateerd.	Cybercriminelen vormen de grootste dreiging voor de zorgsector. Interne medewerkers worden gezien als belangrijke actor door de mogelijkheid van onbewust lekken van informatie. Hacktivisten hebben soms ook aandacht voor het aanvallen van de zorgsector.	Gedetecteerde hulpmiddelen zijn bijvoorbeeld zelf ingebrachte access points in het netwerk en het op afstand beheren van apparatuur door leveranciers, waarmee toegang tot het netwerk wordt verkregen. Phishing-e-mails worden steeds verfijnder, waardoor de kans op besmetting groter wordt.

Weerbaarheid: kwetsbaarheden	Weerbaarheid: maatregelen	Belangen
ICS worden veelvuldig gebruikt in de transportsector. Voor deze systemen komen vaak geen updates uit of deze worden door leveranciers niet doorgevoerd. Bij ICS en andere systemen zorgt de toename van beheer op afstand voor kwetsbaarheden. Een andere specifieke kwetsbaarheid is het beheer van gebruikersaccounts door ketenpartners. Samenwerkende partijen zijn vaak zelf verantwoordelijk voor het beheren van accounts op systemen van ketenpartners. Gebruik van cloudoplossingen door medewerkers vormen een kwetsbaarheid.	Er wordt meer netwerksegmentatie doorgevoerd. Daarnaast wordt vulnerability scanning en netwerkmonitoring steeds meer toegepast. Lifecyclemanagement zorgt ervoor dat zowel kantoor- als procesautomatiseringssystemen vervangen worden, waarmee het landschap langzaamaan ontdaan wordt van niet-ondersteunde systemen.	De kwaliteit van digitale dienstverlening wordt belangrijker doordat de concurrentie van met name havens groeit. De transportsector is belangrijk voor de economie, wat goede bescherming op cybersecuritygebied belangrijk maakt. Tegelijkertijd biedt dit kansen: excelleren op cybersecurity kan concurrentievoordelen opleveren.
Gebruik van cloudoplossingen, soms op eigen initiatief door eigen medewerkers, zorgen voor kwetsbaarheden in de processen van verzekeraars. Bij het gebruik van agile softwareontwikkeling merken de verzekeraars dat security niet altijd de juiste prioriteit krijgt van scrummasters.	Maatregelen tegen DDoS-aanvallen zijn effectief gebleken. Het whitelisten van voor medewerkers toegestane applicaties wordt als succesvol ervaren, net als het blokkeren van usb-poorten en het gebruik van adblockers voor het blokkeren van advertenties en daarmee het tegengaan van malvertising.	Uitbreiding van de Wbp maakt dat de impact (financieel en imago) van het niet tijdig detecteren en melden van datalekken bij de toezichthouder, sterk toeneemt. Door de meldplicht datalekken is de verwachting van klanten over de veiligheid digitale dienstverlening hoger. Daardoor zijn maatregelen voor bescherming van persoonsgegevens belangrijker geworden.
De mens wordt gezien als grootste kwetsbaarheid. Fusies van organisaties versterken het risico, omdat aandacht naar andere zaken gaat en de motivatie om zaken aan te pakken vermindert. Technische kwetsbaarheden zijn bijvoorbeeld het koppelen van medische apparatuur aan netwerken, het door medewerkers gebruiken van software die zij zelf installeren en (medische) apparatuur met verouderde versies van besturingssystemen. Gebruik van privé-apparaten met apps zorgt voor kwetsbaarheden. Er ontstaan datalekken als artsen berichtenapps gebruiken om patiëntgegevens uit te wisselen.	De zorg is bezig met het opzetten van een Zorg-CERT. De implementatie van NEN 7510, 7512 en 7513 zorgt voor meer controle op het gebied van informatiebeveiliging. Aan de technische kant worden meer IDS/IPS- en SIEM-systemen ingezet. Op werkstations wordt soms gebruikgemaakt van geavanceerde beschermingsmaatregelen die kijken naar gedrag in plaats van patronen.	De zorg werkt in ketens en wisselt in deze keten steeds meer digitaal uit. Dit zorgt voor een afhankelijkheid. Door centrale infrastructuren groeien deze ketenafhankelijkheden ook.

Bijlage 3 Afkortingen- en begrippenlijst

0-day	Zie Zero-daykwetsbaarheid.
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.
Bad hosting	Bad hosting is het door een provider (bewust of onbewust) bieden van hosting ter gebruik voor cybercrimedoeleinden.
Bitcoin	Munteenheid, zie cryptocurrency.
Booterservice	Online dienst die tegen betaling DDoS-aanvallen uitvoert voor actoren zonder technische kennis.
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.
BYOD	Bring your own device (BYOD) is een regeling in organisaties waarbij personeel eigen consumentenapparatuur voor het werk kan gebruiken.
C2	Een Command & Control (C2)-server is een centraal systeem in een botnet van waaruit het botnet wordt aangestuurd.
CEO-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.
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 vooral gebruikgemaakt wordt van software-as-a-service (SaaS).
Cryptocurrency	Verzamelnaam voor digitale munteenheden die cryptografische berekeningen gebruiken als echtheidskenmerk en voor transacties. De bitcoin komt daarbij het meest voor.
Cryptoware	Type ransomware dat bestanden op een computer of in een netwerk versleutelt. De sleutel wordt alleen tegen betaling vrijgegeven.
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.
Dark web	Dark web wordt gebruikt als benaming voor websites die uitsluitend via Tor bereikbaar zijn zodat alle handelingen daarop technisch niet tot de eindgebruiker te traceren zijn.
Datalek	Het opzettelijk of onopzettelijk naar buiten komen van vertrouwelijke gegevens.
(D)DoS	(Distributed) Denial of Service is de benaming voor een type aanval die een bepaalde dienst (bijvoorbeeld een website) onbereikbaar maakt voor de gebruikelijke afnemers. Een DoS op een website wordt vaak uitgevoerd door de website te bestoken met veel netwerkverkeer, waardoor deze onbereikbaar wordt.
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 '62.100.52.106'.
DNSSEC	DNS Security Extensions (DNSSEC) is een uitbreiding op DNS met een extra authenticiteits- en integriteitscontrole.
Doxing	Doxing is het verzamelen van persoonlijke gegevens uit verschillende bronnen, doorgaans om die vervolgens online te publiceren.
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.
Dropper	Malware kan worden verpakt in een dropper om detectie te omzeilen. De functie van de dropper is om de malware te installeren op het systeem waar het wordt uitgevoerd.

Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
ENISA	Europees Agentschap voor netwerk- en informatiebeveiliging
EMV	Europay Mastercard Visa (EMV) is een standaard voor betaalkaartsystemen op basis van chipkaarten en chipkaartbetaalterminals. De chipkaart vervangt kaarten met een magneetstrip, die makkelijk te kopiëren zijn.
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.
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
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.
ICS	Industriële controlesystemen (ook Supervisory Control And Data Acqusition, SCADA genoemd) 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.
Internet der dingen	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 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.
MitM	Man-in-the-middle (MitM) is een aanvalstechniek waarbij de aanvaller zich tussen twee partijen bevindt, bijvoorbeeld een internetwinkel en een klant. De aanvaller doet zich richting de klant voor als de winkel en andersom. Als tussenpersoon kan de aanvaller uitgewisselde gegevens afluisteren en/of manipuleren.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
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 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.
SCADA	Zie ICS.
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
Skimmen	Het onrechtmatig kopiëren van de gegevens van een elektronische betaalkaart, bijvoorbeeld een pinpas of creditcard. Skimmen gaat vaak gepaard met het bemachtigen van pincodes, met als uiteindelijk doel betalingen te verrichten of geld op te nemen van de rekening van het slachtoffer.
Social engineering	Een aanvalstechniek waarbij misbruik wordt gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht om vertrouwelijke informatie te verkrijgen of het slachtoffer een bepaalde handeling te laten verrichten.

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.
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. TLS is de opvolger van Secure Sockets Layer (SSL).
Tweefactorauthenticatie	Een manier van authenticeren 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.
VPN	Een Virtual Private Network (VPN) is een geïsoleerde, versleutelde verbinding tussen een apparaat en een bepaalde server op het internet. Dit kan worden toegepast om veilig bedrijfs- of internettoegang te verkrijgen vanaf niet-vertrouwde netwerken.
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.

Uitgave
Nationaal Cyber Security Centrum
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 55 55

Meer informatie
www.ncsc.nl
csbn@ncsc.nl

Tweede druk september 2016