Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Cybersecuritybeeld Nederland

CSBN-3

Cybersecuritybeeld Nederland

CSBN-3

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Per 23 augustus 2013:
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070-888 75 55
F 070-888 75 50
csbn@ncsc.nl
www.ncsc.nl

Juni 2013

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 geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in 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).

Samenwerking en bronnen

Dit rapport is opgesteld door het NCSC. De ministeries, MIVD, AIVD, politie (Nationale Politie, THTC), OM (LP), ACM, NFI, CBS, leden van de ISAC's, Nederland ICT, SIDN, VNO-NCW, NVB, NCTV, wetenschappelijke instellingen, universiteiten en individuele experts uit het cybersecuritywerkveld hebben aan het NCSC informatie beschikbaar gesteld op basis waarvan het Cybersecuritybeeld Nederland mede is samengesteld. Hun bijdragen, de inhoudelijke reviews alsmede openbaar toegankelijke bronnen, een enquête, informatie van de vitale sectoren en analyses van het NCSC hebben in sterke mate bijgedragen aan de inhoudelijke kwaliteit van het beeld.

Voorwoord

Cybersecurity staat meer dan ooit in de belangstelling. Elke dag is het in het nieuws, zowel in klassieke als in nieuwe media. Ook in de politiek en de bestuurskamer is cybersecurity nadrukkelijker op de agenda komen te staan, niet in de laatste plaats door enkele prominente incidenten.

Al die aandacht onderstreept dat cybersecurity hét veiligheidsonderwerp van nu is. Maar de berichtgeving roept ook vragen op: Is het echt zo erg? Wordt het probleem overdreven of is dit nog maar het topje van de ijsberg? Een goede aanpak van cybersecurity, met proportionele acties gericht tegen de juiste dreigingen, vereist inzicht. Inzicht in de belangen die we moeten beschermen, vanuit welke hoek de grootste dreigingen komen en op welke punten onze digitale samenleving kwetsbaar is.

Met dit derde Cybersecuritybeeld Nederland (CSBN-3) geeft het Nationaal Cyber Security Centrum, in nauwe samenwerking met andere partijen, een beeld van de ontwikkelingen op deze aspecten in de afgelopen twaalf maanden. Dit beeld is erop gericht iedereen die een belang heeft bij cybersecurity – publiek, privaat, wetenschappelijk en ideëel – handvatten te bieden om de aanpak van cybersecurity te versterken. Want zoals dit CSBN-3 laat zien, wordt de uitdaging van cybersecurity steeds complexer en alleen met de juiste aanpak kunnen we onze digitale samenleving veilig en open houden.

Een veilige en open digitale samenleving vraagt om het vergroten van de digitale weerbaarheid. De weerbaarheid van Nederland op het gebied van cybersecurity is een publiek goed, maar kan niet door de overheid alleen tot stand worden gebracht. Cybersecurity is namelijk per definitie mondiaal en zonder grenzen. Bovendien is kritieke infrastructuur en kennis vooral in handen van private partijen. Samenwerking tussen bedrijfsleven, wetenschap en overheid is daarom voor alle partijen essentieel om sectoroverstijgend inzicht en handelingsperspectief te ontwikkelen.

Voor dit CSBN hebben we intensief gebruik gemaakt van die samenwerking. Dat heeft de inzichten verbreed en de inschattingen verscherpt. Bij dezen wil ik alle betrokkenen uit bedrijfsleven, wetenschap, overheid en de *security community* die hieraan hebben bijgedragen, bedanken voor hun inzet en waardevolle inzichten.

CSBN-3 bouwt voort op de twee eerdere edities. Zowel in de structuur als in de duiding is een stap vooruit gemaakt. En de diepgang is versterkt in de vorm van verdiepingskaternen, voor de lezer die meer wil weten dan alleen de hoofdlijnen. Daarmee is CSBN-3 de volgende stap in het vergroten van het inzicht in cybersecurity-ontwikkelingen.

Maar voor de lange termijn is nog meer nodig. De inzichten in belangen, dreigingen en weerbaarheid moeten nog verder worden verbeterd. Daar wordt al aan gewerkt door wetenschappers, bedrijven, overheden en enthousiastelingen, vaak gezamenlijk. Maar gezien de snelle ontwikkelingen van cybersecurity kan en moet dat nog krachtiger en sneller. Het Nationaal Cyber Security Centrum nodigt partijen die na lezing van dit CSBN menen daar aan bij te kunnen dragen, graag uit tot participatie.

Het is evident: cybersecurity is van grote waarde voor onze maatschappij en economie. Velen van u hebben een rol in de realisatie daarvan. Onze intentie is dat dit CSBN u helpt te bepalen wat de ontwikkelingen betekenen voor uw organisatie en voor uw rol in het cybersecuritydomein. Want alleen als u weet wat er op u af komt, kunt u zich goed beschermen. En daar gaat het ons allen om.


U kunt nu tanken

Inhoud

Samenvatting

Het Cybersecuritybeeld Nederland (CSBN) wordt elk jaar door het Nationaal Cyber Security Centrum (NCSC) gepubliceerd en komt tot stand in nauwe samenwerking met publieke en private partijen. Het is bedoeld voor beleidsmakers van de overheid en de vitale sectoren om inzicht te bieden in ontwikkelingen, ter beoordeling van mogelijke maatregelen om de digitale weerbaarheid van Nederland te versterken of lopende cybersecurity-programma's te verbeteren. De rapportageperiode bestrijkt de maanden april 2012 tot en met maart 2013. Belangrijke ontwikkelingen tot begin mei 2013 zijn eveneens meegenomen.

ICT raakt steeds meer verweven met maatschappelijke processen en is daarmee een belangrijk onderdeel van ons dagelijks leven. Steeds meer apparatuur is online verbonden met internet: computers en telefoons natuurlijk, maar ook auto's, televisies, thermostaten, weegschalen en ga zo maar door. Die steeds verdergaande digitalisering dient niet alleen gemak en plezier, maar is ook een belangrijke drijfveer voor innovatie, verhoging van productiviteit en economische groei.

Dat er risico's kleven aan de digitalisering, is mede door diverse incidenten in het afgelopen jaar steeds duidelijker. ICT is vaak kwetsbaar. De omgang met en het belang van digitaal opgeslagen of uitgewisselde informatie groeit iedere dag. Dat maakt ICT en vertrouwelijke informatie een interessant doelwit voor kwaadwillenden, variërend van criminelen tot staten. De incidenten in het afgelopen jaar laten zien dat veel organisaties hun digitale weerbaarheid nog niet op een niveau hebben gebracht dat recht doet aan die risico's. Cybersecurity is daarom een onderwerp van toenemend belang.

Kernbevindingen

De belangrijkste bevindingen van CSBN-3 zijn de volgende:

1. Een aantal trends toont aan dat de afhankelijkheid van ICT aanzienlijk is. Deze neemt sterk toe door ontwikkelingen als hyperconnectiviteit, cloudcomputing en het gemak waarmee internet wordt ingezet. De potentiële impact van incidenten wordt daardoor groter.
2. Digitale spionage en cybercriminaliteit blijven de grootste dreigingen voor overheid en bedrijfsleven. Dit betreft:
   a) Digitale spionage vanuit staten, gericht op overheid en bedrijfsleven. Activiteiten zijn vastgesteld vanuit onder meer China, Rusland, Iran en Syrië.
   b) Overname van ICT via malware-infecties door criminelen, gericht op overheid, bedrijfsleven en burgers. Criminelen worden brutaler in hun handelen om snel geld te verdienen, bijvoorbeeld door de burger telefonisch te benaderen of ze in ransomware te confronteren met schokkende beelden.
   c) Manipulatie van informatie (fraude) door criminelen, gericht op het bedrijfsleven. Meest in het oog springend is daarbij fraude met internetbankieren waarvan banken en burgers het slachtoffer zijn.
3. Staten zijn in staat om geavanceerde hulpmiddelen te ontwikkelen en te gebruiken, terwijl cybercriminelen vooral bestaande hulpmiddelen doorontwikkelen. Afgelopen jaar is een criminele cyberdienstensector, waarin hulpmiddelen via 'cybercrime-as-a-service' commercieel beschikbaar worden gesteld, nadrukkelijk zichtbaar geworden. Daarmee is de toegang tot deze hulpmiddelen laagdrempeliger geworden voor verschillende actoren.
4. Burgers, maar ook bedrijven en overheden zijn nog regelmatig het slachtoffer van botnets en ransomware. Malware muteert zo snel waardoor antivirusprogramma's deze niet allemaal kunnen detecteren. Hoewel botnets veelal gericht zijn op manipulatie van (financiële) transacties, tonen incidenten (zoals Pobelka) aan dat de impact van met botnets ontvreemde informatie (als bijvangst) groot kan zijn.
5. De kwetsbaarheid van ICT blijft onverminderd hoog. Na een aantal jaar daling neemt het aantal gepubliceerde kwetsbaarheden in software weer toe. Ook brengen clouddiensten, mobiele diensten en innovatieve apparatuur nieuwe kwetsbaarheden met zich mee.
6. De eindgebruiker krijgt een grote verantwoordelijkheid toegedicht voor beveiliging, maar hij wordt steeds vaker geconfronteerd met kwetsbaarheden in apparaten en diensten waar hij beperkte invloed op heeft of geen kennis van heeft.
7. Publieke en private partijen nemen, afzonderlijk en gezamenlijk, verschillende initiatieven om de digitale weerbaarheid te vergroten. Daarmee spelen zij in op de toenemende afhankelijkheid van ICT en veranderende dreigingen. De effectiviteit hiervan op de lange termijn is nu nog niet in te schatten.

8. De verstoring van ICT is nadrukkelijk zichtbaar geweest, vooral verstoring als gevolg van DDoS-aanvallen. De weerbaarheid hiertegen was soms onvoldoende, waardoor de onlinedienstverlening van organisaties minder beschikbaar was. Daarnaast zijn basisvoorzieningen zoals DigiD en iDeal verstoord als gevolg van DDoS-aanvallen, wat heeft geresulteerd in keteneffecten bij overheden en bedrijven die gebruikmaken van deze diensten. Het is niet duidelijk welke actoren de DDoS-aanvallen hebben gepleegd.
9. Een brede groep organisaties heeft belangrijke (technische) basismaatregelen, zoals het patchen en updaten van systemen of het wachtwoordenbeleid, nog niet op orde. Waar individuele organisaties hun basisbeveiliging wel op orde hebben, blijken gedeelde services en infrastructuur nog kwetsbaar, waardoor een risico bestaat voor organisatieoverstijgende belangen.
10. De inherente dynamiek van cybersecurity vereist een vernieuwende aanpak. Statische informatiebeveiligingsmaatregelen zijn niet meer voldoende, organisaties hebben meer inzicht nodig in dreigingen (detectie) en hebben capaciteit nodig om te handelen bij dreigingen (response).

Concluderend kunnen we stellen dat a) de afhankelijkheid van ICT voor individuen, organisaties, ketens en de maatschappij is gegroeid, b) een aantal dreigingen is toegenomen en uitgaat van vooral staten en beroepscriminelen tegen overwegend overheden en private organisaties en c) de weerbaarheid ongeveer gelijk is gebleven omdat er meer initiatieven en maatregelen worden genomen die niet altijd gelijke tred houden met de kwetsbaarheden, en basismaatregelen niet altijd zijn getroffen.

Tabel 1 geeft inzicht in de dreigingen die de verschillende actoren gebruiken om de doelwitten 'overheden', 'private organisaties' en 'burgers' aan te vallen. Zie hoofdstuk 6 van het kernbeeld voor informatie over de wijzigingen ten opzichte van het voorgaande cybersecuritybeeld.

Belangen

Belangen in het kader van cybersecurity kennen verschillende niveaus: persoonlijke belangen, organisatiebelangen, ketenbelangen en maatschappelijke belangen. Cybersecurity vereist bescherming van al die belangen.

Evenals als in voorgaande jaren neemt de afhankelijkheid van ICT steeds meer toe met als gevolg dat het niet-functioneren ervan of de inbreuk op de vertrouwelijkheid en integriteit van informatie steeds meer belangen raakt en met grotere gevolgen. Deze toenemende afhankelijkheid is ook van toepassing op de vitale sectoren. Daarbij worden de sectoren elektriciteit, Telecom en IT-services als randvoorwaardelijk gezien vanuit perspectief van cybersecurity. De toegenomen afhankelijkheid is zeker van toepassing op gedeelde onlinediensten zoals DigiD en iDeal.

Actuele ontwikkelingen, zoals cloudcomputing, sociale media en hyperconnectiviteit, leiden tot een stijgend gebruik van het internet als platform voor zakelijke transacties, de verwerking van vertrouwelijke informatie en het gebruik van ICT voor de aansturing van maatschappelijk belangrijke processen. Het gemak waarmee het internet toegepast kan worden, versterkt deze ontwikkeling en brengt tegelijkertijd risico's met zich mee waar niet altijd voldoende over wordt nagedacht. Omdat Nederland sterk heeft ingezet op de elektronische dienstverlening, kunnen cybersecurityincidenten een grote impact hebben.

Dreigingen: actoren en hun intenties

De grootste dreiging gaat op dit moment uit van staten en beroepscriminelen en in mindere mate van cybervandalen, scriptkiddies en hacktivisten. Het is niet altijd mogelijk om te achterhalen welk type actor achter een cyberaanval zit: het attributievraagstuk.

Staten vormen vooral een dreiging in de vorm van diefstal van informatie (digitale spionage), gericht op vertrouwelijke of concurrentiegevoelige informatie van overheden en bedrijven. De AIVD heeft het afgelopen jaar spionageaanvallen vastgesteld op Nederlandse civiele organisaties dan wel via de Nederlandse ICT-infrastructuur, vanuit onder meer China, Rusland, Iran en Syrië. De MIVD constateert dat de defensie-industrie een gewild doelwit is van cyberspionage en beschikt over aanwijzingen dat de cyberspionagedreiging zich eveneens richt op partijen met wie de defensie-industrie samenwerkt. Informatie verkregen door spionage op deze industrie dient het belang van staten. Daarnaast constateert de MIVD kwaadaardige phishingactiviteiten richting Nederlandse militaire vertegenwoordigingen in het buitenland.

Van beroepscriminelen blijft een grote dreiging uitgaan. De afgelopen periode uitte dat zich in financiële fraude en diefstal door aanpassing van onlinetransacties, veelal na diefstal en misbruik van financiële (inlog)gegevens (fraude met internetbankieren). Voorts maakten criminelen zich schuldig aan digitale inbraak om informatie te stelen voor criminele doeleinden of om te verkopen in het criminele circuit. Tot slot blijft de overname van ICT, bijvoorbeeld door malwarebesmettingen, een onderwerp van zorg (zie het Pobelka-botnet), net als de toename van het plaatsen van ransomware om eindgebruikers te kunnen chanteren. Incidenten, waaronder het Pobelka-botnet, tonen dat botnets die zich richten op financiële transacties ook veel andere gevoelige gegevens buitmaken die een significant risico kunnen vormen. Bij Pobelka bleken gevoelige gegevens van bedrijven en overheden uit vitale sectoren, evenals veel persoonlijke gegevens van burgers, buitgemaakt te zijn.

Criminelen worden brutaler in hun handelen om daarmee veel geld te verdienen. Een voorbeeld hiervan is het automatisch downloaden en tonen van kinderporno in ransomware om slachtoffers te dwingen geld te betalen. De politie constateert dat de wereld van cybercrime meer verweven raakt met de normale harde criminaliteit. Recente onderzoeken tonen aan dat burgers bijna even vaak slachtoffer zijn van 'hacken' als van fietsendiefstal.

Cybervandalen, scriptkiddies en hacktivisten vielen de afgelopen periode op door verstoring van de onlinedienstverlening van

Doelwitten			
Actoren (dreigers)	**Overheden**	**Private organisaties**	**Burgers**
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Verstoring ICT (inzet offensieve capaciteiten) ★	Verstoring ICT (inzet offensieve capaciteiten) ★	
Terroristen	Verstoring ICT	Verstoring ICT	
(Beroeps)criminelen	Diefstal en verkoop van informatie ★	Diefstal en verkoop van informatie ★	Diefstal en verkoop van informatie ★
	Manipulatie van informatie★	Manipulatie van informatie★	Manipulatie van informatie★
	Verstoring ICT	Verstoring ICT ⇧	
	Overname ICT	Overname ICT	Overname ICT
Cybervandalen en Scriptkiddies	Diefstal en publicatie van informatie ★	Diefstal en publicatie van informatie ★	Diefstal en publicatie van informatie ★
	Verstoring ICT	Verstoring ICT	
		Overname ICT ★	
Hacktivisten	Diefstal en publicatie van informatie ⇩	Diefstal en publicatie van informatie ⇩	Diefstal en publicatie van informatie ⇩
	Verstoring ICT	Verstoring ICT	Verstoring ICT ⇩
		Overname ICT ★	
	Digitale bekladding ★	Digitale bekladding ★	
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie	Diefstal en publicatie of verkoop verkregen informatie (chantage)	
	Verstoring ICT ★	Verstoring ICT ★	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private organisaties		Diefstal van informatie (bedrijfsspionage) ⇧	
Geen actor	Uitval ICT ⇩	Uitval ICT ⇩	Uitval ICT ⇩

Tabel 1. Overzicht dreigingen en doelwitten

Legenda relevantie		
Laag	**Midden**	**Hoog**
Er worden geen nieuwe trends of fenomenen onderkend waar de dreiging van uitgaat. **OF** Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. **OF** Er hebben zich geen noemenswaardige incidenten van de dreiging voorgedaan in de rapportageperiode	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 duideljke ontwikkelingen die de dreiging opportuun maken. **OF** Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft. **OF** Incidenten hebben zich voorgedaan in Nederland.

Legenda wijzigingen: ⇧ dreiging is toegenomen ⇩ dreiging is afgenomen ★ dreiging/regel is nieuw

overheden en bedrijven en het publiceren van vertrouwelijke gegevens. Scriptkiddies en cybervandalen hebben daar in principe geen wezenlijk eigen belang bij, anders dan de kick. Over het algemeen worden de technische hulpmiddelen voor scriptkiddies beter en makkelijker te gebruiken. Daardoor kunnen zij grotere schade aanrichten. De cybervandaal heeft aan de andere kant veel kennis en kan daarbij substantiële schade aanrichten. Niet altijd is te herleiden hoe groot het aandeel van hacktivisten in opzettelijke verstoringen van ICT is. Aangenomen wordt dat zij betrokken zijn bij de vele DDoS-aanvallen en bij de (pogingen tot) publicatie van met digitale inbraak gestolen informatie.

Cyberaanvallen door terroristen tegen het internet of via het internet met ontwrichtende schade hebben zich voor zover bekend nog niet voorgedaan. Terroristen beschikken (nog) niet over voldoende vaardigheden en middelen voor maatschappijontwrichtende cyberaanvallen.

Dreigingen: hulpmiddelen

Voor het uitvoeren van aanvallen maken actoren gebruik van (technische) hulpmiddelen om kwetsbaarheden te misbruiken en/of te vergroten. Actoren gebruiken vooral de talrijke zelfontwikkelde of beschikbare exploits, botnets, (spear)phishing en (mobiele) malware. Staten zijn in staat om geavanceerde hulpmiddelen te ontwikkelen en te gebruiken, terwijl cybercriminelen vooral bestaande hulpmiddelen doorontwikkelen. Cybercrime professionaliseert verder in het bieden van diensten voor het huren van hulpmiddelen voor cyberaanvallen en het wegsluizen van geld. Deze criminele cyberdienstensector wordt ook wel 'cybercrime-as-a-service' genoemd. De verhuur van botnets voor DDoS-aanvallen is hier een voorbeeld van.

Van de technische hulpmiddelen worden exploitkits, malware en botnets het meest toegepast. De steeds makkelijker te gebruiken exploitkits maken het eenvoudiger om het stijgend aantal technische kwetsbaarheden te misbruiken. Ook tools voor DDoS-aanvallen zijn laagdrempelig beschikbaar. Mutaties van malware zorgen ervoor dat er zoveel varianten van malware in omloop komen, dat antivirusprogramma's deze niet allemaal kunnen detecteren. Botnets blijven een belangrijk hulpmiddel voor staten en cybercriminelen dat voor de eigenaren van misbruikte ICT-middelen veelal onder de radar bleef. Met de stijging van het gebruik van mobiele apparatuur, neemt ook de stijging van mobiele malware toe.

Aan de menskant zien we dat criminelen steeds brutaler worden. Phishing blijft een succesvolle methode om gebruikers te verleiden. Gebruikers zijn steeds vaker het slachtoffer van ransomware, een specifieke vorm van malware waarmee de computer van de gebruiker wordt gegijzeld. Ook zijn afgelopen jaar telefonische phishingacties nadrukkelijk in beeld geweest.

Weerbaarheid: kwetsbaarheden

De weerbaarheid bestaat enerzijds uit (het afwezig zijn van) de kwetsbaarheid van de te verdedigen belangen en anderzijds uit maatregelen om de kwetsbaarheid te verminderen. Kwetsbaarheden zorgen ervoor dat onze maatschappij kwetsbaar blijft voor cyberaanvallen.

De kwetsbaarheid van ICT blijft onverminderd hoog. Na een aantal jaar daling neemt het aantal gepubliceerde kwetsbaarheden in standaardsoftware weer toe (+27 procent) en stijgt het aantal gepubliceerde kwetsbaarheden in industriële automatisering. Gegevens zijn mobiel geworden, verlies of diefstal van een mobiel apparaat maakt de opgeslagen gegevens mogelijk toegankelijk voor de vinder. Bij hyperconnectiviteit worden alle apparaten met elkaar verbonden, niet alleen smartphones, tablets of computers maar alle denkbare apparaten, van koelkasten tot auto's waardoor bestaande kwetsbaarheden op meer manieren kunnen worden misbruikt.

De eindgebruiker krijgt een grote verantwoordelijkheid toegedicht voor beveiliging, maar hij wordt steeds vaker geconfronteerd met kwetsbaarheden in apparaten waarop hij beperkte invloed heeft. Daar komt bij dat beveiliging van computers en apparaten kennis vereist die veel eindgebruikers niet hebben. Consumerization brengt daarnaast met zich mee dat privé- en zakelijk gebruik door elkaar gaan lopen terwijl zij elkaar niet altijd verdragen. Zakelijke informatie komt buiten beheer van de organisatie en kan in een privéomgeving uitlekken en privé-informatie kan toegankelijk worden voor organisaties.

Cloudcomputing heeft vele voordelen maar brengt ook risico's met zich mee, onder meer omdat de toegang niet altijd even goed is beveiligd en de cloud de autonomie van organisaties over de omgang met bevragingen door buitenlandse overheden vermindert. Cloudcomputing brengt daarnaast uitdagingen voor de opsporing en vervolging van misdaad met zich mee.

Veel organisaties hebben de basismaatregelen, zoals het patchen en updaten van systemen of het wachtwoordenbeleid nog niet op orde. Daarom zijn oude kwetsbaarheden en aanvalsmethoden nog steeds effectief. Een belangrijke kwetsbaarheid is ten slotte dat veel organisaties de juiste kennis, de detectiemiddelen en het vermogen ontberen om incidenten afdoende af te handelen.

Weerbaarheid: maatregelen

Veel weerbaarheidsinitiatieven die in de vorige editie van het CSBN werden genoemd, zijn ook daadwerkelijk gestart of al in volle uitvoering. In het afgelopen jaar is – mede door grote incidenten – de publieke en politieke aandacht voor cybersecurity flink toegenomen. De noodzaak is ook doorgedrongen in de directiekamer, zodat vaker de portefeuille cybersecurity of informatiebeveiliging expliciet op hoog niveau wordt belegd. Overheid en bedrijfsleven besteden meer dan voorheen aandacht aan maatregelen en dit gebeurt steeds vaker in gezamenlijkheid.

In het oog springend zijn de bewustwordingscampagnes, zoals 'Alert Online', 'Bankgegevens en inlogcodes. Hou ze geheim' en 'Bescherm je bedrijf '. Daarnaast zijn de intensivering van de samenwerking op het gebied van informatie-uitwisseling en de

afspraken tussen banken en overheid naar aanleiding van de DDoS-aanvallen sprekende voorbeelden. Op het gebied van onderzoek en innovatie zijn verschillende onderzoeksprogramma's opgezet om vraagstukken op het gebied van cybersecurity in samenwerking met overheid, bedrijfsleven en wetenschap aan te pakken. Ook is een leidraad gepubliceerd voor het opstellen van beleid voor Responsible Disclosure, het op verantwoorde wijze bekendmaken van kwetsbaarheden in ICT. Dit is een handreiking voor organisaties en melders voor het op een verantwoordelijke wijze melden en afhandelen van kwetsbaarheden in informatiesystemen en (software)producten.

Het toegenomen bewustzijn leidde de afgelopen periode ook tot nieuwe initiatieven en aanvullende maatregelen op nationaal niveau en bij afzonderlijke organisaties. Daarmee spelen zij in op de toenemende afhankelijkheid van ICT en veranderende dreigingen. De effectiviteit hiervan op de lange termijn is nu nog niet in te schatten.

Manifestaties

Voor overheden is de grootste dreiging momenteel gericht op het belang van de vertrouwelijkheid van informatie (met name tegen spionage) en continuïteit van onlinedienstverlening (incl. generieke voorzieningen) en eigen ICT. Deze dreiging komt uit verschillende hoeken: beroepscriminelen, hacktivisten en cybervandalen/scriptkiddies.

Voor het bedrijfsleven gaat de belangrijkste dreiging uit van spionage gericht op concurrentiegevoelige informatie en van misbruik van financiële gegevens voor diefstal van geldelijke waarden. Dit gebeurt ook door manipulatie van informatie in de vorm van aanpassing van (bank)transacties. Daarnaast is voor bedrijven die vitale onlinediensten aanbieden ook verstoring van onlinedienstverlening een belangrijke dreiging die in het afgelopen jaar is toegenomen. Ook wordt bedrijfsinformatie van allerlei aard door meerdere groepen actoren gestolen voor eigen gebruik, publicatie of verkoop aan derden. Denk aan klantgegevens of informatie over de ICT-voorzieningen van bedrijven.

Burgers worden geraakt door identiteitsfraude en chantage. Burgers raken betrokken wanneer het hun gegevens betreft die worden gestolen, gepubliceerd, verkocht of misbruikt. Ook wanneer de ontvreemding van informatie rechtstreeks bij hen gebeurt, staan belangen als geld (schade door aanvallen op elektronisch bankieren), privacy, beschikbaarheid van onlinediensten en digitale identiteit op het spel. Burgers hebben vooral te kampen met het vrijwaren van hun eigen computers en elektronica van malware en ransomware. Burgers worden indirect geraakt wanneer zij betrokken raken bij een cyberaanval doordat hun eigen ICT onderdeel geworden is van een botnet.

Het aantal door NCSC afgehandelde incidenten is in de rapportageperiode sterk toegenomen. De voornaamste reden voor deze stijging is dat per 1 januari 2012 private partijen ook door het NCSC worden bediend. In de aard van de incidenten bij de overheid is een relatieve stijging te zien van malware-infecties (+13 procent) en poging tot hacken (+5 procent).

Het bekend worden van het Pobelka-botnet heeft inzicht gegeven in de aanzienlijke aantallen besmette computers en de omvang van de gelekte gegevens van een tot dan toe onopgemerkt gebleven botnet. Waarschijnlijk zijn er veel meer niet-ontdekte botnets. Dit laat tevens zien dat de middelen die beschikbaar zijn voor detectie van dit soort aanvallen, tekortschieten.

De afgelopen periode zijn basisvoorzieningen het doelwit geweest van aanvallen. Het gaat bijvoorbeeld om aanvallen op iDeal, waardoor betalen bij webwinkels tijdelijk niet mogelijk was, en DigiD waardoor overheidsdiensten, waarvoor inloggen noodzakelijk is, tijdelijk niet toegankelijk waren. «

Inleiding

ICT is doorgedrongen tot in de haarvaten van onze maatschappij en haar functioneren is ervan afhankelijk geworden. Steeds meer gebruiksvoorwerpen bevatten elektronica en software en steeds vaker zijn ze verbonden met het internet en daarmee onderdeel van het cyberdomein. Die digitalisering en verbinding is zo doorgevoerd, dat we het ons vaak niet eens meer realiseren. Kantoren, huishoudens, fabrieken en winkels zijn allemaal onderdeel van deze ontwikkeling. ICT is daarmee een belangrijke drijfveer voor innovatie, verhoging van productiviteit en economische groei.

ICT is soms ook feilbaar en kwetsbaar en de opgeslagen of uitgewisselde informatie is steeds waardevoller. Er zijn tal van partijen die misbruik willen maken van kwetsbaarheden en toegang willen krijgen tot informatie om die al dan niet te manipuleren of te publiceren. Cybersecurity is daarom een onderwerp van toenemend belang.

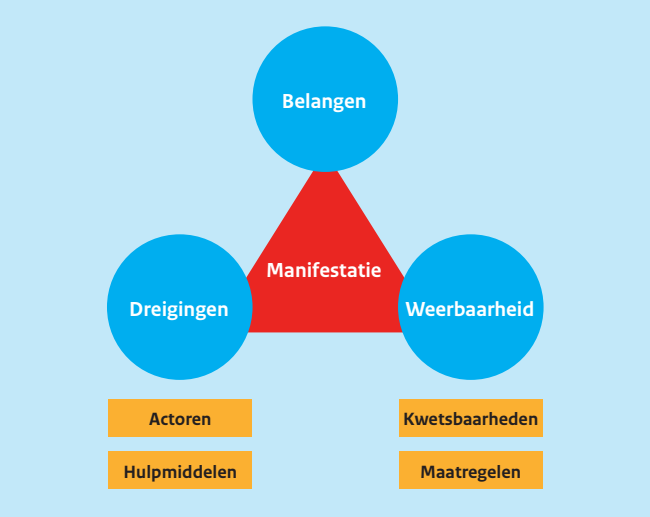
Vanwege het grote belang van cybersecurity is in 2011 een Nationale Cyber Security Strategie[1] geformuleerd. Een van de actielijnen die de strategie beschrijft, is de realisatie van adequate en actuele dreigings- en risicoanalyses. Preventie en bestrijding van cyberaanvallen vereisen namelijk een overzicht van en inzicht in ontwikkelingen en incidenten die zich voordoen. Dat is nodig om de juiste koers te bepalen voor (nieuwe) maatregelen. Dit derde Cybersecuritybeeld Nederland (CSBN) is de volgende stap in de uitvoering van die actielijn. Afgeleid van de doelstelling gelden de onderstaande hoofdvragen voor het Cybersecuritybeeld:

- 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*)
- Welke gebeurtenissen of welke activiteiten van welke actoren kunnen ICT-belangen aantasten, welke hulpmiddelen 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*)

Het CSBN levert inzichten ter beantwoording van deze vraagstukken. Dit derde Cybersecuritybeeld bouwt voort op de eerdere beelden en kan daar ook niet los van worden gezien. De rapportageperiode beslaat april 2012 tot en met maart 2013, waarbij relevante ontwikkelingen die speelden tot begin mei 2013 eveneens zijn meegenomen. De focus van het CSBN ligt op de ontwikkelingen in Nederland, waarbij belangwekkende ontwikkelingen vanuit elders in de wereld zijn meegenomen. Het CSBN is een feitelijke beschrijving, met duiding op basis van inzicht en expertise vanuit overheidsdiensten en de vitale sectoren zelf. Het beschrijft ontwikkelingen in kwalitatieve vorm en geeft, daar waar in betrouwbare vorm voorhanden, een kwantitatieve onderbouwing. Zaken die ten opzichte van de vorige edities niet of nauwelijks zijn veranderd, zijn niet of beknopt beschreven.

Leeswijzer

Deze editie (CSBN-3) bestaat voor het eerst uit een kernbeeld en verdiepende katernen. Het kernbeeld heeft tot doel om een zo scherp en zo volledig mogelijk inzicht te geven in (veranderingen in) Nederlandse 'Belangen' die kunnen worden geschaad, de 'Dreigingen' die daarop van invloed zijn en de mate waarin de samenleving 'Weerbaar' is op het gebied van cybersecurity. Het kernbeeld is opgebouwd (zie onderstaande figuur) op basis van de driehoek Belangen, Dreigingen en Weerbaarheid, hetgeen aansluit op de indeling die in andere dreigingsbeelden, zoals voor terrorisme[2], wordt gehanteerd.



Bij *Belangen* (hoofdstuk 1) wordt ingegaan op de Nederlandse belangen die kunnen worden geschaad door aantasting van de

1 Nationale Cyber Security Strategie, een nieuwe versie van deze strategie is bij schrijven in ontwikkeling.

2 Bron: NCTV.

beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie en ontwikkelingen die zich daarbij voordoen.

De *Dreigingen* bestaan enerzijds uit onopzettelijke gebeurtenissen of onachtzaamheid en anderzijds uit opzettelijke activiteiten van *actoren* (hoofdstuk 2) en hun intenties. Een aanval kan zich manifesteren, maar gedetecteerd en afgeslagen worden. De dreiging manifesteert zich dan wel, maar de weerbaarheid is toereikend. De mate waarin die actoren over de intentie en vaardigheden beschikken om zich van technische en andere *hulpmiddelen* (hoofdstuk 3) te voorzien, bepaalt verder in hoge mate hun potentiële impact en de kans van slagen.

De *Weerbaarheid* van eindgebruikers, organisaties en de samenleving kan de kans dat een dreiging zich manifesteert en de impact ervan beperken. De weerbaarheid bestaat uit de af- of aanwezigheid van *kwetsbaarheden* bij mensen, organisatie of technologie (hoofdstuk 4) en *maatregelen* om weerstand en veerkracht te sterken en kwetsbaarheden te beperken (hoofdstuk 5).

In hoofstuk 6 is beschreven welke zaken zich hebben *gemanifesteerd* in de driehoek Belangen, Dreigingen en Weerbaarheid. Tevens zijn in dit hoofdstuk verwachtingen over de ontwikkeling van dreigingen beschreven.

Voor onderwerpen uit het Cybersecuritybeeld die anno 2013 van bijzonder belang zijn, is een nadere uitwerking opgenomen in verdiepingskaternen. Het betreft de thema's: Cybercrime, Cyberspionage, Botnets, DDoS, Hyperconnectiviteit, Grip op informatie, Kwetsbaarheid van ICT, Kwetsbaarheid van de eindgebruiker en Industriële controlesystemen (ICS). De keuze voor deze onderwerpen is tot stand gekomen op basis van afstemming met een groot deel van de partijen die hebben meegewerkt aan dit CSBN.

Bij het opstellen van het kernbeeld is gebruikgemaakt van informatie uit de verdiepingskaternen, omwille van de leesbaarheid is daar niet altijd expliciet naar verwezen. Voorts zijn in de bijlagen een overzicht van de door NCSC afgehandelde incidenten, een afkortingen- en begrippenlijst, en een referentielijst opgenomen. In de tekst wordt met cijfers in superscript verwezen naar voetnoten op dezelfde pagina. Verwijzigingen naar documenten in de referentielijst zijn tussen blokhaken opgenomen. «

Kernbeeld

1 Belangen

De Nationale Cyber Security Strategie 2011 omschrijft cybersecurity als volgt:

Cybersecurity is het vrij zijn van gevaar of schade, veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar van of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van vertrouwelijkheid van de in ICT opgeslagen informatie of schade aan de integriteit van die informatie.

Het gaat dus om de bescherming van het functioneren van ICT en van informatie. Wanneer ICT niet (naar behoren) functioneert of de vertrouwelijkheid en integriteit van informatie in het geding zijn, kunnen belangen in onze samenleving worden geschaad. Dit hoofdstuk gaat in op de relatie tussen ICT-veiligheid en die belangen.

1.1 Belang van ICT-veiligheid voor de samenleving

De toenemende digitalisering van onze samenleving is voor bijna iedereen merkbaar. Daardoor kan aantasting van de ICT-veiligheid een steeds grotere impact hebben op de belangen van die samenleving. We onderscheiden in het kader van cybersecurity de vier soorten te beschermen belangen uit het onderstaande overzicht:

Individuele belangen
- Privacy
- Vrijheid van meningsuiting
- Toegang tot dienstverlening
- Fysieke veiligheid

Organisatorische belangen
- Producten en diensten
- Productiemiddelen (w.o. geld, octrooien)
- Reputatie
- Vertrouwen

Ketenbelangen
- Verantwoordelijkheid voor informatie van burgers of klanten
- Beheer van algemene voorzieningen en stelsels, zoals GBA, iDeal en DigiD
- Onderlinge afhankelijkheid tussen organisaties

Maatschappelijke belangen
- Beschikbaarheid van vitale diensten
- Bescherming van de (democratische) rechtsorde en nationale veiligheid
- Infrastructuur van het internet
- Vrij verkeer van diensten
- Digitale veiligheid

Vanuit cybersecurity moet rekening worden gehouden met elk van deze belangen. Deze belangen zullen voor eenieder een ander gewicht hebben en kunnen tegenstrijdig zijn.

Individuele belangen

Dit zijn belangen die (individuele) personen van belang achten en beschermen. Denk hierbij aan grondrechten als privacy of het belang van vrijheid van meningsuiting en ook de veiligheid van iemands digitale identiteit en het belang van toegang tot online-dienstverlening. In Europees perspectief maken relatief veel Nederlanders gebruik van het internet voor bijvoorbeeld winkelen (76 procent) en bankieren (82 tot 84 procent).[3: CBS 2012] Afgezet tegen andere EU-lidstaten geven Nederlanders opvallend vaak (28 tegenover 13 procent gemiddeld) aan dat ze geen gebruik konden maken van onlinedienstverlening vanwege cyberaanvallen.[12: EC 2013-2][3] Zorgen over privacy zijn voor 35 procent van de Nederlanders die afzien van gebruik van een internetdienst, de grootste reden om dat te doen.[49: TNO 2012]

Organisatorische belangen

Dit zijn belangen waar een organisatie voor het bereiken van haar doelstellingen en/of zelfs haar voortbestaan van afhankelijk is. Een geslaagde hack kan een organisatie voor aanzienlijke kosten plaatsen voor herstel of voor het afslaan van een aanval, maar ook leiden tot reputatieverlies. Niet alleen uitval, ook inbreuk op de integriteit (juistheid, actualiteit en/of volledigheid) van data kan zeer negatieve effecten hebben. Zo is voor een webwinkel de beschikbaarheid en het functioneren van de website van cruciaal belang en kan disfunctioneren leiden tot een forse omzetdaling. Wanneer het procescontrolesysteem van een chemische fabriek uitvalt of de besturing zou worden overgenomen, kan de veiligheid ernstig in het geding zijn.

Ketenbelangen

Dit zijn organisatieoverstijgende belangen. Denk bijvoorbeeld aan de verantwoordelijkheid voor informatie van burgers of klanten en leveranciers of beschikbaarheid van digitale diensten, maar ook het belang van basisvoorzieningen, zoals die voor onlinebetalen. Het belang van een keten komt in het geding wanneer cyberaanvallen belangen raken van derden. Bijvoorbeeld door het lekken van persoonsgegevens of wanneer onlinediensten, waar andere organisaties van afhankelijk zijn, niet meer beschikbaar zijn. De gedeeltelijke uitval van iDeal na cyberaanvallen in april 2013 is hier een voorbeeld van.[4]

Maatschappelijke belangen

Dit zijn belangen die het belang van de eigen organisatie overstijgen en voor de Nederlandse samenleving als geheel van belang zijn. Denk daarbij aan de beschikbaarheid van vitale diensten zoals elektriciteit. Cyberaanvallen tegen een bedrijf of sector kunnen

3 De meetperiode was maart 2012, ruim vóór de cyberaanvallen in april-mei 2013.
4 http://tweakers.net/nieuws/88305/storingen-ideal-en-ing-kwamen-door-ddos-aanval.html

uiteindelijk ook de maatschappij als geheel raken. Zo kan langdurige uitval van bijvoorbeeld het betalingsverkeer of de elektriciteitsvoorziening als gevolg van een cyberaanval het economisch belang van Nederland treffen en leiden tot maatschappelijke ontwrichting.

1.2 Afhankelijkheid

De afhankelijkheid van ICT neemt steeds verder toe, waardoor de potentiële impact van cyberaanvallen toeneemt. Zowel incidenten als oefeningen laten zien dat belangen vaak onderling samenhangen. Bij aantasting van een van die belangen kunnen al snel zogenaamde keten- of cascade-effecten optreden. De vitale sectoren van de Nederlandse samenleving zijn ingedeeld in 12 vitale sectoren met 31 vitale producten of diensten.[5] Wat opvalt, is dat in deze indeling de, voor cybersecurity zeer relevante, sector IT-services niet is benoemd. Zo zijn ICT, telecommunicatie en elektriciteit randvoorwaardelijk voor het functioneren van veel (andere) vitale sectoren en processen in de samenleving. Uitval in een van deze sectoren kan leiden tot schadelijke effecten in alle sectoren. ICT-incidenten zoals DigiNotar in 2011 en recentere incidenten laten zien dat voor cybersecurity ook het goed functioneren van de sector IT-services (met bijvoorbeeld (web)hosting en leveranciers van digitale certificaten) randvoorwaardelijk is.

De veiligheid van concurrentiegevoelige informatie en hoogwaardige technologische kennis van bedrijven en andere organisaties is essentieel voor de economische groei van Nederland. Dit zijn belangen waarvan aantasting van de vertrouwelijkheid geen acute maatschappelijke ontwrichting veroorzaakt, maar waarbij de impact pas op langere termijn zichtbaar is. Dit leidt tot onderschatting van het risico. Een voorbeeld is ontvreemding van intellectueel eigendom via digitale spionage in de petrochemische, automobiel-, farmaceutische, maritieme, lucht- en ruimtevaart- en defensie-industrie.[8]

Vitale sectoren zijn een gewild doelwit voor digitale spionage door statelijke actoren. Het competitief voordeel van de betreffende Nederlandse bedrijven wordt door deze digitale spionage aangetast. Juist de topsectoren waar Nederland op inzet zijn hiervoor gevoelig. Het ontvreemden van de informatie door buitenlandse regeringen en bedrijven verstoort het economische 'level playing field' en brengt de Nederlandse economie schade toe waarvan de hoogte lastig is vast te stellen.

De communicatie van de Nederlandse overheid verloopt grotendeels elektronisch. Voor het correct en doeltreffend kunnen functioneren van ministeries, lokale overheden, buitenlandse posten en andere aan de overheid gelieerde organisaties is de vertrouwelijkheid van informatie vaak een randvoorwaarde. Hierbij kan onder meer worden gedacht aan de communicatie over standpunten van de Nederlandse regering voor internationaal overleg en commercieel-vertrouwelijke informatie over aanbestedingen.

Adequate cybersecurity (en het doen van de bijbehorende investeringen) kan een concurrentievoordeel opleveren voor bedrijven. Een aantoonbaar goede beveiliging van online- en offlinediensten draagt immers bij aan een goede reputatie en beperkt het feitelijk voordoen van incidenten en de bijkomende schade. Een pleidooi hiervoor staat bijvoorbeeld in de nieuwe EU-strategie voor cybersecurity: *"The take up of a cybersecurity culture could enhance business opportunities and competitiveness in the private sector, which could make cybersecurity a selling point."* [11: EC 2013-1]

1.3 Ontwikkelingen hebben invloed op belangen

Er komen voortdurend nieuwe technieken en toepassingen bij, die invloed hebben op de afhankelijkheid van onze maatschappij van ICT en de te verdedigen belangen. Hierna zijn de belangrijkste ontwikkelingen geschetst die momenteel voor de digitale veiligheid relevant zijn.

Afhankelijkheid van ICT neemt nog altijd toe

De conclusie uit de vorige edities van het CSBN, dat onze afhankelijkheid van ICT toeneemt, geldt nog altijd. Zowel burgers, overheden als bedrijven gebruiken ICT voor steeds meer functies, bijvoorbeeld voor online-interactie met klanten/burgers, efficiënter werken, beter samenwerken, fysieke veiligheid, communicatie of vermaak. Een direct gevolg is ook dat steeds meer en meer informatie wordt vastgelegd, verwerkt, geanalyseerd en uitgewisseld. Het gemak waarmee het internet toegepast kan worden, versterkt deze groei en brengt tegelijkertijd risico's met zich mee waar niet altijd voldoende over wordt nagedacht. Daarbij komt dat analoge alternatieven steeds minder achter de hand worden gehouden om op terug te vallen.

Ook zorg afhankelijker van ICT

De zorgsector beweegt bijvoorbeeld naar bedrijfsprocessen waarin digitale gegevensontsluiting van zeer groot belang is, zowel voor informatieverwerking binnen de zorginstelling (bijvoorbeeld ZIS en EPD) als voor externe gegevensuitwisseling om de kwaliteit van zorg te verbeteren.[18: IGZ 2011] Onderzoeksdata voor zowel zorg als wetenschappelijk onderzoek is in de meeste gevallen digitaal opgeslagen. Ook vanuit het oogpunt van kosten en effectiviteit groeit de behoefte aan digitale data-uitwisseling binnen een instelling en tussen een instelling en externe locaties. De hoeveelheid informatie en complexiteit van de informatievoorziening nemen in snel tempo toe.

Grotere afhankelijkheid van het mobiele platform

In ons ICT-gebruik neemt het mobiele platform een steeds prominentere rol in. Burgers, bedrijven en overheden benutten mobiele apparaten en toepassingen steeds meer voor nieuwe functionaliteiten en om (persoons)gegevens op te slaan. Dit uit zich

5 Zie http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2010/06/23/informatie-vitale-sectoren/vitale-sectoren.pdf.

in een toenemend aantal mobiele breedbandinternetaansluitingen. Aan het einde van het tweede kwartaal van 2012 zijn er 9,8 miljoen aansluitingen voor mobiel breedband (+2,1 miljoen).[6] Het totaal aantal mobiele aansluitingen blijft redelijk stabiel op ongeveer 21,7 miljoen.

Circa 23 procent van de internetters in Nederland heeft inmiddels een tablet. Smartphones hebben een aandeel van 48 procent.[7] Door de groei van zowel het gebruik van mobiele ICT-platforms als de informatie die daarop wordt verzameld, verwerkt en uitgewisseld, nemen de gevolgen van succesvolle cyberaanvallen tegen of via deze platformen toe.

Omvangrijk gebruik sociale media

Sociale media zijn populair in Nederland. We behoren relatief gezien tot de grootste sociale mediagebruikers ter wereld.[3: CBS 2012] Cijfers uit 2011 van het CBS laten zien dat vooral jongeren in de leeftijd van 12 tot 25 jaar veel gebruikmaken van sociale media, maar liefst 95 procent.[3: CBS 2012] Deze gebruikscijfers nemen in hogere leeftijdscategorieën af. Iets meer dan een vijfde van de 65- tot 75-jarige internetgebruikers nam bijvoorbeeld in 2011 deel aan een sociaal netwerk.

Door de groei van zowel het gebruik van sociale media als de informatie die daarop wordt verzameld, verwerkt en uitgewisseld, nemen de gevolgen van cyberaanvallen tegen of via sociale media toe. Privacy, intellectueel eigendom en vertrouwelijke informatie over het functioneren van de organisatie zijn belangen die op het spel staan als informatie, gedeeld via sociale media, in handen valt van mensen waarvoor het niet bedoeld is. Denk aan de sollicitant die zich afgewezen ziet, omdat de werkgever al te frivole tweets of foto's op Facebook aantrof.

Twitter en Wordpress-accounts van Reuters gehackt
In de zomer van 2012 nam het Syrian Electronic Army meerdere malen Twitter[8] en Wordpress-accounts van het persbureau Reuters over, om daar vervolgens onjuiste berichten te plaatsen over het conflict in Syrië en het welzijn van buitenlandse politici.[9]

Toename gebruik cloud

Zowel voor bedrijven en overheden als voor burgers zijn clouddiensten interessant vanuit het oogpunt van flexibliteit, kosten en gebruiksgemak. Medewerkers gebruiken onlinediensten op eigen initiatief, bijvoorbeeld online filesharing, zoals Yousendit.com, voor het geval het e-mailsysteem van het bedrijf geen grote bijlagen toestaat, of Dropbox voor het opslaan en delen van bestanden met collega's of derden buiten de organisatie. Dit leidt ertoe dat zowel persoonlijke als bedrijfsgegevens meer en meer in de cloud worden opgeslagen. Mobiele oplossingen faciliteren dit proces verder, omdat de gebruiker de gegevens tussen zijn apparaten eenvoudig kan uitwisselen en ze in de cloud zijn veiliggesteld voor verlies.

Door de toename van het gebruik van de cloud neemt de afhankelijkheid van derde partijen toe. Immers aanvallen op clouddiensten en -dienstverleners raken ook degenen die hun informatie in de cloud hebben geplaatst. Aan de andere kant biedt het kleinere organisaties met minder beveiligingsexpertise ook de mogelijkheid om tegen aanvaardbare kosten een hoger beveiligingsniveau te bereiken door samen te werken met een leverancier die dit beter kan.

Het kabinet heeft er, gezien de risico's van cloudcomputing, voor gekozen een gesloten Rijkscloud in eigen beheer in te richten als een voorziening die generieke diensten levert binnen de Rijksdienst.[10]

'Big data gets bigger'

Big data (bijvoorbeeld in de consumentenmarketing, zakelijke dienstverlening, opsporing en het financiële verkeer) staat in de belangstelling van grote informatieverwerkers én technologieleveranciers, en het gebruik van big-data-technieken mag dan ook verwacht worden te stijgen. Wanneer het persoonsgegevens betreft, levert het aanleggen van grote dataverzamelingen risico's op voor privacy. De grote databestanden vormen verder op zichzelf een nieuw, gevoelig te beschermen belang voor een organisatie en in sommige gevallen mogelijk ook voor de samenleving. Het databestand vertegenwoordigt namelijk grote waarde voor kwaadwillenden, die de data kunnen gebruiken voor aanvallen tegen derden, zoals identiteitsfraude. Het is echter de vraag of de eigenaar van de big data zich altijd bewust is van de risico's en bereid is de noodzakelijke maatregelen te nemen om de belangen van derden te beschermen.

Groei onlinetransacties burgers

Burgers vinden steeds meer het onlinekanaal. Zo neemt het gebruik en de omzet van onlinewinkelen in Nederland nog altijd toe, naar een omzet van 9,8 miljard euro in 2012 (+ 9 procent ten opzichte van 2011).[11] Nederland is in Europa een van de koplopers in percentage mensen van de bevolking dat wel eens online koopt.[12] Ook in de gamingindustrie groeit het belang van het onlinekanaal (aangezwengeld door jongeren) en zal het naar verwachting qua omzet de fysieke verkoop wereldwijd in 2013 gaan overtreffen.[13]

6 OPTA 2013.
7 TNO 2013.
8 http://www.reuters.com/article/2012/08/06/net-us-reuters-syria-hacking-idUSBRE8721B420120806
9 http://www.bbc.co.uk/news/technology-19280905
10 http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/04/20/kamerbrief-over-cloud-computing/kamerbrief-over-cloud-computing.pdf
11 http://www.thuiswinkel.org/groei-online-markt-9-naar-98-miljard-ondanks-recessie
12 TNO 2013, op basis van cijfers van Eurostat uit 2011.
13 PwC, Global Entertainment & Media Outlook 2012-2016, 2012. Aangevuld met Nederlandse situatie in http://www.marketingfacts.nl/berichten/in-2013-meer-online-gamers-dan-console-gamers

Verder maken Nederlanders relatief veel gebruik van internetbankieren (82 procent van alle internetgebruikers). In alle leeftijdscategorieën is het gebruik van internetbankieren de afgelopen jaren sterk gegroeid, blijkt uit cijfers van het CBS.[3: CBS 2012] Ruim zeven op de tien Nederlanders van 12 jaar en ouder regelden vorig jaar hun bankzaken via het internet. Door de toename van onlinetransacties neemt de economische impact van ICT-verstoringen en cyberaanvallen toe. Randvoorwaardelijk hiervoor is het vertrouwen van burgers in de betrouwbaarheid van de onlinevoorzieningen (ketenbelang).

Digitale identiteit

Mede door het toenemende gebruik van onlinetransacties voor winkelen, bankieren en overheidsdiensten, is de digitale identiteit van burgers en werknemers van overheden en bedrijven een zelfstandig belang geworden. Voor kwaadwillenden vertegenwoordigt die digitale identiteit de sleutel tot gevoelige data, geld en nuttige diensten. Wanneer die identiteit onvoldoende kan worden gewaarborgd, zijn de individuele belangen van burgers en de belangen van organisaties in het geding.

Toename ICT-afhankelijkheid elektriciteitsvoorziening

De introductie van *smart grid* en *smart meters* vergroten het belang van ICT voor onze stroomvoorziening nog verder. De term smart grid wordt gebruikt voor de toepassing van ICT om de fluctuerende lokale vraag en aanbod van elektriciteit met elkaar te matchen om overbelasting van het netwerk te voorkomen. In Nederland worden al smart meters uitgerold bij huishoudens. Dit zijn digitale elektriciteitsmeters, die de netbeheerder op afstand kan uitlezen en bedienen. Ook gas- en watermeters wacht digitalisering.

Met deze digitalisering komt er een forse datacomponent bij. Gegevens over gebruik én productie door burgers en bedrijven en over productie door energiecentrales en dergelijke zullen namelijk in meer detail worden verzonden, verwerkt en opgeslagen dan nu het geval is. Beschikbaarheid en integriteit van deze data zijn een randvoorwaarde voor het goed functioneren van het grid. Vertrouwelijkheid is dat ook, gezien de privacyrisico's die aan gegevens over gebruikers kleven.

Hyperconnectiviteit: alles wordt altijd met alles verbonden

Een tweetal trends tonen de behoefte van de mens om altijd, overal en met verschillende middelen toegang te hebben tot onlinediensten. Enerzijds de trend om steeds meer mobiele apparatuur (zoals smartphones en tablets) te gebruiken en hiermee permanent, via het internet verbonden te zijn; anderzijds de trend om steeds meer (consumenten)producten als auto's, koffieautomaten en koelkasten van rekenkracht en netwerkmogelijkheden te voorzien. Deze trends worden tezamen ook wel hyperconnectiviteit genoemd.

1.4 Conclusie

Belangen in het kader van cybersecurity kennen verschillende niveaus: persoonlijke belangen, organisatiebelangen, ketenbelangen en maatschappelijke belangen. Cybersecurity vereist bescherming van al die belangen.

Evenals in voorgaande jaren neemt de afhankelijkheid van ICT steeds meer toe met als gevolg dat het niet-functioneren ervan of inbreuk op de vertrouwelijkheid en integriteit van informatie steeds meer belangen raakt en met grotere gevolgen. Deze toenemende afhankelijkheid is ook van toepassing op de vitale sectoren. Daarbij worden de sectoren elektriciteit, Telecom en IT-services als randvoorwaardelijk gezien vanuit perspectief van cybersecurity. De toegenomen afhankelijkheid is zeker van toepassing op gedeelde onlinediensten zoals DigiD en iDeal.

Actuele ontwikkelingen, zoals cloudcomputing, sociale media en hyperconnectiviteit, leiden tot een stijgend gebruik van het internet als platform voor zakelijke transacties, de verwerking van vertrouwelijke informatie en het gebruik van ICT voor de aansturing van maatschappelijk belangrijke processen. Het gemak waarmee het internet toegepast kan worden, versterkt deze ontwikkeling en brengt tegelijkertijd risico's met zich mee waar niet altijd voldoende over wordt nagedacht. Omdat Nederland sterk heeft ingezet op de elektronische dienstverlening, kunnen cybersecurity-incidenten een grote impact hebben. «

2 Dreigingen: actoren en hun intenties

Dit hoofdstuk gaat in op het eerste aspect van dreigingen, te weten de actoren, hun intenties en ontwikkelingen op dit vlak. Een 'actor' is een rol die een partij speelt op het gebied van cybersecurity. Partijen kunnen meerdere rollen hebben en dus als verschillende actoren optreden. Ook kunnen actoren bedoeld of onbedoeld van elkaars capaciteiten gebruikmaken.

Na de beschrijving van de actoren is een overzicht opgenomen waarin de actoren, hun intentie, vaardigheden en primaire doelwitten zijn samengebracht.

Het is niet altijd met zekerheid vast te stellen welk type actor achter een bepaalde cyberaanval zit, dit is het attributievraagstuk. Voorbeelden zijn de DDoS-aanvallen op diverse Nederlandse banken, KLM en DigiD, waarvan (nog) niet met zekerheid kan worden aangegeven welke actor ervoor verantwoordelijk is. Ook als een aanval door een actor wordt geclaimd, dan is het nog maar de vraag of de claim juist is.

2.1 Staten

Onder 'statelijke actoren' verstaan we actoren die onderdeel vormen van de overheid van een land. Staten hebben als dreiger de intentie om hun geopolitieke positie (bijvoorbeeld diplomatiek, militair of economisch) te verbeteren of om bijvoorbeeld invloed uit te oefenen op dissidenten of oppositiegroeperingen die zich verzetten tegen het heersende regime. Wereldwijd zijn regeringen zich bewust van de strategische betekenis van het cyberdomein. Verschillende staten versterken daarom hun digitale vaardigheden en ontwikkelen of investeren in digitale hulpmiddelen (cybercapaciteiten).

Verstoring van ICT door inzet van offensieve cybercapaciteiten (in verschillende gradaties) kan als middel worden ingezet door staten of aan staten gerelateerde actoren. Hierbij kan ook gebruikgemaakt worden van andere actoren, onder meer om attributie naar een staat te voorkomen.

Digitale spionage door staten, gesteund door staten, toegestaan door staten of met de staat als uiteindelijke begunstigde, vormt een grote dreiging voor de Nederlandse economie en de nationale veiligheid. Uit onderzoek van de Nederlandse inlichtingendiensten blijkt dat deze spionageactiviteiten in Nederland vooral gericht zijn op overheidsinstanties, non-gouvernementele organisaties, het bedrijfsleven, de wetenschap, dissidenten en oppositionele groeperingen. Dergelijke activiteiten worden ook wel aangeduid als Advanced Persistent Threat (APT). De grootste cyberspionagedreiging tegen Nederlandse belangen gaat momenteel uit van actoren die te relateren zijn aan China, Rusland, Iran en in mindere mate Syrië.[14]

Zo zijn er aanwijzingen dat binnen China diverse actoren zoals inlichtingendiensten, leger, hackersgroepen en universiteiten te relateren zijn aan digitale inlichtingenactiviteiten. Er zijn wereldwijd grootschalige aanvallen afkomstig van Chinese actoren onderkend, die zich onder meer richten op de petrochemische, automobiel-, farmaceutische, defensie-, maritieme, lucht- en ruimtevaartindustrie. Deze aanvallen hebben als doel het verkrijgen van militaire en economisch relevante informatie.[14]

Digitale inlichtingenactiviteiten van actoren die te relateren zijn aan Rusland richten zich op overheidsinstanties (vooral ministeries van defensie en buitenlandse zaken), internationale organisaties (vooral de NAVO), defensietoeleveringsbedrijven, het bankwezen, de energiesector en Russische dissidenten. De vanuit Syrië afkomstige digitale inlichtingenactiviteiten zijn vooral gericht op het intimideren van Syrische dissidenten en het verstoren van hun communicatie.

Statelijke actoren die investeren in offensieve cybercapaciteiten kunnen deze inzetten tijdens conflicten met andere staten of oppositionele groepen. Een dergelijk conflict in het cyberdomein zou veelal dezelfde elementen als in de fysieke wereld omvatten, namelijk propaganda, spionage, observatie, manipulatie, sabotage of (tijdelijke) disruptie, verkenningen, intimidatie van opposanten en gerichte aanvallen. Zo zou de Shamoon-malware (zie paragraaf 2.10) zijn verspreid door een statelijke actor als vergeldingsactie voor Stuxnet.

De meest vergaande vorm van de inzet van offensieve cybercapaciteiten is wanneer deze wordt ingezet als onderdeel van oorlogsvoering. Digitale oorlogsvoering is *"het uitvoeren van militaire operaties die erop zijn gericht om met digitale middelen computersystemen of netwerken van een tegenstander te verstoren, misleiden, veranderen of vernietigen"*.[15] Om te kunnen spreken van oorlogsvoering, moet wel aan de voorwaarden daarvoor zijn voldaan: een gewelddadige handeling die instrumenteel is aan een politiek doel (van een staat), namelijk om een tegenstander zijn wil op te leggen.[44: Rid 2012] Bij conflicten die (deels) worden uitgevochten in het digitale domein, kunnen partijen worden geschaad die niet rechtstreeks betrokken zijn bij het conflict. Zo kunnen statelijke actoren gebruikmaken van kwetsbaarheden in privé- en bedrijfscomputers.

2.2 Terroristen

'Terroristen' handelen vanuit ideologische motieven. Hun doel is maatschappelijke veranderingen te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden. Zij schuwen daarbij geen middelen en gebruiken gericht

14 Jaarverslag 2012 van de AIVD.
15 Adviesraad Internationale Vraagstukken, Commissie van Advies Inzake Volkenrechtelijke Vraagstukken, Digitale Oorlogvoering, No 77, AIV/No 22, CAVV december 2011.

geweld tegen mensen of richten maatschappijontwrichtende schade aan.[16] Terroristen kunnen cyberaanvallen uitvoeren tegen de infrastructuur van het internet (internet als doelwit), via het internet fysieke doelen zoals een elektriciteitscentrale treffen (internet als wapen) of het internet gebruiken als ondersteuning voor hun terroristische activiteiten, zoals voor het voeren van propaganda (internet als middel).

Cyberaanvallen door terroristen tegen het internet of via het internet met ontwrichtende schade hebben zich voor zover bekend nog niet voorgedaan. Om daadwerkelijk maatschappijontwrichtende schade aan te richten, zijn complexe destructieve cyberaanvallen vereist of is een gericht aanvalsplan vereist waarin optimaal gebruik wordt gemaakt van zwakke plekken. Terroristen beschikken (nog) niet over voldoende vaardigheden en middelen voor maatschappijontwrichtende cyberaanvallen. Wel groeit onder jihadisten de interesse voor cyberjihad en er verschijnen postings op internationale jihadistische fora waarin wordt opgeroepen tot cyberaanvallen. Jihadisten hebben in het buitenland kleinschalige en eenvoudige cyberaanvallen (defacements en DDoS-aanvallen) uitgevoerd. Wraak in combinatie met propaganda lijkt een voornaam motief. Terroristen en zeker jihadisten gebruiken al jaren het internet als middel voor bijvoorbeeld propaganda, informatie-inwinning, virtuele netwerkvorming, onderlinge communicatie, aansturing of planning van aanslagen. Bij sommige vormen van dit gebruik benutten jihadisten hackvaardigheden, bijvoorbeeld voor informatie-inwinning of propaganda. Zo was een buitenlandse terroristische groep op zoek naar een hacker om zo aan informatie uit systemen te komen. Verder bleek begin 2013 dat jihadisten wereldwijd een tiental sites hadden gehackt om zo serverruimte ter beschikking te krijgen voor het down- en uploaden van jihadistische propaganda.[17] Daaronder bevond zich een site van een Nederlander.[18] De kennis die terroristen met dit type hackvaardigheden opdoen, kunnen zij uiteindelijk ook ten goede laten komen aan het uitvoeren van meer geavanceerde cyberaanvallen.

Jihadisten kunnen een cyberdreiging vormen voor de nationale veiligheid. De inlichtingendiensten schatten hun digitale potentie momenteel in als beperkt en daarmee ontoereikend om hun cyberterroristische intenties waar te maken. De cyberdreiging afkomstig van jihadisten vormt dan ook een kleine tot gemiddelde dreiging voor de nationale veiligheid.

16 De officiële definitie van terrorisme luidt: Het uit ideologische motieven dreigen met, voorbereiden of plegen van op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappijontwrichtende zaakschade, met als doel maatschappelijke veranderingen te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden.

17 'Jihadist Turns Hacked Websites into File Servers for Jihadi Propaganda', Site Monitoring Service Jihadist Threat, February 12 2013.

18 Het hacken van serverruimte heeft zich eerder voorgedaan waaronder in Nederland, zie hiervoor NCTb, 'Jihadisten en het internet', 2006.

2.3 Beroepscriminelen

'Beroepscriminelen', ook wel aangeduid als cybercriminelen, zijn personen en groepen van personen die criminele activiteiten ontplooien 'als beroep'. De primaire drijfveer van beroepscriminelen is het verdienen van geld. Het internet is een aantrekkelijke omgeving voor beroepscriminelen om dit financiële gewin te bereiken, bijvoorbeeld door aanvallen op internetbankieren.

Bedrijfsspionage

"Hightechcriminelen beschouwen grote multinationals als aantrekkelijk doelwit voor bedrijfsspionage. Dergelijke organisaties maken doorgaans gebruik van complexe ICT-systemen en -netwerken. Aangezien deze bovengemiddeld beveiligd zijn – of verondersteld worden dat te zijn – gaat het in veel gevallen om gerichte aanvallen die hoge eisen stellen aan de organisatievorm en werkwijze van de daders. De criminele samenwerkingsverbanden zijn goed georganiseerd en gebruiken relatief nieuwe, geavanceerde technieken en middelen. Ze kunnen bijvoorbeeld langs technologische weg de beveiliging van een ICT-systeem doorbreken en malware installeren. Hiervoor gebruiken ze vooral spyware. Daders zullen zich richten op de zwakste schakel in de beveiliging. Dat kunnen technologische kwetsbaarheden zijn, maar ook mensen."[29: NP 2012-2]

Er zijn (groepen van) criminelen die beschikken over geavanceerde cybervaardigheden en over professionele middelen. Er is zelfs een relatief kleine groep specialisten te onderkennen die een uitzonderlijk hoog niveau van kennis en expertise heeft. Zij zijn de motor achter nieuwe ontwikkelingen in cyberaanvallen met een crimineel oogmerk. Deze groep werkt soms intensief samen om zo te kunnen specialiseren en differentiëren. Toch is het niet zo dat iedere beroepscrimineel hoeft te beschikken over geavanceerde cybervaardigheden en professionele middelen om geld te kunnen verdienen. Er is er een zeer levendige ondergrondse economie ontstaan, een criminele cyberdienstensector, waarin de vraag naar en het aanbod van illegale virtuele activiteiten samenkomen. Zo bieden de meer professionele criminelen hun botnets te huur aan, hetzij voor eenmalige acties of voor langere perioden. Soms komen ook constructies voor die op een vorm van pacht lijken, ook wel 'malware-as-a-service' of 'cybercrime-as-a-service' genoemd.

In de werkwijze van criminelen heeft in de rapportageperiode geen substantiële verandering plaatsgevonden. Wel worden criminelen brutaler in hun handelen. Een voorbeeld hiervan is het gebruik van *ransomware*. Botnets blijven een geliefd hulpmiddel voor criminelen om veel geld te verdienen, zoals het Dorifel-botnet en het Pobelka-botnet hebben laten zien. Criminelen maken vaker gebruik van malware om computers over te nemen en minder van phishing om inloggegevens te bemachtigen.

Hoewel criminelen digitale spionage of sabotage niet als hoofddoel hebben, gaat er een zekere dreiging van deze actor uit tegen de

nationale veiligheid wanneer zij hun capaciteiten in dienst stellen van staten.

Creditcardfraude na diefstal van digitale gegevens
"Een specifieke vorm van fraude met betaalkaarten is de zogenoemde card-not-presentfraude. De helft van alle creditcardfraude wordt op die wijze gepleegd. Bij deze vorm wordt op afstand betaald via de post, de telefoon of het internet. Vaak gaat het om betalingen van aankopen in webwinkels. Er is geen direct contact tussen de koper en verkoper en de fysieke kaart wordt niet gecontroleerd. De koper vult de heimelijk verkregen gegevens in zoals naam, nummer, vervaldatum en verificatiecode. Als die kloppen, verstuurt de verkoper de gekochte goederen. De fraudeurs verkrijgen deze informatie niet alleen via phishing, ook worden servers van webwinkels gehackt om creditcardgegevens te stelen."[29: NP 2012-2]

2.4 Cybervandalen en scriptkiddies

Cybervandalen hebben veel kennis, ontwikkelen hun eigen hulpmiddelen of breiden die van anderen uit. Hun motieven zijn niet financieel of ideologisch van aard, want zij voeren hacks uit omdat het kan of om aan te tonen dat zij ertoe in staat zijn.

Scriptkiddies zijn hackers met beperkte kennis, die gebruikmaken van technieken en hulpmiddelen die door anderen zijn bedacht en ontwikkeld. Vaak zijn het jongeren en meestal zijn zij zich nauwelijks bewust van of geïnteresseerd in de gevolgen van hun handelen. Hun motieven zijn vaak baldadigheid en het zoeken van een uitdaging. Zij kunnen met hun acties voor maatschappelijke onrust zorgen, vooral wanneer deze op sociale en reguliere media worden uitvergroot. De toenemende vereenvoudiging van de bediening van hackertools in combinatie met rijkere functionaliteit zorgt ervoor dat ook scriptkiddies met hun beperkte kennis steeds meer mogelijkheden krijgen voor inbraak, spionage / gluren[19] en sabotage.

2.5 Hacktivisten

'Hacktivisten' zijn personen of groeperingen die ideologisch gemotiveerd cyberaanvallen uitvoeren. De ideologische motieven van hacktivisten zijn divers en kunnen in de tijd en tussen (groepen van) hacktivisten variëren. Zo strijden hacktivisten onder de noemer 'Anonymous' voor vrijheid van het internet en tegen controle en censuur van het internet. Sinds begin 2012 wordt onder de naam Anonymous een verscheidenheid aan acties geclaimd: publiceren van gegevens van bankmanagers[20], DDoS-aanvallen op overheidwebsites[21], uit de lucht halen van kinderpornowebsites[22], kraken van twee websites van MIT[23], publiceren van de broncode van VMware[24] en aanvallen tegen Israëlische websites[25]. Overigens blijkt uit gesprekken van een onderzoeksjournalist met gearresteerde hackers dat het sommigen te doen was om de lol, terwijl anderen meer ideologisch gedreven waren. Soms werd overigens na een hack pas het motief bedacht.[40: Olson 2012]

Andere groepen hacktivisten hebben weer andere motieven. Zo maken moslims die ageren tegen 'islamvijandige' westerse uitingen, geregeld ook gebruik van virtuele acties, zoals defacements en (D)DoS-aanvallen. Ideologisch gemotiveerde cyberaanvallen, variërend van defacements en (D)DoS-aanvallen tot diefstal van informatie die vervolgens wordt gepubliceerd, lijken mondiaal steeds vaker voor te komen.[28: NP 2012-1] Overigens is niet helder of ideologisch gedreven personen en groepen steeds vaker kiezen voor cyberaanvallen of dat hackers steeds vaker uit ideologische motieven handelen.

Tal van succesvolle hacktivistische cyberaanvallen hebben wel aangetoond dat hacktivisten over vaardigheden beschikken voor grote en succesvolle hacks. Toch kunnen die vaardigheden sterk verschillen binnen en tussen netwerken en sterk afhankelijk zijn van tal van factoren. Zo opereren hacktivisten veelal in fluïde netwerken die vaak openstaan voor bijdragen van iedereen. Wel zijn er mensen aan te wijzen die een belangrijke rol spelen in de aanvallen, bijvoorbeeld door hun ervaring, kennis, middelen of positie in bijvoorbeeld IRC-kanalen.[40: Olson 2012] Deze kunnen het verschil uitmaken tussen de groepen wat betreft vaardigheden om spraakmakende hacks uit te voeren. Ook is het zo dat kennis en middelen veelal vrijelijk en onvoorwaardelijk worden gedeeld.[28: NP 2012-1] Verder kunnen tijdens een campagne hackers spontaan hun kennis van kwetsbaarheden of hun eerder gestolen informatie aanbieden. Hierdoor lijkt het dat de hacks binnen de campagne hebben plaatsgevonden.[40: Olson 2012] Deze reeks aan succesvolle hacks draagt bij aan het gepercipieerde succes van de campagne.

Ideologisch gemotiveerde cyberaanvallen zijn, ondanks specifieke claims, soms toch lastig toe te wijzen aan een specifieke actor(groep). Zo valt soms weinig samenhang te ontdekken in claims en claimen sommigen uit naam van een groep een actie die later wordt weersproken. Ook het fluïde karakter van netwerken maakt het lastig cyberaanvallen specifiek toe te wijzen aan een specifieke actor(groep).

19 https://www.security.nl/artikel/44879/1/Hackertool_laat_hackers_via_webcam_meegluren.html
20 Zie onder andere http://www.zdnet.com/anonymous-posts-over-4000-u-s-bank-executive-credentials-7000010740/
21 http://news.techworld.com/security/3379510/hacktivists-ddos-uk-us-swedish-government-websites/, http://news.techworld.com/security/3377063/uk-government-websites-attacked-by-anonymous-over-assange/
22 http://pastebin.com/NAzTGeM2
23 http://tweakers.net/nieuws/86620/anonymous-kraakt-websites-mit-na-zelfmoord-aaron-swartz.html
24 https://www.security.nl/artikel/43806/Anonymous_publiceert_broncode_VMware_ESX.html
25 'Anonymous wil Israël van internet verwijderen', ANP, 6-4-2013.

Hacktivisten voeren vanuit activistische motieven digitale aanvallen uit. Zij doen dit veelal echter niet met de intentie de maatschappij te ontwrichten. Zij kunnen in theorie wel voor dit doel ingezet worden. Op basis van voorbeelden in het buitenland, waarbij in enkele gevallen sprake was van ernstige verstoringen, wordt de cyberdreiging tegen Nederland van hacktivisten als gemiddeld ingeschat.

2.6 Interne actoren

'Interne actoren' zijn individuen die (tijdelijk) in een organisatie aanwezig zijn of zijn geweest, zoals (oud-)medewerkers, inhuurkrachten en leveranciers. Hun intentie kan wraak zijn, bijvoorbeeld naar aanleiding van ontslag. Er kan ook sprake zijn van financiële of politieke motieven. Interne actoren kunnen diensten ook aanbieden aan anderen of daartoe worden benaderd of aangezet door bijvoorbeeld staten voor spionagedoeleinden. Zij kunnen bij kwade intenties of nalatigheid een grote dreiging voor een organisatie vormen en significante schade veroorzaken, juist omdat ze over veel interne kennis beschikken. Dat het hierbij niet (altijd) hoeft te gaan om geavanceerde cyberaanvallen, blijkt uit een rapport van het CERT Coordination Center. USB-sticks zijn bijvoorbeeld een ideale manier voor kwaadwillend personeel om vertrouwelijke bedrijfsgegevens te stelen, maar veel bedrijven staan hier niet bij stil.[26] Bovendien kan een interne actor ook onbewust betrokken raken bij een cyberaanval, bijvoorbeeld door op een phishing e-mail te reageren.

Ondanks dat in menig rapport wordt gewezen op het gevaar dat interne actoren betrokken raken bij cyberaanvallen of deze zelf uitvoeren, laten verschillende internationale onderzoeken zien dat deze groep in ieder geval een klein aandeel heeft in cybercrime. [4: CERT-AU 2012][54: Verizon 2012] In open bronnen zijn weinig voorbeelden bekend waarbij interne actoren cyberaanvallen hebben uitgevoerd of daaraan hebben bijgedragen. Dat kan te maken hebben met terughoudendheid van organisaties om hiervan melding te maken.[27] Dat de gevolgen van 'hacks' door interne actoren groot kunnen zijn, blijkt wel uit de WikiLeaks affaire in 2010. Verder zou volgens sommige mediaberichten in de casus van Saudia Aramco, een incident met grote gevolgen voor het bedrijf, sprake zijn geweest van betrokkenheid van een interne actor.

2.7 Cyberonderzoekers

Onder 'cyberonderzoekers' verstaan we actoren die op zoek gaan naar kwetsbaarheden en/of inbreken in ICT-omgevingen om de (te) zwakke beveiliging ervan aan de kaak te stellen. Deze groep omvat ideële onderzoekers, partijen die geld willen verdienen aan hun onderzoek en universitaire onderzoekers die al dan niet in opdracht van overheden of andere organisaties werken. De vaardigheden van cyberonderzoekers kunnen variëren en zij kunnen al dan niet de vaardigheden inhuren van andere hackers en deskundigen. Zij gebruiken vaak de media om hun bevindingen te publiceren en de bewustwording over de noodzaak van cybersecurity te vergroten. Naast deze positieve bijdrage aan verdere bewustwording, kunnen de activiteiten en publiciteit van cyberonderzoekers vooral overheidsinstellingen en bedrijven wel (tijdelijk) extra kwetsbaar maken doordat anderen kunnen proberen te profiteren van de onderzoeksbevindingen en leiden tot imagoschade.

Onlinewinkels kwetsbaar

Een onderzoek dat is uitgevoerd in opdracht van NRC Handelsblad[28] toonde aan dat minstens twaalf door een keurmerk gecertificeerde winkels gevoelig waren voor datadiefstal door SQL-injectieaanvallen. Hiermee zijn persoonsgegevens en (versleutelde) wachtwoorden in te zien en te gebruiken voor ongeëigende doeleinden, ten koste van de privacy of financiën van burgers en organisaties. De verschillende keurmerken schrijven overigens weinig voor over beveiliging.

In de afgelopen periode waren cyberonderzoekers onder meer actief met de verdere ontwikkeling en vrijgave van hacking toolkits voor bijvoorbeeld Android[29] en search engine hacking[30]. Daarnaast verschenen publicaties over vernieuwing van aanvalsmethoden op bijvoorbeeld authenticatie van webtransacties[31], pinapparaten[32] en de encryptiemethode RC4[33] en het plaatsen van achterdeurtjes op hardware (BIOS chips, firmware, EPROMs)[34]. Van andere orde is het aantonen van statelijke spionageactiviteiten, zoals de toepassing van de spionagetool Finfisher of FinSpy in meer dan 25 landen[35] en (meer details over) de structuur van StuxNet, Flame, Gauss en andere platforms. Ten slotte waren er in 2012 diverse gevallen waarin onderzoekers kwetsbaarheden van systemen in de praktijk blootlegden.

2.8 Private organisaties

'Private organisaties', bijvoorbeeld bedrijven, kunnen als organisatie een dreiger zijn. Private organisaties kunnen via internet veel (openbare) informatie over concurrenten en klanten verkrijgen om hun concurrentiepositie te verbeteren. De grens tussen legitieme analyse en 'profiling' van organisaties en mensen binnen de grenzen van de wet en illegale bedrijfsspionage en schending van

26 'USB-stick ideale backdoor voor kwaadwillend personeel', Security.nl, 7-5-2013 (https://www.security.nl/artikel/46159/1/USB-stick_ideale_backdoor_voor_kwaadwillend_personeel.html)
27 Angela Gendron, Martin Rudner, 'Assessing cyber threats to Canadian infrastructure. Report prepared for the Canadian security intelligence service', March 2012.
28 NRC Handelsblad, Geen enkele webwinkel is totaal veilig, 5 april 2013.
29 http://tweakers.net/nieuws/83575/onderzoekers-brengen-malware-developmentkit-uit-voor-android.html, http://toorcamp.org/content12/38
30 http://www.darkreading.com/cloud-security/167901092/security/vulnerabilities/240004376/researchers-to-launch-new-tools-for-search-engine-hacking.html.
31 http://www.pcworld.com/businesscenter/article/261988/security_researchers_to_present_new_crime_attack_against_ssltls.html
32 http://tweakers.net/nieuws/83355/pinapparaat-te-hacken-via-nep-pinpas.html
33 https://www.security.nl/artikel/45522/1/Onderzoekers_kraken_RC4-encryptie.html
34 http://www.hotforsecurity.com/blog/security-researcher-introduces-proof-of-concept-tool-to-infect-bios-network-cards-cd-roms-2906.html - onderliggende paper: Jonathan Brossard, Hardware backdooring is practical, 2012.
35 http://www.theregister.co.uk/2013/03/19/finfisher_spyware_apac_countries/; https://citizenlab.org/2013/04/for-their-eyes-only-2/

privacy is daarbij niet altijd duidelijk. In algemene zin valt er weinig te zeggen over de vaardigheden van deze actor: die kunnen variëren van heel beperkt tot heel geavanceerd. In de afgelopen periode is er geen significante wijziging opgetreden in het handelen van private organisaties als dreiger.

2.9 Burgers

Onder de actor 'burgers' valt iedere particulier die niet de rol van een andere actor aanneemt. Burgers kunnen direct of indirect een doelwit vormen van staten, terroristen, beroepscriminelen, hacktivisten, cybervandalen en scriptkiddies. Dissidenten afkomstig uit andere landen zouden bijvoorbeeld een direct doelwit kunnen zijn van een regime waarvoor zij zijn gevlucht. Het gaat dan veelal om spionage of verstoring van ICT. Criminelen hebben het gemunt op bank- of identiteitsgegevens van burgers of kunnen proberen ICT van burgers over te nemen zodat die onderdeel gaat uitmaken van een botnet. Burgers kunnen ook te maken krijgen met een aanval tegen voor hen belangrijke dienstverlening. Illustratief in dat kader is de storing bij een bank in april 2013, waardoor klanten geen gebruik konden maken van internetbankieren, maar sommigen ook nog eens te maken kregen met onterechte, dubbele afboekingen van hun rekening. Verder kunnen burgers een indirect doelwit zijn van bijvoorbeeld digitale diefstal door hacktivisten of cyberonderzoekers. Na een hack komt immers soms gevoelige informatie, zoals wachtwoorden, persoons- of financiële informatie in de openbaarheid.

Burgers zijn kwetsbaar voor cyberaanvallen tegen hun ICT en/of al dan niet bij anderen opgeslagen informatie, hebben soms een laag veiligheidsbewustzijn en beperkte expertise om de weerbaarheid tegen dreigingen te verhogen.

2.10 Beoordeling

Actoren waar een dreiging van uitgaat verschillen wat betreft hun intentie, vaardigheden en doelwitkeuze. Bij incidenten die zich hebben voorgedaan, is het niet altijd eenvoudig om het achterliggende type actor te achterhalen. Niet alle aanvallen worden geclaimd en als ze wel worden geclaimd, is het ook lang niet altijd zeker of de claim wel de ware intentie blootlegt. De politie stelt dat veel hacktivistische activiteiten door scriptkiddies worden uitgevoerd.[28: NP 2012-1] In het geval van cyberaanvallen als reactie op gepercipieerde islamvijandigheden is ook lang niet altijd helder of het gaat om hacktivisten of wellicht terroristen. In het geval van hacktivisten in conflictsituaties gaat het niet altijd om onafhankelijke personen of groepen die los van een staat vanuit hun eigen ideologische of andere motieven handelen. Ook in het geval van de Shamoon-malware, dat gericht was tegen een grote oliemaatschappij in Saoedi-Arabië, is niet helder wie daarachter zat. Zo stelde: 'Cutting Sword of Justice', de groep die de aanval claimde, dat Saoedi-Arabië de inkomsten uit olie misbruikt om corrupte regimes financieel te steunen en dat daarom de oliemaatschappij werd aangevallen. In mediaberichten is echter Iran menigmaal genoemd als mogelijke dader met 'Cutting Sword of Justice' als rookgordijn, hoewel niet iedereen daarvan overtuigd is.

De typen actoren kunnen bovendien onderling samenwerken, waarbij de ene partij de ander inhuurt of zich een gelegenheid voordoet waar beide partijen van kunnen profiteren. Zo zou een criminele botnetbeheerder zijn diensten hebben aangeboden voor een aanval tegen de geruchtmakende cyberaanval van Anonymous tegen PayPal in 2010.[40: Olson 2012] Ook kunnen ze van elkaars kennis en gebruikte methoden leren. De gepubliceerde kennis en ontwikkelde tooling van bijvoorbeeld cyberonderzoekers kunnen andere actoren benutten voor hun aanvallen. Algemeen wordt ook aangenomen dat diverse partijen hebben geleerd van Stuxnet, de zeer geavanceerde cyberaanval, door deze grondig te bestuderen. Op die wijze is sprake van proliferatie van kennis.

2.11 Conclusie

Tabel 2 bevat een overzicht van actoren, hun intentie, vaardigheden en primaire doelwitten.

De grootste dreiging gaat op dit moment uit van staten en beroepscriminelen en in mindere mate van cybervandalen, scriptkiddies en hacktivisten. Het is niet altijd mogelijk om te achterhalen welk type actor achter een cyberaanval zit: het attributievraagstuk.

Staten vormen vooral een dreiging in de vorm van diefstal van informatie (digitale spionage), gericht op vertrouwelijke of concurrentiegevoelige informatie van overheden en bedrijven. De AIVD heeft het afgelopen jaar spionageaanvallen op Nederlandse civiele organisaties dan wel via de Nederlandse ICT-infrastructuur, vastgesteld vanuit onder meer China, Rusland, Iran en Syrië. De MIVD constateert dat de defensie-industrie een gewild doelwit is van cyberspionage en beschikt over aanwijzingen dat de cyberspionagedreiging zich eveneens richt op partijen met wie de defensie-industrie samenwerkt. Informatie verkregen door spionage op deze industrie dient het belang van staten. Daarnaast constateert de MIVD kwaadaardige phishingactiviteiten richting Nederlandse militaire vertegenwoordigingen in het buitenland.

Van beroepscriminelen blijft een grote dreiging uitgaan. De afgelopen periode uitte dat zich in financiële fraude en diefstal door aanpassing van onlinetransacties, veelal na diefstal en misbruik van financiële (inlog)gegevens (fraude met internetbankieren). Voorts maakten criminelen zich schuldig aan digitale inbraak om informatie te stelen voor criminele doeleinden of om te verkopen in het criminele circuit. Tot slot blijft de overname van ICT, bijvoorbeeld door malware-besmettingen, een onderwerp van zorg (zie het Pobelka-botnet), net als de toename van het plaatsen van ransomware om eindgebruikers te kunnen chanteren. Incidenten, waaronder het Pobelka-botnet, tonen dat botnets die zich richten op financiële transacties ook veel andere gevoelige gegevens buitmaken die een significant risico kunnen vormen. Bij Pobelka bleken gevoelige gegevens van bedrijven en overheden uit vitale sectoren, evenals veel persoonlijke gegevens van burgers, buitgemaakt te zijn.

Criminelen worden brutaler in hun handelen om daarmee veel geld te verdienen. Een voorbeeld hiervan is het automatisch downloa-

Actor	Intenties	Vaardigheden	Doelwitten
Staten	Geopolitieke of (interne) machtspositie verbeteren	Veel	Overheidsinstanties, non-gouvernementele organisaties, bedrijfsleven, wetenschappers, personen met relevante kennis, dissidenten en oppositionele groeperingen
Terroristen	Maatschappelijke veranderingen bewerkstelligen, bevolking ernstige vrees aanjagen of politieke besluitvorming beïnvloeden	Weinig tot gemiddeld	Doelwitten met hoge impact, ideologische symboolfunctie
Beroepscriminelen	Geldelijk gewin (direct of indirect)	Gemiddeld tot veel	Financiële producten en -dienstverlening, ICT en identiteit van burgers
Cybervandalen en Scriptkiddies	Aantonen van kwetsbaarheden Hacken omdat het kan Baldadigheid, zoeken van uitdaging	Weinig tot veel	Uiteenlopend
Hacktivisten	Ideologie	Gemiddeld	Uiteenlopend
Interne actoren	Wraak, geldelijk gewin of ideologisch (mogelijk 'aangestuurd')	Weinig tot veel	Huidige en/of voormalige werkomgeving
Cyberonderzoekers	Aantonen zwakheden, eigen profilering	Gemiddeld tot veel	Uiteenlopend
Private organisaties	Verkrijging waardevolle informatie	Weinig tot veel	Concurrenten, burgers, klanten
Burgers	n.v.t.	n.v.t.	n.v.t.

Tabel 2. Actoren waar dreiging van uitgaat, intenties, vaardigheden en doelwitten

den en tonen van kinderporno in ransomware om slachtoffers te dwingen geld te betalen. De politie constateert dat de wereld van cybercrime meer verweven raakt met de normale harde criminaliteit. Recente onderzoeken tonen aan dat burgers bijna even vaak slachtoffer zijn van 'hacken' als van fietsendiefstal.

Cybervandalen, scriptkiddies en hacktivisten vielen de afgelopen periode op door verstoring van de onlinedienstverlening van overheden en bedrijven en het publiceren van vertrouwelijke gegevens. Scriptkiddies en cybervandalen hebben daar in principe geen wezenlijk eigen belang bij, anders dan de kick. Over het algemeen worden de technische hulpmiddelen voor scriptkiddies beter en makkelijker te gebruiken. Daardoor kunnen zij grotere schade aanrichten. De cybervandaal heeft aan de andere kant veel kennis en kan daarbij substantiële schade aanrichten. Niet altijd is te herleiden hoe groot het aandeel van hacktivisten in opzettelijke verstoringen van ICT is. Aangenomen wordt dat zij betrokken zijn bij de vele DDoS-aanvallen en bij de (pogingen tot) publicatie van met digitale inbraak gestolen informatie.

Cyberaanvallen door terroristen tegen het internet of via het internet met ontwrichtende schade hebben zich voor zover bekend nog niet voorgedaan. Terroristen beschikken (nog) niet over voldoende vaardigheden en middelen voor maatschappijontwrichtende cyberaanvallen. «

3 Dreigingen: hulpmiddelen

In het vorige hoofdstuk is beschreven door welke actoren en waarom digitale aanvallen gepleegd worden. Voor het uitvoeren van aanvallen maken actoren gebruik van (technische) hulpmiddelen om kwetsbaarheden te misbruiken en/of te vergroten. Bij hulpmiddelen kan het zowel gaan om technische hulpmiddelen als om aanvalsmethoden.

3.1 Technische hulpmiddelen

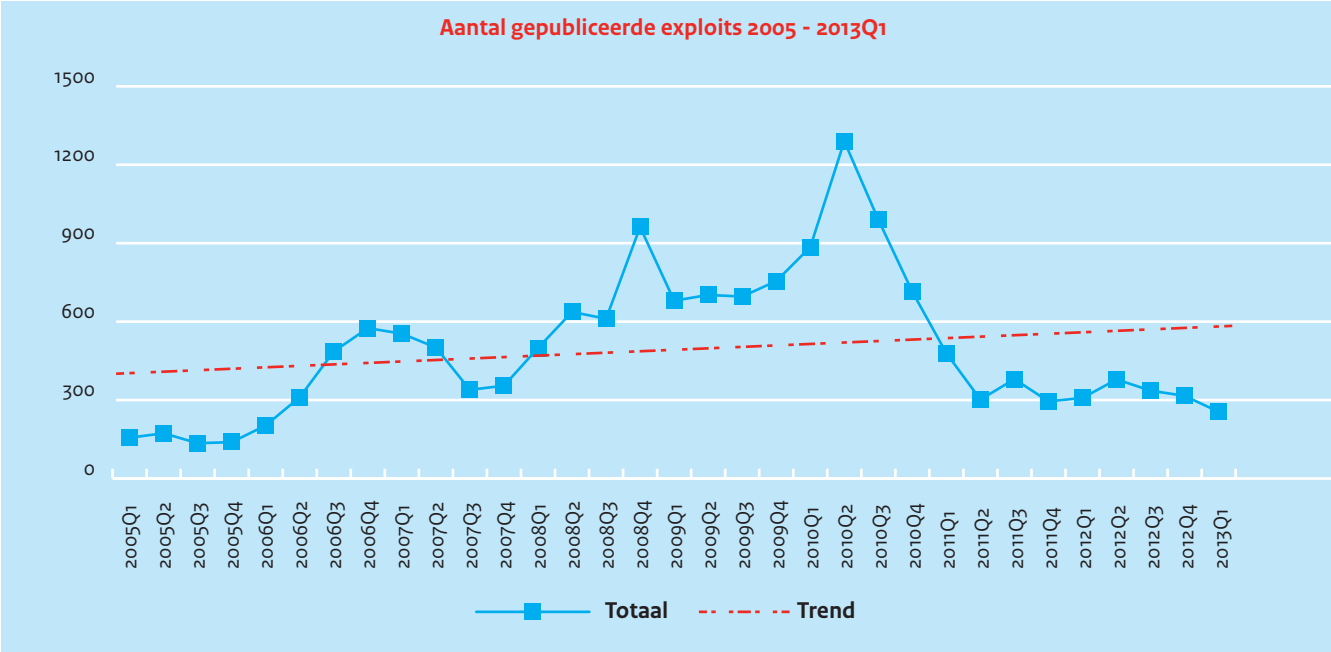
3.1.1 *Exploits*

Een exploit is een middel om misbruik te maken van een kwetsbaarheid. Het kan bestaan uit software, data of een opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software en/of hardware om ongewenst gedrag te veroorzaken. Het aantal gepubliceerde exploits is over de rapportageperiode afgenomen (zie figuur 1). De langetermijntrend is sinds 2005 licht stijgend. De exploits richten zich voornamelijk op webplatformen en Microsoft Windows. Een deel van de verklaring voor de afname van het aantal exploits ligt in maatregelen die in de ontwikkeling en het onderhoud van besturingsystemen zijn genomen. Het kan ook zijn dat leveranciers of andere ontdekkers exploits voor zichzelf houden of alleen delen met beveiligingsbedrijven.

De meest opvallende ontwikkeling op het gebied van exploitkits was het grote aantal Java-kwetsbaarheden dat wordt misbruikt.[37][38][39] Uit onderzoek van Websense blijkt dat 5 procent van de systemen met Java gebruikmaakt van de laatste versie. Omdat systemen vaak langdurig niet gepatcht worden, is de malware in exploitkits vaak erg effectief.

3.1.2 *Hulpmiddelen steeds eenvoudiger te gebruiken*

Net als vorig jaar zijn exploitkits steeds beter beschikbaar op meerdere ICT-platforms en neemt het gebruiksgemak toe. Een voorbeeld van een bekende exploitkit is Blackhole. Ook andere tools, bijvoorbeeld voor DDoS-aanvallen en SQL-injectie, winnen aan gebruiksgemak waardoor ook scriptkiddies zonder veel kennis van zaken steeds geavanceerdere aanvallen kunnen uitvoeren. DDoS-hulpmiddelen worden ook als dienst aangeboden.[40]



Figuur 1. Het aantal gepubliceerde exploits per kwartaal[36]

36 http://www.Exploit-db.com
37 http://community.websense.com/blogs/securitylabs/archive/2013/03/22/how-are-java-attacks-getting-through.aspx
38 http://community.websense.com/blogs/securitylabs/archive/2013/01/10/new-java-zero-day-used-in-exploit-kits.aspx
39 http://krebsonsecurity.com/2012/03/new-java-attack-rolled-into-exploit-packs/
40 http://krebsonsecurity.com/2012/08/booter-shells-turn-web-sites-into-weapons/

Tutorials op Youtube helpen de scriptkiddies op weg. Een voorbeeld is de SQL-injectietool Havij, waarmee met een paar muisklikken databases van onvoldoende beveiligde websites kunnen worden opgevraagd.[41]

Casus Humannet

In april 2012 komt via een reportage van het televisieprogramma *Zembla* aan het licht dat de beveiliging van de internetapplicatie Humannet, dat gebruikt wordt door verzuimbedrijven om klant-, medische- en verzuimgegevens te verwerken, niet op orde is. De applicatie biedt onder water nog steeds toegang tot een oude inlogpagina welke niet voorzien is van de laatste beveiligingspatches. Door middel van SQL-injectie blijkt de applicatie relatief eenvoudig te hacken. Gegevens van 300.000 patiënten zijn hierdoor gecompromitteerd. Dat de applicatie draait en dat de gegevens opgeslagen worden bij een extern bedrijf ontslaat de verwerker en de eigenaar van de gegevens, in dit geval de verzuimbedrijven, niet van de verantwoordelijkheid over de beveiliging van de gegevens.

3.1.3 *Hoeveelheid unieke malware neemt toe*

Het aantal unieke stuks malware nam de afgelopen jaren sterk toe. Het AV-TEST Institute registreert dagelijks meer dan 200.000 nieuwe exemplaren.[42] Deze aanhoudende stijging wordt vermoedelijk veroorzaakt door vele (automatisch gegenereerde) varianten van hetzelfde type malware en 'morphing' (gedaanteverandering) van malware. Gevolg is dat het analyseren en herkennen van de 'signatures' van malware technisch gezien onmogelijk wordt. Meerdere antivirusoplossingen kijken daarom ook naar gedragskenmerken om malware te detecteren.

3.1.4 *Security-oplossing aanvallen om beveiliging te omzeilen*

Een alternatieve aanpak is het gebruik van een lijst van betrouwbare software ('whitelisting') als hulpmiddel. Staat software (dus malware, zo is de gedachte) niet op de lijst, dan wordt deze niet geïnstalleerd. Begin 2013 werd echter bekend dat kwaadwillenden tijdelijk in staat waren de witte lijst van het softwarebeveiligingsbedrijf Bit9 te vervuilen, omdat zij illegaal toegang hadden gekregen tot een voorziening om softwaresamples digitaal te certificeren als bonafide.[43] Sommige van hun klanten herkenden deze samples dankzij andere antivirusoplossingen alsnog als malware.

3.1.5 *Ransomware*

Ransomware is een bestaand fenomeen, maar het afgelopen jaar werden gebruikers ook afgeperst met vermeende misdrijven als computercriminaliteit, echt of gefingeerd bezoek van pornosites en kinderporno. Door het toepassen van grove drukmiddelen als het tonen van politielogo's, kinderporno en de gebruiker zelf (via diens webcam), neemt de impact op het slachtoffer toe. Meer nog dan hacking, skimmen en fraude met internetbankieren raakt dit direct het veiligheidsgevoel van individuele burgers.

Ransomware kaapt functionaliteit van het besmette systeem, bijvoorbeeld door het versleutelen van bestanden of het blokkeren van de werking van het besturingssysteem. De malware eist een betaling van de gebruiker om de geblokkeerde functionaliteit te herstellen en zet de gebruiker doorgaans onder druk om geen aangifte te doen. Hierbij maken de criminelen gebruik van encryptie en virtueel digitaal geld om onder de radar te blijven. Er zijn inmiddels verschillende, vernieuwde versies van specifiek op Nederland gerichte 'politieransomware' (Reveton en Urausy)[44], die computers vergrendelen in naam van de politie.

3.1.6 *Mobiele malware*

De groei van de dreiging voor mobiele platforms zet door. Vooral Android is het doelwit.[46: Sophos 2012] De meest gebruikte aanvalsmethoden zijn: scams, spam en phishing.[1: Blue Coat 2013] De methodes zijn nog relatief simpel, maar klaarblijkelijk winstgevend. Gebruikers worden verleid om nep-antivirus en nep-apps te installeren (bijvoorbeeld Angry Birds Space of Instagram). Deze apps installeren malware op het apparaat of versturen ongewenste en ongeautoriseerde sms-berichten naar dure nummers.[50: TM 2013] Het verkrijgen van complete toegangsrechten tot de gegevens op een mobiel apparaat is een ander doel van malware (bijvoorbeeld GinMaster[45]).

Daarnaast is er net als vorig jaar malware, gericht op financiële dienstverlening, in diverse varianten actief: Zitmo, Spitmo, de mobiele varianten van Zeus en SpyEye. Deze richten zich op een breed scala aan informatie, waaronder binnenkomende sms-berichten, wachtwoorden en contactgegevens. Hoewel deze aanvalsmiddelen in opkomst zijn, is de hoeveelheid malware gericht op mobiele platformen op dit moment nog maar een fractie van de malware gericht op reguliere computers.

41 http://www.troyhunt.com/2012/10/hacking-is-childs-play-sql-injection.html
42 www.AVtest.org, gegevens opgehaald op 14 mei 2013
43 http://krebsonsecurity.com/2013/02/security-firm-bit9-hacked-used-to-spread-malware/
44 https://www.security.nl/artikel/45214/1/Nederlands_politievirus_dreigt_met_niet_bestaande_wet.html, https://www.security.nl/artikel/45117/1/Nederlands_politievirus_krijgt_make-over_%2Aupdate%2A.html
45 http://malwarealert.org/trojanandroidginmaster-a/

3.1.7 Botnets

Botnets zijn netwerken van samenwerkende apparaten, meestal privé- of bedrijfscomputers, de zogeheten 'bots', die met dezelfde malware zijn besmet. Criminelen kunnen een botnet centraal aansturen om de computerkracht voor eigen doeleinden in te zetten. Botnets worden veelal ingezet voor het versturen van spam en het uitvoeren van DDoS-aanvallen.

Het landschap aan malware waarmee botnets kunnen worden gemaakt, wordt momenteel gedomineerd door een aantal malwarefamilies. Het meest in het oog springend is de familie van ZeuS. Een hiervan afgeleide[46] maar opzichzelfstaande groep zijn de botnets gebaseerd op de Citadel-malware, zoals Pobelka en Plitfi. De Citadel-botnets hebben in Nederland media-aandacht genoten naar aanleiding van incidenten rondom Dorifel en Pobelka. Botnets staan bekend om hun gebruik door criminelen om financiële transacties te manipuleren. Maar het Pobelka-botnet heeft aangetoond dat botnets die zich richten op financiële transacties ook veel andere gegevens buitmaken die een significant risico kunnen vormen. Bij Pobelka bleken gevoelige gegevens van bedrijven en overheden uit vitale sectoren, alsmede veel persoonlijke gegevens van burgers, buitgemaakt te zijn.

3.1.8 Apparaten van Apple in beeld voor botnets

Het toegenomen privé- en zakelijk gebruik van iMacs, Macbooks, iPhones en iPads maakt dit platform tot een steeds aantrekkelijker doelwit. Net als bij mobiel zijn het ook de platformonafhankelijke methoden die het eerst opduiken (spam, scam, phishing, social engineering). Vorig jaar werden meerdere varianten van nep-antivirussoftware aangetroffen, zoals MacDefender en MacGuard.[47] In april 2012 is een eerste, groot botnet ontdekt bestaand uit computers van Apple met het OS X-besturingssysteem. Uit een analyse van de Morcut/Crisis-malware die zich richt op OS X, blijkt een grote kennis van OS X.[46: Sophos 2012] Er is echter nog geen sprake van een grootschalige groei van malware specifiek gericht op het OS X-platform.

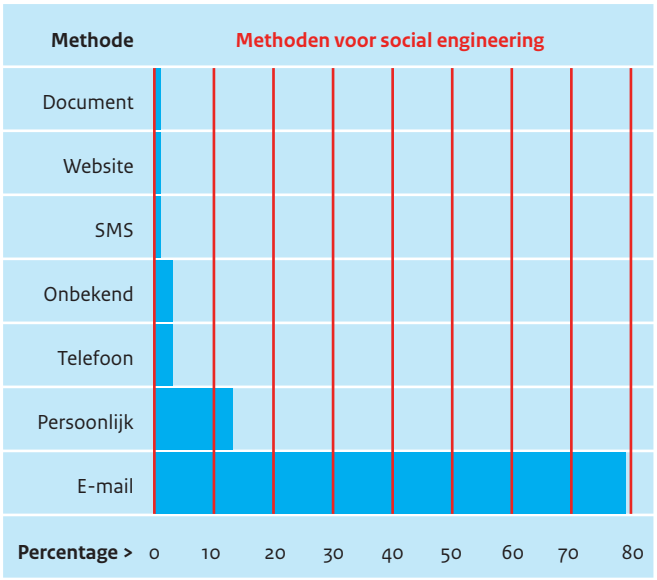
3.1.9 Kwetsbare DNS-servers faciliteren specifieke DDoS-vorm

Bij DDoS-aanvallen wordt soms gebruikgemaakt van Domain Name Server (DNS) amplificatie (versterking). De DNS-amplificatie-aanval maakt er gebruik van dat een korte vraag een erg lang antwoord kan genereren.[48] Bij dit soort DDoS-aanvallen wordt vaak gebruikgemaakt van systemen die onnodig onveilig geconfigureerd zijn. Door een groot aantal DNS-servers deze lange antwoorden naar het doelwit te laten sturen, is het gevolg dat het doelwit niet of slecht bereikbaar is.

3.2 Werkwijze en organisatie

3.2.1 Werkwijze cybercriminelen brutaal en meer gericht op de mens

Er is een lichte verschuiving in de aandacht van cybercriminelen van kwetsbaarheden in ICT naar een andere zwakke schakel: de mens. Via verschillende wegen kunnen cybercriminelen met social engineering hun slachtoffers bewegen tot het verstrekken van inloggegevens of het installeren van malware. Het afgelopen jaar was een aantal gevallen van social engineering te zien met een grote brutaliteit. Opvallend was de scamoperatie, waarbij zogenaamde medewerkers van de Microsoft helpdesk mensen opbelden en hen trachtten in (Indiaas) Engels en Nederlands te verleiden software te installeren waarmee de scammers de computer konden overnemen.[49] De oplichters proberen hun slachtoffer eerst te overtuigen van de ernst van de situatie. Vervolgens bieden ze een oplossing aan waarvoor betaald moet worden. Deze social-engineeringoperatie heeft geruime tijd geduurd. De operatie is opvallend, omdat het doorgaans e-mail is waarmee getracht wordt gegevens of acties gedaan te krijgen (phishing).



Figuur 2. Verdeling gebruikte methoden voor social engineering (wereldwijd) [54: Verizon 2012]

Steeds vaker maken criminelen gebruik van middelen om relatief anoniem te surfen, zoals Tor, en om te betalen zonder identificatie, zoals met bitcoins (zie kader).

46 https://www.botnets.fr/index.php/Citadel_ZeuS_bot
47 http://www.computerworld.com/s/article/9217061/Newest_MacDefender_scareware_installs_without_a_password
48 http://www.us-cert.gov/ncas/alerts/TA13-088A Zie http://dnssec.nl/cases/dns-amplificatie-aanvallen-straks-niet-meer-te-stoppen-zonder-bcp-38.html
49 http://www.waarschuwingsdienst.nl/Risicos/Oplichting/nep-microsoftmedewerker.html, https://www.security.nl/artikel/41862/1/Politie_waarschuwt_voor_Microsoft_telefoonscam.html

Bitcoin
Door de grote koersschommelingen heeft de bitcoin in de eerste maanden van 2013 veel aandacht gekregen. De bitcoin is een gedecentraliseerde peer-to-peer (P2P), virtuele munteenheid. De koers van de bitcoin liep van rond de 10 euro aan het eind van 2012 op naar bijna 200 euro in april 2013.[50] Individuen kunnen zelf bitcoins genereren en verhandelen waarbij er enige mate van anonimiteit is. De FBI verwacht dat op de korte termijn cybercriminelen bitcoins zullen gebruiken naast de al bestaande meer traditionele en andere virtuele munteenheden zoals WebMoney.[51] Activiteiten waarbij bitcoins kunnen worden gebruikt, zijn betalingen, witwassen, diefstal van bitcoins van individuen en bitcoindiensten of het genereren van bitcoins met botnets. Omdat bitcoins geen centrale autoriteit kennen, maakt dit het voor opsporingsdiensten moeilijker om verdachte activiteiten te detecteren, gebruikers te identificeren en transactiegegevens te verkijgen.

3.2.2 De cloud als hulpmiddel

Het WODC [57: WODC 2012] heeft onderzoek gedaan naar de gevolgen van cloudcomputing voor de Nederlandse opsporing en vervolging. Dit onderzoek laat zien dat er juridische knelpunten zijn over de status van de cloudaanbieder, de aard van gegevens en territoriale grenzen, bij het gebruik van clouddiensten door verdachten. Dat laatste is niet nieuw, maar krijgt een extra dimensie wanneer databestanden in een cloud – opgeknipt over meerdere locaties – zijn opgeslagen. Er is dan sprake van 'verlies van locatie', er is niet één plek waarop de data staat en niet één land waar een rechtshulpverzoek aan kan worden gedaan. Bij vervolging is er tenslotte nog de uitdaging het bewijs technisch rond te krijgen: kun je aantonen dat wat uit de cloud komt, ook datgene is wat erin is opgeslagen?

3.2.3 Handel in exploits en kennis over kwetsbaarheden

Omdat staten op zoek zijn naar nieuwe exploits voor bijvoorbeeld spionage, ontstaat er een markt.[52] Digitale wapenhandel bestaat al enkele jaren, zeker in de Verenigde Staten waar grote defensiebedrijven en specialisten activiteiten op dit gebied ontplooien. Ook in Europa en Azië verschijnen handelaren in exploits, exploitkits en kennis van kwetsbaarheden. Bepaalde partijen verhandelen deze technologie ook aan landen met repressieve regimes, voor surveillance op activisten en journalisten.[53]

3.2.4 Aanpassing en hergebruik van hulpmiddelen

Eenmaal gebruikte en al dan niet gepubliceerde hulpmiddelen kunnen door anderen worden aangepast en hergebruikt. De afgelopen jaren zijn zeer geavanceerde cyberaanvallen uitgevoerd tegen onder andere Iraanse nucleaire installaties (Stuxnet) en ter verkrijging van allerlei gevoelige informatie (Flame). Breed wordt verondersteld dat hier statelijke actoren achter zitten en in media-berichten wordt gespeculeerd dat het hier gaat om Israël en/of de Verenigde Staten.[54] Deskundigen hebben de gebruikte tools grondig geanalyseerd en de resultaten gepubliceerd.[55] Er is hierbij al gewezen op het gevaar van reverse engineeren van de aanval en de tools. Hiermee kunnen anderen delen van deze geavanceerde hulpmiddelen aanpassen en hergebruiken voor een nieuwe aanval. Als gevolg hiervan is bijvoorbeeld een deel van de werking van Stuxnet opnieuw gecodeerd en op het internet beschikbaar. Een ander voorbeeld is het hergebruik van technieken van de zogenaamde Wiper-malware, die eerder was ingezet tegen Iraanse oliemaatschappijen in de aanval op Saudia Aramco met Shamoon.[56]

3.3 Conclusie

Voor het uitvoeren van aanvallen maken actoren gebruik van (technische) hulpmiddelen om kwetsbaarheden te misbruiken en/of te vergroten. Actoren gebruiken vooral de talrijke zelf ontwikkelde of beschikbare exploits, botnets, (spear)phishing en (mobiele) malware. Staten zijn in staat om geavanceerde hulpmiddelen te ontwikkelen en te gebruiken, terwijl cybercriminelen vooral bestaande hulpmiddelen doorontwikkelen. Cybercrime professionaliseert verder in het bieden van diensten voor het huren van hulpmiddelen voor cyberaanvallen en het wegsluizen van geld. Deze criminele cyberdienstensector wordt ook wel 'cybercrime-as-a-service' genoemd. De verhuur van botnets voor DDoS-aanvallen is hier een voorbeeld van.

Bij de technische hulpmiddelen worden exploitkits, malware en botnets het meest toegepast. De steeds makkelijker te gebruiken exploitkits maken het eenvoudiger om het stijgend aantal technische kwetsbaarheden te misbruiken. Ook tools voor DDoS-aanvallen zijn laagdrempelig beschikbaar. Mutaties van malware zorgen ervoor dat er zoveel varianten van malware in omloop komen, dat antivirusprogramma's deze niet allemaal kunnen detecteren. Botnets blijven een belangrijk hulpmiddel voor staten en cybercriminelen dat voor de eigenaren van misbruikte ICT-middelen veelal onder de radar bleef. Met de stijging van het gebruik van mobiele apparatuur, neemt ook de stijging van mobiele malware toe.

Aan de menskant zien we dat criminelen steeds brutaler worden. Phishing blijft een succesvolle methode om gebruikers te verleiden en gebruikers zijn steeds vaker het slachtoffer van ransomware, een specifieke vorm van malware waarmee de computer van de gebruiker wordt gegijzeld. Ook zijn afgelopen jaar telefonische phishingacties nadrukkelijk in beeld geweest. «

50 http://www.bitcoinspot.nl/bitcoin-wisselkoers-euro.html
51 FBI, Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity, 2012.
52 http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510
53 Zie onder andere Ben Wagner, Exporting Censorship And Surveillance Technology, 2012 en http://www.dw.de/eu-bans-export-of-internet-surveillance-gear-to-iran/a-15829335
54 Uitgebreid gereconstrueerd in David E. Sanger, Confront and Conceal, 2012.
55 W.o. Ralph Langner, Symantec en Kaspersky.
56 http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work

4 Weerbaarheid: kwetsbaarheden

In de vorige hoofdstukken is ingegaan op belangen en de verschillende aspecten van dreigingen. Het derde aspect van de driehoek vanwaaruit we cybersecurity benaderen is de weerbaarheid van individuen, organisaties en de samenleving. Deze weerbaarheid bestaat enerzijds uit (het afwezig zijn van) de kwetsbaarheid van de te verdedigen belangen en anderzijds uit maatregelen om de kwetsbaarheid te verminderen. In dit hoofdstuk zijn ontwikkelingen op het gebied van kwetsbaarheden beschreven. Kwetsbaarheden waarin zich geen noemenswaardige verschuivingen hebben voorgedaan, worden niet of kort behandeld.

Een 'kwetsbaarheid' is een eigenschap van ICT, organisaties of gebruikers die bij misbruik door een actor kan leiden tot 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. Een kwetsbaarheid is ook een eigenschap van ICT die als gevolg van een natuurlijke of technische gebeurtenis of menselijk falen kan leiden tot de genoemde gevolgen. 'Eigenschap van ICT' moet in dit kader ruim worden opgevat. Het gaat ook om aan ICT gerelateerde kwetsbaarheden bij de mens en binnen of tussen organisaties.

4.1 Kwetsbaarheden veroorzaakt door menselijke en organisatorische factoren

4.1.1 *Grote verantwoordelijkheid ligt bij eindgebruiker*

Eindgebruikers worden steeds vaker geconfronteerd met kwetsbaarheden in ICT-middelen waar zij beperkte invloed op hebben.[57] Dit is mede het gevolg van het groeiend aantal apparaten in huis dat een netwerkverbinding heeft. Het gaat daarbij om randapparatuur zoals modems, routers, printers, scanners, televisies, webcams en apparatuur voor netwerkopslag. De standaardbeveiliging van deze apparatuur schiet vaak tekort of het is onduidelijk hoe een apparaat veilig ingesteld moet worden. Hierdoor ligt er een grote last en verantwoordelijkheid bij de eindgebruiker. Het ontbreekt de eindgebruiker veelal aan de technische kennis die vereist is om de nodige (complexe) beveiligingsmaatregelen te treffen.

Daarnaast wordt ook door een laag beveiligingsbewustzijn of simpel gemakzucht apparatuur onjuist ingesteld door gebruikers, met als gevolg dat privégegevens via internet door niet-geautoriseerden zijn te benaderen en te misbruiken. Naast de noodzaak dat apparatuur en software standaard veiliger worden zodat gebruikers beter beschermd zijn, heeft de eindgebruiker de verantwoordelijkheid voor basale beveiligingsmaatregelen waar hij wel invloed op kan hebben, zoals tijdig updaten, goede wachtwoorden en gebruiken van antivirusoplossingen voor computers.

Op 8 december 2012 meldt het KRO-programma *Reporter* in haar uitzending dat door een groot lek in computerrandapparatuur de vertrouwelijke en privacy-gevoelige gegevens van tienduizenden particulieren en bedrijven via internet openlijk toegankelijk zijn. Aanleiding is dat steeds meer verschillende apparaten aan een thuis- of kantoornetwerk worden gekoppeld. Door onjuiste configuratie ontstaat het risico dat deze apparaten direct vanaf internet te benaderen zijn. Kwaadwillenden kunnen zo de informatie die is opgeslagen in deze apparaten opvragen of veranderen. Ook is het apparaat, afhankelijk van het type, mogelijk op afstand te bedienen. Direct uit de doos zijn dergelijke apparaten meestal niet zo ingesteld dat de juiste veiligheidsopties aan staan en het ontbreekt bij veel gebruikers aan de 'technische' kennis om deze apparaten zo in te stellen dat hun informatie veilig is.

Zie het factsheet 'Beveilig apparaten gekoppeld aan het internet' van het NCSC voor meer informatie.[34: NCSC 2012-2]

In het informatica-onderwijs van het voortgezet onderwijs ligt de focus op het werken met producten van een specifieke leverancier en wordt weinig tot niets geleerd over informatiebeveiliging en over concepten van hoe computers werken. Het de jeugd leren om op een veilige manier met informatievoorziening om te gaan, is een voorwaarde om op langere termijn een stap te kunnen maken in veiliger gedrag en betere systemen.

4.1.2 *Consumerization: de gebruiker aan het roer*

Consumerization is de trend dat nieuwe technologieën eerst doorbreken in de consumentenmarkt en vandaaruit doordringen in organisaties. Smartphones en tablets zijn volwaardige computers die ook nog eens vaak of permanent online zijn. Mede vanwege het gemak schakelen gebruikers snel laagdrempelige clouddiensten in en downloaden zij eenvoudig nieuwe toepassingen ('apps'), zowel voor privé- als zakelijk gebruik. Consumenten/werknemers en hun leidinggevenden zijn zich onvoldoende bewust van de risico's die zij nemen en stellen niet of nauwelijks beveiligingseisen aan leveranciers. Zij richten zich namelijk meer op de features en minder op de veiligheid.

57 Een uitgebreide toelichting hierin is beschreven in de verdiepingskaternen.

Consumerization brengt verder met zich mee dat privé- en zakelijk gebruik door elkaar gaan lopen, terwijl zij elkaar niet altijd verdragen. Zakelijke informatie komt buiten beheer van de organisatie en kan in een privéomgeving uitlekken en privé-informatie kan toegankelijk worden voor organisaties. Bovendien kan zakelijke informatie online worden geplaatst in onbekende omgevingen (cloud), waarvan de beveiliging onbekend en mogelijk onvoldoende is. Hierdoor ontstaat het risico van het lekken van gegevens. Consumerization levert dus kwetsbaarheden op, maar er kan nog niet gezegd worden dat het aantal incidenten dat rechtstreeks toe te wijzen is aan consumerization sterk toeneemt of omvangrijk is.

4.1.3 Onvoldoende inzicht in dreigingen en incidenten

Cybersecurity vereist een actueel en breed zicht op nieuwe ontwikkelingen, kwetsbaarheden, aanvalsmethoden en verdedigingsmechanismen. Voor organisaties vereist dit een dusdanig inzicht in de eigen ICT-omgeving dat aanvallen op of penetraties van die omgeving snel worden opgemerkt. Naast inzicht en detectie vereist cybersecurity ook de capaciteit om snel en adequaat te kunnen reageren op dreigingen en incidenten: cybersecurity goed inrichten vereist ook een *ability to act*. De praktijk wijst immers uit dat incidenten nooit volledig te voorkomen zijn en het is derhalve van belang goed voorbereid te zijn.

Op dit moment ontbeert het nog veel organisaties aan de juiste kennis, detectiemiddelen en het vermogen om incidenten af te handelen. Incidenten zoals het Pobelka-botnet laten zien dat bij veel organisaties het netwerk is binnengedrongen en computers zijn geïnfecteerd, maar dat dat vaak maandenlang onopgemerkt blijft. Organisaties richten hun informatiebeveiliging in veel gevallen in op basis van standaarden zoals ISO2700x, maar dat leidt tot relatief statisch ingerichte informatiebeveiliging. De moderne dreigingen vereisen dat zij ook hun inzicht en hun vermogen om te handelen op niveau brengen.

4.1.4 Efficiency en klantvriendelijkheid zetten privacy onder druk

Het College Bescherming Persoonsgegevens (CBP) constateert in zijn terugblik op 2012 dat de overheid in toenemende mate persoonsgegevens verzamelt en aan elkaar koppelt.[2: CBP 2013] Omdat burgers in veel gevallen verplicht zijn om persoonsgegevens aan de overheid af te staan, is het essentieel dat burgers erop kunnen vertrouwen dat met die gegevens zorgvuldig wordt omgegaan, conform de wet. Volgens het CBP blijkt echter, dat de overheid – aangemoedigd door technologische ontwikkelingen en de wens om efficiënt en klantvriendelijk te zijn – steeds meer persoonsgegevens aan elkaar koppelt om deze gegevens vervolgens te gebruiken voor geheel andere doeleinden dan waarvoor zij oorspronkelijk waren bedoeld. Hetzelfde kan overigens ook worden gezegd van bedrijven die grootschalig klantgegevens verwerven en opslaan.

4.1.5 Kwetsbaarheid bij gebruik clouddiensten

Cloudcomputing heeft voordelen maar brengt ook risico's met zich mee, onder meer omdat de toegang niet altijd even goed is beveiligd en cloudleveranciers zich rechten voor gebruik van de gegevens toe-eigenen in telkens veranderende algemene voorwaarden. Wat privacy betreft lopen de Amerikaanse en Europese regels uiteen, maar de EU beschouwt Amerikaanse clouddienstverleners als voldoende veilig mits ze als 'safe harbor' zijn aangemerkt en beschikken over certificering.

Afnemers kunnen desondanks te maken krijgen met regelgeving uit het buitenland die mogelijk strijdig is met de te beschermen belangen (en eventueel lokale regelgeving), zoals privacy van klanten/patiënten/burgers, intellectueel eigendom en continuïteit van de bedrijfsvoering. Met de Patriot Act als symbool, krijgt dit vraagstuk in toenemende mate aandacht van politiek en wetenschap, en van organisaties die een (Amerikaanse) clouddienst overwegen aan te schaffen.

Bescherming medische gegevens

In 2012 is uit een onderzoek in opdracht van het CBP gebleken dat een groot deel van de ziekenhuizen onvoldoende beveiligingsmaatregelen heeft genomen om kwetsbaarheden weg te nemen ten aanzien van vertrouwelijkheid, integriteit en beschikbaarheid van patiënt- en medische gegevens.
In september 2012 bijvoorbeeld heeft het een ziekenhuis berispt[58] en opgedragen verbeteringen aan te brengen naar aanleiding van audits waaruit bleek dat identificatie, authenticatie en autorisatie onvoldoende is geregeld voor de systemen met gedigitaliseerde patiëntendossiers. Medewerkers hadden hierdoor meer toegang tot de gegevens dan zij vanuit hun functie nodig zouden hebben.

Volgens de Special Interest Group Informatiebeveiliging Universitaire Ziekenhuizen zijn er ook aan de patiëntenzijde ontwikkelingen die bijdragen aan de flexibiliteit en efficiëntie van persoonlijke zorgverlening, maar anderzijds zijn er ook weer risico's op ongewilde en onbedoelde ontsluiting van medische gegevens. Er worden apps aangeboden via welke een patiënt zijn persoonlijke en medische gegevens kan invoeren en delen met een zorgaanbieder. Deze apps worden echter aangeboden door derde partijen en het blijft onduidelijk waar de gegevens worden opgeslagen en welk beveiligingsregime ervoor gehanteerd wordt.

58 www.cbpweb.nl/pages/med_20120920-beveiliging-medische-gegevens-rpz-ziekenhuis.aspx

Vele landen kennen vergelijkbare regelgeving aan de Patriot Act en de daaruit voortvloeiende bevoegdheden kunnen niet worden uitgesloten door contractuele waarborgen of Nederlandse wetgeving. Volgens onderzoek van de Universiteit van Amsterdam zal door de overgang naar clouddiensten sprake zijn van een autonomievermindering van de organisaties over de omgang met bevragingen door buitenlandse overheden.[53: UvA 2012]

Het is bekend dat clouddiensten worden gebruikt voor opslag en uitwisseling van illegaal materiaal en voor het plegen van botnet-aanvallen.[59] Cloudcomputing brengt uitdagingen voor de opsporing en vervolging van misdaad met zich mee.[57: WODC 2012]

4.1.6 Sociale media blijven een onbedoelde bron van informatie

Sociale media staan in grote belangstelling bij kwaadwillenden vanwege de persoonlijke informatie die hier beschikbaar is, het onderlinge vertrouwen tussen deelnemers van een sociaal netwerk en het grote aantal gebruikers dat hierop is geabonneerd. Kwaadwillenden zijn altijd op zoek naar informatie om beter gepersonaliseerde e-mails te creëren en deze via spam en phishing persoonlijk aan hun slachtoffers te richten. Dergelijke gerichte aanvallen bieden vaak meer kans van slagen. Door het gebruik van sociale media kunnen bijvoorbeeld bedrijfsgegevens, onderzoeksresultaten of klantinformatie uitlekken, gevoelige informatie over medewerkers worden prijsgegeven of kan de organisatie onjuist en negatief worden gerepresenteerd. De organisatie kan hierdoor (reputatie- of financiële) schade ondervinden of kwetsbaarder worden voor cyberaanvallen. Daarnaast kunnen sociale media de veiligheid van personen ondermijnen (sabotage en chantage).

4.1.7 Zwakke wachtwoorden blijven een kwetsbaarheid

Uit onderzoek naar het veiligheidsbewustzijn van consumenten blijkt dat de kwaliteit van wachtwoorden nog te wensen overlaat.[27: Motivaction 2012] Minder dan de helft geeft aan dat zijn wachtwoord bestaat uit meer dan tien karakters of speciale tekens bevat. Het bewustzijn van het belang van sterke wachtwoorden is nog lager. Verder is het regelmatig wijzigen van belangrijke wachtwoorden bij veel Nederlandse consumenten nog geen automatisme.[12: EC 2013-2] De meesten wijzigen hun wachtwoorden minder vaak dan eens per drie maanden of nooit. Slechts 38 procent van de Nederlanders gebruikt verschillende wachtwoorden voor verschillende onlinediensten.[12: EC 2013-2] Ten opzichte van inwoners van andere EU-landen scoort Nederland hiermee dan nog relatief goed.

Aan de kant van de beheerder kan het ook verkeerd gaan door zwakke wachtwoorden toe te staan, wachtwoorden onversleuteld op te slaan of onvoldoende veilige methoden voor de versleuteling van wachtwoorden te gebruiken.

4.1.8 Einde ondersteuning Windows-XP risico voor organisaties en eindgebruikers

Microsoft zal op 8 april 2014 de ondersteuning voor Windows XP beëindigen. Daarmee worden er ook geen beveiligingsupdates meer uitgebracht. Dit zal risico's opleveren voor de beveiliging en daarmee de betrouwbaarheid en beschikbaarheid van de systemen die hierop draaien. Het is verstandig om over te stappen naar een systeem dat wel ondersteund wordt. In Nederland gebruikt nog ongeveer 40 procent van de zakelijke gebruikers Windows XP.[60] Omdat sommige programmatuur en randapparatuur niet meer werken met een nieuwe versie, kan het overstappen lang duren.

4.2 Technische kwetsbaarheden

4.2.1 Meer kwetsbaarheden en meer kans op keteneffecten door hyperconnectiviteit

Met hyperconnectiviteit wordt een tweetal trends bedoeld, enerzijds de trend om steeds meer mobiele apparatuur (zoals smartphones en tablets) te gebruiken en hiermee permanent via het internet verbonden te zijn; anderzijds de trend om steeds meer (consumenten)producten als auto's, koffieautomaten en koelkasten van rekenkracht en netwerkmogelijkheden te voorzien. Deze toenemende verbondenheid creëert nieuwe mogelijkheden om aan te vallen.

Beveiliging is op deze veelheid aan nieuwe op het netwerk aan te sluiten apparaten niet altijd een aandachtspunt, waardoor aanvallers misbruik kunnen blijven maken van bestaande kwetsbaarheden in protocollen, applicaties en besturingssystemen. Het maakt niet uit of die draaien op een smartphone, een tablet, een computer of zelfs in een auto. De koppeling met de fysieke wereld zorgt er echter wel voor dat de gevolgen anders zijn. Denk bijvoorbeeld aan het overnemen van de functies in een auto die van belang zijn voor de besturing van de auto en veiligheid van de inzittenden.[61]

4.2.2 Mobiel opgeslagen data kwetsbaar

Gegevens zijn mobiel geworden en dat leidt tot kwetsbaarheden. Verlies of diefstal van een apparaat maakt de opgeslagen gegevens mogelijk toegankelijk voor de vinder. Mobiele apparatuur kan ook besmet worden met kwaadaardige software die gegevens afluistert of het apparaat manipuleert.[46: Sophos 2012] Smartphones of tablets bevatten vaak veel persoonlijke gegevens van de gebruikers, zoals e-mail, contacten, agenda's, locatiegegevens, creditcardgegevens, foto's, video's en login-gegevens. Het verwerken van deze gegevens op smartphones en tablets brengt risico's met zich mee voor bedrijven en de persoonlijke levenssfeer van de gebruikers als de privacywetgeving niet wordt nageleefd door de leverancier van

59 http://news.cnet.com/8301-1009_3-10413951-83.html

60 http://www.nu.nl/gadgets/3393144/27-miljoen-nederlanders-gebruiken-nog-windows-xp.html

61 Chris Bryant, (22 Maart 2013) Cars could be the next victim of cyber attacks, Financial Times, The Financial Times Limited 2013.

apps.[62] Onderzoek naar 13.500 gratis apps in de Google Play Market wees uit dat 8 procent van deze apps kwetsbaar waren voor man-in-the-middle aanvallen. Bij 41 van de 100 handmatig onderzochte apps waren onderzoekers daardoor in staat om inloggegevens voor creditcards, Paypal, bankrekeningen, sociale media, e-mailaccounts en dergelijke te vergaren.[63]

4.2.3 Kwetsbaarheden Industriële Controlesystemen meer in beeld

Deze rapportageperiode is wederom een aantal nieuwe kwetsbaarheden op het gebied van industriële controlesystemen (ICS, waaronder SCADA) bekend geworden. Hoewel grote incidenten zijn uitgebleven, kan niet worden geconstateerd dat de dreiging is afgenomen. Omdat incidenten uitblijven, is het besef over de ernst van de situatie onvoldoende en ondernemen veel organisaties te weinig actie. Hierbij moet worden opgemerkt dat met name grote operators van vitale infrastructuren en enkele (grote) leveranciers van ICS/SCADA-toepassingen wel degelijk de ernst van de situatie beseffen en overeenkomstig handelen.

Doordat bij het ontwerpen, implementeren en beheren van ICS-omgevingen security niet altijd de aandacht krijgt die het verdient, lopen dergelijke omgevingen (onnodig) risico. De toenemende wens tot informatie-uitwisseling tussen de proces- en kantooromgeving legt extra druk op security. Ook de behoefte voor toegang op afstand, om bijvoorbeeld onderhoud te kunnen plegen, draagt hieraan bij. Ook het gebruik van internetverbindingen, zonder daarbij voldoende securitymaatregelen te treffen, leidt tot een vergroot risico. Vooral kleine bedrijven, lagere overheden en particulieren beseffen zelden dat hun systemen direct via internet bereikbaar blijken te zijn. Andere veelvoorkomende securityproblemen in ICS-omgevingen komen voort uit het toenemende gebruik van generieke ICT-middelen en onvoldoende awareness en kennis bij het personeel.

Defensie en ICS

In de wapen-, communicatie- en sensorsystemen van defensie zijn zowel digitale netwerken als aan SCADA verwante besturingscomputers aanwezig. Deze digitale systemen zijn essentieel voor het functioneren van het betreffende wapen-, communicatie- of sensorsysteem. De kwetsbaarheden zoals die in civiele systemen worden onderkend, zijn in principe ook aanwezig in defensiesystemen. Vanwege de specifieke architectuur, gebruikte software en het feit dat deze systemen geen directe verbinding met het internet hebben, is beïnvloeding van buitenaf complexer waardoor het risico voor uitval relatief lager is. Daarnaast zijn veel systemen redundant uitgevoerd. Defensie besteedt met nadruk aandacht aan de bescherming van wapen-, communicatie- en sensorsystemen. In de CERT-organisatie van defensie (DefCERT) zijn hiervoor specifieke functies gecreëerd.

4.2.4 SSL kwetsbaar of niet veilig geconfigureerd

Het NCSC heeft in de afgelopen periode onderzocht hoeveel websites met SSL zijn beveiligd. In meer dan 40 procent van de gevallen blijkt dat onveilige versleutelingsalgoritmen worden gebruikt waardoor datacommunicatie mogelijk afgeluisterd of gemanipuleerd kan worden. Ook verouderde versies van SSL, versie 2, worden in bijna 18 procent van de gevallen nog ondersteund. Deze kwetsbaarheid wordt versterkt door gebrekkig inzicht van gebruikers in de mate waarin hun internetactiviteit beschermd is. Uit onderzoek blijkt dat de helft van de ondervraagde gebruikers niet in staat was om correct te bepalen of hun browsersessie goed beveiligd was met SSL of niet.[64]

Ook is opnieuw gebleken dat het SSL-protocol gevoelig is voor aanvallen, door kwetsbaarheden in de implementatie van het protocol of de encryptie. Zo werden aanvallen op SSL getoond met welluidende namen als CRIME[65] en Lucky13[66] en een aanval op RC4-encryptie in TLS[67]. Doordat TLS/SSL een fundamenteel onderdeel is van de veiligheid van internetverbindingen vormen deze kwetsbaarheden een risico voor de vertrouwelijkheid van webverbindingen.

4.2.5 Trendbreuk: stijging aantal kwetsbaarheden in software

Op basis van een analyse van de Amerikaanse National Vulnerability Database (NVD) en de beveiligingsadviezen van het Nederlandse NCSC is het aantal kwetsbaarheden in software in kaart gebracht (zie figuur 3). In het voorgaande Cybersecuritybeeld Nederland is geconcludeerd dat het aantal geregistreerde kwetsbaarheden op jaarbasis al een aantal jaren afnam. Deze neerwaartse trend is doorbroken en het aantal kwetsbaarheden is in 2012 weer fors toegenomen. Het aantal geregistreerde kwetsbaarheden steeg naar 5.300 ten opzichte van ongeveer 4.000 een jaar eerder (+27 procent).[68] Er is geen specifiek product of specifieke leverancier aanwijsbaar als oorzaak voor deze stijging.

62 Bron: CBP – 'Europese privacytoezichthouders publiceren opinie over mobiele apps - Gebruik persoonsgegevens door app alleen toegestaan met toestemming gebruiker', d.d. 14-3-2013, http://www.cbpweb.nl/Pages/pb_20130314-wp29-opinie-mobiele-apps.aspx

63 S. Fahl e.a., Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security, Leibniz University of Hannover, 2012.

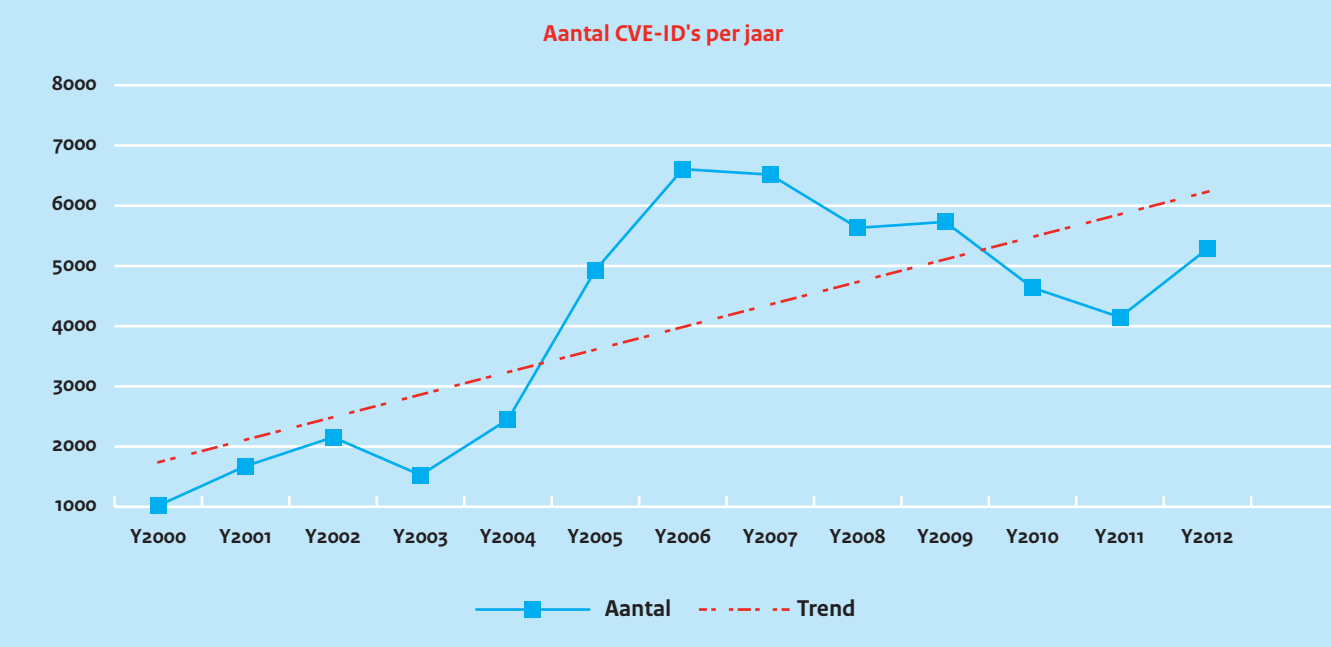
64 S. Fahl e.a., Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security, Leibniz University of Hannover, 2012.

65 Zie http://arstechnica.com/security/2012/09/crime-hijacks-https-sessions/

66 Zie http://www.isg.rhul.ac.uk/tls/Lucky13.html

67 Zie http://www.isg.rhul.ac.uk/tls/

68 Bron: National Vulnerability Database (NVD) van het Amerikaanse National Institute of Standards and Technology (NIST).

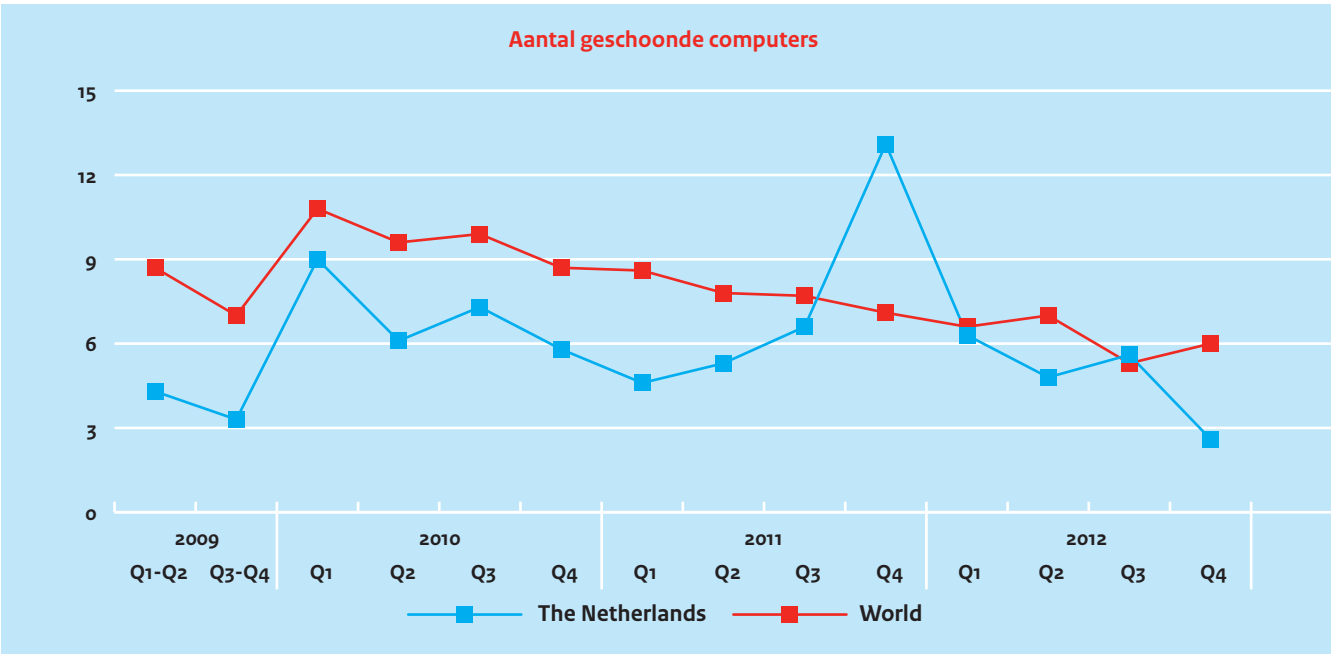


Figuur 3. Aantal unieke geregistreerde kwetsbaarheden per jaar (bron: NVD)

4.2.6 Aantal infecties in Nederland ligt lager dan wereldwijde gemiddelde

Microsoft meet al een aantal jaren het aantal geschoonde computers per duizend executies van antimalware software (Computers Cleaned per Mille, CCM). In figuur 4 is dit uitgezet in de tijd. Nederland scoort hierbij bijna altijd lager, wat een indicatie is dat het aantal besmette computers in Nederland lager is dan het wereldwijde gemiddelde.

Het aantal geschoonde computers van individuele landen kan significant schommelen per kwartaal. Dit komt enerzijds door het aantal geïnfecteerde computers en anderzijds door verbeterde detectiemethodes. In het vierde kwartaal van 2011 toonde het aantal geschoonde computers in Nederland een piek, die te verklaren is door het toevoegen van detectie van de EyeStye-malwarefamilie. Wereldwijd scoren Zuid-Korea (93,0), Pakistan (26,8), Palestina



Figuur 4. Relatieve hoeveelheid gedetecteerde infecties per duizend scans in Nederland en de rest van de wereld [24: MS 2012-1]

(26,2), Georgië (24,2) en Egypte (22,3) het slechtst. De landen met de beste scores zijn: Japan (0,7), Finland (0,8), Denemarken (1,5) en Tsjechië (1,6). Het verschil tussen het slechtste en beste land is meer dan een factor 100.

4.2.7 Ernstigste kwetsbaarheden in standaardsoftware nemen in aandeel toe

Niet alleen het aantal kwetsbaarheden is van belang, ook de impact en het gemak waarmee kwetsbaarheden zijn uit te buiten zijn van belang. Uit een analyse van CVE-registraties en NCSC-beveiligingsadviezen blijkt dat 46 tot 61 procent van alle kwetsbaarheden een gemiddelde impact heeft. Wat opvalt, is dat het relatieve aantal van de meest ernstige kwetsbaarheden[69] vanaf 2011 is toegenomen. Tussen 2007 en 2011 kreeg ongeveer 6 tot 8 procent van alle geregistreerde kwetsbaarheden de hoogste score, vanaf 2011 verandert dat en sinds het begin van 2012 is dat 12 procent. Dit betekent dat relatief meer kwetsbaarheden eenvoudig uit te buiten zijn (op afstand, niet complex en zonder authenticatie) en daarnaast een hoge impact hebben, zowel beschikbaarheid, integriteit als vertrouwelijkheid komen in het geding.

4.3 Conclusie

De weerbaarheid bestaat enerzijds uit (het afwezig zijn van) de kwetsbaarheid van de te verdedigen belangen en anderzijds uit maatregelen om de kwetsbaarheid te verminderen. Kwetsbaarheden zorgen ervoor dat onze maatschappij kwetsbaar blijft voor cyberaanvallen.

De kwetsbaarheid van ICT blijft onverminderd hoog. Na een aantal jaar daling neemt het aantal gepubliceerde kwetsbaarheden in standaardsoftware weer toe (+27 procent) en stijgt het aantal gepubliceerde kwetsbaarheden in industriële automatisering. Gegevens zijn mobiel geworden, verlies of diefstal van een mobiel apparaat maakt de opgeslagen gegevens mogelijk toegankelijk voor de vinder. Bij hyperconnectiviteit worden alle apparaten met elkaar verbonden, niet alleen smartphones, tablets of computers maar alle denkbare apparaten, van koelkasten tot auto's waardoor bestaande kwetsbaarheden op meer manieren kunnen worden misbruikt.

De eindgebruiker krijgt een grote verantwoordelijkheid toegedicht voor beveiliging, maar hij wordt steeds vaker geconfronteerd met kwetsbaarheden in apparaten waarop hij beperkte invloed heeft. Daar komt bij dat beveiliging van computers en apparaten kennis vereist die veel eindgebruikers niet hebben. Consumerization brengt daarnaast met zich mee dat privé- en zakelijk gebruik door elkaar gaan lopen, terwijl zij elkaar niet altijd verdragen. Zakelijke informatie komt buiten beheer van de organisatie en kan in een privéomgeving uitlekken en privé-informatie kan toegankelijk worden voor organisaties.

Cloudcomputing heeft vele voordelen maar brengt ook risico's met zich mee, onder meer omdat de toegang niet altijd even goed is beveiligd en de cloud de autonomie van organisaties over de omgang met bevragingen door buitenlandse overheden vermindert. Cloudcomputing brengt daarnaast uitdagingen voor de opsporing en vervolging van misdaad met zich mee.

Veel organisaties hebben de basismaatregelen, zoals het patchen en updaten van systemen of het wachtwoordenbeleid nog niet op orde. Daarom zijn oude kwetsbaarheden en aanvalsmethoden nog steeds effectief. Een belangrijke kwetsbaarheid is ten slotte dat veel organisaties de juiste kennis, de detectiemiddelen en het vermogen ontberen om incidenten afdoende af te handelen. «

69 Dat zijn de kwetsbaarheden die een 10 scoren op het Common Vulnerability Scoring System, zie http://www.first.org/cvss/cvss-guide

5 Weerbaarheid: maatregelen

Dit hoofdstuk richt zich op de maatregelenkant van weerbaarheid en schetst de belangrijkste ontwikkelingen op het gebied van maatregelen over de afgelopen periode die tot doel hebben om de digitale weerbaarheid van individuen, organisaties en de samenleving te versterken. De beschrijvingen zijn gebaseerd op open bronnen en informatie die door diverse partijen beschikbaar is gesteld.

5.1 Nationale Cyber Security Strategie

Een belangrijke bron van maatregelen op het gebied van weerbaarheid van de gehele Nederlandse samenleving tegen cyberdreigingen is de Nationale Cyber Security Strategie, welke in 2013 wordt herzien. De activiteiten die in de eerste strategie zijn beschreven, zijn grotendeels in gang gezet.[70] Met de komende Nationale Cyber Security Strategie heeft de overheid de ambitie om met publiek-private inzet voor Nederland de visie op groei, veiligheid en vrijheid in de cybersamenleving te schetsen. Daarnaast zal de strategie een actieprogramma bevatten gericht op weerbaarheidsverhoging. Parallel hieraan loopt de ontwikkeling van een EU-strategie en EU-richtlijn voor netwerk- en informatiebeveiliging. Deze moeten een hoog niveau van cybersecurity in de EU waarborgen. Nederland behoort tot de landen in de EU waar veel van de voorgestelde EU-maatregelen reeds zijn gerealiseerd dan wel in voorbereiding zijn.

5.2 Bewustwording

Het creëeren en onderhouden van bewustwording (of awareness) van de risico's in de digitale wereld en het handelingsperspectief, is een randvoorwaardelijke maatregel voor cybersecurity. Zonder bewustwording op alle niveaus (van bestuurders tot medewerkers en consumenten) zijn andere maatregelen namelijk al snel minder effectief.

Partnership for Cyber Resilience
Het toenemend bewustzijn uit zich onder meer in de ondertekening door een groeiend aantal Nederlandse bedrijven en instellingen van de principles voor het internationale Partnership for Cyber Resilience van het World Economic Forum[58: WEF 2012]. Hiertoe behoorden het afgelopen jaar organisaties als TNO, KPN, Alliander, Schiphol Group, Unilever en Havenbedrijf Rotterdam.

Het afgelopen jaar zijn verschillende internationale en landelijke campagnes gevoerd, onder meer Cyber Security Month (oktober 2012, ENISA), Alert Online[71] (november 2012, coördinatie NCTV), de Veilig bankieren-campagne 'Bankgegevens en inlogcodes. Hou ze geheim'[72] (NVB), Safer Internet Day (februari 2013, DigiBewust)[73], Bescherm je bedrijf[74] (voor MKB, Nederland ICT) en de oprichting van de Taskforce Bestuur en Informatieveiligheid Dienstverlening in februari 2013. Deze Taskforce heeft als doel het bewustzijn van informatieveiligheid en de sturing hierop te versterken bij bestuurders van gemeenten, provincies, waterschappen, ministeries en hun uitvoeringsorganisaties.[75]

Enerzijds krijgt de burger een grotere verantwoordelijkheid toegedicht voor beveiliging dan hij kan waarmaken. Anderzijds komt uit onderzoeken naar voren dat Nederlandse burgers een relatief hoog vertrouwen hebben in de veiligheid van de ICT-infrastructuur en de rol van de overheid daarbij.[76] Dit vertrouwen is een van de bijdragende factoren van het hoge gebruik van internet en diensten als onlinewinkelen en -bankieren. Ook in Europees perspectief zijn Nederlanders goed onderlegde veelgebruikers en geeft een bovengemiddeld aantal van hen aan redelijk tot goed geïnformeerd te zijn over de risico's van cybercrime (54 procent).[77] Het internationaal gezien relatief beperkte aantal besmettingen bevestigt het vertrouwen dat Nederlandse burgers als eindgebruikers hebben in hun eigen weerbaarheid.[78]

5.3 Technologie

Normen, richtlijnen en standaarden op het gebied van cybersecurity helpen organisaties om de beveiliging van hun informatievoorziening op een hoger niveau te brengen. Hierna zijn de belangrijkste ontwikkelingen op dit gebied samengevat.

5.3.1 *Migratie naar DNSSEC vordert*

DNSSEC is een uitbreiding van het DNS-protocol (Domain Name Server). Systemen die dit protocol ondersteunen, ontvangen van de *domain name server* adresinformatie voorzien van een digitale handtekening, waarmee de authenticiteit van deze informatie gecontroleerd kan worden. In Nederland biedt SIDN, de .nl-registry, de mogelijkheid .nl-domeinnamen te beveiligen met DNSSEC. Begin september 2012 waren al meer dan 1 miljoen van de ruim 5 miljoen domeinnamen beveiligd met DNSSEC.
De sterke groei vlakte daarna af. SIDN geeft aan dat de goede

70 Brieven aan de Tweede Kamer over Voortgang Nationale Cyber Security Strategie,Tweede Kamerstukken 26 643 (bijv. nr. 202, juli 2012).

71 http://www.nctv.nl/pp/alertonline/
72 http://www.veiligbankieren.nl/nl/
73 http://www.saferinternetday.nl/
74 http://beschermjebedrijf.nl/
75 Vergaderjaar 2012-2013, Kamerstuk 26643, nr 269.
76 TNO 2013; Capgemini, Trends in Veiligheid 2013, o.b.v. onderzoek van TNS/NIPO. Deze cijfers zijn van vóór de serie DDoS-aanvallen in april 2013. Het effect daarvan is nog onbekend.
77 European Commission, Special Eurobarometer 390 Cyber Security, 2012.
78 Microsoft Security Intelligence Report, Volume 13, 2012.

Status cybersecuritybewustzijn in Nederland
In november 2012 verscheen een onderzoek van Motivaction naar het digitale veiligheidsbewustzijn bij overheden, vitale sectoren, (overige) bedrijven en consumenten.[27: Motivaction 2012] Meer dan 80 procent van alle respondenten zei te weten welke informatie vertrouwelijk is en ruim tweederde gaf aan te weten wat te moeten doen bij een incident. Toch deelt zes op de tien medewerkers naar eigen zeggen wel eens gevoelige informatie via een onveilig medium.
Het rapport concludeerde verder dat er opvallende verschillen waren tussen de verschillende groepen. Vitale sectoren hebben het best verankerde cybersecuritybeleid, gevolgd door het Rijk, aldus het rapport. In het Rijk en de gemeenten is echter het hoogste gevoel van eigen verantwoordelijkheid bij medewerkers. Het digitale veiligheidsbeleid is bij gemeenten het minst sterk geborgd. Gemeenteambtenaren geven de laagste rapportcijfers voor cybersecurity, zowel aan de organisatie, aan collega's als aan zichzelf.
De Nederlandse consument ten slotte heeft een beperkt beeld bij het begrip cybersecurity, maar kent bijvoorbeeld wel phishing als fenomeen, onder andere door de intensieve NVB-campagnes. Volgens consumenten is het grootste risico dat via het internet hun persoonlijke informatie ongewenst wordt gedeeld.

Nederlandse documentatie voor de invoering van DNSSEC, kwaliteit van de software en prijsvoordelen voor grote afnemers deze groei hebben gestimuleerd.

5.3.2 *Gebruik IPv6 in Nederland groeit*

IPv6 maakt het mogelijk om gegevens tijdens transport te voorzien van beveiliging door middel van encryptie en authenticatie van data. Daarentegen kan gebrekkige implementatie van IPv6 ook tot kwetsbaarheid leiden. De uitgifte van IPv6 groeide afgelopen jaar met bijna 4,5 miljoen adressen, na een groei van 15 miljoen in 2011.[79] In oktober 2012 was ongeveer 18 procent van alle Nederlandse websites via IPv6 bereikbaar.

5.3.3 *DKIM op 'pas toe of leg uit'-lijst*

DomainKeys Identified Mail Signatures (DKIM) is een protocol waarmee een e-mail aan een domeinnaam wordt gekoppeld met behulp van een digitale handtekening. Het stelt de ontvanger in staat om te bepalen welke domeinnaam (en daarmee welke achterliggende organisatie) verantwoordelijk is voor het zenden van de e-mail. Daardoor kunnen spam- en phishingmails beter worden gefilterd.[80] Sinds 2012 staat ook DKIM op de 'pas toe of leg uit'-lijst van het College Standaardisatie.

79 TNO 2013.
80 https://lijsten.forumstandaardisatie.nl/open-standaard/dkim

5.3.4 *Security Development Lifecycle*

De Security Development Lifecycle aanpak van Microsoft[81], die is overgenomen door verschillende andere partijen, zoals Adobe[82] en Cisco[83], SCADA-leveranciers[84] en financiële instellingen,[85] zorgt ervoor dat Security een integraal onderdeel is van de ontwikkeling en het onderhoud van software. De aanpak volgt bij elk van deze leveranciers de stappen: analyse (threat modelling, requirements, ontwerp), ontwikkeling, testen, implementatie en onderhoud. Transparantie naar stakeholders hoort ook bij deze aanpak.

5.3.5 *ICT-beveiligingsassessments DigiD*

Op basis van de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het NCSC is door de minister van Binnenlandse Zaken en Koninkrijksrelaties de DigiD-aansluitnorm vastgesteld. Toetsing bij zes grootverbruikers (waaronder DUO en Belastingdienst) heeft volgens de minister bij geen van hen tot de conclusie geleid dat sprake is van een zodanig serieus en acuut beveiligingsrisico.[86] Uit de betreffende auditrapporten komen wel bevindingen naar voren die aanleiding geven voor maatregelen. Om gemeenten te ondersteunen is KING (Kwaliteits Instituut Nederlandse Gemeenten) in opdracht van BZK en de Vereniging van Nederlandse Gemeenten het project Ondersteuning ICT-Beveiligingsassessment DigiD gestart.[87] De in 2012 opgerichte Informatiebeveiligingsdienst voert dit project momenteel uit, opdat eind 2013 alle gemeenten zijn doorgelicht.

5.3.6 *Voorbeelden van technische maatregelen*

Organisaties implementeren tal van technische (en deels organisatorische) maatregelen om kwetsbaarheden te lijf te gaan en daarmee incidenten te voorkomen, waaronder:
» Webmail van organisaties zoals Google en Microsoft worden beveiligd met vormen van two-factor authenticatie.
» Banken implementeren Geo-Blocking om geldopnames met gekopieerde (geskimde) bankpassen te verhinderen.
» Google's Chrome blokkeert vanaf versie 25 stille installatie van extensies en is daardoor minder vatbaar voor malware.

5.4 Cyberoefeningen

Oefeningen helpen medewerkers en organisaties te leren wat gedaan moet en kan worden bij (dreigende) incidenten. Net als voorgaande jaren waren er diverse internationale cyberoefeningen, zoals Cyber Europe 2012 van de EU, Cyber Coalition van de NATO, Cyberstorm IV (onder regie van US Department of Homeland Security) en @TOMIC 2012, een nucleaire oefening met cybersecuritycomponent. De minister van Veiligheid en Justitie sprak verder

81 http://www.microsoft.com/security/sdl/default.aspx
82 http://www.adobe.com/security/splc/
83 http://www.cisco.com/web/about/security/cspo/csdl/index.html
84 http://www.darkreading.com/advanced-threats/167901091/security/application-security/240000526/scada-smart-grid-vendor-adopts-microsoft-s-secure-software-development-program.html
85 http://www.darkreading.com/advanced-threats/167901091/security/application-security/240000526/scada-smart-grid-vendor-adopts-microsoft-s-secure-software-development-program.html
86 Brief MinBZK, ICT beveiligingsassessments en Taskforce Bestuur en informatieveiligheid Dienstverlening, Kamerstukken 26643, nr. 269.
87 https://new.kinggemeenten.nl/informatiebeveiliging/assessment-digid

met zijn Duitse ambtgenoot af een Duits-Nederlandse cyberoefening te beleggen. Ook binnen vitale sectoren vinden oefeningen plaats, zowel voor afzonderlijke bedrijven als voor groepen.

5.5 Detectie en situational awareness

De afgelopen jaren is er in de aandacht van security experts een verschuiving opgetreden van preventie naar detectie. De praktijk laat zien dat aanvallen niet buiten de deur te houden zijn en dat het opmerken van aanvallen en incidenten (detectie) en een goed inzicht in de situatie van groot belang zijn voor een tijdige en adequate reactie. Diverse private en publieke partijen in Nederland hebben 'honeypots' en andere technische sensoren om op operationeel niveau cyberaanvallen te detecteren en te analyseren. Ook op tactisch en strategisch niveau monitoren bedrijven (met name multinationals) en overheidsorganisaties relevante ontwikkelingen.

Dit heeft tot dusverre echter nog niet geleid tot een continu gedeeld beeld van de status van cybersecurity, oftewel 'situational awareness'. Het NCSC bouwt in het kader van het Nationaal Detectie Netwerk verder aan de juiste indicatoren in een netwerk waarin technische, bestuurlijke, sociale en andere nuttige informatie uitgewisseld wordt en daarmee de informatiepositie versterkt voor alle betrokken organisaties.

CERTs hebben ook een alerteringsfunctie richting hun achterban. In de rapportageperiode heeft het NCSC 1672 advisories uitgebracht, waarvan 899 updates op bestaande advisories. In de voorgaande rapportageperiode was het totaal 1135, waarvan 567 updates.

De behoefte aan een betere informatiepositie bij zowel overheden als bedrijven leidt tot een intensivering van de samenwerking op het gebied van informatie-uitwisseling. De afgelopen periode is onder andere een nieuwe Information Sharing and Analysis Centers (ISAC) opgericht voor de zorgsector, naast de al bestaande voor Financial Institutions, Multinationals, Telecom, Water, Nucleair, Energy, Havens, Airport en Managed Services Providers. Hiermee zijn veel, maar nog niet alle vitale sectoren afgedekt. Verder zijn er liaisons geplaatst bij het NCSC vanuit de AIVD, MIVD, politie (Team High Tech Crime), OM, NFI, ACM, IT-leveranciers, SIDN en binnenkort ook vanuit de banken. Naar aanleiding van de DDoS-aanvallen in april 2013 hebben banken en NCSC verdere afspraken gemaakt om te komen tot een betere uitwisseling van informatie.

5.6 Response

De weerbaarheid van onze samenleving is gebaat bij een effectief landelijk netwerk van (sectorale) informatiebeveiligingsdiensten, die in geval van incidenten samenwerken aan response, naast het nemen van de eigen verantwoordelijkheid voor de eigen digitale veiligheid. Dit netwerk is nog in ontwikkeling. Op nationaal niveau zijn sinds 2012 twee nieuwe sectorale schakelorganisaties gestart: de eerdergenoemde Informatiebeveiligingsdienst (IBD) voor gemeenten en het Centrum Informatiebeveiliging en Privacybescherming (CIP). Deze laatste is een samenwerkingsverband van overheidsorganisaties in de uitvoering (waaronder UWV, SVB, DUO en de Belastingdienst) en een aantal marktpartijen.

Het ministerie van Veiligheid en Justitie heeft voorts de ICT-crisisaanpak en -organisatie versterkt om via gepaste opschalingsniveaus een (dreiging van) ICT-crisis te bestrijden binnen de nationale crisisstructuur. Deze structuur is tijdens de DDoS-aanvallen in april 2013 ingezet.

5.7 Meldingen

In de rapportageperiode zijn verschillende maatregelen gestart om meer meldingen over cyberincidenten te krijgen en om efficiënter om te gaan met verkregen meldingen. De effecten van deze initiatieven zijn nog niet meetbaar.

Samenwerking abusemeldingen in telecom

'Abuse' staat voor bewust of onbewust misbruik van internet. Om misbruik van hun diensten tegen te gaan, beschikken de meeste internetserviceproviders over een meldpunt, een Abusedesk. In oktober 2012 werd Abuse Information Exchange opgericht door de internetproviders KPN, SOLCON, Tele2, UPC, XS4ALL, Zeelandnet en Ziggo, SIDN, de .nl-registry en ECP, Platform voor de Informatiesamenleving.[88] Abuse Information Exchange is bedoeld om meldingen over botnetbesmettingen via één loket te verzamelen en de informatie vervolgens door te sturen naar de aangesloten providers. Door deze aanpak kunnen de providers sneller schakelen en kosten besparen.

Meldplicht voor datalekken uitgebreid

Er geldt een meldplicht voor verstoringen in de continuïteit van het netwerk van openbare aanbieders voor elektronische communicatienetwerken en -diensten.[89] Met ingang van 5 juni 2012 zijn aanbieders van openbare elektronische communicatiediensten ook wettelijk verplicht om beveiligingsincidenten te melden waarbij de bescherming van persoonsgegevens in het geding is.

Op basis van voorgenomen aanscherping van Europese regels voor privacybescherming ligt er een wetsvoorstel voor een bredere meldplicht van datalekken waarbij persoonsgegevens zijn betrokken.[90] Ook datalekken met medische gegevens zullen onder deze meldplicht vallen.[91] Met de meldplicht, in combinatie met de boetebevoegdheid van het College Bescherming Persoonsgegevens (CBP), worden bedrijven en overheden gestimuleerd om al in de ontwerpfase van diensten en producten goed na te denken over een goede beveiliging om lekken te voorkomen. De afgelopen twee jaar heeft het CBP drie meldingen binnengekregen van datalekken met

88 http://www.ecp.nl/abuse-ix-strijdt-tegen-botnets
89 http://www.meldplichttelecomwet.nl
90 http://www.rijksoverheid.nl/documenten-en-publicaties/wetsvoorstellen/2012/11/01/wijziging-wet-bescherming-persoonsgegevens-meldplicht-datalekken
91 Brief van de minister van VWS, Kamerstukken 27 529, 121 (ICT in de zorg).

persoonsgegevens.[92] De verwachting is dat een wettelijke verplichting het aantal meldingen zal doen toenemen, zodat ook meer inzicht ontstaat in de situatie.

Spam

Het spamverbod (artikel 11.7 Telecommunicatiewet) beoogt de eindgebruiker te beschermen tegen ongewenste elektronische berichten (via bijvoorbeeld e-mail, fax, SMS of sociale media). Toezicht op het spamverbod is belegd bij de ACM, die hiervoor onder andere een speciaal klachtenportaal (www.spamklacht.nl) heeft ingericht voor consumenten en bedrijven. Op dit meldpunt heeft de ACM in 2012 24.536 klachten over spam ontvangen. Naast het uitvoeren van onderzoek, zoekt de ACM actief samenwerking met (inter)nationale publieke en private partijen. Juridische uitspraken in spamonderzoeken uit 2012 zijn terug te vinden in het ACM jaarverslag 2012.[38: OPTA 2013]

Responsible disclosure geïntroduceerd

Responsible disclosure binnen de ICT-wereld is het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid.[32: NCSC 2013-1] Toepassing van responsible disclosure kan een goede bijdrage leveren aan het verhogen van de veiligheid van informatiesystemen en (software)producten. In 2013 is de leidraad voor de totstandkoming tot een praktijk van responsible disclosure in Nederland uitgebracht.[32: NCSC 2013-1] Dit is een handreiking voor organisaties en melders voor het op een verantwoordelijke wijze melden en afhandelen van kwetsbaarheden in informatiesystemen en (software)producten. Het is nu aan organisaties om een eigen responsible disclosurebeleid te implementeren en te publiceren. Begin 2013 zijn de eerste meldingen binnengekomen bij het NCSC, maar het is nog te vroeg om daar conclusies aan te verbinden.

5.8 Cyberoperations bij Defensie

In juni 2012 heeft de Minister van Defensie de Defensie Cyber Strategie uitgegeven met daarin zes speerpunten. De speerpunten voor Defensie zijn een integrale aanpak, de versterking van de digitale weerbaarheid ('defensief'), het militair vermogen om cyberoperations uit te voeren ('offensief'), de vergroting van de cyberinlichtingencapaciteit, het adaptief en innovatief vermogen en de samenwerking.[93] Defensie breidt haar cybercapaciteiten uit teneinde de inzet van de Nederlandse strijdkrachten te waarborgen alsmede de effectiviteit van de inzet te vergroten. De prioriteit ligt bij het vergroten van de eigen weerbaarheid van Defensie en het versterken van de inlichtingenpositie.

In 2012 is een Taskforce Cyber opgericht om de intensivering te faciliteren. Tevens is begonnen met de uitbreiding van de capaciteiten van het Defensie Computer Emergency Response Team (DefCERT) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Tegelijk is de samenwerking met NCSC en andere partners geïntensiveerd. Ter verhoging van de interne bewustwording zijn diverse leeromgevingen geïntroduceerd en is aan diverse cyberoefeningen deelgenomen. Verder zal door de Taskforce het vermogen om cyber in het militair optreden toe te passen (inclusief offensieve capaciteit) worden opgezet. Daartoe worden het Defensie Cybercommando en het Defensie Cyber Expertise Centrum (DCEC) opgericht.

DefCERT ziet toe op de bescherming van de netwerken van Defensie. De huidige capaciteit van DefCERT wordt uitgebreid met specialisten op ICS en Proces Control- of Supervisory Control And Data Aquisition (SCADA) systemen. Daarmee wordt een belangrijke stap gezet voor het vergroten van de bescherming van wapen- en sensorsystemen.

De MIVD doet onderzoek naar alle actoren die een cyberdreiging vormen voor de Nederlandse krijgsmacht en de defensie-industrie. De MIVD versterkt zijn informatiepositie in het cyberdomein teneinde digitale aanvallen van (potentiële) tegenstanders te detecteren, te duiden en tegen te gaan. Op deze manier levert de MIVD een bijdrage aan het bestrijden van cyberdreigingen met als doel de inzetbaarheid en paraatheid van de Nederlandse krijgsmacht te blijven garanderen. Vanwege zijn expertise en bijzondere wettelijke bevoegdheden vervult de MIVD, in samenwerking met het Defensie Cybercommando, een essentiële rol bij de ontwikkeling van de offensieve cybercapaciteiten van Defensie. Tevens zal met de AIVD het project Symbolon geïmplementeerd worden, waarmee beide inlichtingendiensten hun cyber- en SIGINT-capaciteit bundelen in een gezamenlijke eenheid.

Digitale oorlogsvoering en cyberconflicten

Staten beperken zich in cyberspace niet enkel tot de verdediging tegen cyberaanvallen, ze ontwikkelen ook in toenemende mate inlichtingen en offensieve cybercapaciteiten. Staten voeren dagelijks digitale verkenningen uit op computernetwerken voor spionage en/of offensieve doeleinden.

De angst voor een koude oorlog in het digitale domein wordt vooral sterk aangewakkerd door de media.[94] In realiteit zijn digitale middelen toegevoegd aan het arsenaal aan wapens dat een staat reeds tot zijn beschikking heeft. De inzet van digitale middelen is relatief laagdrempelig vanwege de mate van anonimiteit en doordat het ontwikkelen en inzetten van digitale middelen eenvoudiger en goedkoper is dan conventionele wapens. Politieke en militaire conflicten vinden al gedeeltelijk plaats in cyberspace en omvatten veelal dezelfde elementen als in de fysieke wereld, zoals propaganda, spionage, verkenningen en gerichte aanvallen.

92 Brief van de minister van Veiligheid en Justitie aan de Tweede Kamer, Antwoorden kamervragen over het bericht dat de Verenigde Staten kiezen voor het vrijwillig melden van cybersecurity incidenten, 24 april 2013.

93 Defensie Cyber Strategie, juni 2012

94 Washington, Beijing in Cyber-war Standoff, Newsline ABC, 12 februari 2013

De Nederlandse krijgsmacht beschouwt daarom cyberspace als het vijfde domein.[95]

Conflicten die (deels) worden uitgevochten in het digitale domein, kunnen een extra dreiging met zich meebrengen wanneer er op grote schaal *spillover* naar de burgermaatschappij plaatsvindt. Offensieve cybercapaciteiten kunnen immers worden ingezet via kwetsbaarheden op privé- en bedrijfscomputers, en op mobiele middelen.[96] Daarnaast is het door middel van een gerichte cyberaanval in theorie mogelijk om van afstand schade toe te brengen aan een land door bijvoorbeeld de SCADA-systemen te infecteren.

De inzet van digitale middelen kan ook met geavanceerde technische aanvallen op militaire installaties plaatsvinden. Zo werd eind 2011 het drone-programma van de Amerikaanse luchtmacht geïnfecteerd met een virus. Het virus heeft het operationele deel van de missie niet in gevaar gebracht, maar heeft wel enige overlast bezorgd.[97][98] Een ander voorbeeld is de hack van Amerikaanse *drones* door *insurgents* in Irak, waarmee livevideobeelden zijn geïntercepteerd zodat de *insurgents* in potentie Amerikaanse militaire operaties konden ontwijken of monitoren.[99] Voorts heeft een Amerikaanse generaal toegegeven dat het Amerikaanse leger offensieve cybercapaciteiten heeft ingezet in Afghanistan. Door het uitvoeren van deze cyberoperaties konden de Verenigde Staten de command-&-control van tegenstanders infecteren.[100]

In de praktijk gebeurt de inzet van digitale middelen vaker (en zeker zichtbaarder) aan de 'zachte' kant van psychologische oorlogsvoering, zoals via Twitter en andere sociale media. Dit was bijvoorbeeld te zien tijdens Israëlische operaties tegen Gaza[101] en ISAF-operaties in Afghanistan, waar Taliban en ISAF elkaar via Twitter de loef probeerden af te steken.[102] Ook de meervoudige inbraken in augustus 2012 in het Twitter-account en de Wordpress blogomgeving van het persbureau Reuters zijn goede voorbeelden. Op deze media verschenen 22 valse tweets en meerdere blogposts, zogenaamd van Reuters journalisten, over de ontwikkelingen in het conflict in Syrië, nadat onbekenden het account en de blogomgeving hadden gehackt.[103]

95 De vier andere domeinen zijn: lucht, zee, land en ruimte.
96 Cyber Crime and Cyber War Predictions, Cyber Defense Magazine, 25 maart 2013.
97 Computer Virus Hits U.S. Drone Fleet, www.wired.com, 7 oktober 2011.
98 Air Force says drone computer virus poses 'no threat', Los Angeles Times, 13 oktober 2011.
99 Insurgents Hack U.S. Drones, The Wall Street Journal, 17 december 2009.
100 Afghanistan Cyber Attack: Lt. Gen. Richard P. Mills claims to have hacked the enemy, Huffington Post, 24 augustus 2012.
101 Editoriaal: Cyber en militair vermogen, Militaire Spectator 12-2012.
102 Jan ven der Meulen en René Moelker, Digital duels in the global public sphere, in: P. Ducheine, F. Osinga, J. Soeters (red), Cyber Warfare – Critical Perspectives, 2012.
103 http://www.reuters.com/article/2012/08/03/net-us-reuters-syria-hacking-idUS-BRE8721B420120803, http://www.reuters.com/article/2012/08/06/net-us-reuters-syria-hacking-idUSBRE8721B420120806, http://www.theregister.co.uk/2012/08/17/reuters_blogs_hacked_again/,http://blogs.wsj.com/cio/2012/08/05/hacked-reuters-wordpress-platform-had-known-security-issue/

Offensieve cybercapaciteiten zullen, binnen het gegeven mandaat, door het Defensie Cybercommando worden ingezet onder verantwoordelijkheid van de Commandant der Strijdkrachten (CDS). De krijgsmacht moet in staat zijn in 2015 offensieve cybercapaciteiten in militaire operaties in te zetten.

Defensie neemt voorts deel aan de Nationale Cyber Security Research Agenda, aan verschillende NAVO- en EU-programma's en aan het Cooperative Cyber Defense Centre of Excellence (CCDCoE) in Tallinn. Ter voorbereiding op de inrichting van een leerstoel in 2014 is in 2012 een Universitair Hoofddocent Cyber Operations aan de Nederlandse Defensie Academie van het ministerie van Defensie aangesteld.

5.9 Onderwijs en onderzoek

Goed onderwijs en onderzoek zijn belangrijk voor duurzame weerbaarheid. In het onderwijs zijn het afgelopen jaar door meerdere hogescholen, universiteiten en bedrijven opleidingen voor cybersecurity opgericht of versterkt. De vraag rijst of deze (semi)publieke en private initiatieven elkaar voldoende aanvullen.

In het kader van de Nationale Cyber Security Research Agenda (NCSRA) zijn twee oproepen voor onderzoeksvoorstellen gedaan, waarvoor € 6,3 miljoen beschikbaar is. Met behulp van de SBIR-regeling[104] zijn ten eerste kortetermijnontwikkeltrajecten getenderd, met als resultaat dat er zeventien haalbaarheidsonderzoeken worden uitgevoerd. Deze zullen medio 2013 worden beoordeeld, om te zien welke trajecten indieners kansrijk kunnen doorontwikkelen. Ten tweede is door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) aan negen projecten voor langetermijnonderzoek gezamenlijk een bedrag van 3,2 miljoen euro toegekend.[105]

5.10 Conclusie

Veel weerbaarheidsinitiatieven die in de vorige editie van het CSBN werden genoemd, zijn ook daadwerkelijk gestart of al in volle uitvoering. In het afgelopen jaar is – mede door grote incidenten – de publieke en politieke aandacht voor cybersecurity flink toegenomen. De noodzaak is ook doorgedrongen in de directiekamer, zodat vaker de portefeuille cybersecurity of informatiebeveiliging expliciet op hoog niveau wordt belegd. Overheid en bedrijfsleven besteden meer dan voorheen aandacht aan maatregelen en dit gebeurt steeds vaker in gezamenlijkheid.

In het oog springend zijn de bewustwordingscampagnes, zoals 'Alert Online', 'Bankgegevens en inlogcodes. Hou ze geheim' en 'Bescherm je bedrijf'. Daarnaast zijn de intensivering van de samenwerking op het gebied van informatie-uitwisseling en de afspraken tussen banken en overheid naar aanleiding van de

104 Small Business Innovation Research programma, http://www.agentschapnl.nl/nl/node/460958
105 http://www.nwo.nl/actueel/nieuws/2013/ew/negen-projecten-in-cyber-security-onderzoek-van-start.html

DDoS-aanvallen sprekende voorbeelden. Op het gebied van onderzoek en innovatie zijn verschillende onderzoeksprogramma's opgezet om vraagstukken op het gebied van cybersecurity in samenwerking tussen overheid, bedrijfsleven en wetenschap aan te pakken. Ook is een leidraad gepubliceerd voor het opstellen van beleid voor Responsible Disclosure, het op verantwoorde wijze bekendmaken van kwetsbaarheden in ICT. Dit is een handreiking voor organisaties en melders voor het op een verantwoordelijke wijze melden en afhandelen van kwetsbaarheden in informatiesystemen en (software)producten.

Het toegenomen bewustzijn leidde de afgelopen periode ook tot nieuwe initiatieven en aanvullende maatregelen op nationaal niveau en bij afzonderlijke organisaties. Daarmee spelen zij in op de toenemende afhankelijkheid van ICT en veranderende dreigingen. De effectiviteit hiervan op de lange termijn is nu nog niet in te schatten. «

6 Manifestaties

In dit hoofdstuk komen de belangen, dreigingen en weerbaarheid samen in manifestaties, zoals weergegeven in de figuur hiernaast. Het beschrijft welke gebeurtenissen of activiteiten van welke actoren (kunnen) leiden tot aantasting van belangen en voorbeelden hiervan in de rapportageperiode van dit CSBN.

Uitgangspunt voor een manifestatie is de 'dreiging' die leidt tot een aantasting van beschikbaarheid, vertrouwelijkheid en/of integriteit van informatie of informatiesystemen. Een dreiging kan werkelijkheid worden door een combinatie van de kwetsbaarheid van het doelwit (het te beschermen belang), de beschikbare hulpmiddelen en een actor met een intentie en capaciteiten om een specifieke aanval uit te voeren. Een dreiging kan afkomstig zijn van een bewust menselijk handelen van een actor, natuurlijke of technische gebeurtenissen en door menselijk falen.

In dit hoofdstuk wordt een indeling gehanteerd die uitgaat van het doelwit waarop een dreiging is gericht: informatie of ICT. Daarbij onderscheiden we de volgende hoofdtypen dreigingen die aanleiding zijn voor een manifestatie:

1. Aanval gericht op informatie
   a) Diefstal van informatie, eventueel voor publicatie of verkoop (bijvoorbeeld digitale spionage en identiteitsdiefstal)
   b) Manipulatie van informatie (bijvoorbeeld fraude met financiële of andere onlinetransacties)
2. Aanval gericht op ICT
   a) Digitale bekladding (defacement)
   b) Verstoring van ICT (bijvoorbeeld DDoS-aanval)
   c) Overname ICT (bijvoorbeeld het onttrekken van resources)
3. Uitval van ICT (door natuurlijke, technische gebeurtenissen of menselijk falen)

Type dreiging	Belangrijkste actor(en) en beoogde doelen
1a) Diefstal informatie, eventueel voor publicatie of verkoop	» Staten: digitale spionage van andere staten en private organisaties » Cybercriminelen: geldelijk gewin » Hacktivisten, cybervandalen, interne actoren: kwetsbaarheden inzichtelijk maken, eigen imago vergroten of schade toebrengen aan anderen
1b) Manipulatie van informatie	» Beroepscriminelen: geldelijk gewin
2a) Defacement	» Hacktivisten: maken van een publiek statement, verspreiden propaganda » Scriptkiddies, cybervandalen: aantonen dat het kan of voor de lol
2b) Verstoring van ICT	» Staten: inzet van offensieve cybercapaciteiten in statelijke conflicten » Terroristen: als wapen tegen fysieke doelen of als ondersteuning voor hun terroristische activiteiten, zoals voor het voeren van propaganda (internet als middel) » Beroepscriminelen: als basis of afleiding voor aanvallen waarbij zij financieel gewin hebben » Hactivisten, Scriptkiddies en cybervandalen: de verstoring is een doel op zich, omdat het kan of voor de lol » Interne actoren: de verstoring is een doel op zich
2c) Overname van ICT	» Criminelen: geldelijk gewin, versturen van SPAM en phishing mails » Hactivisten: hosten van gegevens om propaganda te verspreiden » Scriptkiddies en cybervandalen: aantonen kwetsbaarheden, omdat het kan of voor de lol
3) Uitval ICT door natuurlijke of technische gebeurtenissen	Niet van toepassing

Tabel 3. Overzicht dreigingen

De voorgaande tabel geeft een overzicht van de verschillende hoofdtypen dreigingen met daarbij de belangrijkste actoren en hun beoogde doelen. In de paragrafen hierna zijn de hoofdtypen dreigingen toegelicht, is aangegeven welke manifestaties zijn gesignaleerd en is duiding gegeven aan het niveau van de dreiging. Het geheel is ten slotte in de conclusie samengevat.

6.1 Aanval gericht op informatie

We produceren, verzamelen, delen en verwerken met elkaar steeds meer informatie. Niemand wil dat zijn financiële gegevens, persoonlijke of zakelijke informatie in verkeerde handen terechtkomt of wordt gemanipuleerd. Cyberaanvallen vormen echter een dreiging die de vertrouwelijkheid en/of integriteit van deze informatie kunnen aantasten. Deze paragraaf onderscheidt twee dreigingssoorten gericht op informatie: a) diefstal van informatie met eventueel publicatie of verkoop van informatie en b) manipulatie van informatie.

6.1.1 Diefstal van informatie

Bij diefstal van informatie (eventueel voor publicatie en verkoop) gaat het om het ontvreemden van vertrouwelijke of waardevolle informatie. Een actor kan eenmaal verkregen informatie voor zichzelf houden en daar zelf van profiteren, maar kan deze ook publiceren of verhandelen. Informatie kan in juridische zin niet worden gestolen, er is sprake van het opheffen van de exclusiviteit van informatie omdat de informatie niet wordt weggenomen.

Informatie over financiële transacties en identiteiten het meest gestolen

Uit onderzoek van Verizon[106] blijkt dat vooral informatie over financiële transacties en identiteiten worden ontvreemd. Verizon meldt dat criminelen de voorkeur geven aan informatie over financiële transacties en persoonlijke informatie die eenvoudig kan worden geconverteerd naar contant geld. Bedrijfspionage richt zich op handelsgeheimen, interne informatie van een organisatie en systeeminformatie. Hacktivisten richten zich op persoonlijke informatie en interne informatie van organisaties. Ten slotte zijn identiteiten voor ieder van deze actoren een gewild gegeven.

Digitale spionage

De meest in het oog springende vorm van informatiediefstal is digitale spionage door (vooral) staten. De intentie achter diefstal van informatie is voor staten politiek, militair of economisch gewin via digitale spionage.[107] De omvang en structurele wijze waarop digitale spionage wordt toegepast, vormt een grote dreiging voor de nationale veiligheid en economie. In de afgelopen rapportageperiode zijn diverse publieke en private organisaties in Nederland hier slachtoffer van geworden. Daarom is deze dreiging 'hoog' geclassificeerd. Digitale spionage van burgers richt zich op bepaalde personen (vaak dissidenten) die door staten worden gevolgd.

Hoewel de herkomst van digitale spionage zelden onomstotelijk vastgesteld kan worden, zijn er diverse aanwijzingen voor betrokkenheid van staten. De AIVD heeft spionageactiviteiten waargenomen vanuit China, Rusland, Iran en Syrië. Zie het verdiepingskatern Cyberspionage voor meer informatie. Afgelopen jaar is het aantal zaken van digitale spionage, dat bekend wordt, toegenomen. De actoren achter deze aanvallen besteden substantiële hoeveelheden geld en tijd aan deze aanvallen. Daarbij wordt het doelwit welbewust gekozen en een aanval gericht ingezet, net zo lang tot het doel bereikt is. Hier wordt ook wel de term *Advcanced Persistent Threat* voor gebruikt.

Advanced Persistent Threat (APT)

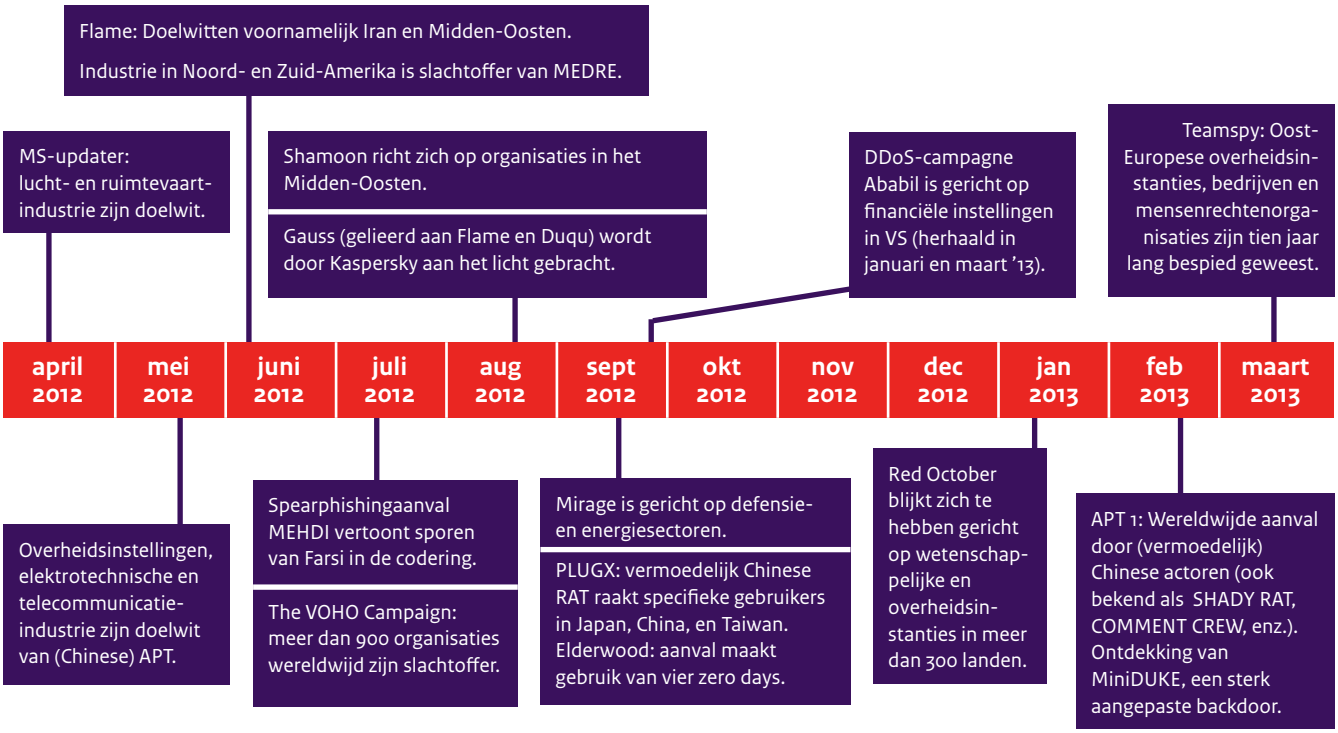
Een Advanced Persistent Threat is de dreiging die uitgaat van een doelgerichte, 'langdurige' cyberaanval op vooral kennisrijke landen en organisaties door statelijke actoren en criminele organisaties. De AIVD doet onderzoek naar APT's. De aanvaller is daarbij volhardend in zowel de pogingen om een organisatie binnen te dringen alsook om binnen de ICT-infrastructuur heimelijk aanwezig te blijven. Tijdens de APT-aanval zal de aanvaller vooral 'vertrouwelijke' informatie verzamelen en/of voorbereidingen treffen om werking van vitale componenten te kunnen verstoren. Het merendeel van deze aanvallen is eenvoudig van aard en vooral succesvol door het ontbreken, binnen organisaties, van adequate detectie en beveiligingsmaatregelen.

Vooral het rapport van de firma Mandiant over de door hen 'APT1' gedoopte spionageaanval heeft veel publiciteit gekregen.[108]

Zie het factsheet 'De aanhouder wint (APT)' van het NCSC en de AIVD voor meer informatie.[35: NCSC 2013-2]

Het overzicht op pagina 45 geeft een indicatie van de omvang en diversiteit van digitale (spionage)aanvallen.[109] De informatie is afkomstig uit open bronnen en is nadrukkelijk geen uitputtend overzicht. Gezien enkele overeenkomstige kenmerken is het mogelijk dat sommige campagnes dezelfde aanval beschrijven. De benoemde data zijn een verwijzing naar eerste publicatiedatum in open bronnen en dus niet de 'startdatum' van de aanval. Deze is in sommige gevallen maanden of zelfs jaren eerder.

106 Verizon Data Breach Investigations report 2013.
107 Zie katern Cyberspionage.
108 http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
109 Zie bijvoorbeeld http://hackmageddon.com en http://csis.org/publication/cyber-events-2006 voor aanvullende overzichten van cyberspionage.



Diefstal van informatie voor financieel gewin

Criminelen stelen informatie voor het toebrengen van schade aan anderen of het onder druk zetten (chantage) van anderen. De verkregen informatie (bijvoorbeeld gebruikersnamen en wachtwoorden) kan bovendien een middel zijn voor de manipulatie van informatie.

Diefstal van informatie vindt vaak plaats vanaf met malware besmette computers, die eventueel onderdeel zijn van een botnet. De computers die onderdeel zijn van een botnet versturen de daarbij buitgemaakte informatie naar een centrale computer. In december 2012 ontving het NCSC informatie van onderzoeksbedrijven Digital Investigation en SurfRight over het Pobelka-botnet, op basis van data afkomstig van een C&C-server. Uit onderzoek van diverse partijen blijkt hoe divers de informatie is die buitgemaakt wordt en hoe gevoelig deze informatie in sommige gevallen is. Zie het verdiepingskatern Botnets voor meer informatie.

De informatie, zoals inlog- of creditcardgegevens, die criminelen buitmaken gebruiken zij voor andere aanvallen of verhandelen zij om direct financieel gewin te hebben. Er bestaan tal van ondergrondse websites waar gestolen informatie te koop kan worden aangeboden, zoals creditcardgegevens, e-mailadressen en andere persoonsgegevens.

Pobelka-botnet verzamelt informatie

Pobelka is een botnet dat net zoals Dorifel gebruikmaakt van het Citadel distributieplatform. Het primaire doel van Citadel-botnets is het manipuleren van financiële transacties. Alle overige gegevens die worden verzameld, kunnen beschouwd worden als 'bijvangst'. De buitgemaakte gegevens zijn persoonidentificerende gegevens, bedrijfsinformatie, informatie over de computer en kwetsbaarheden in de software gebruikt door de getroffen organisatie of persoon. Delen van deze bijvangst worden vaak ook, in bulk, gebruikt en soms voor grote bedragen doorverkocht. Persoonsidentificerende gegevens worden ook gebruikt voor identiteitsfraude of voor het misleiden van personen, bijvoorbeeld met social engineering.

De dreiging van diefstal van informatie door criminelen is 'hoog' geclassificeerd omdat zij op grote schaal informatie ontvreemden voor geldelijk gewin, bij zowel overheden, private organisaties als burgers.

Diefstal en publicatie van informatie met activistische doelen

De overige actoren (hacktivisten, cybervandalen en interne actoren) gebruiken de publicatie van gestolen gegevens om kwetsbaarheden inzichtelijk te maken, het eigen imago te vergroten of schade toe te brengen aan anderen.

Te denken valt aan publicatie van verkregen vertrouwelijke bedrijfs- of persoonsgegevens. Eenmaal 'gestolen' informatie kan op vele manieren en laagdrempelig worden gepubliceerd. De website 'pastebin.com' is daarvoor een veelgebruikt middel, omdat

daar anoniem informatie kan worden geplaatst. Zo publiceren kwaadwillenden veelvuldig bestanden met daarin gebruikersnamen en wachtwoorden van klanten van een bedrijf, veelal met een activistische motivatie.

Actoren kunnen toegang krijgen tot informatie door bijvoorbeeld in te breken op een website of database. Een voorbeeld hiervan is het Groene Hartziekenhuis, dat in verlegenheid werd gebracht omdat een hacker in staat was geweest medische dossiers van patiënten in te zien. Een andere digitale inbraak bij een medische instelling heeft betrekking op Diagnostiek voor U, bekend van de zaak Henk Krol. Digitale inbraken kunnen ook vanuit ideologische intentie plaatsvinden: in januari 2013 claimde een hackersgroep de digitale inbraak in een archiefcentrum van het Franse ministerie van Defensie[110] en pleegde ook inbraken in Azië[111].

Hackers hebben het bij uitstek gemunt op informatie over hoogwaardigheidbekleders, op 11 maart 2013 zijn bijvoorbeeld persoonlijke gegevens (onder meer financiële situatie) van o.a. Joe Biden (Amerikaanse vice-president) en Hillary Clinton gepubliceerd op de website exposed.su.

Opvallend is dat het aantal door NCSC afgehandelde incidenten met informatiediefstal bij de overheid afgenomen is in vergelijking met het vorige CSBN. De oorzaak hiervan kan zijn dat in de vorige periode veel aandacht bestond voor het publiceren van informatie met activistische motieven, bijvoorbeeld om beveiligingsproblemen aan te tonen. In de rapportageperiode is de aandacht daarvoor afgenomen. De dreiging van de publicatie van informatie door hacktivisten en cybervandalen wordt daarom op 'laag' geclassificeerd. De dreiging van publicatie van informatie door interne actoren wordt net als vorig jaar op 'midden' geclassificeerd.

6.1.2 *Manipulatie van informatie*

Waar bij diefstal van informatie onbevoegd toegang is verkregen tot informatie en deze wordt 'ontvreemd', gaat manipulatie een stap verder, omdat informatie onbevoegd wordt gemuteerd of zelfs vernietigd. Het gaat criminelen daarbij vooral om fraude met internetbankieren, gericht op geldelijk gewin.

Een aanzienlijke fraude was de diefstal van 45 miljoen via manipulatie van debit cards en de gekoppelde rekeningen.[112] Dit is de grootste fraude met geldautomaten die tot nu toe is gepleegd. In Nederland is de digitale fraude in 2012 gedaald (zie kader Daling fraude met skimming en internetbankieren). Deze manipulatie van informatie is geclassificeerd als 'hoog' omdat dit in Nederland voorkomt met de grootste impact op financiële instellingen. Gezien het toenemende gebruik en de toenemende waarde van (financiële) transacties via internet is het voor criminelen steeds interessanter om daar fraude mee te plegen.

Daling fraude met skimming en internetbankieren[113]
De Nederlandse Vereniging van Banken (NVB) rapporteerde in april 2013 een daling van de fraude met skimming en internetbankieren. In heel 2012 bedroeg de fraude met internetbankieren 34,8 miljoen euro, tegen 35 miljoen in 2011. Skimming nam nog verder af, van 38,9 miljoen in 2011 naar 29 miljoen in 2012. De invoering van de EMV-chip en beperking van werking van de magneetstrip op de pinpas tot Europa zijn belangrijke maatregelen geweest, aldus de NVB. Voor de fraude van internetbankieren signaleert de NVB een verschuiving van phishing naar specifieke trojan horses om computers te besmetten en over te nemen.

Manipulatie van informatie kan ook betrekking hebben op het wissen van informatie, zoals in het geval van de cyberaanval op het olieconcern Saudi Aramco. Hoewel de impact van het wissen van informatie groot kan zijn, is voor Nederland op dit vlak geen significante kwaadaardige dreiging gebleken.

Cybersabotage case Saudia Aramco[114]
In augustus 2012 werd bekend dat het Saoedische olieconcern Saudia Aramco slachtoffer was geworden van een cyberaanval met (vermoedelijk) de Shamoon-malware. Opvallend aan deze aanval was het destructieve karakter. Shamoon overschrijft namelijk bestanden op de computers waar het op terechtkomt, nadat deze bestanden naar een C&C-server van de aanvaller zijn gestuurd. Als gevolg van deze aanval moesten ruim 30.000 werkstations opnieuw worden opge-bouwd en bedrijfsnetwerken worden afgesloten van het internet. De productie van Saudia Aramco zou niet in gevaar zijn geweest.

6.2 Aanval gericht op ICT

Deze paragraaf onderscheidt drie dreigingssoorten die zijn gerelateerd aan aanval op ICT, te weten a) digitale bekladding, b) verstoring van ICT en c) overname van ICT.

110 'XTNR3VOLT Claims Hacking Of French Ministry Of Defense Website', Site monitoring service, 15-1-2013.
111 Voorbeelden: http://www.zdnet.com/ph/hackers-take-sabah-conflict-to-cyber-space-7000012061/, http://www.ehackingnews.com/2012/06/50-pakistani-sites-hacked-by-silent.html
112 voetnoot die we niet meer kunnen toevoegen: http://www.independent.co.uk/news/world/americas/gang-steals-45m-in-worlds-biggest-atm-fraud-8610833.html
113 Persbericht NVB, Scherpe daling fraude internetbankieren, 2 april 2013.
114 (http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work; http://www.securelist.com/en/blog/208193834/Shamoon_The_Wiper_further_details_Part_II); http://blog.seculert.com/2012/08/shamoon-two-stage-targeted-attack.html; http://www.bloomberg.com/news/2012-10-25/code-in-aramco-cyber-attack-indicates-lone-perpetrator.html. Tevens gebaseerd op commentaar op eerdere versie van reviewer.

6.2.1 *Digitale bekladding*

Digitale bekladding (defacement) is het onbevoegd en vaak met kwaadaardige intentie vervangen of beschadigen van de inhoud van een bestaande webpagina. Daarvoor moet de kwaadwillende zich toegang hebben verschaft tot een webserver, wat goed mogelijk is vanwege vele bekende kwetsbaarheden. In 2013 zijn in Nederland een aantal websites gedefaced omdat de contentmanagement software die was geïnstalleerd, verouderd was.[115]

Vooral hacktivisten, scriptkiddies en cybervandalen maken zich schuldig aan defacements. Een defacement is voor een hacktivist aantrekkelijk voor het maken van een publiek statement en om daarmee het slachtoffer (vaak een organisatie) in verlegenheid te brengen. Voor een scriptkiddie en cybervandaal gaat het om de lol en/of het aantonen dat het kan.

Defacements van websites blijken aan de orde van de dag: in de periode april 2012 tot en met maart 2013 zijn ongeveer 4.000 defacements op het .nl-domein in ZoneH teruggevonden, een site waar aanvallers dit soort defacements – en eventuele details – vaak registreren. In enkele gevallen was sprake van zogenoemde 'mass defacements' waarbij in één keer een groot aantal websites geautomatiseerd wordt aangevallen via dezelfde kwetsbaarheid bij een provider. Zo werd in april 2012 één IP-adres aangevallen waarop 2.789 websites geconfigureerd waren. De belangrijkste bij registratie op zone-h.org opgegeven redenen om een defacement uit te voeren, zijn: voor de lol (41 procent) en om de beste defacer te zijn (34 procent). In slechts 1 procent van de gevallen vindt de defacement plaats uit politieke overwegingen. Bij 20 procent van de defacements heeft de aanvaller geen reden opgegeven.

Enkele hackersgroepen hebben (voor zover bekend) in het najaar van 2012 naar aanleiding van *Innocence of Muslims*, de film die in het najaar van 2012 tot veel ophef leidde onder moslims, enkele tientallen willekeurige Nederlandse sites gedefaced. Ook zijn patriottische, hacktivistische groepen actief in conflictsituaties zoals in Syrië.[116]

De dreiging die van defacement uitgaat is als 'laag' geclassificeerd voor overheden en private organisaties omdat de impact ervan beperkt is tot imagoschade. Tevens zien we dat het middel van defacement door de actoren slechts in beperkte mate wordt aangegrepen.

6.2.2 *Verstoring van ICT*

De verstoring van ICT is erop gericht om de beschikbaarheid van de informatievoorziening, al dan niet langdurig, te schaden. Voor hacktivisten, cybervandalen, scriptkiddies en interne actoren zal verstoring van dienstverlening een doel op zich zijn, terwijl criminelen verstoring als basis of afleiding kunnen gebruiken voor aanvallen waarmee zij financieel gewin hebben. Terroristen kunnen verstoring van ICT gebruiken door het internet als wapen in te zetten tegen fysieke doelen of als ondersteuning voor hun terroristische activiteiten, zoals voor het voeren van propaganda (internet als middel).

Voor staten betreft het de verstoring van de ICT van een samenleving door de inzet van offensieve cybercapaciteiten door statelijke actoren. Effecten kunnen zich daarnaast ook buiten het cyberdomein voordoen, aangezien offensieve cybercapaciteiten op zichzelf al een machtsmiddel vormen in handen van staten die able and willing zijn deze in te zetten.

Een voorbeeld van een middel om ICT te verstoren zijn de DDoS-aanvallen (zie kader). Begin 2013 zijn DDoS-aanvallen uitgevoerd op verschillende organisaties in Nederland, zoals banken en een luchtvaartmaatschappij. De impact van deze aanvallen was beperkt tot het niet beschikbaar zijn van de dienstverlening van specifieke organisaties. Daarnaast zijn DDoS-aanvallen uitgevoerd op basisvoorzieningen. Het gaat bijvoorbeeld om aanvallen op iDeal, waardoor betalen bij webwinkels tijdelijk niet mogelijk was, en DigiD waardoor overheidsdiensten waarvoor inloggen noodzakelijk is, tijdelijk niet toegankelijk waren. Verstoring van deze basisvoorzieningen heeft een grote impact omdat alle diensten geraakt worden die daar gebruik van maken. Verder kan sprake zijn van gevolgen in een keten, bij het niet beschikbaar zijn van DigiD als gevolg van een aanval, kunnen bij de Belastingdienst bijvoorbeeld geen toeslagen worden aangevraagd. Het is niet altijd duidelijk welke actor achter een DDoS-aanval zit (het attributievraagstuk). De hiervoor benoemde DDoS-aanvallen in Nederland zijn waarschijnlijk het werk van criminelen, hacktivisten, scriptkiddies of cybervandalen.

(D)DoS-aanvallen

Denial of Service (DoS) of Distributed Denial of Service (DDoS) is de benaming voor een type aanval waarbij een actor een slachtoffer, bijvoorbeeld een onlinedienst, website of applicatie, probeert te saboteren door grote hoeveelheden berichten te versturen of op andere wijze te verzadigen of te laten crashen zodat het slachtoffer niet meer bereikbaar is. Het type aanval bestaat al meerdere jaren, maar nam het afgelopen jaar in aantallen en vooral in kracht, gebruikte bandbreedte, toe. In 2012 en de eerste maanden van 2013 hebben kwaadwillenden regelmatig gebruikgemaakt van DDoS-aanvallen om onlinedienstverlening te verstoren. Prominente 'slachtoffers' waren onder andere banken, luchtvaartmaatschappijen en overheidsdiensten. Met relatief beperkte middelen kan een groot effect worden bereikt. De intentie achter een DDoS-aanval is veelal wraak, sabotage, afpersing of gewoon 'voor de lol'.

115 https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2013-0026+1.00+Kwetsbaarheid+in+Joomla+component+comjce+actief+misbruikt.html

116 http://www.theregister.co.uk/2012/08/17/reuters_blogs_hacked_again/, http://www.informationweek.com/security/attacks/how-syrian-electronic-army-unpeeled-the/240154504

De hackersgroep die zich de 'Izz ad-Din al-Qassam Cyber Fighters' noemt, heeft vanaf september 2012 tot in ieder geval mei 2013 DDoS-aanvallen uitgevoerd op tal van vooral Amerikaanse banken. Uit de claims valt op te maken dat de acties een reactie zijn op de film *Innocence of Muslims* en de hackers kondigen aan door te gaan met deze acties totdat de film van het internet is verwijderd. Overigens stellen, volgens mediaberichten, Amerikaanse overheidsofficials dat Iran achter de aanvallen zit, hoewel niet alle veiligheidsexperts daarvan overtuigd zijn.[117]

Naast DDoS kunnen andere middelen, zoals malware, worden gebruikt om de werking van ICT te verstoren. Een bijzondere vorm van malware is ransomware, door criminelen ingezet om gebruikers te chanteren. De ransomware zorgt ervoor dat het systeem door de gebruiker niet meer functioneert. In CSBN-2 is al onderkend dat ransomware een grote rol speelt bij cybercrime direct gericht op eindgebruikers. Het gebruik hiervan is in de rapportageperiode fors toegenomen.

Ook zogenaamde industriële controle systemen (ICS) zijn kwetsbaar voor verstoring. Security van ICS is nog steeds een groot probleem, want industriële systemen zijn kwetsbaar en er gebeurt nog te weinig om dat goed op te lossen. Gelukkig ontbreekt het bij de actoren nog aan zowel motieven als capaciteiten, waardoor grote problemen tot op heden zijn uitgebleven. Zie het verdiepingskatern ICS voor nadere informatie.

De dreiging van verstoring van ICT wordt bij ieder van de actoren maximaal als 'midden' geclassificeerd. Vanwege de (mogelijke) impact van de DDoS-aanvallen op online diensteverlening is de dreiging voor private organisaties als 'midden' geclassificeerd.

6.2.3 *Overname van ICT*

Bij overname van ICT verkrijgt een actor de controle over ICT-systemen van een doelwit, met het doel om de resources te gebruiken. Deze misbruik onttrekt zich vaak aan de aandacht van de gebruiker omdat de kwaadwillende er baat bij heeft dat hij de resources kan blijven gebruiken. De overname van ICT kan een doel op zich zijn. De intentie hierachter voor hacktivisten is veelal wraak, chantage of sabotage. Scriptkiddies en cybervandalen kunnen ICT overnemen om kwetsbaarheden aan te tonen of doen het voor de lol. De overname is voor cybercriminelen een middel voor direct geldelijk gewin of inzet voor andere aanvallen.

De overname van ICT kan op een aantal manieren worden gerealiseerd, zowel geautomatiseerd als handmatig. Door malware kan een systeem gecompromitteerd worden waardoor kwaadwillenden het kunnen overnemen en het daarmee een middel is voor bijvoorbeeld diefstal of manipulatie van informatie, bitcoin mining, het versturen van SPAM of phishing mails en het hosten van informatie. Ook worden systemen overgenomen om te worden opgenomen in een botnet.

Websites die veel bezoekers trekken, zijn doelwit van criminelen om malware te verspreiden (zie kader Malware op legitieme websites: casus Telegraaf.nl). Advertentieplatformen zijn hierbij regelmatig doelwit, omdat via het platform de drukbezochte website malware verspreid.

Er wordt ook gesproken van overname wanneer apparatuur wordt misbruikt als middel voor een aanval. Zo suggereren mediaberichten dat telecommunicatieapparatuur van een Chinese fabrikant achterdeuren kan bevatten. Hierdoor zouden de netwerken die daar gebruik van maken, kwetsbaar zijn.[118] Tot slot is denkbaar dat procesbesturingssystemen, in het bijzonder ICS, worden overgenomen door kwaadwillenden. Doordat vooral kleinschalige procesbesturingssystemen onvoldoende beveiligd zijn, kan overname van dergelijke systemen relatief laagdrempelig zijn. Cyberonderzoekers tonen regelmatig aan dat ook in Nederland dergelijke systemen kwetsbaar zijn. Hoewel in Nederland overname van dergelijke systemen met kwaadaardige intentie in de praktijk nog niet merkbaar is geweest, maakt de kwetsbaarheid van deze systemen het risico van overname wel reëel.

De verwachting is dat de dreiging van overname van ICT toeneemt omdat het voor kwaadwillenden, vooral in de vorm van botnets, een bewezen en succesvol middel is. Overname van ICT van burgers door cybercriminelen is als 'hoog' geclassificeerd omdat zij deze als opstap gebruiken om informatie te stelen en om financiële transacties te manipuleren.

Malware op legitieme websites: casus Telegraaf.nl
Via de website telegraaf.nl is op donderdag 6 september 2012 kortstondig kwaadaardige software verspreid, waardoor de pc's van bezoekers van deze website werden aangevallen. Het doel van deze aanvallen was om deze pc's te besmetten met kwaadaardige software. Bezoekers met kwetsbare versies van Adobe- en Java-software geïnstalleerd op hun pc's, zijn besmet met Banking malware en ransomware.[119]

6.3 Uitval van ICT

Uitval van ICT tast de beschikbaarheid van ICT aan en vormt daardoor een dreiging. Uitval kan plaatsvinden door natuurlijke en technische gebeurtenissen of door menselijk falen. Zoals de storm Sandy in combinatie met een overstroming in de Verenigde Staten in oktober 2012 heeft aangetoond, kunnen natuurlijke gebeurtenis-

117 'Bank Hacking Was the Work of Iranians, Officials Say', The New York Times, 8-1-2013, 'Is Iran really behind recent stream of DDoS bank attacks?', Computer News Middle East, 13-01-2013.

118 'VS beschuldigt telecomreuzen Huawei en ZTE van corruptie', NRC Handelsblad, 9-10-2012.

119 http://hitmanpro.wordpress.com/2012/09/08/banking-trojan-keeps-hitting-the-dutch-hard/, http://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Virussen+en+wormen/WD-2012-080+Nieuwssite+telegraaf.nl+serveert+link+naar+malware.html

sen leiden tot uitval van ICT op grote schaal en gedurende lange tijd. Ook door technische gebeurtenissen en/of menselijk falen kan uitval van (een van de onderdelen) van ICT plaatsvinden met gevolgen voor de processen van een organisatie.

Ondanks zorgvuldig en professioneel beheersen van software en hardware en ondanks aandacht voor preventieve maatregelen, zijn incidenten en verstoringen niet helemaal te voorkomen. Ook als gevolg van de nog steeds toenemende complexiteit van systemen en het steeds intensievere gebruik is aannemelijk dat incidenten zullen optreden.

Daarnaast kan een aanval op een derde partij of uitval bij een derde partij waarvan een organisatie afhankelijk is, leiden tot grote gevolgen voor de eigen bedrijfsvoering (een voorbeeld van ketenbelangen). Outsourcing van taken levert kwetsbaarheden op in het geval de derde partij wordt aangevallen of te kampen heeft met uitval, zowel vanuit het oogpunt van kwetsbaarheid van leveranciers en klanten als in verband met het gevaar van mogelijke achterdeuren in hardware. De gevolgen van een aanval tegen en uitval bij een derde partij kunnen vergaand de direct getroffen organisatie overstijgen. Als gevolg daarvan kan een sector of zelfs een land getroffen worden. Zo hadden klanten van het bedrijf Cloudflare als gevolg van de DDoS-aanval op Spamhaus, klant van Cloudflare, eveneens last van die DDoS-aanval. Cloudflare levert namelijk (onder andere) diensten die websites beveiligen tegen (D)DoS-aanvallen.

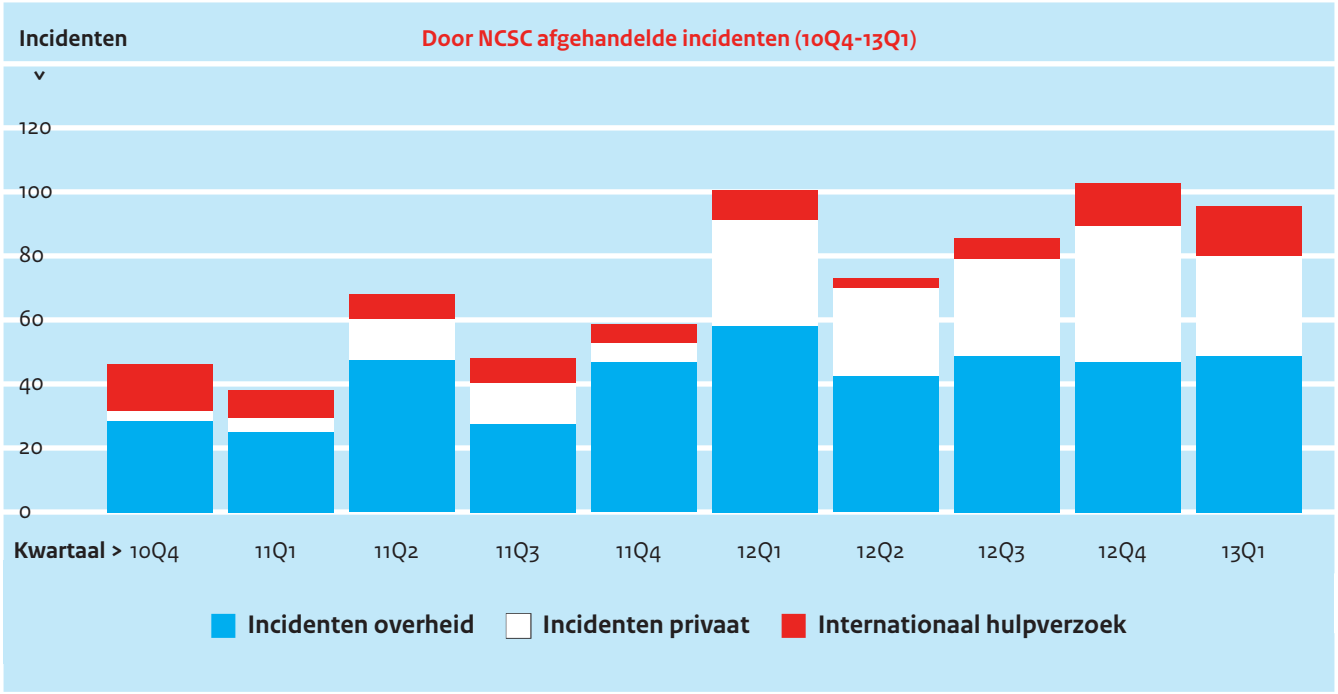
Omdat organisaties in toenemende mate maatregelen nemen om uitval van ICT te voorkomen, is de dreiging geclassificeerd als ‘laag’.

6.4 Door NCSC afgehandelde incidenten

Het NCSC ondersteunt overheden en organisaties in vitale sectoren bij het afhandelen van incidenten op gebied van ICT-veiligheid. In die rol worden bij het NCSC incidenten gemeld en worden incidenten en kwetsbaarheden ook door het NCSC zelf geïdentificeerd, bijvoorbeeld op basis van detectie. Daarnaast acteert NCSC op verzoek van internationale partijen met name richting internetserviceproviders om te ondersteunen bij het bestrijden van cyberincidenten in het buitenland, die hun oorsprong vinden in Nederland (bijvoorbeeld vanaf een webserver of vanaf geïnfecteerde pc’s in Nederland). Dit schaart NCSC onder de noemer ‘internationale hulpverzoeken’.

Het aantal door NCSC afgehandelde incidenten laat, zoals onderstaande figuur toont, de afgelopen kwartalen geen duidelijk stijgend of dalend beeld zien. Na een flinke afname in het tweede kwartaal van 2012 (↓ 27 incidenten ten opzichte van het eerste kwartaal) steeg het aantal incidenten in de resterende kwartalen van 2012 om vervolgens in het eerste kwartaal van 2013 weer te dalen. Het aandeel incidenten gemeld vanuit of betrekking hebbend op de overheid is gedurende de rapportageperiode van dit CSBN redelijk stabiel: tussen de 42 en 48 incidenten per kwartaal. De fluctuatie in incidenten wordt dus vooral veroorzaakt door incidenten die betrekking hebben op de private sector (28 tot 42 per kwartaal) en het aantal internationale hulpverzoeken (3 tot 14 per kwartaal).

Bij incidenten maakt het NCSC onderscheid tussen dreigingen, aanvallen en kwetsbaarheden. Kijkend naar de incidenten bij de overheid, zien we dat aanvallen ongeveer 75 procent van de incidenten uitmaken. Van de overgebleven dreigingen zien we het aandeel dreigingen afnemen (van 17 naar 5 procent) en het aandeel kwetsbaarheden toenemen (van 14 naar 20 procent).



Afname aantal security-incidenten bij SURFcert
SURFcert ziet bij aangesloten onderwijsinstellingen een afname van circa 16 procent in het aantal geregistreerde incidenten ten opzichte van 2011. Daar is geen specifieke oorzaak voor aan te wijzen, maar SURFcert ziet wel dat de instellingen steeds adequater kunnen reageren en ook meer preventieve maatregelen nemen. De aandacht in de pers voor dit soort incidenten speelt daarbij een rol, maar ook de kennisdeling via bijvoorbeeld de SURFnet Community van Incident Response Teams (SCIRT). Er is wel een toename in DDoS-aanvallen op aangesloten instellingen, voornamelijk RoC's, en af en toe ook op hogescholen en universiteiten.

6.5 Conclusie

De tabel op pagina 51 geeft een overzicht van de dreigingen die van de verschillende actoren uitgaat om de doelwitten 'overheden', 'private organisaties' en 'burgers' aan te vallen.

Belangrijke oorzaken voor het niveau van de dreigingen zijn enerzijds de groeiende afhankelijkheid van ICT en anderzijds de voortschrijdende innovatie van hulpmiddelen die ervoor zorgt dat actoren tot steeds meer in staat zijn én dat relatief krachtige hulpmiddelen ook minder onderlegde actoren de mogelijkheid geven om een succesvolle cyberaanval te plegen. Staten zijn in staat om geavanceerde hulpmiddelen te ontwikkelen en te gebruiken, terwijl cybercriminelen vooral bestaande hulpmiddelen doorontwikkelen. Cybercrime professionaliseert verder in het bieden van commerciële diensten voor het huren van hulpmiddelen voor cyberaanvallen en het wegsluizen van geld ('cybercrime-as-a-service'). Oude, bekende zwakheden blijven voor cybercriminelen een middel voor misbruik. Dit geldt ook voor hacktivisten, die vooral vertrouwen op (varianten van) DDoS en defacement. Botnets zijn ten slotte een belangrijk hulpmiddel voor verschillende actoren.

Voor overheden is de grootste dreiging momenteel gericht op het belang van de vertrouwelijkheid van informatie (met name tegen spionage) en continuïteit van onlinedienstverlening (incl. generieke voorzieningen) en eigen ICT. Deze dreiging komt uit verschillende hoeken: staten, beroepscriminelen, hacktivisten en cybervandalen/scriptkiddies.

Voor het bedrijfsleven gaat de belangrijkste dreiging uit van spionage gericht op concurrentiegevoelige informatie en van misbruik van financiële gegevens voor diefstal van geldelijke waarden. Dit gebeurt ook door manipulatie van informatie in de vorm van aanpassing van (bank)transacties. Daarnaast is voor bedrijven die vitale onlinediensten aanbieden ook verstoring van onlinedienstverlening een belangrijke dreiging die in het afgelopen jaar is toegenomen. Ook wordt bedrijfsinformatie van allerlei aard door meerdere groepen actoren gestolen voor eigen gebruik, publicatie of verkoop aan derden. Denk aan klantgegevens of informatie over de ICT-voorzieningen van bedrijven.

Burgers worden geraakt door identiteitsfraude en chantage. Burgers raken betrokken wanneer het hun gegevens betreft die worden gestolen, gepubliceerd, verkocht of misbruikt. Ook wanneer de ontvreemding van informatie rechtstreeks bij hen gebeurt, staan belangen als geld (schade door aanvallen op elektronisch bankieren), privacy, beschikbaarheid van onlinediensten en digitale identiteit op het spel. Burgers hebben vooral te kampen met het vrijwaren van hun eigen computers en elektronica van malware en ransomware. Burgers worden indirect geraakt wanneer zij betrokken raken bij een cyberaanval doordat hun eigen ICT onderdeel geworden is van een botnet.

Het aantal door NCSC afgehandelde incidenten is in de rapportageperiode sterk toegenomen. De voornaamste reden voor deze stijging is dat per 1 januari 2012 private partijen ook door het NCSC worden bediend. In de aard van de incidenten bij de overheid is een relatieve stijging te zien van malwareinfecties (+13 procent) en poging tot hacken (+5 procent).

Het bekend worden van het Pobelka-botnet heeft inzicht gegeven in de aanzienlijke aantallen besmette computers en de omvang van de gelekte gegevens van een dan toe onopgemerkt gebleven botnet. Waarschijnlijk zijn er veel meer niet-ontdekte botnets. Dit laat tevens zien dat de middelen die beschikbaar zijn voor detectie van dit soort aanvallen tekortschieten.

De afgelopen periode zijn basisvoorzieningen het doelwit geweest van aanvallen. Het gaat bijvoorbeeld om aanvallen op iDeal, waardoor betalen bij webwinkels tijdelijk niet mogelijk was, en DigiD waardoor overheidsdiensten, waarvoor inloggen noodzakelijk is, tijdelijk niet toegankelijk waren. «

Doelwitten			
Actoren (dreigers)	**Overheden**	**Private organisaties**	**Burgers**
Staten	Digitale spionage	Digitale spionage	Digitale spionage
	Verstoring ICT (inzet offensieve capaciteiten) ★	Verstoring ICT (inzet offensieve capaciteiten) ★	
Terroristen	Verstoring ICT	Verstoring ICT	
(Beroeps)criminelen	Diefstal en verkoop van informatie ★	Diefstal en verkoop van informatie ★	Diefstal en verkoop van informatie ★
	Manipulatie van informatie★	Manipulatie van informatie★	Manipulatie van informatie★
	Verstoring ICT	Verstoring ICT ⇧	
	Overname ICT	Overname ICT	Overname ICT
Cybervandalen en Scriptkiddies	Diefstal en publicatie van informatie ★	Diefstal en publicatie van informatie ★	Diefstal en publicatie van informatie ★
	Verstoring ICT	Verstoring ICT	
		Overname ICT ★	
Hacktivisten	Diefstal en publicatie van informatie ⇩	Diefstal en publicatie van informatie ⇩	Diefstal en publicatie van informatie ⇩
	Verstoring ICT	Verstoring ICT	Verstoring ICT ⇩
		Overname ICT ★	
	Digitale bekladding ★	Digitale bekladding ★	
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie	Diefstal en publicatie of verkoop verkregen informatie (chantage)	
	Verstoring ICT ★	Verstoring ICT ★	
Cyberonderzoekers	Verkrijging en publicatie van informatie	Verkrijging en publicatie van informatie	
Private organisaties		Diefstal van informatie (bedrijfsspionage) ⇧	
Geen actor	Uitval ICT ⇩	Uitval ICT ⇩	Uitval ICT ⇩

Tabel 4. Overzicht dreigingen en doelwitten

Legenda relevantie		
Laag	**Midden**	**Hoog**
Er worden geen nieuwe trends of fenomenen onderkend waar de dreiging van uitgaat. **OF** Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. **OF** Er hebben zich geen noemenswaardige incidenten van de dreiging voorgedaan in de rapportageperiode	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 duideljke ontwikkelingen die de dreiging opportuun maken. **OF** Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft. **OF** Incidenten hebben zich voorgedaan in Nederland.

Legenda wijzigingen: ⇧ dreiging is toegenomen ⇩ dreiging is afgenomen ★ dreiging/regel is nieuw

Verdiepingskaternen

1 Cybercrime

Cybercriminelen zijn een relevante factor in het veroorzaken van cybersecurity-incidenten. Aanvallen die organisaties en burgers treffen, bijvoorbeeld met malware of DDoS, dragen direct bij aan de beeldvorming dat de maatschappij kwetsbaar is op ICT-gebied. Gewone burgers worden steeds vaker slachtoffer van cybercrime.

1.1 Inleiding

Recente onderzoeken tonen aan dat burgers bijna even vaak slachtoffer zijn van hacken als van fietsendiefstal.[47: Stol 2013] Potentieel dreigt een verlies aan vertrouwen in het gebruik van internet. De rechtshandhaving op het internet wordt daarom toenemend belangrijk, zeker als sprake is van een verschuiving van criminaliteit, zoals bij bancaire fraude waar fysieke bankovervallen zeldzamer worden.

Ook in de media is het afgelopen jaar veel te doen geweest over cybercrime. Het gaat dan om criminaliteit waarbij ICT zowel middel als doel is van het gepleegde misdrijf. Enkele geruchtmakende zaken zorgden voor veel aandacht. Zo werd het Groene Hartziekenhuis in verlegenheid gebracht doordat een hacker in staat was geweest medische dossiers van patiënten in te zien. Verder zagen we in de afgelopen rapportageperiode toenemende aandacht voor DDoS-aanvallen op vitale infrastructuur en een verdere professionalisering en verharding van ransomware. Ook de uitbraak van Pobelka heeft tot veel headlines geleid.

In het politiedomein is het Team High Tech Crime (THTC) op landelijk niveau belast met de bestrijding van complexe, innovatieve en/of ondermijnende vormen van cybercrime met hoge maatschappelijke impact. Het THTC biedt onderdak aan de Electronic Crimes Taskforce (zie kader). Het overgrote deel van de cybercrime is geen hightechcrime en de opsporing daarvan is toegewezen aan de regionale eenheden van de politie.

Electronic Crimes Taskforce – Samenwerken om digitale bancaire fraude te bestrijden

De Electronic Crimes Taskforce (ECTF) is een samenwerking tussen (onder andere) de vier grote banken, de NVB, het OM en de politie. In dit 'bankenteam' wordt informatie en expertise samengebracht om criminaliteit te voorkomen en op te sporen. Het team is opgericht om digitale bancaire fraude effectiever te kunnen bestrijden, met name phishing en banking malware. Bij het ter perse gaan van dit CSBN was de ECTF betrokken bij vijftien onderzoeken naar digitale bancaire fraude. Sinds begin 2011 zijn – mede door de samenwerking via het ECTF – meer dan honderd verdachten aangehouden, waaronder ronselaars, katvangers en corrupte medewerkers van bedrijven.

1.2 Criminele actoren

Een belangrijke dimensie waarop cybercriminelen zich van elkaar onderscheiden, is het niveau van hun kennis en vaardigheden. De motor van nieuwe ontwikkelingen op het gebied van cybercrime is een relatief kleine groep specialisten binnen de totale subjectenpool. Een uitzonderlijk hoog niveau van kennis en expertise stelt hen in staat geavanceerde aanvallen te ontwikkelen.

Gesloten criminele netwerken kennen steeds meer geharde professionals. Hedendaagse cybercriminelen zijn internationaal actief en lijken in toenemende mate verbonden te raken met georganiseerde 'analoge' criminaliteit. Door het heimelijke karakter van hun handelingen is het niet mogelijk om een schatting te geven van het aantal cybercriminelen dat actief is.

Cybercriminelen handelen meestal niet alleen: ze houden, met name online, contact om tactieken uit te wisselen en van elkaars expertise en middelen gebruik te maken. Deze samenwerking stelt criminelen ook in staat om zich te specialiseren in een bepaald onderdeel van een crimineel proces. Steeds vaker maken criminelen gebruik van middelen om relatief anoniem te surfen, zoals Tor, en om te betalen zonder identificatie, zoals met bitcoins.

Niet alleen de professionele cybercriminelen veroorzaken schade, ook scriptkiddies, hackers met beperkte kennis die gebruikmaken van technieken en hulpmiddelen die door anderen zijn bedacht en ontwikkeld, veroorzaken in toenemende mate maatschappelijke schade.

Een specifieke groep wordt gevormd door de ondersteuners, wiens dienstverlening bedoeld dan wel onbedoeld cybercrime faciliteert. Deze ondersteuners helpen met hun diensten Nederland tot doorvoerland van cybercrime te maken. Het gaat dan vooral om hostingproviders en aanbieders van virtuele betalingen. Hier zijn legitieme providers actief die onbewust criminaliteit faciliteren,

maar ook 'bulletproof' providers die dit bewust doen en bedrijven die in het schemergebied opereren. Internationale aanbieders van virtuele betalingen worden veelvuldig door (hightech)criminelen gebruikt vanwege de snelheid en anonimiteit.

1.3 Door criminelen gebruikte hulpmiddelen

In de werkwijze van criminelen heeft in de rapportageperiode geen substantiële verandering plaatsgevonden. Wel worden criminelen agressiever in hun handelen. Een voorbeeld hiervan is het automatisch downloaden en tonen van kinderporno in ransomware.
Botnets blijven een geliefd hulpmiddel om veel geld te verdienen. Er wordt meer gebruikgemaakt van malware om computers over te nemen en minder van phishing om inloggegevens te bemachtigen. In CSBN-2 is al onderkend dat ransomware een grote rol speelt bij cybercrime direct gericht op eindgebruikers. Het gebruik hiervan is in de rapportageperiode fors toegenomen, evenals de inzet van encryptie om opsporing te bemoeilijken.

Botnets

Botnets, clusters van op afstand bestuurbare geïnfecteerde computersystemen, zijn aanhoudend de belangrijkste bouwsteen van cybercrime. Een belangrijke eigenschap is dat botnets dusdanig zijn opgezet dat ze moeilijk uit de lucht zijn te halen. Zie het verdiepingskatern over botnets voor informatie over de werking van botnets en actuele cases zoals Pobelka.
Het verdienmodel van een botnetbeheerder bestaat onder meer uit het verhuren van zijn botnet voor uiteenlopende diensten. Zo worden botnets met een omvang van 100.000 bots te huur aangeboden voor grootschalige aanvallen voor enkele honderden dollars per etmaal.

Malware

Veel malware richt zich op het achterhalen van financieel relevante gegevens. Een belangrijke categorie van malware zijn de banking trojans. Deze zijn erop gericht om misbruik te maken van de internetbankieromgeving van de eigenaar van het systeem.
Het komt er vaak op neer dat de malware de inloggegevens van de betreffende gebruiker probeert te achterhalen of ongemerkt digitale overschrijvingen probeert te manipuleren.

Encryptie en cloud

Voor de opsporing is een complicerende factor de toename van encryptie op zowel communicatie als bestandsopslag. De groei van het gebruik van clouddiensten brengt naast technische ook juridische uitdagingen met zich mee, onder meer op het gebied van jurisdictie.

Ransomware

Sterk in opkomst binnen het aandachtsgebied cybercrime is de verspreiding van zogeheten ransomware. In CSBN-2 is al gesignaleerd dat ransomware in opkomst was. Ransomware kaapt functionaliteit van het besmette systeem, bijvoorbeeld door het versleutelen van bestanden of het blokkeren van de werking van het besturingssysteem. De malware eist een betaling van de gebruiker om de geblokkeerde functionaliteit te herstellen (wat vervolgens zelden gebeurt) en zet de gebruiker doorgaans onder druk om geen aangifte te doen.

Professionalisering ransomware
De professionaliteit van ransomware neemt zienderogen toe. Criminelen maken gebruik van encryptie en virtueel geld om onder de radar te blijven. Ook de impact op het slachtoffer neemt toe. Criminelen schuwen geen middel om de gebruiker te bewegen wél te betalen, maar géén aangifte te doen. Bijvoorbeeld door het gebruik van politielogo's, de weergave van daadwerkelijke kinderporno en het aanzetten van opname-apparatuur van de computer waarbij de gebruiker zelf getoond wordt. Onder de verkeerde omstandigheden kan een besmetting met ransomware, zoals elke vorm van malware, op het reguliere internet worden opgelopen. Meer nog dan hacken, skimmen en fraude met internetbankieren raakt dit direct het veiligheidsgevoel van individuele burgers.

Na de eerste verschijnselen in 2009 in Rusland en Oost-Europa heeft ransomware zich inmiddels verspreid naar West-Europa, de Verenigde Staten en vele andere landen.

1.4 Uitdagingen bij de opsporing van cybercrime

Het onderscheid tussen hightechcrime en 'reguliere' cybercrime heeft grote invloed op de opsporingspraktijk. Daarom is het zeer waardevol om te investeren in het opsporen en vervolgen van hightechcrime. De schaal waarop de effecten van deze vorm van cybercrime zich manifesteren, is immers groot. Ook nemen minder kundige aanvallers de hulpmiddelen en werkwijze van deze criminelen vaak over. Tegelijkertijd vraagt deze opsporing van de politie een relatief grote investering in mensen, middelen en expertise.

Naast operationele beperkingen gelden er ook technische complicaties bij het digitale recherchewerk. Dadersporen die naar het buitenland leiden (zoals het IP-adres) kunnen tot jurisdictievraagstukken leiden. Ook gebruiken daders in toenemende mate software om hun locatie volledig te verhullen: een populair voorbeeld is Tor. Een nieuw fenomeen is dat data van een verdachte in toenemende mate in de cloud te vinden is. Koops [57: WODC 2012] onderzocht de gevolgen van de cloud voor de opsporing en vervolging. Zijn voornaamste conclusie is dat de cloud geen geheel nieuwe problemen oplevert, maar wel alle bestaande juridische en technische aspecten op scherp zet.

Om deze problemen het hoofd te kunnen bieden, heeft de minister van Veiligheid en Justitie in mei 2013 een voorstel gedaan voor het uitbreiden van opsporingsbevoegdheden omtrent het binnentreden van systemen die via internet te benaderen zijn. Deze bevoegdheden voorzien ook in het geval dat geheel onbekend is wat de fysieke locatie is van het systeem.

Een ander probleem van technische aard bij de opsporing van cybercrime is het gebruik van encryptie, zowel bij communicatie als

bij opgeslagen data. De kwaliteit hiervan is zodanig dat kundig versleutelde data niet altijd zonder medewerking van de eigenaar te ontsleutelen is. Ook bij het onderzoeken van inbeslaggenomen systemen vormt encryptie een probleem. In het kader van opsporingsonderzoek bestaat de bevoegdheid al om aan derden te bevelen tot decryptie van versleutelde informatie. De minister van Veiligheid en Justitie heeft aangekondigd te komen met een wetsvoorstel dat eveneens in mei 2013 in consultatie is gegaan. Het gaat om uitbreiding van de opsporingsbevoegdheden en het stellen van meer expliciete kaders voor bestaande bevoegdheden.

1.5 Wat zijn de gevolgen/kosten van cybercrime?

Op basis van onderzoeken kan geconcludeerd worden dat het slachtofferschap van cybercrime aanzienlijk is: de omvang wordt steeds beter aantoonbaar, het vormt een groot deel van de criminaliteit en is waarschijnlijk toenemend. In recent onderzoek door W. Stol[47: Stol 2013] is nagegaan wat de mate is waarin burgers slachtoffer worden van cybercrime. Het bleek dat dit frequent aan de orde was: er gaven bijna net zoveel burgers (van 15 jaar en ouder) aan slachtoffer te zijn geworden van hacken (4,3 procent) als van fietsdiefstal (4,8 procent). Ook de Veiligheidsmonitor 2012[120] rapporteert over slachtofferschap op het gebied van cybercrime: de daarin genoemde aantallen zijn iets hoger dan die in het eerdergenoemde onderzoeksrapport (bijvoorbeeld 6 procent voor hacken).

Om uiteenlopende redenen is het beeld over slachtofferschap van cybercrime niet volledig. Bedrijven die worden aangevallen vrezen reputatieschade als ze aangifte doen en burgers doen vaak geen aangifte als ze het slachtoffer worden van een delict (13,4 procent van de slachtoffers van een digitaal delict doet aangifte). Cybercrime wordt door de politie niet apart geregistreerd, wat het lastig maakt een volledig beeld te schetsen van het aantal aangiftes. Wel kan op basis van de beschikbare gegevens worden gesteld dat het aantal aangiftes de afgelopen jaren sterk is toegenomen.

De financiële gevolgen van cybercrime kunnen voor bedrijven en overheden divers en vergaand zijn. Burgers merken onder meer de gevolgen van identiteitsfraude bij internetbankieren en skimming. De afgelopen jaren is het totale bedrag dat langs deze weg is ontvreemd, steeds gestegen.[bron: CSBN-2] In 2012 is daar voor het eerst verandering in gekomen. De totale fraude in het betalingsverkeer was in 2012 11 procent lager dan in 2011 en kwam uit op 82 miljoen euro.De fraude door skimming is met ruim een kwart gedaald van 38,9 tot 29 miljoen euro. De fraude met internetbankieren bleef met 34,8 miljoen euro ongeveer gelijk (35,0 miljoen in 2011).[37: NVB 2013] Het grootste gedeelte daarvan kwam voor rekening van het eerste halfjaar (24,8 miljoen euro).

Drie mogelijke verklaringen voor de daling in fraude door skimming zijn effectievere monitoringssystemen van banken, de invoering van de EMV-chip (ter vervanging van de misbruikgevoelige magneetstrip) en het standaard blokkeren van betaalpassen buiten Europa (geoblocking). Ook de komst in 2011 van de Electronic Crimes Task Force (ECTF) werpt zijn vruchten af.

Team High Tech Crime

Na een ruime capaciteitsverdubbeling van 30 naar 63 fte gedurende het afgelopen jaar staat het Team High Tech Crime (THTC) van de politie wederom aan de vooravond van een uitbreiding. In 2014 is hier 119 fte aan digitaal, tactisch en financieel hoogopgeleid personeel actief om hightechcrime effectief te bestrijden. Om tot een effectieve aanpak te komen van ransomware, aanvallen op vitale infrastructuren en andere hightechcrime werkt het THTC samen met nationale en internationale publieke en private partners. Dat gebeurt onder andere door het doen uitgaan van rechtshulpverzoeken en middels spoedafspraken via het wereldwijde '24/7-network', dat voor alle landen die partij zijn in het internationale Cybercrimeverdrag directe response garandeert in geval van behoefte aan acute assistentie.

120 http://veiligheidsmonitor.nl/dsresource?objectid=325461

2 Cyberspionage

De omvang en structurele wijze waarop digitale spionage wordt toegepast vormt een grote dreiging voor de nationale veiligheid en economie. In de afgelopen rapportageperiode zijn diverse publieke en private organisaties in Nederland hier slachtoffer van geworden. Hoewel de herkomst van digitale spionage zelden onomstotelijk vastgesteld kan worden, zijn er diverse aanwijzingen voor betrokkenheid van staten.

2.1 Inleiding

In het voorgaande CSBN is reeds benoemd dat digitale spionage een grote dreiging is voor de overheid en het bedrijfsleven in zowel Nederland als de rest van de wereld. In de afgelopen rapportageperiode hebben de inlichtingendiensten AIVD en MIVD vastgesteld dat deze dreiging onverminderd groot en actueel blijft. De maatschappelijke aandacht voor deze dreiging wordt ook steeds groter. Dit wordt mede ingegeven door toenemende mediaberichtgeving over aansprekende incidenten. Zo is er recent veel aandacht geweest voor de analyse van het commerciële onderzoeksbureau *Mandiant*, over de vermeende betrokkenheid van het Chinese leger bij wereldwijde digitale spionageactiviteiten.

In dit verdiepingskatern geven de AIVD en MIVD meer openbaarheid over hun onderzoeksresultaten op het vlak van digitale spionage en de dreiging die hiervan uitgaat voor Nederland en de operaties van de Nederlandse krijgsmacht. Steeds vaker worden daarbij specifieke actoren en dreigingen genoemd. Vanwege wettelijke bepalingen en de beschikbare capaciteit kunnen de AIVD en MIVD maar een deel van de alomvattende cyberspionagedreiging richting Nederlandse belangen waarnemen, onderzoeken en openbaren.

2.2 Cyberdreiging afkomstig van staten

2.2.1 *Doelwitten*

Digitale spionage door staten, dan wel gesteund, toegestaan of met de staat als uiteindelijke begunstigde, vormt een grote dreiging voor de Nederlandse economie en de nationale veiligheid. Staten steunen of tolereren dat digitale spionage plaatsvindt jegens Nederlandse bedrijven, organisaties en personen om politieke, financiële, technisch-wetenschappelijke, economische en militaire informatie te vergaren.

De MIVD constateert dat de defensie-industrie een gewild doelwit is op het gebied van cyberspionage. Informatie verkregen door spionage op deze industrie dient nog immer de militaire, diplomatieke en economische belangen van staten. Verkregen informatie kan bijdragen aan het verkrijgen van inzicht in de militair-technische capaciteiten van de Nederlandse krijgsmacht en zijn bondgenoten. Een operationeel voordeel kan teniet worden gedaan indien technische details van wapensystemen zijn gelekt middels (digitale) spionage. In potentie kan cyberspionage de paraatheid en inzetbaarheid van de krijgsmacht zeer schaden. Het is bekend dat actoren in het cyberdomein veelvuldig op netwerken van verschillende bedrijven in de defensie-industrie proberen in te breken met als doel gevoelige informatie over lopende projecten buit te maken.

Zo heeft de Amerikaanse defensietoeleverancier Lockheed Martin in november 2012 aangegeven dat het aantal digitale aanvallen op haar netwerken de afgelopen jaren drastisch is gestegen. Een deel van deze dreigingen wordt beschouwd als 'advanced persistent threat' (APT), met andere woorden langdurige en gerichte aanvallen door staten of goed georganiseerde groepen die informatie trachten te stelen. De MIVD doet onderzoek naar digitale aanvallen op de Nederlandse defensie-industrie om zodoende digitale spionage richting deze sector te duiden en te voorkomen. Daarnaast hebben de ontwikkelingen van digitale aanvallen op de defensie-industrie wereldwijd de aandacht van de MIVD indien deze de Nederlandse belangen kunnen schaden.

De MIVD beschikt voorts over aanwijzingen dat de cyberspionagedreiging zich niet alleen rechtstreeks richt op de defensie-industrie, maar ook op partijen met wie de defensie-industrie samenwerkt, zoals financiële instellingen, patentkantoren, advocatenkantoren of consultancyfirma's. Met dergelijke externe partijen wordt soms gevoelige bedrijfsinformatie gedeeld, terwijl het beheer over de afscherming van deze informatie niet altijd volledig in eigen hand is. Uit de modus operandi van daders van cyberspionage blijkt dat deze kwetsbaarheid daadwerkelijk wordt benut en 'derde partijen' een gewild doelwit zijn voor het ontvreemden van gevoelige bedrijfsinformatie.

De MIVD constateert kwaadaardige phishingactiviteiten richting Nederlandse militaire vertegenwoordigingen in het buitenland, waarbij aannemelijk is dat een Aziatische statelijke actor betrokken en/of uiteindelijke begunstigde is. Voor buitenlandse mogendheden is digitale spionage, naast klassieke spionagemethodieken, een in potentie zeer effectief en 'veilig' middel om de hand te leggen op vertrouwelijke informatie bij dergelijke sleutelfunctionarissen.

Echter, bedrijven uit andere sectoren zoals petrochemie, elektronica, farmacie, etc. evenals (inter)nationale overheidsinstellingen, kennisinstellingen en NGO's zijn slachtoffer van digitale spionageactiviteiten door staten of daaraan verbonden actoren. Deze partijen kunnen ook aangevallen worden via zakelijke dienstverleners en overige derden. Dit kan leiden tot tastbare schade voor de Nederlandse economie als geheel.

2.2.2 *Actoren*

De AIVD heeft het afgelopen jaar spionageaanvallen op Nederlandse civiele organisaties dan wel via de Nederlandse ICT-infrastructuur vastgesteld vanuit onder meer China, Rusland, Iran en Syrië. Deze worden hierna verder toegelicht. Echter, ondermeer gezien de wereldwijde omvang van digitale spionage-incidenten is het aantal incidenten in Nederland vermoedelijk vele malen hoger.

China

Er zijn wereldwijd diverse grootschalige Chinese aanvallen onderkend die zich ondermeer richten op overheidsinstellingen, dissidentenorganisaties, NGO's, kennisinstellingen en bedrijven uit diverse sectoren. Er zijn aanwijzingen dat binnen China diverse actoren als het leger, hackersgroepen, onderwijsinstellingen, inlichtingen- en veiligheidsdiensten te relateren zijn aan deze aanvallen. Deze aanvallen hebben als doel het verkrijgen van militaire en economisch relevante informatie. Ook in Nederland zijn het afgelopen jaar diverse aanvallen geconstateerd op bedrijven, dissidentenorganisaties, overheids-en kennisinstellingen waarvan de kenmerken richting China wijzen.

De AIVD verricht onderzoek naar een grootschalige digitale aanval op een sector die hoogwaardige technologische toepassingen ontwikkelt voor economische en militaire doeleinden. Bedrijven uit deze sector in Europa, Amerika en Azië zijn doelwit van de aanval. Bij diverse bedrijven in verschillende landen heeft de aanvaller toegang weten te krijgen tot een bedrijfsnetwerk. Deze bedrijfsnetwerken zijn lange tijd ongemerkt onderzocht en grote hoeveelheden hooggespecialiseerde, vertrouwelijke informatie zijn door de aanvaller bemachtigd.

Naast bedrijven zijn ook Nederlandse overheidsinstanties, in Nederland gevestigde NGO's en intergouvernementele organisaties doelwit van digitale aanvallen afkomstig uit China geweest.
Uit onderzoek van de AIVD naar een grootschalige internationale digitale aanval die gericht is op verschillende intergouvernementele organisaties, is gebleken dat deze aanvallen worden uitgevoerd door e-mails met malware te versturen aan medewerkers van deze organisaties. Om de kans te vergroten dat de e-mails door de geadresseerden geopend worden, worden ze verstuurd vanaf vervalste e-mailadressen die eruitzien als de adressen van vertrouwde (overheids)instellingen waarmee de getroffen organisaties banden onderhouden. De onderwerpen en bijlagen van deze mails ogen authentiek en sluiten aan bij de actualiteit en werkzaamheden van de getroffen medewerkers.

Hoewel hiervoor geen sluitend bewijs is, suggereren de omvang, tijdsduur, doelwitkeuze en professionele opzet van bovengenoemde aanvallen, een van overheidswege geïnitieerde of gesponsorde aanval. Gezien het gebruik van Chinese domeinnamen en IP-adressen en in de malware aangetroffen Chinese tijd- en taalinstellingen, is het waarschijnlijk dat de aanvaller uit China afkomstig is of dit wil suggereren.

De AIVD en MIVD schatten de cybercapaciteiten uit China momenteel in als groot. Hoewel actoren uit China veelvuldig gebruikmaken van relatief eenvoudige digitale spionagemiddelen, zijn de aanvallen op bovengenoemde (Nederlandse) doelwitten dermate grootschalig, structureel en vasthoudend van aard dat hier een permanent grote dreiging van uitgaat. Tevens maken Chinese actoren gebruik van de Nederlandse ICT-infrastructuur voor digitale spionageaanvallen op andere landen. Gezien de toename van het aantal aan Chinese actoren te relateren digitale spionageaanvallen en de toename van het aantal bij deze aanvallen betrokken Chinese actoren, neemt deze dreiging toe.

Rusland

De digitale inlichtingenactiviteiten van actoren die te relateren zijn aan Rusland richten zich op overheidsinstanties (vooral ministeries van defensie en buitenlandse zaken), internationale organisaties (vooral de NAVO), defensietoeleveringsbedrijven, het bankwezen, de energiesector en Russische dissidenten. In het afgelopen jaar zijn vooral aan Russische actoren toe te schrijven digitale aanvallen op buitenlandse overheidsinstanties waargenomen. De AIVD heeft ook geconstateerd dat Nederland doelwit was van aan Rusland toe te schrijven digitale aanvallen.

De AIVD en MIVD schatten de cybercapaciteiten vanuit Rusland momenteel in als groot. De onderkende aanvallen zijn professioneel uitgevoerd met unieke, geavanceerde malware, waardoor zij lastig zijn te onderkennen. De met deze malware gestolen data getuigt van een spionagemotief. Gezien de doelwitkeuze en de geavanceerde opzet van deze aanvallen is het aannemelijk dat de Russische autoriteiten bij deze aanvallen zijn betrokken.
De Russische digitale inlichtingenactiviteiten vormen een reële dreiging voor Nederland.

Iran

De cyberactiviteiten van de Iraanse overheid richten zich primair op digitale controle en inlichtingenvergaring ten aanzien van eigen burgers. De Iraanse overheid heeft het binnenlandse internetverkeer praktisch volledig onder controle waarbij men zich vooral richt op opposanten van het regime.

Uit AIVD-onderzoek is gebleken dat Iran zich de laatste jaren sterker is gaan richten op disruptieve cyberactiviteiten gericht tegen het buitenland. Een voorbeeld dat waarschijnlijk aan Iran is toe te schrijven, betreft de aanvallen met behulp van de zogenaamde Mahdi-malware medio 2012. Dit virus wordt verspreid door middel van gerichte e-mails met geïnfecteerde bijlagen. Ondanks het feit dat de bijlagen bij antivirussoftware tot een viruswaarschuwing leiden, hebben wereldwijd enkele honderden personen het bestand toch geopend. De Mahdi-malware lijkt een tweeledig doel te hebben: het bespioneren van personen, bedrijven en organisaties in Iran zelf en buiten Iran (met name Israël). Mede gezien het geringe aantal infecties in Nederland is het onwaarschijnlijk dat Nederland specifiek een doelwit is geweest van deze malware. Gezien de doelwitkeuze is het aannemelijk dat de Iraanse overheid op enigerlei wijze bij deze aanval betrokken is geweest.

Daarnaast worden vanuit Iran vele defacements en DDoS-aanvallen op websites van binnen- en buitenlandse opposanten van het Iraanse regime uitgevoerd en is de inschatting dat deze met medeweten van de Iraanse overheid worden uitgevoerd. Een voorbeeld hiervan betreft een defacementaanval begin 2012 op diverse Azerbeidjaanse overheidswebsites, waarbij ondermeer misbruik werd gemaakt van Nederlandse ICT infrastructuur. Op de beginpagina's van deze websites werden door de hackers opruiende en religieus getinte afbeeldingen en teksten geplaatst waarin stelling werd genomen tegen de vermeende nauwe banden tussen Israël en de huidige Azerbeidjaanse regering. De hackers riepen tevens op tot het starten van een 'Arabische Lente' in Azerbeidjaan. Er zijn aanwijzingen dat er Iraanse hackers betrokken waren bij de uitvoering van deze aanval.

De AIVD en MIVD schatten de cybercapaciteiten uit Iran momenteel in als gemiddeld, maar dat Iran tevens bezig is deze verder te ontwikkelen. Iran heeft een jonge hoogopgeleide bevolking, ook op technisch gebied. Er zijn thans geen aanwijzingen dat deze capaciteiten zich specifiek richten op Nederland. Bij een oplopende spanning tussen Iran en Nederland kunnen deze capaciteiten in theorie ook op Nederland gericht worden. Iraanse actoren maken voor hun cyberdoeleinden misbruik van digitale kwetsbaarheden in systemen en van de internationale infrastructuur, waaronder ook in Nederland.

Syrië

De Syrische digitale inlichtingenactiviteiten zijn met name gericht op het intimideren van Syrische dissidenten en het verstoren van hun communicatie. De AIVD stelt vast dat de Syrische overheid hiervoor onder meer een groep patriottische hackers lijkt in te zetten verenigd in het Syrian Electronic Army (SEA). Zij voeren vooral digitale aanvallen uit op websites en sociale mediasites van dissidenten in binnen- en buitenland, waaronder in Nederland. Ook heeft het SEA dergelijke aanvallen uitgevoerd op sites van wereldleiders, beroemdheden, overheidsinstellingen, mensenrechten- en nieuwsorganisaties die zich negatief hebben uitgelaten over de Syrische autoriteiten. Tevens zijn willekeurige Nederlandse websites aangevallen en van pro-Syrische boodschappen voorzien.

Naast het intimideren van dissidenten trachten de Syrische autoriteiten ook met relatief eenvoudige malware de activiteiten van dissidenten te bespioneren. Dergelijke aanvallen zijn vooralsnog niet in Nederland waargenomen. De dreiging voor in Nederland woonachtige Syrische dissidenten blijft thans beperkt tot digitale intimidatie (DDoS en defacements).

2.3 Conclusie

De grootste cyberspionagedreiging tegen Nederlandse belangen gaat momenteel uit van actoren die te relateren zijn aan China, Rusland, Iran en in mindere mate Syrië. De huidige cyberspionagedreigingen die een gevaar voor de nationale veiligheid vormen, zijn omvangrijk. Naar verwachting zullen deze cyberdreigingen in de nabije toekomst verder toenemen. Een aantal ontwikkelingen ligt onder meer ten grondslag aan deze verwachting:

- De samenleving zal nog afhankelijker worden van via internet gekoppelde, complexe systemen en netwerken. Deze afhankelijkheid leidt tot een toenemende kwetsbaarheid.
- De weerstand tegen dergelijke kwetsbaarheden is bij veel (potentiële) doelwitten gering en zal door de toenemende ICT-complexiteit naar verwachting eerder af- dan toenemen.
- De huidige en toekomstige ICT-ontwikkelingen gaan dermate snel dat de wet- en regelgeving nog verder zal gaan achterlopen.
- Door bovenstaande ontwikkelingen zal het gemak en het succes waarmee ongewenste cyberactiviteiten kunnen worden uitgevoerd, verder toenemen. Het gemak en succes wordt onder meer bepaald door het bereik van een digitale aanval, de snelheid en de geringe kosten waarmee een dergelijke aanval kan worden uitgevoerd en de toenemende mogelijkheid om (bijna) volledig anoniem te opereren. «

De AIVD en MIVD investeren in cybersecurity

De AIVD en MIVD onderzoeken digitale aanvallen die de nationale veiligheid, de democratische rechtsorde, de bevordering van de internationale rechtsorde of andere gewichtige belangen van staat aantasten. Daartoe behoren ook digitale aanvallen die leiden tot maatschappelijke ontwrichting of die de economische veiligheid schaden. De AIVD richt zich primair op digitale spionage, sabotage en terrorisme. De MIVD richt zich primair op militair relevante dreigingen en ontwikkelingen in het digitale domein, zoals cyber in relatie tot gewapende conflicten, digitale aanvallen tegen de defensie-industrie en het waarborgen van de doeltreffende inzet van de krijgsmacht. Een belangrijke taak is ook het verhogen van de weerbaarheid tegen digitale aanvallen bij overheid en vitale sectoren. De AIVD en MIVD werken nauw samen in de op te richten sigint/cybereenheid Symbolon en wisselen kennis uit met buitenlandse inlichtingen- en veiligheidsdiensten. Beide diensten werken bovendien samen met het NCSC en het THTC.

3 Botnets

Botnets blijven voor cybercriminelen een geliefd hulpmiddel om geld te verdienen, waardoor er een levendige ondergrondse economie rondom het hulpmiddel is ontstaan. De combinatie van de lage detectie en anderzijds de grote gevolgen die kunnen voortkomen uit de inzet van botnets, vereist een gerichte aanpak.

3.1 Inleiding

In dit verdiepingskatern wordt nader ingegaan op de problematiek van botnets. Het schetst een beeld van de actuele situatie en de uitdagingen waarvoor antivirusindustrie en opsporingsinstanties staan bij het voorkomen en bestrijden van botnets.

Een botnet is een netwerk van samenwerkende apparaten, meestal privé- of bedrijfscomputers, de zogeheten 'bots', die met dezelfde malware zijn besmet. Daarnaast komt het – echter in mindere mate – voor dat servers, routers, mobiele telefoons en dergelijke besmet zijn. Criminelen kunnen een botnet centraal aansturen om de bots voor eigen doeleinden in te zetten.

Om een apparaat op te nemen in een botnet wordt specifieke malware gebruikt die zo min mogelijk opvalt voor de gebruiker, omdat het voor de criminelen van belang is dat de bot zo lang mogelijk blijft functioneren. Daarom zal een gebruiker doorgaans weinig merken van een besmetting.

3.2 Achtergrond

3.2.1 *Actoren achter botnets*

Het opzetten, beheren en exploiteren van een botnet is doorgaans geen eenmanszaak. Criminelen werken samen en nemen elk een deel op zich, verhandelen hun producten en diensten en concurreren levendig met elkaar.[13: FS 2013]

Om een botnet op te zetten is als eerste specifieke botnetmalware nodig om apparatuur te infecteren en op te nemen in een botnet. De malware wordt door een ontwikkelaar gemaakt en maakt eventueel gebruik van een of meer gekochte kwetsbaarheden en exploits. De malwareontwikkelaar kan ervoor kiezen om de malware zelf te verspreiden of om zijn malware te verkopen aan criminelen.

Criminelen zetten botnets in voor een ruim palet aan activiteiten, waarbij het botnet hun ook anonimiteit verschaft.

Veelvoorkomende inzetmogelijkheden van botnets zijn:
- het versturen van spam en phishing-e-mails;
- het uitvoeren van DDoS-aanvallen;
- klikfraude (in grote aantallen klikken op advertenties waarbij de adverteerder per klik betaalt);
- het verspreiden van andere malware;
- het aftappen van wachtwoorden;
- het onderscheppen en manipuleren van (financiële) transacties;
- brute-forceaanvallen, bijvoorbeeld voor het kraken van encryptie.

Het daadwerkelijke gebruik van een botnet voor criminele doeleinden wordt niet altijd door de beheerders zelf gedaan. Botnets worden vaak te huur aangeboden, ook wel 'malware-as-a-service' genoemd.[13: FS 2013] Zie tabel 5 voor een voorbeeldprijslijst.

Dienst	Kosten
Spam (eenvoudig)	$10 per 1.000.000 e-mails
Spam (geverifieerde en/of gelokaliseerde adressen)	$50 tot $500 per 50.000 tot 1.000.000 e-mails
DDoS	$10 per uur, $50 per dag, $150 per week, $1.200 per maand
Koopprijs overname botnet[121]	$200 per 2.000 bots

Tabel 5. Voorbeeldprijslijst botnetgebruik (in US dollar) [51: TM 2012]

3.2.2 *Techniek*

De verspreiding van botnetmalware kan, zoals alle andere malware, op meerdere manieren gebeuren:
- Als bijlage of hyperlink in een vals e-mailbericht: grote hoeveelheden spam-e-mails worden verstuurd met teksten die het aantrekkelijk maken de geïnfecteerde bijlage te openen.
- Via sociale netwerken: korte berichten worden verspreid via besmette profielpagina's van vrienden, vaak met berichten als "is dit een foto van jou?" met een link naar de malware.[122]
- Via besmette USB-sticks: dankzij de toenemende effectiviteit van spamfilters en beveiligingswaarschuwingen gaat de aandacht terug naar dit type verspreiding.
- Gebruikmakend van nog niet gepubliceerde of nog niet gepatchte lekken in veelgebruikte software: soms worden populaire websites gehackt om een exploit te kunnen plaatsen, die door het lek ongemerkt binnensluipt (ook wel 'drive-by download' genoemd).

121 In de praktijk worden botnets zelden te koop aangeboden, omdat de exploitatie vaak zeer winstgevend is.
122 http://www.securelist.com/en/blog/208194206/An_avalanche_in_Skype

Wanneer een computer eenmaal is besmet, zorgt de malware ervoor dat een achterdeur op de computer wordt opengezet, waardoor de botnetbeheerder opdrachten aan de besmette computer kan geven. Zodoende is de computer een bot geworden in het botnet, ook wel 'zombie' genoemd. De malware probeert zo min mogelijk op te vallen. Door bijvoorbeeld de prioriteit van zijn eigen proces voor het besturingssysteem te verlagen krijgen alle handelingen die de gebruiker uitvoert voorrang, waardoor er nauwelijks achteruitgang in de prestaties van de computer te merken is.

In een traditioneel botnet ontvangt een bot de instructies van een zogenaamde 'command & control' (C&C) server. De botnetbeheerder verspreidt via deze server de opdrachten om het botnet in te zetten. De C&C-server is daarmee de kritische component waar de bestrijding van botnets zich op richt. Als die machine eenmaal is uitgeschakeld, is het botnet immers niet meer aan te sturen en zullen de bots inactief blijven. Om daar minder kwetsbaar voor te zijn, zorgen beheerders voor een infrastructuur met soms honderden[13: FS 2013] individuele C&C-servers binnen hetzelfde botnet.

Een alternatieve architectuur die wordt toegepast om bestrijding te bemoeilijken, is het 'peer-to-peer' (P2P) botnet. Hierin wordt een bot geïnstrueerd, die de opdracht doorgeeft aan de volgende bot, om zo als een olievlek over het botnet te worden verspreid. Omdat steeds een andere machine als ingangspunt wordt gebruikt, is de bron van de instructies moeilijk te achterhalen.

Daarnaast worden instructies ook wel verspreid via sociale media. Vanwege het astronomische volume van berichten op netwerken als Facebook en Twitter valt niet te monitoren of er accounts tussen zitten die gecodeerde opdrachten versturen die worden gelezen door bots. Daarnaast wordt herhaaldelijk gewisseld tussen accounts.

3.3 Ontwikkelingen

3.3.1 Huidige situatie

Het botnetlandschap wordt momenteel gedomineerd door een aantal botnetfamilies. Het meest in het oog springend is de familie van Zeus-botnets. Hiervan afgeleid is Citadel, welke in Nederland media-aandacht heeft genoten naar aanleiding van incidenten rondom Dorifel en Pobelka (zie kaderteksten). Naast Zeus zijn ook ZeroAccess en Carberp veel voorkomend.

ZeroAccess wordt vaak ingezet om naast klikfraude ook de rekenkracht van bots te benutten voor bitcoin-mining. De bitcoin is een digitale munteenheid die niet wordt beheerd door een centrale bank, niet wordt erkend door internationale organisaties, maar steeds vaker wordt geaccepteerd als betaalmiddel. Het werkt op basis van cryptografische principes en wordt 'gedolven' door het uitvoeren van complexe berekeningen. Het inzetten van een heel botnet voor het delven van bitcoins is daarom lucratief.

Carberp staat bekend om het leveren van felle concurrentie in de ondergrondse economie. Het botnet probeert andere malware uit te schakelen[123] en zelf controle over een bot te krijgen. De organisatie is dermate professioneel dat achter dit botnet vermoedelijk een marketingafdeling zit om meer klanten te trekken.

Mobiele telefoons, vooral smartphones, worden steeds vaker het doelwit van malware, wat leidt tot het ontstaan van mobiele botnets. Malware die financiële transacties probeert te onderscheppen, verschijnt soms op zowel de computer als de mobiele telefoon, om naast de transactie in de internetbrowser ook een via sms toegezonden autorisatiecode te kunnen onderscheppen.

Ook in de strijd tegen opsporing laten botnetontwikkelaars innovatie zien. Naast de steeds vaker voorkomende P2P-architectuur[124] wordt encryptie toegepast en communiceren de beheerders om anoniem te blijven via Tor. Grote botnets worden slechts in kleine delen ingezet en richten zich op zeer beperkte doelen om zo veel mogelijk onder de radar te blijven.[125] De conventionele wijze van het uitschakelen van botnets via hun C&C-servers is daarom nauwelijks nog toepasbaar.

Botnets steken vaak opnieuw de kop op door de eenvoud en snelheid waarmee de netwerken zijn op te bouwen en door het hoge percentage geïnfecteerde computers. Zo werd in het CSBN-2 nog gesproken van de ontmanteling van het Kelihos-botnet[126], maar dit botnet is in september 2012 opnieuw op de radar van antivirusbedrijven verschenen.[21: McAfee 2013-1]

3.3.2 Verwachtingen

Het succes van het ontmantelen van botnets kan worden gezien in de dalende hoeveelheid spam die deze botnets versturen.[127] Omdat de aandacht van spammers verschuift naar sociale media, worden nieuwe botnets ingericht voor andere functies, zoals DDoS-aanvallen. Daardoor is het niet mogelijk aan de hand van het spamvolume in te schatten hoe effectief het ontmantelen is.

Op korte en middellange termijn wordt een toename in het aantal en de omvang van botnets verwacht. Aanjagers hiervoor zijn:
- de blijvend hoge opbrengsten van verhuur;
- de toenemende belangstelling om DDoS-aanvallen uit te voeren;
- het toenemende gebruiksgemak van 'maak-je-eigen-botnetpakketten';
- de stijgende koers van de bitcoin.

Op dit moment is de pc nog het meest voorkomende besmette apparaat. De verwachting is dat dit zo blijft, zeker gezien het marktaandeel, maar naar verhouding zullen de botnets voor apparaten met Mac OS X, iOS en Android significant toenemen.

123 Microsoft Threat Encyclopedia, W32/Carberp http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32%2fCarberp
124 C. Rossow et. al.: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets http://www.christian-rossow.de/publications/p2pwned-ieee2013.pdf
125 http://webwereld.nl/nieuws/112177/update-maakt-botnet-citadel-langer-onzichtbaar.html
126 NCSC Cybersecuritybeeld Nederland CSBN-2, p. 52.
127 http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport

Casus Dorifel

Detectie en incidentresponse

Op 8 augustus 2012 werden bij het NCSC uitvallende systemen gemeld. Deze systemen waren door besmetting onderdeel van het Citadel-botnet. Deze systemen hadden via het Citadel-botnet de opdracht gekregen om nieuwe malware uit te voeren die later Dorifel is genoemd. De Dorifel-malware is een banking trojan, malware die erop gericht was inloggegevens voor internetbankieren te stelen. De makers van antivirussoftware hadden de volgende dag de eerste antivirusupdates beschikbaar waardoor gebruikers met up-to-date antivirussoftware vanaf dat moment geen gevaar meer liepen voor nieuwe infecties. Dit was maar beperkt effectief omdat deze malware de antivirussoftware ongemerkt kon uitschakelen. Daarom waren met Citadel geïnfecteerde systemen nog steeds kwetsbaar. De Dorifel-malware versleutelde bestanden op het systeem en de netwerkopslag. De Nederlandse antivirusmaker SurfRight publiceerde een programma dat deze versleuteling ongedaan kon maken.

Het NCSC heeft verschillende doelgroepen geïnformeerd over de risico's en het handelingsperspectief. Voor de analyse van de malware is intensief samengewerkt met particuliere onderzoeksorganisaties. Veel expertise op dit gebied blijkt voornamelijk bij private organisaties aanwezig te zijn en beperkt bij de overheid.

Impact

De versie die in Nederland opdook, was mogelijk een testversie. De gevolgen waren groot omdat door deze versie systemen uitvielen. Als de malware naar behoren had gewerkt, was deze aanval wellicht onopgemerkt gebleven.

Intussen is duidelijk geworden dat het aantal besmettingen in Nederland veel groter is dan in het buitenland. De IP-adressen die op C&C-servers van Dorifel zijn aangetroffen tonen aan dat ten minste 150.000 Nederlandse systemen besmet zijn (geweest) met als gevolg dat ondere andere organisaties niet konden werken.

Omdat Dorifel waarschijnlijk niet is verspreid via een zogenaamde 0-day, is het aannemelijk dat organisaties onzorgvuldig zijn geweest bij het voorkomen en detecteren van besmetting met bekende malware. De getroffen organisaties omvatten in elk geval gemeenten, ziekenhuizen, onderdelen van de Rijksoverheid en overheidsgerelateerde organen. Van organisaties in de vitale sectoren zijn geen gegevens bekend van het aantal besmettingen.

De grote mate van spreiding bij de slachtoffers doet vermoeden dat bij uiteenlopende organisaties data ontvreemd is. Het is echter onbekend of en welke data er is ontvreemd door Dorifel.

3.4 Voorkomen en bestrijden

3.4.1 Bestrijding

Het opsporen en bestrijden van botnets wordt steeds moeilijker. Er wordt vaker gebruikgemaakt van een P2P-architectuur, encryptie en op grote schaal willekeurig aangemaakte domeinnamen om opsporing, infiltratie en ontmanteling te verhinderen. Binnen de huidige wetgeving zijn er weinig mogelijkheden voor onderzoekers, bedrijven en overheid om de geavanceerde botnets aan te pakken.

Onderzoek, infiltratie en sabotage van botnets wordt veelal door private partijen uitgevoerd. Onderzoeksinstellingen en securitybedrijven kunnen vrijer opereren dan de overheid in een gebied waar juridisch nog veel onduidelijkheden zijn. Onderzoekers zelf roepen ook op tot een maatschappelijke discussie over de wenselijkheid van infiltratie van botnets door overheden vanwege de grote impact op de privacy van (onschuldige) gebruikers.[128]

Overheidsdiensten handelen voornamelijk reactief tijdens incidenten en missen een tijdig, volledig en gedetailleerd beeld van malware- en botnetactiviteit. Door gebrek aan informatievoorziening en coördinatie van activiteiten op dit gebied zijn de inspanningen van de private sector vaak tijdelijk en beperkt in reikwijdte of effect, omdat de inspanningen van verschillende actoren elkaar tegenwerken. Een voorbeeld hiervan is het uitschakelen van het Waledac-botnet door Microsoft, iets wat volgens onder andere onderzoekers van Fox-IT een onverstandige en ongewenste actie was omdat het botnet was geïnfiltreerd en men niet meer in staat was om informatie over infecties te verzamelen.

3.4.2 Verantwoordelijkheden

Het voorkomen van besmetting door malware blijft grotendeels de verantwoordelijkheid van de eigenaar (of gedelegeerd beheerder) van een systeem. Ook hebben softwaremakers, sitebeheerders, ISP's, etc. een deel van de verantwoordelijkheid.

Voor de gebruiker gelden de aloude aanbevelingen zoals het bijhouden van updates, bewust klikken op links en gebruikmaken van een virusscanner. Het blijft voor de technisch minder onderlegde eindgebruiker lastig om technische maatregelen te nemen, het kost tijd en moeite en malware verspreidt zich via steeds vernieuwende manieren van social engineering. Het herkennen van besmetting met malware is vrijwel onmogelijk zonder voldoende kennis van de werking van een computer.[129]

128 http://www.f-secure.com/weblog/archives/00002056.html

129 Drie van de vijf kenmerken in onderstaand advies vereisen technische kennis om te achterhalen, de andere twee zijn bij botnets niet van toepassing: https://www.security.nl/artikel/45721/1/Vijf_kenmerken_van_een_besmette_computer.html

Casus Pobelka

Detectie en incidentresponse

In december 2012 ontving het NCSC informatie van onderzoeksbedrijven Digital Investigation en SurfRight over het Pobelka-botnet, op basis van data afkomstig van een C&C-server. Pobelka is een botnet dat net zoals Dorifel gebruikmaakt van het Citadel distributieplatform. Uit het SurfRight-rapport[130] bleek dat het overgrote deel van de geïnfecteerde computers van het Pobelka-botnet in Nederland en Duitsland staan. De IP-adressen zijn met het NCSC gedeeld, dat vervolgens controleerde of deze in gebruik zijn bij de overheid en vitale sectoren, en conform afspraken zijn deze IP-adressen vervolgens gedeeld met deze partijen, waaronder de Internet Service Providers (ISP's).

Media-aandacht

In februari 2013 werd in het NOS Journaal aandacht besteed aan het Pobelka-botnet. Journalisten hebben van Digital Investigation inzage gekregen tot de dataset van 750GB die op de C&C-server heeft gestaan. De reportage laat zien hoe divers de buitgemaakte informatie is. De informatie die door het Pobelka-botnet en Citadel werd buitgemaakt is gevoelig.
Immers, alle informatie die via de internetbrowser werd verstuurd, werd afgevangen en verstuurd naar de C&C-server.

Nadere analyse

Naar aanleiding van de media-aandacht is besloten de dataset van Digital Investigation alsnog te onderzoeken door een taskforce waarin wordt samengewerkt tussen het NCSC, de politie, het OM, de AIVD, de MIVD en de NCTV.

Het primaire doel van Citadel-botnets is het manipuleren van financiële transacties. Alle overige gegevens die worden verzameld, kunnen beschouwd worden als 'bijvangst'. Door Pobelka zijn ook internetbankiersessies gefilmd, hetgeen zeer privacybedreigend is omdat het complete computerscherm zichtbaar is, inclusief elke muisbeweging en toetsklik. De buitgemaakte gegevens zijn persoonidentificerende gegevens, bedrijfsinformatie, informatie over de computer en kwetsbaarheden in de software gebruikt door de getroffen organisatie of persoon. Delen van deze bijvangst worden vaak ook, in bulk, gebruikt en soms voor grote bedragen doorverkocht. Kant-en-klare informatieverzamelingen die relatief eenvoudig te verhandelen zijn, zijn steeds vaker te koop. Persoonsidentificerende gegevens worden ook gebruikt voor identiteitsfraude of voor het misleiden van personen, bijvoorbeeld met social engineering.

Op basis van de buitgemaakte gegevens zijn er geen aanwijzingen gevonden dat de aard van dit botnet anders is dan andere vergelijkbare (Citadel-)botnets. Wie verantwoordelijk is voor het botnet, is op het moment van schrijven nog niet bekend.

Software-uitgevers moeten veilige software ontwikkelen en zorgen dat eventuele lekken worden gedicht. Van site-ontwikkelaars en beheerders mag verwacht worden dat zij besmetting van websites voorkomen (denk aan de OWASP[131]-aanbevelingen voor de beveiliging van webapplicaties) en snel acteren en communiceren wanneer er een besmetting is.

Het Pobelka-incident heeft eens temeer duidelijk gemaakt dat ook van de Nederlandse overheid daadkracht wordt verwacht in het tegengaan van botnets. De nog altijd onverminderde uitdagingen zijn vooral op het gebied van samenwerking, zowel tussen publieke en private organisaties als internationaal.

Hoewel in sommige gevallen een botnet specifiek gericht is op bepaalde landen, zoals Dorifel en Pobelka zich op Nederland richtten (zie kaderteksten), verspreiden de meeste botnets zich over de gehele wereld. De botnetbeheerders, C&C-servers, huurders en uiteindelijke doelwitten kunnen zich elk in verschillende landen bevinden. Dit maakt opsporing, bestrijding en vervolging buitengewoon ingewikkeld. Cybercriminelen zijn vaak juist gevestigd in landen waar de pakkans klein is, zeker als er andere misdaadproblemen zijn die voorrang van de lokale autoriteiten krijgen.[132]

3.5 Tot slot

De beste methode om te beschermen tegen botnets blijft het voorkomen van besmettingen. Het kunnen voorkomen van malwarebesmetting is des te belangrijker gelet op de moeilijkheden op het gebied van bestrijding. Zowel thuisgebruikers als organisaties, maar ook software- en netwerkleveranciers hebben hierin een eigen verantwoordelijkheid. Daarnaast is van groot belang om goed publiek/privaat samen te werken. Om bestrijding effectiever te maken, moet enerzijds een detectie- en informatieproces zijn ingericht zodat eindgebruikers snel op de hoogte zijn van een besmetting. Anderzijds moeten cybercriminelen worden opgespoord en vervolgd. «

130 http://www.surfright.nl/nl/hitmanpro/pobelka

131 www.owasp.org

132 http://www.f-secure.com/weblog/archives/00002530.html

4 DDoS

DDoS-aanvallen hebben ervoor gezorgd dat de dienstverlening van organisaties uit de vitale infrastructuur (onder andere de onlinedienstverlening van banken en luchtvaart) is geschaad. Daarnaast zijn ook basisvoorzieningen, zoals iDeal en DigiD, geraakt door DDoS-aanvallen. Hiermee wordt aangetoond dat kwaadwillenden met eenvoudig te verkrijgen middelen grote schade kunnen aanrichten.

4.1 Inleiding

In het afgelopen jaar is de publieke aandacht voor DDoS-aanvallen aanmerkelijk toegenomen. Dit verdiepingskatern gaat nader in op de technische achtergrond, de actoren die verantwoordelijk (kunnen) zijn en de maatregelen die genomen worden.

DDoS is een aanvalstechniek van kwaadwillenden waarbij de capaciteit van de onlinediensten, websites of infrastructuur van een organisatie wordt overbelast door dataverkeer. De onlinediensten of infrastructuur zijn dan niet meer of slecht bereikbaar voor het legitieme verkeer. Waar bij een DoS-aanval de acties vanaf één systeem worden uitgevoerd, wordt bij een DDoS de aanval uitgevoerd vanaf meerdere locaties en systemen.[33: NCSC 2013-3] Dit verdiepingskatern gaat nader in op de problematiek en incidenten veroorzaakt door DDoS-aanvallen.

4.2 Achtergrond

DDoS-aanvallen zijn geen nieuwe ontwikkeling en komen al meer dan tien jaar voor. De laatste jaren nemen de aanvallen echter toe. In 2012 en het eerste kwartaal van 2013 is het aantal DDoS-aanvallen gestegen en is de intensiteit van de aanvallen enorm toegenomen.[133] DDoS-aanvallen worden meestal uitgevoerd door het aansturen van een aanval via een botnet[134] of vanaf meerdere systemen tegelijkertijd. De middelen om een DDoS-aanval te starten, zijn relatief laagdrempelig en kunnen door iedereen met voldoende kennis van ICT en het internet toegepast worden. De slagingskans van een aanval is sterk afhankelijk van het kennisniveau en de gebruikte middelen van de aanvaller en van de maatregelen die de organisatie die het doelwit is, heeft getroffen. Bij veel organisaties ontbreekt het aan de kennis en/of middelen om afdoende en effectieve maatregelen te nemen die de impact en gevolgschade van een DDoS-aanval kunnen beperken. Tegen een DDoS-aanval is feitelijk niet zo heel veel te doen buiten het nemen van maatregelen die het effect van de aanval verkleinen.

4.2.1 Actoren en hun drijfveer

DDoS-aanvallen worden met uiteenlopende redenen en door verschillende actoren uitgevoerd. De capaciteit en techniek voor een DDoS-aanval zijn te koop op het internet. Cybercriminelen bieden een DDoS-aanval als 'dienst' aan.[135] De prijzen voor het gebruikmaken van deze diensten zijn de afgelopen jaren gedaald.[136] Actoren hoeven hierdoor niet zelf over veel vaardigheden te beschikken. Het zelfstandig opzetten van een DDoS-aanval vereist wel meer kennis en vaardigheden.

Scriptkiddies

De drijfveer van een scriptkiddie bij een DDoS-aanval is meestal verhoging van eigenwaarde doordat een geslaagde aanval in de pers vermeld wordt.

Hacktivisten

Hacktivisten kunnen een DDoS-aanval ondernemen tegen bedrijven, organisaties of overheden die, in hun ogen, handelen in strijd met hun ideologie of overtuiging.

Criminelen

Criminelen gebruiken de DDoS-aanvallen om bedrijven af te persen door een DDoS uit te voeren en vervolgens geld te eisen van het slachtoffer om de aanval te stoppen of om een langdurige nog zwaardere aanval te voorkomen. Ook kunnen DDoS-aanvallen worden ingezet als afleiding om de 'echte' aanval waar het om te doen is, bijvoorbeeld spionage of criminele handelingen, te camoufleren. Dit hebben wij in Nederland echter nog niet gezien. Georganiseerde criminelen beschikken in een aantal gevallen zelf over de kennis en vaardigheden of kopen botnetdiensten in van een 'botnetbeheerder'.

Staten

Een DDoS-aanval kan wellicht ook worden uitgevoerd door een staat, met als reden geopolitiek of als onderdeel van cyberwarfare.

4.2.2 *Techniek*

De techniek van een DDoS-aanval kent verschillende varianten. Alleen al van DDoS-aanvallen op het IP-protocol zijn tientallen vormen bekend. Er worden vaak aanvalsvormen gecombineerd, waarbij gelijktijdig of achterelkaar verschillende technieken worden

133 Prolexic Quaterly Global DDoS attack Report Q1-13.
134 Zie het verdiepingskatern Botnets.
135 'Cyberaanval te koop op internet', Trouw, 11 april 2013. http://www.trouw.nl/tr/nl/5133/Media-technologie/article/detail/3423959/2013/04/11/Cyberaanval-te-koop-op-internet.dhtml
136 Chris Verhoef, hoogleraar Informatica aan de Vrije universiteit: de Volkskrant, 9 april 2013: 'Cyberaanvallen: lekker zieken op het Internet'.

ingezet en waardoor het lastiger is om de juiste soort aanval te detecteren en daarop te reageren. Doorgaans worden twee categorieën aanvallen onderscheiden:

» op volume gerichte aanvallen die de bandbreedte van het netwerk en de infrastructuur verzadigen;
» aanvallen op de applicatielaag, gericht op het met een veel lager volume aan berichten treffen van specifieke diensten en op het uitputten van resources.

Hieronder is een aantal veelgebruikte DDoS-aanvallen uitgelegd.

SYN-flood

Een SYN-bericht wordt door een computer, bronsysteem, gestuurd naar een doelsysteem, bijvoorbeeld een webserver, om als eerste stap een connectie te maken via het TCP-protocol. SYN staat voor 'synchronise'. Als het doelsysteem een SYN-bericht ontvangt, beantwoordt het dit met een SYN-ACK-bericht waarna het bronsysteem weer een ACK-bericht terugstuurt. ACK staat voor 'acknowledge'. Op deze wijze wordt de communicatie tot stand gebracht. Bij een SYN flood-aanval wordt een groot aantal SYN-berichten naar bijvoorbeeld een webserver gestuurd, maar beantwoordt het bronsysteem niet met een ACK. Het doelsysteem blijft hierdoor wachten op een veelvoud aan berichten waarbij elk onbeantwoord bericht resources van het doelsysteem in beslag neemt. Als het aantal berichten maar groot genoeg is, kan het systeem onbereikbaar zijn geworden voor legitieme berichten. De internetadressen van de bronsystemen waarvandaan de aanval wordt ingezet, zijn over het algemeen nep of van systemen die onderdeel zijn van een botnet en waarvan de eigenaar zich niet bewust is dat deze onderdeel zijn van de aanval.

ICMP attacks

Het ICMP-protocol wordt gebruikt door systemen om status- en errorberichten naar elkaar te versturen. Een van de functies is het zenden van een PING om te zien of een doelsysteem aan staat en functioneert. Zo'n doelsysteem stuurt dan een 'Echo' terug als antwoord. Een PING-bericht kan gericht naar een systeem gestuurd worden of 'gebroadcast' worden over een volledig netwerk. Er zijn DDoS-aanvallen die dit protocol misbruiken, zoals de Smurf-attack. Bij een Smurf-attack worden vanaf een of meerdere bronsystemen PING-commando's naar een netwerkrouter met broadcastfunctionaliteit gestuurd die op zijn beurt het PING-verzoek over het hele netwerk verspreidt. Het bronsysteem heeft echter in de PING-berichten het IP-adres van het slachtoffer als zender toegevoegd. Alle systemen in het netwerk dat het PING-bericht hebben opgepakt, versturen nu een ECHO-antwoord naar het slachtoffer. Netwerk- en systeembandbreedte zullen hierdoor opgebruikt raken en voor legitiem verkeer niet of minder bereikbaar zijn.[137]

DNS amplification attack

Het DNS-protocol, bedoeld om een 'vertaling' te maken van domeinnamen naar IP-adressen, kan misbruikt worden voor een DDoS-aanval waarbij een doelsysteem wordt overspoeld met aanvragen. De aanvaller stuurt via een door hem gecontroleerd botnet verzoeken naar servers in het internet die acteren als een zogenaamde 'open' DNS-resolver. Normaal gesproken wordt een DNS-verzoek gedaan met een gerichte naam van een bestaande website. Als nu, eenvoudig uitgelegd, een DNS-verzoek wordt gedaan met de aanvraag ANY, beantwoordt deze open DNS-resolver de vraag met een grote lijst aan antwoorden. Het oorspronkelijke en relatief kleine bericht veroorzaakt hiermee een antwoord wat soms wel tot 50 keer de oorspronkelijke grootte is. De aanvallers hebben in het DNS-verzoek het eigen afzenderadres vervangen door dat van het slachtoffer, waardoor een zeer grote hoeveelheid berichten op het doel worden afgestuurd dat daarmee uiteindelijk overbelast raakt.[138]

Casus Spamhaus Project – DDoS-aanval met grootste intensiteit

The Spamhaus Project is een not-for-profit organisatie die o.a. verantwoordelijk is voor het beheer van databases en 'zwarte lijsten' van IP-adressen en domeinnamen die gebruikt zijn of kunnen worden om spam te versturen. De gegevens van Spamhaus, zoals de 'Spamhaus blacklist', worden veel door e-mailproviders gebruikt in hun spamfilter om e-mail afkomstig van daarin geregistreerde domeinen te blokkeren. In maart 2013 werd de website van Spamhaus met een DNS-reflection aangevallen. De aanval werd achteraf getypeerd als de grootste DDoS-aanval die tot dan toe had plaatsgevonden. De aanval begon op 18 maart 2013 waarbij in het begin 10 Gbps aan verkeer werd gemeten met uitschieters tot 100Gbps in de avond.[139] Nadat Spamhaus een externe leverancier van anti-DDoS-diensten had ingeschakeld, waren de diensten op 20 maart weer beschikbaar. Toen de aanvallers onderkenden dat de maatregelen van de leverancier effect hadden, verplaatsten zij de aanval Spamhaus naar de internetexchange-punten via welke de leverancier zijn diensten levert en die ook grote ISP's gebruiken voor hun communicatie. Deze aanval haalde waarden tot 300Gbps en had in een aantal Europese en Aziatische landen zelfs merkbare gevolgen voor de performance van het internet.[140] Volgens de leverancier waren door de aanvallers ongeveer 30.000 open DNS-resolvers ingeschakeld om de DDoS-aanval uit te voeren.

137 http://www.cert.org/advisories/CA-1998-01.html

138 http://blog.cloudfare.com/deep-inside-a-dns-amplification-ddos-attack
139 http://blog.cloudfare.com/the-ddos-that-knocked-spamhaus-offline-and-ho
140 http://www.nytimes.com/interactive/2013/03/30/technology/how-the-cyberattack-on-spamhaus-unfolded.html?_r=0

Casus bRobot – DDoS-aanval op Amerikaanse banken
PHP.bRobot is een malafide PHP-script dat op gecompromitteerde webservers kan worden geplaatst om denial-of-service-aanvallen uit te voeren op derden. Sinds september 2012 liggen Amerikaanse banken op grote schaal onder vuur door deze bRobot denial-of-service-aanval. Amerikaanse overheidsdiensten verdenken Iran ervan de aanval te sponsoren. Iran ontkent betrokkenheid. De 'Izz ad-Din al-Qassam Cyber Fighters' hebben de aanval opgeëist en voeren deze naar eigen zeggen uit omdat Amerika de anti-Islamvideo *Innocence of Muslims* niet van het internet heeft verwijderd. De aanval is technisch gezien niet geavanceerd en is eenvoudig op te zetten. De aanval is moeilijk te stoppen omdat de aanvallers een zeer groot aantal kwetsbare webservers kunnen misbruiken voor het uitvoeren van de bRobot-malware. Ook Nederlandse webservers zijn ingezet als systeem om de Amerikaanse banken aan te vallen.[141]

4.3 Weerbaarheid

Een DDoS-aanval is nagenoeg niet te voorkomen. In analogie met reguliere criminaliteit is het ook niet te voorkomen dat er pogingen worden gedaan door criminelen om in een bedrijf of huis in te breken, maar men kan wel maatregelen treffen om de slagingskans te verminderen. Van belang is dat er bij een vermeende DDoS-aanval wordt geanalyseerd of het wel om een DDoS-aanval gaat of dat het een reguliere storing betreft. Ook kan een beperkte beschikbaarheid van bijvoorbeeld een website worden veroorzaakt door ongewoon veel bezoekers op die pagina's. Een goede analyse van de oorzaak is dus belangrijk.

Exacte cijfers over het absolute aantal DDoS-aanvallen zijn lastig te achterhalen. Het aantal aanvallen in Nederland lijkt toe te nemen in frequentie en ernst, terwijl de middelen om een aanval te lanceren eenvoudiger worden en de aanvaltools steeds makkelijker beschikbaar zijn. Doordat de aanvallen ook steeds complexer worden, zijn de traditionele detectie- en responsemethoden vaak ontoereikend en wordt het steeds moeilijker om de aanvallen tegen te gaan.[142] Vooral de aanvallen gericht op de applicatielaag zijn toegenomen.[143]

Voor de bekende technieken van DDoS-aanvallen is een aantal maatregelen door te voeren die de slagingskans of het effect van een aanval kunnen verminderen. Het NCSC heeft in haar factsheet 'FS 2013-01 Continuïteit van onlinediensten'[33: NCSC 2013-3] een lijst van deze mitigerende maatregelen en andere adviezen ten aanzien van DDoS-aanvallen opgenomen. «

141 http://www.forbes.com/sites/sap/2013/01/18/cyber-attacks-against-banks-continue-wall-street-we-have-a-problemo-bro
142 Karine de Ponteves, 'De vele gezichten van de DDoS-aanval', Webwereld, 4 maart 2013. http://webwereld.nl/beveiliging/389-de-vele-gezichten-van-de-ddos-aanval
143 Enisa: 'Enisa Threat lanscape. Responding to the evolving threat Environment', 28-9-2012.

5 Hyperconnectiviteit

Alles is met elkaar verbonden en dat is de toekomst. Er is een verhoogd risico ontstaan met de alsmaar groeiende aantallen apparaten en bijbehorende internetverbindingen. Het economisch belang en de toenemende complexiteit staan haaks op het inbouwen van beveiliging. Er zijn daarom grote aantallen kwetsbare apparaten, die steeds vaker continu aan een netwerk en het internet zijn gekoppeld.

5.1 Inleiding

In dit verdiepingskatern wordt nader ingegaan op hyperconnectiviteit. Hyperconnectiviteit is een relatief nieuw begrip waarvoor de basis gelegd wordt in een artikel van Barry Wellman.[56: Wellmann 2001] Het brengt een aantal trends in de informatietechnologie onder één noemer, in het bijzonder:

- toenemend gebruik van mobiele apparatuur en het hiermee permanent, via het internet, met andere gebruikers en met onlinediensten (vaak in de cloud) verbonden zijn;
- toenemend voorzien van producten met rekenkracht en netwerkmogelijkheden inclusief het aansluiten op internet, ook producten waar men dit niet direct van zou verwachten zoals auto's, koelkasten en koffiezetapparaten;
- steeds meer industriële systemen voorzien van netwerkmogelijkheden voor centraal beheer en schaalvergroting, tegen lagere exploitatiekosten.

De achterliggende oorzaken hierbij zijn onder andere de groeiende behoefte en noodzaak van gebruikers om altijd en overal bereikbaar te zijn en de toenemende populariteit van mobiele apparaten, sociale media en clouddiensten. Ook de toenemende technische mogelijkheden zoals altijd online (WiFi, GSM/2G, UMTS/3G, 4G), de toenemende bandbreedte van netwerken en de beschikbaarheid van de schier onuitputtelijke adresruimte van IPv6 speelt hierbij een rol.

Op 6 december 2012 waarschuwt het NCSC het Nederlandse publiek over kwetsbaarheden die kunnen ontstaan bij het koppelen van apparaten aan het internet met het Factsheet 'Beveilig apparaten gekoppeld aan het internet'.[34: NCSC 2012-2] Aanleiding voor deze waarschuwing was de media-aandacht voor een aantal incidenten. Gevoelige gegevens van personen en bedrijven waren volgens het televisieprogramma *Reporter* op het internet beschikbaar via apparatuur met onbedoelde koppelingen naar het internet.

5.2 Alles wordt overal bereikbaar

De grote aantallen apparaten die zijn gekoppeld aan internet monden uit in een alsmaar groeiend aantal verbindingen naar verschillende internetdiensten. Zoals beschreven in het Cisco jaarlijkse securityrapport [5: Cisco 2013] zijn die connecties van meerwaarde voor de gebruiker, maar leveren ze ook meer en andere risico's op. De grotere aantallen connecties resulteren ook in meer ingangen naar de netwerken binnen organisaties. De primaire processen binnen organisaties zijn van deze netwerken afhankelijk en worden daarmee kwetsbaarder. Ook wordt de groei veroorzaakt door de verschuiving van lokale dataopslag naar de cloud. Onze data is daarmee altijd beschikbaar op servers die gekoppeld zijn aan het internet.

Naast de bestaande apparatuur worden steeds meer nieuwe soorten apparatuur op netwerken aangesloten. Hiervan zijn de functionaliteit, mogelijkheden voor misbruik en beveiliging minder bekend en hier ontstaan nieuwe risico's. Denk bijvoorbeeld aan elektronische horloges en brillen, slimme lampen en de netwerkapparatuur die in auto's en vliegtuigen wordt geplaatst.

5.3 Misbruik verandert niet

Aanvallen blijven bij hyperconnectiviteit misbruik maken van kwetsbaarheden in protocollen, applicaties en besturingssystemen. Het maakt niet uit of die draaien op een smartphone, een tablet, een computer of zelfs in een auto.

Een recent artikel in de Financial Times[144] gaat in op de kwetsbaarheden in auto's. Hierin wordt gerefereerd aan een onderzoek dat is uitgevoerd in 2010.[20: Koscher 2010] In dit onderzoek wordt gebruikgemaakt van een langer bestaande methode om kwetsbaarheden te vinden die ook gebruikt wordt voor webapplicaties: fuzzing.[145] Het blijkt met deze methode relatief eenvoudig om de beveiliging van de systemen in een moderne auto te omzeilen en zelfs kritieke functies over te nemen.

144 Chris Bryant, (22 Maart 2013) Cars could be the next victim of cyber attacks, Financial Times, The Financial Times Limited 2013.

145 OWASP, the Open Webapplication Security Project, Fuzzing, https://www.owasp.org/index.php/Fuzzing

Een aanvaller kan op verschillende manieren misbruik maken van aan het internet gekoppelde apparatuur:

- Direct misbruik verwerkingscapaciteit, connectiviteit en bandbreedte: een aanvaller kan systemen overnemen en ze vervolgens opnemen in een botnet. Een dergelijk botnet is voor vele malafide doelen in te zetten.
- Misbruik als 'stepping stone': een aanvaller kan vanuit één overgenomen systeem andere systemen verkennen en aanvallen.
- Stelen (vertrouwelijke) persoonlijke of zakelijke data: een aanvaller kan gevoelige gegevens stelen die op het systeem zijn opgeslagen (e-mail, documenten, databases).
- Profilering persoonlijk gedrag: een aanvaller kan gegevens verzamelen over het gedrag van de gebruiker van het apparaat (locatiegegevens, bezochte websites, gedane aankopen). Misbruik van deze informatie is interessant voor gerichte aanvallen.
- Achterhalen en stelen persoonlijke identiteit: een aanvaller doet zich voor als iemand anders (spoofing) en behaalt daar voordeel mee. Een aanvaller kan ook de identiteit van gebruikers onder pseudoniem achterhalen en hier misbruik van maken (doxing).
- Stelen 'credentials' voor toegang tot diensten: een aanvaller kan identificerende gegevens (accountnaam, wachtwoord, toegangscode, cryptografische sleutel) van de gebruiker achterhalen en hiermee toegang verkrijgen tot diensten van de gebruiker (webdiensten, e-mail, clouddiensten, internetwinkels, banken) en berichten versturen of transacties uitvoeren.
- Denial of service, sabotage: een aanvaller kan de apparatuur saboteren en daarmee schade toebrengen.

	Direct misbruik	Stepping Stone	Stelen data	Profilering	Stelen identiteit	Stelen credentials	Denial of Service
Consumenten-computerapparatuur	Praktijk	Praktijk	Praktijk	Praktijk[a]	Praktijk	Praktijk	Praktijk
Consumenten-netwerkapparatuur	Praktijk[b]	Praktijk	Praktijk	Theorie	PoC	Praktijk	Praktijk
Mobiele consumenten-apparatuur	Theorie Praktijk	PoC / Praktijk[c]	Praktijk	Praktijk	Praktijk	Praktijk	-
Vaste consumentenapparatuur	Theorie	Theorie	-	PoC[d]	-	-	Theorie
Vaste technische en zakelijke apparatuur	PoC[e]	Praktijk	Theorie	-	-	Praktijk	PoC
Mobiele technische apparatuur	-	-	-	PoC[f]	-	-	PoC

Tabel 6. Matrix misbruikmogelijkheid apparaatcategorieën

[a]) Consumentencomputerapparatuur zoals laptops en pc's hebben meestal geen locatiesensor. De gebruiker is wel te profileren met cookies, IP-adres en gebruik van locatieprogrammatuur zoals Google Maps.

[b]) Consumentenrouters hebben aandacht nodig met betrekking tot beveiliging. Zo alarmeerde de Consumentenbond begin dit jaar haar leden voor gemakkelijk te kraken wachtwoorden van deze routers.[146]

[c]) Eerdere ontkrachte geruchten over een botnet op mobiele apparaten werden later bevestigd door de BBC.[147] Verder speculeerde McAfee Labs [22: McAfee 2013-2] over een Near Field Communication (NFC) worm.

[d]) Mede naar aanleiding van vermeende grootschalige elektriciteitsmeterfraude bracht de Europese netwerkbeveiligingsorganisatie ENISA in mei 2012 een rapport uit over de beveiliging van elektriciteitsnetwerken.[9: Enisa 2012]

[e]) Al in 2010 toonde Barnaby Jack op de beveiligingsconferentie Black Hat aan dat pinautomaten kwetsbaar konden zijn voor misbruik. Door misbruik van technische kwetsbaarheden kon grote hoeveelheden geld uit een pinautomaat worden gehaald.[148]

[f]) Tijdens de RSA-beveiligingsconferentie in 2012 in San Francisco laat een beveiligingsonderzoeker zien dat een draadloze insulinepomp op afstand misbruikt kan worden om een dodelijke lading insuline toe te dienen.[149]

146 Consumentenbond,Actueel, (3 januari 2013), http://www.consumentenbond.nl/actueel/nieuws/nieuwsoverzicht-2013/Half-miljoen-wifi-routers-lek/

147 BBC news, China mobile users warned about large botnet threat, (15 januari 2013), http://www.bbc.co.uk/news/technology-21026667

148 Wired Threatlevel,(juli 2010), Researcher Demonstrates ATM 'Jackpotting' at Black Hat Conference, http://www.wired.com/threatlevel/2010/07/atms-jackpotted/ en IT SECURITY BLOG, (Augustus 2012), Exploiting ATMs: a quick overview of recent hacks, http://security.blogoverflow.com/2012/08/exploiting-atms-a-quick-overview-of-recent-hacks/

149 Bloomberg Techblog, (29 februari 2012), Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device.

5.4 Stand van zaken

Om te bepalen hoe actueel een dreiging is, wordt het volgende misbruik onderscheiden:

- Theorie: de mogelijkheid is geopperd door beveiligingsonderzoekers en wordt als geloofwaardig beschouwd.
- Proof of Concept: aanvallen zijn gedemonstreerd door beveiligingsonderzoekers. Voor zover zij in de praktijk worden aangetroffen, gebeurt dit slechts incidenteel en is de schade overwegend gering.
- Praktijk: aanvallen worden in de praktijk aangetroffen en er is meer dan incidentele schade gerapporteerd. De uitvoering van de aanvallen wordt gemakkelijk gemaakt door eenvoudige tools.

Tabel 6 geeft de status van mogelijk misbruik weer per apparaatcategorie. In de voetnoten staan opvallende voorbeelden die de afgelopen periode in de media bekend zijn geworden.

De risico's die gekoppeld zijn aan de nieuwste soorten netwerkapparatuur lijken beperkt. De op dit moment bekende aanvallen zijn vaak onder speciale randvoorwaarden uitgevoerd. Zo blijkt de malware van het hiervoor (noot c) beschreven botnet gebruikgemaakt te hebben van applicaties die vanuit een niet-officiële applicatiestore waren geïnstalleerd.

5.5 De verdiensten van IPv6

De invoering van IPv6 zal leiden tot een verschuiving van risico's in de wereld van hyperconnectieve apparaten. IPv6 is onder andere ontwikkeld om de beperkingen in de vorige adresseringsstandaard IPv4 te verhelpen. De grotere adresruimte en eenduidiger netwerksegmentering zou moeten leiden tot een eenvoudiger te onderhouden netwerk.

In de praktijk blijkt dat IPv6 zodanig verschilt van IPv4, dat de invoering van IPv6 zonder een gedegen kennis leidt tot beveiligingsrisico's. Vaak is aangeschafte apparatuur automatisch of voorgeconfigureerd voor IPv6. Door het aansluiten van een apparaat met IPv6, is het dan in de regel vanaf het internet bereikbaar. De eerste DDoS-aanvallen via IPv6 zijn in 2012 gemeld.[150]

Voor de huidige veelgebruikte mobiele besturingssystemen is het IPv6-protocol al bijna standaard.[151] Vooralsnog kiest de fabrikant en/of de applicatieontwikkelaar er nog wel zelf voor in hoeverre het nieuwe protocol wordt gebruikt op het apparaat.

5.6 Verhoogd risico is aanwezig

Er is een verhoogd risico gemoeid met de alsmaar groeiende aantallen apparaten en de daarbij behorende internetverbindingen. Fabrikanten hebben over het algemeen – veelal vanuit economisch belang – geen noodzaak om apparatuur te beveiligen en om eventuele kwetsbaarheden te verhelpen. Daarnaast kunnen kwetsbaarheden vaak niet eenvoudig worden weggenomen. Vaak zijn er grote aantallen kwetsbare apparaten in omloop die bij gebruik bijna continu aan het netwerk gekoppeld zijn. Hoewel de schade bij een overgenomen koelkast of koffiezetapparaat in eerste instantie klein lijkt, kan een overgenomen apparaat in een botnet veel schade veroorzaken.

Een onderzoek[152] naar kwetsbare, via internet bereikbare apparaten laat zien hoe deze in kaart kunnen worden gebracht. Door het plaatsen van programmacode op kwetsbare apparaten om te zoeken naar andere kwetsbare apparaten, kan de zoektijd exponentieel worden bekort. Hierdoor kan de impact van een kwetsbaarheid in een aanzienlijk kortere tijd worden aangetoond.

5.7 Oorzaken

Via het internet zijn grote aantallen kwetsbare apparaten te vinden. De oorzaken hiervoor liggen voor een groot deel bij de beperkte mogelijkheden voor updates en slecht onderhoud op deze apparatuur. Deze oorzaken liggen bij verschillende stakeholders. Economische factoren bij leveranciers spelen hierbij een rol. Door commerciële druk om snel nieuwe versies uit te brengen en geen ondersteuning voor oudere versies te geven, worden beveiligingsfouten niet hersteld. Onderhoud en updates brengen relatief hoge kosten en lage opbrengsten met zich mee. Leveranciers willen graag voor de laagste prijs aanbieden en bezuinigen daarom op beveiliging. Leveranciers van technische apparatuur (telefooncentrales, zendinstallaties en medische apparatuur) willen de apparatuur graag onder eigen beheer hebben en verbieden vaak het installeren van updates door anderen, met als gevolg dat apparatuur soms onnodig kwetsbaar is.

Door de toegenomen wens om apparaten te verbinden, wordt apparatuur die oorspronkelijk niet aan internet verbonden zou worden (zoals industriële controlesystemen) vanwege gemak en efficiency hier toch mee verbonden, terwijl in het ontwerp geen rekening gehouden is met de beveiliging hiervan. Apparatuur bezit regelmatig netwerkfuncties waarvan de beveiligingsrisico's niet duidelijk zijn en die voor consumenten lastig te configureren zijn.

Er is een gebrek aan kennis en beveiligingsbewustzijn bij ontwikkelaars. In IT-opleidingen en publicaties over internetplatformen wordt vaak de meeste aandacht gegeven aan functionaliteit en te weinig aan beveiliging. Als er al aandacht is voor beveiliging gaat het om het beveiligen van de functionaliteit en niet om de

150 Steven J. Vaughan-Nichols, First IPv6 Distributed Denial of Service Internet attacks seen, ZDnet, (20 februari, 2012) http://www.zdnet.com/blog/networking/first-ipv6-distributed-denial-of-service-internet-attacks-seen/2039

151 Wikipedia, Comparison of IPv6 support in operating systems, (http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems).

152 http://internetcensus2012.bitbucket.org/paper.html

technische beveiligingsaspecten.[153] Bij de ontwikkeling van apparatuur wordt vaak van dezelfde functionele softwaremodules gebruikgemaakt. In de praktijk blijkt dat vaak te oude en onveilige versies van deze softwaremodules worden gebruikt.[154]

Veel gebruikers, zeker waar het consumentenproducten betreft, weten weinig over beveiligingsproblemen en beseffen niet dat updates nodig zijn en weten vaak niet hoe deze te installeren zijn, zeker als het firmware-updates betreft. «

153 Andy Balinsky, Cisco Blog, Security Features vs. Securing Features, (december 2012), http://blogs.cisco.com/security/security-features-vs-securing-features/
154 Rapid7, Security Flaws in Universal Plug and Play, Unplug, Don't play, RSA Conference 2013.

6 Grip op informatie

We produceren, verzamelen en verwerken met zijn allen steeds meer informatie. Dat heeft voordelen, want de bundeling van al die data biedt waardevolle inzichten voor wetenschap en bedrijven. Maar er zitten ook maatschappelijke en technische risico's aan ten aanzien van privacy en informatiebeveiliging. Overzien we die risico's voldoende en wat kunnen we doen om ze te verkleinen?

6.1 Inleiding

We produceren, verzamelen, analyseren en verwerken steeds meer informatie. Dit informatietijdperk heeft voordelen, want de bundeling van al die informatie biedt waardevolle inzichten en levert een duidelijke bijdrage aan de economische en sociale welvaart. Er zitten echter maatschappelijke en technische risico's aan omtrent privacy en informatiebeveiliging. Tegelijkertijd is het bewustzijn van deze risico's beperkt. Recente incidenten maken duidelijk wat de gevolgen kunnen zijn op het moment dat er wat misgaat, van schending van de privacy zoals bij de datalekken van Bol.com[155], Groene Hart Ziekenhuis[156] of Tix.nl[157] tot zelfs verstoring van de openbare orde zoals bij het project-X-feest in Haren[158].

Overzien we de privacyrisico's en de informatiemacht van grote partijen door deze vergaande digitalisering en ontwikkelingen zoals Internet of Things, mobiele apparaten, big data, cloud en sociale media? Hoe zorgen we dat we grip houden op deze informatie?

6.2 Aggregatie en uitwisseling van informatie

Burgers, bedrijven en overheden produceren en aggregeren steeds meer informatie en die informatie wordt ook steeds meer uitgewisseld. Dit vergroot het belang en de waarde van informatie voor deze groepen in onze samenleving.

Burgers

De trend is dat de burger steeds meer informatie, zoals persoonlijke informatie, foto's en video's, deelt op sociale media en dat sociale media een steeds belangrijke rol gaat spelen in de wijze waarop informatie wordt gedeeld. Gemiddeld besteden Europeanen 6,7 uur per maand aan sociale netwerken en blogs.[7: CS 2013]

In tabel 7 zijn de gebruikscijfers van de verschillende sociale netwerken in Nederland weergegeven,[36: Newcom 2013] het laatste halfjaar groeide het aantal Facebookgebruikers in Nederland met bijna 250.000.[159] Wereldwijd loggen maandelijks 1 miljard gebruikers in op Facebook en uploaden zij 300 miljoen foto's per dag op Facebook, wat resulteert in 7 petabytes (1 petabyte = 10^{15} bytes) aan fotocontent per maand.

Sociale Media	Aantal gebruikers	Aantal gebruikers dagelijks
Facebook	7.900.000	500.000
Youtube	7.100.000	900.000
LinkedIn	3.900.000	400.000
Twitter	3.300.000	1.600.000
Google+	2.000.000	500.000
Hyves	1.200.000	300.000

Tabel 7. Gebruikscijfers van de verschillende sociale netwerken in Nederland

Bedrijven

Bedrijven hebben concurrentiegevoelige informatie, productie-informatie, gegevens van medewerkers, klanten, etc. Zij verzamelen en analyseren al geruime tijd informatie van klanten, maar combineren steeds vaker verbruiks- en locatiegerelateerde gegevens met bedrijfsgegevens om nieuwe inzichten en diensten te creëren. Andere trends zijn dat consumentenapparatuur steeds vaker in organisaties wordt gebruikt (consumerization) en vragen, klachten of problemen rond bedrijven steeds vaker via sociale media worden benoemd.[160]

Overheden

De informatiehuishouding van de overheid omvat allerlei gegevens van personen, bedrijven, adressen, gebouwen, voertuigen en inkomens. Het toegankelijk maken en beschikbaar stellen van informatie (open data[161]) is een actuele trend. De overheid beheert zowel open data zoals voertuiggegevens als (gesloten) centrale registraties zoals de Gemeentelijke Basisadministratie Persoonsgegevens (GBA).

Er is een iOverheid ontstaan, gekenmerkt door informatiestromen en -netwerken en gericht op niet alleen dienstverlening, maar ook

155 http://webwereld.nl/nieuws/111012/marketingsite-bol-com-lekt-gegevens-84-000-mensen.html
156 http://www.ghz.nl/over-ghz/organisatie/faq-inbraak-op-server-groene-hart-ziekenhuis/
157 http://www.nu.nl/internet/2895992/tixnl-lekt-duizenden-paspoorten-bankafschriften-en-creditcards-.html
158 http://nl.wikipedia.org/wiki/Project_X_Haren

159 SocialBakers: Netherlands Facebook Statistics, http://www.socialbakers.com/facebook-statistics/netherlands
160 Interxion: Big Data – Beyond the hype, http://www.interxion.com/about-us/whats-new/only-a-quarter-of-eu-organisations-have-built-a-business-case-for-big-data-finds-survey/
161 Zie de websites https://data.overheid.nl/ en http://opendatanederland.org/ voor informatie over de beschikbare Nederlandse open datasets.

op controle en zorg. Deze iOverheid brengt vergaande veranderingen in de relatie tussen burgers en overheden met zich mee. [59: WRR 2011]

In 2017 moeten bedrijven en burgers zaken die ze met de overheid doen – zoals het aanvragen van een vergunning – digitaal kunnen afhandelen.[45: Rijksoverheid 2012] Belangrijk hierbij is dat burgers en bedrijven daartoe slechts één keer hun gegevens aan hoeven te leveren.[162]

6.3 Het risico van vergaande digitalisering

De verwachting is dat er in de toekomst meer geïnvesteerd zal worden in het verkrijgen van inzicht in de beschikbare grote hoeveelheden data dan in het verkrijgen van deze data. [16: IDC 2013] De belangrijkste ontwikkelingen en bijkomende risico's zijn hierna opgesomd.

Internet of Things

Steeds meer apparaten zijn op het internet aangesloten en communiceren met elkaar om het leven van de gebruiker makkelijker te maken. Binnen een paar jaar zullen miljarden apparaten enorme hoeveelheden informatie uitwisselen.[6: Cisco 2011] Het Internet of Things heeft juridische gevolgen. Bijvoorbeeld, hoe wordt met de privacy van de gebruikers omgesprongen? Wie is eigenlijk eigenaar van al die informatie en wie is aansprakelijk als er dingen mislopen? Belangrijke vragen die zich hierbij voordoen, zijn: Valt nog te traceren welk apparaat precies welke informatie genereert? En welk ander apparaat er gebruik van maakt? Wie is er verantwoordelijk voor en beheert deze informatie?

Mobiele apparaten

Smartphones of tablets bevatten vaak veel persoonlijke gegevens van de gebruikers, zoals e-mail, contactpersonen, agenda's, locatiegegevens, creditcardgegevens, foto's, video's en inloggegevens. Het verwerken van deze gegevens brengt risico's met zich mee voor bedrijven en de persoonlijke levenssfeer van de gebruikers als de privacywetgeving niet wordt nageleefd.[163]

Privacyrisico's zijn onder andere dat een app zonder dat de gebruiker dat weet of daarvoor toestemming heeft gegeven, toegang tot persoonsgegevens verkrijgt, informatie op smartphones of tablets opslaat, de informatie over gebruik van apps deelt met derden of onversleuteld over het internet verstuurd. Ook bestaat het risico dat apps veel meer gegevens gebruiken dan zij nodig hebben voor de werking van de app.

Gebruikers en de verantwoordelijken binnen organisaties hebben vaak nauwelijks een idee van de risico's. Een spelletje dat in de achtergrond de contactpersonendatabase uploadt? Salesmedewerkers van de concurrent volgen dankzij een gratis parkeer-app? Het kan allemaal. Schokkend eenvoudig zelfs.[164] Ook het consumentgedreven gebruik van ICT (Consumerization) brengt beveiligingsrisico's met zich mee waar veel organisaties nog geen antwoord op hebben. [30: NCSC 2012-1]

Big data

Er wordt door bedrijven en overheden in systemen steeds meer data vastgelegd en verzameld voor logging, datamining, marketing en meer. Het bestaat uit een grote diversiteit aan gegevens, gestructureerd en ongestructureerd (bijvoorbeeld e-mails, tweets en Facebook posts) en bestaat vaak uit een enorme hoeveelheid kleinere datasets.

Om een beeld te kunnen vormen van onze 'verzamelwoede' volgen hieronder relevante cijfers met betrekking tot big data. [17: IDC 2012][165][166]

- Van 2005 tot 2020 zal het digitale universum groeien met een factor 300, van 130 exabyte (1 exabyte = 10^{18} bytes) naar 40.000 exabytes, dat is meer dan 5.200 gigabyte voor iedere man, vrouw en kind in 2020.
- 90 procent van de data wereldwijd is de afgelopen 2 jaar geproduceerd en iedere dag wordt 2,2 miljoen terabytes (1 terabyte = 10^{12} bytes) aan data gecreëerd.
- Tussen de 10 en 20 procent van de data wereldwijd is gestructureerde data en tussen de 80 en 90 procent is ongestructureerde data (bijvoorbeeld e-mails, tweets, Facebookposts, muziek en mobieletelefoongesprekken).
- De hoeveelheid ongestructureerde data groeit 15 maal harder dan de hoeveelheid gestructureerde data.

Deze ongeremde dataverzameling, -opslag en -bewerking brengt technische en maatschappelijke beveiligingsuitdagingen met zich mee, terwijl vaak nog geen goede technische beveiligingsmaatregelen zijn ingebouwd.

Big data is meer dan een kwestie van opslag van veel data. Het is een kans om inzicht te krijgen in deze data, zodat bedrijven en overheden flexibeler kunnen inspelen op nieuwe en relevante ontwikkelingen, en het biedt de mogelijkheid om vragen te beantwoorden die voorheen niet konden worden beantwoord. Door gebruik te maken van big data kunnen criminele netwerken in kaart worden gebracht, kan worden vastgesteld hoe deze netwerken reageren op verschillende interventiestrategieën en kunnen mogelijke cyberaanvallen worden voorspeld en voorkomen.[167] Dit geldt overigens niet alleen voor cybercriminaliteit, maar ook voor de 'reguliere' criminaliteit.[168] Kwaadwillenden verzamelen echter ook steeds

162 http://ibestuur.nl/magazine/stef-blok-rijksoverheid-in-2017-volledig-digitaal
163 http://www.cbpweb.nl/Pages/pb_20130314-wp29-opinie-mobiele-apps.aspx
164 http://www.automatiseringgids.nl/achtergrond/2012/20/apps-maken-bedrijfsspionage-gevaarlijk-simpel
165 http://venturebeat.com/2012/06/11/autonomy-big-data-infographic/
166 IBM: Understandig Big Data, http://www-01.ibm.com/software/data/bigdata/
167 http://www.emc.com/about/news/press/2013/20130226-02.htm
168 http://www.automatiseringgids.nl/nieuws/2013/08/big-data-helpt-criminaliteit-opsporen

meer data om zo hun (potentiële) slachtoffers beter te leren kennen en aan te kunnen vallen.

Cloud

Cloudcomputing is de ontwikkeling waarbij ICT-diensten zijn verbonden via het publieke internet en data steeds meer worden opgeslagen en (eventueel) verwerkt op plaatsen buiten de eigen organisatie en directe invloed van de eigenaren.

Veel organisaties onderzoeken de mogelijkheden om hun ICT onder te brengen in de cloud of doen dat al. Cloud is ook voor individuele medewerkers eenvoudig in te zetten. Bijvoorbeeld door op de werkplek gegevens in de cloud te zetten om te delen met collega's of thuis eenvoudig te kunnen benaderen.

Cloudcomputing brengt risico's met zich mee, onder meer omdat de toegang vaak beperkt is beveiligd en cloudleveranciers zich allerlei rechten voor gebruik van de gegevens toe-eigenen [31: NCSC 2011] en dit (semi-)juridisch in overeenkomsten afdekken. Het onderbrengen van informatie bij een cloudleverancier brengt tevens met zich mee dat deze informatie makkelijker en sneller opgevraagd kan worden door overheidsinstanties en veiligheidsdiensten.[53: UvA 2012][14: Google 2012][23: MS 2012-2] Ondanks het onvoldoende duidelijk zijn van de risico's zet de 'migratie naar de cloud' onverminderd door.

Sociale media

Sociale media zoals Twitter en Facebook zijn niet meer weg te denken uit de digitale samenleving. Overheden, bedrijven en burgers zijn steeds meer bereid om dit medium in te zetten om informatie te delen met de rest van de wereld.[169] Deze niet te keren trend brengt ook bedreigingen met zich mee, zoals: [39: Ordina 2011]

- Gevoelige informatie wordt (per ongeluk) openbaar gemaakt.
- Informatie wordt misbruikt bij social-engineeringaanvallen.
- Informatie en personen worden aan elkaar gekoppeld waardoor mogelijk ongewenst verbanden zichtbaar worden.
- Prijsgeven van informatie waarmee wachtwoorden zijn te achterhalen.

Door het gebruik van sociale media kunnen bijvoorbeeld bedrijfsgegevens, onderzoeksresultaten of klantinformatie uitlekken, gevoelige informatie over medewerkers worden prijsgegeven of de organisatie onjuist en negatief worden gerepresenteerd. De organisatie kan hierdoor (reputatie- of financiële) schade ondervinden of kwetsbaarder worden voor cyberaanvallen. Daarnaast kunnen sociale media de veiligheid van personen ondermijnen (sabotage en chantage).

169 http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/

Op Facebook wordt iedere dag 2,7 miljard keer 'geliked',[170] waarbij ongemerkt veel (persoonlijke) informatie wordt vrijgegeven. Onschuldig lijkende informatie kan gecombineerd een gedetailleerd beeld geven van gebruikers.[42: PNAS 2013] Individuele kenmerken en voorkeuren van gebruikers geven kwaadwillenden informatie over potentiële slachtoffers. Zo biedt de in de afgelopen periode geïntroduceerde Facebookfunctionaliteit 'graph search'[171][172] kwaadwillenden een (makkelijke) manier om informatie over potentiële slachtoffers te verzamelen.

Een risico is ook dat sociale mediabedrijven hun privacyvoorwaarden en standaardinstellingen van hun sociale netwerksites wijzigen die in het nadeel van privacy kunnen zijn of zelfs in strijd met privacyrichtlijnen.[173][174][175]

6.4 Risico's door verminderde grip op informatie

Privacyrisico's

Een gemiddelde burger in Nederland komt met zijn gegevens voor in honderden tot duizenden bestanden in zowel de publieke als private sector.[176] We maken ons zorgen om onze privacy: de Elektronische Patiëntendossiers (EPD), de OV-chipkaart, de centrale databank met vingerafdrukken, alom aanwezig cameratoezicht, het monitoren en het door opsporingsdiensten aftappen van internet- en telefoonverkeer, etc. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens voldoende worden beveiligd tegen diefstal, verlies en misbruik van persoonsgegevens, zoals identiteitsfraude. Bedrijven en overheden die persoonsgegevens verwerken moeten deze volgens de Wet bescherming persoonsgegevens (Wbp) beveiligen en leggen passende technische en organisatorische maatregelen ten uitvoer of dragen zorg dat voldoende waarborgen worden geboden ten aanzien van deze beveiligingsmaatregelen.[177]

Het College Bescherming Persoonsgegevens (CBP) constateert in zijn terugblik op 2012 dat de overheid in toenemende mate persoonsgegevens verzamelt en aan elkaar koppelt.[2: CBP 2013] Daar burgers in veel gevallen verplicht zijn om persoonsgegevens aan de overheid af te staan, is het essentieel dat burgers erop kunnen vertrouwen dat met die gegevens zorgvuldig en in overeenstemming met de WBP wordt omgesprongen. Uit de praktijk blijkt echter dat de overheid – aangemoedigd door de technologische ontwikkelingen in combinatie met de wens om efficiënt en klantvriendelijk te zijn – steeds meer persoonsgegevens uit de verschillende databases aan elkaar koppelt om deze gegevens vervolgens te gebruiken voor geheel andere doeleinden dan

170 http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers/
171 http://newsroom.fb.com/News/562/Introducing-Graph-Search-Beta
172 In Nederland zal Facebook deze functionaliteit onder de naam 'Zoeken in Facebook-sociogram' gaan aanbieden.
173 http://www.cbpweb.nl/Pages/pb_20121016-privacyvoorwaarden-google-in-strijd-met-eu-richtlijn.aspx
174 http://www.cbpweb.nl/Pages/med_20100513_facebook.aspx
175 LinkedIn: Ads enhanced by the power of your network
176 http://www.cbpweb.nl/Pages/rap_2009_onze_digitale_schaduw.aspx
177 http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx

waarvoor zij oorspronkelijk verzameld werden. Onze digitale gegevens worden continu door anderen gebruikt en verwerkt in risico- en klantprofielen.[8: Tokmetzis 2012]

Informatiemacht van de grote partijen op het internet

De grote partijen op het gebied van sociale media, zoekmachines en webwinkels hebben een onvoorstelbare hoeveelheid data tot hun beschikking, waaruit allerlei profielen te destilleren zijn. Deze partijen zijn steeds meer op weg naar het vercommercialiseren van deze data. Aanbieders zoals Google en Facebook koppelen steeds meer diensten tot één ervaring en positioneren zich als de persoonlijke toegangspoort tot het internet. Uit een onderzoek uitgevoerd door het Rathenau Instituut blijkt dat we als internetgebruikers niet alleen de controle verliezen over onze persoonlijke data. Nog veel belangrijker, we verliezen ook de controle over ons informatieaanbod.[178]

Privacytoezichthouders maken zich onder andere zorgen over het combineren van persoonsgegevens die door verschillende (online) diensten worden verkregen[179], het verzamelen van het surfgedrag van internetters[180] en de blijvendheid van data op het internet (ontgoogelen).

Een voorbeeld is dat onze zoekopdrachten worden beïnvloed[181] en steeds persoonlijker worden. [41: Olsthoorn 2010]. Zij worden aangevuld op basis van eerder ingevulde zoektermen, het internetgedrag en de locatie van waar gezocht wordt. Het gevolg is dat iedereen andere zoekresultaten krijgt: vrouwen krijgen andere zoekresultaten dan mannen, Amsterdammers krijgen andere zoekresultaten dan Rotterdammers, etc. Dit kan leiden tot betere zoekresultaten, maar heeft ook tot gevolg dat de eindgebruiker minder grip heeft op wat hij vindt.

6.5 Hoe houden we grip?

De voorgaande paragrafen samenvattend, kan geconstateerd worden dat informatie in rap tempo digitaliseert. Dat brengt een groot aantal nieuwe dreigingen met zich mee. Wat wordt er gedaan om nog enigszins grip te houden?

Gebruikers

De gebruiker kan geadviseerd worden over hoe om te gaan met zijn (persoonlijke) gegevens, maar hij blijft in belangrijke mate afhankelijk van de mate van beveiliging die producten en aanbieders inbouwen. Een van de verantwoordelijkheden van gebruikers is het bewust kiezen welke informatie wordt gepubliceerd en met wie deze wordt gedeeld. Dit verkleint de privacyrisico's en maakt het kwaadwillenden moeilijker om deze informatie te achterhalen en hiervan misbruik te maken. De trend is dat Nederlanders beter controleren aan wie persoonlijke gegevens worden gestuurd en zij veranderen ook vaker hun wachtwoorden[52: UT 2012]. Het CBP biedt burgers praktische informatie over het beschermen van hun privacy op http://www.mijnprivacy.nl.

Bedrijven en overheden

Ontwikkelingen zoals cloud en mobiel vragen om een blijvende aandacht voor beveiliging zodat klanten en burgers op een veilige manier van dienstverlening gebruik kunnen maken en dat hun privacy wordt gewaarborgd.

Met de steeds verdere digitalisering van de overheid is het veiligheidsaspect belangrijk, hiertoe werken diverse partijen samen met als doel overheidsorganisaties weerbaarder te maken en ervoor te zorgen dat ze zich na een veiligheidsincident snel kunnen herstellen.[182] Het CBP biedt bedrijven en organisaties informatie over het beschermen van privacy op http://www.cbpweb.nl/.

Overheidsorganisaties steunen voor een groot deel op procedures en veel minder op technische beveiligingsmaatregelen. Dit hoeft geen probleem te zijn, als het bewustzijn hoog genoeg is om de procedurele maatregelen na te leven. Dit blijkt echter op basis van onderzoek niet het geval te zijn.[10: E&Y 2012]

De verwachting is dat organisaties steeds vaker een private cloudomgeving zullen implementeren en big data (weer) in eigen beheer nemen in plaats van deze onder te brengen bij externe partijen.[43: Quocirca 2013] Hierdoor kan de betreffende organisatie betere en duidelijkere controle over de eigen gegevens (her)krijgen. Organisaties denken beter na over wat ze in huis hebben en wat de beste invulling is, de balans tussen security, privacy en kosten afwegend.

Zorg- en meldplicht

Naast het transparant zijn hoe organisaties omgaan met de verzamelde gegevens en deze beveiligen, hebben deze ook een zorg- en meldplicht. Telecomaanbieders zijn vanaf 5 juni 2012 verplicht om alle beveiligingsincidenten waarbij persoonsgegevens zijn betrokken, te melden bij de Autoriteit Consument & Markt (ACM).[183] Heeft het incident ongunstige gevolgen voor klanten? Dan moeten de telecomaanbieders ook de getroffen klanten inlichten. Deze meldplicht houdt verband met de zorgplicht: bedrijven moeten de persoonsgegevens van hun klanten goed beschermen.

178 http://www.rathenau.nl/actueel/nieuws/nieuwsberichten/2012/03/online-keuzevrijheid-consument-beter-waarborgen.html
179 http://www.cbpweb.nl/Pages/pb_20121016-privacyvoorwaarden-google-in-strijd-met-eu-richtlijn.aspx
180 http://www.cbpweb.nl/Pages/med_20121005-volgen-surfgedrag-internet.aspx
181 Vara: Google-bubble: Wat Je Zoekt Ben Je Zelf, http://kassa.vara.nl/tv/afspeelpagina/fragment/google-bubble-wat-je-zoekt-ben-je-zelf/speel/1/
182 http://www.taskforcebid.nl/
183 https://www.acm.nl/nl/onderwerpen/telecommunicatie/internet/meldplicht-inbreuk-bescherming-persoonsgegevens/

Het CBP heeft als toezichthouder in 2012 een 25-tal (mogelijke) beveiligings- en datalekken onderzocht.[2: CBP 2013][184] Bij de onderzochte datalekken werden burgers bijvoorbeeld vaak gevraagd op een webformulier persoonsgegevens (waaronder bijvoorbeeld medische gegevens) in te vullen, die vervolgens onbeveiligd via het internet werden verstuurd. Bedrijven en overheden zijn op dit moment nog niet verplicht datalekken te melden. Er is wel een wetgeving in de maak die een meldplicht datalekken invoert.[185]

184 http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx
185 http://www.rijksoverheid.nl/documenten-en-publicaties/wetsvoorstellen/2012/11/01/wijziging-wet-bescherming-persoonsgegevens-meldplicht-datalekken

7 Kwetsbaarheid van ICT

Alle ICT is kwetsbaar, maar toch hebben we ons lot eraan verbonden. Enerzijds moeten we accepteren dat ICT niet foutloos kan zijn, anderzijds moet de oorzaak van het probleem wel aangepakt worden: ICT móet veiliger dan het nu is (zowel de producten als de inrichting als het gebruik ervan). De basis qua beveiliging ontbreekt in veel organisaties nog steeds. Principes rondom beheer en beveiliging worden door organisaties van allerlei aard en omvang met voeten getreden. Daarbij gaat het niet alleen om het implementeren van risicomanagement, maar ook om het nemen, evalueren en bijstellen van concrete maatregelen, zoals patchmanagement en richtlijnen voor webapplicaties.

7.1 Inleiding

Een belangrijk deel van de aandacht die naar cybersecurity uitgaat, moet worden geschonken aan het mitigeren van de kwetsbaarheden in ICT. Aangezien daders lastig traceerbaar zijn, is de staat van de verdediging tegen kwetsbaarheden op dit moment de belangrijkste graadmeter van de status van ICT-veiligheid in Nederland.

Vanaf het moment dat het eerste virus zijn intrede deed op een computer, meer dan 30 jaar geleden, zijn de kwetsbaarheden van ICT in beeld geweest bij partijen die ICT-producten produceren en gebruiken. De afgelopen jaren worden steeds vaker zorgen over de veiligheid van de gebruikte middelen onderkend. Beveiliging van ICT is namelijk nog steeds een zorgenkind. In de ontwikkeling is veiligheid vaak een ondergeschoven kindje. Toch heeft de samenleving zich in grote mate aan deze technologie verbonden, aangezien de voordelen van het gebruik simpelweg te groot zijn om te laten liggen. Deze voordelen zijn tevens een belangrijke motor van innovatie en groei in de Nederlandse samenleving.

Door de vele beveiligingsincidenten van de afgelopen jaren is het besef bij gebruikers gegroeid dat ICT niet foutloos kan zijn, maar tegelijkertijd tonen diezelfde incidenten aan dat de oorzaak van het probleem wel aangepakt moet worden: ICT móet volgens velen veiliger dan het nu is, zowel de producten als de inrichting en het gebruik ervan. Maar in de tussenliggende tijd moet desondanks geaccepteerd worden dat ICT tot op zekere hoogte kwetsbaar blijft en incidenten zich zullen blijven voordoen en er dus maatregelen nodig zijn.

De realisatie dat leveranciers én gebruikers nog onvoldoende doen om software veilig te maken, is een waarschuwing voor de toekomst. Dit kan tevens de motivatie zijn om de vraag te stellen in hoeverre het gebruik van (internetgeralateerde) ICT noodzakelijk is voor het ontwikkelen van een dienst of product. Dit is ook de reden dat het NCSC organisaties adviseert om alleen diensten via een netwerk bereikbaar te maken als dat noodzakelijk is.
Dit verdiepingskatern benoemt een aantal trends in de kwetsbaarheden in ICT. ICT-kwetsbaarheden liggen ten grondslag aan veel van de aanvallen die plaatsvinden op infrastructuren en software.

7.2 Softwarekwetsbaarheden

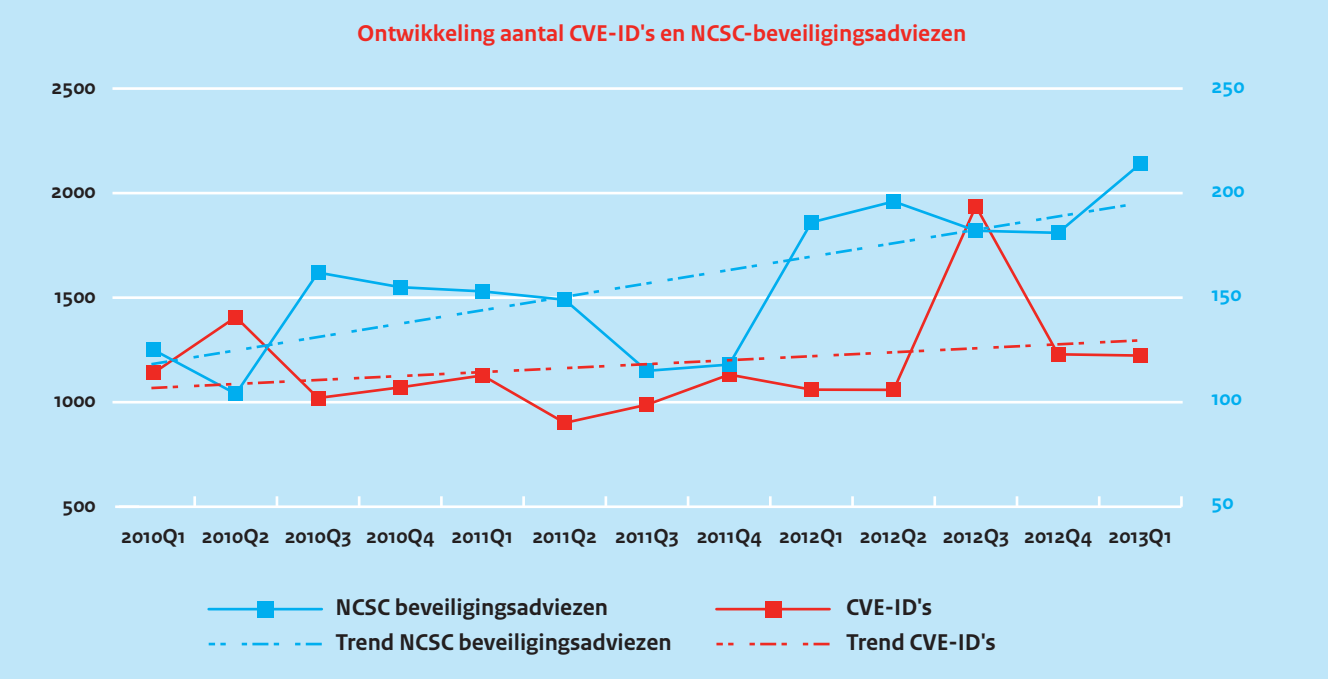
Op basis van een analyse van de Amerikaanse National Vulnerability Database (NVD) en de beveiligingsadviezen van het Nederlandse Nationaal Cyber Security Centrum geeft deze paragraaf inzicht in de hoeveelheid en de ernst van kwetsbaarheden die in software aanwezig zijn. In de NVD vormen de zogenaamde Common Vulnerabilities and Exposures (CVE's) een eenduidige en wereldwijd erkende identificatie van publiek bekende informatiebeveiligingskwetsbaarheden.

7.2.1 *Aantallen registraties*

In het voorgaande Cybersecuritybeeld concludeerden we dat het aantal CVE-registraties op jaarbasis afnam. Inmiddels is deze trend doorbroken en is het aantal CVE-registraties, na een daling in 2010 en 2011, in 2012 weer toegenomen (figuur 5). Het aantal kwetsbaarheden in de CVE-database in 2012 kwam neer op bijna 5.300, ten opzichte van iets meer dan 4.000 een jaar eerder (↑ 27 procent). Het aantal CVE-registraties laat per kwartaal een redelijk stabiel beeld zien, al kende het wel een duidelijke piek in het derde kwartaal van 2012. Deze piek werd vooral veroorzaakt door een groot aantal CVE-ID's in augustus en september van dat jaar (figuur 5, rode lijn). Diverse leveranciers zoals Mozilla, Adobe, Oracle, Apple en Google brachten in de betreffende maanden patches uit voor gevonden kwetsbaarheden, wat hoogstwaarschijnlijk heeft gezorgd voor de grote hoeveelheid nieuwe CVE-ID's.

Het aantal beveiligingsadviezen van het NCSC (figuur 5, blauwe lijn) heeft een duidelijke vlucht genomen sinds het eerste kwartaal van 2012.[186] Dit kan niet eenduidig toegeschreven worden aan een stijging in het aantal kwetsbaarheden; sinds januari 2012 worden de beveiligingsadviezen niet alleen meer richting een vaste groep van contactpersonen gepubliceerd, maar ook op de website www.ncsc.nl.[187] Met het breder beschikbaar komen van de beveiligingsadviezen, neemt ook de lijst met producten waarvoor het NCSC een beveiligingsadvies publiceert toe. Dit verklaart grotendeels de stijging in het aantal adviezen sinds het eerste kwartaal van

186 Het betreft hier het aantal initiële beveiligingsadviezen (versie 1.00) en niet de updates hierop.
187 https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen

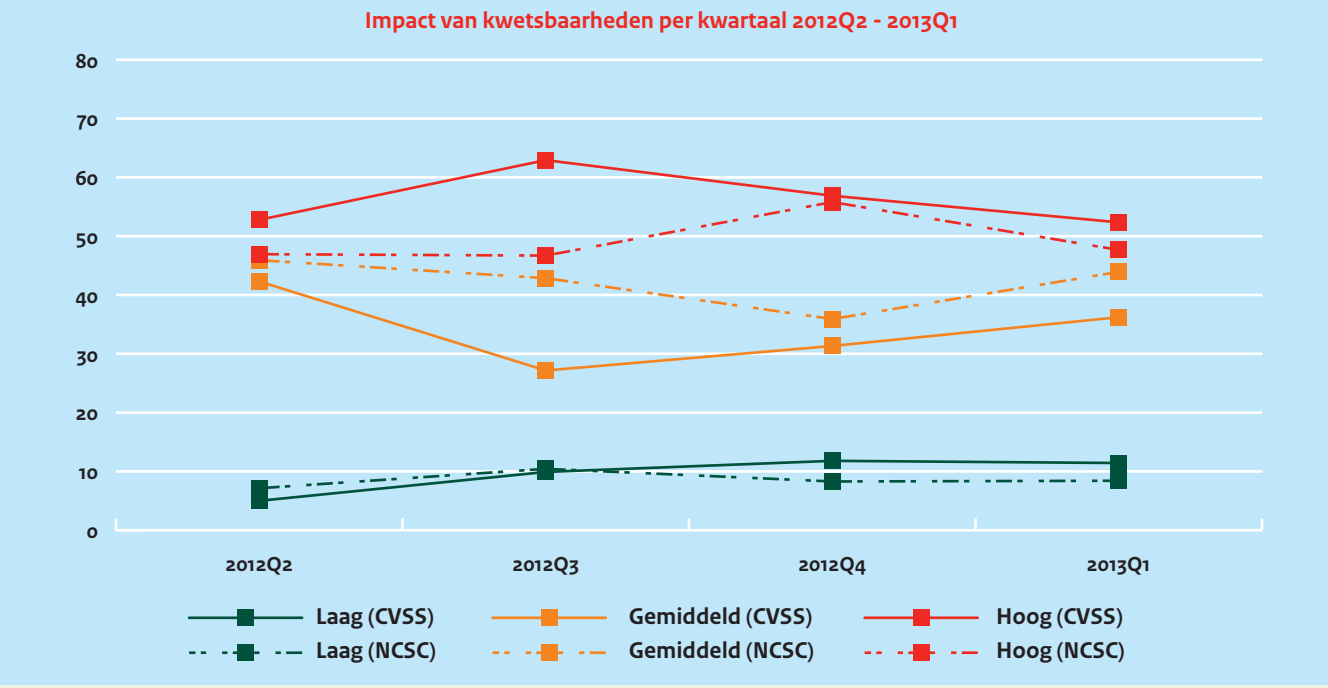


Figuur 5. Aantal CVE-ID's per kwartaal

2012.[188] De analyse van deze (bekende) kwetsbaarheden laat onverlet dat er sprake is van een (groot) aantal onbekende kwetsbaarheden.

7.2.2 Impact van kwetsbaarheden in software

Een analyse van de CVE-registraties en NCSC-beveiligingsadviezen laat zien dat de meeste kwetsbaarheden een gemiddelde impact hebben: dit geldt voor ongeveer 40 tot 61 procent van alle kwets-



Figuur 6. Ernst van de kwetsbaarheden per kwartaal

188 Belangrijk te vermelden is dat een CVE-ID in veel gevallen een enkele kwetsbaarheid beschrijft, terwijl een NCSC-beveiligingsadvies meerdere CVE-ID's kan koppelen indien het bijvoorbeeld een patch van een leverancier betreft waarmee deze leverancier een groot aantal kwetsbaarheden in één keer verhelpt.

baarheden (figuur 6). Gedurende de afgelopen vier kwartalen hebben zich weinig veranderingen voorgedaan in de impact van kwetsbaarheden.

Wat opvalt, is dat het aandeel kwetsbaarheden met de hoogste CVSS-score (10) in de afgelopen jaren is toegenomen. Dit betekent dat voor een steeds groter gedeelte van de kwetsbaarheden geldt dat deze eenvoudig zijn uit te buiten (op afstand, niet complex en zonder authenticatie) en deze daarnaast een hoge impact hebben (zowel beschikbaarheid, integriteit als vertrouwelijkheid komen in het geding). Dit benadrukt het belang van patchen van software.

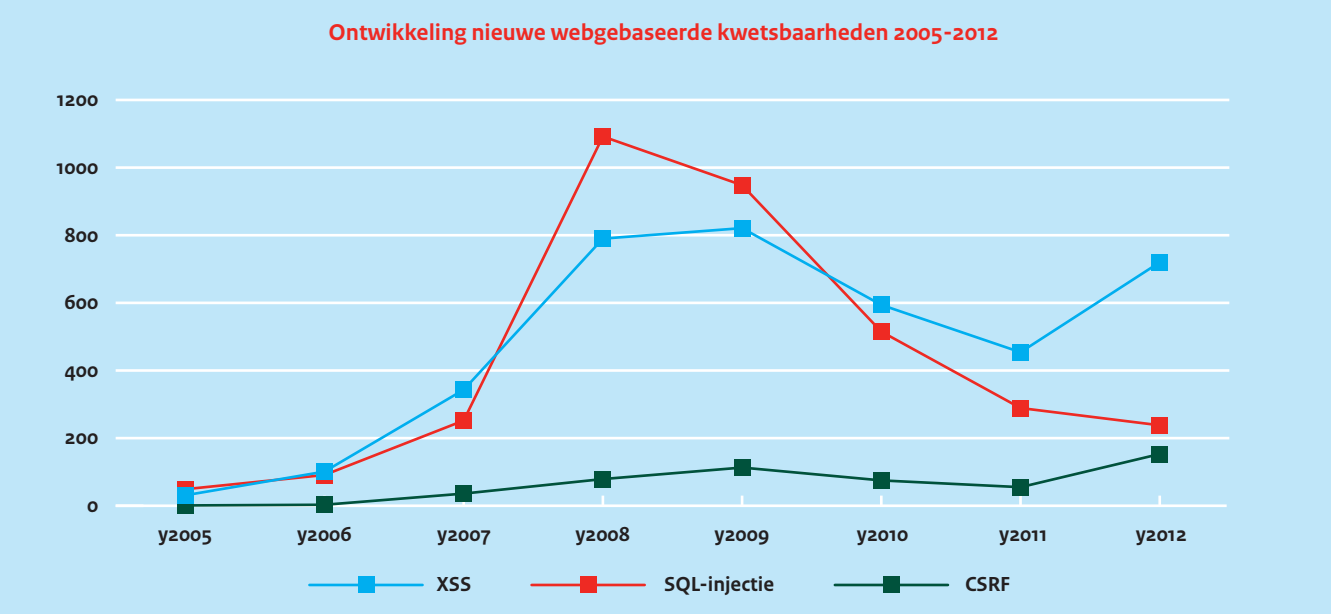
7.2.3 *Oorzaken van kwetsbaarheden in software*

Tabel 8 beschrijft de top 10 oorzaken van kwetsbaarheden in de rapportageperiode van dit CSBN.

Onderzoek toont aan dat fouten met geheugenbeheer (voornamelijk bufferoverflows) in standaardsoftware al meer dan 25 jaar de meest voorkomende kwetsbaarheden zijn, ondanks de vele maatregelen die in de tussentijd zijn ontwikkeld.[55: VU 2012]

	Omschrijving	Aantal registraties
1	**Bufferoverflow**	625
2	**Cross-site scripting (XSS)**	556
3	**Onvoldoende invoervalidatie**	503
4	**Probleem in rechten en toegangsbeperkingen**	498
5	**Resourcemanagement**	283
6	**Onbedoelde vrijgave van informatie**	184
7	**SQL-injectie**	146
8	**Reken- en conversiefouten**	124
9	**Cross-site request forgery (CSRF)**	122
10	**Code-injectie**	105

Tabel 8. Belangrijkste oorzaken van kwetsbaarheden



Figuur 7. Ontwikkeling webgebaseerde kwetsbaarheden

Opvallend is dat veel van de kwetsbaarheden verband houden met webapplicaties: cross-site scripting (XSS), SQL-injectie en cross-site request forgery (CSRF) komen vaak voor in webapplicaties en vormen daarmee ook de oorzaak van veel kwetsbaarheden. In het geval van SQL-injectie zien we een duidelijke daling sinds een piek in 2008 (figuur 7). Voor XSS zien we helaas echter weer een toename. Dit is opmerkelijk, zeker gezien het feit dat XSS bij ontwikkelaars inmiddels een bekende kwetsbaarheid verondersteld mag worden. De onderstaande grafiek schetst de trendmatige ontwikkeling van deze webgebaseerde kwetsbaarheden gedurende de afgelopen jaren.

7.2.4 *Gevolgen van kwetsbaarheden in software*

Het NCSC maakt gebruik van een standaardlijst van schadeomschrijvingen om de impact van het misbruik van een kwetsbaarheid te categoriseren. Ieder beveiligingsadvies wordt aan één of meerdere van deze standaardschadeomschrijvingen gekoppeld, waardoor een beeld ontstaat van de belangrijkste schades van kwetsbaarheden. De onderstaande tabel toont de schades die gekoppeld zijn aan de NCSC-beveiligingsadviezen die gedurende de periode van dit CSBN

zijn uitgebracht.[189] De meeste beveiligingsadviezen hadden als belangrijkste schade de mogelijkheid tot het uitvoeren van een DoS-aanval Daarna volgen het uitvoeren van willekeurige code met beperkte rechten en de toegang tot gevoelige gegevens.

	Schade	Percentage
1	Denial-of-service (DoS)	45,7%
2	Uitvoeren van willekeurige code (met gebruikersrechten)	39,1%
3	Toegang tot gevoelige gegevens	19,7%
4	Omzeilen van een beveiligingsmaatregel	17,1%
5	Verhoogde gebruikersrechten	14,4%
6	Toegang tot systeemgegevens	10,1%
7	Omzeilen van authenticatie	5,8%
8	Uitvoeren van willekeurige code (met beheerdersrechten)	4,8%
9	Spoofing	3,5%
10	Manipulatie van gegevens	3,4%

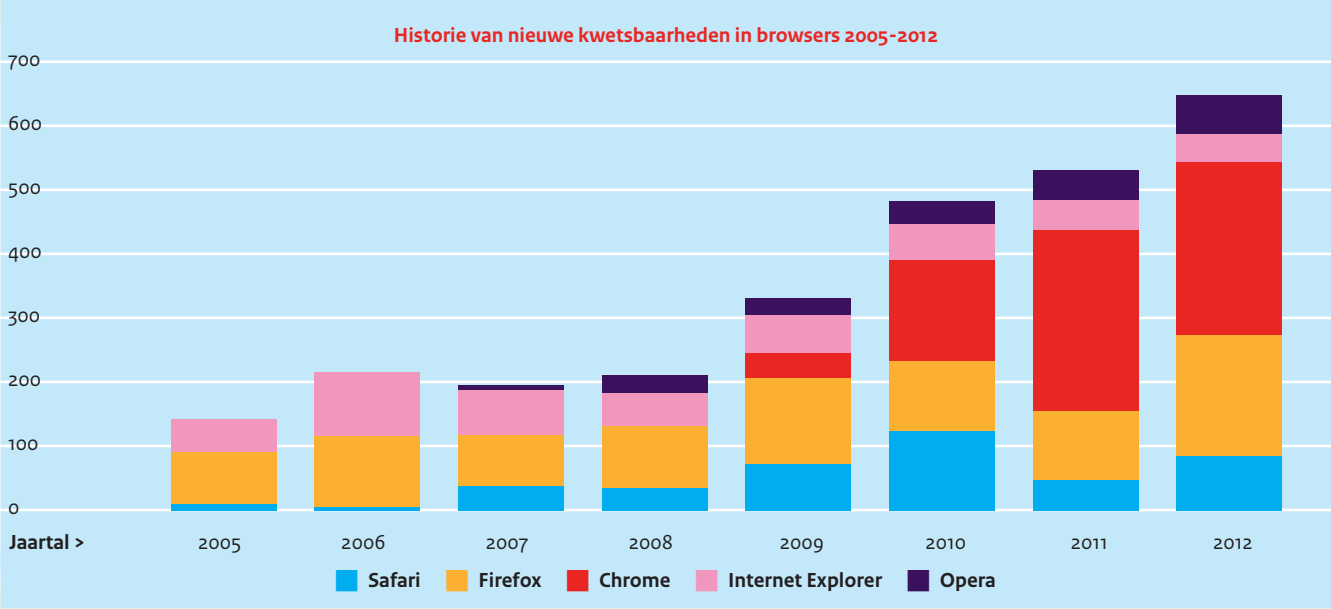
Tabel 9. Schadeomschrijvingen bij NCSC-beveiligingsadviezen

7.2.5 *Kwetsbaarheden in browsers en CMS'en*

In het vorige Cybersecuritybeeld concludeerden we al dat van alle geregistreerde kwetsbaarheden een groot deel wordt gevonden in webbrowsers. Ook in deze rapportageperiode blijken veel populaire webbrowsers (Google Chrome, Mozilla Firefox en Apple Safari) voor te komen in de top 10 met kwetsbaarheden. Ook twee populaire toevoegingen voor webbrowsers (Oracle Java en Adobe Flash Player) komen wederom voor in de top 10.

Wanneer we kijken naar het totaal aantal kwetsbaarheden in populaire webbrowsers gedurende de afgelopen jaren zien we een continue toename van kwetsbaarheden sinds 2008 (figuur 8).[190] Een mogelijke verklaring hiervoor vormt Google Chrome: een belangrijk deel van de nieuwe kwetsbaarheden bevindt zich in Google Chrome (figuur 8). Dit is logisch gezien het feit dat Google onderzoekers aanmoedigt om nieuwe kwetsbaarheden te melden. Google beloont hierbij onderzoekers wanneer er daadwerkelijk een kwetsbaarheid aanwezig blijkt te zijn.

Een andere interessante groep van applicaties vormen de *content management systems* (CMS). Met een CMS wordt de inhoud van een website gebouwd en beheerd. In het vorige Cybersecuritybeeld werd al geconcludeerd dat veel CMS-installaties (28 procent) niet voorzien zijn van de laatste updates. Eind 2012 maakte de zogenoemde bRobot-malware misbruik van kwetsbaarheden in dit type software om een malafide PHP-script[191] op kwetsbare servers te plaatsen. Via het script was het mogelijk om DDoS-aanvallen uit te voeren waarbij voornamelijk financiële instellingen in de Verenigde Staten het doelwit waren.[192] De historie van kwetsbaarheden in



Figuur 8. Ontwikkeling kwetsbaarheden in browsers

189 Aangezien een beveiligingsadvies gekoppeld kan zijn aan meerdere schadeomschrijvingen, is het totaal van de omschrijvingen uit tabel 9 meer dan 100%.

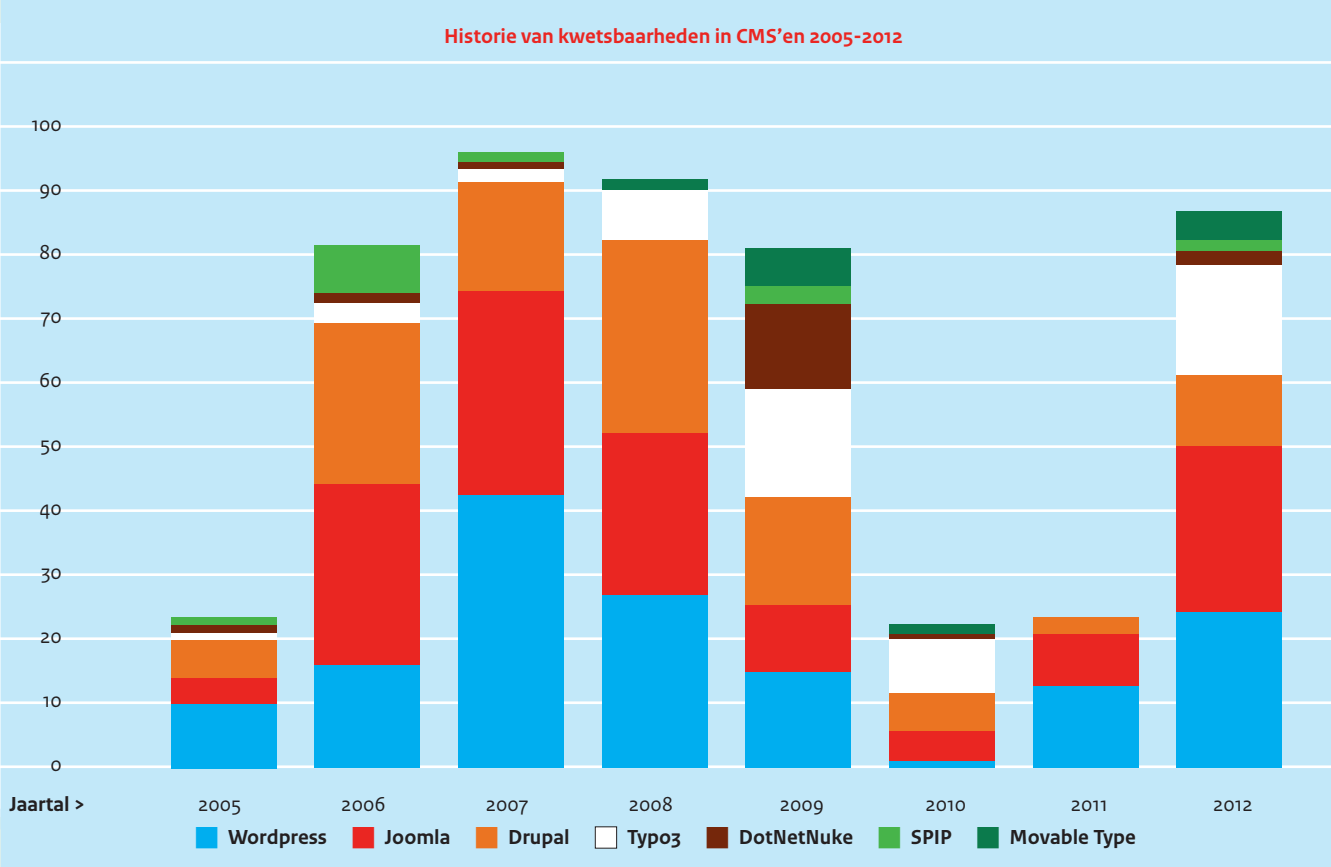
190 Het aantal kwetsbaarheden wil uiteraard niets zeggen over de aard van deze kwetsbaarheden.

191 PHP is een van de meest gebruikte programmeertalen voor websites.

192 http://ddos.arbornetworks.com/2012/12/lessons-learned-from-the-u-s-financial-services-ddos-attacks/

populaire CMS'en toont over het afgelopen jaar een enorme toename in kwetsbaarheden ten opzichte van de voorgaande twee jaren. In 2010 en 2011 waren voor deze producten respectievelijk 22 en 23 CVE-ID's bekend. In 2012 was dit aantal 86 (↑ 374 procent ten opzichte van 2011). Daarbij moet wel worden aangetekend dat de kwetsbaarheden zich veelal bevinden in toevoegingen (plug-ins) van andere partijen en niet zozeer in de kern van het CMS zelf.

langer meer door de leverancier van het CMS wordt ondersteund. Het is echter gevaarlijk om puur en alleen op basis van de versienummers conclusies te trekken over de kwetsbaarheden die aanwezig zijn. Zo bieden Linux-distributies bijvoorbeeld kant-en-klare CMS-packages aan die gebaseerd zijn op een oudere versie van het CMS, maar in sommige gevallen wel security fixes van nieuwere versies bevatten (*security fix backporting*). Uitgaande van een zeer



Figuur 9. Ontwikkeling CMS-gebaseerde kwetsbaarheden

7.2.6 *Stand van zaken websites in het .nl-domein*

Net als in het vorige Cybersecuritybeeld is ook dit keer een analyse gemaakt van de websites binnen het .nl-domein. De websites vallen uiteen in drie verschillende domeinen: overheid algemeen, overheid gemeenten en Alexa top 1.000 (top 1.000 van meest bezochte .nl-domeinen, www.alexa.com)

CMS-versies

Net als in 2012 is voor dit Cybersecuritybeeld een onderzoek verricht naar de gebruikte versies van populaire CMS-software. In totaal zijn 290 installaties van Joomla, Drupal, Wordpress en Typo3 onderzocht. Over het geheel genomen blijkt dat 38,6 procent van alle installaties volledig up-to-date is en gebruikmaakt van de laatste beschikbare versie van het CMS. In totaal loopt 16,2 procent één versie achter en 45,2 procent van alle installaties heeft een versienummer dat minimaal twee security-updates achterloopt of niet positief scenario (de door de distributies aangeboden versies zijn up-to-date) komt het percentage systemen dat niet up-to-date is rond de 10 procent te liggen. Dit zorgt ervoor dat deze websites kwetsbaar zijn.

SSL-configuraties

Binnen het onderzoek zijn in totaal 1.107 systemen geïdentificeerd die op basis van SSL te bereiken zijn. Om te beoordelen in hoeverre de betreffende SSL-systemen veilig geconfigureerd zijn, zijn deze gecontroleerd op vier relevante aanbevelingen uit de 'SSL/TLS Deployment Best Practices Guide'.[193] Tabel 10 op pagina 86 toont hoeveel systemen een kwetsbare configuratie kennen.

193 https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.0.pdf

Kwetsbaarheid	Aantal systemen	Pct
"SSL v2 is insecure and must not be used"	194	17,5%
"Anonymous Diffie-Hellman (ADH) suites do not provide authentication"	20	1,8%
"NULL cipher suites provide no encryption"	1	0,1%
"Suites with weak ciphers (typically of 40 and 56 bits) use encryption that can easily be broken"	1 (40 bits) 212 (56 bits) 266 (40+56 bits)	43,3%

Tabel 10. SSL-configuraties

Wat vooral een groot probleem lijkt, is dat veel SSL-systemen nog steeds sleutels van 40 of 56 bits ondersteunen om een versleutelde verbinding met de client tot stand te brengen. Hoewel dit in de praktijk waarschijnlijk niet vaak zal gebeuren (omdat het systeem ook langere sleutellengtes ondersteunt), is het een best practice om via een configuratiewijziging dergelijke zwakke verbindingen onmogelijk te maken. Aangetekend dient te worden dat hier alleen is gekeken naar systemen die SSL aanbieden. Er zijn nog grotere aantallen sites die verbindingen aanbieden die niet met SSL zijn beveiligd.

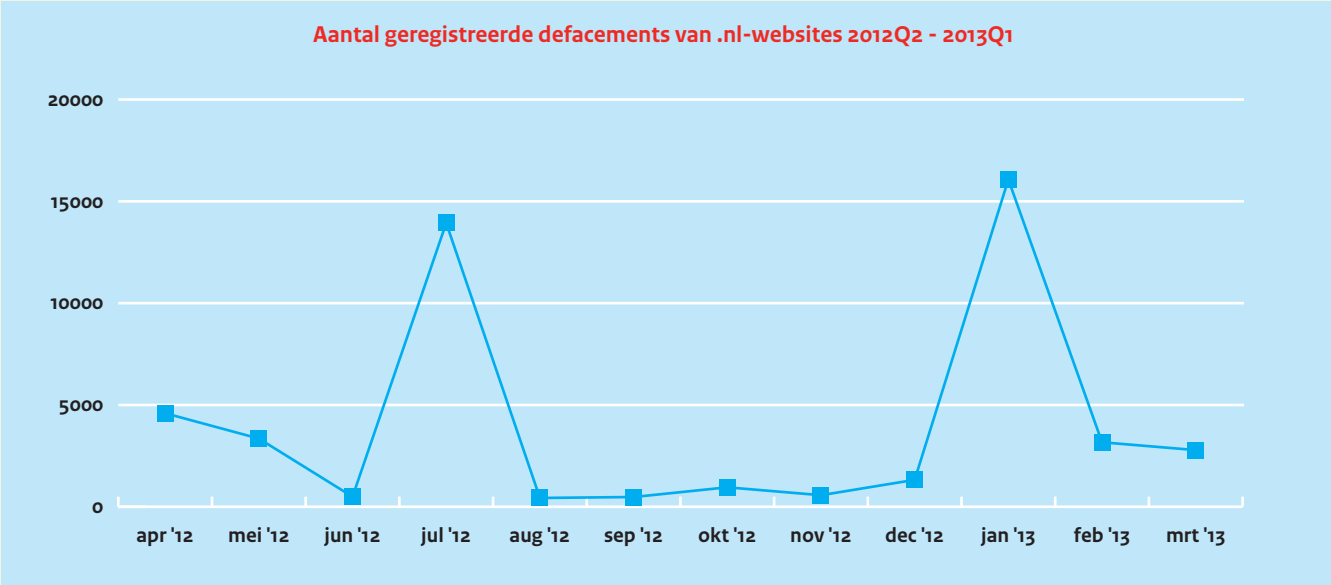
Defacements

In de periode van dit Cybersecuritybeeld werden bijna 50.000 defacements uitgevoerd op websites binnen het .nl-domein.[194] Bij een defacement plaatst een aanvaller een eigen pagina op een webserver om op die manier bijvoorbeeld een boodschap te verspreiden of om aan te tonen dat een webserver een lek bevat. Aangezien aanvallers dit soort defacements – en eventuele details – vaak registreren bij ZoneH, biedt deze site waardevolle informatie over deze defacements en de achterliggende aanvallen.

Helaas blijken defacements van websites aan de orde van de dag: gemiddeld worden ongeveer 4.000 defacements op het .nl-domein teruggevonden in ZoneH. Daarbij zijn wel grote uitschieters terug te vinden: zo vonden er in januari 2013 bijvoorbeeld meer dan 16.000 defacements plaats en in augustus 2012 slechts 434. In enkele gevallen was sprake van zogenoemde 'mass defacements' waarbij in één keer een groot aantal websites wordt aangevallen via eenzelfde kwetsbaarheid bij eenzelfde provider. Zo werd in april 2012 bijvoorbeeld één IP-adres aangevallen waarop 2.789 websites geconfigureerd waren.

Andere punten die naar voren komen uit de registraties van defacements zijn:

- De belangrijkste kwetsbaarheid die werd misbruikt voor het compromitteren van de websites was file inclusion (36 procent), gevolgd door een aanval op de inloggegevens van de beheerder (8,7 procent) en SQL-injectie (3,2 procent). In ruim 43 procent van de gevallen is niet opgegeven wat de oorzaak is.
- Defacements vonden veruit het vaakst plaats richting Linux-systemen: in ruim 61 procent van de gevallen draaide een website op dit besturingssysteem. In 30 procent van de gevallen was het besturingssysteem onbekend. Op afstand van Linux volgen Microsoft Windows (2,5 procent) en FreeBSD (2,1 procent) als gebruikte platformen.
- De belangrijkste redenen om een defacement uit te voeren zijn voor de lol (41 procent) en om de beste defacer te zijn (34 procent). In slechts 1 procent van de gevallen vindt de defacement plaats uit politieke overwegingen. Bij 20 procent van de defacements heeft de aanvaller geen reden opgegeven.



Figuur 10. Defacements binnen het .nl-domein (bron: ZoneH)

194 Bron: meldingen ZoneH voor het .nl-domein.

» Bijna een derde van de defacements (32 procent) vond plaats op zaterdag.
» Ruim een kwart van de defacements (27 procent) is uitgevoerd door dezelfde hacker of hackersgroep ('Tor3x').

IPv6 en DNSSEC

Tijdens het onderzoek naar de eigenschappen van websites is ook gekeken naar de ondersteuning van DNSSEC en IPv6 binnen de eerdergenoemde categorieën. Dit levert de volgende bevindingen op:

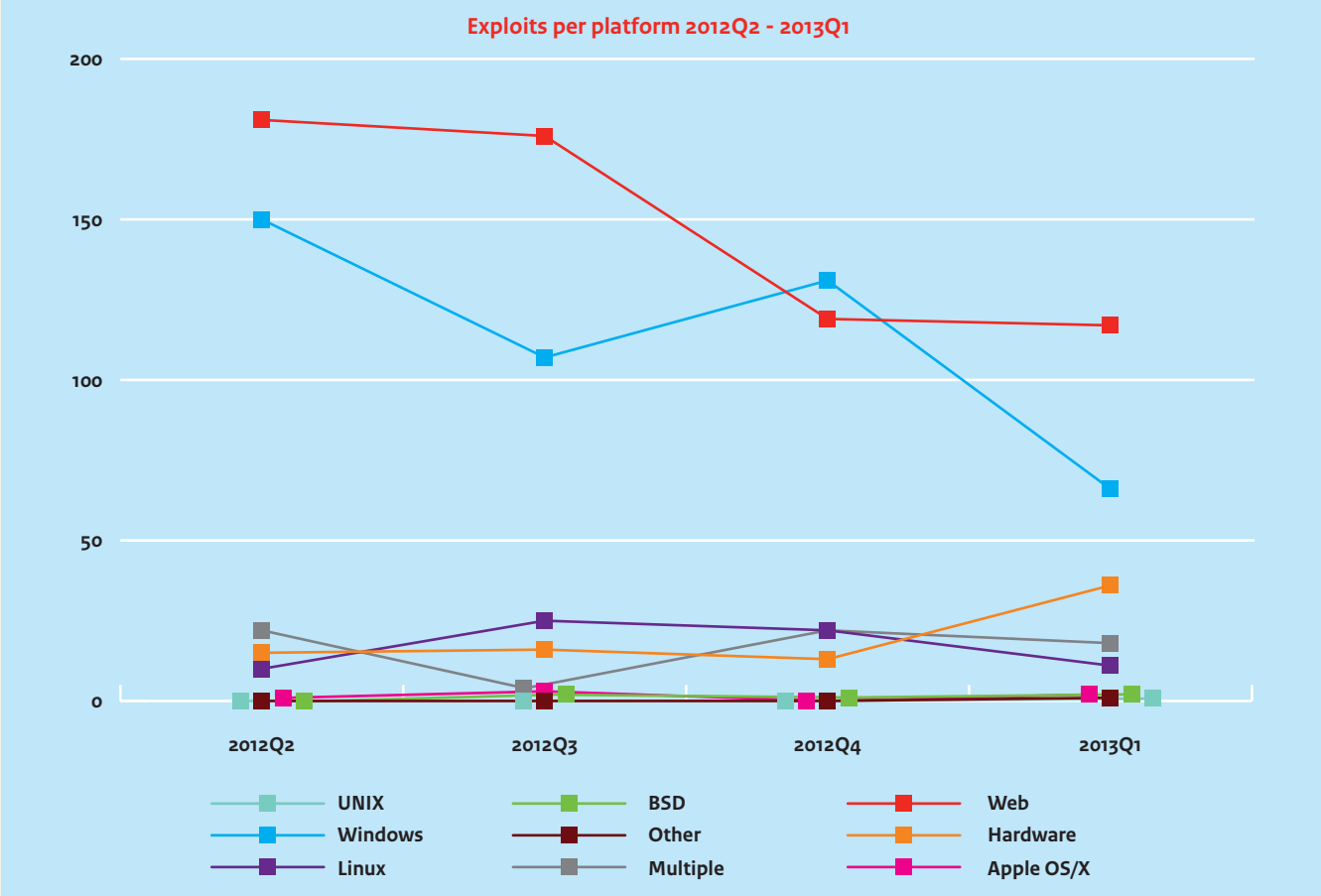
» Ongeveer 12 procent van de bijna 2.000 onderzochte domeinen heeft ondersteuning voor DNSSEC. Deze ondersteuning is vooral aanwezig in de grootste 1.000 domeinen volgens Alexa.com (17 procent) en veel minder bij de overheid en gemeenten (beide 7 procent).
» Ondersteuning voor IPv6 lijkt achter te blijven bij de ondersteuning van DNSSEC: voor ongeveer 3 procent van alle domeinen is er een IPv6-adres gekoppeld aan de 'www'-host voor dat domein. Ook hier lijkt de Alexa top 1.000 voor te lopen op de overheid: 4,5 procent tegen 2,4 procent bij de overheid en 0,6 procent bij gemeenten. Het gemiddelde is consistent met het beeld van bijvoorbeeld IBM die in juni 2012 vaststelde dat circa 3procent van alle internetsites voorzien is van een IPv6-adres.

7.3 Gebruikte hulpmiddelen

Twee soorten hulpmiddelen zijn, als verdieping op het kernbeeld, in dit hoofdstuk nader uitgewerkt, te weten exploits en malware. Het hulpmiddel botnets komt in een separaat verdiepingskatern aan de orde.

7.3.1 Exploits

Op internet verschijnen regelmatig exploits waarmee op eenvoudige wijze misbruik kan worden gemaakt van bekende en onbekende kwetsbaarheden. Een analyse van de uitgebrachte exploits levert inzicht in de ontwikkeling van deze exploits gedurende de jaren. Exploit-db.com is een website die exploits verzamelt en deze beschikbaar stelt voor iedereen. Kijkende naar de exploits die vanaf 2005 gepubliceerd zijn, zien we sinds het derde kwartaal van 2010 een flinke afname van publiek beschikbare exploits. Ook IBM meldt een afname van publieke exploits te zien sinds een top in 2010.[15: IBM 2012] Als belangrijkste oorzaak hiervan noemt IBM de veranderingen die in software zijn doorgevoerd waardoor het moeilijker is geworden om kwetsbaarheden uit te buiten. Een andere mogelijke oorzaak is dat nieuwe (nog onbekende) kwetsbaarheden nu commercieel verhandeld worden.



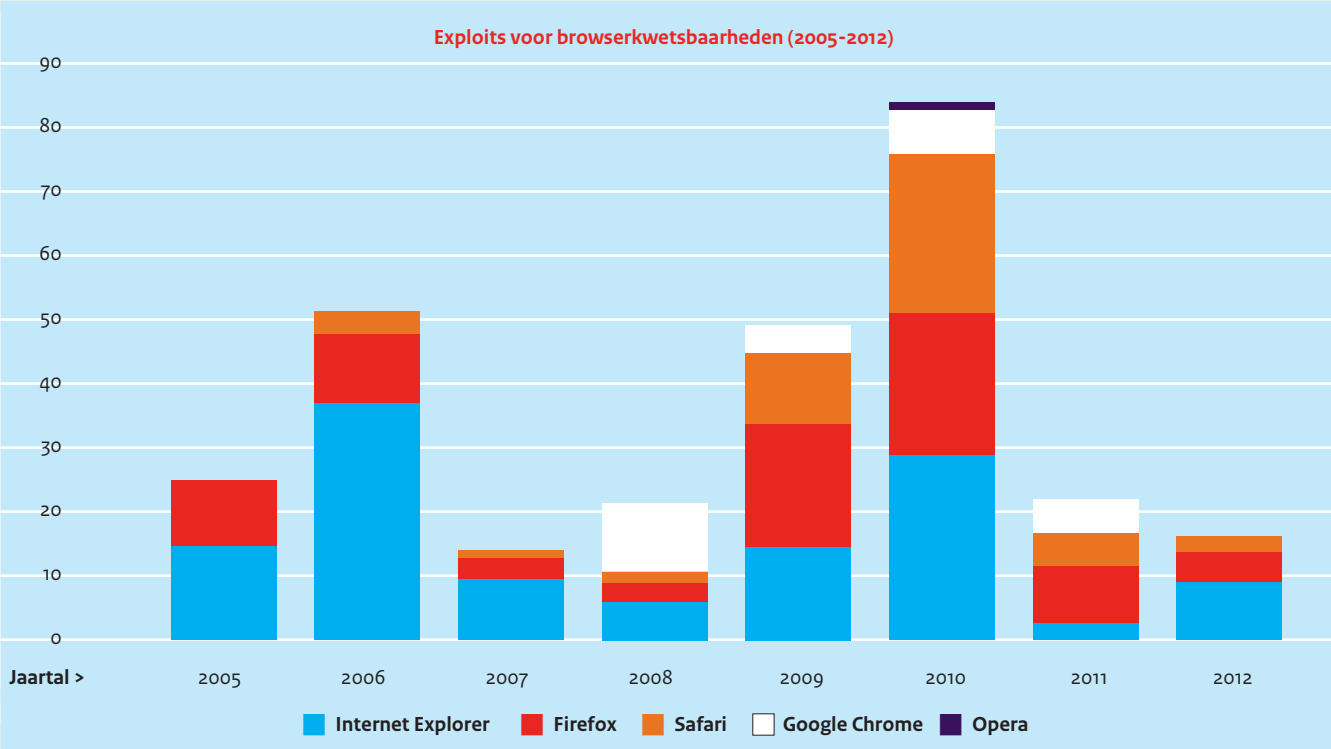
Figuur 11. Exploits per platform

Exploits richten zich voornamelijk op webplatformen en Microsoft Windows. Vooral PHP vormt een populair aanvalsplatform; veel open source PHP-applicaties en plug-ins voor CMS-toepassingen zoals Wordpress zijn terug te vinden tussen de PHP-exploits.

Zoals eerder is beschreven, neemt het totaal aantal kwetsbaarheden in browsers steeds verder toe. Op basis hiervan zou men kunnen verwachten dat ook het aantal beschikbare exploits voor browsers stijgt. Dit blijkt echter niet het geval. Figuur 12 toont het totaal aantal exploits dat beschikbaar is voor de browsers zoals eerder ook al beschreven bij de kwetsbaarheden.

misbruiken. Een actueel overzicht[196] van 38 verschillende exploitkits (en versies daarop) leert dat er 65 kwetsbaarheden bestaan die deze exploitkits gezamenlijk actief misbruiken. Sommige exploitkits bevatten slechts 2 exploits terwijl andere exploitkits er meer dan 10 misbruiken.

Exploitkits bevatten in de regel exploits die effectief blijken te zijn en misbruik maken van kwetsbaarheden in software die op veel systemen geïnstalleerd is. Op die manier is de kans het grootst dat via het exploitkit in korte tijd grote aantallen systemen kunnen worden geïnfecteerd. Het blijkt dat Oracle Java en Microsoft Internet



Figuur 12. Ontwikkeling aantal exploits voor browsers

Uit deze figuur blijkt dat het aantal browserexploits een toppunt bereikte in 2010 (84 exploits) en daarna zeer snel afnam tot slechts 16 in 2012.

7.3.2 *Exploitkits*

Exploitkits bundelen kant-en-klare exploits voor kwetsbaarheden waarmee het eenvoudig is om in korte tijd grote hoeveelheden systemen te infecteren. Vaak zetten criminelen exploitkits in om via zogenoemde 'drive by'-aanvallen een botnet op te bouwen. Contagiodump[195] is een bron op internet die informatie over exploitkits verzamelt en beschikbaar stelt, waardoor inzicht ontstaat in de exploitkits die er bestaan en de kwetsbaarheden die zij

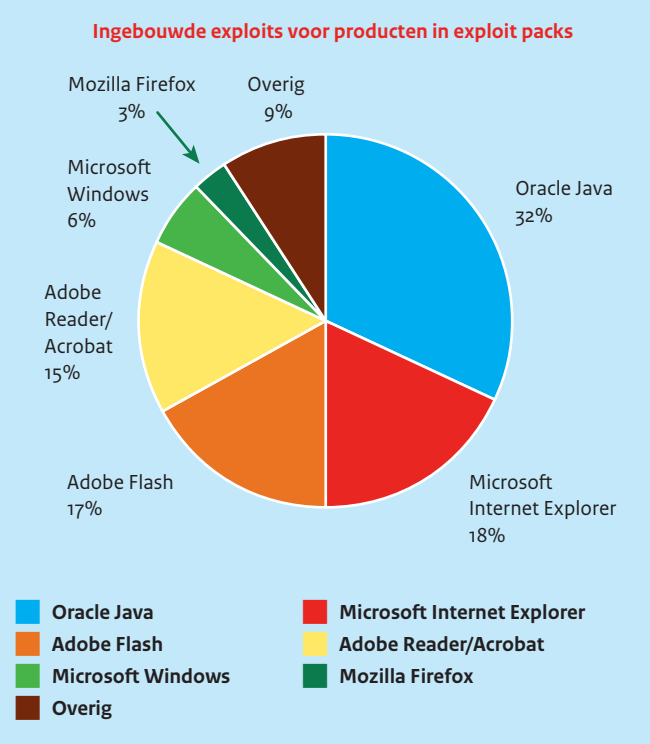
Explorer veruit de populairste aanvalsdoelen zijn van de exploitkits: de helft van alle exploits heeft betrekking op deze producten.

Daarna volgen Adobe Flash en Adobe Reader. Figuur 13 toont een overzicht van de producten waarop de exploitkits zich richten.

De exploitkits bevatten in sommige gevallen zelfs nog exploits voor kwetsbaarheden in Internet Explorer uit 2004 en 2005 (Internet Explorer 5.01, 5.5 en 6, die vaak nog in gebruik zijn in combinatie met Windows XP). Dit duidt erop dat deze verouderde en soms al niet meer ondersteunde versies nog steeds in gebruik zijn.

195 http://contagiodump.blogspot.com

196 https://docs.google.com/spreadsheet/ccc?key=0AjvsQV3iSLa1dE9EVGhjeUhvQTNReko3c2xhTmphLUE&usp=sharing (bijgewerkt maart 2013).



Figuur 13. Misbruikte software door exploit kits

Dat aanvallen op genoemde producten succesvol kunnen zijn, volgt ook uit cijfers die Microsoft publiceerde aangaande het installeren van beveiligingsupdates door eindgebruikers.[24: MS 2012-1] Uit deze cijfers blijkt bijvoorbeeld dat 94 procent van de wereldwijde computers met Java de laatste update van deze software niet heeft geïnstalleerd en dat 51 procent van alle computers zelfs de laatste drie updates van Java mist. Ook voor andere software zoals Adobe Reader en Flash Player geldt dat bijna de helft van de eindgebruikers de laatste drie updates van deze software missen. Een andere alarmerende conclusie van Microsoft is dat 7 procent van alle gebruikers van Adobe Reader een versie hebben die niet langer meer door Adobe wordt ondersteund en waarvoor Adobe dus geen updates meer uitbrengt. Voor Microsoft Word ligt dit percentage zelfs op 9 procent.

Populaire exploitkits zoals BlackHole, Cool Exploit, Eleanore, Incognito, Yes en Crimepack automatiseren het infecteren van computers via het misbruiken van kwetsbaarheden. Vaak zijn de misbruikte kwetsbaarheden bekend en niet nieuw. In sommige gevallen gaat het om zero-day kwetsbaarheden. De meest opvallende ontwikkeling op het gebied van exploitkits was het disproportionele aantal Java-kwetsbaarheden dat wordt misbruikt.

7.3.3 Malware en infrastructuur

De meeste malware richt zich op het verzamelen van financieel aantrekkelijke gegevens zoals creditcard- of userid/password-gegevens. Vaak wordt de bijvangst – zoals bezochte websites, ingevulde formuliergegevens en toetsaanslagen – ook verzameld.

De mogelijkheden die de gemiddelde malware heeft, zijn breder. Zo is het vaak ook mogelijk om heimelijk documenten te kopiëren, schermafbeeldingen te maken of opnames met webcam of ingebouwde microfoon te maken. Er zijn reeds voorvallen bekend waar dergelijke technieken zijn ingezet voor spionage, maar ook voor afpersing of voyeurisme. Het wordt voor kwaadwillenden steeds makkelijker en aantrekkelijker om dergelijke gegevens te bemachtigen en te misbruiken of te verkopen.

Zoals in het kernbeeld omschreven, vormt malware een vast onderdeel van cybercrime. De verspreiding van malware wordt steeds massaler en makkelijker. Een van de huidige trends is het verspreiden van malware via legitieme websites. Malware richt zich steeds vaker op verschillende platformen, waaronder ook Mac OS X, mobiele platformen en in het geval van statelijke malware ook op specifieke industriële systemen. Tools voor het ontwikkelen, verspreiden en beheren van malware en malafide infrastructuur wordt steeds professioneler. Nieuwe malware wordt in beperkte mate gedetecteerd door virusscanners en malware is steeds lastiger te verwijderen van een systeem. In het voorgaande CSBN is al aangegeven dat ongeveer 30 procent van de computers besmet is met malware.

Het NCSC beschikt in toenemende mate over informatie over malware-infecties, malafide infrastructuren en indicatoren over geavanceerde malware. Organisaties hebben echter vaak nog geen goed ingerichte detectiemechanismen. Als respons wordt door getroffen organisaties doorgaans volstaan met het opnieuw inspoelen van geïnfecteerde systemen. Hierdoor is achteraf niet vast te stellen wat de impact van een infectie is geweest.

Afgaande op informatie uit openbare bronnen kunnen de ontwikkelingen op het gebied van geavanceerde aanvallen, malware en malafide infrastructuur als volgt worden samengevat:

- Er is een toename waargenomen in statelijke cyberspionage en -sabotageactiviteiten.
- Geavanceerde aanvallen worden steeds vaker ook op kleinere organisaties uitgevoerd.[48: Symantec 2013]
- Geavanceerde technieken die gebruikt zijn door statelijke actoren worden overgenomen door georganiseerde criminelen.[197]
- De aanvaller raakt steeds meer in het voordeel. Ondanks diverse initiatieven voor verbetering raken de verdedigingsmaatregelen, -methodes en -initiatieven steeds verder achter ten opzichte van de mogelijkheden van de opponenten.

7.3.4 Geavanceerde malware

Sinds het voorgaande CSBN zijn er opnieuw vormen van zeer geavanceerde malware ontdekt door onderzoekers. De Wiper-, Flame-, Miniflame- en Gauss-malware is verbonden met eerder

197 http://blogs.mcafee.com/mcafee-labs/signed-malware-you-can-runbut-you-cant-hide, https://www.securelist.com/en/blog/682/Mediyes_the_dropper_with_a_valid_signature, http://arstechnica.com/security/2012/09/adobe-to-revoke-crypto-key-abused-to-sign-5000-malware-apps/

Geavanceerde malware

In het CSBN-1 en -2 is aandacht geschonken aan de Stuxnet- en Duqu-malware. Het afgelopen jaar is meer gelijksoortige geavanceerde malware gevonden door onderzoekers. Flame, Miniflame, Wiper en Gauss zouden meerdere overeenkomsten vertonen met Stuxnet en Duqu. De overeenkomsten beperken zich niet alleen tot de gebruikte technieken, de slachtoffers bevinden zich voornamelijk in het Midden-Oosten. Volgens de Wall Street Journal, de New York Times en The Washington Post is deze malware onderdeel van een campagne genaamd 'Olympic Games'. De Verenigde Staten zou samen met Israël sinds 2006 hebben gewerkt aan een serie aanvallen gericht op met name doelen in het Midden-Oosten. De verschillende malware zou onder andere worden gebruikt voor het verzamelen van inlichtingen over en het saboteren van het Iraanse kernprogramma, en spionage bij Libanese banken.
Onderzoekers vinden steeds meer aanwijzingen dat er een statelijke actor met een zeer hoog kennisniveau achter de aanvallen zit. Cryptanalist Marc Stevens van het Centrum Wiskunde & Informatica (CWI) in Amsterdam heeft bijvoorbeeld ontdekt dat Flame een compleet nieuwe, tot nu toe onbekende cryptografische aanvalsvariant gebruikt. Flame gebruikt een geheel nieuwe variant van een 'chosen prefix collision' aanval om zich voor te doen als een legale beveiligingsupdate van Microsoft. Het ontwikkelen van een dergelijke aanval vereist cryptanalytische kennis van hoog niveau. Verder is gebruikgemaakt van tot dusverre onbekende kwetsbaarheden en vervalste certificaten. Uit analyses van onder andere Symantec blijkt ook dat de toegang en rolverdeling van de aanvallers op C&C-servers en het opschonen hiervan buitengewoon professioneel is ingericht. Interessant is ook de tijd die ogenschijnlijk heeft gelegen tussen verspreiding van de malware en de ontdekking hiervan door onderzoekers. Het toont aan dat detectiemechanismen niet goed in staat zijn geavanceerde dreigingen te onderkennen.

Meer informatie is te vinden op:

http://online.wsj.com/article/SB10001424052702303506404577448563517340188.html?mod=WSJ_hpp_LEFTTopStories
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=2&
http://www.cwi.nl/nieuws/2012/cwi-cryptanalist-ontdekt-nieuwe-cryptografische-aanvalsvariant-in-flame-virus
http://www.fireeye.com/blog/technical/malware-research/2012/08/guys-behind-gauss-and-flame-are-the-same.html
http://online.wsj.com/article/SB10001424052702303506404577448563517340188.html?mod=WSJ_hpp_LEFTTopStories
http://www.securelist.com/en/blog/750/Full_Analysis_of_Flames_Command_Control_servers
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_flamer_newsforyou.pdf
http://www.symantec.com/connect/blogs/have-i-got-newsforyou-analysis-flamer-cc-servers
http://www.securelist.com/en/blog/20819308/What_was_that_Wiper_thing

gevonden malware zoals Stuxnet en Duqu. Berichtgeving verbindt dit vaak aan onderdelen van een Amerikaanse/Israëlische spionagecampagne gericht tegen doelen in het Midden-Oosten, met een nadruk op Iran. Andere geavanceerde malwarefamilies die onlangs zijn ontdekt, betreffen Miniduke[198], Itaduke, RedOctober[199] en TeamSpy[200]. Het is volgens openbare bronnen zeer waarschijnlijk dat inmiddels meerdere staten actief geavanceerde malware gebruiken.

De gebruikte technieken lijken door verschillende actoren te worden gekopieerd. De Shamoon-malware gebruikt een techniek om bestanden te verminken, die is gebaseerd op de Wiper-malware. Wiper is gebruikt om systemen van Iraanse oliemaatschappijen onklaar te maken. Shamoon is gebruikt in een aanval op Saudi/Aramco en RasGas.[201] Waar in het geval van Wiper sprake is van een geavanceerde en professionele aanval, gaat het in het geval van Shamoon ogenschijnlijk om kopieerwerk door een aan Iran gelieerde actor. Een ander voorbeeld van waarschijnlijk uit Iran afkomstige spionagemalware is Mahdi[202], ook deze malware is niet zeer geavanceerd en wordt waarschijnlijk gebruikt voor spionage vanuit Iran.

Westerse organisaties bieden geavanceerde vormen van spionagetechnologie, waaronder malware, op commerciële basis aan. Varianten van het door het Duits/Engelse Gamma International op de markt gebrachte FinSpy[203] bleek eerder al gebruikt te worden door opsporings- en inlichtingendiensten. Inmiddels lijkt het ook te zijn gebruikt om tegenstanders

198 http://www.h-online.com/security/news/item/Highly-specialised-MiniDuke-malware-targets-decision-makers-1813304.html
199 http://threatpost.com/en_us/blogs/rocra-espionage-malware-campaign-uncovered-after-five-years-activity-011113
200 http://threatpost.com/en_us/blogs/researchers-uncover-teamspy-attack-campaign-targeting-government-research-targets-032013
201 http://www.nytimes.com/2012/04/24/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html?_r=1 & http://www.theregister.co.uk/2012/08/30/rasgas_malware_outbreak/
202 http://www.informationweek.com/security/attacks/mahdi-malware-makers-push-anti-american/240004380
203 https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

van het regime in Bahrein te bespioneren of te censureren. Gamma International zegt de software niet aan Bahrein te hebben verkocht en vermoedt dat deze illegaal verkregen is.[204]

Er zijn volgens de media in de afgelopen periode meer situaties aan het licht gekomen waar actoren uit landen als China[205], Libië[206], Marokko, Vietnam en Syrië[207] gebruik hebben gemaakt van in het westen ontwikkelde spionagesoftware voor surveillance op activisten en journalisten.

Ook voor private organisaties blijft digitale spionage een serieuze dreiging. Het zicht op daadwerkelijke incidenten is verbeterd door publiek-private samenwerking en het delen van informatie zoals indicatoren op incidentele basis.

7.4 Tot slot

Waar de aantallen kwetsbaarheden toenemen, kan (opnieuw) geconstateerd worden dat het hier gaat om bekende kwetsbaarheden, die door goed patchen en updaten ondervangen kunnen worden. Aangezien dit echter onvoldoende gebeurt, wordt de impact van de kwetsbaarheden steeds groter. In het grootste aantal gevallen kunnen deze kwetsbaarheden leiden tot gebruik bij een DoS-aanval. Daarna volgen het uitvoeren van willekeurige code met beperkte rechten en de toegang tot gevoelige gegevens. Het aantal kwetsbaarheden in webbrowsers en CMS'en laat dit jaar een toename in kwetsbaarheden zien.

De hulpmiddelenkant heeft het afgelopen jaar een afname in het aantal gepubliceerde exploits laten zien. De oorzaak hiervan ligt waarschijnlijk in software-aanpassingen. Het gaat hierbij vooral om webplatforms, Windows en PHP. Bij de bestudering van exploitkits blijkt opnieuw dat achterstallig onderhoud op updates veel problemen veroorzaakt. Op het gebied van malware is vooral sprake van een inhoudelijk snelle ontwikkeling. Hierbij is de ontwikkeling van geavanceerde malware, vooral in relatie tot statelijke actoren, een belangwekkende trend.

De boodschap van eerdere CSBN-edities was dat bekende kwetsbaarheden de grootste problemen veroorzaken. Dit is een boodschap die onverminderd van toepassing is. «

204 http://www.bloomberg.com/news/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-may-be-stolen-copy.html
205 http://www.nytimes.com/2013/01/16/business/rights-group-reports-on-abuses-of-surveillance-and-censorship-technology.html?_r=1&
206 http://www.pcworld.com/article/2030602/reporters-without-borders-slams-five-nations-for-spying-on-media-activists.html
207 http://www.bloomberg.com/news/2012-04-24/unplug-companies-that-help-iran-and-syria-spy-on-citizens.html

8 Kwetsbaarheid van de eindgebruiker

De eindgebruiker wordt vaak genoemd als de zwakste schakel in beveiliging. Er wordt echter te veel verantwoordelijkheid bij de eindgebruiker neergelegd. Deze onderkent steeds vaker de risico's van gebruik, maar heeft te beperkte kennis en middelen om cybersecurity zelf afdoende ter hand te nemen. In plaats van een bewustwordingsprobleem kunnen we spreken van een beperkt handelingsperspectief.

Eindgebruikers vormen een belangrijk onderdeel in het beveiligen van de informatieketen. De eindgebruiker is zelf verantwoordelijkheid voor de beveiliging van zijn eigen ICT, maar kan hij deze verantwoordelijkheid wel dragen? Dit verdiepingskatern geeft inzicht in de belangen, dreigingen en kwetsbaarheden rond de eindgebruiker.

8.1 De eindgebruiker digitaliseert zowel privé als zakelijk

Eindgebruikers maken massaal gebruik van het internet, mobiele apparaten en mobiele toepassingen. Volgens onderzoek van de Universiteit Twente gebruikt 87 procent van de Nederlanders het internet dagelijks[52: UT 2012]. De voorkeursplaats van gebruik is nog steeds thuis, maar steeds vaker mobiel. Het aantal bezitters van een smartphone is in 2012 met 1 miljoen toegenomen tot circa 7 miljoen in december 2012.[19: IMGFK 2012] Waar in 2011 31 procent van de Nederlanders toegang had tot internet via een smartphone, is dit percentage in een jaar tijd gestegen tot 42 procent.

De toegenomen beschikbaarheid van internet vertaalt zich ook in toegenomen gebruik van het internet. Op een werkdag (inclusief vrije tijd) maakt de Nederlander gemiddeld 4 uur en 48 minuten gebruik van het internet. De toegenomen gebruiksduur gaat hand in hand met de toegenomen populariteit van onlinetoepassingen. Uit onderzoek van de Universiteit Twente [52: UT 2012] volgt een top 5 van internetgebruik:

1. Informatie (informatie zoeken).
2. Vermaak (internetten voor het plezier).
3. Interactie met bekenden (contacten onderhouden).
4. Transactie (aankopen doen).
5. Persoonlijke ontwikkeling (leren via het internet).

Eindgebruikers slaan hun vertrouwelijke gegevens steeds meer op in verschillende apparaten (smartphones, tablets, etc.) en (online) toepassingen en hun gegevens worden op steeds meer plekken elektronisch verwerkt. Eindgebruikers delen deze gegevens, soms zelfs noodzakelijk voor het afnemen van een dienst, met organisaties voor onlinediensten en dataopslag.

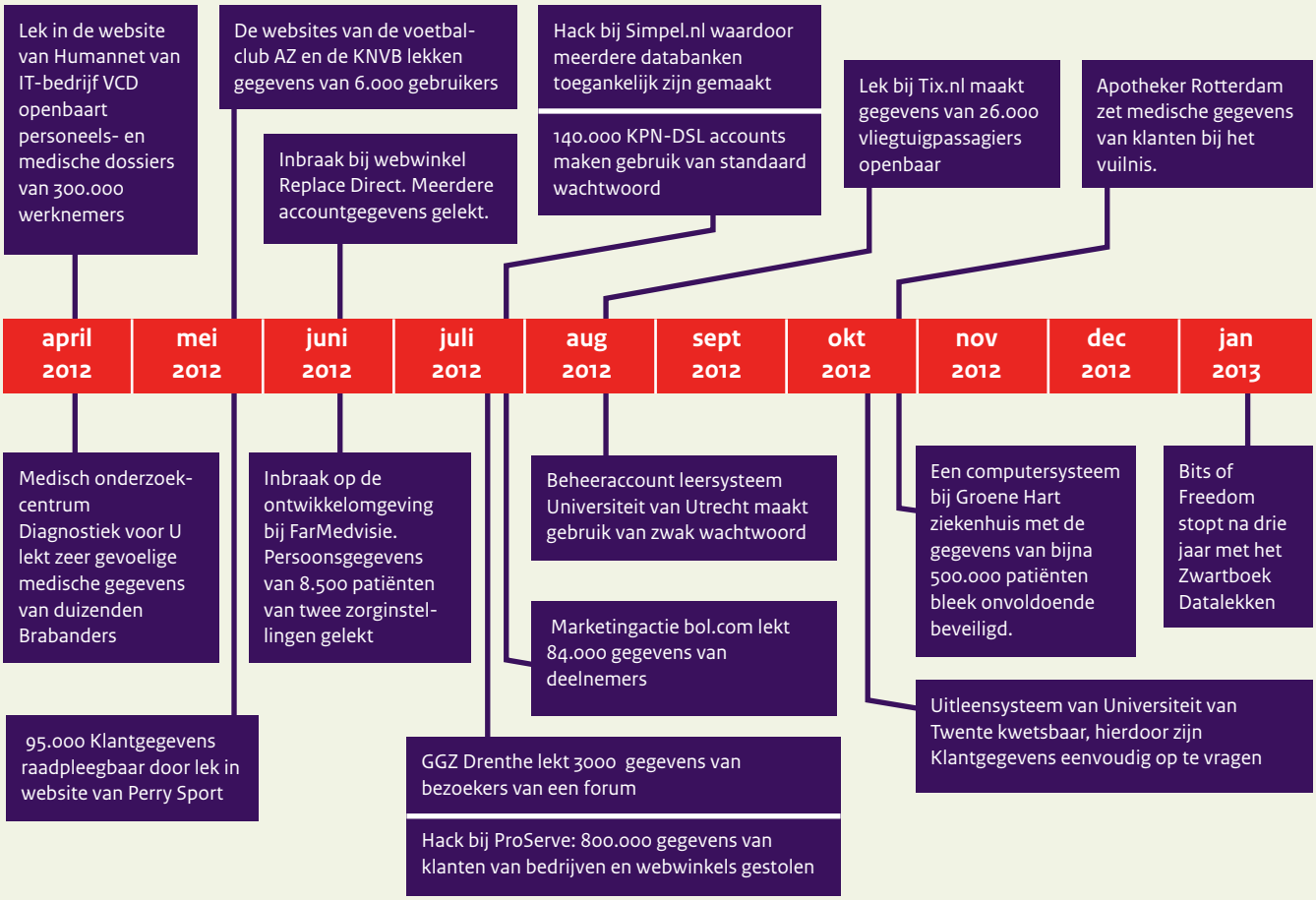
Ook het aantal apparaten in huishoudens met een internetverbinding neemt toe, zonder dat de gebruiker zich daarvan bewust is. Niet alleen smartphones en tablets zijn online, dat geldt ook voor printers, netwerkschijven (NAS), mediaplayers, etc. Zo maken bijvoorbeeld smart-tv's gebruik van het internet voor softwareupdates of voor het ophalen van programma-informatie. Ook andere slimme apparaten zoals thermostaten en beveiligingscamera's hebben een internetverbinding. Nieuw zijn de slimme energiemeters welke in steeds meer huishoudens worden geplaatst. Nu gebeurt dat nog op vrijwillige basis, maar dergelijke meters zullen binnen afzienbare tijd standaard worden geplaatst als vervangers van bestaande meters.

8.2 De eindgebruiker loopt risico

De eindgebruiker wordt bestookt met een scala aan middelen om gegevens en geld buit te maken. Relevante vormen hiervan zijn:

- Bij phishing zoeken kwaadwillenden gericht het internet af naar informatie over hun slachtoffers, die vervolgens telefonisch worden benaderd. In het verleden was deze vorm van oplichting voornamelijk gericht op financiële instellingen. In 2012 is een uitbreiding waarneembaar richting (software)leveranciers.
- Door het installeren van malware kunnen eindgebruikers worden opgenomen in een botnet. Op deze manier kan de computer van een eindgebruiker onbewust worden ingezet voor illegale handelingen, zoals het uitvoeren van DDoS-aanvallen of het verspreiden van spam. Andere malware, bijvoorbeeld banking trojans, heeft als doel om slachtoffers geld afhandig te maken bij het gebruik van internetbankieren.
- Ransomware (gijzelingssoftware) kaapt de functionaliteit van het besmette systeem, bijvoorbeeld door het versleutelen van bestanden of het blokkeren van de werking van het besturingssysteem. Om weer toegang te krijgen tot de bestanden, is zogenaamd een code vereist waarvoor het slachtoffer moet betalen.
- Een nep-antivirusproduct maakt misbruik van de behoefte aan veiligheid van computergebruikers met als doel om kwaadaardige software op de computer te installeren. Op het scherm van een gebruiker verschijnt een venster dat meldt dat de gebruiker besmet is met allerlei virussen. Na deze nepmelding volgt het verzoek om een geldbedrag te betalen, zogenaamd om de computer schoon te maken.

Ook datalekken blijven een dreiging voor eindgebruikers. Door een hack bij een onlinedienstverlener kunnen de vertrouwelijke gegevens van een eindgebruiker in handen van onbevoegden komen. Maar ook eindgebruikers zijn zelf onvoorzichtig in de omvang met privacygevoelige informatie, bijvoorbeeld door het onbeveiligd opslaan van inlognamen en wachtwoorden. Gebleken



is dat malware vaak op zoek is naar deze informatie en daarmee in handen van criminelen komt. Op het internet gepubliceerde gegevens, bijvoorbeeld de online-identiteit van een gebruiker, kunnen door anderen worden misbruikt voor het versturen van e-mailberichten, toegang tot sociale media of het uitvoeren van (financiële) onlinetransacties.

De bovenstaande figuur toont de datalekken in Nederland, die tot 14 januari 2013 door privacy-organisatie Bits of Freedom in een zwartboek zijn bijgehouden.[208]

8.3 De eindgebruiker wordt opgescheept met beveiligingsproblemen

De apparatuur die door eindgebruikers wordt aangeschaft (smartphones, laptops, printers, routers, etc.) is standaard niet altijd veilig geconfigureerd of de gebruikersinterface is onduidelijk. Leveranciers bepalen zelf hoe apparatuur standaard wordt ingesteld en zijn hierbij niet aan regels gebonden. Daardoor is het voor een gebruiker moeilijk om de apparatuur zelf veilig in te stellen en up-to-date te houden qua beveiliging. Het gevolg kan zijn dat gegevens door derden worden ingezien of gemanipuleerd.

Kwetsbaarheden in online-apparaten

In december 2012 maakte het Amerikaanse beveiligingsbedrijf Rapid7 bekend (zie ook een uitzending van KRO Reporter[209]) wereldwijd 83 miljoen apparaten aangetroffen te hebben die bereikbaar zijn voor UPnP-besturingscommando's vanaf het internet. Reden hiervoor waren de onveilige configuratie-instellingen, vaak standaard vanuit de fabriek, van UPnP (Universal Plug and Play). Hierdoor kunnen kwaadwillenden deze apparaten via het internet benaderen en vervolgens onbeschikbaar maken, de instellingen aanpassen, mee kijken met camera's of de inhoud van een netwerkschijf lezen. Van deze apparaten is een kwart zodanig ingesteld dat er ook daadwerkelijk misbruik van gemaakt kan worden.

Eindgebruikers lopen steeds meer risico door kwetsbaarheden in software die toegvoegd is aan standaard software zoals 'third-party'-add-ons en (browser)plug-ins. Volgens recent onderzoek van Secunia[210] is het aandeel van kwetsbaarheden in deze software, ten

208 https://www.bof.nl/category/zwartboek-datalekken/

209 https://www.ncsc.nl/actueel/nieuwsberichten/upnp-beperk-het-gebruik.html, http://reporter.kro.nl/seizoenen/2012/afleveringen/07-12-2012

210 http://secunia.com/vulnerability-review/vendor_update.html

opzichte van kwetsbaarheden in het standaardbesturingssysteem, gestegen van 57 procent in 2007 naar 86 procent in 2012. Een analyse van sinds 2010 uitgebrachte, unieke NCSC-advisories bevestigt deze trend.

Het bezoeken van gerespecteerde websites, zoals nieuwssites, kan eveneens een risico inhouden. Bij het bezoeken van een geïnfecteerde site wordt geprobeerd malware op de computer te installeren. Deze manier van besmetting staat bekend onder de naam 'drive-by-download'. Dit is mogelijk omdat (web)hosters gebruikmaken van kwetsbare software of omdat malware zich bijvoorbeeld in advertentiebanners bevindt.

Malware op legitieme websites: casus Telegraaf.nl
Via de website telegraaf.nl is op donderdag 6 september 2012 kortstondig kwaadaardige software verspreid, waardoor de pc's van bezoekers van deze website werden aangevallen. Het doel van deze aanvallen was om deze pc's te besmetten met kwaadaardige software. Bezoekers, met kwetsbare versies van Adobe- en Java-software geïnstalleerd op hun pc's, zijn besmet met banking malware en ransomware.[211]

8.4 De eindgebruiker in de beveiligingsketen

De toenemende complexiteit en de groter wordende afhankelijkheid van ICT vraagt zorgvuldig handelen van eindgebruikers. Dit houdt in het goed onderhouden van eigen apparatuur (het tijdig installeren van patches en updates, gebruik van anti-virussoftware/spamfilters), maar heeft ook betrekking op het gedrag van een gebruiker op het internet (wachtwoordgebruik, delen van informatie, bezoeken van websites, downloaden van bestanden).

Voor de eindgebruiker kan het moeilijk zijn om zijn ICT-middelen veilig te houden, omdat het vaak veel inhoudelijke kennis vergt om systemen veilig te configureren, problemen op te lossen en de juiste updates te installeren. Recent onderzoek van Secunia[212] toont aan dat de tijd tussen het bekend worden van een kwetsbaarheid en het uitbrengen van updates door leveranciers de afgelopen jaren sterk afneemt. Onderzoek van Microsoft toont echter aan dat ook wanneer updates beschikbaar zijn, een groot aantal gebruikers kwetsbare software blijft gebruiken. Wanneer een applicatie voor de gebruiker nog voldoet, kiest deze ervoor om niet te upgraden, terwijl leveranciers veelal alleen voor de laatste versie beveiligingsupdates maken.

Zowel de overheid als de private sector informeert eindgebruikers over de mogelijke gevaren op het internet door bewustwordingscampagnes. Voorbeelden van campagnes zijn AlertOnline (gericht op de burger en het MKB), beschermjebedrijf.nl (gericht op MKB van ICT-Nederland), veiligbankieren.nl (gericht op eindgebruikers van (internet)bankieren), DigiVaardig/DigiBewust (platform ECP-NL) en 'Laat je Niet Hacken, Thuis Veilig Online', een initiatief van de Consumentenbond.

Het eerdergenoemde rapport van de Universiteit Twente geeft een overzicht van de maatregelen die Nederlanders in 2012 namen om zichzelf op internet te beschermen. Onderstaande bevindingen tonen dat het bewustzijn bij de eindgebruiker toeneemt.

- Het aantal mensen dat een virusscanner gebruikt, is toegenomen van 82 procent naar 87 procent.
- Het laten installeren van automatische updates is gestegen van 53 procent naar 59 procent.
- Het werken met een spamfilter is opgelopen van 54 procent naar 58 procent.
- Het controleren met wie wel en niet persoonlijke gegevens worden gedeeld, stijgt van 33 procent naar 39 procent.
- Het percentage van internetgebruikers dat regelmatig wachtwoorden verandert, is gestegen van 31 naar 38 procent.

8.5 Wie helpt de eindgebruiker?

8.5.1 *Overheid*

Naast bewustwordingscampagnes heeft de overheid ook wet- en regelgeving die erop is gericht om de eindgebruiker te beschermen, waaronder:

- Zorg- en meldplicht zoals beschreven in de Telecommunicatiewet (Tw) (hoofdstuk 11a / artikelen 11a.1 en 11a.2). Bedrijven die diensten leveren voor telefonie en internet zijn vanaf 5 juni 2012 verplicht om incidenten bij de Autoriteit Consument & Markt (ACM, voorheen Opta) te melden. Het gaat om incidenten waarbij het risico heeft bestaan dat anderen bij de persoonsgegevens van klanten konden komen. In sommige gevallen moeten de Telecombedrijven ook de personen informeren van wie de gegevens gelekt zijn. Bedrijven uit andere sectoren en overheden zijn echter nog niet verplicht datalekken te melden. Er is wetgeving in de maak die een meldplicht datalekken invoert,[213]
- Conform de Wet Bescherming Persoonsgegevens (WBP) heeft een betrokkene (eindgebruiker) die meent dat er onzorgvuldig met zijn persoonlijke gegevens wordt omgegaan, het recht op inzage, correctie, verwijdering en verzet. Het College Bescherming Persoonsgegevens (CBP) heeft een website[214] waar concrete hulpmiddelen voor betrokkenen zijn gepubliceerd. Het CBP zelf heeft de wettelijke taak om toe te zien op de naleving van de WBP.

211 http://hitmanpro.wordpress.com/2012/09/08/banking-trojan-keeps-hitting-the-dutch-hard/, http://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Virussen+en+wormen/WD-2012-080+Nieuwssite+telegraaf.nl+serveert+link+naar+malware.html
212 http://secunia.com/vulnerability-review/time_to_patch.html
213 http://www.rijksoverheid.nl/documenten-en-publicaties/wetsvoorstellen/2012/11/01/wijziging-wet-bescherming-persoonsgegevens-meldplicht-datalekken
214 http://www.mijnprivacy.nl/Pages/Home.aspx

De ACM heeft in 2012 in totaal 143 meldingen ontvangen in het kader van de meldplicht.[38: OPTA 2013]

» Bij 60 procent van de meldingen heeft het incident helemaal geen gevolg gehad voor de privacy van de klanten. Het ging bijvoorbeeld om een gestolen laptop, waarbij de informatie over klanten zo opgeslagen was dat deze niet te lezen was.
» Bij 7 meldingen was sprake van een computervirus of van een hacker die toegang had gekregen tot computers van het bedrijf.
» Bij 39 meldingen heeft het bedrijf de klanten ingelicht. Als klanten worden ingelicht zijn zij in staat om eventuele gevolgschade te voorkomen of te beperken.

In 2012 is OPTA na meldingen actief geweest met het controleren dat malware via legitieme websites werd verspreid en heeft daarna geholpen bij de mitigatie

» Het spamverbod (artikel 11.7 Tw) beoogt de eindgebruiker te beschermen tegen ongewenste elektronische berichten (via bijvoorbeeld e-mail, fax, SMS of sociale media). Toezicht op het spamverbod is belegd bij de ACM, die hiervoor onder andere een speciaal klachtenportaal (www.spamklacht.nl) heeft ingericht voor consumenten en bedrijven. Op dit meldpunt heeft de ACM in 2012 24.536 klachten over spam ontvangen. Naast het uitvoeren van onderzoek, zoekt de ACM actief samenwerking met (inter)nationale publieke en private partijen. Juridische uitspraken in spamonderzoeken uit 2012 zijn terug te vinden in het ACM jaarverslag 2012. [38: OPTA 2013]
» Daarnaast is de ACM verantwoordelijk voor de bescherming van eindgebruikers tegen het zonder toestemming plaatsen of uitlezen van gegevens van hun randapparatuur. Zowel malware als cookies vallen onder deze wettelijke bepaling, neergelegd in artikel 11.7a Tw. De ACM reageert waar mogelijk op signalen van (grootschalige) verspreiding van malware binnen Nederland, zoals in 2012 meermaals is gebeurd bij advertentienetwerken van populaire Nederlandse websites. De ACM probeert dan zo snel mogelijk de bron te achterhalen en de verspreiding te helpen stoppen. De ACM monitort niet actief op de verspreiding van malware, maar is voor haar aanpak afhankelijk van signalen van publieke en private partners en zoekt continu naar mogelijkheden om haar informatiepositie te versterken.
» Naast het uitvoeren van onderzoek, zoekt de ACM actief samenwerking met (inter)nationale publieke en private partijen voor de bestrijding van spam en malware. Deze samenwerking heeft in 2012 tot ongeveer 100 signalen geleid die voor het grootste gedeelte adequaat zijn opgevolgd.

8.5.2 *Internetservice- en hostingproviders*

De internetservice- en hostingproviders in Nederland hebben, als best practice, abuse-desks ingericht waar informatie over besmettingen bij klanten gemeld wordt. Vervolgens maken providers zelf een afweging of en hoe eindgebruikers geïnformeerd worden. Om het botnetprobleem gezamenlijk aan te pakken, hebben meerdere providers in Nederland samen met SIDN en het Platform Internetveiligheid (PIV) van ECP-NL een Abuse Information Exchange-initiatief gelanceerd. Abuse Information Exchange[215] wordt in 2013 operationeel en zal op één centraal punt alle informatie over botnetbesmettingen verzamelen en bewerken. Op die manier zullen besmette computers sneller worden opgemerkt en kunnen klanten beter en sneller worden geïnformeerd.

Ook informeren ISP's actief, conform de zorgplicht in de Telecomwet, klanten (ook eindgebruikers) op de risico's van het gebruik van internet. Dit gebeurt door het uitsturen van nieuwsbrieven via een webpagina met informatie over veilig internetgebruik of via een twitteraccount/facebookpagina waardoor de servicedesk benaderbaar is voor vragen van eindgebruikers.

8.5.3 *(Software)leveranciers*

De rol van leveranciers is voornamelijk beperkt tot het beschikbaar stellen van updates van producten en software. Een voorname rol voor leveranciers is het ontwikkelen en uitbrengen van producten en software die de gebruiker beter beschermt (Security by design).

8.5.4 *Banken*

Banken geven op hun websites uitgebreide uitleg over de wijze waarop criminelen aanvallen plegen, welke maatregelen de banken zelf hebben genomen en hoe klanten hun apparatuur zo goed mogelijk kunnen beveiligen.[216] Banken informeren hun klanten als ze besmet zijn geraakt met banking malware en daardoor, via hun computer, geld afhandig is gemaakt door criminelen. Daarnaast heeft de Nederlandse Vereniging van Banken (NVB) een bewustwordingswebsite opgezet[217] en wordt er actief gewezen op de risico's van (spear)phishing in boodschappen op televisie en radio. Banken implementeren daarnaast mechanismen om de effecten van misbruik te beperken. Geo-blocking zorgt er bijvoorbeeld voor dat een geskimde pas niet buiten het voor de gebruiker normale geografische gebied kan worden gebruikt. «

215 http://www.rijksoverheid.nl/nieuws/2012/10/24/internetproviders-strijden-tegen-computervirussen.html
216 www.ing.nl/de-ing/veilig-bankieren/index.aspx, www.abnamro.nl/nl/prive/abnamro/veiligheid/index.html, www.rabobank.nl/particulieren/servicemenu/veilig_bankieren/, www.snsbank.nl/particulier/over-sns-bank/veilig-bankieren.html
217 http://www.veiligbankieren.nl/nl/

9 Industriële controlesystemen (ICS)

Security van ICS is nog steeds een groot probleem. Want industriële systemen zijn kwetsbaar en er gebeurt nog te weinig om dat goed op te lossen. Gelukkig ontbreekt het bij de bekende actoren nog aan zowel motieven als capaciteiten, maar blijft dat zo? Daarom een hernieuwde waarschuwing, want anders gaat het straks een keer écht mis.

9.1 Inleiding

In de rapportageperiode van het tweede Cybersecuritybeeld haalde een aantal kwetsbaarheden in industriële controlesystemen (ICS, waaronder SCADA) de media. Niet alleen was er een toename in het aantal kwetsbaarheden, ook werd de dreiging van een gerichte verstoring van deze systemen reëler. Deze rapportageperiode is een aantal nieuwe kwetsbaarheden in ICS bekend geworden. Hoewel grote incidenten zijn uitgebleven, is de dreiging onverminderd groot.

De huidige beveiligingsstatus van ICS verslechtert steeds meer, maar dit gaat geleidelijk waardoor besef over het ernstiger worden van de situatie uitblijft en veel organisaties onvoldoende actie ondernemen. Hierbij moet worden opgemerkt dat met name grote operators van vitale infrastructuren en enkele (grote) leveranciers van ICS-toepassingen wel degelijk de ernst van de situatie beseffen en overeenkomstig handelen.

9.2 De potentiële impact van cyberincidenten met ICS

ICS worden in vitale en (andere) industriële sectoren gebruikt voor de aansturing van fysieke processen. Dit betekent dat wanneer deze systemen niet naar behoren functioneren, er in de fysieke wereld ook iets mis kan gaan. Het is deze fysieke impact van digitale incidenten die het belangrijk maakt dat de beveiliging van ICS op orde is.

Omdat ICS op verschillende manieren en binnen verschillende sectoren toegepast worden, verschilt de soort en de grootte van de impact per incident. Het is mogelijk dat een incident ernstige schade toebrengt aan de economie, het milieu en/of de levens van mensen en dieren. Om de ernst van incidenten met ICS beter te kunnen duiden, wordt onderscheid gemaakt in de drie navolgende niveaus waarop deze systemen toegepast worden.

Wat zijn ICS?

Bij termen als computers, automatisering en het internet denkt men vaak aan de traditionele ICT-omgeving: desktop computers en laptops voor het gebruik thuis en op kantoor. Ook bij informatiebeveiliging en cybersecurity denkt men al snel in deze richting. Binnen de vitale en (andere) industriële sectoren wordt voor automatisering echter gebruikgemaakt van een ander soort systemen: procescontrolesystemen of industriële controlesystemen (ICS). Deze systemen hebben niet alleen een andere functie en werking dan traditionele ICT-systemen, maar er zijn ook andere risico's aan verbonden.

ICS worden binnen vitale en (andere) industriële sectoren gebruikt voor de automatische monitoring en besturing van fysieke processen. Voor de productie, het transport en de distributie binnen de energie- en drinkwatervoorziening wordt gebruikgemaakt van ICS. Ook de productieprocessen van raffinaderijen, de chemische, farmaceutische en voedingsmiddelenindustrie worden (grotendeels) aangestuurd door ICS. Daarnaast worden ICS steeds vaker toegepast binnen de verkeersinfrastructuur (verkeersregeling, bruggen, sluizen, tunnels) in gebouwbeheerssystemen (klimaatcontrole, brandmelding, verlichting) en voor toegangscontrole (slagbomen, elektronische hekwerken).

In het verleden communiceerden ICS rechtstreeks met elkaar in een gesloten netwerk, de systemen waren niet gekoppeld aan het internet of andere netwerken. Tegenwoordig zijn ICS echter vaak gekoppeld aan de kantoorautomatisering van het bedrijf en ook toegankelijk via het internet. Dit brengt bepaalde veiligheidsrisico's met zich mee, waar niet altijd rekening mee wordt gehouden.

In de media worden SCADA (Supervisory Control And Data Acquisition) systemen dikwijls gelijkgesteld aan ICS. In het nieuws wordt dan bijvoorbeeld gesproken over 'beveiligingsproblemen met SCADA-software' of over 'SCADA-lekken'. ICS is echter een algemene term die verschillende soorten controlesystemen omvat, waaronder SCADA. In dit Cybersecuritybeeld wordt gesproken over de overkoepelende term ICS.

SCADA-systemen (computers met daarop SCADA-software) worden gebruikt voor het bedienen en visualiseren van (industriële) processen. Het monitoren kan dan vanuit één plaats (bijvoorbeeld de controlekamer) plaatsvinden. Met behulp van de verzamelde en opgeslagen procesgegevens kunnen rapportages worden opgemaakt, welke op hun beurt weer geanalyseerd en gebruikt kunnen worden voor het optimaliseren van het proces.

Andere belangrijke subgroepen van ICS zijn DCS (Distributed Control Systems) en PLC's (Programmable Logic Controllers).

SOHO en individuele toepassingen

(bijvoorbeeld klimaatregelsystemen, toegangscontrole)

Digitale incidenten op dit niveau zijn vervelend voor de betrokkenen, maar de schade blijft beperkt en is voornamelijk van praktische en financiële aard. Denk hierbij aan een situatie waarin het verwarmingssysteem van een bedrijf ontregeld raakt of de slagbomen tot het parkeerterrein niet meer opengaan. Het is vervelend dat het personeel en de bezoekers elders moeten parkeren of dat medewerkers het koud of warm krijgen, maar veel erger dan dat wordt het over het algemeen niet.

Lokaal/Regionaal

(bijvoorbeeld verkeersregelinstallaties, bediening rioleringspompen en bruggen, losse windmolens)

Digitale incidenten op dit niveau kunnen een grote impact hebben, maar de schade blijft beperkt tot lokaal of regionaal niveau en is ook voornamelijk van praktische en financiële aard. Denk aan een brug die open blijft staan waardoor het verkeer vastloopt of aan een bedrijf dat grote financiële schade lijdt doordat de systemen in een van zijn fabrieken uitvallen en de productie daarmee enkele dagen stil komt te liggen.

Nationaal

(vitale infrastructuur, bijvoorbeeld de energie- en drinkwatervoorziening)

Digitale incidenten binnen de vitale sectoren kunnen leiden tot maatschappelijke ontwrichting en daarmee tot aantasting van de nationale veiligheid. Er kan sprake zijn van veel slachtoffers en/of grote economische schade en het herstel kan lang duren, terwijl deze producten en diensten onmisbaar zijn. ICT, telecommunicatie (vast en mobiel) en elektriciteit zijn randvoorwaardelijk voor het functioneren van de vitale sectoren van de samenleving. Uitval hiervan kan leiden tot schadelijke effecten in andere sectoren en de impact van een incident nog meer vergroten. Voor het Cybersecuritybeeld Nederland zijn deze incidenten het meest relevant omdat zij een directe impact kunnen hebben op grote groepen burgers, bedrijven en overheden.

9.3 Incidenten met ICS

Het is niet mogelijk om goede statistieken over ICS-gerelateerde incidenten in Nederland te geven. Getroffen organisaties zijn vooralsnog terughoudend met het delen van informatie over dit onderwerp. In de periode juni 2011-november 2012 ontving NCSC.nl slechts elf meldingen. Vanwege dit lage aantal wordt gekeken naar het Amerikaanse ICS-CERT, als een van de weinige beschikbare publieke bronnen. Daarnaast wordt naar een ruime rapportageperiode gekeken om de geleidelijke ontwikkelingen in beeld te brengen. De ICS-CERT jaaroverzichten met meldingen van incidenten zijn samengevat in tabel 11.[218]

Jaar	# Meldingen	# Onderzoeken
2010	39	57
2011	204	70
2012	138	89

Tabel 11. Ontwikkelingen in aantal meldingen in de VS

Het aantal onderzoeken blijft toenemen, wat een indicatie is voor een toenemend aantal incidenten. Op basis van de beperkte detailinformatie over ICS-gerelateerde incidenten zijn deze gerangschikt in de onderstaande drie categorieën.

Incidenten door internetconnectiviteit

Vanaf 2011 besteden verschillende onderzoekers aandacht aan systemen die met behulp van Shodan[219] en andere zoekmachines via het internet te bereiken zijn[220]. Voornamelijk kleinere bedrijven, lagere overheden en particulieren beseffen onvoldoende dat hun systemen (meestal SOHO en individuele toepassingen) direct via internet bereikbaar zijn. De combinatie van kwetsbaarheden in de software, het gebruik van zwakke wachtwoorden, etc. zorgt er in veel gevallen voor dat onrechtmatig toegang tot deze systemen is te verkrijgen. Deze kwetsbaarheden komen vaak voort uit onvoldoende afspraken over beveiliging met derden, die voor de aanleg en/of het beheer zorgen.

Vooral begin 2012 nam de aandacht voor de risico's van de koppeling van ICS met het internet toe, wat resulteerde in veel publieke incidentmeldingen. Alle meldingen betroffen systemen die via het internet vindbaar waren met de zoekmachine Shodan.[221] Hoewel deze categorie kwetsbaarheden veruit de meeste aandacht en publiciteit krijgt, liggen hier op dit moment niet de grootste risico's voor de nationale veiligheid omdat de overgrote meerderheid valt in de categorie SOHO.

Incidenten door kwetsbaarheden in generieke ICT-middelen (categorie 'collateral damage')

Binnen ICS-omgevingen wordt steeds vaker gebruikgemaakt van generieke ICT-middelen, zogenaamde COTS-producten. Dit geldt niet alleen voor hardware, maar vooral ook voor software zoals besturingssystemen, webtechnologieën en databases. Gebruik van deze COTS-producten heeft weliswaar veel voordelen (zoals lagere kosten), maar heeft ook tot gevolg dat kwetsbaarheden in deze producten een springplank kunnen vormen voor uiteindelijke manipulatie van de procesbesturingen. Daarnaast worden ICS-

218 Of het hier om daadwerkelijke ICS-incidenten gaat, is niet gerapporteerd. Na onderzoek kan blijken dat er geen sprake was van een security-incident (maar van een storing) of dat het geen ICS/SCADA betrof. Ook kunnen er meerdere meldingen van hetzelfde incident zijn gedaan.

219 SHODAN is een internet-zoekmachine waarmee gericht gezocht kan worden naar computers die op het internet zijn aangesloten.

220 Voorbeelden hiervan zijn: Eirann Leverett: http://www.blackhat.com/usa/speakers/Eireann-Leverett.html, Project SHINE: http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf en HDMoore: https://community.rapid7.com/community/metasploit/blog/2013/04/23/serial-offenders-widespread-flaws-in-serial-port-servers

221 De (weinige) aan Nederland gemelde gevallen uit deze onderzoeken bleken niet gerelateerd aan vitale infrastructuren.

omgevingen daarmee ook vatbaarder voor malware die eigenlijk (alleen) bedoeld is voor standaard ICT-voorzieningen. Zo hebben uitbraken van de computerwormen Slammer en Conficker in netwerken van fabrieken geleid tot het moeten stilleggen van de productie. Ook keyloggers, banking trojans en andere generieke malware die onbedoeld ICS-omgevingen infecteren, kunnen leiden tot storingen.

Incidenten door de 'menselijke factor'

Circa de helft van de door ICS-CERT benoemde onderzoeken betreft gevallen van spearphishing, met mogelijk de intentie om de ICS-omgeving binnen te komen of ICS-gerelateerde informatie te zoeken en/of deze te manipuleren. Bij geen van de onderzochte incidenten is dit aangetoond. In het najaar van 2012 vond in de Verenigde Staten een gerichte spearphishingaanval plaats, gericht op de energiesector. Medewerkers waren gericht benaderd nadat via OSINT informatie was verkregen. In deze specifieke case bleek niet dat het daadwerkelijk was gelukt om binnen te dringen.[222] Hoewel in Nederland nog geen gerichte aanvallen met behulp van spearphishing op ICS-omgevingen bekend zijn, moeten organisaties daar wel rekening mee houden.

9.4 Ontwikkelingen in kwetsbaarheden in ICS

Voor kwetsbaarheden wordt uitgegaan van de 'National Vulnerability Database' (NVD[223]) van het National Institute of Standards and Technology (NIST). Deze database richt zich op ontdekte 'software flaws', dus op fouten in de software. Zaken als misconfiguraties en onjuiste toepassingen van producten vallen hier niet onder. De NVD bevat op dit moment 84 ICS-gerelateerde kwetsbaarheden, ondanks dat de NVD niet volledig is.[224] Tientallen bekende kwetsbaarheden zijn (nog) niet opgenomen in de NVD. Daarnaast bezit ICS-CERT grote aantallen meldingen van potentiële kwetsbaarheden die nog onderzocht moeten worden.

Tabel 12 maakt duidelijk dat met de toenemende belangstelling voor ICS-security het aantal ontdekte/gemelde kwetsbaarheden ook toeneemt, al dan niet versterkt door de ontdekking van 'Stuxnet' in 2010 en het oprichten van ICS-CERT eind 2009. Afgezet tegen het totaal aantal systeemkwetsbaarheden in de NVD-database (ruim 55.000, over een periode van 15 jaar) is het aantal ICS-gerelateerde kwetsbaarheden echter marginaal (circa 2 procent).

Jaar	Totaal # ICS-gerelateerde kwetsbaarheden in NVD	# ICS-CERT information products[225]
2006	1	-
2007	1	-
2008	4	-
2009	14	0 (ICS-CERT is sinds november 2009 publiek van start gegaan.)
2010	19	138
2011	46	283
2012	79	343
2013	84 (tot Q1)	41 (tot Q1)

Tabel 12. Ontwikkeling in aantallen ICS-gerelateerde kwetsbaarheden.

Na een zeer sterke toename in de periode 2010-2012 lijkt in Q1-2013 een afvlakking in bekendgemaakte kwetsbaarheden plaats te vinden. Het is echter nog te vroeg om hier conclusies aan te verbinden. Bijvoorbeeld omdat in het verleden een aantal hacker-conferenties steeds in de tweede helft van het jaar veel nieuwe problemen aan de kaak stelden. Daarnaast worden kwetsbaarheden ontdekt door het gebruik van tooling die ook voor generieke ICT wordt toegepast, bijvoorbeeld fuzzing-tools. Gebruik van deze tools door ontwikkelaars kan leiden tot software met minder kwetsbaarheden. Een andere verklaring is wellicht het aangepaste blikveld van diverse onderzoekers; het aantonen van een zoveelste 'buffer-overflow in just another HMI' levert niet zoveel toegevoegde waarde op. Tot slot geldt dat sommige leveranciers niet publiek communiceren over kwetsbaarheden in hun producten en nieuwe versies uitbrengen zonder te vermelden welke kwetsbaarheden daarbij verholpen zijn.

Een deel van het risico dat men loopt, gerelateerd aan een kwetsbaarheid, hangt samen met het gemak of de kennis die nodig is om die kwetsbaarheid te kunnen misbruiken. De afgelopen periode is het aantal publiek beschikbare exploits opnieuw gestegen. Zo bevat het exploit pack GLEG agora SCADA+ inmiddels 143 ICS/SCADA gerelateerde exploits. Slechts voor 67 van de bijbehorende kwetsbaarheden is een CVE-nummer bekend. Opvallend is ook dat er van de meest recente 35 exploits nauwelijks CVE's en alerts zijn verschenen. Het is voor betrokkenen daarmee lastig goed op de hoogte te blijven van de laatste kwetsbaarheden.

9.5 Actoren

In de Nederlandse context is een beperkt aantal actoren betrokken bij dreigingen binnen het ICS-domein:

- Meerdere staten zijn bezig met het opzetten van offensieve cybercapaciteiten. Het is aannemelijk dat daarbij ook kennis wordt opgebouwd van ICS om vitale processen te kunnen verstoren.
- De resultaten van cyberonderzoekers in het ICS-domein leiden tot nieuwe kwetsbaarheden en tooling. Zo worden regelmatig

222 http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monitor_Jan-Mar2013.pdf
223 http://vd.nist.gov
224 Stand per 25 maart 2013. Gezocht is op trefwoord SCADA. Getallen kunnen afwijken van andere gepubliceerde overzichten omdat sommige ICS-gerelateerde kwetsbaarheden niet via het trefwoord SCADA te vinden zijn.
225 Deze cijfers komen uit ICS-CERT year in review 2012. Indien er een update op een publicatie uitgebracht is, is deze apart geteld.

exploitcode toegevoegd aan testtools en exploitpacks. Ook verschijnt informatie over de vindbaarheid van op het internet aangesloten systemen, die door anderen kan worden misbruikt, bijvoorbeeld door scriptkiddies.

» Vorig jaar signaleerde ICS-CERT dat verschillende groeperingen (onder meer hacktivisten en anarchisten) in toenemende mate belangstelling tonen voor ICS die via het internet te benaderen zijn.[226] Behoudens een beperkt aantal berichten over kennisvergaring door hacktivisten/terroristen, zijn er op dit moment nog geen aanvallen bekend die op ICS gericht waren.

Duidelijk is dat een aantal actoren steeds meer kennis over beveiligingsproblemen van ICS opdoet. Tot op heden zien we vooral activiteiten van actoren met goedbedoelde intenties (hoewel de 'slachtoffers' dit niet altijd zo ervaren), soms ingegeven door het (direct) toepassen van 'full disclosure' bij een ontdekking. Kijkend naar de ontwikkelingen rond generieke ICT-beveiliging, wordt verwacht dat actoren de beschikbare kennis/tooling ook tegen ICS zullen inzetten. Overigens vormen meerdere categorieën actoren nu al indirect een bedreiging, omdat malware bedoeld voor andere (ICT-)toepassingen collateral damage kan veroorzaken in ICS-omgevingen.

9.6 De weerbaarheid van ICS

Security van ICS heeft de afgelopen jaren niet dezelfde aandacht gekregen als security in reguliere ICT en staat daarmee nog in de kinderschoenen. De ICS-wereld kent een eigen cultuur met een vaak behoudende technische organisatie, waarbij aandacht voor security niet vanzelfsprekend is.[227] Dit behelst ook de menselijke en organisatorische factoren, zoals onvoldoende awareness, het ontbreken van ownership en het onvoldoende aansturen van ingehuurde partijen met betrekking tot beveiligingseisen.

Het weerbaarheidsprobleem ligt echter niet alleen bij bestaande systemen. Ook bij het realiseren van nieuwe ICS moet rekening rekening worden gehouden met veiligheidsrisico's, als integraal onderdeel van het 'lifecycle-management'. Bij het ontwerpen, implementeren en beheren van ICS-systemen wordt niet direct rekening gehouden met securityrisico's, omdat 'security by design' ontbreekt. Controle op de identiteit van de gebruiker (authenticatie) en waar deze gebruiker toegang toe heeft (autorisatie), vindt bijvoorbeeld niet altijd plaats omdat dit geen standaard functies zijn in ICS. Manipulatie van besturingen kan hierdoor op eenvoudige wijze plaatsvinden.

Vanwege de lange levensduur van ICS (circa 10-30 jaar) zijn er vaak verouderde systeemcomponenten en besturingssystemen in gebruik. Het probleem daarmee is dat de ondersteuning van de fabrikant op een gegeven moment vervalt. Daar waar specifieke ICS-onderdelen langdurig ondersteund worden, is dat voor generieke ICT-middelen veelal niet het geval. Neem bijvoorbeeld het in ICS nog vaak gebruikte Windows XP. Microsoft zal op 8 april 2014 de ondersteuning voor dit besturingssysteem beëindigen, waardoor nieuwe beveiligingslekken niet meer worden gedicht.

Leveranciers van ICS/SCADA geven soms geen garantie meer op de juiste werking van het systeem indien er overgestapt wordt naar een nieuw besturingssysteem, asset owners zijn terughoudend bij het uitrollen van patches onder het motto 'zolang het werkt niet wijzigen'. Maar ook is het stilleggen van processen om de besturingscomputers te kunnen patchen niet altijd mogelijk en/of zeer kostbaar. Ten slotte zien leveranciers niet altijd de noodzaak voor het uitbrengen van patches op oudere componenten, waardoor kwetsbaarheden niet verholpen worden.

Niet altijd schade

Cyberincidenten kunnen plaatsvinden op verschillende plaatsen binnen ICS. Dit is ook van invloed op de soort en grootte van de impact. Het manipuleren van een enkel onderdeel zal andere gevolgen hebben dan het manipuleren van de verschillende functies van een systeem. Daarnaast zijn vaak 'flankerende maatregelen' getroffen die manipulatie (vroegtijdig) kunnen ontdekken dan wel de gevolgen ervan beperken. Als uitsluitend de aansturing van een machine wordt gemanipuleerd, hoeft er niet per definitie schade te ontstaan. Indien de alarmfunctie goed werkt, wordt de operator tijdig geïnformeerd waardoor hij/zij kan ingrijpen. Naast de aansturing kan er echter ook met de alarm- en visualisatiefuncties worden geknoeid. Stel dat bij een chemische fabriek tanks met een inhoud van 100 liter worden gevuld met chemische stoffen. Het vullen stopt normaal gesproken automatisch zodra ze voor driekwart gevuld zijn. Nu wordt het systeem zodanig gemanipuleerd dat het vullen niet zal stoppen, dat er geen alarm zal afgaan en dat dit ook niet zichtbaar zal zijn op het visualisatiescherm. Het vullen van de tank loopt door terwijl er op de monitor in de controlekamer niets afwijkends te zien is. De tank loopt over en de ruimte raakt gevuld met chemische dampen. Wanneer personeel vervolgens nietsvermoedend de ruimte binnenloopt, kan dit ernstige gevolgen hebben voor hun gezondheid.

226 ICS-CERT Alert 15 February 2012, http://ics-cert.us.gov/pdf/ICS-ALERT-12-046-01.pdf

227 Het NCSC heeft de factsheet 'Checklist beveiliging van ICS/SCADA systemen' gepubliceerd met 15 punten om ICS te beveiligen en incidenten te voorkomen: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/checklist-beveiliging-van-ics-scada-systemen.html

9.7 Tot slot

In het CSBN-2 werd vastgesteld dat de dreigingen voor ICS reëler waren geworden ten opzichte van de periode ervoor. Hoewel over de afgelopen rapportageperiode geen spraakmakende incidenten naar buiten zijn gebracht, kunnen we niet stellen dat de beveiligingsstatus van ICS is verbeterd. Alhoewel er zeker organisaties en leveranciers zijn die goede stappen zetten, blijft het overall beeld somber, met name bij eindgebruikers en leveranciers van de kleinere toepassingen. De situatie is hetzelfde gebleven of misschien wel verergerd, het is alleen niet direct zichtbaar. Kwetsbaarheden blijven toenemen, de belangstelling van actoren neemt toe, terwijl het bewustzijn niet lijkt mee te groeien. Het is noodzakelijk dat maatregelen worden getroffen omdat digitale incidenten in vitale sectoren een grote impact kunnen hebben.

Bijlage » 1 Referenties

[1: Blue Coat 2013]	Blue Coat: 2013 Mobile Malware Report
[2: CBP 2013]	CBP: Het CBP in 2012, http://www.cbpweb.nl/pages/jv_2012.aspx
[3: CBS 2012]	CBS: ICT, kennis en economie
[4: CERT-AU 2012]	CERT Australia: Cyber Crime & Security Survey Report 2012
[5: Cisco 2013]	Cisco: 2013 Annual Security Report
[6: Cisco 2011]	Cisco Internet Business Solutions Group: The Internet of Things http://share.cisco.com/internet-of-things.html
[7: CS 2013]	comScore: 2013 Europe Digital Future in Focus, http://www.marketingfacts.nl/images/uploads/2013_europe_digital_future_in_focus.pdf
[8: Tokmetzis 2012]	Dimitri Tokmetzis: De digitale schaduw http://www.unieboekspectrum.nl/boek/9789000306350/De-digitale-schaduw/
[9: Enisa 2012]	Enisa: Smart Grid Security
[10: E&Y 2012]	Ernst & Young: Voortschrijdende techniek: Valkuil of goudmijn? http://www.ey.com/Publication/vwLUAssets/Voortschrijdende_techniek_-_Valkuil_of_goudmijn/$FILE/Voortschrijdende%20techniek%20-%20Valkuil%20of%20goudmijn.pdf
[11: EC 2013-1]	Europese Commissie: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
[12: EC 2013-2]	Europese Commissie: SPECIAL EUROBAROMETER 390
[13: FS 2013]	F-Secure: Threat Report 2012 H2 http://www.f-secure.com/static/doc/labs_global/Research/Threat_Report_H2_2012.pdf
[14: Google 2012]	Google: Transparency Report, http://www.google.com/transparencyreport/
[15: IBM 2012]	IBM: X-Force 2012 Mid-year Trend and Risk Report
[16: IDC 2013]	IDC: IDC Predictions 2013: Big Data Battle for Dominance in the Intelligent Economy http://event.lvl3.on24.com/event/54/34/13/rt/1/documents/slidepdf/wc20130108.pdf
[17: IDC 2012]	IDC: The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East http://www.emc.com/collateral/analyst-reports/idc-the-digital-universe-in-2020.pdf
[18: IGZ 2011]	Inspectie voor de Gezondheidszorg: Staat van de Gezondheidszorg
[19: IMGFK 2012]	IntoMart GFK: Trends in de media http://www.intomartgfk.nl/imperia/md/content/intomart/12-12-13_pb_trends_in_de_media_v2.pdf
[20: Koscher 2010]	Karl Koscher et al: Experimental Security Analysis of a Modern Automobile
[21: McAfee 2013-1]	McAfee: Threats Report Q4 2012 http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q4-2012.pdf

[22: McAfee 2013-2]	McAfee: Threats Predictions 2013 http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf
[23: MS 2012-2]	Microsoft: Law Enforcement Requests Report http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
[24: MS 2012-1]	Microsoft: Security Intelligence Report http://www.microsoft.com/sir/
[25: MS 2009]	Microsoft Research: So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users
[26: MinDef 2012]	Ministerie van Defensie: Cyber Strategie
[27: Motivaction 2012]	Motivaction: Cyber Security Awareness. Een onderzoek naar kennis, bewustzijn en gedrag ten aanzien van cybersecurity
[28: NP 2012-1]	Nationale Politie: High Tech Crime. Criminaliteitsbeeldanalyse 2012
[29: NP 2012-2]	Nationale Politie: Nationaal Dreigingsbeeld 2012 Georganiseerde criminaliteit
[30: NCSC 2012-1]	NCSC: Consumerization en security https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/consumerization--security.html
[31: NCSC 2011]	NCSC: Whitepaper cloudcomputing https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
[32: NCSC 2013-1]	NCSC: Leidraad responsible disclosure https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html
[33: NCSC 2013-3]	NCSC: Factsheet Continuïteit van onlinediensten https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-continuiteit-van-online-diensten.html
[34: NCSC 2012-2]	NCSC: Factsheet Beveilig apparaten gekoppeld aan het internet https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-beveilig-apparaten-gekoppeld-aan-internet.html
[35: NCSC 2013-2]	NCSC: Factsheet De aanhouder wint – advanced persistent threats https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-de-aanhouder-wint-advanced-persistent-threats.html
[36: Newcom 2013]	Newcom Research & Consultancy: Social Media in Nederland 2013 http://www.newcomresearch.nl/socialmedia
[37: NVB 2013]	NVB: Jaarverslag 2012
[38: OPTA 2013]	Opta: Jaarverslag 2012, http://optajaarverslag2012.acm.nl/download/OPTA%20Jaarverslag%202012.pdf
[39: Ordina 2011]	Ordina: Security gevaren bij Online Sociale Netwerken http://www.ordina.nl/downloadcentrum/~/media/Files/Expertises/Consulting/Whitepaper%20Security%20bij%20Online%20Sociale%20Netwerken.ashx?forcedownload=1
[40: Olson 2012]	Parmy Olson: Wij zijn Anonymous. Een inside verslag van de beruchte hackersbeweging

[41: Olsthoorn 2010]	Peter Olsthoorn: De macht van Google - Werkt Google voor jou of werk jij voor Google http://www.demachtvangoogle.nl/
[42: PNAS 2013]	Proceedings of the National Academy of Sciences: Private traits and attributes are predictable from digital records of human behavior http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html
[43: Quocirca 2013]	Quocirca: Next Generation Data Centre Index – Cycle III http://www.quocirca.com/media/reports/032013/811/Oracle%20NGD%20report%20final%20March%202013.pdf
[44: Rid 2012]	Rid, T.: Cyber War Will Not Take Place, in: P. Ducheine, F. Osinga, J. Soeters (red): Cyber Warfare – Critical Perspectives
[45: Rijksoverheid 2012]	Rijksoverheid: Regeerakkoord 'Bruggen slaan' http://www.rijksoverheid.nl/regering/documenten-en-publicaties/rapporten/2012/10/29/regeerakkoord.html
[46: Sophos 2012]	Sophos: Security Threat Report 2012
[47: Stol 2013]	Stol, W.: Slachtofferschap in een gedigitaliseerde samenleving
[48: Symantec 2013]	Symantec: Internet Security Threat Report 2013
[49: TNO 2012]	TNO: Monitor ICT vertrouwen en veiligheid
[50: TM 2013]	Trend Micro: 2012 Mobile Threat and Security Roundup
[51: TM 2012]	Trend Micro: Russian Underground 101 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf
[52: UT 2012]	Universiteit Twente: Trendrapport Internetgebruik http://www.utwente.nl/ctit/cfes/docs/Rapporten/2012_Trendrapport_Internetgebruik.pdf
[53: UvA 2012]	Universiteit van Amsterdam: Clouddiensten in hoger onderwijs en onderzoek en de USA Patriot Act
[54: Verizon 2012]	Verizon: Data Breach Investigations Report 2012
[55: VU 2012]	VU Amsterdam: Memory Errors: The Past, the Present, and the Future, 12 september 2012 http://www.few.vu.nl/~herbertb/papers/memerrors_raid12.pdf
[56: Wellmann 2001]	Wellmann, B.: Physical place and Cyberplace: The Rise of Personalized Networking
[57: WODC 2012]	B-J. Koops e.a., Misdaad en opsporing in de wolken. Knelpunten en kansen van cloud computing voor de Nederlandse opsporing , http://www.wodc.nl/onderzoeksdatabase/cloud-computing.aspx
[58: WEF 2012]	World Economic Forum: Risk and Responsibility in a Hyperconnected World: Principles and Guidelines
[59: WRR 2011]	WRR: WRR-rapport 86: iOverheid, http://www.wrr.nl/publicaties/publicatie/article/ioverheid/

Bijlage » 2 Incidenten

Incidenten geregistreerd bij het NCSC

Het NCSC ondersteunt overheden en organisaties in vitale sectoren bij het afhandelen van incidenten op gebied van ICT-veiligheid. In die rol worden bij het NCSC incidenten gemeld en worden incidenten en kwetsbaarheden ook door het NCSC zelf geïdentificeerd, bijvoorbeeld op basis van detectie.

Daarnaast acteert NCSC op verzoek van internationale partijen met name richting internetserviceproviders om te ondersteunen bij het bestrijden van cyberincidenten in het buitenland die hun oorsprong vinden in Nederland (bijvoorbeeld vanaf een webserver of vanaf geïnfecteerde pc's in Nederland). Dit schaart NCSC onder de noemer 'internationale hulpverzoeken'.

Aantallen afgehandelde incidenten per doelgroep

Het aantal door NCSC afgehandelde incidenten laat de afgelopen kwartalen geen duidelijk stijgend of dalend beeld zien. Na een flinke afname in het tweede kwartaal van 2012 (➘ 27 incidenten ten opzichte van het eerste kwartaal) steeg het aantal incidenten in de resterende kwartalen van 2012 om vervolgens in het eerste kwartaal van 2013 weer te dalen (figuur 14).

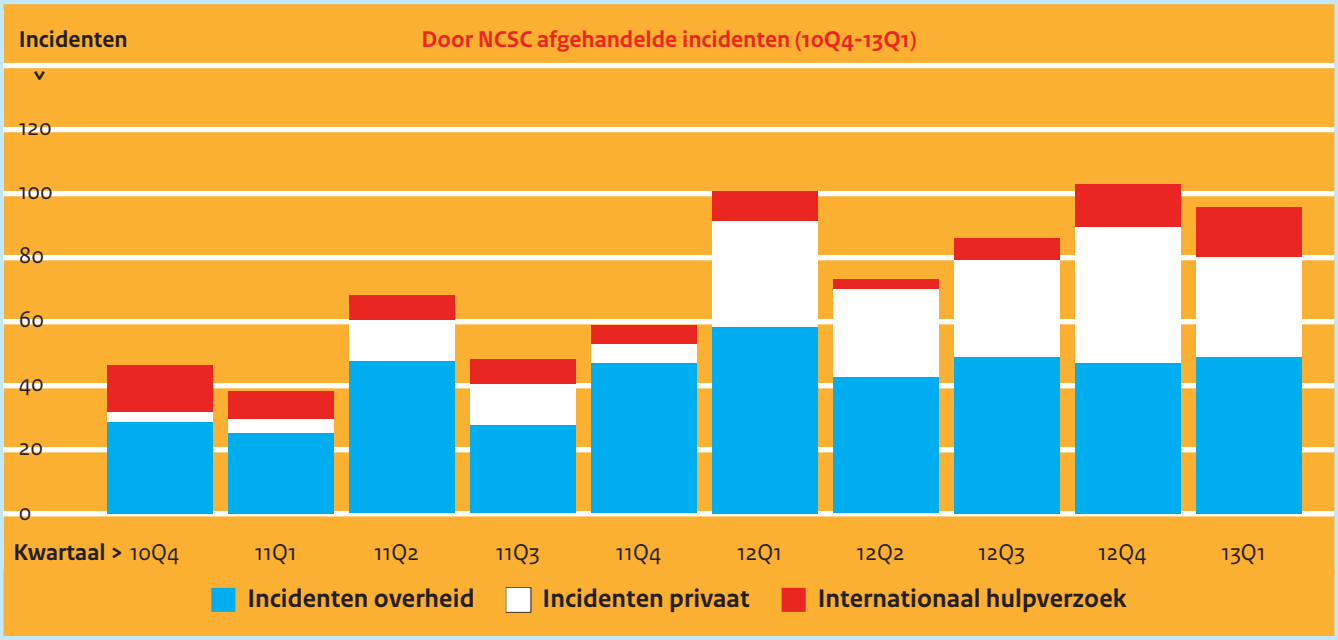
Het aandeel incidenten gemeld vanuit of betrekking hebbend op de overheid is gedurende de rapportageperiode van dit CSBN redelijk stabiel: tussen de 42 en 48 incidenten per kwartaal. De fluctuatie in incidenten wordt dus vooral veroorzaakt door incidenten die betrekking hebben op de private sector (28 tot 42 per kwartaal) en het aantal internationale hulpverzoeken (3 tot 14 per kwartaal).

Onder incident verstaat NCSC 'een ICT-gerelateerd beveiligingsvoorval dat is gemeld of ontdekt waarbij zich een acuut gevaar voor of schade aan ICT-systemen of electronische informatie voordeed, betrekking hebbend op een of meer specifieke organisaties, waarop NCSC reactief heeft opgetreden richting deze organisaties.' Deze afbakening geeft aan dat een incident niet altijd al tot schade heeft geleid, maar ook een gevaar kan zijn zonder dat al schade is veroorzaakt. Meer specifiek vallen incidenten in drie soorten uiteen:

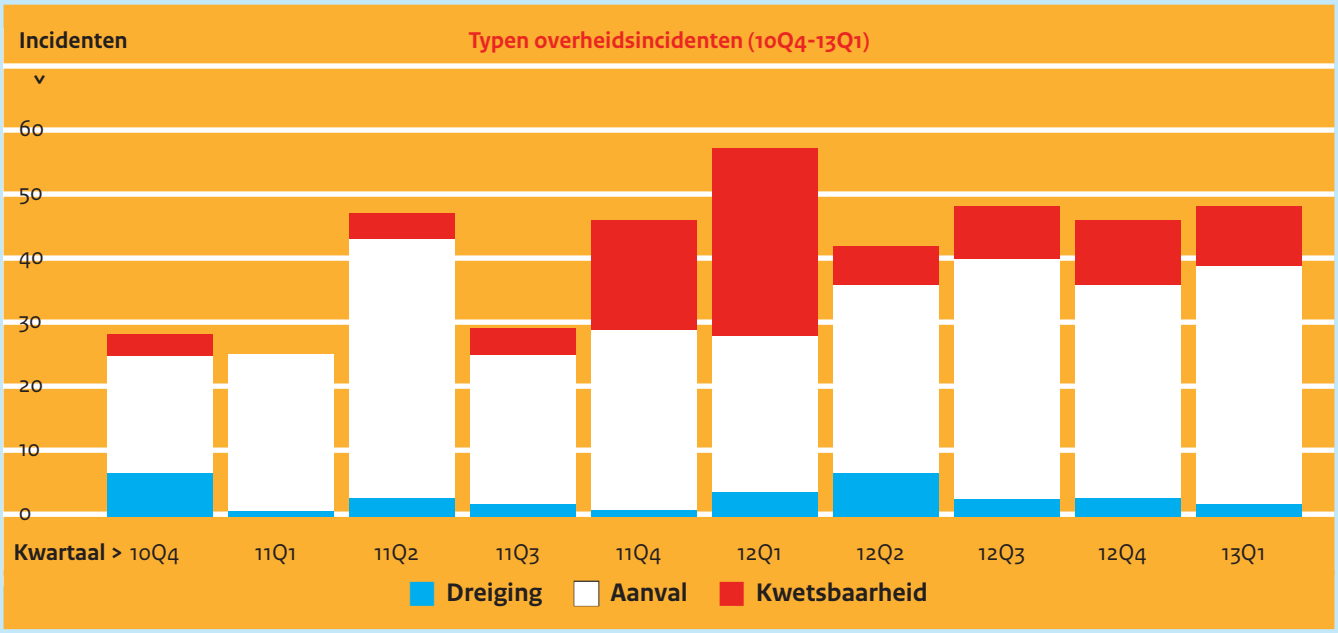
- Aanval: er heeft daadwerkelijk een (poging tot een) aanval plaatsgevonden met zo mogelijk een inbreuk op de beveiliging tot gevolg. Hierbij gaat het om bijvoorbeeld hacks, malware-infecties, DDoS-aanvallen.
- Dreiging: er bestaat een kwaadaardige intentie bij een actor om een aanval uit te voeren, maar deze is nog niet uitgevoerd.
- Kwetsbaarheid: een ICT-omgeving is kwetsbaar, als gevolg van bijvoorbeeld een fout in software, hardware of systeemconfiguratie. Bij een kwetsbaarheid is (nog) geen sprake van een dreiging of aanval, maar biedt wel gelegenheid tot misbruik.

Aard van de incidenten bij de overheid

Bij incidenten maakt het NCSC onderscheid tussen dreigingen, aanvallen en kwetsbaarheden. Kijkend naar de incidenten bij de



Figuur 14. Door NCSC afgehandelde incidenten (totaal)



Figuur 15. Door NCSC afgehandelde incidenten (overheid)

overheid (figuur 15), zien we dat aanvallen ongeveer 75 procent van de incidenten uitmaken. Van de overgebleven dreigingen zien we het aandeel dreigingen afnemen (van 17 naar 5 procent) en het aandeel kwetsbaarheden toenemen (van 14 naar 20 procent).

Nadere detaillering van de typen incidenten

Wanneer de incidenten bij de overheid nader gedetailleerd worden naar type, dan is te zien dat malware-infecties duidelijk het belangrijkste deel van alle incidenten uitmaken: ongeveer 44 procent van alle geregistreerde incidenten hadden betrekking op malware-infecties (tabel 13). Veel van deze malware-infecties werden door het NCSC gedetecteerd als gevolg van de geautomatiseerde controles die het NCSC op dagelijkse basis uitvoert op de informatie die het aangeleverd krijgt uit diverse bronnen. Bij deze controles bekijkt een systeem van het NCSC of geïnfecteerde systemen binnen Nederland kunnen worden gekoppeld aan een, bij het NCSC bekende, organisatie op basis van IP-adres, AS-nummer of domeinnaam. Indien dit het geval is, verstuurt het NCSC een alertering aan de betreffende organisatie. De berichtgeving rondom Pobelka heeft ertoe geleid dat meer organisaties hun netwerkinformatie hebben aangeleverd aan het NCSC waardoor de verwachting is dat het aantal incidenten betreffende malware-infecties de komende periode zal toenemen. Dit laatste komt dan niet zozeer door het feit dat er meer malware-infecties plaatsvinden, maar omdat het NCSC in meer gevallen een infectie zal kunnen matchen aan een organisatie.

Incidenttype	CSBN-2	CSBN-3	Verschil
Malware-infectie	31%	44%	▲ 13%
Websitekwetsbaarheid	24%	15%	▼ 9%
Poging tot hacken	3%	8%	▲ 5%
Onbeschermd/ kwetsbaar systeem	5%	8%	▲ 3%
Aanvalsdreiging	6%	8%	▲ 2%
Phishing	7%	5%	▼ 2%
Uitlekken informatie	10%	5%	▼ 5%
DDoS-aanval	5%	1%	▼ 4%
Overig	9%	6%	▼ 3%

Tabel 13. Ontwikkeling incidenten bij de overheid

In het CSBN-2 voerden we eenzelfde analyse uit over de incidenten bij de overheid. In tabel 13 zijn opgenomen: het percentage van incidenten dat voldeed aan het genoemde incidenttype in CSBN-2, de huidige rapportage (CSBN-3) en de verschuivingen die we kunnen waarnemen tussen deze twee. De belangrijkste verschuiving die we hierin terugzien, is vooral een relatieve toename van het aantal incidenten die betrekking hebben op malware-infecties (▲ 13 procent) en een relatieve afname van incidenten betreffende kwetsbaarheden in websites (▼ 9 procent). «

Bijlage » 3 Afkortingen- en begrippenlijst

0-day	Zie Zero day exploit.
2G/3G	2G is een afkorting voor tweede generatie draadloze telefoontechnologie. Het voordeel van 2G was dat de verbindingen digitaal versleuteld werden. 3G is de opvolger van 2G, ook wel UMTS genoemd. 3G heeft voordelen voor beveiliging en communicatiesnelheid ten opzichte van 2G.
ACM	De Autoriteit Consument en Markt (ACM) is ontstaan uit de samenvoeging van de Nederlandse Mededingingsautoriteit (NMA), Consumentenautoriteit en Onafhankelijke Post- en Telecommunicatieautoriteit (OPTA).
Actor	Een rol die een partij speelt in een ontwikkeling op het gebied van cybersecurity. In veel gevallen gaat het hierbij om een rol die duidelijk aanvallend of verdedigend is, maar dit onderscheid is niet altijd scherp te maken. Een partij kan meerdere rollen spelen, die eventueel gaandeweg ook nog kunnen veranderen.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst.
APT	Een Advanced Persistent Threat (APT) is een gemotiveerde (soms geavanceerde) doelgerichte aanval op een natie, organisatie, persoon of groep van personen.
Authenticatie	Authenticatie is het nagaan of een bewijs van identiteit van een gebruiker, computer of applicatie overeenkomt met vooraf vastgelegde echtheidskenmerken.
Beveiligen	Onttrekken aan geweld, bedreiging, gevaar of schade door het treffen van maatregelen.
Beveiligingsincident	Een (informatie)beveiligingsincident is een enkele of serie van ongewenste of onverwachte gebeurtenissen die een significante kans hebben op het veroorzaken van een ramp, het compromitteren van de bedrijfsprocessen en een bedreiging vormen ten aanzien van de beveiliging.
Bevoegden	Diegenen die een geautoriseerde/functionele toegang hebben tot (onderdelen van) het bedrijf, de locatie, het proces, de middelen of informatie.
BoF	Bits of Freedom (BoF) is een digitale burgerrechtenbeweging.
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 kunnen worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.
Botnetbeheerder	Persoon of organisatie die een botnet onderhoudt en de inzet ervan coördineert.
Bufferoverflow	Een bufferoverflow of bufferoverloop vindt plaats wanneer een programma of proces meer data in het tijdelijk geheugen probeert op te slaan dan mogelijk is. Het teveel aan data overschrijft andere geheugenadressen en dit veroorzaakt problemen in de werking van het programma of proces.
BYOD	Bring Your Own Device (BYOD) is een regeling in organisaties waarbij personeel eigen consumenten-apparatuur kan gebruiken voor het uitvoeren van de organisationele taken.
CA	Een Certificate Authority (CA) is, in een PKI-stelsel, een organisatorisch verband dat wordt vertrouwd om certificaten te maken (genereren), toe te wijzen en in te trekken.
CBS	Centraal Bureau voor de Statistiek.

C&C	Een Command & Control (C&C)-server is een centraal systeem in een botnet van waaruit het botnet wordt aangestuurd.
CERT	Een Computer Emergency Response Team (CERT) is een team dat primair tot doel heeft om incidenten te voorkomen en, wanneer deze toch optreden, adequaat op te treden om de impact ervan te beperken.
Certificaat	Zie Secure Sockets Layer-certificaat.
Cloud/Clouddiensten	Een op internet (de 'wolk') gebaseerd model voor systeemarchitectuur, waarbij vooral gebruikgemaakt wordt van Software as a Service (SaaS).
Compromittering	De kennisname dan wel de mogelijkheid van een niet-gerechtigde tot het kennisnemen van bijzondere informatie.
Cookie	Een cookie is informatie die door een webserver op de computer van een eindgebruiker wordt opgeslagen. Deze informatie kan bij een volgend bezoek van de eindgebruiker aan de webserver weer opgevraagd worden. Cookies kunnen worden gebruikt om gebruikersinstellingen te bewaren en ook om de gebruiker te volgen.
COTS	Commercial Off-The-Shelf (COTS) verwijst naar 'kant-en-klare' software- en hardwareproducten die publiek te koop zijn.
CPNI.NL	Centre for Protection of the National Infrastructure (CPNI.NL) is het Nederlandse platform voor cybersecurity, ondergebracht bij TNO.
CVE	Common Vulnerabilities and Exposures (CVE) is een unieke gemeenschappelijke identificatie van publiekbekende informatiebeveiligingskwetsbaarheden.
Cybercrime	Vorm van criminaliteit waarbij een ICT-systeem of de informatie die daardoor wordt verwerkt, het doelwit is.
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.
Data breach/datalek	Het opzettelijk of onopzettelijk naar buiten komen van vertrouwelijke gegevens.
DCS	De Directie Cybersecurity (DCS), waar onder andere het NCSC onder valt, is onderdeel van de NCTV.
(D)DoS	(Distributed) Denial of Service is de benaming voor een type aanval waarbij een bepaalde dienst (bijvoorbeeld een website) onbereikbaar wordt voor de gebruikelijke afnemers van de dienst. 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.
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 waarbij een authenticiteits- en integriteitscontrole wordt toegevoegd aan het bestaande systeem.

Document	Het begrip document heeft betrekking op brieven, notities, memo's, rapporten, presentaties, tekeningen, foto's, film, kaarten, geluidsopnamen, sms'en, digitale dragers (cd-rom, USB) of enig ander fysiek medium waar informatie op weergegeven kan zijn.
Dreiging	Het Cybersecuritybeeld definieert doel en dreiging als volgt: » Het hogere doel (intentie) kan zijn het verstevigen van de concurrentiepositie; politiek/landelijk gewin, maatschappelijke ontwrichting, levensbedreiging, etc. » Dreigingen in het beeld zijn o.a. ingedeeld als: digitale spionage, digitale sabotage, publicatie van vertrouwelijke gegevens, digitale verstoring, cybercrime en indirecte verstoringen.
ECTF	De Electronic Crimes Taskforce (ECTF) is een samenwerkingsverband tussen de Nationale Politie, het Landelijk Parket, de banken en CPNI.NL, ook wel het 'bankenteam' genoemd. De ECTF heeft een faciliterende rol in de aanpak van op de financiële sector gerichte cybercrime.
Encryptie	Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden.
End of life	In de softwarewereld betekent de end of life van een product de datum waarop een product niet langer door de leverancier als gangbare software wordt beschouwd. Als software end of life is, maakt de leverancier over het algemeen geen updates meer en wordt ook geen ondersteuning meer geleverd.
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/exploitcode	Software, gegevens of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software en/of hardware om ongewenste functies en/of gedrag te veroorzaken.
File inclusion	Aanvalstechniek die voornamelijk bij webapplicaties wordt toegepast, waarbij een gebruiker een bestand met eigen code kan toevoegen om de werking van de applicatie te beïnvloeden.
Fuzzing	Het aanbieden van net onjuiste (input)informatie aan een systeem om te bepalen hoe dit met onjuiste invoer omgaat.
Gerubriceerde gegevens	Door een partij en/of eigenaar gewaarmerkte gegevens, inclusief documenten, of materiaal die beschermd moeten worden tegen ongeoorloofde openbaarmaking en die als zodanig gewaarmerkt zijn in een beveiligingsrubricering.
Gevoelige informatie	Gegevens over kritieke (vitale) infrastructuur die, wanneer zij openbaar worden gemaakt, zouden kunnen worden gebruikt om plannen te maken en feiten te plegen om kritieke infrastructuurinstallaties te verstoren of te vernietigen.
Gps	Het Global Positioning System (GPS) is een plaatsbepalingssysteem op basis van satellieten met een nauwkeurigheid tot op enkele meters. Gps wordt onder andere gebruikt voor navigatie.
Gsm	Global System for Mobile Communications (GSM) is een standaard voor digitale mobiele telefonie. Gsm wordt beschouwd als de tweede generatie mobiele telefoontechnologie (2G).
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 met als doel beperkingen te omzeilen of onverwachte effecten te bereiken.
HTML	HyperText Markup Language (HTML) is een opmaaktaal voor de specificatie van documenten, voornamelijk bedoeld voor webpagina's.

Hulpmiddel	Een techniek of computerprogramma waarmee een aanvaller misbruik kan maken van bestaande kwetsbaarheden of deze kan vergroten.
ICS/SCADA	Industrial Control Systems (ICS) / Supervisory Control And Data Acqusition (SCADA) zijn meet- en regelsystemen, bijvoorbeeld voor de aansturing van industriële processen of gebouwbeheersystemen. ICS/SCADA-systemen verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten.
Identiteitsfraude	Het bewust de schijn oproepen dat een kwaadwillende de identiteit van een ander heeft die niet bij hem hoort.
Incident	Een (cyber)incident is een ICT-verstoring in de dienstverlening waardoor de te verwachten beschikbaarheid van de dienstverlening geheel of gedeeltelijk is verdwenen, en/of het ongeoorloofd openbaren, verkrijgen en/of wijzigen van informatie.
Informatie	Een verzameling van gegevens (met of zonder context) opgeslagen in gedachten, in geschriften (op bijvoorbeeld papier) en/of op digitale informatiedragers (elektronisch, optisch magnetisch).
Informatiebeveiliging	Het proces van vaststellen van de vereiste kwaliteit van informatie(systemen) in termen van vertrouwelijkheid, beschikbaarheid, integriteit, onweerlegbaarheid en controleerbaarheid alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende (fysieke, organisatorische en logische) beveiligingsmaatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
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).
Internet of Things	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 Internet Protocol (IP) zorgt voor adressering van datapakketten, zodat ze bij het beoogde doel aankomen.
IPv4/IPv6	IPv4 is een versie van IP met een adresruimte van ruim 4 miljard adressen. IPv6 is de opvolger daarvan met 3,4×1038 mogelijke adressen, dat zijn 50 miljard keer miljard keer miljard adressen per aardbewoner.
ISAC	Information Sharing and Analysis Centre.
ISP	Een Internet Service Provider (ISP) is een leverancier van internetdiensten, vaak simpelweg aangeduid als ‘provider’. De geleverde diensten kunnen zowel betrekking hebben op de internetverbinding zelf als op de diensten die men op het internet kan gebruiken.
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 dan wel ongeautoriseerd te benaderen.
Lifecycle-management	Lifecycle-management is een onderhoudsmethodiek die erop is gericht om systemen gedurende hun gehele levensduur het bedrijfsproces zo optimaal mogelijk te laten ondersteunen. Doel is het verbeteren van de continuïteit en efficiëntie van productieprocessen.

Malware	Samentrekking van 'malicious' en 'software', kortom: kwaadaardige software. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden.
Merking	Aanduiding die een bepaalde wijze van behandelen van bijzondere informatie aangeeft.
MitM	Man-in-the-middle (MitM) is een aanvalstechniek waarbij de aanvaller zich tussen twee partijen bevindt, bijvoorbeeld een internetwinkel en een klant. Hierbij doet de aanvaller 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, onderdeel van het Ministerie van Veiligheid en Justitie.
NFI	Nederlands Forensisch Instituut.
NVB	Nederlandse Vereniging van Banken.
OM	Openbaar Ministerie.
Ontgoogelen	Informatie over personen of zaken van het internet verwijderen met het doel dat deze inhoud ook uit zoekresultaten verdwijnt.
OSINT	Open Source Intelligence (OSINT) is het vergaren van informatie over iemand door openbare bronnen te raadplegen.
OWASP	Het Open Web Application Security Project (OWASP) is een wereldwijde non-profitorganisatie, gericht op het verbeteren van de beveiliging van webapplicaties.
Patch	Een patch (letterlijk: 'pleister') kan bestaan uit reparatiesoftware of kan wijzigingen bevatten, die direct in een programma worden doorgevoerd om het desbetreffende 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. Spearphishing is een variant die zich richt op één persoon of een zeer beperkte groep personen in bijvoorbeeld een organisatie, die specifiek worden uitgekozen op basis van hun toegangspositie om een zo groot mogelijk effect te sorteren zonder al te veel op te vallen.
PKI	Een Public Key Infrastructure (PKI) is een verzameling organisatorische en technische middelen waarmee je op een betrouwbare manier een aantal zaken kunt regelen, zoals het versleutelen en ondertekenen van informatie en het vaststellen van de identiteit van een andere partij.
Relevantie	Geeft de verhouding weer tussen de verschillende dreigingen, dreigers en doelwitten. Om de verschillende dreigingsniveaus in het CSBN te bepalen worden incidenten, dreigingen binnen de analyses gewogen met de criteria van 'laag', 'midden' en 'hoog'.
Remote Access	Op afstand kunnen verwerken van gegevens met een communicatieverbinding.
Rootkit	Een stuk software dat een aanvaller meer rechten op een computersysteem geeft, terwijl de aanwezigheid van deze software wordt verborgen voor het besturingssysteem.

RFID	Radio Frequency Identification (RFID) devices zijn kleine chips die door middel van identificatie met radiogolven op afstand informatie kunnen opslaan en/of zijn uit te lezen. De zogenaamde RFID-tags kunnen op of in objecten of levende wezens (katten- of hondenchip) zitten.
Rubricering	Vaststellen en aangeven dat een gegeven bijzondere informatie is en het bepalen en aangeven van de mate van beveiliging die aan deze informatie moet worden gegeven.
SIDN	Stichting Internet Domeinregistratie Nederland.
SCADA	Zie ICS/SCADA.
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 met als doel vertrouwelijke informatie te verkrijgen of het slachtoffer een bepaalde handeling te laten verrichten.
SOHO	Small Office/Home Office (SOHO) wordt gebruikt om te verwijzen naar gebruik in thuissituaties en kleine bedrijfjes en kantoren.
Spearphishing	Zie phishing
Spoofen/IP-Spoofing	Spoofen betekent 'je voordoen als een ander', meestal in kwaadaardige zin. Bij IP-Spoofing wordt het IP-adres van een andere computer gebruikt, hetzij om de herkomst van netwerkverkeer te maskeren, hetzij om de computer daadwerkelijk als een andere computer voor te laten doen.
SQL-injectie	Aanvalstechniek waarbij de communicatie tussen een applicatie en de achterliggende database kan worden beïnvloed door de gebruiker, met hoofdzakelijk als doel gegevens in de database te manipuleren of te stelen.
SSL-certificaat	Een Secure Socket Layer (SSL)-certificaat is een bestand dat fungeert als digitale identificatie van een persoon of systeem. Het bevat tevens PKI-sleutels om gegevens tijdens transport te versleutelen. Een bekende toepassing van SSL-certificaten zijn de met HTTPS beveiligde websites.
Staatsgeheim	Bijzondere informatie waarvan de geheimhouding door het belang van de Staat of haar bondgenoten wordt geboden.
Stepping Stone	Een Stepping Stone-aanval is een aanval via meerdere systemen en/of organisaties, ofwel ketenaanval. In een serie van eerder gehackte machines komt een kwaadwillende uiteindelijk bij het doel. Stepping Stone is ook een hulpmiddel om de eigen ware identiteit te verbergen.
Tablet	Een draagbare computer waarbij het beeldscherm tevens de belangrijkste invoermogelijkheid is.
THTC	Team High Tech Crime (Nationale Politie).
TNO	Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek.
Tweefactorauthenticatie	Een manier van authenticeren waarbij twee onafhankelijke bewijzen voor een identiteit zijn vereist. Dit bewijs kan zijn: kennis over, bezit van of biometrische eigenschappen die de identiteit van de aanvrager bewijst.
UMTS	Universal Mobile Telecommunications System; zie 2G/3G.

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 gerechtigd is het gegeven te benaderen. Wie gerechtigd is een gegeven te benaderen, wordt vastgesteld door de eigenaar van het gegeven.
VNO-NCW	Verbond van Nederlandse Ondernemingen - Nederlands Christelijk Werkgeversverbond.
Webapplicatie	De term waarmee het geheel wordt aangeduid van software, databases en systemen die betrokken zijn bij het correct functioneren van een website, waarbij de website het zichtbare gedeelte is.
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.
Wifi/Wi-Fi	Een handelsmerk van de Wi-Fi Alliance. Een apparaat met Wi-Fi kan draadloos communiceren met andere apparatuur tot op enkele honderden meters.
Zero day exploit	Een zero day exploit is een exploit die misbruik maakt van een kwetsbaarheid waarvoor nog geen patch beschikbaar is.

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Per 23 augustus 2013:
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070-888 75 55
F 070-888 75 50
csbn@ncsc.nl
www.ncsc.nl

Juni 2013