Rijksoverheid

Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010

Wanneer is iets een trend?
In dit rapport wordt onder een trend verstaan: (een beschrijving van) het verloop van een bepaalde macro-ontwikkeling op langere termijn. De tijdshorizon die hierbij is aangehouden, is drie tot vijf jaar. Trends hebben strategische impact op Nederland, afgemeten aan het maatschappelijk effect. De trends zijn waar mogelijk gebaseerd op specifieke en aantoonbare data, hoewel dat voor sommige onderwerpen, zoals digitale spionage of cyberwarfare lastig blijkt te zijn, gezien de heimelijke aard van deze fenomenen.

Hoe zijn de trends bepaald?
De trends zijn bepaald op basis van bestaande trendrapportages van overheidsdiensten (zie laatste pagina binnenzijde omslag voor betrokken organisaties uit overheid, wetenschap en bedrijfsleven). Selectie en verdere duiding van de meest relevante trends heeft plaatsgevonden in drie expert-sessies. Ter aanvulling van deze bronnen is literatuuronderzoek uitgevoerd en zijn interviews met experts gehouden.

Waar richt het Trendrapport zich op?
Zoals de titel aangeeft, richt het rapport zich op trends op het gebied van cybercrime en digitale veiligheid. Maar wat is cybercrime? En wat wordt verstaan onder digitale veiligheid?

Cybercrime
Onder cybercrime wordt verstaan: "Elke strafbare gedraging voor de uitvoering van cybercrime waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is." De term 'geautomatiseerde werken' slaat hierbij niet alleen op computers, maar bijvoorbeeld ook op mobiele telefoons, creditcards en andere vormen van geavanceerde technologie. Deze definitie is gebaseerd op de definitie van het KLPD, met dien verstande dat ook cyberwarfare, illegaal gebruik van internet om politieke redenen en digitale spionage binnen de scope van dit Trendrapport vallen.

Digitale veiligheid
Digitale veiligheid is het verzamelbegrip voor een betrouwbare en veilige ICT-omgeving: voorkomen en bestrijden van misbruik en het herstel ervan. Binnen de scope van dit rapport vallen alle verstoringen op deze ICT-omgeving. De nadruk ligt echter op bewuste aanvallen. Veiligheid staat voor zowel de feitelijke veiligheid (aantallen incidenten, schade, etc.) als de perceptie ervan (veiligheidsgevoelens).

Meer dan internet alleen
Als het gaat over cyber of cyberspace, dan wordt hier niet alleen het internet bedoeld, maar alle ICT. Ook vallen in deze categorie alle niet met internet verbonden netwerken of andere digitale apparaten, zoals USB-sticks en software in energiemeters of in andere apparaten.

Rijksoverheid

Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010

Inhoudsopgave


Kaarten
Foto's
iTunes
Klok
vrijdag
10
Agenda
Weer
23°
Calculator
App Store
iPod
Mail
VM TV Gids
Contacten
Instellingen
Aandelen
SMS
Safari
Tekst

Hoofdtrends

Dit is het eerste Nationaal Trendrapport Cybercrime en Digitale Veiligheid (hierna Trendrapport). Het Trendrapport heeft als doel de belangrijkste trends op het gebied van cybercrime en digitale veiligheid te bundelen en in verband met elkaar te brengen. De trends zijn gebaseerd op bestaande rapportages van onder meer de KLPD, NCTb, AIVD en MIVD, OPTA en GOVCERT.NL en is aangevuld met de inzichten van een brede groep van experts. Het rapport kent een strategisch en beleidsarm karakter. In het rapport zijn in de verschillende hoofdstukken trends beschreven, die samengevat kunnen worden in de volgende hoofdtrends:

Cybercriminaliteit wordt geavanceerder en gerichter

Hightech cybercriminaliteit is zeer aantrekkelijk. Het kan namelijk met een beperkte investering snel winstgevend zijn, terwijl de pakkans laag is. Hightech cybercriminelen lopen voorop in het verbeteren van aanvalsmethoden om hun aanvallen minder zichtbaar en gerichter te maken. Cybercriminelen zijn goed georganiseerd en hebben specialisaties die zij als dienstverlening aanbieden. Zij voeren hun aanvallen uit in tijdelijke samenwerkingsverbanden die zij op internetfora aangaan.

De dreiging van digitale spionage neemt toe

Digitale spionage vormt een onderdeel van voor Nederland ongewenste activiteiten vanuit het buitenland. Het wordt ingezet voor het verkrijgen van gevoelige informatie op economisch, politiek en militair terrein. Dankzij het internet is het veel eenvoudiger geworden om op afstand snel grote hoeveelheden data te ontvreemden en kunnen inlichtingendiensten of concurrerende bedrijven gevoelige informatie gericht uit een organisatie halen. Dit wordt bevorderd doordat het risicobewustzijn van spionage vaak laag is.

Illegaal gebruik van internet om politieke redenen is vooral gericht op bedreiging, defacements en propaganda

Het zijn vooral activiteiten met beperkte maatschappelijke impact die illegaal en om politieke redenen worden uitgevoerd. Zij beperken zich tot op heden vooral tot activistische uitingen. De voornaamste ontwikkeling is een toename van bedreigingen via internet, defacements van websites en uitingen van propaganda.

Burgers, overheid en bedrijven blijven kwetsbaar voor digitaal misbruik

Het afgelopen jaar is weer een groot aantal nieuwe kwetsbaarheden in software ontdekt, hoewel de groei ten opzichte van de voorgaande jaren gestabiliseerd is. Deze softwarelekken maken zowel overheden als bedrijven en burgers kwetsbaar voor aanvallen van cybercriminelen. Het gebruik van mobiele apparatuur is sterk gegroeid en introduceert extra risico's, onder andere omdat deze apparatuur vaak voor zowel privé- als zakelijke doeleinden wordt gebruikt. Organisaties passen best practices voor informatiebeveiliging niet altijd toe. Computergebruikers zijn zich niet altijd voldoende bewust van de risico's van ICT en internet.

Privacy staat meer onder druk

Zowel overheid als bedrijfsleven registreren veel persoonsgegevens, die zij niet altijd adequaat beschermen. De privacy van burgers staat ook onder druk doordat zij vrijwillig, in bijvoorbeeld sociale netwerken, veel persoonlijke informatie delen zonder daarvan in alle gevallen de consequenties te overzien.

Beveiliging van ICT wordt lastiger door uitbesteding en cloudcomputing

Uitbesteding van ICT en het gebruik van

cloudcomputing in het bijzonder nemen verder toe. Dit heeft effecten op de risico's die een organisatie loopt. Bedrijfsinformatie beperkt zich in dergelijke situaties namelijk niet langer tot het eigen bedrijfsnetwerk.
Dit leidt vaak tot verminderde controle op de locatie van systemen en gegevens en minder zicht op wat er met de eigen bedrijfsinformatie gebeurt.

Procesautomatisering loopt meer risico

Systemen in de procesautomatisering, vaak gebruikt in vitale sectoren, lopen momenteel meer risico dan voorheen. Dit komt door een toename van het aantal externe koppelingen, een gebrek aan ingebouwde beveiliging en het traag updaten van systemen. Daarnaast groeit het gebruik van standaard ICT-componenten waarmee ook de problemen van standaard ICT bij procesautomatisering geïntroduceerd worden.

Burgers en bedrijfsleven vinden ICT veilig genoeg om te gebruiken

Het vertrouwen dat Nederlandse burgers en bedrijven hebben in de veiligheid van ICT en internet in het bijzonder is hoog in vergelijking met andere landen. Burgers zijn naar eigen beleving voldoende voorgelicht en toegerust om veilig gebruik te kunnen maken van internet.

Er zijn veel initiatieven voor ICT-veiligheid, maar coördinatie blijft een aandachtspunt

Burgers, bedrijfsleven en overheid hebben elk een eigen rol te vervullen bij het behoud van veiligheid op internet. De overheid neemt in toenemende mate (beleids)maatregelen waarvan de reikwijdte tegelijkertijd breder wordt. In het eerste decennium van deze eeuw ging het vooral om bescherming van vitale sectoren en bestrijding van cybercrime in enge zin, maar inmiddels staan ook cyberwarfare en een integrale cybersecuritystrategie op de politieke agenda. Daarbij vereist het grensoverschrijdende karakter een goede internationale samenwerking. Overheidsbrede coördinatie over alle eigen initiatieven en maatregelen, maar ook coördinatie met bedrijfsleven, blijft een aandachtspunt.

Cyberspace is in opkomst als vijfde domein van de krijgsmacht

Cyberspace krijgt veel aandacht als vijfde domein voor militaire operaties, naast land, zee, lucht en de ruimte. Een groeiend aantal landen bouwt offensieve cybercapaciteiten op of defensieve capaciteiten met een offensief karakter. De doelwitten zijn zowel militair als civiel. Het achterliggende doel is met zo min mogelijk fysieke middelen zo snel mogelijk een tegenstander op de knieën te krijgen. Er zijn incidenten bekend waarbij militaire cyberaanvallen een rol speelden.


XII
III

1 Inleiding

Dit eerste Nationaal Trendrapport Cybercrime en Digitale Veiligheid is opgesteld door GOVCERT.NL onder gezamenlijk opdrachtgeverschap van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Justitie.

1.1 Aanleiding

Het gebruik van informatie- en communicatietechnologie (ICT) is de afgelopen decennia enorm toegenomen in onze maatschappij. Als samenleving profiteren we daarvan, maar het groeiend gebruik heeft ook een keerzijde. De toename in gebruik gaat gepaard met toename in misbruik. De digitale wereld biedt nieuwe ingangen om bij onze persoonsgegevens, ons geld en ons intellectueel eigendom te komen.
Om dergelijk misbruik te voorkomen en te bestrijden is inzicht nodig. Inzicht in de exacte werking en herkomst van allerlei verschijnselen, maar ook in de grote lijnen. In dit Trendrapport richten we ons op die grote lijnen, de strategische trends op het gebied van cybercrime en digitale veiligheid en op de effecten die dat heeft op Nederland.

1.2 Doel en doelgroep

Het Trendrapport bundelt de beschikbare strategische inzichten in de belangrijkste trends op het gebied van cybercrime en digitale veiligheid en brengt deze met elkaar in verband. Dat is waar dit Trendrapport zich onderscheidt ten opzichte van bestaande rapportages van onder meer de KLPD, NCTb, AIVD en MIVD, OPTA en GOVCERT.NL. Die zijn namelijk meer tactisch of operationeel van aard en richten zich doorgaans op hun afzonderlijke vakgebieden. Dit rapport heeft als doel om een gezamenlijk, beleidsneutraal en strategisch perspectief te bieden.
De opstellers van de bestaande rapportages hebben zelf meegewerkt aan de totstandkoming van dit Trendrapport. Het is de bedoeling dat vanuit deze samenwerking het Trendrapport de komende jaren verder kan groeien in zijn strategische functie naast de bestaande rapporten.
Het Trendrapport is openbaar en richt zich primair op overheden en bedrijven in vitale sectoren. Beleidsmakers binnen de Rijksoverheid kunnen het gebruiken als voeding voor toekomstig beleid. Voor (informatiebeveiligings)professionals kan het Trendrapport input zijn voor strategische besluitvorming.

1.3 Leeswijzer

Het Trendrapport is als volgt opgebouwd. Eerst worden de belangrijkste trends in afhankelijkheden (hoofdstuk 2) en kwetsbaarheden (hoofdstuk 3) verkend. Vervolgens komen in hoofdstuk 4 de trends binnen aanvalsmethoden aan de orde. Het gaat dan specifiek om aanvalstechnieken waarbij misbruik wordt gemaakt van zwakke plekken in onze ICT. Daarna beschrijft hoofdstuk 5 trends in de verschillende manifestaties van deze aanvalsmethoden, zoals cybercrime en digitale spionage. Hoofdstuk 6 benoemt trends in risicobeleving en op het gebied van maatregelen in nationale en internationale context. Tot slot zijn in hoofdstuk 7 de impact en het effect weergegeven.

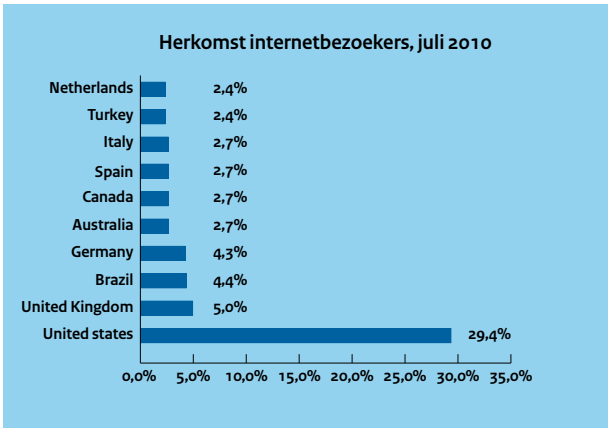

MAX.G.W.
30.480 KGS
67.200 LBS
TARE
3.820 KGS
8.420 LBS
MAX.C.W.
26.660 KGS
58.780 LBS

2
Afhankelijkheden

In dit hoofdstuk wordt in het kort een beeld geschetst van de trends in maatschappelijke afhankelijkheden van ICT. Zo blijft het internetgebruik groeien en raakt ICT steeds verder verweven met ons dagelijks leven. Ook krijgt internet een groter aandeel in het economisch verkeer. Daarnaast is ICT een veelgebruikt middel voor de realisatie van beleidsdoelen van de overheid.

2.1
Burger en bedrijf kunnen niet meer zonder ICT

De afhankelijkheid van ICT wordt misschien wel het best geïllustreerd door de 'adoptie' van internet in Nederland. Uit cijfers van internettoegang en -gebruik blijkt dat internet zeer relevant is voor Nederland en de Nederlanders.[1] In ons land heeft bijvoorbeeld 90% van de huishoudens toegang tot internet, waarvan ongeveer 37% gebruikmaakt van breedbandinternettoegang.[2] In internationaal opzicht hoort Nederland met deze cijfers tot de wereldtop. Nederland staat ook in de wereldwijde top 10 als het gaat om het aantal webpaginabezoeken. Verder verplaatsen we steeds meer activiteiten naar het internet. Dit verschijnsel noemen we substitutie. Zo gebruiken Nederlanders internet meer en meer als alternatief voor winkelen en bankieren. In 2009 kochten Nederlanders relatief meer online dan andere West-Europeanen. Maar liefst 71% van de Nederlandse internetgebruikers koopt wel eens iets via internet en dit percentage zal de komende jaren naar verwachting nog verder toenemen. De komst van iDEAL als betaalsysteem gaf e-commerce in Nederland een stevige duw in de rug: in 2009 maakte 45% van de Nederlandse internetgebruikers hier



Figuur 2-1 Herkomst internetbezoekers webpagina's[3]

gebruik van. De groei van online winkelen wordt geholpen doordat we erop vertrouwen dat het veilig is: slechts 7% van de Nederlandse shoppers vindt het niet veilig om online te kopen. Dit percentage is lager dan in andere Europese landen.[4]

Ook elektronisch bankieren groeit in Nederland. Van 9,7 miljoen gebruikers in 2008 tot naar verwachting 11,2 miljoen in 2013, zowel privé als zakelijk.[5] En ook hier is het vertrouwen redelijk groot: een peiling uit 2009 wijst uit dat 70% van de internetgebruikers elektronisch bankieren veilig vindt.[6] Ook de grote meerderheid van Nederlandse bedrijven en organisaties is – naar eigen zeggen – al (zeer) afhankelijk van ICT voor het functioneren.[7]
ICT is bovendien een van de grote motoren achter de stijging van de productiviteit in de Nederlandse en Europese economie. De productiviteitsgroei van de

1 TNO, Marktrapportage Elektronische Communicatie, mei 2010
2 http://www.oecd.org/document/54/0,3343,en_2649_34225_38690102_1_1_1_1,00.html
3 http://www.w3counter.com/globalstats.php
4 Forrester Research, Western European Online Retail Forecast, 2009 to 2014, maart 2010
5 Forrester Research, Dutch Online Banking Forecast: 2008 to 2013, april 2008
6 TNO, Perceptieonderzoek Veilig Internet Onderzoek naar de ruimte tussen wat (on)veilig is en wat als zodanig gepercipieerd wordt, april 2009
7 Ernst & Young, ICT Barometer over cybercrime, 24 februari 2010

afgelopen 15 jaar in Europa is volgens de Europese Unie (EU) voor de helft toe te schrijven aan het gebruik van ICT.[8] De Digitale Agenda van de Europese Commissie (EC) moet zorgen voor een verdere substantiële bijdrage van ICT aan de economische groei in de EU.

2.2 Fysieke en digitale wereld steeds meer verweven

ICT zal steeds verder ons leven binnendringen en dat geldt ook voor internet als belangrijkste digitale verkeersader. Steeds meer apparaten worden uitgerust met een eigen internetadres. Vaak met als doel: betere dienstverlening op afstand door leverancier, arts, helpdesk of monteur of meer gebruiksgemak. Maar er zitten ook risico's aan de verbinding van allerlei apparaten om ons heen met internet. De kans op inbreuk op de privacy neemt toe door het automatisch verzamelen en/of weglekken van persoons- of andere gegevens. Daarnaast verdwijnt het overzicht voor gebruikers en beheerders door het groeiend aantal verbindingen met internet. Ten slotte zijn fysieke middelen via internet bereikbaar geworden voor aanvallen op afstand. Aanvallen op pacemakers bijvoorbeeld zijn theoretisch al mogelijk.[10]

Voorbeelden van verwevenheid fysieke en digitale wereld:
- Op het werk: pc, telefonie, kopieerapparaat, RFID[9], klimaatregeling, beveiliging
- Op straat: pinautomaat, cameratoezicht, verkeersregeling
- In de auto: navigatie, motormanagement
- In ons huis: pc, televisie, domotica, slimme energiemeters, koelkast
- In ons lichaam: pacemaker, insuline-automaat (beide nog in ontwikkeling)

2.3 Belangrijke overheidsdiensten afhankelijk van werking ICT

Net als het bedrijfsleven maken ook Nederlandse overheden steeds intensiever gebruik van ICT. Het wordt op grote schaal ingezet voor de eigen interne bedrijfsvoering en voor het ondersteunen van maatschappelijke ontwikkelingen. Denk bijvoorbeeld aan de OV-chipkaart of e-government ter verbetering van de dienstverlening aan de burger. Zie wat dat laatste betreft bijvoorbeeld de Versnellingsagenda 2009-2010 'Betere dienstverlening met minder regeldruk' en het 'Nationaal Uitvoeringsprogramma dienstverlening en e-overheid' (NUP).
Ook versterkt de overheid de ICT-governance door het instellen van een Rijks-CIO en CIO's per departement en hun onderlinge interdepartementale samenwerking. Er is bijvoorbeeld een portefeuillehouder onder de CIO's aangewezen voor informatiebeveiliging. Steeds vaker zijn informatiesystemen onderling met elkaar verbonden om informatie uit te wisselen. Voorbeelden zijn het Elektronisch Kinddossier en het Elektronisch Patiëntendossier, maar ook logistieke ketens met (private) leveranciers. De verbindingen worden doorgaans gelegd via het publieke internet of andere publieke netwerken (met een bepaalde mate van extra beveiliging). Ook de overheid wordt dus steeds afhankelijker van ICT en internet in het bijzonder en daarmee kwetsbaarder voor de risico's die daaraan verbonden zijn.

Geen trams in Utrecht door uitval mobiel netwerk

In november 2009 viel een deel van het netwerk van een mobiele netwerkoperator langdurig uit. Als gevolg daarvan konden de trams in en rond Utrecht niet meer rijden, omdat deze gebruikmaken van dit netwerk voor communicatie met de verkeerscentrale. Uit veiligheidsoverwegingen besloot de vervoersmaatschappij de trams stil te zetten.

[8] Digitale Agenda van de Europese Commissie, IP/10/571, mei 2010
[9] Radio Frequency IDentification, ofwel draadloze identificatie van objecten
[10] Korps Landelijke Politiediensten, Hightech crime, Criminaliteitsbeeldanalyse 2009, 2010

3
Kwetsbaarheden

Ons vertrouwen in ICT is groot en ICT-oplossingen worden omarmd voor allerlei doeleinden. Onze maatschappij wordt echter kwetsbaarder voor verstoringen van ICT, naarmate de afhankelijkheid van ICT groeit. In dit hoofdstuk worden de belangrijkste kwetsbaarheden toegelicht.

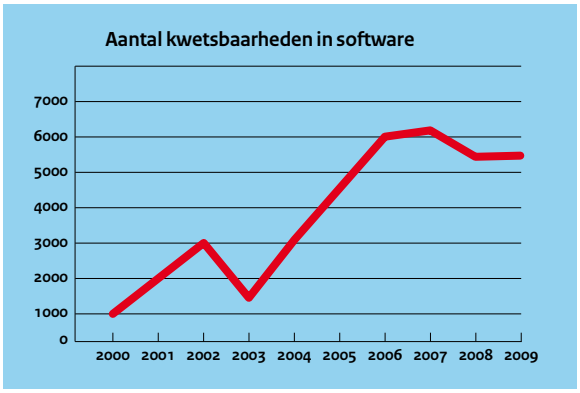
3.1
Techniek blijft kwetsbaar

Software wordt nog altijd gezien als een van de belangrijkste bronnen van kwetsbaarheden. De groei van het aantal nieuw bekend geworden ernstige en middelzware kwetsbaarheden in software stabiliseert nu na jaren van sterke groei, zij het op een tamelijk hoog niveau (ruim 5.500 nieuwe kwetsbaarheden in 2009). Afgezet tegen een nog altijd sterk groeiende hoeveelheid softwareregels en toename in complexiteit van programmatuur, is die stabilisatie een gunstige ontwikkeling.

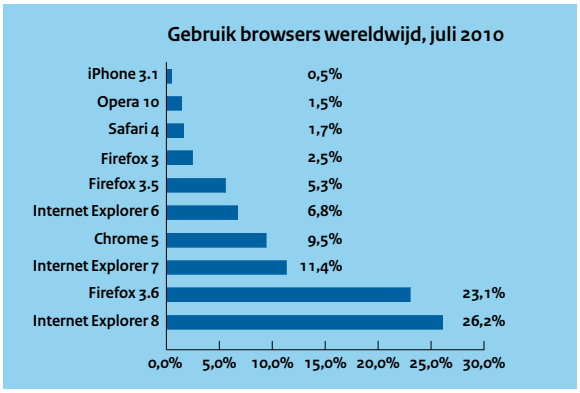
Een mogelijke verklaring voor deze ontwikkeling is de toegenomen aandacht voor beveiliging bij het ontwerp en de ontwikkeling van software. Vaak is beveiliging een ondergeschoven kindje ten opzichte van kosten, time-to-market en functionaliteit. Ook schiet de beveiligingskennis bij ontwerpers en ontwikkelaars nog wel eens tekort.

Aandacht voor beveiliging bij het ontwerp en de ontwikkeling van software kan ertoe leiden dat nieuwe software minder kwetsbaarheden bevat, maar is niet van invloed op kwetsbaarheden in al bestaande software. Dat is dan ook een belangrijke reden dat veel systemen kwetsbaar zijn: de software die erop draait is niet gepatcht of wordt zelfs helemaal niet meer ondersteund door de fabrikant. Internetstatistieken onderbouwen dit. Er wordt veel software gebruikt die verouderd is of niet meer ondersteund wordt. In figuur 3-2 staat een overzicht van gebruikte browsers uit juli 2010 waarvan een deel door de leverancier niet meer wordt ondersteund (bijvoorbeeld Internet Explorer 6).

Een positieve ontwikkeling is het toenemende aantal leveranciers dat een automatisch patchmechanisme inbouwt in hun software. Hiertoe behoren enkele



Figuur 3-1 Aantal kwetsbaarheden in software



Figuur 3-2 Gebruik browsers wereldwijd, juli 2010[11]

[11] http://www.w3counter.com/globalstats.php?year=2010&month=7

belangrijke bedrijven: Google, Microsoft, Apple en Adobe. Met automatisch patchen worden automatisch de laatste updates geïnstalleerd. De gebruiker hoeft zelf weinig te doen, waardoor de software makkelijker up-to-date blijft.

Daarnaast zien we ook veel kwetsbaarheden in webapplicaties. De belangrijkste redenen van de kwetsbaarheden zijn onvoldoende validatie van ingevoerde gegevens, het lage kennisniveau van programmeurs van informatiebeveiligingsmaatregelen en het ontbreken van een standaard voor veilig ontwikkelen.[12]

Een monocultuur van gebruikte software is eveneens een kwetsbaarheid. Grote groepen gebruikers kunnen in deze situatie op dezelfde manier worden aangevallen en vormen een aantrekkelijk doelwit volgens het principe van de economy of scale.
Er is in Nederland een monocultuur op het gebied van besturingssystemen voor pc's en laptops (90% penetratie Windows in alle voorkomende versies) en browsers (bijna 70% Microsoft Internet Explorer in alle voorkomende versies), pdf-readers (Adobe Acrobat) en Adobe Flash (98% penetratie wereldwijd).[14]

Persoonsgegevens lekken uit overheidswebsite[13]
Een website om reizigers te verleiden om een op naam gestelde ov-chipkaart te kopen, bleek onvoldoende beveiligd. De persoonlijke gegevens van ruim 168.000 reizigers bleken voor hackers inzichtelijk te zijn, te veranderen, toe te voegen en te verwijderen. Door een fout in de website werd bij foute invoer te veel informatie teruggegeven. Daardoor was het mogelijk rechtstreeks met de database te communiceren. Dit incident leidde tot Kamervragen.

Het is voorts voorstelbaar dat hardware 'achterdeurtjes' bevat, waarlangs derden (zoals inlichtingendiensten) ongemerkt informatie kunnen aftappen of anderszins toegang tot systemen krijgen.[15] Het gaat dan om achterdeurtjes in fysieke componenten (chips) of firmware van apparaten als routers, laptops of servers. Nederland is vrijwel geheel afhankelijk van buitenlandse leveranciers voor hardware.

Ten slotte bevat ook de internetinfrastructuur kwetsbaarheden, die van belang zijn omdat het internet als basis wordt gebruikt voor veel zakelijke en privétoepassingen. De zwakte zit in de protocollen waarop internet als netwerk functioneert. Protocollen als IP (Internet Protocol), BGP (Border Gateway Protocol) en DNS (Domain Name System) zijn ruim veertig jaar oud en destijds ontworpen voor het routeren van gegevens, niet voor vertrouwelijkheid en integriteit van gegevens. Daarom is men nu bezig met de overgang van enkele oude protocollen – DNS en IPv4 – naar nieuwe, veiligere protocollen – DNSSEC en IPv6. Uiteraard zijn DNSSEC en IPv6 geen Haarlemmerolie: beide introduceren ook nieuwe kwetsbaarheden en risico's.

3.2 Beveiliging bij procesautomatisering loopt meer risico

Procescontrolesystemen, of Industrial Control Systems (ICS), zoals supervisory control and data acquisition systemen (SCADA) en Distributed Control Systems (DCS) vormen het kloppend hart van veel essentiële fysieke processen in onze samenleving. Denk aan drinkwatervoorzieningen, energieopwekking en -distributie, chemie, voedsel, transport en de beheersing van oppervlaktewater. Bij het niet correct functioneren of uitvallen van de procesbesturing kunnen de processen verstoord raken of uitvallen. De potentiële schade van dergelijke verstoringen is groot.

Vanuit technisch oogpunt schuilen de grootste kwetsbaarheden van procescontrolesystemen in het toepassen van generieke ICT-middelen, het gebruik van verouderde besturingssystemen, communicatie die via open netwerken plaatsvindt en de gebruikte protocollen.[16]

In toenemende mate wordt bij procesautomatisering gebruikgemaakt van generieke ICT-middelen. Hiermee worden ook de standaard ICT-problemen in de procesautomatisering geïntroduceerd.

[12] Zie voor een nadere analyse van kwetsbaarheden van webapplicaties ook GOVCERT.NL, Raamwerk Beveiliging Webapplicaties, 2010 en Factsheet FS-2010-01 De beveiliging van webapplicaties, 2010

[13] Zie voor het originele verhaal: http://webwereld.nl/nieuws/66012/ov-site-lekt-persoonlijke-data-168-000-reizigers.html

[14] TNO (2010) en Adobe, Penetratie in Europa, juni 2010, http://www.adobe.com/products/player_census/flashplayer/version_penetration.html. Voor Windows is vooral een verschuiving tussen verschillende versies te zien: van XP en Vista naar Windows 7

[15] AIVD, Kwetsbaarheidsanalyse spionage. Spionagerisico's en de nationale veiligheid, 2010

[16] NICC, Process Control Security in het Informatieknooppunt Cybercrime, 2009

Stuxnet: een gerichte aanval op processontrolesystemen[17]

In juni 2010 is een aanval ontdekt die Stuxnet wordt genoemd en die gericht was op procescontrolesystemen. Deze aanval was gericht op specifieke Siemens systemen en waarschijnlijk op een specifieke sector.

De aanval was behoorlijk complex. Stuxnet maakte gebruik van een aantal kwetsbaarheden in Windows waarvan een aantal 'zero-day' kwetsbaarheden. Stuxnet verbergt zijn aanwezigheid, kent verschillende manieren van verspreiding en maakt gebruik van het gegeven dat procescontrole-systemen met hard-gecodeerde wachtwoorden kunnen werken. Onderdeel van Stuxnet is een elektronisch ondertekende driver, die ondertekend is met gestolen certificaten.

Uitbuiting van de kwetsbaarheden is waarschijnlijk gedaan vanaf eind 2009, mogelijk zelfs eerder. In september 2010 waren nog niet voor alle uitgebuite kwetsbaarheden patches uitgebracht.

Niet alleen procescontrolesystemen zijn door Stuxnet besmet. Ook andere Windows computers kunnen door Stuxnet worden besmet. Waarschijnlijk zijn honderdduizenden computers hierdoor besmet. Omdat Stuxnet op zoek is naar specifieke Siemens systemen, houdt besmetting niet per definitie in dat gegevens verdwijnen of processen worden verstoord.

Het oorspronkelijke doel van Stuxnet leek bedrijfsspionage. Wanneer een procescontrolesysteem door Stuxnet is besmet is het echter eveneens mogelijk de besturing van industriële processen te beïnvloeden en te verstoren, waaronder de aansturing van apparatuur zoals pompen en motoren. Stuxnet is daarom te beschouwen als een uiterst serieus te nemen waarschuwing ten aanzien van de uitbuiting van de kwetsbaarheid van procescontrolesystemen.

Zo kunnen bijvoorbeeld standaard hackertools gebruikt worden voor het vinden van kwetsbaarheden en kunnen standaard exploits toegepast worden.

Procescontrolesystemen hebben vaak een levenscyclus van tien tot dertig jaar. Op deze systemen draaien vaak besturingssystemen die niet meer ondersteund worden door de oorspronkelijke leverancier. Oude kwetsbaarheden blijven daardoor bestaan, omdat er geen patches meer worden gemaakt. Het patchen van een procescontrolesysteem in een industriële procesomgeving is op zichzelf al een complexe aangelegenheid, omdat tijdelijke uitschakeling van systemen zeer ongewenst is. Dit komt door de vereiste continuïteit (bijvoorbeeld water, elektriciteit) of de opstarttijd en -kosten van de processen. Ook geven leveranciers niet altijd garantie voor de juiste werking van systemen wanneer een patch wordt uitgevoerd.

ICS-systemen staan steeds minder vaak in een geïsoleerde omgeving. Bedrijven koppelen steeds vaker procescontrolenetwerken met andere netwerken binnen of buiten de organisatie, omdat vanuit de kantooromgeving toegang tot procesgegevens gewenst is. Dit geldt ook voor efficiënt onderhoud op afstand en dagelijkse controle. Met deze externe verbindingen worden onbedoeld ook routes aangelegd voor besmetting.[18]
Een ander aspect betreft de communicatieprotocollen die worden toegepast. Deze waren oorspronkelijk bedoeld voor gesloten netwerken. Daarom is er bij het ontwerp weinig of geen aandacht geschonken aan informatiebeveiligingsaspecten. Procescontrolesystemen kunnen daarom kwetsbaar zijn via communicatie-interfaces.[19]

Maatregelen om risico's te verminderen, zoals het gebruik van anti-virussoftware, hebben in een procesautomatiseringsomgeving vaak ongewenste neveneffecten. Leveranciers garanderen de juiste werking soms niet meer en er kunnen performanceproblemen ontstaan.

Opvallend is verder dat de aandacht vanuit securityonderzoekers en hackers voor het ICS-domein toeneemt. Op een aantal grote beveiligingsconferenties werden presentaties gegeven die gerelateerd zijn aan dit onderwerp.

Gezien bovenstaande factoren is in veel gevallen een weinig geavanceerde aanval nodig om de werking van procescontrolesystemen te verstoren. Voor het overnemen van het proces is meer kennis nodig.

[17] GOVCERT.NL Factsheet 2010-02 Stuxnet - een geavanceerde en gerichte aanval, http://www.govcert.nl/download.html?f=163

[18] KLPD (2010), NICC (2009)

[19] World Economic Forum, Global Risks 2010, A Global Risk Network Report, januari 2010

Overigens hebben zich tot dusverre geen publiekelijk bekend geworden incidenten voorgedaan in Nederland.

3.3 Mobiele apparatuur is een aantrekkelijk doelwit

Steeds meer mensen gebruiken hun smartphone voor meer dan alleen telefoneren, bijvoorbeeld om te mailen of bedrijfsinformatie te raadplegen. Het gebruik van dergelijke apparaten brengt een aantal risico's met zich mee.[20] Ten eerste staan ze vaker en langer aan dan gewone computers en hebben ze meerdere verbindingen met de digitale buitenwereld, zoals GSM, GPRS, 3G, bluetooth, UMTS, USB en WiFi. Het apparaat is dus voortdurend bereikbaar van buitenaf. Ten tweede bepalen veel smartphones hun locatie met GPS of WiFi. Zo is duidelijk waar het apparaat (en vaak ook de eigenaar) zich bevindt. Sommige programma's op een smartphone geven deze locatiegegevens prijs zonder dat de gebruiker er erg in heeft. Ten derde is het mogelijk om zonder tussenkomst van de gebruiker acties uit te voeren die geld in het laatje brengen van criminelen: bijvoorbeeld sms'en gekoppeld aan een duur abonnement. Ten vierde schiet de kennis van ICT-organisaties vaak tekort over het veilig beheren van mobiele apparatuur en is het voor hen ook minder beheersbaar dan vaste apparatuur. Tot slot zijn de apparaten zelf ook interessant om te stelen, vanwege de waarde van het apparaat of juist vanwege de informatie die erop staat.

De dreiging van malware-aanvallen op mobiele telefoons is nog klein, maar groeit.[21] Aanvallen via mobiele toepassingen zijn mogelijk, maar in de praktijk nog te ingewikkeld om (nu) grootschalig te realiseren. Er is nog steeds geen grote uitbraak van een virus geweest, wel diverse kleinere incidenten.[22] Daar is een aantal mogelijke redenen voor aan te wijzen. Ten eerste is de diversiteit van besturingssystemen op mobiele apparatuur groot, waardoor er per besturingssysteem minder gebruikers zijn.[23] Ten tweede worden bij het ontwerp van mobiele besturingssystemen eerder geleerde beveiligingslessen van vaste besturingssystemen toegepast.

GOVCERT.NL 3 maart 2010: Afluisteren van GSM-communicatie dichterbij (FS 2009-05)
Spraakverkeer over mobiele telefoons werd tot dusverre redelijk veilig geacht. Er is echter een kwetsbaarheid gevonden in de beveiliging van GSM-communicatie. Onderzoeker Karsten Kohl heeft in oktober 2009 aangekondigd snel een aanpak te publiceren waarmee GSM-encryptie gekraakt kan worden. Daarmee is theoretisch afluisteren van gesprekken en SMS-berichten mogelijk (bijvoorbeeld voor authenticatie). UMTS en GPRS gebruiken andere technologie (andere encryptiealgoritmes), die niet dezelfde kwetsbaarheid bevat. Voor vertrouwelijke communicatie is GSM minder geschikt geworden.

3.4 Overzicht en controle lastiger door uitbesteding en cloudcomputing

Voor veel organisaties is het bedrijfsnetwerk als harde buitengrens van de eigen digitale omgeving vervaagd. Mobiel werken, het koppelen van bedrijfsnetwerken en het aansluiten van privéapparatuur op het bedrijfsnetwerk hebben de buitengrens veranderd in een dun membraam.[24] Het ICT-landschap bij organisaties is daardoor complexer geworden en moeilijker te overzien en te beheren gezien vanuit de eigenaar van de informatie. Dit effect wordt versterkt door een tweetal verwante trends: het uitbesteden van ICT en het gebruik van cloudcomputingdiensten. Waar men zich niet altijd bewust van is, is dat de verantwoordelijkheid niet uitbesteed kan worden.

Het uitbesteden van bedrijfsprocessen introduceert nieuwe kwetsbaarheden in het ICT-landschap van een organisatie. Het zicht vermindert op wat er met de bedrijfsinformatie gebeurt. Dit geldt in versterkte mate bij uitbesteding naar een ander land of wanneer een leverancier op zijn beurt gebruikmaakt van een (buitenlandse) onderaannemer. Zeker wanneer gevoelige bedrijfsinformatie naar het buitenland

[20] GOVCERT.NL, Beveiliging van mobiele apparatuur en datadragers, 2009

[21] Mikko Hyppönen van F-Secure en Juan Santana van Panda, in 'Mobieltje voorlopig veilig' Vijf vragen aan de beveiligingsexperts van F-secure en Panda, Automatiseringsgids, 4 juni 2010

[22] Zie bijvoorbeeld http://www.theregister.co.uk/2009/08/21/locked_down_phones (operator pushed malware naar blackberry's) http://www.theregister.co.uk/2010/06/03/samsung_wave_pre_pwned/ (malware meegeleverd op geheugenkaart), http://www.theregister.co.uk/2009/12/22/iphone_worm_analysis/ (iphones als botnet clients)

[23] Juan Santana van Panda, in 'Mobieltje voorlopig veilig' Vijf vragen aan de beveiligingsexperts van F-secure en Panda, Automatiseringsgids, 4 juni 2010

[24] Information Security Platform Limited (2010)

verhuist, brengt dit extra risico's met zich mee. Ingrijpen op kwetsbaarheden is over het algemeen moeilijker bij activiteiten in eigen huis.

Hetzelfde geldt ook bij de inzet van toepassingen onder de noemer Software as a Service (SaaS), of cloudcomputing. Denk aan toepassingen voor boekhouding, commerciële ondersteuning of recruitment. Het gebruik hiervan neemt toe, ingegeven door voordelen als lagere kosten, snelle ingebruikname en hergebruik van bestaande functionaliteit.[25] Er dreigt een 'vlucht' naar cloudcomputing zonder passend risicomanagement.[26] Over het algemeen is bij cloudcomputing geen controle over of kennis van de exacte soms wisselende locatie van de ICT-omgeving, die zich soms in het buitenland bevindt of met anderen wordt gedeeld. Het is daardoor moeilijk te overzien of voor de bedrijfsinformatie wordt voldaan aan de privacy- en vertrouwelijkheidseisen, welk juridisch regime geldt voor incidenten of voor terbeschikkingstelling van data aan overheidsdiensten ter plaatse. Specifieke eisen aan beveiliging en beheer van standaard cloudcomputingdiensten zijn nauwelijks te stellen. De mate van 'besturing' is dan voor de individuele opdrachtgever minder groot, misschien zelfs onvoldoende om te voldoen aan regelgeving. Dit geldt overigens vooral voor publieke cloudcomputing. Op bedrijfseigen clouds heeft een organisatie vanzelfsprekend veel meer grip.

Grote cloudcomputingleveranciers – zeker die met interessante klanten – zijn een aantrekkelijk doelwit voor cybercriminelen. Hoe meer data in huis, des te aantrekkelijker. De klant krijgt dan onbedoeld een hoger risicoprofiel door aansluiting bij die leverancier.

3.5 De mens is een zwakke schakel

Mensen zijn zowel thuis als zakelijk een zwakke schakel bij de beveiliging van informatie, bijvoorbeeld omdat ze besmette USB-sticks gebruiken, ingaan op phishingmails of (al te) persoonlijke gegevens plaatsen op sociale netwerken.[27]

Dit wordt de afgelopen jaren versterkt doordat mensen in toenemende mate privéapparatuur en tools op internet – zoals social network sites, instant messaging en blogs – niet alleen thuis maar ook op het werk gebruiken.[28] De beveiliging van een organisatie wordt hierdoor beïnvloed.

Burgers delen via publieke sites zoals Hyves, Facebook, YouTube en LinkedIn, vrijwillig en op grote schaal persoonlijke gegevens, zoals foto's, films, concrete informatie over adres, thuissituatie, interesses en werk. Op internet zijn over de meeste mensen zo al zeer veel persoonsgegevens te vinden. Lang niet iedereen is zich hiervan bewust. Vaak verstrekken mensen persoonsgegevens wel vrijwillig, maar alleen omdat ze ernaar gevraagd worden in ruil voor een dienst. Denk aan het verstrekken van naam- en adresgegevens om een interessant rapport te kunnen downloaden of voor het aanvragen van een klantenkaart.

Daarnaast verzamelen en gebruiken meer bedrijven in toenemende mate persoonsgegevens. Denk hierbij aan gegevens over surfgedrag of e-mailinhoud en daaruit blijkende interesses, om gerichter te kunnen adverteren. Met enige regelmaat komen berichten naar buiten over dit soort activiteiten en soms leidt dit tot enige onrust. Bijvoorbeeld in het geval van Google die gegevens van draadloze netwerken verzamelde en de maatschappelijke verontrusting die hierover ontstond.

Elke eindgebruiker heeft een eigen verantwoordelijkheid. Helaas kunnen ze vaak gemakkelijk verleid worden omdat niet alle software even gebruikersvriendelijk is en met een laag kennisniveau goed en veilig in te stellen is. Onder andere automatisch patchen en standaard veilige instellingen kunnen wel zorgen voor een hoger beveiligingsniveau zonder handelingen van de eindgebruiker.

[25] Gartner, Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014, 2010

[26] Zie ook Gartner: Security in 2013 and beyond, 2010

[27] Zie ook KLPD (2010)

[28] Uit de expertsessies. Zie over de achterliggende ontwikkeling van consumerization: Gartner, Key Issues for the Consumerization of IT, 2009. Gartner, Findings: In January 2010, the Consumerization of IT Became a Business Strategy

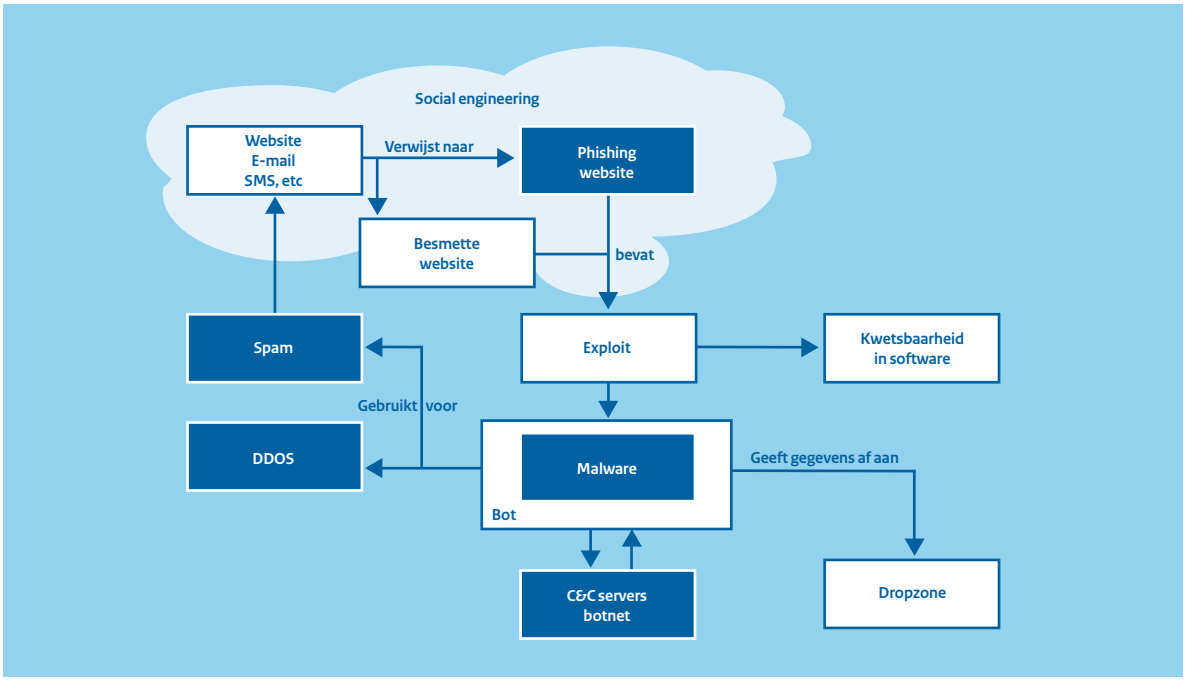
4
Aanvalsmethoden

In het algemeen zoeken aanvallers naar het zwakste punt in de beveiliging. Een aanvalsmethode maakt gebruik van een kwetsbaarheid. Als een kwetsbaarheid is verholpen, gaan ze op zoek naar nieuwe kwetsbaarheden. Bestaande aanvalsmethoden blijven echter succesvol, wanneer bekende kwetsbaarheden niet worden weggenomen. In dit hoofdstuk zijn de belangrijkste trends in aanvalsmethoden op hoofdlijnen beschreven. Voor een meer gedetailleerde beschrijving van verschillende aanvalsmethoden verwijzen we graag naar de afzonderlijke (trend) rapportages en ander materiaal van onder andere GOVCERT.NL[29] en het KLPD Team High Tech Crime.

4.1
Bestaande methoden blijven succesvol

Om meerdere redenen blijven bestaande methoden succesvol. Zolang oude kwetsbaarheden blijven bestaan, blijven oudere varianten van aanvalsmethoden gericht op exploitatie van die kwetsbaarheid succesvol. Bovendien kunnen dezelfde aanvalsmethoden op nieuwe kwetsbaarheden worden toegepast.

De verschillende methodes staan meestal niet op zichzelf, maar hebben een relatie met elkaar. Botnets nemen een centrale plaats in bij de aanvalsmethoden. Een botnet verstuurt bijvoorbeeld spam om



Figuur 4-1 Relatie tussen aanvalsmethoden

[29] Zie www.govcert.nl/trends en www.govcert.nl/kennis

gebruikers te lokken naar een besmette website. Via een besmette website kan malware worden geïnstalleerd met een exploit door misbruik te maken van een kwetsbaarheid in software van de eindgebruiker.
De malware kan de besmette computer tot een bot maken en daarmee onderdeel van een botnet.
De malware kan gegevens inzien op de computer en meekijken welke handelingen de gebruiker uitvoert. Gegevens worden van de computer afgevangen en opgeslagen op een door de aanvaller bepaalde locatie ('drop zone'). De Command & Control (C&C)-servers zorgen voor updates van een bot met verbeterde functionaliteit. In onderstaande figuur staat de wijze waarop de belangrijkste aanvalsmethoden met elkaar samenhangen.

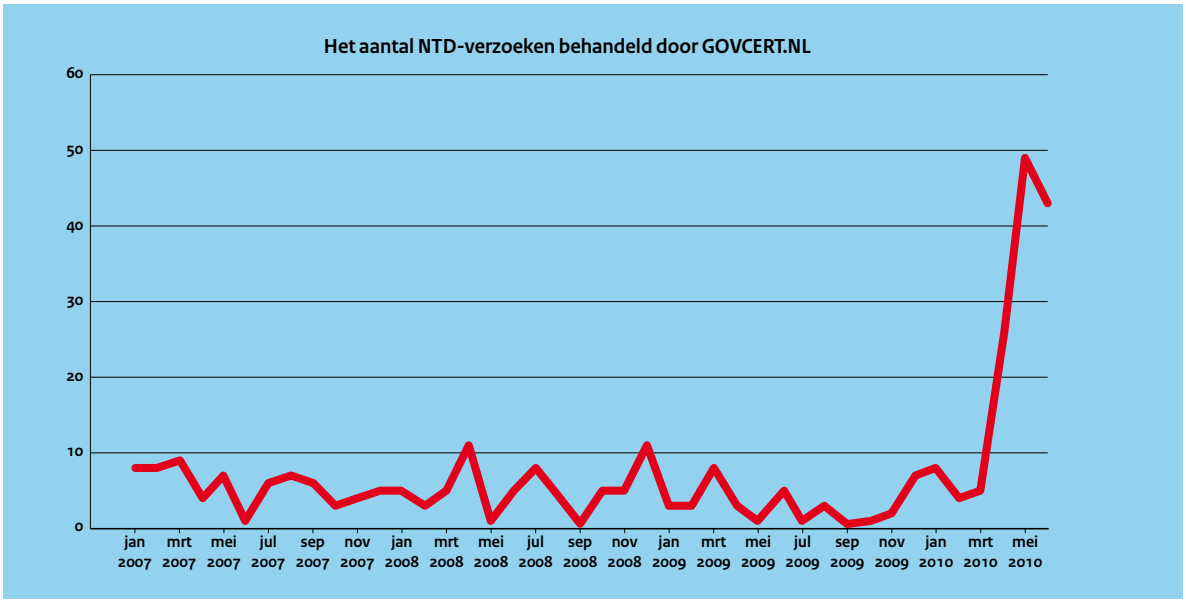
Malware

Naar schatting is 0,5% tot 5% van alle aan het internet verbonden computers geïnfecteerd met malware die het mogelijk koppelt aan een botnet.[30] Het zijn vooral de computers van kleine bedrijven en particulieren die besmet raken. Deze groep is zich niet altijd voldoende bewust van de risico's en heeft minder middelen voor het nemen van preventieve maatregelen. Niet alleen pc's worden aangevallen, maar ook andere apparatuur zoals routers.[31]
Hoewel het vooral computers van kleine bedrijven en particulieren zijn die besmet raken, hebben grote organisaties ook regelmatig last van grootschalige besmettingen. Er is het afgelopen jaar een aantal grote incidenten geweest waarbij de informatievoorziening van grote organisaties een week of meer verstoord is geweest als gevolg van een uitbraak van het Conficker virus.

Malware brengt op meerdere manieren economische schade toe, zowel in de vorm van directe als indirecte kosten. De OECD signaleert dat de exacte totale kosten van malware onbekend zijn, maar een stijgende trend zeer waarschijnlijk is.[32] Een case studie door de TU Delft in opdracht van de OPTA becijfert de kosten van een onderzochte aanval op 17,5 miljoen euro.[33] Dit bestaat vooral uit kosten voor herstel en productiviteitsverlies.

Phishing neemt weer toe

In vergelijking met andere landen had Nederland de laatste jaren relatief weinig te kampen met phishing e-mails.[34] In de periode 2008 tot 2010 daalde het aantal phishing e-mails zelfs, mede als gevolg van enkele opsporingssuccessen. Sinds begin 2010 neemt het aantal waargenomen phishingaanvallen echter weer toe. In het tweede kwartaal van 2010 heeft GOVCERT.NL een grote stijging in het aantal Notice and Takedown (NTD) verzoeken gehad. Dit zijn verzoeken om websites, die bijvoorbeeld worden



Figuur 4-2 Aantal NTD-verzoeken behandeld door GOVCERT.NL

[30] Zie o.a. KLPD (2010); Michel van Eeten e.a. The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data, 2010
[31] http://seclists.org/fulldisclosure/2010/Feb/387 (over het Chuck Norris Botnet)
[32] OECD, Computer Viruses and Other Malicious Software. What Can Be Done?, 2009
[33] M. van Eeten e.a., Damages from internet security incidents. A framework and toolkit for assessing the economic costs of security breaches, February 2009
[34] AWPG, Global Phishing Survey: Trends and Domain Name Use in 2H2009, May 2010; Vergelijkbaar met de conclusies uit MessageLabs Intelligence reports

gebruikt voor phishing of voor het verspreiden van malware, uit de lucht te halen. Nederland staat met enige regelmaat in de top 10-overzichten van landen die phishingsites hosten (met een marktaandeel variërend van 1 tot 5%).[35]

Botnets blijven het Zwitsers zakmes voor cybercriminelen

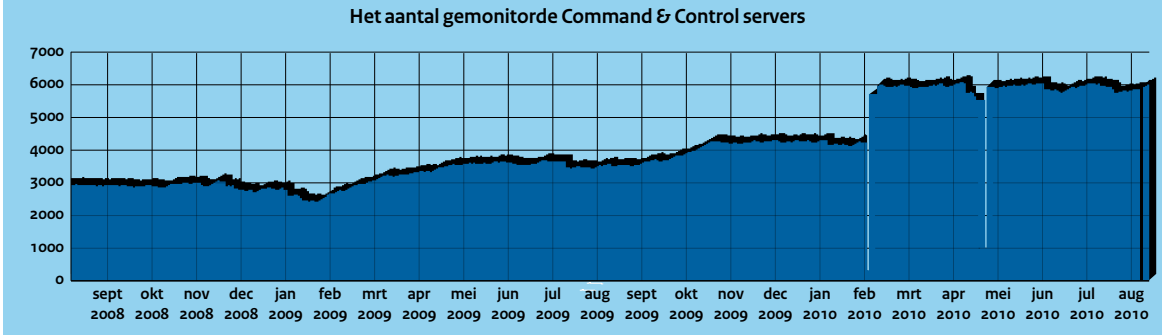
Botnets zijn verzamelingen geïnfecteerde computers die centraal bestuurd kunnen worden. Het zijn krachtige en flexibele hulpmiddelen voor cybercrime. Botnets worden gebruikt om (persoonlijke) gegevens van eindgebruikers te achterhalen (inclusief inlogcodes), grote hoeveelheden spam te verzenden of een gedistribueerde aanval uit te voeren waardoor andere computersystemen niet meer bereikbaar zijn (Distributed Denial of Service, DDoS).[36]
Omdat software nog veel kwetsbaarheden heeft, eindgebruikers onvoldoende bewust zijn en niet altijd voldoende kennis hebben, zijn cybercriminelen in staat om botnets van voldoende omvang op te zetten. Botnets zijn daarmee een soort cloudcomputing voor cybercriminelen.

Botnets bestaan in verschillende maten. Van kleine gespecialiseerde botnets van een paar honderd bots, tot giganten als Rustock en Grum met een miljoen of meer bots.[37] De omvang van botnets varieert onder andere door nieuwe besmettingen, opschoningsacties en het 'neerhalen' van hostingfaciliteiten voor botnets. In figuur 4-3 is te zien dat het totaal aantal

ZeuS, koning der botnets[38]
ZeuS is een wijd verspreid botnet dat speciaal gebruikt wordt voor het stelen van vertrouwelijke (bank)gegevens. Later werd ZeuS ook gebruikt voor andere doeleinden. ZeuS kent een uitgebreide functionaliteit om gebruikers vertrouwelijke gegevens te ontfutselen: zoals het ongemerkt en gestructureerd afvangen van toetsaanslagen, het ongemerkt kopiëren van documenten, het omleiden van internetbankierensessies en het on-the-fly toevoegen van invoervelden op websites voor phishing. ZeuS bots kunnen bij hun Command & Control servers ook nieuwe functionaliteit ophalen.[39]

ZeuS verstuurde via Facebook sinds oktober 2009 al meer dan 1,5 miljoen phishingberichten, waarin gebruikers worden gewaarschuwd voor bijvoorbeeld problemen met hun financiële informatie. Het bericht deed de suggestie om op een link te klikken. De computer van de gebruiker werd besmet wanneer de bezoeker (zonder bescherming) de link aanklikte.

Afhankelijk van de versie is een ZeuS toolkit voor 700 tot 4000 dollar te koop, of sommige versies zelfs om niet. Afgemeten aan de criminele winst die met het stelen van inloggegevens van banken binnengehaald kan worden, een schijntje.[40]



Figuur 4-3 Het aantal gemonitorde Command & Control servers (bron: Shadowserver, augustus 2010)

[35] AWPG, Phishing Activity Trends Report, 3rd Quarter / 2009
[36] KLPD (2010)
[37] MessageLabs, Intelligence, april 2010
[38] KLPD (2010); Nicolas Falliere and Eric Chien, ZeuS: King of the Bots, 2009; Secureworks, ZeuS Banking Trojan Report, 2010
[39] KLPD (2010)
[40] Zie AD.nl, België legt fraude met onlinebankieren bloot, 24 juli 2010 voor een voorbeeld van een succesvolle aanval die met ZeuS is uitgevoerd

gemonitorde C&C-servers van botnets de afgelopen jaren is verdubbeld en daarna min of meer stabiliseert.[41] Omdat ShadowServer slechts een beperkt deel van het internetverkeer ziet, staat in deze grafiek een deel van het totaal aantal C&C-servers.

Spam blijft omvangrijk

Per dag worden per e-mail alleen al 100 tot 200 miljard spamberichten verstuurd. Dit is 88 tot 92% van het totaal aantal verzonden e-mailberichten.[42] Nederland komt met percentages tussen de 90 en 92% van al het ontvangen e-mailverkeer al jaren voor in de top 10 van meest gespamde landen.[43] De totale schade van spam voor de Nederlandse samenleving is niet bekend. De direct toewijsbare economische schade van een onderzochte spamaanval van 4,5 miljoen berichten (De Thuiswerkcentrale) is op ruim 1,6 miljoen euro geschat. Het merendeel was het gevolg van het ingaan op het spambericht (het bellen van een telefoonnummer met hoge gesprekskosten). De rest, voornamelijk herstelkosten, bedroegen ruim 250.000 euro.[44]

De economische schade van spam zit in deze case dus vooral in de gevolgschade, die ontstaat door in te gaan op de inhoud van het spambericht. Dit kan velerlei vormen aannemen, zoals het verleiden tot het bellen van een betaalnummer, het klikken op een link naar een website met malware of het invoeren van inloggegevens. In veel gevallen hebben we het dan eigenlijk over de schade van phishing.

Skimming

Skimming is het buitmaken van debit- en creditcardgegevens om op naam van slachtoffers betalingen te doen. Bankpassen en creditcards zijn voorzien van een magneetstrip die door skimmers gekopieerd wordt door hardwarematige aanpassingen in kaartlezers in pin- of betaalautomaten. De pincode wordt achterhaald met een verborgen camera of door het afluisteren van het toetsenbord.

Social engineering verhoogt slagingskans aanval

Om de slagingskans van hun aanvallen te verhogen, gaan cybercriminelen steeds gerichter te werk op specifieke slachtoffers. In openbare bronnen als sociale netwerken is veel persoonlijke informatie beschikbaar. Met deze informatie worden mensen verleid tot het verstrekken van vertrouwelijke informatie, zoals (inlog)codes en wachtwoorden om beveiligingsmaatregelen te omzeilen.
Een ander (ironisch) voorbeeld is de opkomst van steeds professionelere nep-antivirusprogrammatuur, compleet met updates, handleiding en ondersteuning vanuit een callcenter. De eindgebruiker denkt hiermee een veiligere computer te krijgen, maar wordt juist tegen betaling besmet.

4.2 Ontwikkelingen in aanvalsmethoden

De technische aanvalsmethoden ontwikkelen zich door. De specialisering en professionalisering van de wereldwijde cyber underground economy draagt hier aan bij.[45] Steeds worden nieuwe zwakke plekken gevonden, onderling gedeeld (meestal tegen betaling) en uitgenut. Bedrijven en burgers nemen beveiligingsmaatregelen tegen bestaande aanvalsmethoden, maar cybercriminelen reageren daar snel op met aanpassingen (bijvoorbeeld door aanpassingen in malware) of combinaties van aanvalsmethoden om de beveiligingsmaatregelen opnieuw te omzeilen. Bovendien worden technieken toegepast die aanvallen moeilijker detecteerbaar maken. Echt volstrekt nieuwe aanvalsmethoden zijn het afgelopen jaar niet waargenomen. Het is vooral doorontwikkeling van bestaande methoden.

Botnets

Door de verbeteringen in de verspreiding van malware zijn botnets nog steeds relatief makkelijk op te zetten. Door botnets decentraal aan te sturen zijn de Command & Control servers minder zichtbaar en kunnen de botnetbeheerders bots makkelijker van updates voorzien en beter beheren. Botnets zijn hierdoor moeilijker te bestrijden.

Combinaties van aanvalsmethoden zorgen voor meer succes

In malware worden meerdere verspreidingstechnieken ingebouwd om een zo groot mogelijke verspreiding te realiseren en detectie te vermijden. Naast het verspreiden van dezelfde malware via e-mail, kan dit ook via websites, netwerken, netwerkschijven en USB-sticks gebeuren.

[41] http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts. De dips zijn veroorzaakt door problemen met de database van Shadowserver. De abrupte stijging van het aantal C&C servers begin 2010 is een verandering in de meting, geen abrupte toename van het aantal C&C servers

[42] Messaging Anti-Abuse Working Group (MAAWG), Email Metrics Program: The Network Operators' Perspective Report #12 – Third and Fourth Quarter 2009, March 2010

[43] O.a. in de maandelijkse MessageLabs Intelligence reports

[44] Van Eeten e.a. (2009)

[45] KLPD (2010)

Aanvalsmethoden groeien ook mee met ontwikkelingen op het internet. Misbruik volgt gebruik. In de combinaties wordt namelijk tegenwoordig ook cloudcomputing toegepast, waarbij het mede door het doorverhuren van diensten moeilijk herleidbaar naar de crimineel is. Ook sociale netwerken en peer-to-peer verbindingen worden ingezet voor het verspreiden van spam of het aansturen van botnets. In toenemende mate worden sociale media als Hyves, Facebook, Twitter en MySpace gebruikt om spam te verspreiden.[46]

Meer unieke malware om virusscanners te omzeilen

Er is een sterke groei van het aantal gevonden unieke varianten van malware.[47] Om virusscanners te omzeilen distribueren cybercriminelen malware in veel verschillende varianten, waarbij één variant een beperkt aantal keer gedistribueerd wordt. Virusscanners die gebaseerd zijn op het herkennen van kenmerken van malware worden daardoor minder effectief, omdat er slechts op een beperkt aantal verschillende kenmerken gescand kan worden. De gemiddelde omvang van malwarecode neemt verder af en veel malware is in staat om zich om te vormen, zodat het nog moeilijker detecteerbaar is.[48]

Aanvallen steeds minder zichtbaar in cyberspace

Op basis van ontdekte zaken, bestaat er het sterke vermoeden dat een groeiend deel van de aanvallen niet meer zichtbaar is met bestaande middelen, of pas nadat de schade is ontstaan. Zeker voor digitale spionage, cyberwarfare en zware cybercriminaliteit is dit interessant.[49]

Verhullen van criminele activiteiten

Criminelen worden beter in het toepassen van technieken als versleuteling van berichtenverkeer en computerfiles (cryptocontainers). Het gebruik van proxy's (tussenstations) en botnets of cloudcomputingtoepassingen bemoeilijken ook de opsporingsactiviteiten door politie en het onderzoek door het Nederlands Forensisch Instituut (NFI).

Shadows in the Cloud

In het Shadows in the Cloud rapport wordt een geavanceerde aanval met verschillende technieken beschreven, in dit geval voor digitale spionage.[50] Via phishingmails werden gericht computers van uitgekozen personen besmet met malware. Deze malware kon ongemerkt documenten wegsluizen, de camera en microfoon van de computer op afstand aan- en uitzetten om conversaties en het toetsenbord af te luisteren. Het betrof onder andere computers op het kantoor van de Dalai Lama en de Indiase overheid. Ook een computer op een NAVO-basis in Nederland was besmet.

De besmette computers werden via een complexe, gelaagde Command & Control infrastructuur aangestuurd. Deze infrastructuur maakte gebruik van sociale media, zoals Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com and Yahoo! Mail. Deze laag leidde besmette computers naar accounts op wisselende gratis webhostingservices en vervolgens naar Command & Control servers in China.

[46] KLPD (2010)
[47] Symantec, Internet Security Threat Report 2009, april 2010
[48] KLPD (2010). Dit wordt ook wel polymorfie genoemd
[49] Information Security Forum Limited (2010)
[50] Zie Shadows in the Cloud, Information Warfare Monitor / Shadowserver Foundation, 2010


Card

5
Manifestaties van cybercrime

Een dreiging manifesteert zich pas als een aanvalsmethode daadwerkelijk wordt gebruikt. In dit hoofdstuk is opgenomen welke trends er zich voordoen op gebied van cybercrime, vanuit verschillende motieven: economische, ideologische of politieke. Aan de orde komen cybercrime (in enge zin), illegaal gebruik van internet om politieke redenen, digitale spionage en cyberwarfare.

5.1
Cybercrime wordt geavanceerder en gerichter

Wat is cybercrime?
Cybercrime omvat elke strafbare gedraging voor de uitvoering van cybercrime waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is. De term 'geautomatiseerde werken' slaat hierbij niet alleen op computers, maar ook op bijvoorbeeld mobiele telefoons, creditcards en andere vormen van geavanceerde technologie.

Voor bijna alle vormen van criminaliteit wordt tegenwoordig in meerdere of mindere mate gebruikgemaakt van ICT. Bij cybercriminaliteit gaat het om die criminele gedragingen waarbij ICT van overwegende betekenis is en die dus niet of moeilijk zonder ICT zouden kunnen plaatsvinden.
Cybercriminaliteit kent vele verschijningsvormen. Enerzijds zijn er strafbare gedragingen die niet zonder tussenkomst of gebruik van ICT gepleegd kunnen worden en waarbij ICT naast middel ook doelwit is. Denk aan inbreuk op het exclusieve gebruik van iemands systemen, zoals skimming, inbreken in computers om gegevens af te tappen (bijvoorbeeld creditcard- of andere persoons- of bedrijfsgegevens) of hun verwerkingscapaciteit te benutten (bijvoorbeeld als zombie voor botnets). Andere voorbeelden zijn defacing, DDOS en andere vormen om de werking van ICT te verstoren.
Anderzijds zijn er strafbare gedragingen, die met behulp van ICT worden uitgevoerd (als middel). Vaak gaat het dan om criminaliteit die ook al in fysieke vorm bestaat: kinderporno, opruiing, stalking, illegale handel of kansspelen, frauderen, oplichting of afpersing. Er is dus sprake van digitalisering van traditionele criminaliteit en niet van nieuwe vormen van criminaliteit.
Hightech crime in de definitie van het KLPD is cybercrime uit de eerste groep strafbare gedragingen, indien sprake is van (innovatieve) vormen van zware en georganiseerde misdaad. Kenmerkend zijn een hogere organisatiegraad, gebruik van geavanceerde digitale technologie en complexe ICT-systemen en -netwerken.

Technische specialisten hebben de leiding
Bij hightech cybercrime hebben technische specialisten de leiding. Zij zoeken hun doelwitten steeds gerichter uit en benaderen ze ook gerichter, bijvoorbeeld door ze in hun eigen taal aan te spreken bij mails en websites voor phishing. Dit verhoogt hun slagingskans. Technisch specialisten bepalen doelwit en modus operandi terwijl minder kundige criminelen specifieke taken uitvoeren, verspreid over de hele wereld als dat nodig is. Op die manier zijn cybercriminelen in staat om internationaal te operen en snel de buit te verzilveren.[51] De innovaties van de technische specialisten worden daarna door anderen gekopieerd en doorverkocht.

[51] Zie Shadows in the Cloud, Information Warfare Monitor / Shadowserver Foundation, 2010

Via internetfora wisselen ze kennis én diensten uit, al dan niet tegen betaling.[52] Zo ontstaan er (ad hoc) virtuele netwerken waarin verschillende specialismen met elkaar samenwerken. Denk aan ontwerpers van malware, ontwerpers van phishingsites, doorverkopers van persoonsgegevens, verzenders van spam, bouwers van botnets, verhuurders en verkopers van botnets, hosters van malafide websites en botnets, gebruikers van botnets en witwassers van geld (money mules).

De groei van de internetfora met allerlei niet vertrouwde of weinig toevoegende newbies en de onderkende infiltratie van internetfora door opsporingsdiensten heeft ertoe geleid dat de echte cybercrimespecialisten zijn ondergedoken op exclusievere (Russischtalige) fora of op een andere manier contact met elkaar hebben.[53] Voor grotere, complexere aanvallen is ook een hogere organisatiegraad nodig dan alleen de contacten via internetfora. Dit wordt dan ook in opsporingszaken aangetroffen.

Het KLPD signaleert ook dat bepaalde specialismen in hightech cybercrime vaak zijn terug te leiden naar steeds dezelfde landen van herkomst. Op basis van verschillende onderzoeken geeft het Team High Tech Crime voorzichtig een lijst met topherkomstlanden van illegale activiteiten met Nederland als doelwit. Dit wil niet zeggen dat specialismen niet afkomstig kunnen zijn uit andere landen, maar dat dit minder vaak voorkomt. Het komt overigens ook vaak voor dat cybercrime wordt gepleegd door groeperingen die afkomstig zijn uit het genoemde land, maar daar niet wonen.[54]

De snelle en stabiele Nederlandse internetverbindingen en de goede dienstverlening hebben een negatief neveneffect. In enkele zaken is geconstateerd dat Nederlandse ICT-voorzieningen zijn gebruikt voor internationale criminele activiteiten, zoals het hosten van phishing-sites, het huisvesten van illegale hackerfora en het tijdelijk opslaan van gestolen data in dropzones bij Nederlandse bullet proof hostingbedrijven.[55] Het leidt er in de praktijk toe, dat buitenlandse opsporingsdiensten een substantieel aantal rechtshulpverzoeken doen aan Nederland voor informatie over in Nederland uitgevoerde activiteiten.

ZeuS streng beveiligd tegen kopiëren[57]
De auteur(s) van het ZeuS botnet hebben de code van de nieuwste versie van hun toolkit beveiligd tegen kopiëren met een licentiesysteem, dat sterk doet denken aan de beveiliging van legale software. De toolkit kan maar op één computer van de koper draaien, met een door de auteur verstrekte digitale sleutel. ZeuS was een van de eerste, zo niet de eerste botnet-toolkit die met zo'n beveiliging is uitgerust.

Het illegale circuit heeft zich geprofessionaliseerd tot een digitale underground economy met een hoge innovatiegraad, snelle onderlinge communicatie en handel. Oudere en simpele versies van malware zijn nog gratis of voor enkele tientallen dollars te krijgen, maar geavanceerdere malware en diensten kosten al snel in de orde van duizenden dollars. De eigenaren van dergelijke diensten hechten daarom ook steeds meer aan hun auteursrecht en beveiligen zich tegen illegaal kopiëren.[56]
Steeds meer hightech middelen komen via deze underground economy ook beschikbaar voor 'lowtech' criminelen.[58] Een voorbeeld hiervan is de verkoop van kant-en-klare botnets, inclusief videohandleiding.[59]

Lowtech crime: traditionele criminaliteit lift mee met cybercrime

Cybercrime is gezien de groeiende beschikbaarheid van hulpmiddelen niet langer het exclusieve domein van specialisten. Ook andere criminelen maken gebruik van ICT (en digitale aanvalsmethoden in het bijzonder) voor steeds meer vormen van traditionele criminaliteit. Uit onderzoek in politiedossiers blijkt dat er een grote groep daders is die – meestal individueel – vooral kleinere cybercrimedelicten

[52] Zie KLPD (2010) voor een veel uitgebreidere beschrijving van de verschillende specialismen en de digitale underground economy als geheel
[53] Zie KLPD (2010)
[54] Zie KLPD (2010)
[55] Zie KLPD (2010)
[56] Zie KLPD (2010)
[57] Secureworks (2010)
[58] Online Identity Theft, OECD 2009, (p28); Canadian Security Intelligence Service, Transnational criminal activity: a global context, 2000; Choo, Trends in Organized Crime, 2008, (p273)
[59] De website 'bullet proof hosting' biedt bijvoorbeeld 'bulk email service' (spamservice) aan inclusief instructievideo. http://www.sendbulkemail.net/nl/bullet-proof-dedicated-servers

pleegt.[60] Cybercrime is voor hen aantrekkelijk vanwege de lage investeringskosten (zeker afgezet tegen de verwachte opbrengst) en de lage pakkans in vergelijking tot die van 'offline' criminaliteit.[61]

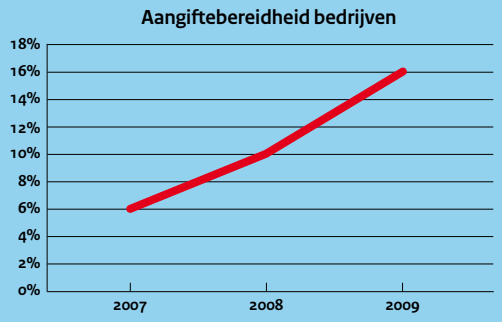
Oplichting via internet
Een 31-jarige man bood vorig jaar via Marktplaats.nl spullen te koop aan. Hij inde het geld maar leverde niets. De verdachte bediende zich van diverse schuilnamen, maar zijn werkwijze was steeds identiek. Hij bood gewilde producten aan zoals spelcomputers en fototoestellen, maar ook een scooter. De man plaatste er een plaatje bij van een scooter in een huiselijk omgeving, zodat de aanbieding vertrouwd overkwam. De slachtoffers waren uit het gehele land afkomstig.

De focus op financieel gewin betekent niet dat alle internetcriminelen ruim verdienen aan hun illegale praktijken. Hightech criminelen maken meer winst dan hun lowtech collega's. Dit wordt ook wel de tragedy of the commons genoemd. De specialisten bezetten door hun kennisvoorsprong als eersten de interessantste doelwitten; de grotere groep die erna komt, verdient gemiddeld minder aan de overblijvende doelwitten. Het ontbreekt de eenvoudige crimineel vaak aan kennis en het netwerk om gerichte aanvallen uit te voeren op interessante doelwitten en om een eventueel vergaarde buit van enige omvang in de echte wereld te verzilveren.

Omvang en aangiftebereidheid

Over de totale omvang van cybercrime met Nederlandse slachtoffers is nog weinig bekend. Er zijn beperkt metingen gedaan, maar er zijn op basis daarvan geen uitspraken over de omvang mogelijk. Uit onderzoek van politiedossiers blijkt wel dat van geregistreerde meldingen en aangiften van twee onderzochte regiokorpsen minder dan 1% cybercrime betreft.[62] In een anonieme enquête gaf één op de acht organisaties aan, dat er bij hen in de afgelopen twaalf maanden fraude had plaatsgevonden door misbruik van computersystemen. Bij tweederde daarvan gebeurde dat meer dan eens.[63]

Dergelijke cijfers zeggen nog niet alles over de omvang, want er wordt een aanzienlijke hoeveelheid niet-geregistreerde criminaliteit vermoed.[64]



Figuur 5-1: Aangiftebereidheid van bedrijven[67]

De bereidheid van burgers en bedrijven om aangifte te doen van cybercrime is namelijk niet erg hoog. Uit een (kleinschalige) internetenquête blijkt bijvoorbeeld een aangiftebereidheid van 4%.[65] Dit is aanzienlijk lager dan voor traditionele criminaliteit (ongeveer 27%).[66] Mogelijke oorzaken die worden genoemd zijn de beperkte impact op het slachtoffer en angst voor imagoschade (vooral bij bedrijven). Bij bedrijven wordt in onderzoeken van Ernst & Young een hogere en stijgende aangiftebereidheid gevonden, vooral bij grote organisaties. Specifiek voor skimming doet Equens namens de banken aangifte per geskimde geld/betaalautomaat, in 2009 in totaal 1263 keer. De gedupeerde klanten hoeven dus niet zelf aangifte te doen per afzonderlijk geval.[68]

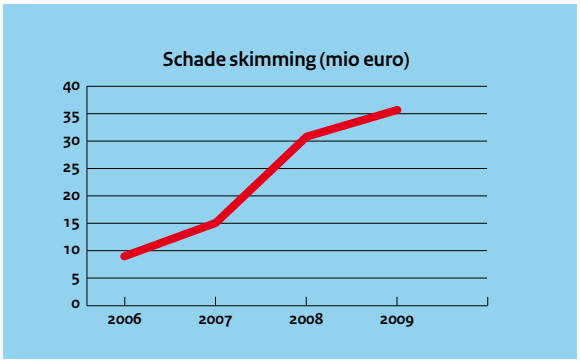
Effect van de trend

Cybercrime raakt vooral het economisch belang van Nederland. Daarnaast zijn privacy en de andere belangen in het geding, maar in mindere mate.

De financiële schade bestaat uit directe schade (het gestolen geld) en uit indirecte schade (kosten voor herstel, onderzoek, aangifte, etc.). Ook brengt een

60 E.R. Leukfeldt, M.M.L. Domenie & W.Ph. Stol. Verkenning Cybercrime in Nederland 2009, 2010
61 IC3, 2010. FBI – Department of Justice
62 Leukfeldt et al., 2010
63 Ernst & Young (2010)
64 Leukfeldt et al., 2010
65 Leukfeldt et al., (2010)
66 CBS, Integrale Veiligheidsmonitor, landelijke rapportage 2009, 2010
67 Naar: Ernst & Young (2010) en dezelfde rapporten over 2008 en 2007
68 www.nvb.nl

dreiging van hightech crime voor bepaalde sectoren zoals banken hoge kosten met zich mee voor preventieve maatregelen. De indirecte schade kan gemakkelijk oplopen tot tien keer de opbrengst voor de cybercrimineel.[69]



Figuur 5-2 Schade door skimming in Nederland (in miljoenen euro's) (Bron: NVB)

De totale directe financiële schade als gevolg van hightech crime in Nederland is niet bekend. In 2009 betrof in Amerika de gerapporteerde schade 560 miljoen dollar en in Groot-Brittannië 440 miljoen pond.[70] Openbare schadecijfers van hightech cybercrime in Nederland betreffen vooralsnog alleen skimming. In 2009 bedroeg de schade voor banken door skimming 36 miljoen euro; dat is zestien procent meer dan het jaar ervoor. (Zie figuur 5-2) Met de invoering van een chip op de pinpas (EMV) en prioritering van de aanpak van skimming door politie en justitie verwacht de Nederlandse Vereniging van Banken (NVB) dat de stijgende trend zal worden gekeerd en de schade als gevolg van skimming in 2010 en 2011 zal afnemen.

Ter illustratie van de schade van lowtech cybercrime: bij het bestuderen van 271 politiedossiers met daarin de materiële schade van natuurlijke personen door cybercrime werden bedragen van 12 tot 67.224 euro gerapporteerd. In de 20 dossiers met schade die bedrijven hadden geleden, werden bedragen van 50 tot 40.500 euro gerapporteerd. Incidenteel kan de schade hoog oplopen, maar in de meeste gevallen ligt de schade onder de 500 euro.[71]
De impact op privacy van burgers betreft vooral identiteitsdiefstal voor fraude met online betalingsverkeer (winkels, bancair). Voor de individuele slachtoffers kan dat grote impact hebben. Verder wordt er bij cybercrime misbruik gemaakt van gegevens die burgers vrijwillig delen via internet, bijvoorbeeld om social engineering technieken succesvol toe te kunnen passen (wat zijn iemands interesses?). Ook diefstal van grote bestanden met persoonsgegevens schaden het privacybelang. Voor cybercriminelen zijn dit soort bestanden van grote waarde.

Er zijn andere effecten van criminaliteit, maar die zijn beperkt van omvang. De door cybercrime veroorzaakte maatschappelijke onrust is niet groot. Dergelijke onrust is overigens wel voorstelbaar wanneer belangrijke bedrijven grote schade ondervinden en op grote schaal vertrouwelijke gegevens worden ontvreemd of op straat komen te liggen.

Van een andere orde zijn de (indirecte) effecten die ontstaan wanneer Nederlandse (ICT-)voorzieningen worden misbruikt voor cybercrime. De dienstverlening van op zichzelf legale bedrijven aan cybercriminelen zorgt voor een vermenging van de onder- en bovenwereld. Rechtshulpverzoeken uit het buitenland en Notice and Take Down-verzoeken zorgen voorts voor additioneel werk voor overheidsdiensten en ISP's.

5.2
Illegaal gebruik internet om politieke redenen veelal gericht op bedreigingen, defacements en propaganda

Politiek gedreven illegaal gebruik van internet door niet-statelijke actoren is grofweg in drie categorieën onder te brengen: het gebruik van het internet als doelwit (gericht tegen het internet zelf of de infrastructuur ervan), als wapen (via het internet fysieke doelen treffen, bijvoorbeeld in de vitale sectoren) of als middel (ondersteunende doeleinden zoals informatie-inwinning, financiering, fondsenwerving, propaganda, rekrutering, creatie van virtuele netwerken, onderlinge communicatie en planning en training).[72]

Welke vormen van illegaal gebruik van internet om politieke redenen zijn er?

Er zijn verschillende dadergroepen die om uiteenlopende politieke redenen op illegale wijze gebruikmaken van het internet. Onderscheid valt te maken tussen activisme – activiteiten binnen de grenzen van

[69] Cormac Herley, So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users, 2009
[70] IC3 (2010): 560 miljoen dollar in de VS in 2009; http://www.ukpayments.org.uk/resources_publications/key_facts_and_figures/card_fraud_facts_and_figures/: 440 miljoen pond in 2009 in Groot-Brittannië,
[71] Leukfeldt et al., (2010)
[72] NCTB Jihadisme Update 2009, 2010

de wet – extremisme – activiteiten waarbij bewust de wet wordt overtreden – en terrorisme – dreigen met, voorbereiden of plegen van daden gericht op maatschappijontwrichtende zaakschade.

Er zijn vele gevallen in Nederland bekend van bedreigingen via het internet van politici, gezagsdragers, opiniemakers en anderen, waaronder uitgezonden militairen. Enkele malen is Nederland geconfronteerd met zogeheten defacements om een politiek statement te maken. Propaganda van uiteenlopende aard vanuit activisten, extremisten en terroristen komt veelvuldig voor. Niet alle vormen van propaganda zijn strafbaar, maar ook niet-strafbare propaganda vormt een voedingsbodem voor radicalisering.

Illegaal gebruik van het internet om politieke redenen beperkt zich vooral tot activistische uitingen. Dit zijn vooral activiteiten waarbij internet als middel wordt benut. Door jihadistische groeperingen (die een terroristische doelstelling hebben) wordt het internet vooral gebruikt als interactief communicatiemedium en daarbinnen vooral voor het verspreiden van propaganda, en bij de voorbereiding van aanslagen. Politieke en dierenrechtenactivisten richten zich mondiaal primair op verminkingen van websites (defacement) en (Distributed) Denial of Service (D) DoS aanvallen,[73] en in Nederland op naming & shaming van organisaties of personen op internetfora.[74] Doorgaans is het specifieke motief het vragen om aandacht voor een bepaalde sociale of politieke kwestie. Aangezien in veel gevallen bij defacements gebruikgemaakt wordt van hackingtechnieken, wordt een dergelijke uitingsvorm ook wel 'hacktivisme' genoemd.

Tot de digitale gereedschapskist van activisten, extremisten en terroristen behoren voornamelijk eenvoudige, minder geavanceerde middelen. Incidenten blijven dan ook hoofdzakelijk beperkt tot activistische uitingen zoals het hacken of verminken van websites, posten op fora, verspreiden van propaganda en het bedreigen van personen, al dan niet op basis van via sociale media verkregen informatie.
Het hacken en verminken van websites van bedrijven, politieke kopstukken of overheden c.q. instanties waartegen men aversie heeft, komt ook in Nederland voor. Een voorbeeld hiervan is de defacing van de website van Geert Wilders op 14 juli 2006.[75] Over langere tijd gemeten werden in Nederland naar schatting zo'n 20.000 websites door defacementacties getroffen naar aanleiding van de film Fitna uit 2008.[76] In het buitenland ziet men dit meer, bijvoorbeeld in het Palestijns-Israëlisch conflict, waarbij door verschillende partijen defacements worden toegepast. Ook Denemarken had met dit fenomeen te maken tijdens de 'cartooncrisis'. Overigens is niet elke defacement onderdeel van hacktivisme, het kan ook gaan om uitingen van (cyber)vandalisme.[77]
Dieren- en milieuactivisten richten zich meer op het publiekelijk te schande maken van individuen op het internet (naming & shaming).[78] Daarbij worden persoonlijke gegevens gepubliceerd van mensen die betrokken zijn bij een organisatie die volgens de betreffende activisten niet door de beugel kan. Dit tast de privacy van betrokkenen aan en kan (indirect en soms onbedoeld) leiden tot gevaarzetting voor deze mensen en hun bezittingen.[79]

Dicht bij huis is een serieuze variant van illegaal gebruik van internet om politieke redenen, de bedreiging door (mogelijk jihadistische) kwaadwillenden die zich tegen de Nederlandse missie in Afghanistan keerden. Door gebruik te maken van op publieke sociale netwerken geplaatste persoonlijke informatie, bijvoorbeeld over een uitgezonden familielid, komen mensen in beeld als doelwit. Het is meermaals voorgekomen dat deze mensen vervolgens bedreigingen ontvingen per telefoon, e-mail, chat of sms.[80] Ook politici of andere individuen die zich over bepaalde politiekgevoelige kwesties uitspreken worden op dergelijke wijze opgespoord en bedreigd. Op deze manier komt pijnlijk naar voren hoe er misbruik gemaakt kan worden van persoonlijke gegevens die met een heel ander doel op internet geplaatst werden.

Cyberaanvallen om politieke redenen gericht tegen het internet zélf of tegen fysieke (vitale) installaties via het internet (internet als doelwit en als wapen), zijn in Nederland nog niet waargenomen. Ook specifieke uitspraken of intenties van jihadisten, gericht op dit soort complexe cyberaanvallen tegen

[73] Zie Steven Murdoch, Destructive Activism: The Double-Edged Sword of Digital Tactics, in: Mary Joyce ed., Digital Activism Decoded, 2010
[74] Jaarverslag AIVD 2009, april 2010
[75] KLPD (2010); Zie bijvoorbeeld http://www.security.nl/artikel/13983/Website_Geert_Wilders_gehackt.html
[76] NCTB Jihadisme Update 2009, 2010
[77] Op www.zone-h.com en (o.a.) Arabische varianten daarvan delen defacers hun successen
[78] Jaarverslag AIVD 2009, april 2010
[79] Murdoch (2010)
[80] Zie http://www.elsevier.nl/web/Nieuws/Nederland/260564/Familieleden-Uruzgantroepen-worden-bedreigd.htm

Nederlandse doelen zijn niet bekend.[81] Vanuit andere landen zijn echter wel voorbeelden bekend die al naar gelang de achterliggende intenties over de verschillende categorieën heen schuiven. Dergelijke cyberaanslagen zijn gezien de geïdentificeerde kwetsbaarheden echter ook in Nederland voorstelbaar en lijken aantrekkelijk voor terroristische groeperingen vanwege de potentieel grote gevolgen. De toenemende afhankelijkheid van ICT in onze maatschappij kan nog een versterkend effect hebben op de impact. Openlijke fondsenwerving en misbruik van liefdadigheidsinstellingen door jihadisten voor financiering van hun acties is goed mogelijk, maar wordt weinig waargenomen.[82] Phishing en fraude door terroristische groeperingen in het algemeen neemt toe, maar deze groeperingen lopen in technologische zin achter bij de georganiseerde cybercriminaliteit.[83]

Effect van de trend

Het effect van de trend, dat illegaal gebruik van internet om politieke redenen zich voornamelijk beperkt tot activisme is tweeledig. Enerzijds is geconstateerd dat de zichtbare uitingsvormen zich beperken tot gebruik van internet als (communicatie) middel en als faciliteit voor het hacken en defacen van websites. Anderzijds is geconstateerd dat tal van kwetsbaarheden en theoretische aanvalsscenario's tegen het internet zelf of tegen de vitale infrastructuur met internet als wapen voorstelbaar zijn.

Het huidige effect van de trend, de beperking tot uitingen van activisme, is momenteel niet bijzonder groot, al kunnen bepaalde vormen van activisme of bedreigingen op de fysieke veiligheid van individuele slachtoffers en hun privacy wel degelijk een grote impact hebben.

Alhoewel een succesvolle terroristische cyberaanval niet is waargenomen en op grote schaal niet waarschijnlijk wordt geacht, is zij op beperkte schaal wel mogelijk. Mocht een dergelijk geval zich voordoen, dan kan dat de territoriale integriteit van Nederland sterk beïnvloeden.

De fysieke veiligheid wordt aangetast indien een dergelijke aanval succesvol wordt uitgevoerd. Economische veiligheid kan een primair doelwit zijn, maar kan ook als secundair effect worden geraakt.

Het verstoren van sociale en politieke stabiliteit is een van de doelen van terroristen. Het is niet duidelijk hoe gemakkelijk dit doel bereikt kan worden met een cyberaanval. Propaganda is hier nadrukkelijk wel op gericht, omdat het bijdraagt aan radicalisering. Jihadistische propaganda via het internet is verder geprofessionaliseerd, heeft een groot bereik en kent relatief weinig weerwoord.[84]

De privacy van burgers is in het geding wanneer het activisme, extremisme of terrorisme zich richt op het gebruiken of misbruiken van persoonsgegevens, of op specifieke individuen. Bijvoorbeeld voor naming & shaming, of voor 'werven van fondsen' via online fraude.

5.3 Digitaal instrumentarium maakt spionage effectiever

Wat is digitale spionage?
Digitale spionage is het verwerven van inlichtingen langs digitale weg. Dit wordt ook wel cyberspionage of e-spionage genoemd. Zowel overheden als bedrijven kunnen digitale spionage inzetten ten bate van hun diplomatieke, militaire of economische belangen.

De AIVD neemt in zijn contraspionageonderzoeken waar dat in Nederland verschillende buitenlandse inlichtingendiensten actief zijn met het heimelijk vergaren van inlichtingen.[85] Zo proberen buitenlandse inlichtingendiensten gevoelige informatie te verwerven over de infrastructuur van de telecomsector. Verder staan gerubriceerde en andere vertrouwelijke (overheids)documenten op politiek, militair en economisch terrein in de belangstelling, ten bate van het eigen belang.

In de rapportage van de AIVD over spionagerisico's zijn de kernbelangen, kwetsbaarheden en methoden van informatie inwinnen beschreven.[86] Dit onderzoek richt zich op spionagerisico's op het terrein van economisch welzijn en wetenschappelijk potentieel, openbaar bestuur en vitale infrastructuur.
De kernbelangen zijn onderverdeeld in de volgende

[81] NCTB (2010)
[82] NCTB (2010)
[83] KLPD (2010)
[84] NCTB (2010)
[85] Zie de AIVD jaarverslagen 2008 en 2009 en Kwetsbaarheidsanalyse spionage. Spionagerisico's en de nationale veiligheid, 2010
[86] AIVD (2010)

categorieën: datasets en blauwdrukken, standpunten en strategie, en opkomende kernbelangen en infrastructuur. Het bewustzijn van de spionagerisico's in de onderzochte sectoren is vaak laag.

Enerzijds proberen inlichtingendiensten informatie te verkrijgen via de inzet van technische middelen zoals hacken, tappen en afluisteren en anderzijds via mensen die (indirect) toegang hebben tot deze informatie.

Gevoelige gegevens in systemen zijn kwetsbaar door de toenemende verwevenheid en complexiteit van informatiesystemen, het uitbesteden van activiteiten zoals het beheer van systemen evenals het koppelen van informatiesystemen. Ook cloudcomputing kan potentieel leiden tot kwetsbaarheden. Methoden om technische toegang te verkrijgen richten zich op de interceptie van vaste en draadloze telecommunicatie, en het afluisteren of fysiek stelen of kopiëren van computersystemen. Ook wordt phishing en gerichte malware ingezet om informatie te vergaren en te versturen.

Naast technische toegang kan de mens toegang geven tot gevoelige informatie. In toenemende mate wordt hierbij gebruikgemaakt van informatie op internet zoals die beschikbaar is via zoekmachines en in sociale netwerken als LinkedIn, Facebook en Hyves. Mensen zijn zich niet altijd bewust van de informatie waarover zij beschikken. Ook is men onbekend met de doelen en werkwijzen van inlichtingendiensten. Methoden die worden toegepast om informatie van personen te verkrijgen zijn social engineering en chantage. Ook kunnen personen bewust informatie prijsgeven, bijvoorbeeld voor persoonlijk gewin of wraak.

Internationaal technisch onderzoek naar digitale spionage laat zien dat 60% van de (bekende) slachtoffers van digitale spionage werkt in midden- en hogere managementlagen (met rollen als director, vicepresident, senior official, manager of executive director).[87] Het zijn niet alleen diplomaten en defensiespecialisten, maar ook mensen uit de financiële wereld, mensenrechtenactivisten of wetenschappers. Het accent lijkt te liggen op Aziaten en personen die zich bezighouden met dossiers over het Verre Oosten.

De vraag of spionage succesvol zou zijn geweest, wordt door deze onderzoekers bevestigd. "It was surprisingly straightforward to identify a great deal of information about the individuals being targeted; the Internet provided plenty of information on around 84% of the individuals in most targeted attacks." Dergelijke, vooral publieke informatie is op zichzelf mogelijk nuttig, maar kan ook worden beschouwd als voorwerk voor verdere spionageactiviteiten.

Operatie Aurora
Op 12 januari 2010 maakte Google bekend, dat Chinese hackers zich met geavanceerde technieken toegang hadden verschaft tot mailaccounts van Chinese mensenrechtenactivisten. Naast de illegale toegang tot mailaccounts, werd ook intellectueel eigendom van Google zelf ontvreemd. De operatie heet Aurora, omdat beveiligingsbedrijven later in de code van gebruikte malware die naam ontdekten. Vermoedelijk noemden de hackers hun operatie ook zo.

Digitale spionage verzwaart de dreiging van 'gewone' spionage. Het digitale instrumentarium stelt aanvallers in staat sneller toegang te krijgen tot meer informatie en snel tot diepere bronnen in een organisatie door te dringen. Digitale spionage is dus effectiever en efficiënter en dat wordt bevorderd doordat aanvalsmethoden voortdurend ontwikkelen en het risicobewustzijn van spionage vaak laag is.

Effect van de trend
Digitale spionage kan bijvoorbeeld de territoriale integriteit in gevaar brengen wanneer een land ondersteuning biedt aan een terroristisch netwerk. Digitale spionage kan ook de economische veiligheid aantasten als bijvoorbeeld bedrijfsgeheimen worden ontvreemd met als gevolg grootschalig verlies van inkomsten en verlies van concurrentiepositie. Ook kan de sociale en politieke stabiliteit aangetast worden door het heimelijk beïnvloeden van het democratisch proces.

5.4
Cyberspace in opkomst als vijfde domein van de krijgsmacht
Diverse landen bouwen capaciteiten op om militaire cyberaanvallen uit te voeren en/of zich er actief tegen te verdedigen in de vorm van afschrikking (cyber deterrence) of preventie (pre-emptive strikes). Veelvuldig genoemde landen zijn: Verenigde Staten, Rusland, China, Israël, Frankrijk, Groot-Brittannië,

[87] Message Labs Intelligence Report (The Nature of Cyber Espionage; Most Malicious File Types Identified and Encrypted Spam from Rustock), March 2010

Duitsland, Noord-Korea, Zuid-Korea, Japan, Taiwan en Iran.[90]

Wat is cyberwarfare?
Cyberwarfare is ongeoorloofde penetratie door, namens of met ondersteuning van een overheid in informatiesystemen en/of netwerken van een andere natie, of elke andere activiteit richting informatiesystemen met als doel toevoeging, verandering of vervalsen van data, of het verstoren of beschadigen van een informatiesysteem, netwerk of het object dat het informatiesysteem controleert.[88] Cyberwarfare is, net als andere vormen van oorlogsvoering, onderdeel van het diplomatieke arsenaal van een staat.
Het verwante begrip cyber defence reserveren we in dit Trendrapport voor het beschermen van vitale (militaire en civiele) voorzieningen tegen cyberwarfare.[89]

De primaire doelwitten van cyberwarfare zijn zowel militair als civiel. Het achterliggend idee is met zo min mogelijk fysieke middelen zo snel mogelijk een militaire tegenstander op de knieën te krijgen. Door vernietiging of manipulatie op afstand van vitale voorzieningen kunnen zowel communicatie en logistiek als moraal worden gebroken. Eventuele fysieke militaire acties ('kinetische oorlogsvoering' in cyberwarfare-taal) zullen dan op minder tegenstand stuiten.

Het bestaan van offensieve capaciteiten (of defensieve met een offensieve kant, zoals bij pre-emptive strikes) is (met publieke bronnen) lastig aan te tonen.

Landen lopen er namelijk zelden mee te koop, de cyberwapens zijn fysiek niet zichtbaar en de feitelijke inzet is beperkt. Bovendien, waar aanvallen wel zichtbaar worden, is niet altijd duidelijk of het om staatsactiviteiten gaat of om acties van niet-statelijke actoren (die al dan niet getolereerd worden door de staat). Attributie is daarmee een probleem.
Eind jaren negentig werd wel duidelijk dat zowel de Verenigde Staten, Rusland als China militaire doctrines ontwikkelden, waarin cyberwarfare een plaats kreeg.[91] Dergelijke doctrines vormen de basis voor militair optreden en de opbouw van de daarvoor noodzakelijke capaciteiten. De genoemde militaire cyber doctrines gaan uit van zowel militaire als civiele doelen. Andere landen volgden later. De UK Cyber Security Strategy uit 2009 bevat bijvoorbeeld offensieve doelstellingen (vanuit defensief perspectief overigens, als afschrikking).

De vorming van militaire organieke verbanden zijn een volgende aanwijzing dat capaciteiten op grote schaal worden ontwikkeld. Denk aan US CYBER COMMAND, 24th Air Force (USAF), US Army Cyber Battallion, de 10th Naval Fleet (US Navy) en de Abteilung Informations- und Computernetzwerkoperationen van de Duitse Bundeswehr.[92]

In het recente verleden zijn voor zover bekend slechts in een beperkt aantal conflicten daadwerkelijk cyberwapens ingezet. Sommige aanvallen vonden parallel plaats aan fysieke conflicten, andere alleen in cyberspace. Bijvoorbeeld de uitschakeling via een cyberaanval van de luchtverdediging bij de Israëlische luchtaanval op een nucleaire installatie in aanbouw in Syrië (2007).[93] Van de cyberaanvallen op Georgië tijdens de Russische interventie in 2008 is onduidelijk of deze acties aangestuurd werden door de Russische overheid (cyberwarfare) of dat de acties enkel werden getolereerd door de overheid (hacktivisme). Verder zijn er steeds meer subtiele en minder subtiele cyberaanvallen geweest in tijden van diplomatieke spanningen, waarbij landen mogelijk een signaal willen afgeven langs digitale weg over hun perceptie van de ernst van de situatie en/of hun macht.[94]

Misschien wel de fraaiste aanwijzing voor de opbouw van cyberwapens zijn de gesprekken van de Verenigde

[88] Richard A. Clarke, Robert K. Knake, Cyber War. The next threat to national security and what to do about it, 2010

[89] Hoewel deze term in de praktijk soms ook wordt gebruikt als eufemistisch alternatief voor cyberwarfare.

[90] Zie ook o.a. Clarke (2010); Jeffrey Carr, Inside Cyber Warfare, 2009; Report: Countries prepping for cyberwar, http://news.cnet.com/8301-27080_3-10399141-245.html; Israel adds cyber-attack to IDF, www.military.com/features/0,15240,210486,00.html; Age of cyber warfare is 'dawning', http://news.bbc.co.uk/2/hi/technology/8363175.stm; http://www.spiegel.de/spiegel/0,1518,606165,00.html; www.thenewnewinternet.com/2010/06/29/uk-has-cyber-attack-capability/; Iran – Enhancing Cyber Defense Capabilities,

[91] Zie Joint Publication 3-13 over Information Operations van het US Departement of Defense, 1999; Unrestricted Warfare van de Chinese kolonels Qiao Liang en Wang Ziangsui uit 1999; over Rusland, zie Carr (2009).

[92] Zie Der Spiegel, Krieg der Zukunft, 9 februari 2009, http://www.spiegel.de/spiegel/0,1518,606165,00.html

[93] O.a. beschreven in Clarke (2010)

[94] Bijvoorbeeld de Noord-Koreaanse '4th of July' aanval op Amerikaanse en Zuid-Koreaanse doelen in 2009, vlak nadat Zuid-Korea bekendmaakte deel te nemen aan de cyber oefening Cyber Storm III. Zie Carr (2009)

Staten, Rusland en vertegenwoordigers van de Verenigde Naties over juist beperkingen van het militaire gebruik van cyberspace.[95]

Aandacht in Nederland neemt toe

Naar aanleiding van de aanval op Estland neemt ook de aandacht in NAVO-verband toe. Tijdens een NAVO-top in 2007 werd besloten om een specifieke NAVO cyber defence policy op te stellen en versterkingen aan te brengen in de eigen verdediging.[96] Tevens accrediteerde de NAVO het Cooperative Cyber Defence Centre of Excellence in Tallinn voor onderzoek en kennisdeling.

In buitenlandse, vooral Amerikaanse, media komt het onderwerp al enkele jaren regelmatig terug op gespecialiseerde internetsites, tijdschriften en boeken. Sinds eind 2009 staat cyberwarfare ook in de belangstelling in Nederland.[97] De motie Knops c.s. van 3 december 2009 constateert dat cyberwarfare niet terugkomt in de Defensiebegroting en verzoekt de regering, vanwege onderkende opbouw van capaciteiten in andere landen, om in interdepartementaal verband een cybersecuritystrategie te ontwikkelen.[98] Met louter defensieve capaciteiten kan volgens de Kamer niet worden volstaan.

In de Defensie Verkenningen krijgen cyberaanvallen en de verdediging ook substantiële aandacht.[99] 'Cyber' is een speerpunt, een van de weinige speerpunten die in alle voorgestelde budgettaire scenario's moet blijven staan, volgens de Verkenningen. Mede naar aanleiding van deze Verkenningen en de motie Knops is het ministerie vervolgens een traject voor de visievorming op cyberoperations gestart bij Defensie. Naast land, zee, lucht en ruimte komt er een vijfde domein bij voor de krijgsmacht: cyberspace.

Effect van de trend

Van alle dreigingen manifesteert cyberwarfare zich op dit moment het minst, maar is het potentiële effect waarschijnlijk het grootst.

Voor Nederland is cyberdefence niet een puur nationale aangelegenheid of afweging. Het NAVO lidmaatschap brengt op zichzelf al verplichtingen met zich mee. In toenemende mate is onze krijgsmacht via digitale lijnen verbonden met netwerken van de NAVO en bondgenoten. Het belang van gezamenlijke bescherming van deze communicatievoorzieningen is evident. Waar Nederland die gebruikt, zal het deze ook mee moeten beschermen tegen aanvallen.

Of een cyberaanval wordt gezien als een aanval in de zin van artikel 5 NAVO, die gezamenlijke reactie vereist, is nog omstreden. Een eventuele offensieve reactie op een cyberaanval op een van de lidstaten zal vooralsnog plaatsvinden met een 'coalition of the willing'[100], offline of online.

Potentieel is de maatschappelijke impact van cyberwarfare aanzienlijk, vanwege het doel (zoals verstoring, vernietiging) en de waarschijnlijke doelwitten in de vitale voorzieningen (zoals elektriciteit, financieel stelsel en telecom). De onderlinge verwevenheid van (internationale) netwerken en systemen kan bij een aanval eenvoudig leiden tot een domino-effect met grote maatschappelijke gevolgen. Hoewel vaak anders gesuggereerd, bestaat er namelijk wel degelijk collateral damage bij cyberaanvallen. Het is misschien ook wel de onderlinge verwevenheid en de angst voor dergelijke oncontroleerbare neveneffecten die inzet van cyberwarfare in toom houdt, zoals bij gewapende conflicten in het algemeen lijkt te gelden.[101] Het verschijnsel dat economische vervlechting leidt tot stabilisatie is overigens niet specifiek voor cyberwarfare. De onberekenbaarheid en snelheid van collateral damage bij cyberwarfare vergroten echter de kans dat het zich voordoet, danwel niet kan worden voorzien.

[95] New York Times, In Shift, U.S. Talks to Russia on Internet Security, 12 december 2009, http://www.nytimes.com/2009/12/13/science/13cyber.html; Wall Street Journal online, U.S. Backs Talks on Cyber Warfare, 4 juni 2010, http://online.wsj.com/article/NA_WSJ_PUB:SB10001424052748703340904575284964215965730.html

[96] Met name versterking van NATO Computer Incident Response Capability (NCIRC) en het instellen van een Cyber Defence Management Authority (CDMA).

[97] Zie bijvoorbeeld: Cyber leger hard nodig, de Pers, 10 november 2009

[98] Motie van het lid Knops c.s., Kamerstuk 2009-2010, 32123 X, nr. 66, Tweede Kamer: "(...) verzoekt de regering in interdepartementaal verband een cyber security strategie te ontwikkelen, actief bij te dragen aan de gedachtevorming over cyberwarfare binnen de NAVO en de Kamer hierover uiterlijk 1 maart 2010 te informeren (...)"

[99] Ministerie van Defensie, Eindrapport Verkenningen, Houvast voor de krijgsmacht van de toekomst, 2010

[100] Zie o.a. http://www.nato-pa.int/default.asp?SHORTCUT=1782

[101] Zie Clarke (2010) en ter illustratie New York Times, Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk, waarin wordt geschetst waarom een Amerikaanse cyberaanval op het financiële ICT-stelsel van Irak uiteindelijk niet door mocht gaan: angst voor collateral damage, mogelijk tot in de Verenigde Staten aan toe http://www.nytimes.com/2009/08/02/us/politics/02cyber.html

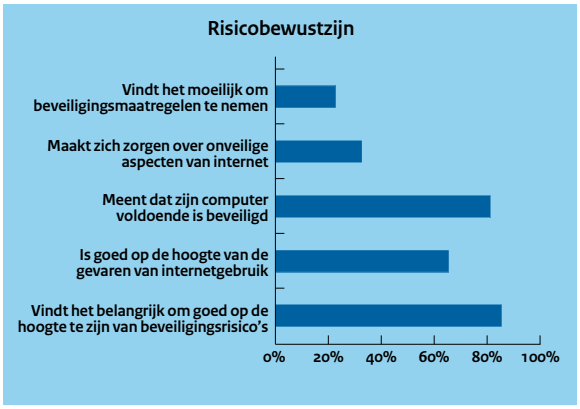

90
80
70

6
Veiligheid en genomen maatregelen

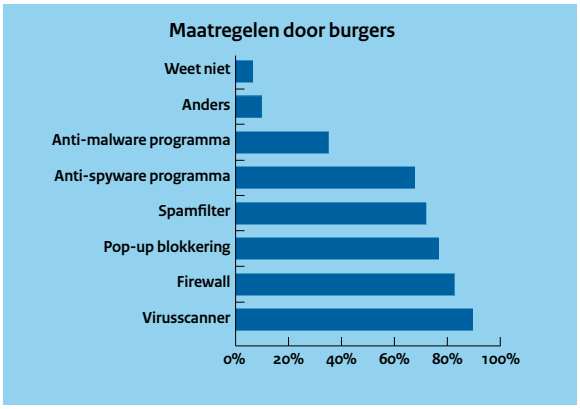
In het vorige hoofdstuk is beschreven hoe dreigingen uit cyberspace zich manifesteren in verschillende vormen vanuit verschillende motieven. Dit hoofdstuk richt zich op de vraag hoe veilig burgers en bedrijven zich voelen bij het gebruik van ICT, de veiligheidsbeleving dus. Daarnaast beschrijven we op welke wijze wordt gewerkt aan cybersecurity, zowel nationaal als internationaal.

6.1
Burgers vinden internet veilig genoeg om te gebruiken

Veel burgers zijn bekend met de risico's van gebruik van het internet en andere ICT. Deze leiden niet tot een zodanig gebrek aan vertrouwen, dat burgers er geen gebruik meer van maken. Slechts een beperkt percentage maakt zich zorgen over onveilige aspecten van internet.[102] Verder lijkt het erop dat in vergelijking met andere landen Nederlanders zich minder zorgen maken om het verlies van persoonsgegevens en andere privacygerelateerde incidenten, ook als het gaat om het gebruik van privacygegevens ten behoeve van strafrechtelijke opsporing of grootschalig verzamelen van persoonsgegevens door bedrijven.[103] Opvallend is dat desgevraagd de meeste burgers het wel belangrijk vinden om goed op de hoogte te zijn van de beveiligingsrisico's. Er bestaat echter weinig behoefte aan extra informatie over veiligheid op internet. De kennis wordt nu vooral opgedaan via de massamedia (tv, kranten, nieuwsberichten op internet). Veel burgers nemen maatregelen om hun computer te beveiligen, zoals een virusscanner of firewall.[104] Het nemen van dergelijke maatregelen draagt waarschijnlijk positief bij aan de veiligheidsbeleving. Ouderen (65+) nemen overigens iets minder vaak dergelijke maatregelen en zijn dus vermoedelijk kwetsbaarder.



Figuur 6-1 Risicobewustzijn van burgers (bron: TNO 2009)



Figuur 6-2 Maatregelen door burgers (bron: TNO 2009)

[102] TNO (2009)

[103] Internationaal vergelijkend onderzoek naar de privacybeleving is niet bekend. Zie ter illustratie echter over commotie in Duitsland over o.a. Google Streetview en bodyscans, http://www.depers.nl/economie/461238/Angst-voor-uberwachungsstaat.html

[104] TNO (2009)

Met name de mate waarin burgers zelf de schade als gevolg van cybercrime moeten dragen, lijkt de beleving te beïnvloeden. Financiële instellingen vergoeden tot nu toe namelijk vaak de schade van burgers als gevolg van bepaalde vormen van cybercriminaliteit zoals skimming, identiteitsdiefstal bij online bankieren en misbruik van creditcards. Deze aanpak leidt ertoe dat burgers zelf bij genoemde cybercrime nauwelijks economische schade ondervinden. Er is in feite sprake van afwenteling van het risico. Zolang de financiële instellingen vergoeden, leidt de burger geen schade.

De veiligheidsperceptie en de mate waarin burgers zelf beveiligingsmaatregelen nemen, is niet alleen relevant voor de betreffende persoon zelf. Als burgers zichzelf niet adequaat beschermen, kunnen ze ook overlast veroorzaken aan anderen, bijvoorbeeld door onbedoelde verdere verspreiding van virussen of deel uitmaken van een botnet.

6.2
Bedrijven voelen zich veilig en hebben vertrouwen in beveiliging

Ook bedrijven hebben een relatief hoog vertrouwen in de veiligheid van ICT en internet. Bedrijven verwachten over het algemeen een beperkte toename van afzonderlijke typen aanvallen, zoals spamming, virussen, fraude met ICT door werknemers en phishing.[105] Spamming en virussen zijn de belangrijkste uitzonderingen: respectievelijk 57% en 47% van de respondenten verwacht een gemiddelde of grote toename. De meeste bedrijven (73%) ziet de grootste dreiging vooral van buiten komen.

Een op de acht bedrijven werd het afgelopen jaar geconfronteerd met enige vorm van cybercriminaliteit, waarbij spam de grootste categorie was.[106] Desgevraagd meent ongeveer de helft van de ondervraagde organisaties dat de overlast gelijk is gebleven en 42% ziet een stijging. Het lijkt er in de onderzoeksresultaten op dat van de aanvallen die nu het meest worden ervaren, ook een grotere toename wordt verwacht.

Het vertrouwen in de beveiliging van de eigen organisatie is het afgelopen jaar toegenomen van 54% naar 80% van de ondervraagde organisaties.[107] De reden voor deze stijging ligt volgens de ondervraagde bedrijven primair in het kleine aantal incidenten en het vertrouwen in de genomen maatregelen. Daarbij wordt aangegeven dat regelmatige aandacht binnen de organisatie voor bewustwording, adequate processen om problemen tijdig te detecteren en goede opvolging van incidenten het vertrouwen sterken. Ook de uitgaven voor informatiebeveiliging groeien nog steeds licht.

De meeste organisaties voeren bij incidenten het onderzoek vooral in eigen beheer uit. Een kleine minderheid doet aangifte, hoewel de aangiftebereidheid in de afgelopen jaren wel is gestegen.[108] Grote organisaties zijn veel meer geneigd om aangifte te doen dan kleine. Van de kleine organisaties zegt de helft zelfs helemaal geen actie te ondernemen bij cybercrime.

6.3
Veel actie ondernomen, afstemming blijft aandachtspunt

De overheid neemt in toenemende mate maatregelen, met een steeds bredere reikwijdte. Ging het in het eerste decennium van deze eeuw vooral om bescherming van vitale sectoren en bestrijding van cybercriminaliteit, inmiddels staan ook cyberwarfare en een integrale cybersecuritystrategie op de politieke agenda. Er zijn vanuit verschillende perspectieven initiatieven genomen. Hieronder noemen we enkele van die initiatieven.

Beleid: het Programma Veiligheid begint bij Voorkomen (VbbV) met als een van de speerpunten cybercrime (Justitie en BZK, zie aantal punten hieronder nader uitgediept); het Programma Versterking Identiteitsketen Publieke Sector (BZK, ter bestrijding van identiteitsfraude); start strategievorming over militaire cyberoperations (Defensie) en start van de vorming van een integrale strategie voor cybersecurity (coördinatie BZK).

Publiek-Private Samenwerking (PPS): gedragscode Notice and Take-Down (oktober 2008), en convenant Botnets (per 1 januari 2010 van kracht) [109] en het Platform Internetveiligheid.

[105] Ernst & Young (2010)
[106] Zelfde onderzoek, slachtofferschap over de afgelopen 12 maanden voorafgaand aan het onderzoek.
[107] Ernst & Young (2010); Vergelijkbare tevredenheid in FBI, CSI Computer Crime and Security Survey, 14th annual, december 2009
[108] Zie hoofdstuk 5, blijkend uit Ernst & Young (2010) over 2009 en dezelfde rapporten over cybercrime over 2008 en 2007
[109] OPTA, Jaarverslag en marktmonitor 2009, 2010

Wet- en regelgeving: aanscherping Telecommunicatiewet voor spamming (1 oktober 2009). Wetgevingsvoorstellen voor diefstal en heling van gegevens, en Notice & Takedown zullen geconcretiseerd worden. Voor het online binnentreden van computers in het kader van opsporing en het kunnen vorderen van encryptiesleutels zijn nog geen wetgevingsvoorstellen voorzien.[110]

Handhaving van regelgeving over spam: OPTA handhaaft regelgeving over verspreiding van spam en malware. Sinds 2004 heeft de OPTA meer dan 20 boetes tussen de 2.000 en 500.000 euro voor spam uitgevaardigd en 4 voor malware (16.000 tot 800.000 euro), evenals meer dan 130 waarschuwingen.[111] Na invoering van nieuwe bepalingen over spam in de Telecommunicatiewet nam het aantal klachten van burgers sterk toe.

Boete voor spamkrabbels
Het college van OPTA legde in december 2009 een privépersoon een boete op van 12.000 euro voor het op grote schaal versturen van spam. De persoon in kwestie stuurde deze ongevraagde berichten in de vorm van 'krabbels' naar gebruikers van netwerksite Hyves. In de krabbels probeerde hij mensen naar zijn website te lokken waar ze (deels tegen betaling) een spel konden spelen. De spamkrabbels zorgden volgens OPTA voor veel overlast bij gebruikers en de aanbieder van Hyves.[112]

Bewustwording: het Stanislav filmpje op Hyves, 3x kloppen (NVB), mijn kind online (stichting Mijn Kind Online i.s.m. KPN, Ouders Online, Digivaardig & Digibewust), mijnprivacy.nl (CBP), Digivaardig & Digibewust (ook PPS), Veilig Internetten (Postbus 51), www.waarschuwingsdienst.nl (GOVCERT.NL). [113]

Kennisdeling: er zijn diverse initiatieven om op strategisch, tactisch en operationeel niveau kennis uit te wisselen. Voor de vitale sectoren faciliteert NICC de Information Sharing and Analysis Centers (ISACs) waarin publieke en private partijen informatie uitwisselen (ook PPS).[114] Verder zijn er het Nationaal Continuïteitsoverleg Telecom (NCO-T), Operationeel IRT-Overleg[115] en de Incident Respons Board.[116] Naast dergelijke geïnstitutionaliseerde vormen van kennisdeling delen verschillende overheidsdiensten (bijvoorbeeld NCTb, AIVD en GOVCERT.NL) hun kennis ook door openbare rapportages, presentaties en individuele voorlichting. GOVCERT.NL heeft een groot internationaal netwerk waarin intensief kennis wordt gedeeld.

Preventie en beperking impact: sinds het begin van de jaren negentig zijn in Nederland diverse Computer Emergency Response Teams (CERTs) opgericht, zoals SURFCERT, KPNCERT, CERT's van banken en universiteiten, GOVCERT.NL en DefCERT. Dit heeft geleid tot een uitgebreid netwerk voor preventie en beperking van de impact van cybercrime activiteiten. Ook de preventieactiviteiten van het Nationaal Bureau Verbindingsveiligheid (NBV) van de AIVD kan in dit kader worden genoemd. Het NBV ondersteunt de Rijksoverheid bij de beveiliging van bijzondere informatie zoals Staatsgeheimen.

Opsporing: bij de politie is opsporing van cybercrime ondergebracht bij het Team High Tech Crime van het KLPD en in beperkte mate bij de regiokorpsen. Het aantal zaken overtreft de capaciteit en – zeker op regionaal niveau – de beschikbare kennis. Er is nog geen sluitende structuur voor de opsporing van de verschillende vormen en niveaus van cybercrime, zoals die voor andere criminele 'lijnen' wel is georganiseerd. Er vindt momenteel een geleidelijke verschuiving plaats van zaak-naar dader-naar fenomeengericht onderzoek.

Het grensoverschrijdende karakter van cybercrime noodzaakt tot internationale samenwerking, ook met landen die het minder nauw nemen met gedragingen die wij in Nederland als crimineel beschouwen.

[110] KLPD (2010)

[111] Bron: OPTA (2010), aangevuld tijdens een expertsessie

[112] Persbericht OPTA, 6 juli 2010, Beslissing op bezwaar overtreding spamverbod door verzenden van Hyveskrabbels en onderliggend document: openbaar besluit college OPTA, met kenmerk OPTA/COL/2010/201040

[113] Zie ook: H.B.M. Leeuw, KU Leuven, hightech crime en voorlichting Een inventarisatie van voorlichtingsinitiatieven in Nederland en een analyse van kansen en mogelijkheden, 2009

[114] NICC, Publiek-private samenwerking in het Informatieknooppunt Cybercrime, 2008. Zie voor een overzicht van ISACs ook http://www.samentegencybercrime.nl/

[115] Samenwerkingsverband tussen Incident Response Teams van Nederlandse organisaties. GOVCERT.NL is oprichter van het Operationeel IRT-Overleg en organiseert de bijeenkomsten

[116] De ICT Response Board biedt private en publieke partijen de gelegenheid om, tijdens een (dreigende) ICT-verstoring, maatregelen af te stemmen en de overheid te adviseren over te nemen crisisbeheersingsmaatregelen

Dit leidt tot soms moeizame en langdurige trajecten of frustreert een onderzoek volledig. De Nederlandse politie werkt overigens internationaal samen met verschillende landen, zoals Rusland, de Oekraïne en de Verenigde Staten, maar ook met Interpol en Europol. Deze samenwerking wordt steeds intensiever. Ook heeft het Team High Tech Crime de samenwerking met private partijen geformaliseerd. De politie constateert behoefte aan meer coördinatie van opsporing van cybercrime .

Het Programma Aanpak Cybercrime (PAC) is erop gericht de korpsen te ondersteunen. Het PAC heeft zes actuele thema's: kinderporno, internetgerelateerde fraude, ICT-gerichte criminaliteit, intake en eerste opvolging van cybercrime, methoden en technieken en opleidingen. Op deze actielijnen en thema's zijn proeftuinen, projecten en pilots gestart.

Opsporing als afschrikking
De afgelopen jaren zijn in enkele grote zaken successen geboekt door het Team High Tech Crime van het KLPD. De inspanningen leiden tot succes, wat ook preventieve werking blijkt te hebben. Via ondergrondse fora delen cybercriminelen informatie over de (vermoede) slagkracht van opsporingsdiensten. Zo informeerden zij elkaar over het succes van het KLPD bij een phishingaanval tegen ABN AMRO en dat Nederland klaarblijkelijk effectief kon samenwerken met opsporingsdiensten uit Rusland en de Oekraïne. In 2008 en 2009 bleven Nederlandse banken vervolgens grotendeels gevrijwaard van aanvallen.[117] In 2010 nam het aantal phishingaanvallen echter weer toe.

Vervolging: vanuit het Versterkingsprogramma Cybercrime bij het Openbaar Ministerie (OM) wordt specifiek aandacht besteed aan intensivering van opsporing en vervolging in samenwerking met de politie. Denk aan gefaseerde uitbreiding van de capaciteit van het OM in de periode 2009-2011, cybercrime-opleidingen, kennis- en expertisecentrum cybercrime, proeftuinen en inzet van ICT-toepassingen om de werking van cybercrime te illustreren in de rechtszaal.[118]
Voor de mensen in de uitvoering (publiek of privaat) ontstaat een gefragmenteerd beeld door al deze nationale en internationale maatregelen. Uit de expertsessies bleek dat de big picture in de zin van (nationale) prioriteiten en samenhang tussen activiteiten voor hen niet helder is. Dit betekent in de praktijk dat afstemming van uitvoeringsactiviteiten vooral ad hoc en bottom-up tot stand komt. Er zijn wel beleidsprogramma's met een (deels) overkoepelend karakter, maar klaarblijkelijk omvatten deze initiatieven nog niet de hele scope.

6.4
Op korte termijn wordt een tekort aan cyberprofessionals verwacht

Zowel nationaal als internationaal neemt het aantal plannen, regelgeving en concrete maatregelen op het gebied van cybersecurity toe. Vrijwel elk initiatief leidt tot een nieuwe behoefte aan mensen, middelen. Op korte termijn dreigt daarom een tekort aan gekwalificeerde cyberprofessionals. Denk aan ethische hackers en technische beveiligingsspecialisten, maar ook aan mensen die de brug kunnen slaan tussen deze technische specialisten en andere disciplines (bijvoorbeeld opsporing, krijgsmacht en beleid). Zowel in de publieke als private sector is het al moeilijk om gekwalificeerde cyberprofessionals te werven. Het is een schaarse deskundigheid. De beloningsverschillen tussen publiek en privaat werken hierbij in het nadeel van de overheid, terwijl juist bij de overheid de vraag naar gekwalificeerd personeel toeneemt als gevolg van een toenemend aantal maatregelen. Denk aan uitbreiding van taken op het gebied van digitale veiligheid, bijvoorbeeld bij politie en Defensie. Dit tekort aan gekwalificeerd personeel betekent dat er werk blijft liggen.

6.5
Groeiende internationale samenwerking in het cyberdomein

De groeiende overheidsinspanningen in Nederland zijn niet uniek. Andere geïndustrialiseerde landen nemen steeds meer beleidsmaatregelen om de digitale veiligheid te vergroten, zowel in nationaal verband als in internationale verdragen. Zeker vanaf 2007 (na de DDOS-aanval op Estland) is er grote aandacht voor cybersecurity op politiek en ambtelijk niveau. In toenemende mate vindt samenwerking met buitenlandse collega-organisaties plaats. Bijvoorbeeld door deelname aan FIRST[119], EU- en NAVO-activiteiten, delen van kennis tussen internationale CERTs en beschikbaar stellen van tools door

[117] KLPD (2010)
[118] Ministeries van BZK en Justitie, Tweede voortgangsrapportage Veiligheid begint bij Voorkomen, TK 28684, nr. 253, oktober 2009
[119] Forum of Incident Response and Security Teams, telt ruim 175 CERT-teams uit de hele wereld

GOVCERT.NL aan collega CERTs. Nederland doet ook actief suggesties voor de bestrijding van cybercrime in internationaal verband[120], zoals het voorstel voor een Europese cyberautoriteit.[121]

In international verband zijn er verdragen gesloten of anderszins afspraken gemaakt. Nederland heeft sterk bijgedragen aan de totstandkoming van het 'Cybercrime Verdrag' van de Raad van Europa. In dit verdrag hebben landen afgesproken tot een gemeenschappelijk strafrechtelijk beleid te komen, gericht op de bescherming van de samenleving tegen strafbare feiten verbonden met elektronische netwerken, vooral door het tot stand brengen van passende wetgeving en het versterken van de internationale samenwerking. Niet alleen Europese landen zijn lid, ook de Verenigde Staten en Japan. Lidstaten Rusland en Turkije hebben niet ondertekend noch geratificeerd. Relevant, want uit deze landen komt bovengemiddeld veel illegale cyberactiviteit.

De Europese Unie heeft inmiddels ook beleid en regelgeving ontwikkeld, ingegeven door het belang van de informatie-infrastructuur voor Europa en het grensoverschrijdende karakter van cyberaanvallen. Het European Network and Information Security Agency (ENISA) werd in 2004 opgericht, met als doel een hoge en effectieve beveiliging van netwerken en informatie in de EU te faciliteren. ENISA heeft taken op het gebied van bewustwording, opleiding, bijstand en advies voor lidstaten. De communautaire digitale defensie kreeg in april 2009 een nieuwe duw in de rug door de EU-top in Tallinn. Daar werd een cyberactieplan van de Europese Commissie overgenomen.[122] In dit actieplan stuurt de EU aan op meer internationale samenwerking bij preventie, detectie en respons, internationale cyberoefeningen en veerkracht en stabiliteit van het internet. Verder komt er een meldplicht voor telecom- en internetproviders voor datalekken (data breaches), wanneer die persoonsgegevens betreffen.[123] Ook de Digitale Agenda van de EU zal waarschijnlijk een extra impuls geven aan internationale samenwerking, aangezien cybersecurity een van de speerpunten in die agenda is. In toenemende mate sturen de lidstaten via de EU gezamenlijk op preventie en bestrijding van cybercrime.

Ook de NAVO herkent cybersecurity als belangrijk aandachtspunt en bezint zich op toekomstig beleid. De expertgroep voor het nieuwe strategische concept van de NAVO stelde onlangs dat cyberaanvallen tot de top 3-bedreigingen van de NAVO behoren.[124] De NAVO moet daarom volgens deze expertgroep haar inspanningen verhogen om de eigen communicatie- en commandostructuur te verdedigen, bondgenoten te helpen met preventie en herstel en een cyberarsenaal op te bouwen voor detectie en afschrikking. Meer inspanningen geïnitieerd door de NAVO zijn dan ook te verwachten.

[120] Ministeries van BZK en Justitie, Naar een veiliger samenleving, TK 2007-2008, 28684, nr 133

[121] Zie als illustratie: Computable 3 juni 2010, Hirsch Ballin wil Europese cyberautoriteit. http://www.computable.nl/artikel/ict_topics/security/3378765/1276896/hirsch-ballin-wil-europese-cyberautoriteit.html

[122] Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur: 'Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht', Brussel, 30 maart 2009 COM(2009) blz. 149

[123] MEMO/09/491, Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens, Brussels, 5 November 2009

[124] NAVO, NATO 2020: Assured Security; Dynamic Engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO, 2010

7
Impact en effect

Onze samenleving wordt steeds afhankelijker van ICT. Het dringt in steeds meer aspecten van ons leven door, soms zelfs zonder dat we het door hebben. Het bestaan van technische, organisatorische en menselijke kwetsbaarheden is echter een gegeven. Waterdichte beveiliging bestaat niet en beveiliging moet wel continu ontwikkeld en verbeterd worden. Aanvalsmethoden veranderen namelijk ook; ze worden geavanceerder, gerichter en minder detecteerbaar.

7.1
Het economisch belang is in het geding

Dat het economisch belang in het geding is, is niet verwonderlijk omdat cybercrime en digitale spionage mede uit financieel gewin plaatsvinden. Het doelwit is dan geld of intellectueel eigendom waarmee geld kan worden verdiend. Bovendien ontstaat indirect schade als gevolg van het moeten herstellen van ICT- of andere voorzieningen, imagoschade, verlies van concurrentiepositie. Daarnaast maken bedrijven hoge kosten voor het nemen van beveiligingsmaatregelen. Gezien de geconstateerde toename van het aantal cybercriminelen en criminele activiteiten, is het aannemelijk dat de totale economische schade de komende jaren ook toeneemt.

7.2
Cybercrime en digitale spionage zijn de belangrijkste manifestaties

Afgemeten aan geconstateerd effect zijn cybercrime en digitale spionage de belangrijkste manifestaties. De totale omvang van de (financiële) schade als gevolg van hightech crime in Nederland is niet bekend, maar hoogstwaarschijnlijk substantieel.
De schade van skimming alleen al was 36 miljoen euro in 2009. Echter, de aangiftebereidheid is laag, zeker bij burgers, waardoor de totale schade onbekend is.

Digitale spionage vormt net als spionage een reële dreiging voor het economisch belang van Nederland. De kennis van bedrijven in de vorm van intellectueel eigendom is een aantrekkelijk doelwit voor sommige inlichtingendiensten en vermoedelijk ook andere bedrijven. De internationale onderhandelingspositie van Nederland kan verzwakken, wanneer standpunten en onderhandelingsstrategie vooraf bij andere landen bekend zijn. De slagkracht van de krijgsmacht wordt aangetast wanneer tegenstanders beschikken over informatie van operationele en ondersteunende aspecten.

De schade in kwantitatieve zin (geld, aantal documenten, ect.) is niet bekend. Vaak weten organisaties niet eens dat ze slachtoffer zijn. Gezien de omvang van wel ontdekte gevallen en de effectiviteit van beschikbare technologie, is die schade substantieel.

7.3
Privacy staat steeds meer onder druk

Een ander belang dat veelvuldig wordt getroffen, is de privacy van burgers. Privacy wordt op veel manieren aangetast. Uit onderzoek uit 2009 is gebleken dat de persoonsgegevens van Nederlanders gemiddeld in 250 tot 500 verschillende gegevensbestanden voorkomen[125].

Dit biedt voor kwaadwillenden veel mogelijkheden. Zij zijn dan ook voortdurend op zoek naar lekken in systemen om persoonsgegevens te ontvreemden om door te verkopen of zelf te misbruiken.
Niet alleen worden persoonsgegevens ontvreemd, ook maken mensen hun eigen persoonsgegevens publiek, bijvoorbeeld via sociale netwerken, zonder dat ze daarbij altijd goed de consequenties van kunnen inzien. Voor de veiligheid is het soms noodzakelijk dat persoonsgegevens worden gedeeld

[125] mr. dr. Bart W. Schermer, mr. Ton Wagemans, Onze digitale schaduw, 2009,

met misdaad- en terrorismebestrijders voor de uitoefening van hun taak.

In de informatiemaatschappij verengt privacy zich langzamerhand tot (afspraken over) goed beheer van persoonsgegevens. Deze veranderende opvatting geldt met name onder jongeren.[126] Verschillende bevolkingsgroepen hebben verschillende percepties over wat wel en niet als inbreuk op hun privacy geldt. Daarnaast zijn er ook grote verschillen tussen landen. De bescherming van privacy heeft bijvoorbeeld in Duitsland een veel hogere prioriteit dan in Nederland. Het gaat dan met name over het gevaar van zogenoemde false positives, de aanzienlijke kans dat onschuldige burgers door fouten in de digitale analyse als verdachte worden aangemerkt.[127]

7.4
De risicobeleving van burgers en bedrijven komt niet overeen met werkelijke risico's

Het vertrouwen van burgers en bedrijven in de veiligheid van ICT en de (zelf) genomen beveiligingsmaatregelen is groot, ook in vergelijking met andere landen. De risicobeleving komt daarmee niet overeen met de werkelijkheid, maar in een aantal gevallen is dit te verklaren.

In het geval van skimming en fraude met internetbankieren bijvoorbeeld is de kans dat iemand er slachtoffer van wordt reëel en zal er schade optreden. Het slachtoffer zal de financiële schade echter vaak vergoed krijgen van zijn bank. Een ander voorbeeld is malware en botnets. Het aantal mensen en organisaties dat te maken heeft met een besmette computer is aanzienlijk en in alle gevallen treedt er schade op als een besmette computer in een botnet wordt ingezet voor criminele activiteiten. In de meeste gevallen ondervindt de eigenaar van de besmette computer daar geen of weinig hinder van. Soms kan vanaf een besmette computer tijdelijk geen e-mail ontvangen en verzonden worden, omdat deze op een zwarte lijst is gezet.
Dat de risicobeleving niet overeenkomt met de werkelijkheid, kan ertoe leiden dat men zich onvoldoende beschermt tegen de werkelijke risico's.

7.5
Beperkte beschikbaarheid van kwantitatieve data

De trends uit dit rapport zijn bepaald in nauwe samenwerking met experts uit wetenschap, bedrijfsleven en overheid en er is intensief gebruikgemaakt van bestaande rapportages en publicaties. Tijdens de totstandkoming van dit Trendrapport bleek echter, dat er weinig betrouwbare kwantitatieve data beschikbaar is, waardoor strategische trends niet altijd kunnen worden onderbouwd met harde cijfers. Veel duidingen zijn dan ook kwalitatief.

Het gebrek aan kwantitatieve data belemmert niet alleen het inzicht in de trends zelf, maar ook het meten van het effect van maatregelen. Dit Trendrapport kan behulpzaam zijn bij het vaststellen van de indicatoren die relevant zijn om kwetsbaarheden, de stand van aanvalsmethoden, veiligheidsperceptie en vooral de (impact van) manifestaties in kaart te brengen.

[126] ECP-EPN - Roadmap: vertrouwen in de informatiesamenleving, 2009
[127] Schermer, B.W., Surveillance and privacy in the network society, 2009


tech·nol·o·gy
To modify or
tech·nol·o·gy
science, esp. to
tific method

Begrippenlijst

Authenticatie
Authenticatie is het nagaan of een bewijs van identiteit van een gebruiker, computer of applicatie overeenkomt met vooraf vastgelegde echtheidskenmerken.

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.

Bulletproof
Een dienst van bepaalde hostingbedrijven om materiaal te kunnen uploaden en/of te distribueren, ongeacht de toelaatbaarheid van de inhoud. Gebruikersgegevens van de dienst worden afgeschermd. Hierdoor biedt het bedrijf de mogelijkheid voor illegale activiteiten.

CERT
Computer Emergency Response Team, 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.

Cloudcomputing
Een op internet (de 'wolk') gebaseerd model voor systeemarchitectuur, waarbij vooral gebruikgemaakt wordt van Software as a Service (SaaS). Afnemers en gebruikers van cloudcomputingdiensten hebben niet noodzakelijkerwijs expertise in of controle over de technologische infrastructuur in de 'cloud'.

Command & Control server (C&C)
Vaak worden bots in een botnet aangestuurd door een centrale computer die ook wel Command & Control server wordt genoemd.

Datalek (of data breach)
Het onopzettelijk naar buiten komen van vertrouwelijke gegevens.

Defacement
Het onbevoegd en vaak met kwaadaardige intentie vervangen of beschadigen van de inhoud van een bestaande webpagina. Vaak gebeurt dit door aanvallers die zichzelf op onrechtmatige wijze toegang hebben weten te verschaffen tot een webserver.

Denial of Service (DoS)
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.

DNS Security Extensions (DNSSEC)
DNSSEC is een uitbreiding aan het oorspronkelijke DNS-protocol, waarmee de afkomst en integriteit van de DNS-gegevens te controleren zijn.

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

Domotica
Het woord Domotica is een samentrekking van domus (woning) en telematica. Domotica staat voor elektronische communicatie tussen allerlei elektrische toepassingen in de woning en woonomgeving ten behoeve van bewoners en dienstverleners.

Drive-by downloads
Het ophalen van malware zonder dat de gebruiker het weet of daar zijn toestemming voor heeft gegeven, bijvoorbeeld door te klikken op een valse foutmelding of via een kwetsbaarheid in de browser, e-mailclient of besturingssysteem.

Dropzone
Computersysteem waar gestolen gegevens (tijdelijk) worden opgeslagen.

Exploit
Software, gegevens, of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om onbedoeld of onverwacht gedrag daarvan te veroorzaken.

Firmware
Firmware is de benaming voor software die standaard geïnstalleerd is op en meegeleverd wordt met bepaalde apparaten. De firmware is nodig om het apparaat te laten functioneren.

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.

Insider threat
De bedreiging voor de digitale veiligheid van een organisatie, opzettelijk of onopzettelijk, door iemand die een werkrelatie of anderszins legale toegang tot de organisatie heeft.

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, worms en trojans.

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

Money mules
Money Mule is de Engelse term voor katvanger, iemand die frauduleus verkregen geld (of goederen) doorsluist naar criminelen. De money mule fungeert als tussenstation en helpt de identiteit van de crimineel te versluieren.

Notice and Take Down (NTD)
Notice and Take Down is een gefaseerde procedure die gebruikt wordt om servers met illegale inhoud van het internet te verwijderen. Voorbeelden van NTD's zijn die voor kinderporno- en phishingsites.

Patch
Een patch (letterlijk: 'pleister') kan bestaan uit reparatiesoftware of kan wijzigingen bevatten die direct in een programma worden doorgevoerd om het desbetreffende programma te repareren of te verbeteren.

Phishing
Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan worden misbruikt voor bijvoorbeeld creditcardfraude, maar ook voor wat in het Engels identity theft wordt genoemd; het stelen van iemands identiteit.

RFID
Radio Frequency IDentification, ofwel draadloze identificatie van objecten.

SaaS
Software as a Service. Software die als een online dienst wordt aangeboden. De gebruiker hoeft de software niet aan te schaffen, maar sluit een contract af voor een vast bedrag per periode voor het gebruik.

SCADA
Supervisory Control And Data Acquisition, het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële procescontrolesystemen.

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.

Sociale netwerken
Sociale netwerksites zijn hulpmiddelen waarmee mensen hun sociale netwerk op internet kunnen onderhouden. Voorbeelden zijn Hyves, Facebook en LinkedIn.

Spam
Spam is grootschalige ongewenste berichtgeving via eenz.ensmail, mobiele telefonie (sms of mms) of via een ander elektronisch kanaal (zoals social networks, fax of bellen door een automatisch oproepsysteem) of bellen.

Spear phishing
Vorm van phishing die specifiek gericht is op een bepaalde gebruiker of groepen van gebruikers, bijvoorbeeld medewerkers van een bepaalde organisatie.

Spyware
Een programma dat informatie over een gebruiker verzamelt en deze zonder dat de gebruiker daarvan op de hoogte is doorstuurt naar een derde partij.

Transmission Control Protocol (TCP)
TCP is het protocol dat gebruikt wordt om de gegevensstroom tussen computers over een verbinding tot stand te brengen en te regelen.

Trojan
Een trojan of trojan horse (Trojaans paard) is de naam voor software die geheime, kwaadaardige functies bevat.

Literatuurlijst

Een aantal bestaande trendrapporten van overheidsorganisaties is gebruikt als basis voor Nationaal Trendrapport Cybercrime. Daarnaast zijn andere schriftelijke bronnen geraadpleegd.

Trendrapportages overheid

Algemene Inlichtingen- en Veiligheidsdienst, Kwetsbaarheidsanalyse spionage. Spionagerisico's en de nationale veiligheid, 2010

GOVCERT.NL, Trendrapport 2009, 2009

Korps Landelijke Politiediensten, Hightech crime, Criminaliteitsbeeldanalyse 2009, 2010

NCTb, Jihadisten en het Internet, update 2009, 2010

OPTA, Jaarverslag en Marktmonitor 2009, 2010

Overige bronnen

Algemene Inlichtingen- en Veiligheidsdienst, Jaarverslag 2009, april 2010 (2)

Algemene Inlichtingen- en Veiligheidsdienst, Digitale spionage. Wat is het risico?, 2010 (3)

Anti-Phishing Working Group (AWPG), Global Phishing Survey: Trends and Domain Name Use in 2H2009, mei 2010

Anti-Phishing Working Group (AWPG), Phishing Activity Trends Report, edities 1H2009 en 3Q2009

Canadian Security Intelligence Service, Transnational criminal activity: a global context, 2000

Carr, Jeffrey, Inside Cyber Warfare, 2009

Centraal Bureau voor de Statistiek, Integrale Veiligheidsmonitor, landelijke rapportage 2009, 2010

Choo, K-K, R., Trends in Organized Crime, 2008

Clarke, Wesley K. en P.L. Levin, Securing the information highway: how to enhance the United States' Electronic Defenses, Foreign Affairs November 2009

Clarke, Richard A., Robert K. Knake, Cyber War. The next threat to national security and what to do about it, 2010

ECP-EPN, Roadmap: vertrouwen in de informatiesamenleving, 2009

Eeten, M. van e.a., Damages from internet security incidents. A framework and toolkit for assessing the economic costs of security breaches, 2009

Eeten, M. van e.a., The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data, 2010

ENISA 2009 spam survey. Measures used by providers to reduce spam, december 2009

ENISA, Country reports France, Germany, Netherlands, Norway, United Kingdom, 2009

Ernst & Young, ICT Barometer over cybercrime, 24 februari 2010

Europese Unie, Digitale Agenda, IP/10/581, 2010

Europese Unie, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's betreffende de bescherming van kritieke informatie-infrastructuur: 'Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht', Brussel, 30 maart 2009 COM blz. 149

Europese Unie, MEMO/09/491, Agreement on EU Telecoms Reform paves way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens, Brussels, 5 November 2009

Falliere, N. and E. Chien, ZeuS: King of the Bots, 2009

FBI, CSI Computer Crime and Security Survey, 14th annual, december 2009

Forrester Research, Dutch Online Banking Forecast: 2008 To 2013, Forrester april 2008

Forrester Research, Western European Online Retail Forecast, 2009 To 2014, maart 2010

Gartner, Findings: In January 2010, the Consumerization of IT Became a Business Strategy Issue, 2010

Gartner, Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014, 2010

Gartner, Key Issues for the Consumerization of IT, 2009

Gartner: Security in 2013 and beyond, 2010

GOVCERT.NL Jaaroverzicht 2009, 2010

GOVCERT.NL, Whitepaper Raamwerk beveiliging webapplicaties, 2009

GOVCERT.NL, Whitepaper Beveiliging van mobiele apparatuur en datadragers, 2009

GOVCERT.NL, Factsheet FS-2010-01 De beveiliging van webapplicaties, 2010

GOVCERT.NL, Factsheet FS 2009-02 Grenzen aan cryptogebruik: werken met vertrouwelijke informatie in het buitenland, 2009

GOVCERT.NL, Factsheet FS 2009-05 Afluisteren van GSM-communicatie dichterbij, 2010

GOVCERT.NL, Factsheet FS-2008-01 Draadloze netwerken, 2009

Herley, Cormac, So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users, 2009

Herley, Cormac and Dinei Florencio, Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy, 2009

Herley, Cormac and Dinei Florencio, A Profitless Endeavor: Phishing as Tragedy of the Commons, 2009

Heukfeldt, E.R., M.M.L. Domenie en W.Ph. Stol, Verkenning cybercrime in Nederland 2009, 2010

Hughes, Rex B., NATO and Cyber Defence, Mission Accomplished?, Atlantisch Perspectief, 2009 nr 1/4

Information Security Platform, Threat Horizon 2012 Information-security related threats of the future, 2010

Information Warfare Monitor & Shadowserver Foundation, Shadows in the cloud: investigating Cyber Espionage 2.0, 6 april 2010

Internet Crime Complaint Center (FBI), 2009 Internet Crime Report, 2010

KLPD - Dienst Nationale Recherche, Overall-beeld Aandachtsgebieden, juli 2010

Leeuw, H.B.M., KU Leuven, HIGHTECH CRIME EN VOORLICHTING Een inventarisatie van voorlichtings-initiatieven in Nederland en een analyse van kansen en mogelijkheden, 2009

LeLarge, M., Economics of Malware: Epidemic Risk Model, Network Externalities and Incentives, presentatie op de WEIS 2009, University College London, juni 2009.

MessageLabs Intelligence Reports, 2010

Messaging Anti-Abuse Working Group (MAAWG), Email Metrics Program: The Network Operators' Perspective Report #12 – Third and Fourth Quarter 2009, maart 2010

Microsoft Security Intelligence Report, Volume 8 (juli - december 2009)

Ministeries van BZK en Justitie, Naar een veiliger samenleving, TK 2007-2008, 28684, nr 133

Ministeries van BZK en Justitie, Tweede voortgangs-rapportage Veiligheid begint bij Voorkomen, TK 28684, nr. 253, oktober 2009

Ministerie van Defensie, Eindrapport Verkenningen, Houvast voor de krijgsmacht van de toekomst, 2010

Murdoch, S., Destructive Activism: The Double-Edged Sword of Digital Tactics, in: Mary Joyce ed., Digital Activism Decoded, 2010

NATO, NATO 2020: Assured Security; Dynamic Engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO, 2010

NICC, Process Control Security in het Informatieknooppunt Cybercrime, 2009

NICC, Publiek-private samenwerking in het Informatieknooppunt Cybercrime, 2008

NVB, De Nederlandse Vereniging van Banken, het Openbaar Ministerie en politie in Nederland binden gezamenlijk de strijd aan tegen skimming, http://www.nvb.nl/index.php?p=514348

OECD, Computer Viruses and Other Malicious Software. What Can Be Done?, 2009

PriceWaterhouseCoopers, Information Security Breaches Survey 2010 - technical report, 2010

Schermer, B.W., Surveillance and privacy in the network society, 2009

Secureworks, ZeuS Banking Trojan Report, 2010

Symantec, Internet Security Threat Report 2009, april 2010

TNO, Marktrapportage Elektronische Communicatie, mei 2010

TNO, Perceptieonderzoek Veilig Internet Onderzoek naar de ruimte tussen wat (on)veilig is en wat als zodanig gepercipieerd wordt, april 2009

UK Cabinet Office, Cyber Security Strategy of the United Kingdom. Safety, Security and Resilience in Cyber Space, juni 2009

Weimann, G.. The Psychology of Mass-mediated Terrorism, American Behavioral, 2008

WODC, High-tech crime, soorten criminaliteit en hun daders 2008

World Economic Forum, Global Risks 2010, A global risk network report, januari 2010

Samenwerkende en geraadpleegde organisaties

Het Nationaal Trendrapport Cybercrime en Digitale Veiligheid is opgesteld door GOVCERT.NL onder gezamenlijk opdrachtgeverschap van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken en Justitie.

Aan de totstandkoming van dit rapport werkten vele partijen mee en is van veel andere organisaties materiaal gebruikt. Zo krijgt dit eerste Nationale Trendrapport ook daadwerkelijk een overkoepelend karakter. De opstellers zijn deze organisaties veel dank verschuldigd voor de door hen ingebrachte deskundigheid tijdens expertsessies en interviews. Hun inzichten hebben een beter licht geworpen op de strategische trends.

De tekst in het Trendrapport is zorgvuldig samengesteld waarbij zoveel mogelijk recht is gedaan aan de input van de verschillende partijen.

Bij de totstandkoming van dit Trendrapport is door GOVCERT.NL nauw samengewerkt met:
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Nationaal Coördinator Terrorismebestrijding (NCTb)
Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA)
Politie - Korps Landelijke Politiediensten (KLPD)

De volgende partijen hebben een belangrijke bijdrage geleverd aan dit Trendrapport:
Capgemini
Business & IT Trends Institute
Ernst & Young
Fox IT
Hague Center for Strategic Studies
Johns Hopkins University
KPMG / i4
KPN
Madison Ghurka
Ministerie van Defensie
Nationale Infrastructuur ter bestrijding van Cybercrime (NICC)
National Institute of Standards and Technology (NIST)
Openbaar Ministerie
Rabobank
Siemens Nederland N.V.
Technische Universiteit Delft
TNO
Universiteit Leiden

GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid.
Wij werken aan het voorkomen en afhandelen van ICT-veiligheidsincidenten, 24 uur per dag, 7 dagen per week. Wij ondersteunen organisaties die een publieke taak uitvoeren, zoals overheidsinstellingen, en werken samen met vitale sectoren. Wij lichten het publiek voor over maatregelen en actuele risico's, die betrekking hebben op computer- en internetgebruik.

Colofon

Uitgave: oktober 2010
Oplage: 1.500
Redactie: GOVCERT.NL
Vormgeving: Delta III, www.delta3.nl
Elektronische versie: www.govcert.nl/trends

GOVCERT.NL
Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postbus 84011
2508 AA Den Haag

T 070 888 7 555
E info@govcert.nl
I www.govcert.nl