Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Cybersecuritybeeld Nederland

CSBN-2

Cybersecuritybeeld Nederland

CSBN-2

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Juni 2012

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 expertise en advies, respons 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 NCTV.

Samenwerking en bronnen

Dit rapport is opgesteld door het NCSC. De ministeries, MIVD, AIVD, politie (KLPD, THTC), OM (LP), KPN, OPTA, NFI, CBS, NVB, ISACs, BoF, NCTV, wetenschappelijke instituten en universiteiten 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

De cyberincidenten van de afgelopen periode laten zien dat het een uitdaging is om adequate en vooral tijdige maatregelen te nemen die Nederland weerbaar maken tegen dreigingen in de digitale wereld. De dagelijkse realiteit laat een breed scala van incidenten zien. In het nieuws wordt regelmatig bericht over aanvallen op kwetsbaarheden en verstoringen van de complexer wordende ICT-infrastructuur.

Nieuwe aanbieders, technieken en diensten zorgen ervoor dat de maatschappelijke afhankelijkheid van internet steeds groter wordt. De cybersecurityincidenten leren echter ook dat internet en ICT kwetsbaarheden bevatten die gebruikt kunnen worden door kwaadwillenden.

De signalen zijn niet nieuw. Als in een mantra volgen incidenten en adviezen elkaar voortdurend op. Maar dat leidt nog niet altijd tot de juiste acties. Een aantal incidenten uit 2011 had voorkomen kunnen worden door het treffen van bekende basismaatregelen. Toch is navolging van de verbeteradviezen bij deze incidenten achterwege gebleven door onbekendheid met de kwetsbaarheden en maatregelen of door onvoldoende gevoel van urgentie. Ook dit Cybersecuritybeeld bevat herhalingen die nog steeds actueel zijn of die door nieuwe ontwikkelingen relevanter zijn geworden.

Dit tweede Cybersecuritybeeld beschrijft de incidenten, dreigingen en kwetsbaarheden die voor Nederland relevant zijn, opdat organisaties en individuen hun inzicht in de cyberrisico's kunnen vergroten en met de juiste maatregelen hun weerbaarheid kunnen verhogen. Ook geeft het voor het eerst een beeld van de ontwikkelingen op het gebied van de digitale weerbaarheid van de Nederlandse samenleving

Ook de komende periode blijven incidenten, kwetsbaarheden en dreigingen een gegeven. De uitdaging is om hieruit lering te trekken, response voor te bereiden en herhaling te voorkomen.

Elly van den Heuvel

General Manager Nationaal Cyber Security Centrum

INHOUD

UITGANGSPUNTEN

Het Cybersecuritybeeld Nederland wordt opgesteld door het Nationaal Cyber Security Centrum (NCSC). Uitgangspunt is dat het NCSC wat betreft de vaststelling van de inhoud van het Cybersecuritybeeld Nederland onafhankelijk is. Bij het opstellen van het Cybersecuritybeeld is samengewerkt met organisaties en diensten die aan het NCSC gelieerd zijn.

Inhoud

Het Cybersecuritybeeld Nederland is een observatie en analyse van de nationale en internationale cybersecurity-ontwikkelingen ten behoeve van de ambtelijke en politieke leiding en beleidsmakers. In de rapportage worden geen aanbevelingen en adviezen gedaan.

Reikwijdte

Het Cybersecuritybeeld Nederland heeft betrekking op Nederland en de Nederlandse belangen in het buitenland. Hierbij is de aandacht primair gevestigd op de (Rijks)overheid, de vitale sectoren en de burger.

Inhoudelijke grondslag

Voor het Cybersecuritybeeld Nederland wordt gebruikgemaakt van (gerubriceerde) informatie van diensten belast met cybersecurity en cybercriminaliteitsbestrijding alsmede openbaar toegankelijke bronnen, bestuurlijke bronnen, informatie van de vitale sectoren en analyses van het NCSC en zijn internationale partners. Kwantitatieve gegevens worden, indien deze beschikbaar zijn, gebruikt om observaties in het Beeld te onderbouwen.

Rapportageperiode

De formele rapportageperiode van dit Cybersecuritybeeld loopt van 1 juli 2011 tot en met 31 maart 2012. Recente ontwikkelingen tot en met begin mei 2012 zijn eveneens in het Beeld verwerkt. Het Cybersecuritybeeld Nederland geeft een zo actueel mogelijke observatie van cybersecurity en is uitdrukkelijk geen trend-, voortgangs- en/of incidentenrapportage.

Presentatie

Het Cybersecuritybeeld wordt door de minister van Veiligheid en Justitie aangeboden aan de ministerraad, de Cyber Security Raad en de Tweede Kamer. Daarnaast wordt het rapport aangeboden aan relaties, belanghebbenden en het publiek via de website van het NCSC.

SAMENVATTING

De beveiliging van informatie en communicatietechnologie (ICT), kortweg cybersecurity, is een serieus onderwerp. De te verdedigen belangen achter ICT-systemen zijn groot en betreffen niet alleen informatie maar ook allerlei diensten die vitaal zijn voor het functioneren van de Nederlandse samenleving. Tegelijkertijd blijkt uit recente incidenten dat ICT-systemen kwetsbaar zijn en dat actoren, met hun motieven, een dreiging kunnen vormen voor de Nederlandse belangen.

Daarbij onderschatten de systeem- en informatie-eigenaren vaak de waarde van informatie. Identiteitsgegevens, bedrijfsinformatie, kwetsbaarheden van software en organisaties hebben voor verschillende actoren een grote waarde en/of worden voor grote bedragen verhandeld. De eenvoudige toegang tot deze handel lokt steeds meer individuen en werkt als een aanjager voor incidenten op het vlak van cybersecurity.

Onze samenleving is kwetsbaar. Het vergroten van de weerbaarheid van de Nederlandse ICT-infrastructuren blijft daarom onverminderd noodzakelijk. Dit besef en de noodzaak voor een integrale aanpak heeft in 2011 geleid tot het formuleren van de Nationale Cyber Security Strategie.

Een van de actielijnen die de strategie beschrijft, is de realisatie van adequate en actuele dreigings- en risicoanalyses. In december 2011 is de eerste stap gezet in de uitvoering van die actielijn: het uitbrengen van het eerste Cybersecuritybeeld. Dit tweede Cybersecuritybeeld beschrijft, net als het eerste, de dreigingen in het nationale ICT-domein.

Op basis van openbare en niet-openbare bronnen, gesprekken, een enquête onder verschillende partijen en (operationele) informatie van het NCSC, de aangesloten liaisons en inlichtingendiensten zijn de dreigingen, incidenten, kwetsbaarheden en de genomen maatregelen op hoofdlijnen in beeld gebracht.

Ten opzichte van de vorige editie is dit Cybersecuritybeeld uitgebreid met dreigingen van de interne actor, calamiteiten, rampen en een hoofdstuk 'weerbaarheid'. Het beeld is versterkt met meer casuïstiek van een aantal typerende securityincidenten, kwantitatieve analyses en de incidentcijfers van het NCSC. Over de hele linie is de basis van het tweede Cybersecuritybeeld Nederland verbreed. Hiermee worden de eerste stappen gezet voor verdere differentiatie en kwantificering in het Cybersecuritybeeld.

Kernbevindingen

- Op hoofdlijnen zijn er geen grote verschuivingen in dreigingen waarneembaar. Gezien de ernst moeten de dreigingen daarom onveranderd de aandacht krijgen. Wel zijn de handelingen van de hacktivisten, beroepscriminelen en cyberonderzoekers de afgelopen periode zichtbaarder geweest. De overige nieuwe dreigersgroepen (interne actoren en calamiteiten) en dreigingen in dit Cybersecuritybeeld vormen vooralsnog een lage tot middelmatige dreiging.
- Digitale spionage en cybercriminaliteit blijven de grootste dreigingen voor overheid en bedrijfsleven.
- De aanvaller is nog steeds in het voordeel. Ondanks diverse initiatieven tot verbetering houden de verdedigingsmaatregelen, -methodes en -initiatieven nog geen gelijke tred met de motivatie, doorzettingsvermogen en de middelen van de opponenten.
- Een aantal incidenten gedurende de rapportageperiode is te wijten aan simpele kwetsbaarheden en was te voorkomen geweest door het navolgen en implementeren van basale beveiligingsmaatregelen.
- Consumerization, mobiel internet en uitbreiding van de internetdienstverlening zorgen voor een uitzonderlijke toename van het aantal op internet aangesloten apparaten. Dit zal resulteren in een grotere maatschappelijke afhankelijkheid, meer (software-)kwetsbaarheden en een exponentiële toename in complexiteit van de beheersvraagstukken.
- Het ontbreekt een doorsnee internetgebruiker (en een aantal organisaties) aan voldoende kennis en kunde om zich goed te beschermen tegen digitale risico's. Verdere toename van consumerization zal deze achterstand vergroten.
- Actoren werken steeds meer samen en delen direct of indirect en bedoeld of onbedoeld kennis. Deze trend geldt zowel voor actoren met een positieve bijdrage aan de veiligheid van internet als voor kwaadwillende actoren.
- Kwaadwillenden zijn steeds sneller in staat zwakheden te misbruiken ten opzichte van de lange doorlooptijden die organisaties nodig hebben om patches te implementeren.

Tijdens het opstellen van het Cybersecuritybeeld Nederland is gebleken dat er door partijen en in publicaties verschillende cybertaxonomieën en registratiemethodes (cyberincidenten en dreigingen) worden gebruikt. Dit bemoeilijkt de analyses op hoofdlijnen en een snelle en eenduidige aggregatie van gegevens.

Actoren

De aard van de activiteiten van actoren is op hoofdlijnen onveranderd ten opzichte van het vorige beeld. Van de (heimelijke) activiteiten van staten en beroepscriminelen is de dreiging nog steeds '**hoog**'. Zowel burgers als private organisaties en staten blijven daarbij kwetsbaar als doelwit.

De verschillende actoren werken steeds meer samen en kennis wordt ten goede en ten kwade steeds meer (in)direct en in sommige gevallen onbedoeld gedeeld.

De afgelopen periode is er ook een verhoogde zichtbaarheid, media-aandacht en toename van het aantal activiteiten waarneembaar van hacktivisten en cyberonderzoekers.

De cyberonderzoeker is in dit Cybersecuritybeeld toegevoegd en heeft de intentie om kwetsbaarheden aan de kaak te stellen en de beveiliging te verbeteren. In dit Cybersecuritybeeld is ook de interne actor toegevoegd, omdat er een significante dreiging van deze actor uitgaat.

Dreigingen

Op basis van analyses en incidenten in deze rapportageperiode zijn '**digitale spionage**' en '**malwarebesmetting en spam**' geschat op een '**hoge**' dreiging voor de '**overheid**'.

'**Private organisaties**' moeten vooral rekening houden met '**digitale spionage**', '**malwarebesmetting en spam**' en '**digitale (identiteits)fraude**'.

'**Malwarebesmetting en spam**' is een '**hoge**' dreiging voor '**burgers**'.

De belangrijkste '**dreigers**' zijn nog steeds '**staten**' met '**digitale spionage**'-activiteiten en '**(beroeps)criminelen**' met activiteiten voor financieel gewin.

De 'nieuwe', in het Cybersecuritybeeld opgenomen, dreigers ('**interne actoren**' en '**cyberonderzoekers**') kunnen met hun handelen een dreiging vormen van het niveau '**laag**' tot '**midden**'.

DOELWITTEN →

DREIGERS ↓

	Overheid	Private organisaties	Burgers
Staten	Digitale spionage	Digitale spionage	Digitale spionage
Private organisaties		Digitale spionage	
(Beroeps)criminelen	Verstoring door malwarebesmetting en spam	Verstoring door malwarebesmetting en spam	Verstoring door malware-besmetting en spam
		Digitale (identiteits)fraude	Digitale (identiteits)fraude
	Chantage	Chantage	Chantage
	Verstoring online dienstverlening	Verstoring online dienstverlening	
Terroristen	Sabotage	Sabotage	
Hacktivisten	Publicatie van vertrouwelijke gegevens	Publicatie van vertrouwelijke gegevens	Publicatie van vertrouwelijke gegevens
	Verstoring vitale infrastructuur	Verstoring vitale infrastructuur	
	Verstoring online dienstverlening	Verstoring online dienstverlening	
	Hoax	Hoax	Hoax
Scriptkiddies	Verstoring online dienstverlening	Verstoring online dienstverlening	
Cyberonderzoekers	Publicatie van vertrouwelijke gegevens	Publicatie van vertrouwelijke gegevens	
Interne actoren	Publicatie van vertrouwelijke gegevens	Publicatie van vertrouwelijke gegevens	
		Chantage	
Geen actor	Brand, waterschade en natuurrampen	Brand, waterschade en natuurrampen	
	Falen en/of ontbreken van hard- en software	Falen en/of ontbreken van hard- en software	

Relevantie: *Onbekend/n.v.t.* *Laag* *Midden* *Hoog* *(duiding: zie bijlage 1)*

Dreigingen zijn er in verschillende vormen: dreigingen die doelbewust veroorzaakt worden door de mens (informatiegerelateerde dreigingen, systeemgerelateerde dreigingen en indirecte dreigingen) en dreigingen in de vorm van calamiteiten door samenloop van omstandigheden. De relevantie van de dreiging in het Cybersecuritybeeld Nederland is een expertinschatting. Deze wordt uitgedrukt in '**hoog**' (rood), '**midden**' (oranje) en '**laag**' (geel). De gehanteerde weging van de dreigingen staat beschreven in bijlage 1.

Kwetsbaarheden

Het blijkt dat het beveiligen van websites nog altijd onvoldoende aandacht krijgt. Kwetsbaarheden worden in onvoldoende mate verholpen waardoor kwaadwillende partijen gegevens kunnen inzien en manipuleren. Ook de toegangsbeveiliging van webapplicaties schiet nog vaak tekort. Gekozen wachtwoorden van gebruikers zijn te eenvoudig of te kort, waardoor ze gemakkelijk door een aanvaller te raden zijn. Daarnaast worden inloggegevens voor een systeem vaak bij andere systemen hergebruikt. Een lek in de beveiliging van de ene website leidt er daardoor toe dat aanvallers ook toegang kunnen krijgen tot andere systemen.

Werknemers bezitten steeds vaker smartphones en tablets die ook worden gebruikt in werkomgevingen. Dit concept, dat Bring Your Own Device (BYOD) heet, zorgt voor een complexer wordend beheer van de ICT-infrastructuur. Doordat een eigenaar zelf 'apps' kan installeren ontstaan er veel verschillende installaties. Dit heeft tot gevolg dat de aanwezigheid van kwetsbaarheden en/of malware vaak laat of niet opgemerkt wordt. Momenteel is het zo dat ontdekte kwetsbaarheden in mobiele besturingssystemen soms maanden onopgelost blijven. Kwaadwillenden kunnen zich langs deze weg toegang verschaffen tot informatie en systemen. Bewezen maatregelen en 'best-practices' voor beveiliging zijn er op dit vlak nog nauwelijks.

In de rapportageperiode van dit Beeld haalde een aantal kwetsbaarheden in ICS/SCADA-systemen de media. Deze systemen worden gebruikt voor de besturing van industriële processen. Het NCSC ontving meldingen van, via internet bereikbare, ICS/SCADA-systemen. Deze systemen vormen waarschijnlijk een langdurige kwetsbaarheid omdat het niet eenvoudig is ze te voorzien van updates wanneer kwetsbaarheden in hun software worden ontdekt. Ook komen steeds meer softwarehulpmiddelen in het publieke domein beschikbaar die een kwaadwillende in staat stellen op een eenvoudige manier misbruik te maken van zulke kwetsbaarheden.

Hulpmiddelen

De belangrijkste technische hulpmiddelen die dreigersgroepen inzetten, zijn nog steeds exploits, malware en botnets. Botnets behouden een spilfunctie bij het uitvoeren van cyberaanvallen. Opvallend is de gestegen aandacht van cybercriminelen voor het Mac-platform, die tot uiting kwam in de vorming van een groot botnet van meer dan 500.000 Mac-computers. Door geavanceerde exploitkits is het voor cybercriminelen makkelijker geworden om botnets op te bouwen. De laatste generatie exploitkits is geschikt gemaakt om meerdere platformen tegelijk aan te vallen en bevat parallel een uitbreidbare reeks van exploits voor verschillende kwetsbaarheden.
De toename in gebruiksvriendelijkheid zorgt ervoor dat zulke tools door een groter wordende groep cybercriminelen en scriptkiddies te gebruiken zijn. Naast exploitkits is in dit Cybersecuritybeeld aandacht voor de wijze waarop webmailaccounts worden overgenomen, die daarna worden misbruikt voor het versturen van spam en malware.
Ook zijn er nieuwe ontwikkelingen op het gebied van ransomware. Er zijn nu varianten die een computer alleen nog laten opstarten indien er losgeld wordt betaald.

In dit Cybersecuritybeeld wordt ook nog een hulpmiddel beschreven dat zowel voor goedaardige als kwaadaardige doeleinden kan worden gebruikt: technieken voor het verhullen van de identiteit. Deze technieken kunnen bijvoorbeeld worden gebruikt door cybercriminelen om opsporing te bemoeilijken maar ook door de politie om onopvallend onderzoek te kunnen doen.

Weerbaarheid

Digitale weerbaarheid is het vermogen om weerstand te bieden aan negatieve invloeden op de beschikbaarheid, vertrouwelijkheid en/of integriteit van (informatie)systemen en digitale informatie. De digitale weerbaarheid staat daarbij in het teken van de continuïteit van de dienstverlening en van de handhaving van de effectiviteit ervan.

Op het gebied van weerbaarheid zijn de afgelopen periode belangrijke initiatieven ontplooid. De meest in het oog springende initiatieven hebben betrekking op het verhogen van het bewustzijn, de toenemende nationale en internationale samenwerking, de stimulering van (wetenschappelijk) onderzoek en het vergroten van de capaciteit van het NCSC, het Team High Tech Crime (THTC) en Defensie op het gebied van cybersecurity. Op meer detailniveau is een toenemende aandacht voor de bestrijding van cybercriminaliteit en botnets. Daarnaast zijn wetsvoorstellen geïnitieerd voor onder andere het melden van datalekken.

In navolging van de aanbevelingen in de Nationale Cyber Security Strategie zijn de Cyber Security Raad en het NCSC opgericht. Het NCSC publiceerde in navolging van grote incidenten in 2011, samen met Logius, het Ministerie van Binnenlandse Zaken en andere belanghebbenden de 'ICT-richtlijnen voor het beveiligen van webapplicaties'. Ook zijn in navolging van het ontdekken van kwetsbaarheden aanbevelingen gepubliceerd rond de beveiliging van ICS/SCADA-omgevingen.

Hoewel veel losstaande initiatieven worden ontplooid rond het thema cybersecurity, blijkt er veel behoefte te zijn aan een integrale aanpak waarin voldoende afstemming plaatsvindt tussen de diverse initiatieven. Deze wens is niet nieuw en werd ook al als boodschap meegegeven in het 'Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010'.

HOOFDSTUK 1

Inleiding

1.1 Opzet

Het Cybersecuritybeeld Nederland (CSBN) wordt elk jaar door het NCSC gepubliceerd. Het rapport, een observatie van de status van cybersecurity binnen Nederland, geeft beleidsmakers inzichten om de weerbaarheid van Nederland tegen cyberdreigingen te versterken en lopende cybersecurityprogramma's te verbeteren.

Op verzoek van zowel de Tweede Kamer als de Cyber Security Raad worden de komende rapportages uitgebreid met een gedetailleerder overzicht van de toestand van cybersecurity binnen de private sectoren en binnen de organisaties uit de vitale sectoren. Dit proces verloopt geleidelijk en beslaat meerdere jaren.

In dit Cybersecuritybeeld zijn voor het eerst opgenomen:

- de (interne of externe) medewerkers als actoren;
- de rol van cyberonderzoeker;
- de dreiging: natuurlijke en onvoorziene omstandigheden, menselijke fouten en het handelen van interne en externe medewerkers;
- een analyse van de weerbaarheid en geboden weerstand tegen dreigingen.

Verder is bij kwalitatieve analyses een kwantitatieve onderbouwing geboden waar deze beschikbaar was. Het NCSC blijft zich ook in de komende periode richten op het verzamelen van meer kwantitatieve informatie teneinde de kwalitatieve analyses uitgebreider te onderbouwen.

1.2 Achtergrond

Dit Cybersecuritybeeld staat niet op zich. Het moet worden gelezen in het kader van eerdere publicaties en andere initiatieven. Het Cybersecuritybeeld bouwt voort op het vorige dat in december 2011 is uitgebracht. Het opstellen van het Cybersecuritybeeld wordt in de Nationale Cyber Security Strategie genoemd als een van de taken van het NCSC.

1.3 Doelstelling

De doelstelling van het Cybersecuritybeeld is het bieden van inzicht over de cybersecurityontwikkelingen en de veiligheid van de digitale samenleving. Het Cybersecuritybeeld maakt duidelijk welke ontwikkelingen zijn te herkennen in de dreigingen, actoren, kwetsbaarheden, hulpmiddelen en tegenmaatregelen.

1.4 Onderzoeksmethoden

Dit Cybersecuritybeeld is een analyse en observatie van de stand van zaken met betrekking tot cybersecurity binnen Nederland. Het internationale karakter van cybersecurity impliceert dat ook internationale ontwikkelingen voor dit onderwerp relevant zijn en dus worden besproken.
Voor het opstellen van het Cybersecuritybeeld is gebruikgemaakt van drie methoden van informatieverzameling, literatuurstudie, enquête en een operationele analyse. Waar mogelijk is bij onderwerpen uitgegaan van rapporten van al eerder uitgevoerde onderzoeken zoals overheidsrapporten, wetenschappelijke artikelen, rapporten van relevante marktpartijen en verslaglegging rond belangrijke gebeurtenissen zoals de DigiNotarcrisis. De hieruit verkregen informatie is verrijkt met interne informatie die het NCSC eerder heeft gegenereerd, zoals adviezen die door het NCSC zijn geschreven.

Operationele analyse

Aanvullend op de hierboven beschreven studie is gebruikgemaakt van expertise en analysecapaciteit van het NCSC en van organisaties die aan het centrum zijn gelieerd. Enerzijds is dit gebeurd door het verspreiden van een enquête; de resultaten hiervan dienden als ondersteuning van meerdere bevindingen uit het Cybersecuritybeeld. Anderzijds vroegen de auteurs operationele informatie op bij de partners en zijn er gesprekken gevoerd met bij het centrum betrokken medewerkers van overheidspartijen en met vertegenwoordigers van organisaties uit de vitale sectoren om de ervaringen over cybersecurity bij deze organisaties mee te nemen in het Beeld.

Informatiepositie

Tijdens het opstellen van het Cybersecuritybeeld Nederland is gebleken dat door partijen en in publicaties verschillende cybertaxonomieën en registratiemethodes (cyberincidenten en dreigingen) worden gebruikt. Gegevens in registratiesystemen en in rapportages zijn niet uniform en eenduidig. Dit leidt tot uiteenlopende inzichten en expertdiscussies over de kwaliteit en juistheid van een rapport of gegeven.

Gebleken is dat elke organisatie anders lijkt om te gaan met rapportageperiodes, het vastleggen van incidenten, zwakheden, dreigingen en calamiteiten in registratiesystemen. Het begrip 'incident' is daarbij ook verwarrend. Een gebeurtenis wordt wel, niet en/of meerdere keren in een registratiesysteem ingevoerd. In de ene organisatie worden alleen werkelijke incidenten als gebeurtenis geregistreerd, terwijl andere registratiesystemen zowel het incident als de detectie van zwakheid en/of pogingen en vermoedens van incidenten vastleggen. Deze uiteenlopende kwaliteit van de gegevens zorgt voor een verminderde efficiëntie en effectiviteit bij het maken van (risico)analyses en het aggregeren van gegevens.

1.5 Leeswijzer

De lezer dient zich bij het doornemen van dit Cybersecuritybeeld bewust te zijn van de opzet ervan. Aspecten van een incident, ontwikkeling of gegeven kunnen daardoor verspreid zijn over meerdere hoofdstukken, waarbij het mogelijk is dat informatie herhaald wordt. Hierbij is een afweging gemaakt tussen de leesbaarheid van het Cybersecuritybeeld als geheel en het begrijpelijk presenteren van informatie in de verschillende onderdelen.

De verschillende hoofdstukken beschrijven de situatie en ontwikkelingen op het gebied van cybersecurity elk op een eigen manier. Hoofdstuk 2 beschrijft de rollen die partijen kunnen spelen in het speelveld van cybersecurity. Om tot een goed begrip van de relevantie van dreigingen te komen, is het belangrijk om inzicht te hebben in de aard, intenties en middelen van de verschillende actoren binnen cybersecurity. In hoofdstuk 3 komen de dreigingen aan bod die deze of andere partijen kunnen vormen voor de beveiliging van burgers, organisaties en de (Rijks)overheid. Hoofdstuk 4 benoemt de kwetsbaarheden die ten grondslag liggen aan geldende cyberdreigingen. Hulpmiddelen waarvan de aanvallende of de verdedigende zijde zich bedient, komen aan bod in hoofdstuk 5. De weerstand die geboden wordt tegen dreigingen, wordt beschreven in hoofdstuk 6.

In het Cybersecuritybeeld zijn casussen opgenomen waarin een relevant en recent incident wordt uitgelicht ter illustratie van de mededeling in de hoofdtekst.

Meer kwantitatieve gegevens en verklaringen van de gebruikte begrippen zijn te vinden in de bijlagen.

1.6 Kernbegrippen

Hiernaast afgebeelde figuur geeft een overzicht van de verschillende objecten die een rol spelen bij de analyses in dit beeld. Belangen van organisaties en de samenleving (daarin specifiek de kwetsbaarheden) kunnen bedreigd worden door handelingen van een actor en/of door gebeurtenissen zonder actor (natuurrampen, brand, et cetera). Indien een belang met bijbehorende zwakheden onvoldoende door de maatregelen (controls) wordt gecompenseerd (verdedigd), dan kan een dreiging tot een incident en in een ernstige gevallen tot een calamiteit leiden.

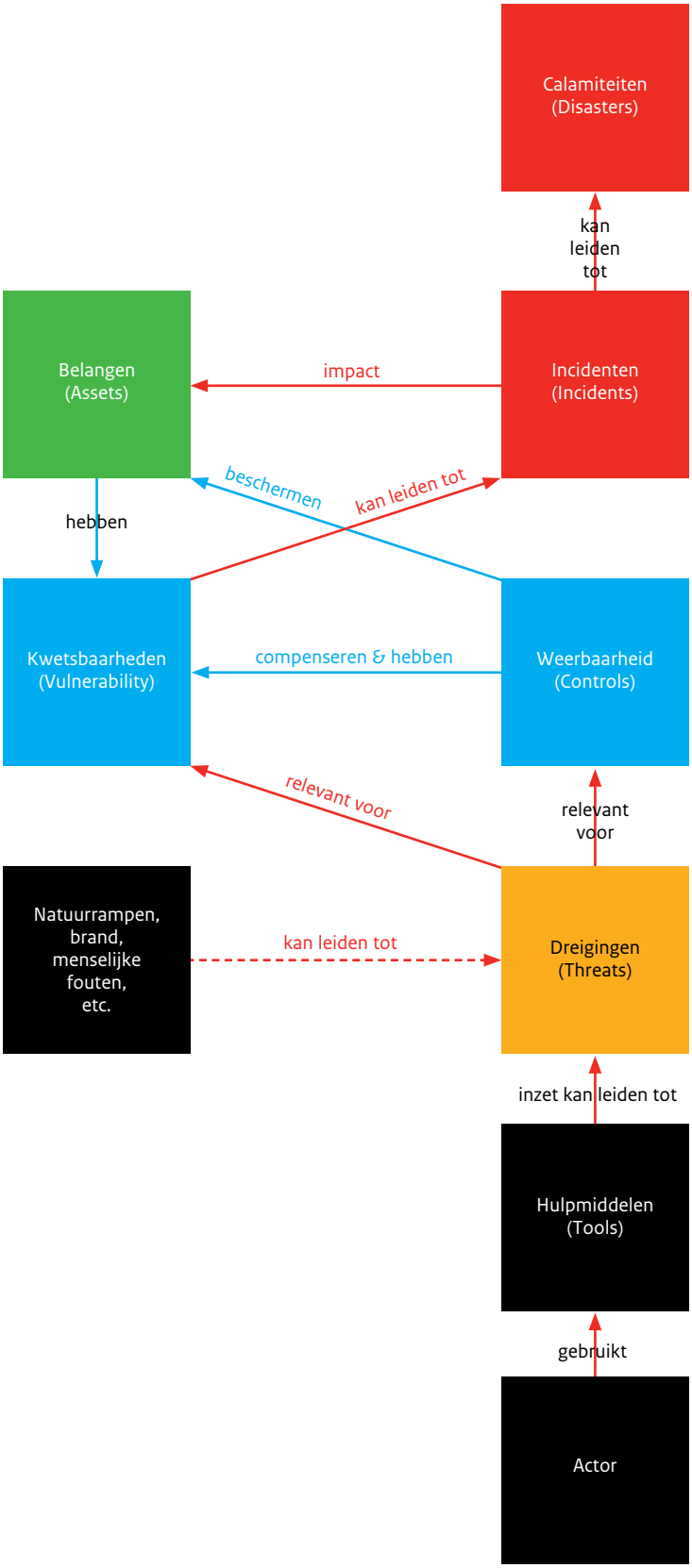
Wat is cybersecurity?

'Cybersecurity' is 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.[1]

Wat is een actor?

Een 'actor' is 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.

Figuur 1. Samenhang tussen kernbegrippen op het vlak van cybersecurity



1. Nationale Cyber Security Strategie

Wat is een dreiging?
Een 'dreiging' is een ongewenste gebeurtenis die kan plaatsvinden. De dreiging kan zowel van buiten als van binnen komen. Een dreiging kan werkelijkheid worden als er een kwetsbaarheid is die de dreiging kan gebruiken. Als de dreiging werkelijkheid wordt, een cybersecurityincident, dan resulteert dat in schade aan waardevolle eigendommen en/of verstoring van waardevolle processen.

Wat is een hulpmiddel?
Een 'hulpmiddel' is een techniek of computerprogramma waarmee een aanvaller misbruik kan maken van bestaande kwetsbaarheden of deze kan vergroten. Eenduidige hulpmiddelen worden in sommige gevallen ook ingezet door een verdedigende partij om kwetsbaarheden te ontdekken en/of als repressie bij aanvallen.

Wat is een kwetsbaarheid?
Een 'kwetsbaarheid' is een 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. Een kwetsbaarheid wordt veroorzaakt door menselijke, organisatorische of technologische factoren. Het verhelpen van kwetsbaarheden is een directe manier om het risico van dreigingen af te doen nemen.

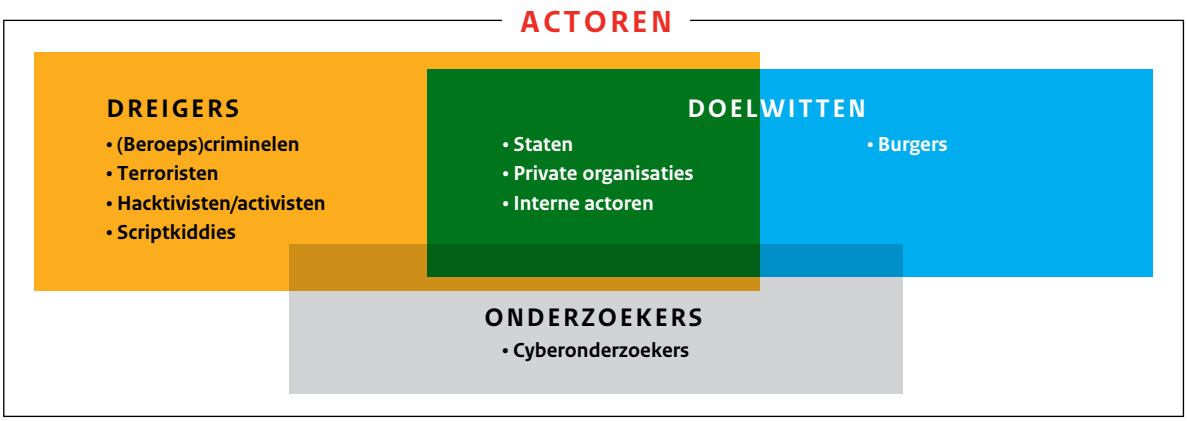
Wat is (digitale) weerbaarheid?
'(Digitale) weerbaarheid' is het vermogen van personen, organisaties of samenlevingen om weerstand te bieden aan negatieve invloeden op de beschikbaarheid, vertrouwelijkheid en/of integriteit van (informatie)systemen en digitale informatie. De digitale weerbaarheid staat daarbij in het teken van de continuïteit van de dienstverlening en de handhaving van de effectiviteit ervan.

Wat is een (cyber) 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. In ernstige gevallen kan een incident escaleren tot een calamiteit.

HOOFDSTUK 2

Actoren

Figuur 2. Clustering van actoren



In dit hoofdstuk worden actoren en hun belangrijkste kenmerken beschreven. Een 'actor' is een rol die een partij speelt op het gebied van cybersecurity. Een partij kan meerdere rollen spelen, die gaandeweg ook nog kunnen veranderen. Ook maken actoren van elkaars capaciteiten gebruik. Actoren worden gekenmerkt door een bepaalde intentie en een bepaald profiel.

In het 'Cybersecuritybeeld Nederland December 2011' zijn actoren ingedeeld in twee categorieën: dreigers en doelwitten. In dit Cybersecuritybeeld is de categorie onderzoeker toegevoegd waar de 'cyberonderzoeker' deel van uitmaakt. Ook is de actor 'interne actor' toegevoegd (zie figuur 2). De cyberonderzoeker kan in sommige gevallen ook als dreiger of doelwit worden gezien. De interne actor is zowel een dreiger als een doelwit. De actoren uit figuur 2 worden in de paragrafen 2.1 tot en met 2.9 beschreven.

Aan een cybersecurityincident is vaak niet eenvoudig te zien door welke actor deze veroorzaakt is: attributie is in cyberspace een complexe aangelegenheid.

Het niveau van expertise en vaardigheden binnen dreigers loopt uiteen van specialisten tot zogeheten scriptkiddies. De potentiële impact van een aanval is echter niet altijd evenredig met de expertise: ook scriptkiddies kunnen veel schade veroorzaken (zie hoofdstuk 3).

In tabel 1 is een overzicht van dreigers weergegeven met hun intenties, primaire doelwitten, middelen, volume aan aanvallen en zichtbaarheid. De burger is niet in dit overzicht opgenomen omdat hij niet tot de dreigers behoort.

De kolommen middelen, volume en zichtbaarheid zijn eigenschappen van actoren die in de loop der tijd kunnen

Tabel 1. Dreigers

Actor	Intentie (doel/uiting)	Primair doelwit	Middelen	Volume	Zichtbaarheid
Staten	Geopolitieke positie verbeteren (interne machtspositie vergroten)	Overheden, multinationals, vitale infrastructuur, burgers (in het geval van bepaalde regimes)	Veel	Midden	Laag
Private organisaties	Informatiepositie verbeteren	Concurrenten	Veel	Laag	Laag
Beroepscriminelen	Geldelijk gewin	Financiële diensten en dienstverlening, burgers	Gemiddeld tot veel	Hoog	Laag tot gemiddeld
Terroristen	Angst zaaien, politieke doelen	Doelwitten met een hoge impact, ideologisch gemotiveerde doelen	Weinig tot gemiddeld	Laag	Hoog
Hacktivisten	Een gedachtegoed uitdragen	Ideologisch gemotiveerde doelwitten (zeer divers)	Gemiddeld	Gemiddeld	Hoog
Scriptkiddies	Kijken of iets kan, voor de lol	Alle doelwitten	Weinig	Hoog	Gemiddeld
Cyberonderzoekers	Aantonen zwakheden, eigen profilering	Alle doelwitten	Gemiddeld	Laag	Hoog
Interne actor	Wraak, slordigheid, onbekwaamheid	Huidige en/of voormalige werkomgeving	Veel (eenvoudig toegang tot interne resources)	Laag	Laag

fluctueren. Op moment van schrijven gelden de in de tabel genoemde inschattingen.

Onder middelen vallen de capaciteiten en instrumenten waarover een actor beschikt of kan beschikken om een aanval uit te voeren. Dit kan indirect ook een indicator zijn voor de mogelijke impact van een dreiger. Als het gaat om middelen, is het denkbaar dat er interactie tussen actoren plaatsvindt, waarbij de ene groep kennis of kunde inkoopt bij de andere groep.

Het volume is een indicatie van de hoeveelheid van dergelijke aanvallen, waarbij moet worden opgemerkt dat dit een zeer grove indicatie is. Vooral de actoren die baat hebben bij een lage zichtbaarheid, opereren grotendeels onder de radar. Inzicht in aantallen aanvallen is daarom lastig te verkrijgen.

Als laatste is de gewenste zichtbaarheid een factor die deels gekoppeld is aan de intentie van de dreiger. Voor een beperkt aantal actoren is de zichtbaarheid van de aanval een belangrijk aspect voor het plegen van de aanval, terwijl anderen juist buiten de schijnwerpers willen blijven.

2.1 Cyberonderzoekers

Onder 'cyberonderzoekers' worden hier actoren verstaan die op zoek gaan naar kwetsbaarheden en/of inbreken in websites en andere ICT-omgevingen om de zwakke beveiliging ervan aan de kaak te stellen. De groep cyberonderzoekers 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.

Een cyberonderzoeker is een bijzondere actor die vooral gekenmerkt wordt door zijn intentie om de digitale weerbaarheid te vergroten. Zijn handelen is gericht op het veiliger maken van de informatiehuishouding van bedrijven en overheden of de digitale samenleving als geheel. Het handelen van de cyberonderzoeker heeft soms ook indirecte gevolgen die hem typeren als dreiger. Zowel testtools als de bevindingen van zijn onderzoek kunnen hergebruikt worden door groepen met minder goede intenties. Ook kunnen bedrijven door de acties van cyberonderzoekers imagoschade lijden. Cyberonderzoekers zijn zelf soms ook een doelwit. De aanvallers hebben daarbij als doel het verkrijgen van onderzoeksgegevens en informatie over kwetsbaarheden.

Cyberonderzoekers gebruiken de media vaak als middel om hun bevindingen te publiceren en bewustwording rondom cybersecurity te vergroten. Een van de overwegingen om dit zo te doen is het journalistieke recht op bronbescherming.

2.2 Interne actoren

'Interne actoren' zijn individuen zoals interne medewerkers, ingehuurde krachten, ex-medewerkers en personen die om allerlei redenen tijdelijk in een bedrijf aanwezig zijn. Zij kunnen bij kwaadwillende intenties een niet te verwaarlozen dreiging vormen en significante schade veroorzaken.

De incidenten van deze actoren vallen uiteen in malafide acties en fouten of blunders zonder malafide bedoelingen. Volgens de jaarlijkse enquête van Computer Security Institute (CSI)[2] is een significant deel van de schade door cyberincidenten te wijten aan het handelen van interne actoren. Het grootste deel van de respondenten van dit onderzoek zegt dat 20 procent van de schade van alle cyberincidenten is toe te wijzen aan niet-malafide medewerkers en 20 procent aan interne medewerkers met malafide bedoelingen.

Motieven van interne actoren met malafide bedoelingen kunnen onvrede, wraak of frustratie zijn. Interne actoren kunnen ook omgekocht of gechanteerd zijn, tegen hun organisatie gekeerd worden en zich bezighouden met bedrijfsspionage. Ook interne actoren die medewerker van een concurrent zijn, kunnen spionage-activiteiten uitvoeren. Interne actoren kunnen ook doelwit zijn van bijvoorbeeld social engineering en vormen vaak een 'stepping stone' voor de aanval van een organisatie.

2.3 Staten

Onder 'staten' verstaan we in dit verband actoren die onderdeel vormen van de overheid van een bepaald land. Staten kunnen zowel dreiger als doelwit zijn. Als dreiger kunnen zij de intentie hebben om hun geopolitieke of economische positie te verbeteren of om bijvoorbeeld invloed uit te oefenen op dissidenten- of oppositiegroeperingen die zich verzetten tegen het heersende regime. Deze intenties kunnen onder andere gestalte krijgen in de vorm van digitale spionage. De dreiging van digitale spionage in Nederland vanuit vreemde landen is vooral gericht op overheidsinstanties, het bedrijfsleven, de academische sector, dissidenten en oppositionele groeperingen.

In februari en maart 2012 is voor dit onderwerp aandacht geweest in de Tweede Kamer.[3] Volgens antwoorden op Kamervragen houden onder andere Rusland, China en Iran zich met (digitale) spionage tegen Nederland en Nederlandse organisaties bezig en zijn ook andere niet-expliciet genoemde leden actief. In hoofdstuk 3 worden een aantal publiekelijk bekende incidenten genoemd. Niet-publiekelijk beschikbare incidenten worden vanwege hun vertrouwelijkheid niet genoemd.

2. Zie o.a. CSI 2010/2011Computer Crime and Security Survey
3. Zie o.a. http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2012/03/22/antwoorden-kamervragen-over-digitale-spionage-van-china-en-rusland/lp-v-j-0000000736.pdf

2.4 Private organisaties

'Private organisaties' kunnen als organisatie een dreiger zijn of worden als doelwit slachtoffer van andere dreigers. Als doelwit hebben zij last van alle dreigers en hebben zij te maken met bijvoorbeeld hacktivisten die inbreken, gegevens buitmaken, DoS-aanvallen uitvoeren, et cetera. Van staten en andere private organisaties hebben zij te vrezen voor spionage. Voor beroepscriminelen moeten zij op hun hoede zijn, omdat die via gerichte of toevallige uitbuiting van kwetsbaarheden financieel gewin kunnen halen ten laste van het doelwit.

Private organisaties kunnen het internet gebruiken om informatie over hun concurrenten te verkrijgen. De grens tussen legitieme analyse en profilering van de concurrentie, waarbij men binnen de grenzen van de wet blijft, en bedrijfsspionage, waarbij men deze grenzen overtreedt, is in de praktijk niet altijd even duidelijk. De verkregen informatie kan variëren van informatie met een lage gevoeligheid zoals prijslijsten van producten, tot informatie met een hoge gevoeligheid zoals geheime recepten of andere informatie die door het intellectueel eigendomsrecht is beschermd.

Het motief van bedrijfsspionage is meestal financieel van aard en is onder andere gericht op het verbeteren van de concurrentiepositie van het bedrijf. Net als in andere landen hebben ook in Nederland gevestigde multinationals last van bedrijfsspionage, zowel door andere bedrijven als door staten.

Meestal willen slachtoffers van bedrijfsspionage dit buiten de publiciteit houden. Volgens de jaarrapportage van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD)[4] is Nederland een aantrekkelijk doelwit voor spionage, is het bewustzijn rondom de risico's van bedrijfsspionage in Nederland niet overal even hoog en blijven incidenten vaak onopgemerkt. Concrete incidenten zijn door hun vertrouwelijkheid niet te noemen.

2.5 Hacktivisten

'Hacktivisten' zijn personen of groeperingen die vaak gemotiveerd worden door een bepaalde ideologie en die voldoende kennis bezitten om deze motivatie om te zetten in acties die de cybersecurity ondermijnen.

Hacktivisten zijn de afgelopen periode veelvuldig in het nieuws geweest als gevolg van de activiteiten van onder andere Anonymous en LulzSec. Hoewel de kennis en kunde van hacktivisten niet noodzakelijk groot hoeft te zijn, zijn er voldoende tools beschikbaar die een gedreven hobbyist ver kan laten komen. Recente incidenten laten zien dat de effecten van hun daden aanzienlijk zijn[5]. Hacktivisten houden zich vooral bezig met veranderingen van webpagina's, dDoS-aanvallen en hacks gevolgd door het publiceren van de buitgemaakte data.

De idealen van hacktivisten zijn erg divers. Volgens het manifest van Anonymous[6] bijvoorbeeld, ligt ten grondslag aan hun activiteiten het realiseren van een vrije stroom van informatie, vrijheid van meningsuiting en vrijheid van internetactiviteiten. Deze idealen uiten zich bijvoorbeeld in protesten tegen de antipiraterijwet, protesten tegen nieuwe wetten die bijvoorbeeld de bescherming van privacy verslechteren, het oppakken van collega-hackers of, zoals begin 2012, het protest tegen het houden van een sportevenement in een land dat volgens hacktivisten geleid wordt door een twijfelachtig regime (Formule 1 in Bahrein).

Hacktivisten zijn vaak georganiseerd in autonome subgroepen zonder centraal gezag voor de gehele organisatie. Splinterpartijen sluiten zich vaak slechts tijdelijk aan bij grotere organisaties en zijn dan uitsluitend actief voor een bepaald doel en/of een bepaalde actie. Ook bestaat de indruk dat niet-aangesloten hackers hun activiteiten en media-uitingen scharen achter een groep met voldoende bekendheid en media-aandacht. Nederland heeft bijvoorbeeld een Anonymous-subgroep met een eigen manifest[7].

Grotere groepen werken vaak onderling samen om maximaal effect te krijgen bij het bereiken van een bepaald doel. In juni 2011 maakte LulzSec bijvoorbeeld bekend dat ze gingen samenwerken met Anonymous in 'Operation AntiSec' met als doel om zoveel mogelijk overheden en banken aan te vallen.

2.6 Scriptkiddies

'Scriptkiddies' zijn hackers met slechts beperkte kennis die gebruikmaken van technieken en hulpmiddelen die door anderen zijn bedacht en ontwikkeld. Vaak zijn het jongeren met een redelijke, maar niet diepgaande, kennis van informatiebeveiliging. Zij zijn zich meestal nauwelijks bewust van of geïnteresseerd in de gevolgen van hun handelen. Hun motieven zijn vaak baldadigheid en het zoeken van een uitdaging.

In het westen komen scriptkiddies in toenemende mate in aanraking met groeperingen met ideologische of criminele beweegredenen. Hierdoor gaan zij soms het pad op van hacktivist of beroepscrimineel en kan niet meer van scriptkiddies worden gesproken.

4. Zie http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/jaarverslagen/2012/04/19/jaarverslag-aivd-2011/jaarverslag-aivd-2011.pdf
5. Zie bijvoorbeeld www.webvivant.com/feature-hacktivism.html
6. http://www.indybay.org/newsitems/2010/12/09/18666107.php
7. http://www.anonymousnetherlands.nl/manifest

2.7 Beroepscriminelen

'Beroepscriminelen' 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. Denk hierbij bijvoorbeeld aan fraude met internetbankieren.

Landen met een hoge graad van informatisering vormen net als in het verleden belangrijke slachtoffers van beroepscriminelen.

Beroepscriminelen werken steeds vaker samen met zogenaamde 'information brokers'. Door deze partijen in te schakelen, hoeven zij niet zelf op zoek naar bijvoorbeeld kennis over de infrastructuren van bedrijven, maar kunnen ze die op bestelling kopen. De brokers hebben deze informatie in een eerder stadium zelf of via andere hackers verzameld. Ook kant-en-klare informatieverzamelingen zijn op deze manier steeds vaker te koop. Een voorbeeld hiervan is de handel in lijsten met creditcardnummers.

2.8 Terroristen

'Terroristen' kunnen het internet als doelwit of als middel gebruiken. Het gebruik door terroristen van het internet als doelwit moet gezien worden als dreiging, waarover vooralsnog geen concrete incidenten bekend zijn. Jihadisten maken al jaren uitgebreid gebruik van de mogelijkheden die internet biedt voor onder meer propaganda, communicatie en informatievergaring (over bijvoorbeeld aanslagmiddelen). Zij gebruiken het internet zelfs voor expertise-uitwisseling en aanslagplanning.

2.9 Burgers

De burger is vooral kwetsbaar voor digitale dreigingen van beroepscriminelen die met financiële motieven uit zijn op de persoonlijke en financiële gegevens. De dreiging dat door een externe oorzaak hun privacy geschonden wordt, is voor hen zeer relevant. De steeds grotere afhankelijkheid van ICT en het internet van deze groep in combinatie met een laag veiligheidsbewustzijn en beperkte expertise om eigen informatie te beveiligen, heeft tot gevolg dat deze groep zeer kwetsbaar is. Uit een onderzoek van het Centraal Bureau voor de Statistiek (CBS)[8] blijkt bijvoorbeeld dat 95 procent van de respondenten het internet gebruikt en dat vooral het gebruik van mobiel internet het afgelopen jaar sterk is toegenomen (van 36 procent van de respondenten in 2010 tot 50 procent in 2011).

8. Zie http://www.utwente.nl/ctit/cfes/docs/rapporten/2011_11_trendrapport2011.pdf

HOOFDSTUK 3

Dreigingen

Een 'dreiging' is een (indicatie van een) ongewenste gebeurtenis die kan plaatsvinden. De dreiging kan zowel van buiten (bijvoorbeeld van een hacker) als van binnen (bijvoorbeeld van een frauderende medewerker) komen. Als de dreiging werkelijkheid wordt, dan resulteert dat in schade aan waardevolle eigendommen, het openbaren van informatie en/of verstoring van waardevolle processen. Een dreiging wordt pas relevant als sprake is van een kwetsbaarheid voor een belang (asset) en een kwaadwillende de intentie heeft om het belang aan te vallen.

De dreigingen worden beschreven in onderstaande secties en met incidenten geïllustreerd. De eerst drie secties beschrijven dreigingen die doelbewust veroorzaakt worden door de mens (informatiegerelateerde dreigingen, systeemgerelateerde dreigingen en indirecte dreigingen). Daarnaast beschrijft dit hoofdstuk ook dreigingen in de vorm van calamiteiten (zoals brand, waterschade of natuurrampen en falen van hard- en software).

Voor iedere dreiging wordt de relevantie voor een doelwit bepaald. De relevantie is een inschatting door experts en wordt uitgedrukt in hoog, midden en laag. Zie bijlage 1.

3.1 Informatiegerelateerde dreigingen

Informatie, in het bijzonder vertrouwelijke en gevoelige informatie, is waardevol voor verschillende dreigers voor financieel gewin, voor het verbeteren van de eigen positie (status, genot) of om schade toe te brengen aan anderen. Ook het in verkeerde handen vallen en/of openbaar worden van waardevolle informatie vormt een dreiging. Deze paragraaf beschrijft de relevante dreigingen en incidenten met betrekking tot de beveiliging van informatie.

3.1.1 *Publicatie van vertrouwelijke gegevens*

Publicatie van vertrouwelijke (persoons)gegevens over klanten, patiënten of leveranciers is een dreiging voor overheden, private organisaties en burgers. De relevantie van deze dreiging voor de overheid en private organisaties is '**midden**', voor burgers is de relevantie van deze dreiging ook '**midden**'. Het aantal incidenten met uitgelekte gegevens dat door het NCSC is afgehandeld, laat in de periode na 1 juli 2011 een stijgende lijn zien. Bijna een op de vijf (19 procent) van alle door NCSC afgehandelde incidenten betrof uitgelekte gegevens.

Tabel 2. Door NCSC afgehandelde incidenten met uitgelekte gegevens

11Q1	11Q2	11Q3	11Q4	12Q1
3	4	11	8	12

9. ICT-barometer, Ernst & Young, http://ict-barometer.nl/nl/persberichten/54
10. Overview on insider threats van CERT Insider Threat Center (Carnegie Mellon): www.cert.org/archive/pdf/12tn001.pdf

Publicatie van vertrouwelijke gegevens van overheden en private organisaties

In het verleden probeerden 'hacktivisten' veelal door publicatie van vertrouwelijke gegevens van overheden en private organisaties aandacht te krijgen voor hun zaak. Steeds vaker zien we steeds dat 'cyberonderzoekers' en 'scriptkiddies' vertrouwelijke gegevens na een hack publiceren.

Acties van cyberonderzoekers kunnen bijdragen aan een verhoging van de weerstand. Toch wordt het als dreigend ervaren als kwetsbaarheden openbaar worden gemaakt. Als een organisatie niet tijdig een lek dicht, is er de dreiging van publicatie van het lek met alle details op internet. Cyberonderzoekers zijn niet de grootste dreiging. Als zij (met beperkte middelen) eenvoudig toegang krijgen, is er de vraag wie allemaal nog meer toegang heeft (gehad) tot die gegevens.

Casus Lektober

In het kader van 'Lektober' werden in oktober 2011 29 lekken bij bedrijfsleven en overheid openbaar gemaakt. Een van de lekken betrof een lek in vijftig gemeentelijke websites, die gevolgen had voor het veilig kunnen gebruikmaken van DigiD. De actie heeft bijgedragen aan het bewustzijn dat dergelijke kwetsbaarheden vrij eenvoudig uitgebuit kunnen worden en grote consequenties kunnen hebben.

Vanuit kwaadwillende (ex)medewerkers (interne actor) kan een belangrijke dreiging uitgaan. Niet alleen hebben ze vergaande kennis van de processen en beveiligingsmaatregelen van hun organisatie, ook hebben ze vaak uitgebreide autorisaties op systemen voor het uitvoeren van hun dagelijkse werkzaamheden. Incidenten waarbij medewerkers betrokken zijn, komen regelmatig voor: in 2011 gaf 8 procent van de ondervraagde managers aan dat hun bedrijf de voorgaande twaalf maanden was getroffen door diefstal van klantgegevens of bedrijfsinformatie door (ex)werknemers.[9] De omvang van de gevolgen van incidenten waarbij medewerkers betrokken zijn, hangt samen met hun autorisatieniveau en/of status binnen de organisatie. Zo bleek bij een steekproef van incidenten, waarbij medewerkers samenwerkten met de georganiseerde misdaad, dat de schade significant hoger was wanneer medewerkers van het managementniveau bij de criminele handelingen betrokken waren.[10]

Publicatie van vertrouwelijke gegevens van burgers

(Privacygevoelige) gegevens van burgers zijn veelal onderwerp van publicatie zonder dat de burger hier specifiek iets aan kan doen. Illustratief is de hack bij de online gamingdienst 'Sega Pass' eind 2011. Nederlandse gebruikers van deze dienst zijn getroffen doordat inlognamen, e-mail-

adressen en versleutelde wachtwoorden zijn buitgemaakt. Er werden wereldwijd van 1,3 miljoen gamers gegevens gestolen. In andere incidenten werden zeer gevoelige gegevens gepubliceerd, zoals bij het incident met een applicatie voor medische laboratoriumuitslagen[11] in april van 2012.

Burgers hebben maar een beperkte invloed op het opslaan en verwijderen van gegevens die over hen worden opgeslagen. Op vele plekken laten mensen digitale sporen achter. Deels gebeurt dit bewust via social media maar vaak ook onbewust; bij het bezoeken van websites of door het gebruik van mobiele apparatuur wordt surfgedrag bijvoorbeeld vastgelegd. De informatie wordt over vele websites geaggregeerd en gecorreleerd waardoor internetgebruikers in zeer gedetailleerde mate geprofileerd worden. De verzameling van deze profielen is een bron van informatie, soms door de combinatie van vertrouwelijke en gevoelige informatie. Deze profielen worden steeds vaker verhandeld en doorverkocht.

Ook komen er steeds meer apparaten en goederen die sensoren en/of draadloze identificatiechips (RFID) bevatten die signalen uitzenden. Onder andere in paspoorten en ov-chipkaarten zitten zulke RFID-chips. Door op stations en andere drukke punten deze signalen op te vangen, kunnen bewegingen geprofileerd en/of mensen gevolgd worden.

3.1.2 *Digitale (identiteits)fraude*

Een andere informatiegerelateerde dreiging is digitale identiteitsfraude. Een identiteitsfraudeur neemt de identiteit van een ander aan om daarmee financieel of materieel gewin mee te behalen. In dat geval spreken we van financiele identiteitsfraude.[12/13] Financiële identiteitsfraude is een belangrijke dreiging voor private organisaties en burgers. De relevantie van deze dreiging is '**hoog**' voor private organisaties (financiële instellingen). Voor de burger is de dreiging van financiële identiteitsfraude ook zeker aanwezig. Door de goede waarborgen van banken is de relevantie van deze dreiging '**midden**' geclassificeerd.

Het onlinebetalingsverkeer wordt dagelijks bedreigd door beroepscriminelen die, door financiële fraude, schade toebrengen aan zowel de banken als de burgers in Nederland. De totale financiële fraude in het betalingsverkeer in Nederland bedroeg in 2011 ruim 92 miljoen euro. Hiervan is ruim 35 miljoen euro als gevolg van internetbankieren en bijna 39 miljoen als gevolg van skimmingfraude.[14] Het resterende bedrag is als gevolg van creditcardfraude en andere vormen van fraude.
Voor criminelen zijn persoonsgegevens een belangrijk hulpmiddel om financiële identiteitsfraude te kunnen plegen. Zij hanteren verschillende methoden om persoonsgegevens te bemachtigen, zoals het onttrekken van persoonsgegevens aan computers die met malware besmet zijn en het hergebruiken van gegevens uit eerdere datalekken en phishing.

Fraude met internetbankieren

De schade in 2010 door fraude met internetbankieren bedroeg 0,001 procent van het transactievolume. De fraude met internetbankieren is de afgelopen jaren gestegen naar 35 miljoen euro in 2011. De totale schade als gevolg van fraude met internetbankieren is weergegeven in onderstaande tabel. In 2011 zijn er in totaal 7584 schadegevallen geweest.

Tabel 3. Schade als gevolg van fraude met internetbankieren[15/16]

Jaar	Schade door fraude met internetbankieren
2008	€ 2,1 miljoen
2009	€ 1,9 miljoen
2010	€ 9,8 miljoen
2011	€ 35,0 miljoen

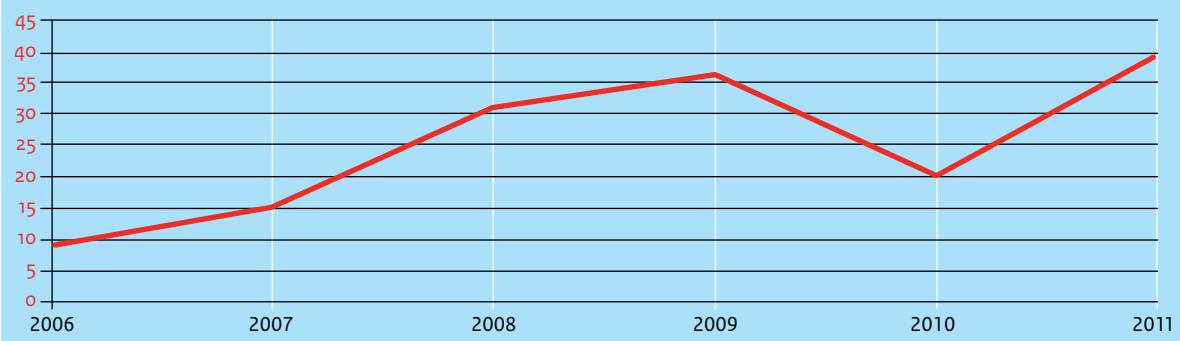
Fraude door skimming van betaalpassen

Nadat in 2010 de schade door skimming (het kopiëren) van betaalpassen was afgenomen, is deze in 2011 weer gestegen. De fraude door skimming steeg van 19,7 miljoen euro in 2010 naar 38,9 miljoen euro in 2011, zie figuur 3. Dit is 0,03 procent van het transactievolume met betaalpassen van 2011 (transactievolume 2011: 138 miljard euro).

De Nederlandse Vereniging van Banken (NVB) gaat ervan uit dat criminelen een laatste, grote aanval hebben uitgevoerd in 2011. Naast de traditionele magneetstrip heeft elke betaalpas in Nederland tegenwoordig een Europay Mastercard Visa (EMV)-chip. Het uitsluitend gebruiken van deze chip maakt het moeilijker om betaalpassen te skimmen. De betaalpassen bevatten naast de EMV-chip ook een magneetstrip, voor gebruik in het buitenland. Deze magneetstrip kan nog steeds worden gekopieerd en misbruikt. Sommige banken hebben aangekondigd de betaalpas standaard te blokkeren voor gebruik buiten Europa.[17] Aanvallers bedenken ook nieuwe aanvalsmethoden op de EMV-chip op de pas. Het blijft daarmee een wedloop tussen criminelen en de financiële instellingen.

11. http://www.medicalfacts.nl/2012/04/19/medische-gegevens-duizenden-brabanders-op-straat-via-diagnostiek-voor-u
12. P. van Schijndel, Identiteitsdiefstal (Den Haag 2008), Bijlage B/figuur 2
13. Een ander motief vormt het plegen van een misdrijf met een gestolen identiteit; de fraudeur leidt het spoor naar de verkeerde persoon. In dat geval spreken we van criminele identiteitsfraude. Deze laatste vorm blijft in deze rapportage buiten beschouwing.
14. http://www.nvb.nl/home-nederlands/nieuws/nieuwsberichten/betalingsverkeer-veilig-ondanks-toename-fraude.html 26 maart 2012
15. Bron: Nederlandse Vereniging van Banken (NVB)
16. http://www.nvb.nl/nieuws/2011-03/q_a_internetbankieren.pdf
17. http://webwereld.nl/nieuws/110409/rabobank-blokkeert-als-eerste-pinpas-buiten-europa.html

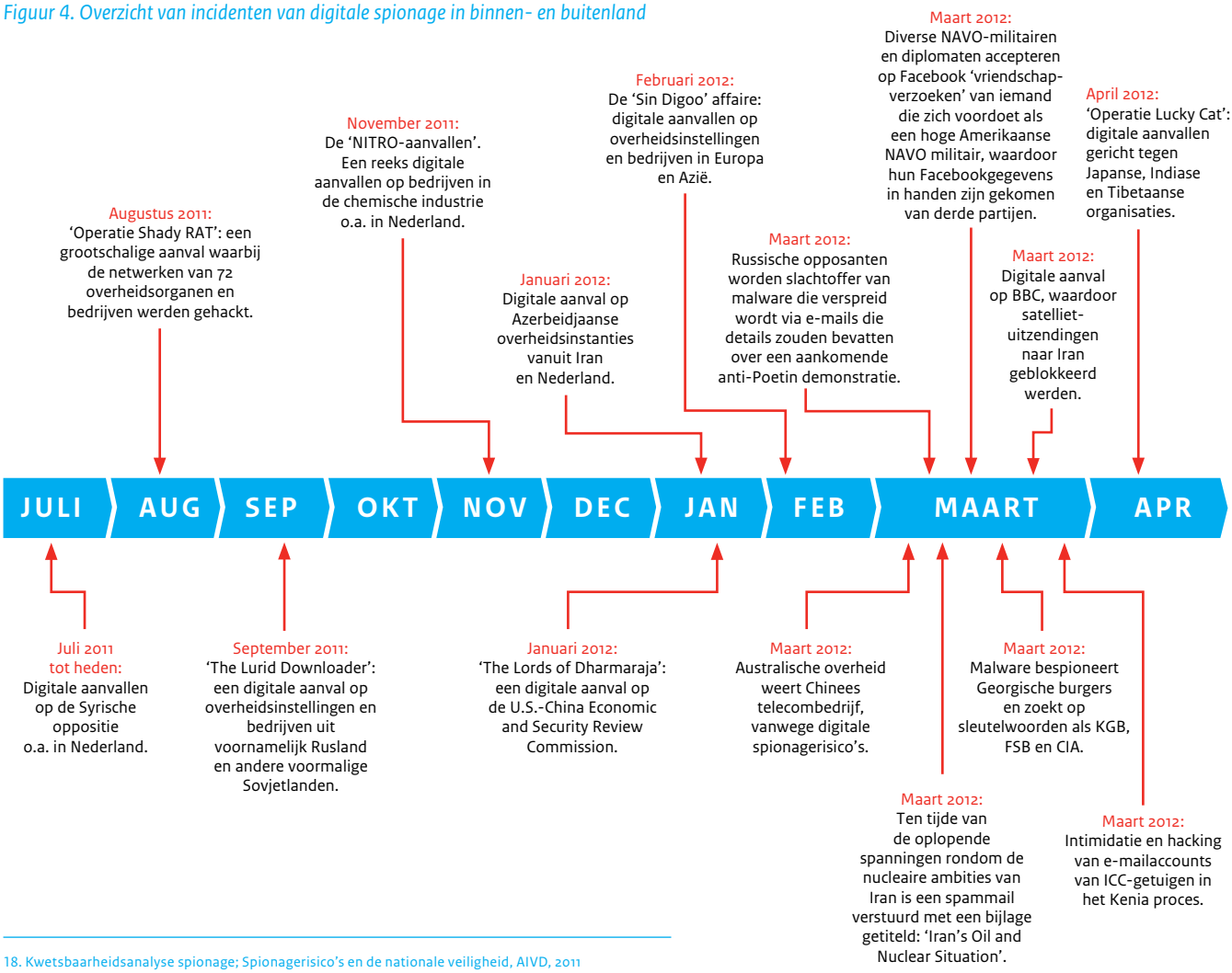
Figuur 3. Schade als gevolg van fraude (skimmen) met bankpassen in miljoenen euro's



3.1.3 *Digitale spionage*

Digitale spionage is gericht op het verkrijgen van vertrouwelijke informatie van bijvoorbeeld economische of politieke waarde, maar kan ook direct geldelijk gewin als doel hebben. Zowel overheden als private organisaties als dissidenten en oppositionele groeperingen zijn potentieel doelwit voor digitale spionage, ook in Nederland. Sinds 2007 wordt door de AIVD melding gemaakt van de concrete dreiging van digitale aanvallen. Meer recent wordt bijvoorbeeld in de Kwetsbaarheidsanalyse Spionage in Nederland (KWAS) van begin 2011, de dreiging van 'digitale aanvallen' als middel voor spionage beschreven.[18] De afgelopen periode is gebleken dat de relevantie van de dreiging van digitale spionage '**hoog**' is voor overheden en '**hoog**' voor private organisaties.

Figuur 4. Overzicht van incidenten van digitale spionage in binnen- en buitenland



18. Kwetsbaarheidsanalyse spionage; Spionagerisico's en de nationale veiligheid, AIVD, 2011

Digitale spionage is een aantrekkelijke vorm van inlichtingenvergaring voor staten, omdat met relatief goedkope middelen een breed scala van doelwitten kan worden aangevallen waarbij het risico op ontdekking klein is. Het gebruik van proxyservers en anonimiseringsdiensten als 'Tor' bemoeilijkt de herkenning en attributie van digitale spionage. De moeilijke attributie maakt een gedegen onderbouwing van het aantal gevallen waarbij een statelijke actor betrokken is bij digitale spionage een precaire zaak.

In figuur 4 op de vorige pagina staan incidenten uit de afgelopen periode. Deze illustreren de omvang, diversiteit en internationale verwevenheid van digitale spionage. Enkele van deze aanvallen tonen gelijkenis op het vlak van gebruikte malware. Dit suggereert dat kwaadwillenden ten minste kennisnemen van elkaars aanvalsmethoden of zelfs gegevens uitwisselen over doelwitten, aanvalstechnieken en/of -instrumenten. Nederland is een elektronisch 'doorvoerland' waardoor er ook spionageactiviteiten plaatsvinden via Nederlandse ICT-infrastructuur.

Digitale spionage gericht op overheden

Er blijft grote interesse in vertrouwelijke overheidsinformatie en aanvallers zijn bereid grote inspanningen te verrichten om een aanval op te zetten en verborgen te houden. Staten zijn hierin de meest voor de hand liggende actoren. Echter, de toewijzing van digitale aanvallen aan specifieke staten is moeilijk vanwege het gebruik van technieken om de herkomst van een aanval af te schermen. Verder worden veel aanvallen uitgevoerd door zogenaamde 'patriottische hackers'. Deze zijn niet of moeilijk te relateren aan overheidsinstanties, waardoor statelijke betrokkenheid te allen tijde valt te ontkennen.

Kwaadwillenden, waaronder andere staten en criminelen, maken veelvuldig gebruik van gerichte aanvallen om systemen binnen overheden te besmetten en op die manier gevoelige informatie te onderscheppen. Een voorbeeld van hoe deze dreiging wordt ervaren is te vinden in Australië.[19] De Australische overheid heeft besloten om een Chinese multinational buiten de deur te houden bij de aanbesteding voor het aanleggen van het nationale glasvezelnetwerk. Dit besluit is gebaseerd op zorgen over denkbare banden met de Chinese overheid en zorgen over cyberaanvallen vanuit China. Er was geen digitale spionage van de marktpartij in kwestie aangetoond. Bescherming van de integriteit en vertrouwelijkheid van het nationale glasvezelnetwerk en de informatie die over het netwerk gaat, staan hier voor Australië voorop.

Digitale spionage gericht op bedrijfsleven

Ook voor private organisaties is digitale spionage een serieuze dreiging. Het zicht op daadwerkelijke incidenten is beperkt, omdat getroffen bedrijven terughoudend zijn met het delen van informatie over dergelijke incidenten. De aard van deze dreiging komt globaal overeen met digitale spionage gericht op overheden. Er worden twee varianten onderkend, spionage direct gericht op intellectueel eigendom van een private organisatie en spionage gericht op informatie over een klant (bijvoorbeeld in geval van de defensie-industrie). In de afgelopen periode zijn vooral aanvallen waargenomen op Nederlandse bedrijven in de defensie-, maritieme, lucht- en ruimtevaart- en (petro)chemische industrie. De casus rondom Duqu-malware illustreert hoe ver sommige actoren willen en/of kunnen gaan om door digitale spionage informatie te verwerven.

Casus

In oktober 2011 is de malware Duqu ontdekt.[20] Vanwege enkele overeenkomsten tussen Duqu en Stuxnet werd Duqu in eerste instantie geïnterpreteerd als dreiging voor ICS/SCADA-systemen. Dit bleek echter onjuist. Duqu malware is ingezet als een gerichte aanval op een beperkt aantal organisaties, met als doel het verzamelen van informatie. Door het beperkt aantal doelwitten is de verspreiding van de malware klein gebleven; zover bekend zijn maar enkele locaties in Europa besmet geraakt. Computers raakten besmet doordat een gebruiker een bijlage van een e-mailbericht, een Word-document, opende dat misbruik maakte van een zero-daylek (TTF lek in win32k.sys) in Windows. Dit lek is inmiddels met een patch verholpen.

Digitale spionage gericht op dissidenten en oppositiegroeperingen

Vooral sinds het uitbreken van de protesten van de 'Groene Beweging' in Iran in 2009 en de 'Arabische Lente' in Syrië in 2011 zijn oppositiegroeperingen uit beide landen regelmatig slachtoffer van digitale aanvallen. Ook in Nederland hebben dergelijke aanvallen plaatsgevonden. Dit blijkt onder andere uit de hack op de in Nederland gevestigde Iraanse oppositiezender 'Radio Zamaneh' in januari 2010 en Facebookpagina's van Syrische oppositiegroeperingen in Nederland in 2011. In beide gevallen bestonden de digitale aanvallen uit 'defacements' van de betreffende sites waarbij de startpagina's werden vervangen door uitingen vóór het geldend regime en dreigementen richting de oppositie. Deze aanvallen zijn geclaimd door respectievelijk 'Iranian Cyber Army' en 'Syrian Electronic Army'. Gezien de strakke overheidscontrole op de internetinfrastructuur in beide landen is het aannemelijk dat zowel de Iraanse als de Syrische autoriteiten weet hebben van deze digitale aanvallen en deze ten minste passief ondersteunen en goedkeuren.

19. http://tweakers.net/nieuws/80885/overheid-australie-boycot-huawei-wegens-chinese-cyberaanvallen.html
20. http://www.govcert.nl/actueel/Nieuws/microsoft-brengt-update-uit-voor-lek-misbruikt-door-duqu-malware.html

3.1.4 *Chantage*

Chantage is een bekend fenomeen, ook in de digitale wereld. In het laatste halfjaar van 2011 en het eerste kwartaal van 2012 is deze dreiging steeds relevanter geworden voor burgers en private organisaties. Vooral door het gebruik van malware genaamd ransomware vindt veelvuldig afpersing plaats. De ransomware waarvoor het Korps Landelijke Politiediensten (KLPD) in maart 2012 waarschuwde, vormt een illustratie hiervan. Via de ransomware werd beweerd dat het KLPD kinderporno op de pc had ontdekt.[21] Er moest eerst 100 euro betaald worden voordat de pc weer zou kunnen worden gebruikt.

Naast ransomware gebruiken criminelen ook meer klassieke instrumenten zoals het dreigen met openbaar maken van vertrouwelijke gevoelige informatie. Een voorbeeld hiervan is de casus van de afpersing van een Belgische kredietverlener.[22]

Het afgelopen halfjaar is er in Nederland een incident bekend geworden waarbij sprake was van het ontvreemden van (digitaal) intellectueel eigendom met de intentie om via chantage financieel gewin te behalen. Niet alleen in Nederland duikt chantage steeds vaker op. Waar vroeger ransomware vooral gebruikt werd in Rusland[23], zien we dat verschillende Europese landen meer last hebben met besmettingen van ransomware. Duitsland heeft bijvoorbeeld 9,6 procent, Frankrijk 4,1 procent besmettingen en Rusland slechts 1,6 procent besmettingen.

De toename van ransomware wordt ook ondersteund door de cijfers van Surfright (zie figuur 5).[24] Uit hun waarnemingen blijkt dat het percentage ransomware van het totaal aan malware vanaf april 2012 snel is toegenomen van minder dan 1% naar meer dan 5%.

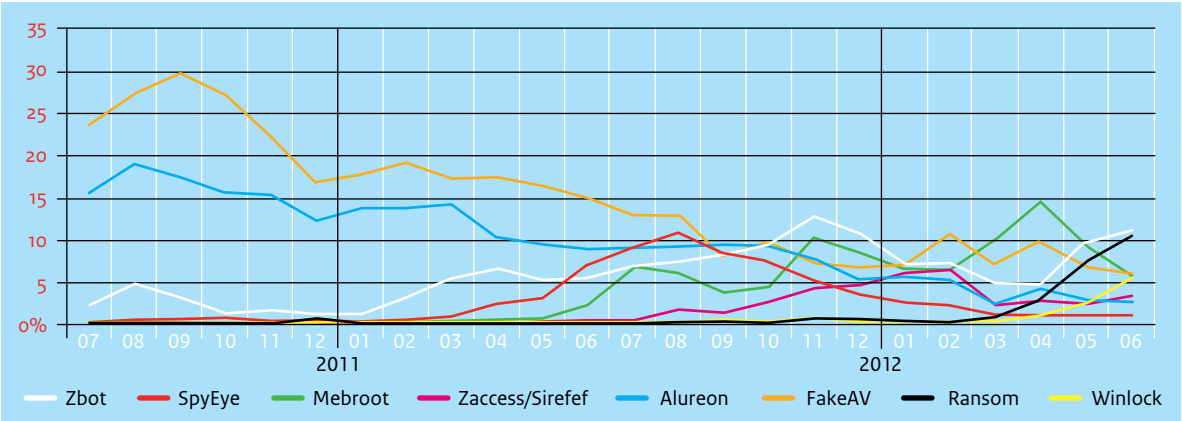
3.2 Terroristische cyberdreiging

Jihadisten maken al jaren uitgebreid gebruik van de mogelijkheden die internet biedt voor onder meer propaganda, communicatie en informatievergaring (over bijvoorbeeld aanslagmiddelen). Zij gebruiken het internet zelfs voor expertise-uitwisseling en aanslagplanning. De functies die het internet vervult voor jihadisten zijn in meer detail beschreven in de door de AIVD uitgebrachte publicatie 'Het jihadistisch internet. Kraamkamer van de hedendaagse jihad'.

Het offensieve gebruik van digitale middelen door jihadisten staat echter nog in de kinderschoenen. Tot op heden zijn slechts beperkte concrete intenties en nauwelijks capaciteiten onderkend tot het doen van Computer Network Exploitation (CNE) en Computer Network Attack (CNA). Wel wordt door jihadisten gefilosofeerd over de mogelijkheden van grootschalige cyberaanvallen en wordt gepoogd technische kennis te bundelen. De nu aanwezige technische kennis is echter niet toereikend voor de uitvoer van de besproken typen aanvallen. Binnen cyberspace is vanuit jihadistische terroristen op dit moment nog geen serieuze aanslagdreiging waargenomen.

Een belangrijke reden is dat jihadisten vooralsnog niet de capaciteiten bezitten die nodig zijn voor dergelijke aanvallen, noch lijken zij op dit moment bereid de benodigde investeringen te doen om deze op te bouwen. De mogelijkheden om fysieke/digitale vitale infrastructuur aan te tasten met digitale middelen is met Stuxnet weliswaar bewezen, maar ligt nog ver buiten het bereik van jihadistische organisaties. De ontwikkeling van een Stuxnet-achtig middel (geschikt om een fysieke impact te kunnen veroorzaken) vergt significante expertise, diverse verschillende specialismen en een behoorlijke ontwikkeltijd.

Figuur 5. Percentage malware per type over periode juli 2010 t/m juni 2012



21. http://www.politie.nl/klpd/nieuws/120316klpdwaarschuwt.asp
22. http://nos.nl/artikel/368857-hackers-chanteren-belgische-bank.html
23. Trend Micro™ Smart Protection Network™ (feedback taken in februari 2012)
24. http://www.surfright.nl/en/hitmanpro/prevalence/april-2012

Het huidige gebrek aan capaciteiten kan natuurlijk veranderen als begaafde hackers zich aansluiten bij terroristen. Zelfs dan zijn de mogelijkheden niet onbeperkt. Hoewel een individuele hacker zeker chaos, overlast en financiële schade kan veroorzaken, is het veroorzaken van maatschappelijke ontwrichting met digitale middelen een complexe operatie. Een Stuxnet-achtig virus, dat een ramp in de fysieke wereld kan veroorzaken, is iets dat meer capaciteiten vergt dan een individuele hacker in huis heeft.

Een tweede mogelijkheid waarmee terroristen hun potentie kunnen verhogen, is als ze erin slagen de expertise extern in te huren bij cybercriminelen. Er zijn tot op heden echter geen signalen dat terroristen dit nasterven. Mogelijk omdat zij de investeringen, afgezet tegen de verwachte impact van een digitale aanval, te hoog vinden. Daarnaast brengt externe inhuur extra risico's op onderkenning door de autoriteiten met zich mee.

Voor een terroristisch streven angst te zaaien en zo de maatschappij te ontwrichten, is een digitale aanval op dit moment mogelijk minder geschikt en minder kostenefficiënt dan een 'traditionele fysieke' aanslag. Daarnaast hebben jihadisten in het verleden bewezen in principe wel over voldoende capaciteiten beschikken om een traditionele aanslag te plegen, terwijl ze de capaciteiten voor een digitale aanslag alsnog lijken te ontberen.

De enige concrete voorbeelden van cyberactiviteit uit de jihadistische hoek zijn defacings van websites. Deze defacings waren relatief eenvoudig uit te voeren; de getroffen websites blonken meestal niet uit qua beveiliging. Kortom: hoewel digitale aanvallen zeer effectief kunnen zijn in het ontregelen van een organisatie, of zelfs van een land als ze op zeer grote schaal worden toegepast, worden dergelijke acties momenteel niet verwacht van jihadistische terroristen.

3.3 Opbouw cyberoffensieve capaciteiten van staten

Het Nederlandse defensieapparaat is door intensief gebruik van hoogwaardige systemen voor uiteenlopende doeleinden afhankelijk van betrouwbare interne en externe netwerken en digitale technologie. Hierdoor kan Defensie kwetsbaar zijn voor digitale aanvallen en moet het ministerie zich daar afdoende tegen verdedigen.

In een militair conflict vormen statelijke actoren een belangrijke dreiging in de vorm van offensieve cybercapaciteiten. Meerdere landen beschikken al over zulke capaciteiten, andere ontwikkelen ze momenteel. Iran is een voorbeeld in dit verband. De aspiraties van de Iraanse krijgsmacht omvatten - naar eigen zeggen - ook het vermogen tot digitale oorlogvoering. Ook de capaciteiten van niet-statelijke actoren tot technologische ontregeling vormen een dreiging voor Defensie. Op de middellange termijn vormen uiteenlopende actoren met hoogwaardige digitale offensieve capaciteiten de grootste dreiging tegen Defensie. Hierbij moet worden gedacht aan aanvallen die gericht zijn op een specifiek militair doel en die de handelingsvrijheid van de krijgsmacht daarmee ernstig kunnen beperken. Een andere bedreiging voor de krijgsmacht is het gebrek aan kennis over en inzicht in de mogelijkheden voor digitale aanvallen.

In de praktijk krijgen krijgsmachten en de met de krijgsmacht samenwerkende technologische industrie voortdurend pogingen tot digitale inbraak te verduren. De strategische en economische waarde van informatie in deze sector is groot, waardoor organisaties bij uitstek blootstaan aan digitale spionage. Zo hebben in de afgelopen jaren verschillende gerenommeerde Amerikaanse defense contractors naar buiten moeten brengen dat er bij digitale inbraken intellectueel eigendom was buitgemaakt. Ook zullen krijgsmachten alert moeten zijn op het heimelijk en opzettelijk toevoegen van kwetsbaarheden aan ICT-producten die voor defensiedoeleinden worden gebruikt. Gelet op de mate waarin het militair optreden afhankelijk is van ICT-middelen, is dit een reële dreiging. Inlichtingendiensten zullen het vooraf manipuleren van aan potentiële opponenten te leveren apparatuur niet schuwen. De complexiteit van en verscheidenheid aan componenten in systemen maakt dit in toenemende mate een risico.

3.4 Systeemgerelateerde dreigingen

Onder systeemgerelateerde dreigingen worden dreigingen verstaan die gericht zijn op verstoring van de beschikbaarheid of uitvoering van een dienst of de werking van een organisatie. Dit kan tot gevolg hebben dat de dienst onbereikbaar gemaakt wordt of gesaboteerd wordt en langdurig buiten werking is of andere, onbedoelde acties gaat uitvoeren. Deze paragraaf beschrijft de relevante dreigingen voor (digitale) verstoring van systemen binnen de vitale infrastructuur en systemen van (online)dienstverlening.

3.4.1 Verstoring van vitale infrastructuur

In het Cybersecuritybeeld van december 2011 is beschreven dat verstoring van ICS/SCADA-systemen een relevante dreiging is. Ten opzichte de vorige periode moeten we vaststellen dat deze dreigingen reëler geworden zijn. Hiervoor zijn twee ontwikkelingen relevant:

- cyberonderzoekers tonen toenemende belangstelling voor de beveiligingsproblemen van ICS/SCADA-systemen, mede ingegeven door de wens aandacht te vestigen op deze problemen.
- hacktivisten lijken op zoek naar kennis over ICS/SCADA en beveiliging daarvan.

In oktober verscheen er een vertrouwelijk document op het internet dat door het Department of Homeland Security van de Verenigde Staten is opgesteld. Dit document, 'Assessment of Anonymous Threat to Control Systems', analyseert aanwijzigen dat de hacktivistische groepering Anonymous een toenemende interesse toont in ICS/SCADA.

In januari, na de start van het NCSC, vroegen meerdere cyberonderzoekers aandacht voor de soms gebrekkige beveiliging van ICS/SCADA-systemen. De meeste meldingen werden niet direct gedaan aan het NCSC of de media, maar gedaan via openbare kanalen als Twitter of Pastebin.com. Bij een aantal van deze meldingen heeft het NCSC bemiddeld tussen de cyberonderzoeker en de betreffende organisatie. Ook heeft het NCSC twee publicaties[25/26] verspreid met informatie over beveiligingsproblemen van ICS/SCADA-systemen.

Een van de meldingen betrof de bediening van een aantal pompen van de riolering van de gemeente Veere. Deze kwetsbaarheid ontstond door een slechte beveiliging van netwerkverbindingen, gecombineerd met eenvoudig te raden inloggegevens. In het televisieprogramma waar deze melding werd gedaan, werd gesuggereerd dat alle gemalen en sluizen gevaar lopen en dat grote delen van het land ongemerkt onder water kunnen worden gezet. Hoewel het misbruiken van deze toegangsmogelijkheid tot schade en overlast had kunnen leiden, was een dergelijk scenario niet mogelijk. Ook bij andere meldingen werd het risico door de meldende partij soms te hoog geschat. Omdat ICS/SCADA-systemen lang niet in alle gevallen onderdeel zijn van de vitale infrastructuur en daarnaast vaak aanvullende maatregelen worden getroffen om ongewenste procesbeïnvloeding te voorkomen of te detecteren, is het voor een buitenstaander niet eenvoudig om een correcte inschatting van de ernst van een kwetsbaarheid te maken.

In januari 2012 vond de specialistische S4-conferentie over de beveiliging van ICS/SCADA-systemen plaats. Op deze conferentie bespraken cyberonderzoekers kwetsbaarheden in ICS/SCADA-systemen. Naar aanleiding van deze bijeenkomst worden regelmatig Metasploit[27]-modules gepubliceerd waarmee de beveiliging van een scala aan ICS/SCADA-systemen kan worden getest. Deze informatie kan ook door kwaadwillenden worden gebruikt om kwetsbaarheden van dergelijke systemen te misbruiken.

3.4.2 *Verstoring door sabotage*

Sabotage van systemen is een klassieke wijze van het verstoren van processen en organisaties. Doelbewust worden systemen vernield om zo veel mogelijk schade aan te richten. Sabotage wordt veelal genoemd in relatie met terroristen, vanwege ideële overwegingen. Toch komt sabotage vaker voor in de vorm van wraak of baldadigheid. De gefrustreerde interne (ex)medewerker is een actor die deze dreiging uitoefent. De casus van 'Shionogi' illustreert deze dreiging.

Casus Shionogi
Een ontslagen medewerker bij het farmaceutische bedrijf Shionogi heeft zijn niet- ingetrokken toegangsrechten gebruikt om grote schade aan te richten. Na zijn ontslag heeft hij via het draadloze netwerk van een fastfoodrestaurant ingelogd op de beheeromgeving van de virtuele servers van zijn vorige werkgever, waarna hij 88 virtuele servers verwijderd heeft. De dader is veroordeeld tot 41 maanden gevangenisstraf en het vergoeden van ruim $ 800.000 schade.[28]

3.4.3 *Verstoring van (online)dienstverlening*

Onlinedienstverlening speelt een belangrijk rol in het economisch verkeer. Verstoring van deze dienstverlening is een relevante (**'midden'**)**dreiging** voor overheden en private organisaties. Bekend zijn de dDos-aanvallen op websites waardoor deze niet meer gebruikt kunnen worden. Daarnaast zijn websites die veel bezoekers trekken een aantrekkelijk doelwit om malafide inhoud te verspreiden (zie casus NU.nl). Criminelen richten zich bewust op populaire websites om zo in zeer korte tijd een groot aantal computers te besmetten. Bij een geslaagde aanval worden deze websites of organisaties gebruikt om bezoekers te besmetten. Daarmee treffen zij gelijktijdig (het vertrouwen in) online-dienstverlening. Veelal betekent dit dat de website tijdelijk buiten werking is en dienstverlening niet mogelijk is.

Voor dit soort gebeurtenissen bestaat geen meldplicht. Ook is de eigenaar van de betrokken website in veel gevallen niet verplicht bezoekers in te lichten over het feit dat zij hebben blootgestaan aan een mogelijke besmetting. Het is dan ook geheel afhankelijk van het verantwoordelijkheidsgevoel van de betrokken website-eigenaar of de bezoeker adequate maatregelen kan treffen.

25. NCSC factsheet FS2012-01 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/beveiligingsrisicos.html
26. Checklijst beveiliging van ICS/SCADA systemen https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/checklist-beveiliging-van-ics-scada-systemen.html
27. Metasploit is een softwarepakket waarmee beveiligingstesten kunnen worden uitgevoerd
28. www.justice.gov/usao/nj/Press/files/Cornish, Jason Sentencing News Release.html

Casus NU.nl
Hackers zijn er op 14 maart 2012 in geslaagd om een kwaadaardige code op de populaire nieuwswebsite NU.nl te plaatsen. Dit gebeurde nadat inloggegevens van het contentmanagementsysteem (CMS) van een van de medewerkers van NU.nl in verkeerde handen raakten.[29] Het doel van de aanval was om bezoekers van de website te besmetten met malware. Onderzoek heeft uitgewezen dat naar schatting 100.000 systemen zijn getroffen.[30] Deze aanvalstactiek staat bekend als een drive-by-download en is niet nieuw. Het is wel uitzonderlijk dat een van de best bezochte Nederlandse websites van een dergelijke aanval onderdeel uit-maakt.[31] Op systemen van de slachtoffers werd Sinowal banking-malware geïnstalleerd. Deze malware is er onder andere op gericht om banktransacties te manipuleren en inloggegevens voor websites te onderscheppen.

Casus KPN/Certificaten
De DigiNotar-crisis heeft het bewustzijn van de afhankelijkheid van cybersecurity van een derde partij vergroot. Organisaties zijn alerter en analyseren hun afhankelijkheden nauwkeuriger. Deze alertheid wordt getoond door een incident bij KPN in november 2011. KPN, een van de vier providers van PKI-overheidscertificaten, staakte uit voorzorg tijdelijk de uitgifte van veiligheidscertificaten. Het vermoeden bestond dat een van de webservers mogelijk gehackt was. Tijdens een intern onderzoek ontdekte KPN een aantal logfiles waaruit bleek dat vier jaar eerder de webserver van KPN gecompromitteerd was. KPN heeft zijn infrastructuur voor het uitgeven en ondertekenen van veiligheidscertificaten weer online gebracht, nadat een onafhankelijke beoordelaar geen onvolkomenheden meer heeft gevonden. Het incident bleek voor KPN en haar klanten geen directe gevolgen te hebben.

3.5 Indirecte dreigingen

Iedereen die gebruikmaakt van ICT is voor een groot deel afhankelijk van de producten en diensten van derde partijen. Daarbij kan het om producenten van applicaties of hardwarecomponenten gaan of om partijen die hard- en software hosten voor de organisatie. Aanvallen op die derde partijen kunnen een grote impact hebben op de beschikbaarheid, vertrouwelijkheid of integriteit van de eigen dienstverlening en informatie.

3.5.1 *(Digitale) verstoring van bedrijfsvoering door aanval bij een derde partij*

Een aanval op een derde partij waarvan de eigen organisatie afhankelijk is, kan leiden tot grote gevolgen voor de eigen bedrijfsvoering. Dit kan daarbij de organisatie overstijgen, waardoor een sector of, in het geval van DigiNotar, het eigen land wordt getroffen.

Afhankelijkheid van derde partijen voor (primaire) bedrijfsvoering wordt steeds groter, mede door ketenafhankelijkheid (en kennis over de keten), vervlechting, complexiteit en outsourcing van bedrijfsprocessen en systemen. Hierdoor is de organisatie net zo kwetsbaar voor een dreiging als haar toeleverancier (derde partij). De dreiging kan voortkomen uit een aanval op de eigen gegevens (bij de derde partij), door een aanval op gegevens van anderen - waardoor wel schade aan eigen gegevens ontstaat - of door de aantrekkelijkheid van grote verzameling van gegevens bij de derde partij. In vergelijking met andere dreigingen is de relevantie van deze dreiging '**laag**' voor zowel overheden als private organisaties. De casus van KPN, waarbij uit voorzorg de uitgifte van certificaten is gestaakt, illustreert deze dreiging (zie kader). Indien gebruikgemaakt wordt van door KPN uitgegeven certificaten, is een organisatie kwetsbaar voor een dreiging die zich bij KPN manifesteert.

3.5.2 *Verstoring door malwarebesmetting en spam*

Verstoring van de bedrijfsvoering als gevolg van een malwarebesmetting en spam vormen een belangrijke dreiging voor overheid, bedrijfsleven en burgers. Het schoonmaken van het netwerk kan kostbaar zijn, zowel in directe kosten voor het schoonmaken als in indirecte kosten als gevolg van verloren productiviteit. Daarom is de relevantie van deze dreiging '**hoog**' voor overheid, private organisaties en burgers.

Het gaat specifiek om besmettingen door 'ongerichte' malware, dat wil zeggen malware die zichzelf ongeremd verspreidt met als doel zoveel mogelijk systemen te besmetten en deze op te nemen in een botnet. Het doel is vaak niet de besmetting op zich, het doel is het creëren van een kwetsbaarheid die voor andere doeleinden gebruikt kan worden en/of het door spam en malware besmetten van andere systemen. Een omvangrijke malwarebesmetting kan (delen van) een bedrijfsnetwerk uitschakelen.

Het NCSC monitort mogelijke malwarebesmettingen. In 2011 en het eerste kwartaal van 2012 waren 2.400 meldingen die betrekking hadden op organisaties die tot de doelgroep van het NCSC behoren. Deze 2.400 meldingen hebben uiteindelijk geresulteerd in 47 incidenten waarbij het NCSC bijstand heeft geleverd.

De meeste van deze 47 incidenten betroffen malware-infecties gerelateerd aan de Conficker en de Zeus-trojan.

29. http://www.nu.nl/media/2763447/korte-tijd-malware-verspreid-via-nunl.html
30. http://blog.fox-it.com/2012/03/16/post-mortem-report-on-the-sinowallnu-nl-incident
31. http://www.alexa.com/topsites/countries/NL

Ook zijn een aantal infecties van de SpyEye-trojan waargenomen. De infecties liepen uiteen van infecties op systemen van de organisatie tot infecties op publieke wifi-netwerken. Dat veel malware-infecties nog steeds afkomstig zijn van Conficker (Conficker dateert uit 2008) laat zien dat veel organisaties beperkt software-updates installeren en dat virusscanners geïnstalleerd zijn.

Spam is veelal een resultaat van malwarebesmettingen en komt in Nederland relatief vaak voor in vergelijking met andere Europese landen.[32] In Nederland verwerkt OPTA de klachten over spam. Via Spamklacht.nl zijn in 2011 27.371 klachten binnengekomen over spam, waarvan het grootste gedeelte betrekking had op spam via de e-mail (24.337 klachten).[33] Voor e-mail betekent dit een toename van ongeveer 7 procent ten opzichte van 2010.[34] Er zijn alleen kleine verschuivingen waar te nemen in de soort spam waarover is geklaagd. In 2011 zijn twee boetes opgelegd voor het versturen van spam, met een totale boetehoogte van € 880.000. Daarnaast zijn tientallen waarschuwingen verstuurd.

In 2011 is een rapport gepubliceerd dat het perspectief van burgers op besmetting door malware onderzocht, met specifieke aandacht voor malware die het doelwit lid maakt van een botnet.[35] 5 tot 10 procent van de Nederlandse huishoudens heeft in 2009 en 2010 ten minste een computer gehad die lid was van een botnet, aldus een voorzichtige schatting uit dit rapport. Uit waarneming van SurfRight (zie figuur 6)[36] ligt het aantal besmette pc's hoger. Het percentage besmette pc's schommelt rond de 30% over een periode van twee jaar. Deze waarneming en het voorgaande onderzoek zijn moeilijk te vergelijken omdat ze op een andere manier meten.

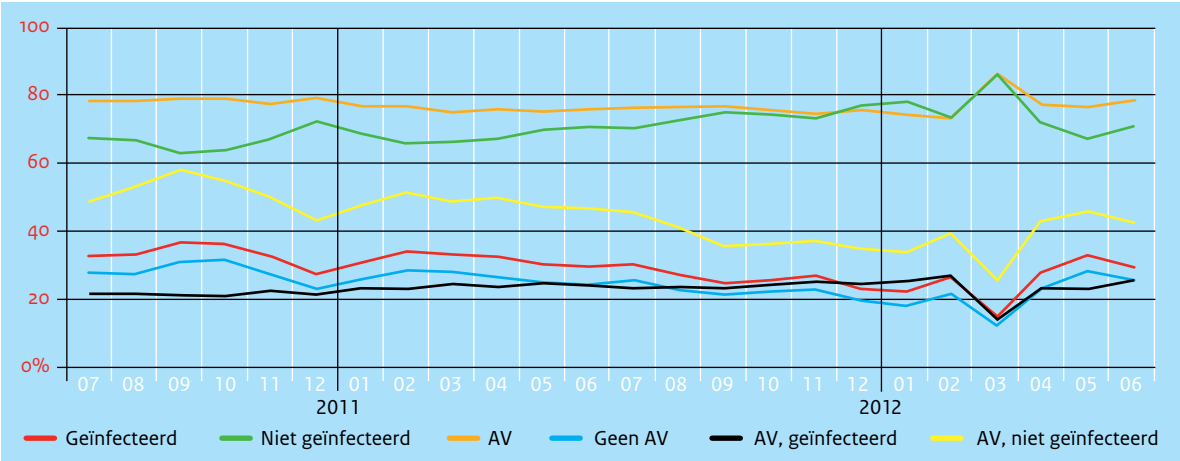
3.5.3 *Hoax als dreiging*

Een 'hoax' is een vals gerucht en/of een nepwaarschuwing. Denk daarbij onder andere aan valse boodschappen in e-mails of social media die de lezer aansporen om zoveel mogelijk mensen te informeren. Hoaxes bestaan al heel lang maar hebben de laatste tijd weer meer aandacht gekregen als gevolg van een aantal incidenten.[37] In mei 2012 is melding gemaakt dat 50.000 usernames en passwords van Twitter op Pastebin.com waren gepubliceerd. De intentie van dergelijke berichten lijkt vooral te maken te hebben met sensatiezucht, erkenning en het willen opblazen van incidenten. Een hoax kan grote gevolgen hebben (zie kader casus KPN), daarom is de relevantie van deze dreiging 'midden' voor zowel overheid als private organisaties.

Vaak hebben hoaxes een redelijk onschuldige karakter. 'Whatsapp' werd bijvoorbeeld in april 2012 getroffen door een nepmelding dat gebruikers inactief werden als ze het bericht niet naar iedereen in hun adresboek verstuurden.[38] Soms worden gebruikers opgeroepen tot een handeling waar ze zelf ook last van kunnen hebben. Een voorbeeld is de waarschuwing van april 2012 die op Facebook circuleert om de sociale webbrowser RockMelt te verwijderen omdat dit een virus zou zijn.[39]

Er zijn diverse websites die informatie geven over hoaxen zoals http://www.virusalert.nl en http://www.hoax-slayer.com.

Figuur 6. Infectiegraad Nederlandse pc's over periode juli 2010 t/m juni 2012



32. Eurostat in Centraal Bureau voor de Statistiek, rapport: ICT, Kennis en Economie
33. OPTA Jaarverslag 2011
34. OPTA Jaarverslag 2010 en 2011
35. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html
36. http://www.surfright.nl
37. http://security.onestopclick.com/technology_news/twitter-hack-a-hoax_202.htm
38. http://www.hoax-slayer.com/whatsapp-servers-full-hoax.shtml
39. http://www.hoax-slayer.com/rockmelt-virus-warning-hoax.shtml

Casus KPN/Babydump
Nadat aanvallers zich toegang verschaften tot de systemen van KPN in november 2011, circuleerde in februari 2012 een valse claim dat bij de hack van KPN inloggegevens van e-mailboxen waren gelekt. Omdat er op de website Pastebin.com ook daadwerkelijk de gegevens van ruim vijfhonderd mensen met een KPN e-mailaccount waren gezet, leek deze claim echt. Dit leidde ertoe dat KPN 24 uur de toegang tot inkomende e-mail van twee miljoen klanten heeft blokkeerde.[40] Ook zijn deze klanten opgeroepen om het wachtwoord van hun e-mailaccount aan te passen. Meer dan duizend klanten hebben bij KPN melding gemaakt van geleden schade als gevolg van het buiten werking stellen van inkomende e-mail.[41] Uiteindelijk bleken de klantgegevens te zijn buitgemaakt via een lek bij een andere website Babydump.nl.[42]
Ook bij Ziggo is er een valse claim geweest dat er inloggegevens zijn gelekt. Hierbij is tijdig ontdekt dat de klantgegevens onjuist waren.[43]

3.6 Calamiteiten en rampen

Door allerlei afhankelijkheden in een keten van informatiesystemen kan een, op het eerste gezicht, kleine verstoring uitgroeien tot grote overlast. Niet altijd worden deze verstoringen veroorzaakt door moedwillig handelen. Brand, waterschade, natuurrampen of het niet goed functioneren van software of het ontbreken van hardware kan grote gevolgen hebben.

3.6.1 Verstoring van bedrijfsvoering als gevolg van brand, waterschade of natuurrampen

Gezien het belang van digitale dienstverlening aan burgers, overheid en bedrijfsleven zijn veerkracht en weerbaarheid tegen verstoringen vereisten voor organisaties die deze dienstverlening leveren. De relevantie van deze dreiging is '**midden**' voor overheid en private organisaties, vooral voor bedrijven uit de vitale sectoren. Iedereen vertrouwt op continuïteit van diensten. Snel herstel in geval van een verstoring is cruciaal. Toch blijkt continuïteit niet altijd eenvoudig te realiseren. Er moet zowel aandacht zijn voor preventie als voor het voorbereiden van het herstellen na een calamiteit. Continuïteitsmanagement is een onderwerp op de agenda van steeds meer organisaties. De casus van Vodafone illustreert het belang van goed voorbereid zijn op calamiteiten.

Casus Vodafone
Een brand in een bedrijfspand naast een pand van Vodafone met netwerkapparatuur zorgde ervoor dat de airconditioning van Vodafone uitviel. Hierdoor raakte de netwerkapparatuur oververhit en functioneerde niet meer goed. Als gevolg hiervan konden miljoenen mensen op 4 april 2012 in de Randstad niet meer mobiel bellen, sms-en of internetten. Onder de getroffenen bevond zich ook de Rijksoverheid die voor mobiel bellen voor het grootste deel van Vodafone afhankelijk is. Ook 'MachinetoMachine'-communicatie werd getroffen zoals 'TomTom Live' en meetstations van het KNMI.

3.6.2 Verstoring van de bedrijfsvoering als gevolg van falen van hardware en/of software

Ondanks zorgvuldig en professioneel beheersen van ICT-software en -hardware en ondanks aandacht voor preventieve maatregelen, zijn incidenten en verstoringen niet te voorkomen. De complexiteit van het samenspel van hardware- en softwarecomponenten maakt het overzicht voor een gemiddelde beheerder moeilijk. Software-updates en vervanging van hardware zijn kwetsbare momenten in de beheersprocessen van een organisatie (zie kader casus NS). Zorgvuldig testen en het hebben van fallbackscenario's, in combinatie met het structureel en uitgebreid testen van uitwijkprocedures, vraagt om 'business continuity planning'. Verstoringen als gevolg van falen van hardware en software zijn een relevante dreiging ('midden') voor overheid en private organisaties.

Casus NS
Op 22 maart heeft de verkeersleiding van de NS besloten het treinverkeer stil te leggen nadat zij geen zicht meer hadden op de treinenloop als gevolg van een serie gerelateerde ICT-storingen. De storingen traden op na het starten van een uitwijkprocedure als gevolg van de ontdekking van een defect hardwarecomponent. Hoewel de verkeersleidingsystemen meervoudig redundant zijn uitgevoerd, bleek de automatische schakeling tussen deze systemen niet goed te werken. Op het moment dat werd overgeschakeld naar een ander systeem, werkte de software niet doordat een onderdeel ontbrak. Dit probleem had uiteindelijk grote gevolgen voor het treinverkeer.

40. http://forum.kpn.com/t5/News-stream/Update-digitale-inbraak/ba-p/16889
41. http://forum.kpn.com/t5/News-stream/KPN-mail-722-000-wachtwoorden-gereset/ba-p/20397
42. http://tweakers.net/nieuws/79953/mailgegevens-kpn-klanten-kwamen-uit-baby-dump-database.html
43. http://www.security.nl/artikel/40802/1/ZIGGO_gehackt.html

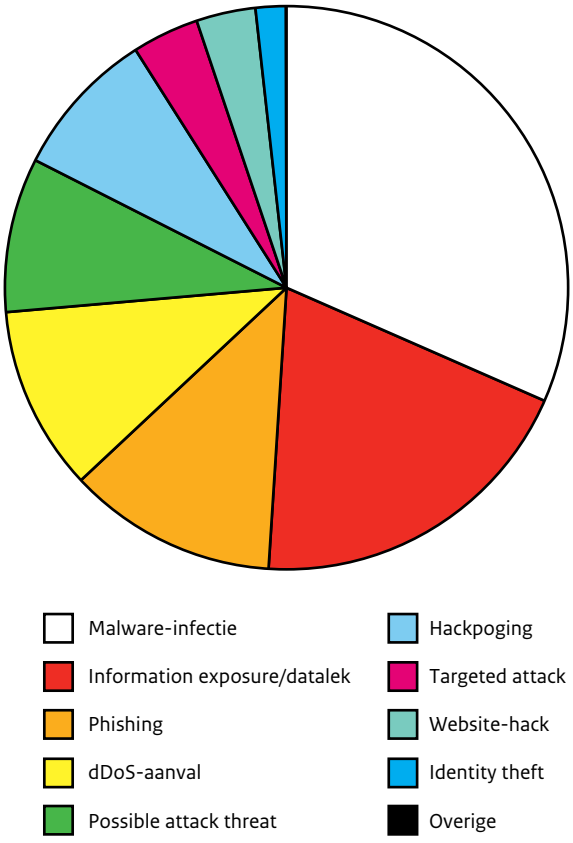
Tabel 4. Aantallen door NCSC afgehandelde dreigingen en incidenten binnen overheden

Type	11Q2 + 11Q3	11Q4 + 12Q1	Percentage 11Q2 + 11Q3	Percentage 11Q4 + 12Q1
Malware-infectie	39	18	57%	30%
Information exposure/datalek	6	11	9%	19%
Phishing	5	7	7%	12%
dDoS-aanval	2	6	3%	11%
Possible attack threat	5	5	7%	9%
Hackpoging	1	5	1%	9%
Targeted attack	3	2	4%	4%
Website-hack	1	2	1%	4%
Identity theft	3	1	7%	2%
Overige	3	-	4%	0%
Totaal	68	57	100%	100%

3.7 Door NCSC afgehandelde dreigingen en incidenten

Door NCSC zijn in de afgelopen twee kwartalen 57 incidenten afgehandeld bij overheden.[44] Hoewel dit minder is dan in het halfjaar daarvoor, is nog niet te stellen dat het aantal incidenten structureel afneemt. Op basis van de gegevens in tabel 4 en figuur 7 kan een analyse worden gemaakt van dreigingen en aanvallen binnen uitsluitend overheden.
Hieruit blijkt dat malware-infecties het grootste deel van de incidenten uitmaken in de periode sinds oktober 2011, hoewel het aantal hiervan gedaald is ten opzichte van het halfjaar daarvoor. Het uitlekken van informatie maakt daarentegen een groter deel uit van de incidenten, met een percentage van 19%. Het aantal dDoS-aanvallen is gestegen ten opzichte van de periode ervoor.

Figuur 7. Verdeling door NCSC afgehandelde dreigingen en incidenten binnen overheden, 11Q4 + 12Q1



44. NCSC bedient ook private sectoren, maar tot 1 januari 2012 bediende GOVCERT.NL primair overheden. Voor de vergelijkbaarheid is deze analyse daarom beperkt tot de overheid.

3.8 Dreigingsoverzicht

3.8.1 *Inschatting*

Op basis van de gepresenteerde actoren in hoofdstuk 2 en de relevante dreigingen zoals beschreven in dit hoofdstuk, is een overzicht van de relevantie gemaakt. In onderstaande tabel leest men af welke dreigingen uitgaan van een actor en hoe relevant deze is voor de doelwitten overheid, private organisatie en burgers. Deze inschatting is een expertmening van verschillende experts van het NCSC en experts gelieerd aan het NCSC.

3.8.2 *Dreigingsperceptie van burgers*

Hoewel de experts binnen het NCSC en experts gelieerd aan het NCSC hun inschatting geven van de dreiging, betekent dit niet dat iedereen deze dreiging ook als zodanig ervaart. TNS NIPO concludeert in een onderzoek[45] naar (internet-) veiligheid onder burgers dat de meerderheid (71 procent) te maken heeft gehad met verschillende vormen van cybercriminaliteit. In een steekproef antwoord 55 procent van de respondenten wel eens slachtoffer te zijn geweest van spam, 62 procent van de respondenten is geconfronteerd met phising (18 procent van de e-mails vragen om bank- en creditcardgegevens) en 26 procent van de respondenten heeft een virus op de computer gehad. Toch zegt meer dan de helft (51 procent) van de respondenten over zichzelf matig tot helemaal niet op de hoogte te zijn van de gevaarlijke kanten van internetgebruik, waaronder cybercriminaliteit, virussen, spam of het bezoeken van valse websites.

DOELWITTEN →

DREIGERS ↓

	Overheid	Private organisaties	Burgers
Staten	Digitale spionage	Digitale spionage	Digitale spionage
Private organisaties		Digitale spionage	
(Beroeps)criminelen	Verstoring door malwarebesmetting en spam	Verstoring door malwarebesmetting en spam	Verstoring door malware-besmetting en spam
		Digitale (identiteits)fraude	Digitale (identiteits)fraude
	Chantage	Chantage	Chantage
	Verstoring online dienstverlening	Verstoring online dienstverlening	
Terroristen	Sabotage	Sabotage	
Hacktivisten	Publicatie van vertrouwelijke gegevens	Publicatie van vertrouwelijke gegevens	Publicatie van vertrouwelijke gegevens
	Verstoring vitale infrastructuur	Verstoring vitale infrastructuur	
	Verstoring online dienstverlening	Verstoring online dienstverlening	
	Hoax	Hoax	Hoax
Scriptkiddies	Verstoring online dienstverlening	Verstoring online dienstverlening	
Cyberonderzoekers	Publicatie van vertrouwelijke gegevens	Publicatie van vertrouwelijke gegevens	
Interne actoren	Publicatie van vertrouwelijke gegevens	Publicatie van vertrouwelijke gegevens	
		Chantage	
Geen actor	Brand, waterschade en natuurrampen	Brand, waterschade en natuurrampen	
	Falen en/of ontbreken van hard- en software	Falen en/of ontbreken van hard- en software	

Relevantie: ☐ *Onbekend/n.v.t.* ☐ *Laag* ☐ *Midden* ☐ *Hoog* *(duiding: zie bijlage 1)*

45. Voor het visierapport 'Trends in Veiligheid 2011-2012' heeft Capgemini door TNS NIPO een onderzoek onder burgers in Nederland laten uitvoeren. Voor dit onderzoek zijn 549 respondenten in de leeftijd 18 jaar en ouder ondervraagd.

Het CBS heeft onderzoek[46] gedaan naar de bezorgdheid onder burgers met betrekking tot veiligheid op internet. Hieruit is gebleken dat burgers zich wel degelijk zorgen maken over de veiligheid op internet. In vergelijking tot dreigingen zoals fraude met betaalkaarten, phishing, computervirussen en spam maken ze zich het meest zorgen over het misbruik van persoonlijke gegevens en privacyschendingen. Burgers hebben het meeste last van computervirussen (24 procent) en spam (bijna 70 procent).

46. Centraal Bureau voor de Statistiek, rapport 'ICT, Kennis en Economie'

HOOFDSTUK 4

Kwetsbaarheden

Een kwetsbaarheid is een eigenschap van een samenleving, organisatie of informatiesysteem of een onderdeel daarvan. Een kwetsbaarheid biedt een kwaadwillende partij de kans om de legitieme toegang tot informatie of functionaliteit te verhinderen en te beïnvloeden dan wel ongeautoriseerd te benaderen. Kwetsbaarheden vormen de 'toegangspoorten' waarlangs dreigingen kunnen leiden tot incidenten. Het verhelpen van kwetsbaarheden is een directe manier om dreigingen af te doen nemen en de kans op incidenten te verkleinen. Een kwetsbaarheid wordt veroorzaakt door diverse factoren. In dit hoofdstuk is onderscheid gemaakt tussen kwetsbaarheden veroorzaakt door enerzijds menselijke en organisatorische factoren en anderzijds technische factoren.

4.1 Kwetsbaarheden veroorzaakt door menselijke en organisatorische factoren

Het besef dat cybersecurityincidenten invloed kunnen hebben op de bedrijfsvoering van een organisatie neemt, gezien de aandacht van politiek en media, toe. De kwetsbaarheden die leiden tot dergelijke incidenten, worden voor een deel veroorzaakt door fouten van gebruikers. Ook kunnen ze ontstaan door tekortkomingen in de structuur van een organisatie.

4.1.1 Onvoldoende beveiligde websites en webapplicaties

Incidenten waarin webapplicaties en websites met onvoldoende beveiliging een rol spelen, zijn net als vorig jaar volop in de aandacht geweest. In oktober 2011 brachten de publicaties in het kader van Lektober kwetsbare websites onder de aandacht. Ook in 2012 blijkt nog dat beveiliging van websites en webapplicaties te wensen overlaat, waardoor klantgegevens en andere gevoelige gegevens gevaar lopen.

De kwetsbaarheden zijn op hoofdlijnen onder te verdelen in drie categorieën:

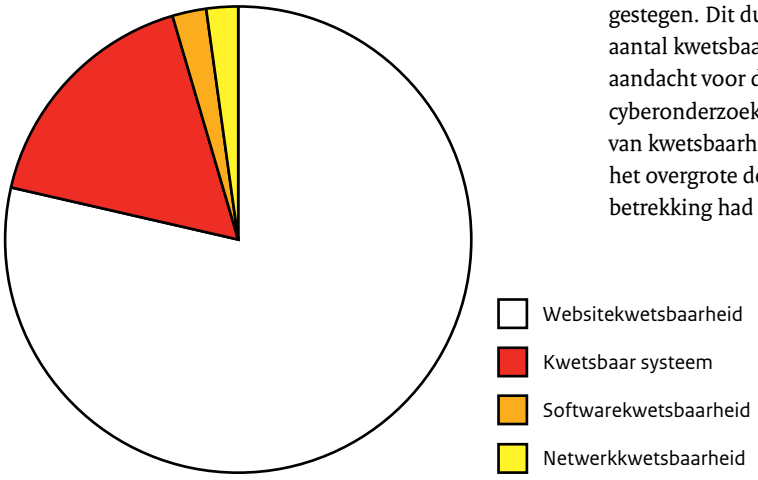
- applicaties die door gebruikers of beheerders onvoldoende beveiligd zijn. Hieronder vallen op internet aangesloten systemen met een standaard of eenvoudig te raden gebruikersnaam en wachtwoord;
- standaardapplicaties, zoals contentmanagementsystemen, waarvan niet alle beveiligingsupdates zijn geïnstalleerd;
- programmeerfouten in (maatwerk)websites en -webapplicaties.
- applicatie- en databaseinjectie en Cross Site Scripting (XSS).

Als onderdeel van de respons op dreigingen en -incidenten handelt NCSC ook ontdekkingen van kwetsbaarheden af. Wanneer alleen een analyse wordt gemaakt van kwetsbaarheden binnen overheden, dan zijn deze als volgt verdeeld:

Tabel 5. Aantallen door NCSC ontdekte kwetsbaarheden binnen overheden

Type	11Q2 + 11Q3	11Q4 + 12Q1	Percentage 11Q2 + 11Q3	Percentage 11Q4 + 12Q1
Websitekwetsbaarheid	**7**	**36**	**87%**	**79%**
Kwetsbaar systeem		**8**	**0%**	**17%**
Softwarekwetsbaarheid	**1**	**1**	**13%**	**2%**
Netwerkkwetsbaarheid		**1**	**0%**	**2%**
Totaal	**8**	**46**	**100%**	**100%**

Figuur 8. Verdeling door NCSC ontdekte kwetsbaarheden binnen overheden



Het aantal door NCSC afgehandelde kwetsbaarheden sinds 1 oktober 2011 is vergeleken met de periode ervoor sterk gestegen. Dit duidt niet zozeer op een toename van het aantal kwetsbaarheden, maar op een toename van de aandacht voor deze kwetsbaarheden van met name cyberonderzoekers. Daardoor is het aantal meldingen van kwetsbaarheden gestegen. Uit de cijfers blijkt dat het overgrote deel van de afgehandelde kwetsbaarheden betrekking had op kwetsbaarheden in websites.

4.1.2 Toegangsbeveiliging eenvoudig te omzeilen

Toegang tot websites en andere applicaties is in veel gevallen nog beveiligd door alleen een gebruikersnaam en een wachtwoord. Door het raden van zwakke wachtwoorden, phishing, het hacken van websites en het hergebruik van wachtwoorden blijkt de toegangsbeveiliging omzeilt te kunnen worden.

Gebruik van standaard, zwakke of gemakkelijk te raden wachtwoorden

Standaard wachtwoorden zijn wachtwoorden die bij uitlevering van producten aanwezig zijn en bij installatie verwijderd of opnieuw ingesteld moeten worden. Dit wordt echter niet altijd gedaan waardoor aanvallers eenvoudig toegang kunnen krijgen tot systemen. Zwakke wachtwoorden zijn vaak eenvoudig te raden en/of te kraken met beschikbare tools. In 2012 is aangetoond dat hierdoor onder andere toegang tot medische systemen en ICS/SCADA-systemen mogelijk was.

Onvoldoende bewustzijn voor gevaren van phishing

Uit analyses van beveiligingsincidenten en oefeningen waarin het NCSC heeft geparticipeerd, blijkt dat phishing een succesvolle manier blijft om toegangsgegevens te achterhalen. Een succesratio van 30 procent is haalbaar. Voorwaarde daarbij is dat een goed op de organisatie gerichte en geschreven phishing e-mail wordt gebruikt. Dit maakt vooral informatiesystemen die via internet toegankelijk zijn en geen gebruikmaken van sterke (bijvoorbeeld two-factor) authenticatie kwetsbaar.

Voorbeeld kwetsbaarheid van webmail

Ruim een derde van de in totaal 679 door het NCSC onderzochte overheidsdomeinen[47] gebruikt een webmaildienst.[48] Eén webmaildienst is afgeschermd op basis van een 'passcode', wat duidt op het gebruik van een token voor authenticatie. Alle andere onderzochte webmaildiensten zijn afgeschermd op basis van alleen een gebruikersnaam en wachtwoord. In het laatste geval kan toegang tot e-mail van overheidsfunctionarissen bemachtigd worden via bijvoorbeeld een phishingactie.

Onvoldoende beveiligde opslag van gebruikersgegevens

Het uitbuiten van kwetsbaarheden in slecht beveiligde websites is een andere manier waarop kwaadwillenden gebruikersnamen en wachtwoorden in handen kunnen krijgen. Vooral als gebruikersnamen en wachtwoorden onvoldoende beveiligd zijn opgeslagen, kunnen hackers deze wachtwoorden vaak eenvoudig achterhalen. Eenmaal verkregen worden de (versleutelde) wachtwoorden steeds vaker gepubliceerd en gedeeld via fora en Pastebin. Een goed voorbeeld daarvan is de LinkedIn hack van juni 2012.

Gebruik van dezelfde gebruikersgegevens voor verschillende diensten

Soms kan het verkrijgen van inloggegevens van ogenschijnlijk onbelangrijke diensten toch een grote winst voor hackers opleveren. Het blijkt namelijk dat gebruikers vaak van dezelfde gebruikersnamen en wachtwoorden voor verschillende diensten gebruikmaken. Als de gegevens voor een dienst achterhaald zijn, zijn ze ook voor andere diensten bekend. Zo kan een inbraak op een webwinkel of verenigingswebsite leiden tot toegang tot vertrouwelijke e-mailberichten.

4.1.3 Niet bijgewerkte software

Software is kwetsbaar in de periode voordat een leverancier een update beschikbaar heeft gesteld. Zolang de update (of patch) niet is geïmplementeerd, blijft de software kwetsbaar. Uit analyse door het NCSC blijkt dat updates vaak niet of niet snel genoeg worden geïnstalleerd. In slechts enkele gevallen werden nog niet bekende kwetsbaarheden (0-days) door kwaadwillenden misbruikt.

Onderzoek naar kwetsbaarheden door het NCSC

Het NCSC publiceert regelmatig beveiligingsadviezen naar aanleiding van software-kwetsbaarheden. Uit analyse van bij NCSC bekende incidenten blijkt dat deze adviezen niet altijd worden opgevolgd.

Het NCSC heeft een onderzoek gedaan naar de gebruikte versienummers van webservers en cms-en van ruim 1.600 domeinen binnen het .nl Top Level Domain (TLD). Het betreft onder andere domeinen van overheidsorganisaties en domeinen uit de top 1000 van populaire sites.

Daarbij zijn webservers aangetroffen, gebaseerd op Apache-webservers en op Microsoft Internet Information Services (IIS). Van de gevonden Apache-webservers blijkt dat 8 procent een verouderde versie gebruikte die al twee jaar niet meer wordt ondersteund, 8 procent up-to-date was en dat van 84 procent van de servers niet kon worden vastgesteld of alle updates geïnstalleerd waren. Vooral van de IIS-installaties is dit moeilijk op afstand te achterhalen. In ieder geval 1 procent van de IIS-installaties bleek verouderd te zijn.
Van de onderzochte cms-en bleek 28 procent verouderd te zijn.

4.1.4 Vastleggen surfgedrag van gebruikers door derde partijen

Het surfgedrag van gebruikers wordt op steeds grotere schaal door allerlei partijen vastgelegd en geanalyseerd. Dit resulteert in kwetsbaarheden voor de privacy. Het vastleggen van surfgedrag noemt men tracking en kan onder

47. Bron: overheid.nl
48. http(s)://webmail.<domein>.nl

andere worden gebruikt om advertenties op maat aan te bieden en voor het optimaliseren van een website.

Het NCSC onderzocht de top 1000 van de meest bezochte Nederlandse websites[49] op het aanbieden van advertenties en op de aanwezigheid van 70 verschillende door derde partijen aangeboden trackingmechanismen. Het onderzoek omvatte ook het gebruik van 1st party cookies. Deze worden gebruikt bij tracking, maar worden ook voor andere doeleinden gebruikt.

Zoals verwacht zijn op de websites van de publieke sector, op een enkele uitzondering na, geen advertenties aangetroffen. Op meer dan 46 procent van de duizend onderzochte websites worden advertenties aangeboden.

In lijn met eerdere bevindingen blijkt op bijna 90 procent van de onderzochte websites tracking te worden toegepast. Uit de detailresultaten van het onderzoek blijkt tracking overigens ook te worden toegepast op websites van bijvoorbeeld ziekenhuizen. Deze groep is verrassend met het oog op mogelijke privacygevoelige gegevens in handen van derde partijen die samenhangen met het surfgedrag op deze sites.

Bijna 80 procent van de duizend onderzochte websites biedt een of meer cookies aan bij het bezoeken van de homepage van de organisatie.

4.1.5 *Het gebruik van mobiele apparaten en consumerization*

BYOD geeft de trend aan dat organisaties voor het verwerken van bedrijfsgegevens persoonlijke apparaten toestaan. De gebruiker is zelf verantwoordelijk en aansprakelijk voor deze apparaten en gebruikt deze apparaten zowel voor persoonlijke als zakelijke doeleinden. Consumerization is een trend die nauw verwant is aan BYOD. Consumerization betekent dat ICT steeds meer wordt ontwikkeld vanuit de eisen van de consument. BYOD en consumerization betekenen voor organisaties dat zij steeds beter moeten inspelen op de eisen van de mobiele medewerker. Uit onderzoek blijkt dat bijna 75 procent van de organisaties toestaat dat bedrijfsmiddelen worden benaderd door apparaten die niet in beheer zijn bij de ICT-afdeling.[50]

Deze ontwikkelingen hebben impact op de informatiebeveiliging van organisaties. Er moet anders worden omgegaan met toegang tot bedrijfsgegevens vanaf eindpunten en het bewaren van deze gegevens. Uit onderzoek[51] blijkt dat hierop aangepast beveiligingsbeleid vaak door medewerkers wordt genegeerd en dat het bewustzijn van de risico's in het lekken van gegevens laag is.[52] Ook blijkt dat bijna de helft van de organisaties een correlatie ziet tussen de toename van het aantal mobiele apparaten en het aantal beveiligingsincidenten.[53]

Consumerization meer dan techniek

Consumerization is niet alleen een technologische kwestie. Social media kunnen een effectief instrument zijn voor organisaties, maar medewerkers moeten begrijpen hoe zij hier veilig en zo effectief mogelijk gebruik van kunnen maken; uit onderzoek blijkt dat meer dan de helft van de organisaties een toename ervaart van malware-aanvallen. Het groeiend gebruik van consumententoepassingen zoals Facebook, LinkedIn en Twitter leidt er dan ook toe dat organisaties het bedrijfs- en communicatiebeleid wijzigen.

Naïviteit van gebruikers bij vrijgeven van persoonsgegevens

Mensen publiceren steeds vaker hun eigen persoonsgegevens via sociale netwerken zonder dat ze daarbij de consequenties overzien. Denk hierbij aan foto's, adresgegevens, hobby's en informatie over het werk. Dat persoonsgegevens worden verzameld, opgeslagen en geanalyseerd, is vaak niet bekend bij de gebruikers. De behoefte om gebruik te maken van een mobiele applicatie of dienst is vaak groter dan het beveiligingsgevoel of de zorgen rondom de privacy. Hier ligt ook uiteraard een verantwoordelijkheid bij organisaties die deze persoonsgegevens verzamelen. Zij moeten helder en eenduidig beschrijven hoe met deze verzamelde persoonsgegevens wordt omgegaan. Hierin is wel een verandering gaande onder druk van diverse organisaties.[54]

4.1.6 *De beveiligingsverantwoordelijkheid van Big Data*

De omvang van de dataverzamelingen, vaak aangeduid met 'Big Data', neemt steeds verder toe en vormt daardoor een magneet voor kwaadwillenden die deze data willen gebruiken.
'Big Data' verzamelingen zijn vaak ongestructureerd van aard en hebben vaak lage eisen met betrekking tot vertrouwelijkheid en integriteit. Informatie als resultaat van de combinatie van vele data-elementen kent vaak andere gevoeligheden en vereist dat de vertrouwelijkheid- en integriteitseisen opnieuw worden vastgesteld. Indien dat niet gebeurt, is het waarschijnlijk dat deze informatie met onvoldoende procedurele en technologische waarborgen wordt beveiligd.

In tegenstelling tot traditionele informatiesystemen is het werken met grote datasets vaak datagestuurd: men begint

49. http://www.alexa.com, site laatst bezocht op 1 april 2011
50. iPass (november 2011) 'The iPass Mobile Enterprise Report': http://info.ipass.com/forms/mobile-enterprise-report
51. Trend Micro (januari 2012) 'Trend Micro Consumerization - The cause and effect of consumerization in the workplace': http://uk.trendmicro.com/imperia/md/content/uk/about/consumerization/consumerization_exec_summary-en.pdf
52. PricewaterhouseCoopers (maart 2012): 'Information Risk Maturity Index': http://continuitycentral.com/BeyondCyberThreats.pdf
53. Trend Micro (februari 2012) 'Mobile Consumerization Trends & Perceptions': http://www.trendmicro.com/cloud-content/us/pdfs/rpt_decisive-analytics_mobile_consumerization_trends_perceptions.pdf
54. Ad.nl (februari 2012) 'Akkoord grote techbedrijven over privacy bij app-gebruik': http://www.ad.nl/ad/nl/5595/Digitaal/article/detail/3197387/2012/02/23/Akkoord-grote-techbedrijven-over-privacy-bij-app-gebruik.dhtml

met de grote ongestructureerde dataset en bekijkt welke informatie daaruit gedestilleerd kan worden. Dat betekent dat er van tevoren niet bepaald kan worden welk niveau van vertrouwelijkheid en integriteit de verkregen informatie zal krijgen. Het gevolg kan zijn dat gebruikers (te) uitgebreide toegangsrechten hebben.

Traditioneel is de informatiesysteemeigenaar verantwoordelijk voor de beveiliging van een informatiesysteem en daarmee van de data. Door datageoriënteerd te werken verschuift zijn rol op dit vlak naar de achtergrond ten gunste van de rol van een data-eigenaar. De beveiligingsverantwoordelijkheid van deze functionaris is onafhankelijk van de plek van deze informatie in een specifiek informatiesysteem. In de praktijk wordt in veel gevallen wel de verantwoordelijkheid van de informatiesysteemeigenaar beperkt, maar wordt er helaas geen data-eigenaar toegewezen. Het gevolg is dat in dergelijke gevallen niemand meer verantwoordelijk is voor de beveiliging van de data, met als gevolg een ontoereikend beveiligingsniveau van de data.

4.1.7 Detectie van onrechtmatigheden is onvoldoende

In de praktijk blijkt dat niet alle organisaties voldoende inzicht hebben in de status van de eigen infrastructuur en alle daarin aanwezige (informatie)systemen. Dit zorgt ervoor dat incidenten en kwetsbaarheden niet tijdig en/of alleen bij toeval ontdekt worden. Kwaadwillenden kunnen zo eenvoudig en langdurig, zonder detectie, aanwezig blijven en veel schade veroorzaken. Passende compenserende en repressieve maatregelen kunnen dan niet tijdig worden genomen.

4.2 Technische kwetsbaarheden

Bij het ontwerp, de implementatie en configuratie van techniek worden fouten gemaakt. Hiermee ontstaat de mogelijkheid voor aanvallers om binnen te dringen in systemen of de werking van deze systemen te beïnvloeden. Deze kwetsbaarheden manifesteren zich zowel in hardware als software.

4.2.1 Afname van kwetsbaarheden in standaard software

Het NCSC maakt bij het beschrijven van kwetsbaarheden in standaardsoftware gebruik van de internationaal geaccepteerde standaard op basis van Common Vulnerabilities and Exposures (CVE). CVE maakt het mogelijk om kwetsbaarheden op een standaard wijze te documenteren en kwetsbaarheden in standaardsoftware uniek te identificeren. De CVE-database leent zich dan ook uitstekend voor het uitvoeren van analyses over bekend geworden kwetsbaarheden. In deze paragraaf wordt een aantal opvallende resultaten op basis van een analyse van deze database beschreven. Daarbij wordt onder andere gebruik gemaakt van een Common Vulnerability Scoring System (CVSS). Er wordt uitgegaan van bekende producten die door de doelgroepen van het NCSC gebruikt worden.

Aantal kwetsbaarheden in standaard software

In figuur 9 is het verloop van het aantal kwetsbaarheden in standaard software in de afgelopen twaalf jaar zichtbaar gemaakt. Het aantal ontdekte kwetsbaarheden groeide tot 2006 en begon, na een korte stabilisatie, af te nemen.

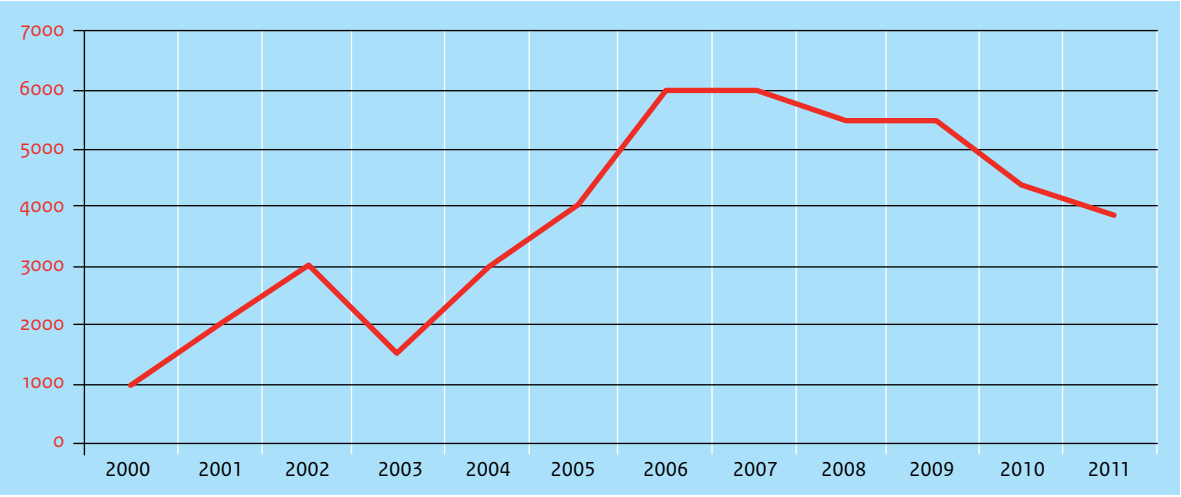
Ruim de helft van de gevonden kwetsbaarheden is relatief eenvoudig uit te buiten

Uit een analyse van de kwetsbaarheden die tussen juli 2011 en maart 2012 bekend zijn geworden, blijkt dat in 55 procent van de gevallen deze relatief eenvoudig uit te buiten is.

Ruim 90 procent van de gevonden kwetsbaarheden is op afstand uit te buiten

Ruim 90 procent van de geanalyseerde kwetsbaarheden is vanaf een extern netwerk uit te buiten. De overige kwets-

Figuur 9. Aantal kwetsbaarheden in standaard software in de afgelopen twaalf jaar



baarheden vereisen fysieke toegang tot het platform of toegang tot het lokale netwerk.

Ruim een derde van de kwetsbaarheden leidt potentieel tot volledige inbreuk op beveiligingsaspecten
Succesvolle uitbuiting leidt bij ruim een derde van de bekende kwetsbaarheden tot volledige inbreuk op beveiligingsaspecten. Kwaadwillenden kunnen in dit geval:
- het systeem volledig onbeschikbaar maken (beschikbaarheid);
- elk bestand op het systeem aanpassen (integriteit);
- toegang verkrijgen tot alle bestanden op het systeem (vertrouwelijkheid).

Te verwachten is dat zelfs met een afnemend aantal bekende kwetsbaarheden deze een belangrijke bron blijven voor toekomstige incidenten. Belangrijkste reden is dat deze niet door organisaties verholpen worden of verholpen kunnen worden.

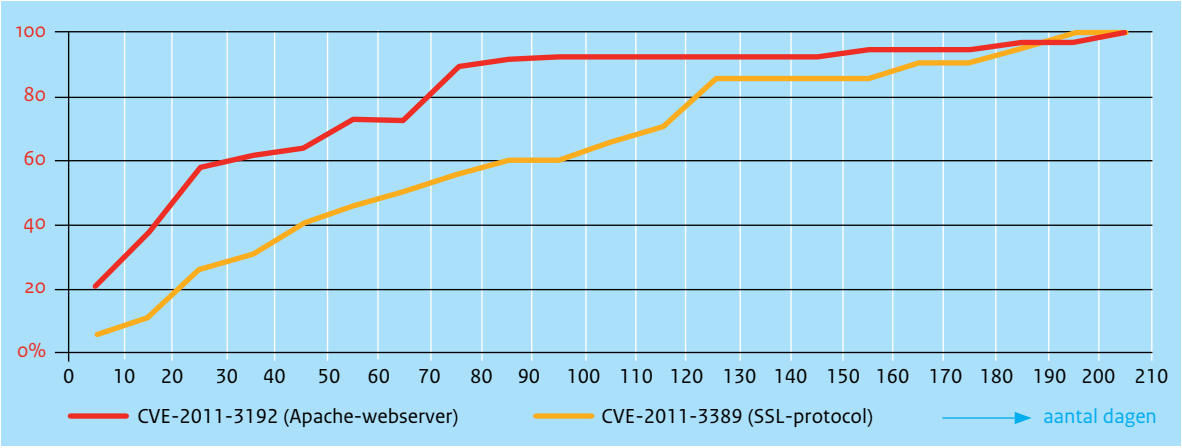
Kwetsbare software
Per kwetsbaarheid registreert de CVE-database ook in welke software de betreffende kwetsbaarheid zich bevindt. Het maakt daarbij onderscheid tussen besturingssystemen en applicaties. Een analyse van 2.870 kwetsbaarheden die in de periode juli 2011 tot en met maart 2012 zijn geregistreerd, laat zien dat een groot deel van de kwetsbaarheden is te vinden in browsers en browsertoevoegingen. In de top tien staan Google Chrome, Mozilla Firefox, Apple Webkit, Opera en Apple Safari. Het aantal kwetsbaarheden dat in de CVE-database voorkomt, kan overigens zijn beïnvloed door het aanmoedigen van het vinden van kwetsbaarheden in specifieke softwareproducten. Op basis van het aantal bekende kwetsbaarheden is te verwachten dat verouderde browsers en browsertoevoegingen zoals Adobe Flash Player, interessante doelen blijven in 2012.

Via malafide of geïnfecteerde websites is het mogelijk om in korte tijd grote aantallen gebruikers aan te vallen, getuige bijvoorbeeld de recente aanval op NU.nl. Dit soort kwetsbaarheden is populair, maar wordt door leveranciers veelvuldig verholpen in nieuwe versies van hun producten. Een manier om het succes van dergelijke aanvallen te beperken, is het zo snel mogelijk installeren van updates. Het niet volledig gepatcht zijn van systemen kan voortkomen uit onachtzaamheid, maar er kunnen ook legitieme redenen een rol spelen. Bijvoorbeeld omdat men wil voorkomen dat de continuïteit van de dienstverlening in gevaar komt door het installeren van een patch die niet volledig getest is.

4.2.2 *Grote variatie in doorlooptijd in verhelpen van kwetsbaarheden*
Er is een groot verschil in de tijd die verschillende leveranciers nodig hebben om kwetsbaarheden in hun producten te verhelpen.
Afhankelijk van de kwetsbaarheid moeten in sommige gevallen meerdere leveranciers updates uitbrengen om de kwetsbaarheid te verhelpen. Dit is bijvoorbeeld het geval bij 'open source'-producten die verschillende Linux-distributies ondersteunen en elke Linux-distributie aanbiedt in een aparte package. Om de respons op kwetsbaarheden te illustreren hebben we van twee verschillende kwetsbaarheden de acties van leveranciers geanalyseerd. Uit de voorbeelden blijkt dat sommige leveranciers bijna direct een update opleveren, terwijl anderen er 200 dagen over kunnen doen en dus al die tijd kwetsbaar zijn.

In figuur 10 zijn twee voorbeelden verwerkt. Het eerste voorbeeld betreft het verhelpen van een kwetsbaarheid in het SSL-protocol.[55] Een ander voorbeeld betreft een kwetsbaarheid in de Apache-webserver die halverwege vorig jaar werd ontdekt.[56]

Figuur 10. Aantal dagen voordat een leverancier een kwetsbaarheid in een product heeft opgelost



55. CVE-2011-3389 (CVSS-score: 4,3)
56. CVE-2011-3192 (CVSS-score: 7,8)

4.2.3 *Kwetsbaarheden voor mobiele malware*

Kwaadwillenden zijn nog steeds op zoek zijn naar een manier om snel en gemakkelijk veel geld te verdienen met mobiele apparaten. Op dit moment is er een toename van kwetsbaarheden voor Android-smartphones, maar niet de verwachte explosieve groei. Voor de toename zijn twee redenen aan te wijzen: Android is een open platform en Android is op dit moment het meest toegepaste besturingssysteem voor smartphone[57] en het marktaandeel lijkt nog steeds groeiende.[58] Overigens worden ook kwetsbaarheden op andere platformen, zoals de iPhone, misbruikt.[59]

Android wordt regelmatig van updates voorzien, maar deze updates zijn in de meeste gevallen niet direct beschikbaar voor de bezitters van een met Android uitgerust apparaat. De maker van het apparaat is verantwoordelijk voor het zodanig aanpassen van de gepubliceerde update dat deze geschikt is voor elk van de door hem uitgebrachte apparaten. In een aantal gevallen worden deze weer aangepast voor providers die een 'branded' versie uitbrengen. Het blijkt dat de fabrikanten van de meeste apparaten met Android gedurende een beperkte periode nieuwe versies van Android beschikbaar maken voor een bepaald toestel. Ook worden er in sommige gevallen zelfs apparaten verkocht waarvan het besturingssysteem niet meer van nieuwe versies wordt voorzien. In zulke gevallen zal een apparaat kwetsbaar zijn en blijven voor alle bekende en nieuw ontdekte kwetsbaarheden in de betreffende versie van het besturingssysteem.

Twee mogelijke scenario's om geld te verdienen met mobiele malware, zijn:

- het sturen van sms-berichten naar zogenoemde 'premium rate services'. Het grootste gedeelte van deze malware kan worden geclassificeerd als 'nep-applicaties' die zich voordoen als een gratis versie van een legitieme toepassing;[60]
- het onderscheppen van authenticatiegegevens die nodig zijn bij het overboeken van geld naar rekeningen van kwaadwillenden. Deze vorm evolueert ook nog steeds en maakt meer en meer gebruik van mobiele applicaties.[61] De verwachting is dat dit in de toekomst toe zal nemen omdat meer gebruikers hun financiën afhandelen op mobiele apparaten. Zitmo (Zeus-in-the-mobile) en Spitmo (SpyEye-in-the-mobile) zijn twee bekende 'families' van mobiele malware die hierbij worden ingezet.[62]

4.2.4 *Kwetsbaarheden door implementatiefouten*

Ondanks dat een cryptografisch algoritme sterk is, kunnen bij de implementatie ervan fouten geïntroduceerd worden waardoor er toch kwetsbaarheden ontstaan. In 2011 hebben onderzoekers ontdekt dat in implementaties van het op zich sterke algoritme RSA, bij de sleutelgeneratie geen goede randomgenerator is gebruikt waardoor er overeenkomsten zijn tussen de sleutels.[63]

RSA gebruikt een publieke en een geheime sleutel. Zoals de namen al suggereren deel je de publieke sleutel met anderen en moet de geheime sleutel geheim blijven. Iemand die in het bezit is van een publieke sleutel die overeenkomsten heeft met een andere publieke sleutel, is in staat om de bijbehorende geheime sleutel te berekenen. Hiermee kan bijvoorbeeld versleutelde communicatie worden ontsleuteld of gemanipuleerd.

Bij hun onderzoek zijn meer dan 6 miljoen publieke RSA-sleutels vergeleken. In 4 procent van de gevallen bleek dat er overeenkomsten waren tussen deze sleutels die erop wezen dat er geen goede randomgenerator is gebruikt. De geheime sleutels hiervan zijn dus te achterhalen. Uit het onderzoek blijkt ook dat RSA voor deze kwetsbaarheid veel gevoeliger is dan andere algoritmen zoals ElGamal, DSA en ECDSA.

Wanneer een organisatie de sleutelgeneratie heeft uitbesteed, zoals bij SSL-certificaten het geval kan zijn, is het voor de organisatie zelf niet na te gaan of de sleutels zijn gegenereerd met een goede randomgenerator, zonder dat zij het onderzoek herhalen.

4.2.5 *Kwetsbaarheden inherent aan het ontwerp van protocollen*

Niet alleen in de implementatie van een beveiligingsprotocol kan zich een kwetsbaarheid bevinden, ook protocollen zelf kunnen kwetsbaar zijn. Soms wordt in een nieuwe versie van het protocol gemaakt om de kwetsbaarheid te verhelpen. In andere gevallen is een herontwerp van het protocol nodig.

Een voorbeeld van een kwetsbaar protocol dat met een nieuwe versie is verbeterd, is SSL/TLS. De versies SSL 2.0, 3.0 en TLS 1.0 zijn kwetsbaar voor een aanval waarbij een aanvaller de beveiligde verbinding kan afluisteren. De nieuwere, veiligere en reeds geruime tijd beschikbare TLS 1.1 en 1.2 werden nog nauwelijks gebruikt. Pas nadat er een Proof of Concept (van BEAST) was gepresenteerd, werden er door

57. Symantec (oktober 2011) 'The Motivations of Recent Android Malware': http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/motivations_of_recent_android_malware.pdf
58. Gartner (november 2011): http://www.gartner.com/it/page.jsp?id=1848514
59. Nu.nl (maart 2012) 'Overheid waarschuwt voor lek in iPhone- en iPadbrowser': http://www.nu.nl/internet/2769765/overheid-waarschuwt-lek-in-iphone--en-ipadbrowser.html of http://www.waarschuwingsdienst.nl/Risicos/Actuele+dreigingen/Softwarelekken/WD-2012-026+Kwetsbaarheid+gevonden+in+Apple+iOS+Webkit.html
60. F-Secure (openbaar gemaakt in februari 2012) 'Mobile threat report Q4': http://www.f-secure.com/weblog/archives/Mobile_Threat_Report_Q4_2011.pdf
61. Tweakers.net (september 2011) 'Malware voor Android onderschept tan-codes internetbankieren': http://tweakers.net/nieuws/76789/malware-voor-android-onderschept-tan-codes-internetbankieren.html
62. McAfee (september 2011) 'Spitmo vs Zitmo: Banking Trojans Target Android': http://blogs.mcafee.com/mcafee-labs/spitmo-vs-zitmo-banking-trojans-target-android
63. http://eprint.iacr.org/2012/064.pdf

dienstaanbieders maatregelen genomen. Nog niet alle softwareoplossingen van eindgebruikers kunnen overweg met de nieuwste versie. Het door dienstaanbieders blokkeren of uitschakelen van de mogelijkheid om met het oude protocol te communiceren, zou dan ook verstoringen voor de eindgebruikers tot gevolg hebben.

Ook is al een aantal jaren bekend dat het SSL/TLS-protocol kwetsbaar is voor DoS-aanvallen omdat het een asymmetrie bevat in de vereiste hoeveelheid computerkracht. Als een cliënt een met SSL/TLS beveiligde verbinding maakt met de server, moet de server ongeveer vijftien keer zoveel berekeningen maken als de cliënt. Door veel SSL/TLS-verbindingen op te zetten, kan een aanvaller overbelasting van de server veroorzaken. De publicatie van de tool thc-ssl-dos die gebruikmaakt van deze kwetsbaarheid, maakt misbruik eenvoudig. Hoewel de gepubliceerde versie van thc-ssl-dos alleen werkt tegen servers die SSL-renegotiation ondersteunen, is de achterliggende kwetsbaarheid aanwezig op alle servers die gebruikmaken van SSL/TLS.

Om deze kwetsbaarheid echt te verhelpen, is een herontwerp van het SSL/TLS-protocol nodig. Overigens is er geen indicatie dat 'thc-ssl-dos' op dit moment daadwerkelijk gebruikt wordt voor DoS-aanvallen op internet.

4.2.6 *Kwetsbaarheden in gsm- en satelliettelefonie*

Bekende kwetsbaarheden in een systeem kunnen ook van toepassing zijn op andere systemen. Voorbeelden hiervan zijn de zwakheden in het gsm-protocol en het effect daarvan op de beveiliging van satelliettelefonie.

De laatste jaren zijn meerdere kwetsbaarheden bekend geworden in het nog steeds veel gebruikte gsm-protocol (2G) dat gebruikt wordt door mobiele telefoons. Eerder is al aangetoond dat men in staat is om met afluisterapparatuur van enkele tientallen euro's een versleuteld gesprek op te vangen, te ontsleutelen en af te spelen. In december 2011 is aangetoond dat men ook in staat is om de mobiele identiteit van iemand anders over te nemen en dus op andermans kosten kan bellen. Tegelijkertijd is er een website gelanceerd[64] waarop per land de verschillen per operator inzichtelijk worden gemaakt met de mogelijkheid van identiteitsfraude, afluisteren en volgen van bezitters van een mobiele telefoon. Deze kaart laat zien dat er in Europa grote verschillen zijn in de maatregelen die operators nemen.

Naast gsm ligt sinds februari 2012 ook satelliettelefonie onder vuur. De geheime versleutelingsalgoritmen van satelliettelefonie, A5-GMR-1 en A5-GMR-2, zijn door twee Duitse onderzoekers gekraakt.[65] De algoritmen van satelliettelefonie lijken heel erg op het versleutelingsalgoritme A5/2 dat ook voor gsm werd gebruikt. Hiermee zijn de onderzoekers in staat om gesprekken af te luisteren. De gebruikers van satelliettelefonie lijken een interessante doelgroep voor aanvallers. De apparatuurkosten van deze aanval liggen rond de 100 euro en komen daarmee in het bereik van een grote groep aanvallers.

4.2.7 *Kwetsbaarheden in SCADA/ICS*

Ten opzichte van het Cybersecuritybeeld uit december 2011 is het aantal ontdekte kwetsbaarheden in SCADA/ICS-systemen opnieuw toegenomen.

In het laatste kwartaal van 2011 bracht ICS-CERT bijna veertig nieuwe alerts en advisories uit die een of meerdere kwetsbaarheden beschreven.[66] In het eerste kwartaal van 2012 was dit significant toegenomen tot bijna vijftig. De toename kan onder andere verklaard worden door de toegenomen belangstelling voor SCADA/ICS. Dit zet enerzijds cyberonderzoekers en andere geïnteresseerden aan tot het zoeken naar kwetsbaarheden en het publiceren daarvan, anderzijds weten zij ICS-CERT steeds beter te vinden. Overigens laten de alerts en advisories van ICS-CERT zich niet 1-op-1 omzetten naar aantallen kwetsbaarheden, omdat een publicatie soms verscheidene (soortgelijke) kwetsbaarheden beschrijft.

De mogelijke impact van een kwetsbaarheid hangt sterk af van het soort systeem dat bestuurd wordt. Daarnaast kunnen flankerende (beveiligings)maatregelen, of juist het ontbreken daarvan, de mogelijke ernst bepalen. Het is daarom lastig om generieke uitspraken te doen over de ernst van kwetsbaarheden. In het publieke domein zijn al langere tijd hulpmiddelen beschikbaar die kwetsbaarheden in ICS/SCADA systemen kunnen uitbuiten. De afgelopen periode is daar een aanzienlijk aantal op ICS/SCADA gerichte exploits aan toegevoegd.
Naast specifieke software voor industriële besturingen wordt ook veel generieke software gebruikt binnen het ICS/SCADA domein. Dit zijn vooral computerbesturingssoftware maar ook databases en webtechnologie. De levensduur (en support) van deze generieke software is meestal korter dan de beoogde levensduur van de industriële installaties. Er wordt soms onvoldoende rekening gehouden dat het vervangen, maar ook actualiseren van deze generieke software, noodzakelijk is.

64. http://www.gsmmap.org
65. Benedikt Driessen en Ralf Hund http://gmr.crypto.rub.de/
66. Dealerts en advisories van ICS-CERT worden gepubliceerd op: http://www.us-cert.gov/control_systems/ics-cert/archive.html

HOOFDSTUK 5

Hulpmiddelen

Voor het uitvoeren van aanvallen maken dreigers gebruik van een aantal hulpmiddelen zoals botnets, phishen voor spam, ransomware en exploitkits. Het laatste hulpmiddel waarover geschreven wordt, hulpmiddelen om je identiteit te verhullen, wordt zowel voor goed- als kwaadaardige doeleinden gebruikt.

5.1 Nieuwe methode voor succesvol versturen van spam

In de afgelopen jaren zijn spamfilters steeds beter geworden in het herkennen en markeren van spam. Mede hierdoor zijn spammers blijvend op zoek naar verbeterde methodes om spam toch succesvol af te leveren. Een van de methodes, waar ook de overheid steeds meer last van heeft, is het inbreken op webmailomgevingen. Daarna kan spam geautomatiseerd via die webmail van een legitieme gebruiker worden verstuurd en wordt zo getracht spamfilters te omzeilen.

De hack van webmail gebeurt als volgt: meerdere gebruikers van een organisatie ontvangen een ogenschijnlijk valide e-mail van de helpdesk met daarin de vraag om in te loggen op de webmailomgeving. De e-mail bevat een URL die lijkt op dat van de eigen webmailomgeving, maar in werkelijkheid is dit een namaak webmailomgeving van de aanvaller. De gebruiker logt hierop in en geeft op deze manier zijn/haar gebruikersnaam en wachtwoord aan de kwaadwillende.
De aanvaller gebruikt vervolgens de gestolen gegevens om zelf in te loggen op de echte webmailomgeving en verstuurt hiervandaan grote hoeveelheden spam.

Deze manier van spammen kan grote gevolgen hebben voor de getroffen organisatie. Er kunnen via de webmail gevoelige gegevens lekken. Daarnaast kan een aanvaller via gestolen accountgegevens dieper in de organisatie doordringen, omdat de aanvaller zich eenvoudig kan voordoen als een eigen medewerker. Ten slotte kunnen de e-mailservers van de getroffen organisatie op een blacklist terechtkomen. Hierdoor wordt het voor deze organisatie bijna onmogelijk om nog e-mails te verzenden naar derde partijen.

Nederland kent in de eerste twee maanden van 2012 een relatief hoog percentage phishing e-mails (in februari 2012 een op de 153 in Nederland tegen een op de 358 wereldwijd).[67]

5.2 De wedloop van het verhullen van de eigen identiteit

Bij alle digitale communicatie worden er sporen achtergelaten. Omdat niet iedereen dat wil, worden hulpmiddelen ingezet om dit zo veel mogelijk te voorkomen. Met dezelfde technieken kan men de identiteit verhullen. In sommige gevallen worden dezelfde technieken gebruikt voor tegengestelde doelen. Bijvoorbeeld door de politie om niet op te vallen tijdens internetonderzoek, maar ook door verdachten om zich beter voor de politie te kunnen verbergen. In een aantal landen kan het gebruik van deze technieken voor het verhullen van de identiteit bij het uiten van een mening zelfs van levensbelang zijn.

Er zijn verschillende methoden en technieken om iemands (internet)identiteit te beschermen. Zo is er software om anoniem via het internet te communiceren of diensten aan te bieden, zoals via Tor[68] en i2p[69], en software om redelijk anoniem betalingen te kunnen verrichten (BitCoin). Deze hulpmiddelen worden steeds gebruiksvriendelijker gemaakt zodat ze voor een breder publiek gemakkelijker te gebruiken zijn. Een voorbeeld daarvan is de Tor-browser bundle.[70]

Naast hulpmiddel zijn deze technieken ook doelwit. Zoals praktisch alle software kwetsbaarheden bevat, kan ook software die de identiteit moet verhullen kwetsbaarheden bevatten. Recent heeft een onderzoeker diverse kwetsbaarheden in UltraSurf blootgelegd.[71] Hij is echter ook een belangrijke ontwikkelaar van Tor, een product met vergelijkbare functionaliteit.

5.3 Nieuwe verschijningsvorm van ransomware

Er zijn virussen die proberen iemand geld te laten betalen om van een virusbesmetting af te komen. Deze virussen, ook wel ransomware genoemd, kapen een computer door bijvoorbeeld documenten en foto's te versleutelen waardoor ze niet meer toegankelijk zijn. Het virus meldt dat een geldbedrag betaald moet worden om van de versleuteling af te komen. Meestal krijgt het slachtoffer na betaling geen werkende oplossing.

Ransomware is al jaren een bekend fenomeen. De laatste maanden heeft deze vorm van besmetting van computers weer een aantal nieuwe verschijningsvormen gekregen. Een nieuwe variant is in staat om het masterbootrecord (MBR) van de harde schijf te infecteren en voorkomt daarmee dat het besturingssysteem opstart.

67. https://www.symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_02_2012.en-us.pdf
68. www.torproject.org
69. http://www.i2p2.de/
70. https://www.torproject.org/projects/torbrowser.html.en
71. https://blog.torproject.org/blog/ultrasurf-definitive-review

5.4 Exploitkits worden verder verfijnd

Ten opzichte van 2010 is een verschuiving waarneembaar in de manier waarop virusbesmettingen plaatsvinden. Veel virussen worden nog steeds verstuurd via e mail en veel computers worden besmet bij het bezoeken van (veelal gehackte) websites. Hierbij worden kwetsbaarheden in de browser misbruikt. Steeds vaker wordt bij de laatste categorie gebruikgemaakt van zogenoemde exploitkits. In plaats van het uitbuiten van een kwetsbaarheid, wordt bij het gebruik van een exploitkit een uitbreidbare reeks aan kwetsbaarheden geprobeerd.

De specifiek gebruikte kwetsbaarheden zijn afhankelijk van het gebruikte besturingssysteem, de browser, de browser-plugins en de locatie van de gebruiker. Een voorbeeld hiervan is de verspreiding van het Sinowal-virus via de website NU.nl.[72] Ook bij deze aanval werden bezoekers van de website geleid naar een exploitkit om malware te installeren op de computer van de bezoeker.

Het gebruik van exploitkits maakt het voor een crimineel gemakkelijker om zelfstandig systemen te infecteren zonder diepgaande technische kennis. Hierdoor is het ook door meer criminelen te gebruiken. Exploitkits worden binnen het criminele circuit verhandeld als kant-en-klare softwarepakketten. Zij zijn vaak al voorzien van bruikbare exploits en wanneer nieuwe exploits beschikbaar komen, kunnen deze vaak als losse modules worden toegevoegd. Veelvoorkomende exploitkits in 2011 en het eerste kwartaal van 2012 zijn de Blackhole en de oudere Phoenix exploitkit.

De effectiviteit van de exploitkits is terug te zien in het aantal malwarebesmettingen. In de tweede helft van 2011 is het aantal besmettingen van Nederlandse pc's met malware aanzienlijk toegenomen.[73] Waar in het eerste kwartaal van 2011 nog sprake was van een infectie bij 4,6 per 1.000 computersystemen, is dit aantal in het vierde kwartaal gestegen tot 13,1 per 1.000 computers. Deze stijging brengt Nederland boven het wereldwijde gemiddelde, dat in het vierde kwartaal van 2011 op 7,1 per 1.000 computers lag. De stijging komt voornamelijk door de trojan EyeStye, die verantwoordelijk is voor 16 procent van de besmettingen in Nederland. Het is onduidelijk waarom deze malware zich juist in Nederland zo snel heeft verspreid.

5.5 Groot botnet met Apple computers ontdekt

In het afgelopen halfjaar zijn platformen die eerder niet als interessante doelwitten werden gezien, nu ook in botnets opgenomen en zijn de methodes die worden gebruikt voor het aansturen van botnets geavanceerder geworden.

In april 2012 is Flashback,[74] het eerste grote botnet bestaande uit Mac-computers ontdekt. Waar tot voor kort gebruikers van een Mac zich relatief veilig waanden voor aanvallen met malware, blijkt nu dat er meer dan 500.000 Mac-computers onderdeel uitmaakten van dit botnet. Opvallend hierbij was dat vier landen gezamenlijk meer dan 95 procent van de geïnfecteerde machines hadden (Verenigde Staten, Canada, Verenigd Koninkrijk en Australië).[75] Het toegenomen marktaandeel van Mac onderstreept dat elk veelgebruikt systeem door beroepscriminelen zal worden misbruikt. Apple heeft een patch uitgebracht voor hun besturingssysteem waarmee een geïnfecteerde machine geschoond kan worden en de misbruikte kwetsbaarheid opgelost wordt.

Niet alleen zijn nu ook Mac-computers doelwit geworden van aanvallen, er is ook een nieuwe wijze van aansturen van een botnet van mobiele apparatuur ontwikkeld: per sms-bericht. De mobiele malware TigerBot wordt op die wijze aangestuurd. Omdat het verzenden van sms-berichten moeilijk gefilterd kan worden, kan daardoor ook de communicatie tussen botnetbeheerder en geïnfecteerde telefoon moeilijk geblokkeerd worden. De normale manier van botnetbestrijding, het achterhalen van de locatie van centrale servers uit de botnetinfrastructuur en het uitschakelen hiervan, is bij deze mobiele malware daarom lastig. De functionaliteit van Tigerbot is verder vergelijkbaar met die van andere mobiele malware.

72. http://blog.fox-it.com/2012/03/16/post-mortem-report-on-the-sinowallnu-nl-incident
73. http://www.microsoft.com/security/sir/archive/default.aspx
74. news.drweb.com/show/?i=2341&lng=en&c=14
75. http://www.security-technologynews.com/news/500000-apple-mac-flashback-trojan-infections.html

HOOFDSTUK 6

Weerbaarheid

Dit hoofdstuk richt zich op de digitale weerbaarheid van de Nederlandse samenleving en de initiatieven die bedrijven, overheid en burgers nemen om die digitale weerbaarheid te vergroten.

Digitale weerbaarheid is het vermogen om weerstand te bieden tegen negatieve invloeden op de beschikbaarheid, vertrouwelijkheid en/of integriteit van (informatie-) systemen en digitale informatie. De digitale weerbaarheid staat daarbij in het teken van de continuïteit van de dienstverlening en de handhaving van de effectiviteit. Informatiesystemen moeten hierbij worden beschouwd als een geheel van mensen, middelen, processen en procedures, inclusief het besturen van dat geheel.

Organisaties zijn in toenemende mate afhankelijk van complexe, dynamische ketens van informatiesystemen. Deze complexiteit houdt onder andere in dat de effecten van invloeden op deze ketens onvoorspelbaar zijn: kleine invloeden kunnen leiden tot grote verstoringen, grote invloeden hebben soms nauwelijks effect. Beveiligingsmaatregelen voor deze keten van systemen moeten daarom in onderlinge samenhang worden beschouwd waarbij rekening wordt gehouden met deze onvoorspelbaarheid. Daarbij moet een balans worden gevonden tussen de prestaties van de informatiesystemen en de weerbaarheid tegen verstoringen. Het aanpassingsvermogen van systemen is daarbij een belangrijke eigenschap.

De initiatieven in dit hoofdstuk worden beschouwd langs vijf thema's: normen, richtlijnen en standaarden, kennis en bewustzijn, handhaving en opsporing, informatie-uitwisseling en samenwerking, en ten slotte cybersecurity-onderzoek en nieuwe methoden. Over het algemeen worden generieke initiatieven beschreven die voor de gehele samenleving, een bepaalde sector of een groep organisaties gelden. De initiatieven zijn tot stand gekomen op basis van open bronnen en informatie die door diverse partijen beschikbaar is gesteld, en vormen zeker geen uitputtende lijst.

De genoemde initiatieven worden beschreven vanuit het primaire oogmerk van het initiatief. Dit oogmerk is zoveel mogelijk weergegeven in titel van de secties. Over de effectiviteit van de maatregelen die onder de initiatieven schuilgaan, is in de meeste gevallen nog geen informatie bekend en/of moeilijk in te schatten.

6.1 Normen, richtlijnen en standaarden

Normen, richtlijnen en standaarden op het gebied van cybersecurity helpen organisaties om de beveiliging van hun informatiesystemen en netwerken op een hoger niveau te brengen. Daarmee verhogen zij de weerbaarheid van organisaties en de Nederlandse samenleving als geheel.

6.1.1 Stappenplan en checklist bieden gemeenten handelingsperspectief na Lektober

Direct na de openbaring van de lekken in vijftig gemeentelijke websites tijdens het 'Lektober'-incident in oktober 2011 heeft het NCSC voor de gemeenten een factsheet uitgebracht met daarin een stappenplan en een checklist. Deze factsheet bevat een samenvatting van informatie die al enige jaren daarvoor was vastgelegd in het Raamwerk Beveiliging Webapplicaties.[76] Op grond van de factsheet hebben de getroffen gemeenten, haar leveranciers en hostingpartijen een zelfevaluatie en verbeterslag gemaakt. De zelfevaluaties zijn door Logius en het NCSC beoordeeld. De verbeterslagen hebben op deelgebieden van de informatievoorziening van gemeenten een aanzienlijke verbetering van de beveiliging tot gevolg gehad. Als spin-off van deze actie is ook het beveiligingsbewustzijn van gemeenten, hun leveranciers en hostingpartijen vergroot.

6.1.2 De 'ICT-beveiligingsrichtlijnen voor webapplicaties' verhogen beveiligingsniveau

Naar aanleiding van een verklaring van de ministerraad aan de Tweede Kamer[77] heeft het NCSC na 'Lektober' in samenwerking met diverse partijen de 'ICT-beveiligingsrichtlijnen voor webapplicaties' opgesteld. Hiermee is voorzien in een duidelijke behoefte in de markt. Diverse organisaties, ook organisaties die niet tot de gebruikers van DigiD behoren, maken intussen gebruik van deze 'ICT-beveiligingsrichtlijnen voor webapplicaties' om de beveiliging van hun webapplicaties op een hoger niveau te brengen.

Bij de ontwikkeling van de 'ICT-beveiligingsrichtlijnen voor webapplicaties' is intensief samengewerkt tussen allerlei partijen. Deze partijen omvatten overheidspartijen als NCSC, Logius, Rijksauditdienst, KING en VNG, commerciële partijen op het vlak van informatiebeveiliging en auditing, samenwerkingsverbanden als OWASP Nederland en diverse organisaties die gebruikmaken van DigiD.

De richtlijnen zijn gebruikt voor het vaststellen van een DigiD-aansluitnorm. De norm is gebaseerd op de 'ICT-beveiligingsrichtlijnen voor webapplicaties' en vastgesteld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in overleg met Logius, de Rijksauditdienst en het NCSC. De norm wordt door geregistreerde EDP-auditors gebruikt om een assessment uit te voeren op grond waarvan een uitspraak gedaan wordt over de beveiliging van de applicaties van DigiD-gebruikende organisaties. Op basis van deze uitspraak kan Logius het gebruik van DigiD al dan niet toestaan.

76. https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/raamwerk-beveiliging-webapplicaties.html
77. http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/10/12/kamerbrief-lekken-in-een-aantal-gemeentelijke-websites.html

6.1.3 *Cookierichtlijn beschermen gebruikers van internet*

Op basis van Europese richtlijnen uit 2009 is het in de toekomst, op enkele uitzonderingen na, niet meer mogelijk gegevens - waaronder cookies - op een computer te plaatsen of uit te lezen zonder voorafgaande toestemming van de computergebruiker. De gebruiker moet voldoende geïnformeerd worden en een weigeringsmogelijkheid geboden worden. Het zoek- en surfgedrag van consumenten mag in de toekomst dus niet zonder meer worden gebruikt voor zaken als gerichte advertenties (behavioral targeting). De betreffende bepaling uit de Europese richtlijn is opgenomen in de herziene Telecommunicatiewet die in mei 2012 door de Eerste Kamer is aangenomen.

6.1.4 *Baseline Informatiebeveiliging Rijksdienst*

Voor de Rijksdienst is in 2011 gewerkt aan de normenkaders van de Baseline Informatiebeveiliging Rijk (BIR). Deze baseline gaat in 2012 of 2013 gelden voor alle onderdelen van de Rijksdienst en vervangt vijf interdepartementale normenkaders en de individuele baselines van de Rijksdienst. De baseline heeft als doel om het juiste beveiligingsniveau te kunnen kiezen, het vertrouwen in netwerken van andere departementen te vergroten en het delen van informatie tussen departementen te bevorderen. Waar nodig kunnen departementen en diensten extra normen aan de BIR toevoegen, afgestemd op hun specifieke beveiligingseisen. De BIR is op moment van schrijven nog niet goedgekeurd en daarom nog niet verplicht.

6.2 Kennis en bewustzijn

De incidenten van het afgelopen jaar (2011) laten zien dat het noodzakelijk blijft om aandacht te schenken aan het verhogen van kennis en bewustzijn op het vlak van cybersecurity. Er zijn diverse initiatieven die zich richten op het verhogen van deze kennis en bewustzijn bij een brede verzameling doelgroepen. Vier invalshoeken die we hier uitlichten zijn het burgerperspectief, de verhoging van bewustzijn rondom ICS/SCADA-systemen, de bewustzijnsverhoging door red teaming en het verhogen van bewustzijn rondom spionage.

6.2.1 *Burgers zijn zich beperkt bewust van cybersecurity*

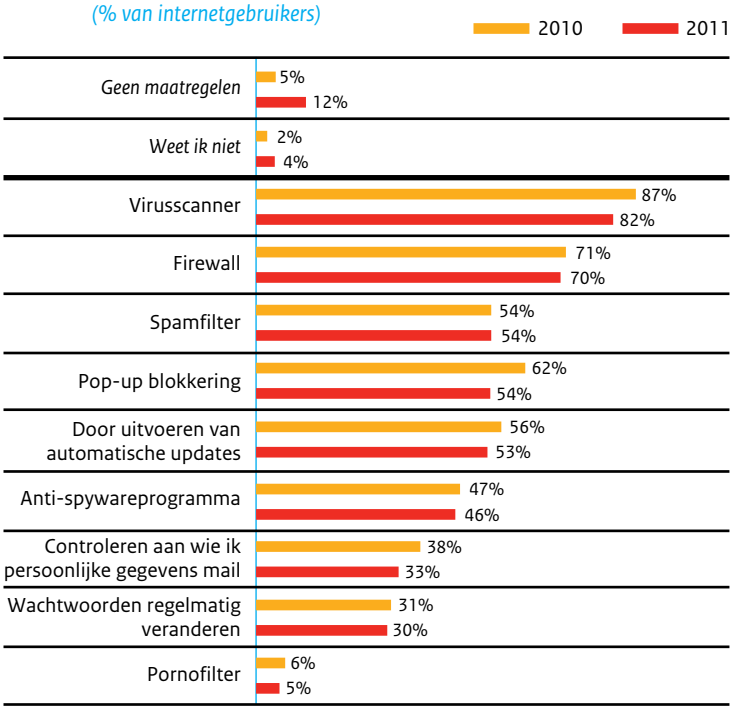
Kennis en bewustzijn van cybersecurity zijn van groot belang voor de bescherming van persoonlijke en financiële gegevens van burgers. Het is een gezamenlijke verantwoordelijkheid van overheid en private partijen om dit te bereiken en er bestaan binnen de overheid en het bedrijfsleven dan ook verschillende campagnes om hem bewust te maken van de gebruikersrisico's van ICT en internet. Voorbeelden zijn het programma 'Digivaardig en Digiveilig'[78] van het ECP voor de Informatiesamenleving, de campagne 'Veilig Bankieren'[79] van de NVB en de campagne over 'pas op je pas'[80] van de NVB en de politie. Het NCSC richt zich eveneens op bewustwording van burgers en doet dat onder andere met online-adviezen op de waarschuwingsdienst.[81]

De genoemde campagnes beogen de digitale vaardigheid, het vertrouwen in ICT en het veiligheidsbewustzijn te vergroten, en de kans op phishing te verminderen en daarmee de digitale weerbaarheid.

Uit een onderzoek van de Universiteit Twente[82] blijkt dat een deel van de burgers zich bewust is dat ze hun computer moeten beveiligen tegen negatieve invloeden van buitenaf en dat zij ook de bijbehorende technische maatregelen nemen zoals in de onderstaande figuur is weergegeven. Ondanks de toegenomen voorlichting rondom cybersecurity blijkt de mate waarin burgers maatregelen nemen niet significant te zijn afgenomen, maar zeker niet te zijn toegenomen.

De verzameling maatregelen die door de Universiteit Twente zijn onderzocht, kunnen worden beschouwd als een minimale set beveiligingsvereisten. Deze set vormt een significante verhoging van de drempel om slachtoffer te worden van beveiligingsincidenten. Dit laat onverlet dat aanvallers steeds beter in staat zijn om deze basismaatregelen te omzeilen. Dit is vooral waarneembaar bij gerichte aanvallen, maar de verwachting is dat dit ook steeds vaker het geval zal zijn bij willekeurige aanvallen op (grote groepen) burgers.

Figuur 11. Maatregelen ter bescherming van internettoegang (% van internetgebruikers)



(Bron: Universiteit Twente/Center for e-Government Studies, Trendrapport Computer- Internetgebruik 2011)

78. Zie www.digivaardigdigibewust.nl
79. Zie www.veiligbankieren.nl
80. Zie www.pasopjepas.nl
81. Zie www.waarschuwingsdienst.nl
82. Universiteit Twente/ Center for e-Government Studies, Trendrapport Computer- Internetgebruik 2011

6.2.2 *Het bewustzijn rondom ICS/SCADA blijft een probleem*

Het NCSC heeft een aantal belangrijke richtlijnen voor het beveiligen van ICS/SCADA-systemen gepubliceerd en daarmee sterk ingezet op het bevorderen van het bewustzijn rondom ICS/SCADA.

De aanbevolen beveiligingsmaatregelen rondom ICS/SCADA-systemen zijn deels algemene maatregelen zoals het inrichten van passwordmanagement, patchmanagement, defence-in-depth principes en monitoring. Daarnaast worden een aantal specifieke maatregelen beschreven zoals het zoveel mogelijk isoleren van ICS/SCADA-systemen van andere systemen en van het internet.

6.2.3 *Red teaming verhoogt het bewustzijn van cybersecurity*

Het NCTV en het onderdeel NCSC hebben het afgelopen jaar diverse 'red teaming'-activiteiten voor organisaties ontplooid en hierdoor organisaties in staat gesteld de weerbaarheid te vergroten.

Red teaming wordt steeds vaker gebruikt en blijkt een effectieve methode om niet alleen de beveiliging op een hoger plan te brengen, maar ook het bewustzijn rondom informatiebeveiliging te verhogen. Bij deze methode kruipt een team in de rol van een aanvaller om de beveiliging van een systeem of een organisatie op de proef te stellen. Red teaming kan worden toegepast op fysieke beveiliging en informatiebeveiliging of op een combinatie van beide.

Bij red teaming wordt een gerichte actie uitgevoerd met een vooraf gesteld doel, bijvoorbeeld om documenten met gevoelige informatie te achterhalen of om gevaarlijke stoffen te bemachtigen. Op het digitale vlak gaat de methode feitelijk verder waar penetratietesten en kwetsbaarheidsanalyses stoppen.

6.2.4 *AIVD verhoogt bewustzijn rondom spionage*

De AIVD geeft voorlichting aan bedrijven en overheidsinstanties die te maken kunnen krijgen met spionage. Hierbij worden zij onder andere bewustgemaakt van de kwetsbaarheden op het vlak van communicatiemiddelen en digitale systemen, en de gevolgen van digitale spionage.

Het ultieme doel van een gerichte aanval is de bemachtiging van gevoelige informatie. Preventieve strategieën gericht op het identificeren en vervolgens beschermen van vertrouwelijke informatie zijn daarom van cruciaal belang. Om dit proces te ondersteunen heeft de AIVD in samenwerking met DGV de kwetsbaarheidanalyse spionage (KWAS) ontwikkeld.[83] Hierin worden handvatten aangereikt waarmee organisaties vertrouwelijke informatie kunnen identificeren en aanbevelingen kunnen formuleren ter beveiliging van deze informatie zodat de weerstand tegen digitale spionage verhoogd kan worden.

6.3 Bestuurlijke handhaving, opsporing en bestrijding

Bestuurlijke handhaving, opsporing en bestrijding op het vlak van cybersecurity is een breed speelveld dat zich niet beperkt tot de landsgrenzen, waar vele organisaties direct of indirect een rol spelen en dat zich richt op alle facetten van cybercriminaliteit en criminaliteitsvormen op het internet in brede zin. In deze paragraaf wordt een aantal relevante ontwikkelingen en initiatieven benoemd. Sommige initiatieven zijn al voor de rapportageperiode gestart, maar zijn nog niet eerder genoemd en zijn hier opgenomen vanwege hun belang voor de weerbaarheid.

6.3.1 *Het Team High Tech Crime van de Dienst Nationale Recherche breidt uit*

Het Team High Tech Crime (THTC) van de Dienst Nationale Recherche richt zich op de opsporing en bestrijding van cybercriminaliteit. In de afgelopen periode zijn zij begonnen met de werving en selectie van dertig nieuwe medewerkers.

6.3.2 *Het THTC arresteert beroepscriminelen en andere dreigers*

Het THTC arresteert, net als collegadiensten in het buitenland, regelmatig beroepscriminelen en andere actoren uit de dreigersgroep. Een recent voorbeeld is de 17-jarige KPN-hacker die door digitale opsporingsmethoden kon worden gelokaliseerd. De hacker heeft intussen bekend en is door de Rechtbank onder voorwaarden in vrijheid gesteld in afwachting van zijn berechting.

Een ander voorbeeld is de aanhouding van vier Nederlandse verdachten door het THTC. Deze aanhoudingen waren onderdeel van een internationale FBI-actie waarbij negentien verdachte leden van Anonymous zijn aangehouden. De verdachten zijn verantwoordelijk voor het hacken van verschillende websites en zijn lid van Antisec NL, een vermeende splintergroepering van Anonymous.

6.3.3 *De THTC zet in op opsporing en bestrijding van kinderporno op internet*

Kinderporno is een vorm van criminaliteit waarbij op grote schaal gebruik wordt gemaakt van internet voor het creëren en in stand houden van netwerken voor de verspreiding en verhandeling van pornografisch materiaal. Hoewel de opsporing en bestrijding van kinderporno niet direct bijdraagt aan de digitale weerbaarheid van de samenleving, vormt deze bestrijding een van de speerpunten van het THTC en verdient dit daarom een plek in het Cybersecuritybeeld Nederland.

Naar aanleiding van het internationale onderzoek 'Descartes' zijn door het THTC diverse onderzoeken gestart met als doel kinderporno op te sporen en te bestrijden. De onderzoeken

83. Zie https://www.aivd.nl/onderwerpen-o/spionage-o

richten zich op de rol die digitale netwerken spelen bij de verspreiding van kinderporno. In de onderzoeken worden met een speciaal zoekprogramma de pseudo-top-level-domeinen van het Tor-netwerk systematisch onderzocht op de aanwezigheid van kinderporno.[84] Het THTC heeft zich daarna toegang verschaft tot een aantal sites en het aangetroffen materiaal veiliggesteld en vernietigd. Bovendien is duidelijk gemaakt dat de politie op de site aanwezig is geweest.

6.3.4 *Cybercriminaliteit wordt ook op Europees niveau bestreden*

Nadat Europol in 2009 al het Analytical Workfile (AWF) Cyborg oprichtte om een grensoverschrijdende informatiepositie op het gebied van cybercriminaliteit op te bouwen en te verbeteren, richt nu ook Europol zijn pijlen nadrukkelijker op cybercriminaliteit met de oprichting van het 'European Cybercrime Centre' (EC3). Dit onderdeel wordt begin 2013 in Den haag gevestigd. Met het centrum wil Europol de Europese strijd tegen onlinemisdrijven coördineren. Hieronder vallen onder andere diefstal van identiteit, kinderpornografie en fraude met creditcards.

6.3.5 *Twee nieuwe meldplichten verplichten tot het melden van privacyschendingen*

In mei 2012 heeft de Eerste Kamer de nieuwe telecommunicatiewet aangenomen. Deze nieuwe wet bevat onder andere een strengere meldplicht voor datalekken.[85] De wet is uitsluitend gericht op aanbieders van elektronische netwerken en verplicht deze partijen om datalekken te melden aan OPTA. Naast deze wet is er een eerste consultatie geweest voor een wetsvoorstel voor 'gebruik camerabeelden en meldplicht datalekken'.[86] In tegenstelling tot het onderdeel in de telecommunicatiewet, geldt deze meldplicht voor alle verwerkers van persoonsgegevens en moet het datalek aan het College Bescherming Persoonsgegevens (CBP) en aan de getroffenen worden gedaan. De melding moet zowel het lek beschrijven als de getroffen maatregelen op juridisch, technisch en beleidsmatig vlak. Het wetsvoorstel 'gebruik camerabeelden en meldplicht datalekken' voorziet in een boetebevoegdheid voor het CBP (louter) als bedrijven en organisaties een datalek niet melden.

De wetsvoorstellen vormen instrumenten om de vertrouwelijkheid van gegevens te kunnen handhaven. Hoewel zij in eerste instantie tot doel hebben de transparantie naar betrokkenen te waarborgen, beogen zij indirect bedrijven te stimuleren om hun beveiliging te verbeteren. Zij passen daarmee binnen een stelsel van maatregelen die het bedrijfsleven en de overheid moeten nemen om gevoelige gegevens te beschermen. Indirect kunnen de maatregelen daarom bijdragen aan een verhoging van de weerbaarheid.

Overigens bestaan er naast de genoemde meldplichten ook andere meldplichten voor specifieke sectoren. Dit geldt bijvoorbeeld voor banken en beursgenoteerde bedrijven.

6.3.6 *Bestrijding botnets gestimuleerd*

Het ontmantelen van het Bredolab-botnet in oktober 2010 lijkt diensten in andere landen te hebben gemotiveerd om zich te oriënteren op de juridische grenzen van hun opsporingsbevoegdheden. Een aanzienlijk aantal botnets is het afgelopen halfjaar met aandacht van de media uit de lucht gehaald. In de meeste van deze gevallen is sprake van publiek-private samenwerking. Hierdoor kon voldoende kennis en mandaat bijeengebracht worden om effectief te kunnen ingrijpen in de werking van het botnet. Zo heeft Microsoft in maart 2012 in samenwerking met private organisaties en opsporingsdiensten Operation B-71 uitgevoerd, waarbij de command & controlservers van meerdere Zeus-botnets uitgeschakeld zijn.[87] In een soortgelijke operatie heeft Kaspersky in samenwerking met partners het Hlux/Kelihos-botnet uitgeschakeld.[88]

Door de flexibiliteit van de aangepakte botnetinfrastructuur is de effectiviteit van dergelijke acties discutabel: bij deze operaties worden bijvoorbeeld de 'Command & Control'-servers uitgeschakeld, maar de botsoftware blijft geïnstalleerd op de geïnfecteerde machines. De botnetbeheerders installeren nieuwe 'Command & Control'-servers, waardoor de beheerder de controle weer kan overnemen.[89] De bestrijding van botnets dient dus niet alleen gericht te zijn op het uitschakelen van de centrale servers, maar gecoördineerd te worden opgepakt met het verstoren van de gebruikte tussenlagen (voor zover die in Nederland worden gehost) en met het aanpakken van de infecties bij (Nederlandse) consumenten. Bij de ontmanteling van Bredolab is dan ook een waarschuwing uitgegaan naar de slachtoffers van geïnfecteerde machines met een uitleg hoe zij hun computer konden opschonen.

Een aantal Nederlandse Internet Serviceproviders (ISPs) en andere martkpartijen hebben zich verenigd in de Werkgroep Botnets. Deze werkgroep vormt een onderdeel van het Platform Internetveiligheid van ECP EPN.[90] De deelnemers in de werkgroep hebben afspraken in een convenant vastgelegd. Voor de aanpak van infecties bij klanten, heeft het kabinet vorig jaar in deze werkgroep voorgesteld om

84. Zie onder andere http://www.sbs6.nl/programmas/undercover-in-nederland/over
85. Zie http://www.eerstekamer.nl/behandeling/20110622/gewijzigd_voorstel_van_wet/f=/viqjihbe44v5.pdf
86. Zie http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/12/20/wijziging-van-de-wet-bescherming-persoonsgegevens-voor-verruiming-gebruik-camerabeelden-en-invoering-van-meldplicht-bij-datalekken/c-documents-and-settings-nsenff-ad-000-desktop-camera-pers-5641a-wetsvoorstel-gebruik-camerabeelden-en-meldplicht-datalekken-versie-consultatie-en-advies-dec-11.pdf
87. Securitywatch.pcmag.com/security/296250-botnets-takedowns-a-game-of-whack-a-mole
88. securitywatch.pcmag.com/malware/295967-kaspersky-crowdstrike-take-down-kelihos-v2-botnet
89. Securitywatch.pcmag.com/security/296250-botnets-takedowns-a-game-of-whack-a-mole
90. http://www.ecp-epn.nl/werkgroep-botnets

een 'clearing house' op te zetten. Hiermee kunnen ISP's klanten informeren die besmet zijn en hen helpen om hun computers te ontsmetten en schoon te houden. Het 'clearing house' is daarmee een belangrijke schakel in de opsporing en ontsmetting van botnets.

6.4 Informatie-uitwisseling en samenwerking

Nationale en internationale informatie-uitwisseling en samenwerking zijn belangrijke middelen om de digitale weerbaarheid van Nederland te vergroten. Samenwerkingsverbanden bevorderen de uitwisseling van cruciale informatie, het bepalen van gezamenlijke strategieën en het effectiever optreden bij incidenten. Op het vlak van cybersecurity zijn er vele samenwerkingsverbanden en worden bijna dagelijks weer nieuwe initiatieven gestart. In deze paragraaf wordt een aantal nieuwe initiatieven genoemd, zonder te proberen volledig te zijn.

6.4.1 Het Nationaal Cyber Security Centrum zet in op samenwerking

Het NCSC dat in januari 2012 is opgericht, is en blijft actief in nationale en internationale netwerken van overheidsorganisaties en bedrijfsleven. Afgelopen jaar is de samenwerking met diverse partijen uitgebreid.

Het NCSC zet sterk in op samenwerking tussen publieke en private organisaties. Het NCSC participeert momenteel in de Information Sharing and Analysis Center (ISACs) die door het CPNI.NL gecoördineerd worden. Deze samenwerking wordt verder versterkt door aansluiting van de ISACs bij het NCSC. Nieuw voor het NCSC is de intensieve samenwerking met liaisons van diverse organisaties. Hieronder vallen vertegenwoordigers van AIVD, KLPD, Defensie, NFI, OM, OPTA en private partijen.

Naast de oprichting van het NCSC heeft de Nationale Cyber Security Strategie (NCSS) medio 2011 ook geleid tot de oprichting van de Cyber Security Raad. De raad vormde de opmaat voor de oprichting van het NCSC en heeft als taak om de regering en private partijen te adviseren over relevante ontwikkelingen op het gebied van digitale veiligheid. De raad stelt prioriteiten in de aanpak van ICT-dreigingen, bekijkt de behoefte aan nadere Research & Development en kijkt hoe deze kennis vervolgens het beste kan worden gedeeld met de samenwerkende publieke en private partijen.

6.4.2 Een ICT-beveiligingsfunctie harmoniseert beveiliging bij het rijk

Eind 2011 is een verkenning uitgevoerd naar de inrichting van een ICT-beveiligingsfunctie die een geharmoniseerd ICT-beveiligingsbeleid voor het hele Rijk gaat uitvoeren. Deze verkenning is onderdeel van het programma compacte Rijksdienst dat tot doel heeft de overheid kleiner en krachtiger te maken. De verkenning geeft inzicht in de wijze waarop de informatiebeveiligingsfunctie binnen de Rijksdienst is georganiseerd. Ook geeft de verkenning inzicht in welke behoeften er nog zijn en welke nieuwe behoeften ontstaan als gevolg van het inrichten van de compacte Rijksdienst en een ICT-infrastructuur. De verkenning is op moment van schrijven in de beoordelingsfase. Het streven is om in de loop van dit jaar invulling te geven aan de voorgestelde elementen uit de verkenning.

6.4.3 Bestrijding cybercriminaliteit: balanceren tussen samenwerken en afdwingen

Om cybercriminaliteit effectief te kunnen bestrijden, werkt het 'Team High Tech Crime' (THTC) continu aan het verbeteren van de samenwerking met diverse partijen (zoals ICANN, RIPE-NCC en SIDN). Van oudsher zijn dergelijke organisaties niet gewend aan of gediend van overheidsbemoeienis. Het vormgeven van samenwerkingsvormen die voor alle betrokken partijen werkbaar is vraagt daarom een investering van jaren.

Alle betrokken partijen hebben sterk behoefte aan helderheid over de grenzen van wat de politie kan vragen en wat andere partijen kunnen bieden. Een voorbeeld waarmee deze helderheid tot stand komt, is de sommatie van het OM aan RIPE-NCC om IP-ranges te bevriezen. Deze sommatie vond plaats na een rechtshulpverzoek. RIPE-NCC heeft hierna een proefproces aangespannen om uit te vinden of een dergelijk bevel rechtmatig en wettig is. Dit moet op den duur jurisprudentie opleveren zodat alle partijen weten waar ze aan toe zijn.

6.4.4 Electronic Crime Taskforce verbetert bestrijding financiële fraude

Het Korps Landelijke Politiediensten (KLPD), het Landelijk Parket, de banken en het Nederlandse Centre for Protection of the National Infrastructure (CPNI) werken samen in de Electronic Crimes Taskforce (ECTF), ook wel het 'bankenteam' genoemd.

De focus van de ECTF ligt vooral op financiële malware, phishing aanvallen en andere cybercriminaliteit gerelateerde incidenten die gericht zijn op de financiële sector. Deelnemers wisselen informatie uit en verbeteren daardoor de informatiepositie en de analysemogelijkheden, doen voorstellen voor interventies en doen concrete (onderzoeks)voorstellen voor een effectieve bestrijding van cybercriminaliteit. Het ECTF is gehuisvest bij het KLPD.

6.4.5 Gemeentelijke ICT-beveiligingsdienst coördineert beveiligingsonderwerpen

De Vereniging Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) hebben de intentie uitgesproken voor de oprichting van een gemeentelijke ICT-beveiligingsdienst. Deze dienst gaat incidenten bij gemeenten afhandelen en de coördinatie

bij beveiligingsproblemen verzorgen. Daardoor hoeven niet alle gemeenten individueel aan de slag, maar kan dit gemeenschappelijke orgaan deze taak op zich nemen. Het is de bedoeling dat nog voor de zomer een voorstel verschijnt voor het opzetten van de dienst. Daarover moet het VNG-bestuur nog beslissen.

6.4.6 *OPTA kiest voor bredere aanpak bij bestrijding cybercriminaliteit*

Hoewel de OPTA de bevoegdheid heeft om handhavend op te treden door middel van het opleggen van boetes of lasten onder dwangsom of het toepassen van bestuursdwang, is zij van mening dat de aanpak van cybercriminaliteit meer gebaat is bij de inzet van een compleet spectrum van formele en informele toezichts- en opsporingsacties dan bij het alleen opleggen van boetes.

OPTA heeft bovenstaande aanpak in 2010 ontwikkeld en in 2011 verder uitgewerkt. De aanpak richt zich op voorlichting, preventie en publiek-private samenwerking met Internet Service Providers (ISP's) en hostingproviders. Net als in 2010 heeft OPTA in 2011 tientallen malen contact gehad met verschillende partijen met als doel hen te wijzen op hun eigen verantwoordelijkheid ten aanzien van de activiteiten van hun klanten. Dit heeft tot resultaat dat malwareverspreiding nu in veel gevallen in een vroeger stadium wordt opgemerkt en door de partijen zelf wordt gestopt.[91] OPTA past deze aanpak ook toe op spam die verstuurd wordt vanuit Nederland naar het buitenland.

6.4.7 *Interpol zet in op internationale samenwerking*

Nederland participeert al sinds de oprichting in 'Interpol's European Working Party on IT Crime' (EWPITC). Deze samenwerking biedt de mogelijkheid om met veel landen gezamenlijke strategische doelstellingen te formuleren.

Een interessante ontwikkeling vormt ook de toekomstige realisatie van Interpol's Global Complex for Innovation in Singapore. Deze biedt mogelijkheden voor wereldwijde samenwerking op het gebied van cybercriminaliteit, bijvoorbeeld door detachering van liaisons uit Nationale High Tech Crime Units in dit complex.

6.5 Cybersecurityonderzoek en nieuwe methoden

Onderzoeksinstellingen houden zich steeds vaker bezig met onderzoeken die uiteindelijk beogen de informatiebeveiliging te verhogen. De overheid treedt coördinerend op om de initiatieven op elkaar en op de marktbehoefte af te stemmen. Ook het bedrijfsleven ontplooit initiatieven die hieraan kunnen bijdragen. Hieronder staan een viertal voorbeelden van initiatieven die deze verschillende categorieën illustreren.

6.5.1 *De overheid stimuleert cybersecurityonderzoek*

Op initiatief van de ministeries van Veiligheid & Justitie, Binnenlandse Zaken, Defensie en Economische Zaken, Landbouw en Innovatie en in samenwerking met de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) wordt een tender uitgebracht voor cybersecurityonderzoek.[92] Hiervoor is 6,3 miljoen euro beschikbaar. Bedrijven en consortia van kennisinstellingen en bedrijven kunnen hiervoor dit jaar onderzoeksvoorstellen indienen. Er worden trajecten voor langetermijn- en kortetermijnonderzoek ingericht.

De tender sluit aan bij de stimulering van onderzoek zoals genoemd in de NCSS en krijgt vorm binnen het zogenaamde topsectorenbeleid. Het cybersecurityonderzoek maakt deel uit van de security roadmap onder de topsector High Tech Systemen en Materialen[93] en de ICT-roadmap.

6.5.2 *Bedrijven certificeren ontwerpers, ontwikkelaars, testers*

Er is een toenemende aandacht voor het inzetten van ethical hackers bij het testen van de security-aspecten van systemen. Diverse organisaties bieden methoden, best practices en certificeringen voor securitytesters en proberen op deze manier het testen van de beveiliging op een hoger plan te brengen. Een (willekeurig) voorbeeld van een dergelijke organisatie is de Council of Registered Ethical Security Testers (CREST).[94] Zij bieden zowel een certificerings- als een opleidingsprogramma. Dit soort initiatieven heeft tot gevolg dat op langere termijn de weerbaarheid vergroot wordt door het opleveren van producten die vanuit beveiligingsbewustzijn zijn ontwikkeld.

6.5.3 *Kostenmodellen moeten kosten van cybersecurity in kaart brengen*

Diverse onderzoeken hebben geprobeerd de kosten van cybercriminaliteit en cybersecurity in kaart te brengen. Dit inzicht is van belang om een goede afweging te kunnen maken bij het nemen van beschermende maatregelen. Dergelijke onderzoeken krijgen doorgaans behoorlijk wat kritiek te verduren. Soms door de gehanteerde methodiek, soms door de gebruikte data en soms door beide. Het onlangs uitgebrachte rapport van TNO vormt daar een prekend voorbeeld van.[95]

Inzicht in kosten vergt een goede methodiek en een goede vastlegging van de kosten bij de bron. In opdracht van OPTA heeft TU Delft al in 2009 onderzoek gedaan naar een model om de economische kosten van spam en malware te

91. http://jaarverslag2011.opta.nl
92. Zie o.a. http://www.nwo.nl/nwohome.nsf/pages/NWOP_8T3ELR
93. Zie http://www.rijksoverheid.nl/onderwerpen/ondernemersklimaat-en-innovatie/investeren-in-topsectoren
94. Zie http://www.crest-approved.org
95. Zie http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=2&item_id=2012-04-10 procent2011:37:10.0

kunnen benaderen.[96] In het onderzoek is een methodisch raamwerk uitgewerkt om de economische kosten systematisch te kunnen inventariseren en de omvang te kunnen schatten. Verdere ontwikkeling en toepassing van dit raamwerk is gewenst.

6.5.4 De AIVD ondersteunt bij Network Security Monitoring

De AIVD bevordert beveiligingsmaatregelen voor het beschermen van gegevens die van belang zijn voor de nationale veiligheid of voor de instandhouding van het maatschappelijk leven. In dit kader draagt de AIVD door inzet van specifieke expertise op verschillende terreinen bij aan de invulling van de NCSS. Een van de activiteiten is het verkrijgen van inzicht in de aard en omvang van digitale aanvallen die de nationale veiligheid kunnen schaden; het kan hier gaan om digitale spionage door statelijke actoren.

Ook wordt door de AIVD bij specifieke organisaties (binnen overheid en bedrijfsleven) gerichte ondersteuning geleverd bij het monitoren van (informatie)systemen. Dit wordt uitgevoerd door netwerkverkeer van en naar organisaties te onderzoeken op sporen van gerichte digitale aanvallen. Door dit onderzoek kunnen signalen die wijzen op aantasting van beveiligingsmaatregelen worden onderkend en kunnen belangendragers geïnformeerd worden zodat zij correctieve of preventieve maatregelen kunnen treffen. Hierdoor kunnen zij de weerbaarheid van kritieke (informatie)systemen verhogen.

Daarnaast werkt de AIVD aan het versterken en uitbreiden van expertise en (inter)nationale samenwerking op het terrein van onderkennen en tegengaan van geavanceerde digitale aanvallen. Hierbij wordt onder andere samengewerkt met commerciële partijen en universiteiten.

6.6 Krijgsmacht vergroot digitale weerbaarheid

Sinds 1 januari 2012 is binnen het Ministerie van Defensie de 'Taskforce Cyber' operationeel. De 'Taskforce Cyber' werkt langs vier operatielijnen: operatiën (defensief en offensief), inlichtingen, opleiding en training (O&T), en Research and Development (R&D). Uitgaande van de 'Uitwerking visie op cyberoperations' van juni 2012 wordt gewerkt naar de oprichting van een Defensie Cyber Expertise centrum (DCEC) eind 2013 en de oprichting van een Defensie Cyber Commando (DCC) eind 2014.

Nationaal wordt op cybergebied intensief samengewerkt. Vanuit de 'Taskforce Cyber' alsmede namens de Militaire Inlichtingen en Veiligheidsdienst (MIVD) is een liaison geplaatst bij het NCSC.

Internationaal zijn diverse initiatieven gestart voor intensieve samenwerking. Recentelijk is de 'note for joining' voor het Cooperative Cyber Defence Centre of Excellence (CCD COE) getekend. Nederland plaatst deze zomer een juridische officier in de 'policy branch' van het CCD COE in Tallinn. Binnen de NAVO wordt meegedaan aan het 'Multinational Cooperation Development Model 2' (MNCD2), een initiatief van de NATO Consultation, Command and Control Agency (NC3A). In dit initiatief wordt een aantal cyberinstrumenten ontwikkeld. Tevens is de observer status verkregen voor het 'Multinational Experiment (MNE) 7' initiatief van de NATO Allied Command Transformation (ACT). Voor cybersecurity worden met name de tracks 'cyber situational awareness' en 'Legal' gevolgd.

De intensivering cyberinlichtingen die al in 2012 start, heeft invulling gekregen met negen exra functies bij de MIVD. Verder wordt binnenkort een universitair hoofddocent aan de Nederlandse Defensie Academie (NLDA) aangesteld.

96. Bron: 'Damages from internet security incidents', d.d. 10 december 2009, TU Delft

Bijlagen

BIJLAGE 1 > BANDBREEDTES CYBERDREIGINGEN

Om de verschillende dreigingsniveaus in het Cybersecuritybeeld Nederland te bepalen, worden incidenten en dreigingen gewogen tegen de criteria van 'laag', 'midden' en 'hoog'. Daar er in deze bandbreedtes geen harde scheidslijnen voorkomen, kunnen schommelingen ontstaan bij het weergeven en classificeren van gebeurtenissen en trends. Onderstaand de Cybersecuritybeeld Nederland beoordelingscriteria van de cyberdreigingen.

Relevantie van de dreigingen:

Laag

- Er worden geen nieuwe trends of fenomenen onderkend waar de dreiging van uitgaat.
- Er zijn (voldoende) maatregelen beschikbaar om de dreiging te mitigeren (te doen wegnemen).
- Er hebben zich geen noemenswaardige incidenten van de dreiging voorgedaan in de rapportageperiode.

Midden

- Er worden nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat.
- Er zijn (beperkte) maatregelen beschikbaar om de dreiging te mitigeren.
- Incidenten hebben zich voorgedaan buiten Nederland, enkele kleine in Nederland.

Hoog

- Er zijn duidelijke ontwikkelingen waargenomen die de dreiging opportuun maken.
- Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft.
- Incidenten hebben zich voorgedaan in Nederland.

BIJLAGE 2 > CASUÏSTIEK

Er zijn in deze rapportageperiode verschillende casussen geweest die betrekking hebben op cybersecurity-incidenten. Hieronder worden enkele van deze casussen benoemd zoals voorbeelden van ICT-problemen en -kwetsbaarheden in kritische infrastructuren en welke impact dergelijke incidenten kunnen hebben. Daarnaast komen SCADA-systemen en voorbeelden van incidenten met malwarebesmettingen aan bod. Lektober, waarbij verschillende lekken zijn blootgelegd in websites, onder andere bij de overheid, wordt ook toegelicht. Als laatste worden voorbeelden genoemd van het lekken van persoonlijke en gevoelige gegevens, die door middel van hacking zijn verkregen.

Kwetsbaarheden in infrastructuur

Er bestaan verschillende kritische infrastructuren, zoals watervoorziening, telecomvoorziening en elektriciteitsnet. Incidenten met dergelijke infrastructuren kunnen een grote impact hebben op de maatschappij. Hieronder staan verschillende voorbeelden van incidenten van deze vorm.

Vodafone

Een brand in een bedrijfspand van Vodafone met netwerkapparatuur heeft er op 30 april 2012 voor gezorgd dat Vodafoneklanten in de Randstad niet meer mobiel konden bellen, sms-en of internetten. Ook 'Machine-to-Machine'-communicatie werd getroffen zoals TomTom Live en meetstations van het KNMI. Onder de getroffenen bevond zich ook de Rijksoverheid die voor mobiel bellen voor het grootste deel van Vodafone afhankelijk is.

Dit incident maakte duidelijk dat fysieke incidenten bij kritische infrastructuren, zoals de brand bij Vodafone, een grote impact kunnen hebben op de beschikbaarheid van digitale dienstverlening. Bij het inrichten van een Information Security Management System (ISMS) is het belangrijk om ook met dergelijke fysieke incidenten rekening te houden.

Daarnaast is het ook opvallend dat de landelijke impact van dit incident groter is dan een brand in een middelgrote onbemande netwerkcentrale. Aan deze netwerkcentrale hingen 700 zendmasten die door de brand niet meer functioneerden. Het opvangen van de verkeersstroom door andere masten veroorzaakte extra verkeer en storingen in andere delen van het netwerk. Een relatief klein knooppunt bleek dus een Single Point of Failure voor een groot gebied te vormen. Dit is zorgwerkend vanuit het volgende gezichtspunt: een dergelijk object kan een eenvoudig doelwit zijn van cybercriminelen (hetzij door een fysieke of door een cyberaanval), die met een kleine inspanning een groot effect kunnen bereiken.

Ten slotte is een discussie ontstaan over de continuering van de dienstverlening. Vodafone bood geen uitwijk- of back-upmogelijkheden.

Stroomstoring Rotterdam

In de eerste maanden van 2012 kampte de gemeente Rotterdam met vier forse stroomstoringen. In een geval kwamen vijftigduizend huishoudens zonder stroom te zitten. De storingen werden veroorzaakt door kortsluitingen, werkzaamheden en defecten, en hadden volgens de betreffende energiebedrijven geen relatie met elkaar. De uitval had gevolgen voor burgers en verschillende organisaties, die noodgedwongen hun werkprocessen moesten staken. In sommige gevallen moesten organisaties ontruimd worden. Het had ook consequenties voor het metro- en tramverkeer dat stilviel en voor het wegverkeer omdat stoplichten niet meer werkten. Rotterdam The Hague Airport en het Erasmus Medisch Centrum vielen bij een incident ook onder het getroffen gebied, maar bleken probleemloos over te kunnen schakelen op noodvoorzieningen. Tijdens verschillende stroomstoringen was het alarmnummer 112 moeilijk tot niet bereikbaar.

Een van de stroomstoringen vond plaats tijdens de uitval van Vodafone. Het niet beschikbaar zijn van de mobiele telefoonverbindingen, verhinderde netbeheerder Stedin om informatie te vergaren en daardoor werd het herstel vertraagd.

Prorail, ICT-storing

Op 22 maart 2012 besloot de verkeersleiding van de NS om het treinverkeer stil te leggen. Hiertoe werd besloten nadat geen zicht bleek op de treinenloop als gevolg van een serie gerelateerde ICT-storingen. De storingen traden op na het opstarten van een uitwijkprocedure als gevolg van de ontdekking van een defect hardwarecomponent. Hoewel de verkeersleidingsystemen meervoudig redundant zijn uitgevoerd, bleek de automatische schakeling tussen deze systemen niet goed te werken. Op het moment dat werd overgeschakeld naar een ander systeem, bleef de software hangen op een systeem dat niet aanwezig was. Dit probleem had uiteindelijk grote gevolgen voor de treinenloop.

Dit incident bevestigt nogmaals dat de (infrastructurele) voorzieningen in onze samenleving steeds meer afhankelijk zijn van ICT en dat verstoringen daarin grote gevolgen hebben. Het voorbeeld illustreert ook het belang van het structureel en uitgebreid testen van uitwijkprocedures als onderdeel van 'business continuity plans'.

ICS/SCADA

Een anonieme twitteraar publiceerde rond de jaarwisseling een aantal berichten waarin hij waarschuwde voor onvoldoende beveiliging van ICS/SCADA-systemen. Omdat deze meldingen slechts bestonden uit het noemen van IP-adressen, zonder verdere duiding, was de analyse ervan niet eenvoudig. Het bleek dat het in een klein deel van de gevallen inderdaad om ICS/SCADA-systemen ging. De rest van de adressen betrof andere ICT-systemen die in de meeste gevallen ook geen kwetsbaarheden bevatten.

In februari 2012 maakte de publieke omroep een uitzending over kwetsbaarheden in ICS/SCADA-systemen van een Nederlandse gemeente. Dit systeem wordt door een leverancier namens de gemeente geleverd en beheerd. Het betreft een systeem voor rioolbemaling waarbij een eenvoudig te raden combinatie van gebruikersnaam en wachtwoord werd gebruikt. De pers meldde dat deze kwetsbaarheid zou kunnen worden gebruikt om het Deltagebied te laten leegstromen. Dit is niet gebeurd.

Verder ontving het NCSC in februari 2012 meldingen over ICS/SCADA-systemen van twee zwembaden en een sporthal. Deze systemen waren via het internet te benaderen door onbevoegden. Zij zouden dan mogelijk deze installaties kunnen bedienen. Mede door deze meldingen werd duidelijk dat de vaak gebrekkige beveiliging van ICS/SCADA-systemen in deze rapportageperiode voor het eerst uitgebreid in de schijnwerpers stond.

Verspreiding malware via veelbezochte websites

In de verslagperiode is enkele malen ontdekt dat malware is verspreid via veelbezochte websites. Voorbeelden hiervan zijn: In een geval werd de malware rond het middaguur verspreid via www.nu.nl, juist op de dag dat er een belangrijk nieuwsfeit speelde, namelijk het busongeluk met schoolkinderen. In twee uur tijd werden ongeveer 1 miljoen computers blootgesteld aan de malware. Hieronder wordt dieper op dit voorbeeld ingegaan. Een soortgelijk incident was de besmetting via de webshop van een speelgoedketen. In een ander geval vond de blootstelling aan malware plaats via de website van een internetjournalist.

Deze incidenten wijzen erop dat internetcriminelen zich bewust richten op populaire websites om in korte tijd een groot aantal computers te besmetten.

NU.nl

Hackers zijn er 14 maart 2012 in geslaagd om een kwaadaardige code op de populaire nieuwssite NU.nl te plaatsen. Dit gebeurde nadat inloggegevens van het cms van een van de medewerkers van NU.nl in verkeerde handen raakten.[97] Het doel van de aanval was om bezoekers van de website te besmetten met malware. Bezoekers die tussen 11.30 en 13.45 uur de website bezochten, liepen risico op besmetting. Onderzoek wees uit dat naar schatting, 100.000 systemen zijn getroffen.[98]

Een van de voorwaarden om getroffen te worden, was de aanwezigheid van verouderde software op het systeem van het mogelijke slachtoffer. De kwaadaardige code maakte namelijk gebruik van kwetsbaarheden in bepaalde oude versies van Adobe Reader en Java. Deze aanvalstactiek staat bekend als een drive-by-download en is niet nieuw. Het is wel uitzonderlijk dat een van de bestbezochte Nederlandse websites van een dergelijke aanval onderdeel uitmaakt.[99]

Op de systemen van de slachtoffers werd Sinowal banking-malware geïnstalleerd. Deze malware is er onder andere op gericht om banktransacties te manipuleren en inloggegevens voor websites te onderscheppen. De gebruikte Sinowal-variant werd op het moment van besmetting door geen enkele virusscanner gedetecteerd. Daarnaast werd een zogenaamde rootkit gebruikt om de herkenning en het verwijderen van de malware te voorkomen. De anti-virustool HitmanPro van het Nederlandse bedrijf Surfright was een dag na de infectie de enige virusscanner die de malware in zijn geheel kon verwijderen.

Ook bij de overheidspartners van het NCSC bleek dat systemen veelal niet voorzien waren van alle updates en dus kwetsbaar waren voor deze aanval. Een groot aantal verschillende partners rapporteerden tientallen tot honderdtallen infecties. Het NCSC heeft aan haar partners instructies beschikbaar gesteld voor het herkennen en verwijderen van mogelijke infecties.

Dit incident maakt het belang van het bijhouden van securitypatches weer eens duidelijk. Het NCSC heeft ruim voor het NU.nl-ncident al in haar advisories voor beide misbruikte kwetsbaarheden gewaarschuwd en maatregelen geadviseerd. Het is duidelijk dat virusscanners alleen niet voldoende zijn om dreigingen af te slaan. Dit incident maakt ook het belang van beveiliging van websites en webapplicaties duidelijk.

97. http://www.nu.nl/media/2763447/korte-tijd-malware-verspreid-via-nunl.html
98. http://blog.fox-it.com/2012/03/16/post-mortem-report-on-the-sinowallnu-nl-incident
99. http://www.alexa.com/topsites/countries/NL

Onbeveiligde webapplicaties

Lektober

Webwereld[100] had oktober 2011 uitgeroepen tot 'Lektober'. Dit hield in dat zij elke werkdag een informatielek van een website of overheidsdienst openbaarde. Uiteindelijk zijn 29 lekken openbaar gemaakt. De belangrijkste publicatie betrof een lek in vijftig gemeentelijke websites.[101] In de meeste gevallen ging het om oude websites en in sommige gevallen om actieve websites. Door zwakheden in die websites bleek DigiD authenticatie te omzeilen. Andere Lektobermeldingen waren het lekken van vertrouwelijke informatie, vaak via SQL-injection. Deze lekken betroffen veelal websites buiten het Rijksoverheiddomein.

Als reactie op dit lek had de minister van Binnenlandse Zaken en Koninkrijksrelaties een brief aan de Tweede Kamer gestuurd. Hierin liet hij weten dat de getroffen gemeentes per direct werden afgesloten van DigiD, dat zij hun beveiliging op orde moesten brengen voordat tot heraansluiting kon worden overgegaan en dat op lange termijn alle DigiD-aansluitingen aan een beveiligingsnorm moeten voldoen die jaarlijks getoetst wordt. De brief geeft aan dat de beveiligingsnorm door NCSC wordt opgesteld.

Naar aanleiding hiervan zijn door Logius, in samenwerking met het NCSC, richtlijnen opgesteld. Hiermee zijn de gemeenten ondersteund bij het op orde krijgen van de beveiliging van hun webapplicaties. Deze richtlijnen bevatten een stappenplan en een checklist. De checklist bevat de belangrijkste punten waar een webapplicatie en de omliggende omgeving minimaal aan moeten voldoen om een veiligheidstoets te kunnen doorstaan. Het NCSC heeft de veiligheidstoetsen van de getroffen gemeenten aan de hand van deze checklist beoordeeld en daar waar nodig verbeteringen voorgesteld of geëist. Door deze procedure hebben deze gemeenten hun beveiliging aanzienlijk verbeterd. In sommige gevallen ging dit gepaard met het volledig vernieuwen van de hard- en software van de servers.

Hoewel bijna alle problemen van de checklist de revue zijn gepasseerd, zijn er wel een aantal tekortkomingen uitgesprongen. Vooral het niet up-to-date zijn van software-componenten (besturingssysteem, webserver, database-managementsysteem, ontwikkelsoftware, et cetera) en de netwerkarchitectuur waren voor verbetering vatbaar. Bij de getroffen gemeenten zijn deze problemen nu opgelost.

Op dit moment worden de eerste partijen getoetst op basis van de 'DigiD-norm' die gebaseerd is op een verzameling richtlijnen die door het NCSC zijn opgezet. De verwachting is dat deze toetsing soortgelijke tekortkomingen aantoont zoals bij de toetsing van de getroffen gemeenten.

Openbaarmakingen van gegevens, verkregen door hacking

In de afgelopen periode zijn er verschillende voorbeelden geweest van openbaarmaking van persoonlijke en gevoelige gegevens op internet. Deze gegevens waren verkregen via hacking. Hieronder volgen enkele voorbeelden uit de afgelopen periode.

Leden van hackersgroep Anonymous publiceerden, via Wikileaks, rond de kerstdagen de gegevens van vele duizenden klanten van het Amerikaanse beveiligingsbedrijf Stratfor. Dit bedrijf levert intelligencegegevens aan overheden. Onder de gepubliceerde klantgegevens bevonden zich ook Nederlandse klanten.

Behalve actiegroepen publiceerden ook hackers zonder hacktivistische motieven, gegevens op internet. Zo verschenen klantgegevens op het internet van diverse bedrijven, waaronder Youporn, Babydump en Humannet. Ook werden IP-adressen van mogelijk lekke systemen in de openbaarheid gebracht.

Het publiceren van gegevens op het internet, die via hacking zijn verkregen, is een vrij nieuw fenomeen. Behalve het in verlegenheid brengen van de eigenaar van de gegevens lijken deze publicaties geen ander doel. Dit neemt niet weg dat het een schending is van de privacy voor de getroffenen. Een bekend voorbeeld van het ogenschijnlijk openbaren van gegevens, die door hacking zijn verkregen, is de hack bij KPN.

KPN

Op 27 januari 2012 meldde KPN bij het NCSC een inbraak in haar internetsystemen. Een aanvaller heeft op 16 januari 2012 diep in de infrastructuur kunnen doordringen en heeft daarbij op honderden servers toegangsrechten op het hoogste niveau gekregen. Deze servers werden gebruikt voor internetdiensten, routering van internet gebaseerde diensten en opslag van (klant)informatie. Het computersysteem raakte beschadigd, omdat er kwaadaardige software op was geplaatst en de normale beveiliging van KPN werd daarmee omzeild.
De hacker heeft ook rechten gehad op de DNS (Domain Name Server) systemen en heeft gebruikersrechten gehad op een van de routers. Daarmee had hij tijdelijk de routering van het internetverkeer van de consumentenklanten van KPN kunnen beïnvloeden. Aangezien via deze routering ook de Voice over IP-dienstverlening loopt en bijvoorbeeld ook de 112-oproepen van klanten via VOIP, werd de dreiging serieus genomen.

Om de dreiging weg te nemen, heeft KPN een groot aantal KPN-systemen geïsoleerd, geschoond en opnieuw geïn-

100. Webwereld (2011, 1)
101. Webwereld (2011, 2)

stalleerd. Deze activiteiten waren op 3 februari volledig afgerond. Nadat op 10 februari op internet schijnbare klantgegevens door de vermeende daders werden gepubliceerd, nam KPN direct rigoureuze maatregelen om de gegevens van haar klanten te beschermen. Zo werd de inkomende e-mail geblokkeerd. Bij analyse van de 'klantgegevens' bleek dat deze echter niet afkomstig waren van de inbraak bij KPN. De klantgegevens waren eerder buitgemaakt bij een inbraak op de webshop van een leverancier van babyartikelen. Uit deze lijst waren slechts de gegevens van KPN-klanten overgenomen en op internet gepubliceerd.

Het NCSC monitorde de mogelijk bredere gevolgen dan alleen de technische kwestie bij KPN en heeft de coördinatie tussen de verschillende overheidspartijen op zich genomen. Hierbij lag de nadruk op de mogelijke gevolgen voor de (Rijks)overheid, de nationale veiligheid en het internetverkeer. Er zijn geen bewijzen dat de hacker de routering van het internetverkeer daadwerkelijk heeft aangepast. Door tijdigheid van de maatregelen en samenwerking tussen diverse partijen is de nationale veiligheid niet in gevaar geweest. De minister van Veiligheid en Justitie heeft de Tweede Kamer op 14 februari geïnformeerd over deze kwestie .

De politie heeft op 20 maart een 17-jarige jongen aangehouden die wordt verdacht van de hack. De nationale recherche volgde wekenlang zijn sporen op internet. De verwachting is dan ook dat nadere gegevens over de modus operandi in de loop van het opsporingsonderzoek bekend zullen worden. Inmiddels is de jongen weer op vrije voeten gesteld, onder voorwaarde dat hij offline blijft.

BIJLAGE 3 > KWETSBAARHEDEN EN INCIDENTEN AFGEHANDELD DOOR NCSC

Het NCSC (en voorheen GOVCERT.NL) ondersteunt overheden en organisaties in vitale sectoren bij het afhandelen van incidenten op gebied van ICT-veiligheid. In die rol worden bij NCSC incidenten gemeld en worden incidenten en kwetsbaarheden ook door het NCSC zelf geïdentificeerd, bijvoorbeeld op basis van monitoring.[102]

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 Govcert 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 heeft plaatsgevonden. 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.

Daarnaast acteert NCSC op verzoek van internationale partijen met name richting Internet Service Providers 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'.

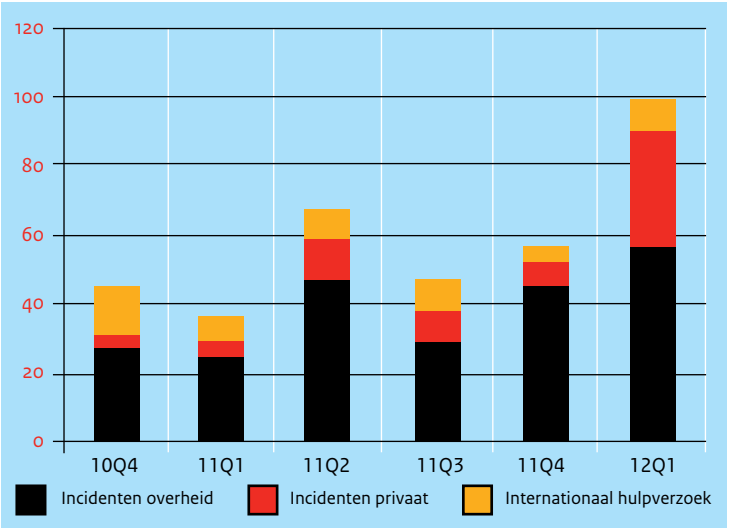
Aantallen afgehandelde incidenten per doelgroep

Een analyse van de incidenten die door het NCSC zijn afgehandeld, laat een aantal ontwikkelingen zien. Zo is een sterke stijging in het aantal incidenten te zien van NCSC per 1 januari 2012. Dit wordt met name veroorzaakt door het aantal afgehandelde incidenten dat in de private sector speelde en is te verklaren doordat NCSC in tegenstelling tot GOVCERT.NL naast de overheid expliciet ook private partijen bedient.

Tabel 6. Door NCSC en GOVCERT.NL afgehandelde incidenten per doelgroep

Actie NCSC	Incidenten overheid	Incidenten privaat	Internationaal hulpverzoek	Totaal
10Q4	28	3	14	45
11Q1	25	4	8	37
11Q2	47	12	8	67
11Q3	29	9	9	47
11Q4	46	6	5	57
12Q1	57	33	9	99
Totaal	**232**	**67**	**53**	**352**

Figuur 12. Door NCSC en GOVCERT.NL totaal afgehandelde incidenten per soort actie

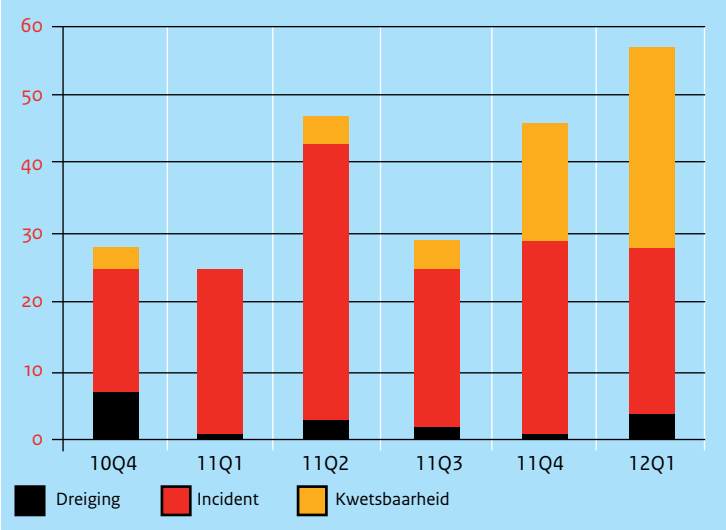


102. Het NCSC registreert incidenten niet op het niveau van individuele systemen of organisaties, maar geclusterd per melding of identificatie. Daarom kan de melding van meerdere kwetsbare systemen als een incident geregistreerd zijn.

Tabel 7. Door NCSC en GOVCERT.NL afgehandelde incidenten per incidentsoort per kwartaal

Periode	Dreiging	Aanval	Kwetsbaarheid	Totaal
10Q4	7	18	3	28
11Q1	1	24		25
11Q2	3	40	4	47
11Q3	2	23	4	29
11Q4	1	28	17	46
12Q1	4	24	29	57
Totaal	18	157	57	232

Figuur 13. Door NCSC en GOVCERT.NL totaal gemelde incidenten per type



Tabel 8. Door NCSC en GOVCERT.NL afgehandelde type incidenten per periode

Type incident	Percentage 10-2011 t/m 03-2012	Percentage 04-2011 t/m 09-2011
Websitekwetsbaarheid	35%	9%
Malware-infectie	17%	51%
Uitlekken van informatie	11%	8%
Onbeschermd of kwetsbaar systeem	8%	0%
Phishing	7%	7%
dDoS-aanval	6%	3%
Aanvalsdreiging	5%	7%
Poging tot hacken	5%	1%
Overige	6%	14%

Aard van incidenten bij de overheid

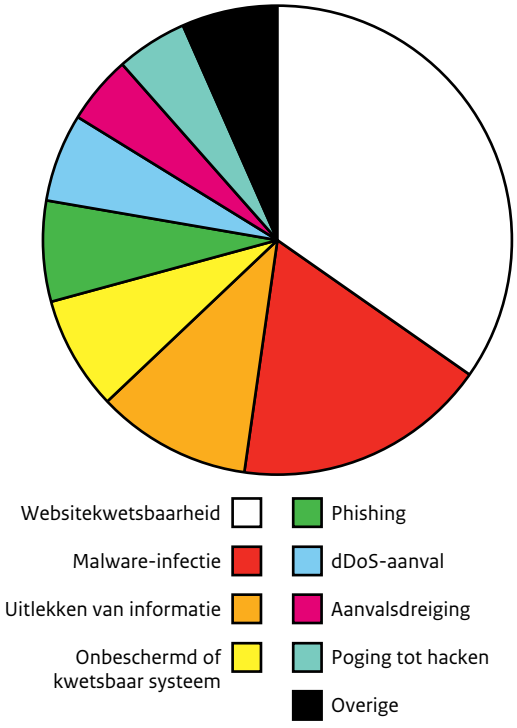
Een analyse van de incidenten die door het NCSC zijn afgehandeld bij overheden, laat in de laatste kwartalen ook een stijging van het aantal incidenten zien. Een nadere specificatie naar aanvallen, dreigingen en kwetsbaarheden toont dat de stijging niet voor alle incidentsoorten geldt. De stijging wordt vooral veroorzaakt door een sterke toename in het aantal afgehandelde kwetsbaarheden.

De oorzaak hiervan moet niet gezocht worden in het feit dat ICT-systemen sinds kort een grotere mate van kwetsbaarheid vertonen. Op basis van de ervaringen uit het verleden kan worden aangenomen dat veel systemen al langer kwetsbaar waren, maar dat de toegenomen aandacht hiervoor bij beveiligingsonderzoekers maakt dat deze kwetsbaarheden meer aan het licht komen. De melding van kwetsbaarheden door onderzoekers met goede intenties maakt dat deze kwetsbaarheden kunnen worden weggenomen en de weerbaarheid van systemen kan worden verhoogd.

Nadere detaillering van de typen incidenten

Wanneer gekeken wordt naar een nadere detaillering van de incidenten bij overheden, dan wordt duidelijk dat het aantal websitekwetsbaarheden is toegenomen. Daarnaast maken malware-infecties een groot deel uit van de afgehandelde incidenten. Samen zijn deze twee typen incidenten goed voor iets meer dan de helft van de afgehandelde incidenten. Uitgelekte (persoons)informatie en onbeschermde/kwetsbare systemen zijn daarnaast ook veel voorkomende typen incidenten.

Figuur 14. Percentage type incidenten periode 10-2011 t/m 03-2012



BIJLAGE 4 > AFKORTINGEN

A	
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
APT	Advanced Persistent Threat
B	
BAVO	Beveiligingsafstemming Vitaal en Overheid
BGP	Border Gateway Protocol
BIR	Baseline Informatiebeveiliging Rijksoverheid
BOF	Bits of Freedom
BYOD	Bring Your Own Device
C	
CA	Certificate Authority
CBP	College Bescherming Persoonsgegevens
CBS	Centraal Bureau voor de Statistiek
CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CMS	Content Management Systeem
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CREST	Council for Registered Ethical Security Testers
CSBN	Cybersecuritybeeld Nederland
CSI	Computer Security Institute
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
D	
DCS	Directie Cyber Secrurity (directie binnen het NCTV)
DNS	Domain Name Service
DNSSEC	Domain Name System Security Extensions
dDos	distributed denial-of-service (aanval)
DoS	Denial of Service
E	
EC	Europese Commissie
ECP	Electronic Commerce Platform Nederland
EDP	Electronic Data Processing
EMV	Europay MasterCard Visa
F	-
G	-
H	-
I	
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
ICS/SCADA	Industrial Control Systems/Supervisory Control And Data Acquisition
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
J	-
K	
KING	Kwaliteitsinstituut Nederlandse Gemeenten
KLPD	Korps Landelijke Politiediensten
KWAS	Kwetsbaarheids Analyse Spionage
L	-
M	
MBR	Master Boot Record
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
N	
NCSS	Nationale Cyber Security Strategie
NCSC	Nationaal Cyber Security Centrum (onderdeel van de Directie Cyber Security)
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NLDA	Nederlandse Defensie Academie
NVB	Nederlandse Vereniging van Banken
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
O	
OM	Openbaar Ministerie
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
OWASP	Open Web Application Security Project
P	
PaaS	Platform as a Service
PKI	Public Key Infrastructure
Q	-
R	
RFID	Radio-frequency identification
S	
SaaS	Software as a Service
SOHO	Small Office Home Office
SSL	Secure Socket Layer
T	
THTC	Team High Tech Crime
TLD	Top Level Domain
TNS/NIPO	Nederlands Instituut voor de Publieke Opinie
TNO	Toegepast Natuurwetenschappelijk Onderzoek
U	
UMTS	Universal Mobile Telecommunications System
V	
VNG	Vereniging van Nederlandse Gemeenten
W	-
X	-
Y	-
Z	-

BIJLAGE 5 > BEGRIPPENLIJST

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 of CDMA genoemd. 3G heeft voordelen voor beveiliging en communicatiesnelheid ten opzichte van 2G.

APT
Een Advanced Persistence 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.

Beveiligingsafstemming
Vitaal en Overheid: Het plan Beveiligingsafstemming Vitaal en Overheid (BAVO) handelt over de afstemming van de interne beveiligingsmaatregelen van een bedrijf uit een van de organisaties uit de vitale sectoren met de op de beveiliging gerichte maatregelen van de gemeente, de regiopolitie en eventueel andere partners.

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.

Bluetooth
Bluetooth is een standaard voor draadloze communicatie voor het uitwisselen van gegevens over korte afstanden, gespecificeerd door Ericsson in 1994.

Border Gateway Protocol (BGP)
Border Gateway Protocol is het belangrijkste routeringsprotocol van het internet: het definieert de manier waarop informatie over netwerkroutes tussen netwerken wordt uitgewisseld.

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.

Card Verification Value (CVV)/Card Verification Code (CVC)
De CVV of CVC is een beveiligingsmaatregel die fraude met credit- of debetkaarten moet tegengaan.

Certificaat
Zie Secure Sockets Layer-certificaat.

Certificate Authority (CA)
Een certificate authority is, in een PKI-stelsel, een organisatorisch verband dat wordt vertrouwd om certificaten te maken (genereren), toe te wijzen en in te trekken.

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.

Common Vulnerabilities and Exposures (CVE)
CVE is een unieke gemeenschappelijke identificatie van publiekbekende informatiebeveiligingskwetsbaarheden.

Computer Emergency Response Team (CERT)
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.

Computer Network Attack (CNA)
Het vernielen van systemen om zo het systeem zelf, de data die zich erin bevindt of de processen die ermee aangestuurd worden, te verstoren of te vernielen.

Computer Network Exploitation (CNE)
Het binnendringen van digitale systemen om zo de informatie die daarin zit of meeverstuurd wordt, te verkrijgen.

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.

Data breach/datalek
Het onopzettelijk naar buiten komen van vertrouwelijke gegevens.

Denial of Service (DoS), Distributed Denial of Service (dDoS)
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.

Derde partijenregel
Analoog aan de in het verkeer tussen inlichtingen- en veiligheidsdiensten gehanteerde regel dat gegevens die men van elkaar ontvangt alleen voor eigen gebruik mogen worden aangewend en niet zonder vooraf verkregen toestemming van de verstrekkende dienst aan derde partijen mogen worden verstrekt (ook wel aangeduid als derdelandregel).

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.

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 enige andere fysieke medium waar informatie op weergegeven kan zijn.

Domain Name System (DNS)
DNS is het systeem dat internetdomeinnamen koppelt aan IP-adressen en omgekeerd. Zo staat het adres 'www.ncsc.nl' bijvoorbeeld voor IP-adres '62.100.52.109'.

Do-not-track (DNT)
Een mogelijkheid die geboden wordt door moderne browsers om te voorkomen dat iemands surfgedrag via cookies door derde partijen wordt gevolgd.

Dreiging
Het Cybersecuritybeeld definieert **doel** en **dreiging** als volgt:
- **Het hogere doel** (intentie) kan zijn het verstevigen van de concurrentie positie; 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, cybercriminaliteit en indirecte verstoringen.

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.

Europay Mastercard Visa (EMV)
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.

General Packet Radio Service (GPRS)
GPRS is een techniek waarmee over een bestaand gsm-netwerk mobiele data verstuurd kan worden.

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.

Global Positioning System (GPS)
Een plaatsbepalingssysteem op basis van satellieten met een nauwkeurigheid tot op enkele meters. GPS wordt onder andere gebruikt voor navigatie.

Global System for Mobile Communications (GSM)
Gsm is een standaard voor digitale mobiele telefonie. Gsm wordt beschouwd als de tweede generatie mobiele telefoontechnologie (2G).

Hacker
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.

HyperText Markup Language (HTML/HTML5)
HTML is een opmaaktaal voor de specificatie van documenten, voornamelijk bedoeld voor webpagina's.

Industrial Control Systems (ICS)/ Supervisory Control And Data Acqusition (SCADA)
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.

Internet Protocol (IP)
Protocol dat zorgt voor adressering van datapakketten, zodat ze bij het beoogde doel aankomen.

Internet Service Provider (ISP)
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.

Informatie
Een verzameling van gegevens (met of zonder context) opgeslagen in gedachten, in geschriften (op bijv. 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).

Kwetsbaarheid
Een zwakke plek in hardware of software, die kan worden misbruikt voor ongewenste activiteiten.

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.

Man-in-the-middle-aanval (MiTM)
Aanval 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.

Meldplicht
In geval van gegevensverlies en integriteitschending van informatiesystemen moet de eigenaar van dit systeem dit melden bij de nationale toezichthouder.

Network Address Translation (NAT)
Een manier om IP-adressen te herbruiken. Een tijdelijk antwoord op het opraken van IP-adressen. Zorgt er mede voor dat systemen buiten een organisatie niet direct bereikbaar zijn.

Merking
Aanduiding die een bepaalde wijze van behandelen van bijzondere informatie aangeeft.

Open Web Application Security Project (OWASP)
OWASP is een not-for-profit wereldwijde organisatie, gericht op het verbeteren van de beveiliging van applicatiesoftware.

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.

Payment Card Industry (PCI) compliance
De Payment Card Industry Data Security Standard (PCI DSS) is een informatiebeveiligingsstandaard voor organisaties die kaarthouderinformatie verwerken voor debit-, credit-, e-purse, GEA- en BEA-kaarten.

Personal Digital Assistant (PDA)
Een PDA is een mobiel apparaat dat functioneert als een persoonlijke informatiemanager.

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 wat in het Engels identity theft wordt genoemd; het stelen van iemands identiteit.

Public Key Infrastructure (PKI)
Een Public Key Infrastructure 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**'. (Zie Bijlage 1 voor de duiding).

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 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.

Secure Sockets Layer (SSL)/SSL-certificaat
Een 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.

Shimmen
Een aanvalsmethode op chipkaarten, waarbij de communicatie tussen terminal en chipkaart wordt afgeluisterd en eventueel gemanipuleerd.

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.

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.

Staatsgeheim
Bijzondere informatie waarvan de geheimhouding door het belang van de Staat of haar bondgenoten wordt geboden.

Stg. Confidentieel
Indien kennisnemen door niet-gerechtigden schade kan toebrengen aan het belang van de Staat of haar bondgenoten.

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.

Token
Een fysiek apparaat dat een geautoriseerde gebruiker van computerdiensten helpt bij het vaststellen van de identiteit van die gebruiker.

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.

Universal Mobile Telecommunications System (UMTS)
Zie 2G/3G.

Universal Serial Bus (USB)
Specificatie van een standaard van de communicatie tussen een apparaat, in veel gevallen een computer, en rand-apparatuur.

Verwerven
Het verzamelen van informatie en inlichtingen in binnen- en buitenland van cybersecurity-ontwikkelingen en -incidenten vormt de basis voor het maken van gedegen dreigingsanalyses.

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.

Voorkomen
In lijn met de internationale ontwikkelingen ligt de focus van de Nederlandse overheid steeds meer op het voorkomen van cybercriminaliteit en cybersecurityincidenten.

Verdedigen
Staat, rechtsorde en (vitale onderdelen van) de Nederlandse samenleving dienen optimaal te worden beschermd tegen cyberdreigingen of incidenten.

Voorbereiden
De Nederlandse samenleving dient zich bewust te zijn van de mogelijkheidvan een cyberdreiging, aanval en/of incident en dient voorbereid te zijn op de (mogelijke) gevolgen ervan.

Vervolgen
Het opsporen, vervolgen en berechten van personen die verdacht worden van het plegen van cybercriminaliteit, of de voorbereiding daarvan, zijn essentiële onderdelen van cybercrimebestrijding en het verhelpen van incidenten.

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.

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.

Colofon

Uitgave
Nationaal Cyber Security Centrum, Den Haag | Juni 2012

Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

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 expertise en advies, respons 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.

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Juni 2012