



# Tendrapport | 2009

Inzicht in cybercrime: trends & cijfers

## **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.

## **GBO.OVERHEID**

Is de Gemeenschappelijke Beheer Organisatie van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties waarvan GOVCERT.NL sinds 1 januari 2006 deel uitmaakt. GBO.Overheid is verantwoordelijk voor het beheer en de verdere ontwikkeling van een aantal overheidsbrede ICT-voorzieningen voor de elektronische overheid.

In Nederland hebben GOVCERT.NL, NCTb en KLPD/THTC namens de overheid een belangrijke rol in de strijd tegen cybercrime (inclusief terrorisme via het internet). Tussen deze organisaties vindt regelmatig overleg plaats inzake incidenten en ontwikkelingen rond dit thema, en zij trachten in hun rapportages een zo compleet mogelijk beeld te geven van de belangrijkste trends. Mede op basis van deze wijze van samenwerking is het beeld in dit GOVCERT.NL-Tendrapport tot stand gekomen.

## Online of offline


“Het afgelopen jaar is zonder twijfel ook het jaar geweest van verdere vervaging tussen de online en offline wereld.” Deze zin uit het derde Trendrapport dat GOVCERT.NL uitgeeft, had mijn speciale aandacht. Ik vroeg mijzelf af in hoeverre dat voor mij en mijn eigen werkomgeving geldt. Ik Twitter en Skype niet en heb geen weblog. En toch: ook ik heb te maken met web 2.0, al was het alleen maar door initiatieven als overheid20.nl. Dit platform is zelfs door mijn eigen ministerie opgezet. Het biedt werkruimtes voor ambtenaren om digitaal informatie uit te wisselen, maar ook burgers kunnen deelnemen en op die manier meepraten en meedenken tijdens de beleidsontwikkeling. Hoewel ‘vervaging tussen de online en offline wereld’ in eerste instantie wat futuristische beelden bij mij opriep, besef ik dat dit precies is waar het over gaat.

Veiligheid van de digitale werkomgeving is essentieel als wij online met elkaar communiceren. Dit Trendrapport zoomt in op internetveiligheid. Zoals gebruikelijk analyseert GOVCERT.NL trends en ontwikkelingen op het gebied van cybercrime en cybersecurity. Zo blijkt dat internetcriminelen zich in het afgelopen jaar niet van bijzondere nieuwe technieken hebben bediend, maar vooral van de al bekende. Geen nieuwe technieken, betekent helaas niet: minder schadelijke gevolgen. Want ook het afgelopen jaar zijn weer veel mensen het slachtoffer van cybercrime geworden, bijvoorbeeld in de vorm van fraude of misbruik van persoonsgegevens. Gelukkig wordt er steeds beter samengewerkt op het gebied van digitale beveiliging en handhaving. Zo leest u in dit Trendrapport over een paar eclatante successen op het gebied van opsporing. In binnen- en buitenland wordt er harder en meer opgetreden tegen criminele organisaties, maar ook tegen organisaties zoals hosting providers, die – bewust of onbewust – toelaten dat er kwaadaardige websites gehost worden. Het sluiten van zo’n bedrijf in het buitenland in november 2008 zorgde onmiddellijk voor een (weliswaar tijdelijke) daling van spam van 75%. Op die manier zetten we stappen vooruit in onze digitale veiligheid!

En dan is er ook nog het vraagstuk ‘is internet nog veilig genoeg?’. Hierover is lange tijd verwoed gediscussieerd in de media en door professionals in de ICT-wereld. Lekken in software, maar ook in essentiële internetprotocollen, kwamen aan het licht en riepen de vraag op of het internet überhaupt nog veilig te gebruiken is. Ik schaar me achter de conclusie in dit rapport: neen, het internet is niet stuk. Maar het heeft wel kwetsbare plekken. Daarom is het belangrijk met securityspecialisten, software- en hardwareleveranciers, beleidsmakers, politici, de media en met thuisgebruikers te blijven werken aan bewustwording én aan technische oplossingen om onze online aanwezigheid zo veilig mogelijk te houden. Een veilige digitale wereld maakt het leven in alle opzichten gemakkelijker en mooier.

### Ank Bijleveld-Schouten

Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

A young boy with dark hair, wearing a light blue t-shirt, is looking through a telescope. The telescope is mounted on a large, grey, metallic-looking structure that resembles a stylized animal head, possibly a dog or a bear, with large ears and a snout. The background is a clear blue sky with some light clouds. The scene is brightly lit, suggesting an outdoor museum or park setting.

Dit Trendrapport 2009 geeft inzicht in de stand van zaken en ontwikkelingen in cybercrime en informatiebeveiliging in Nederland. Het rapport bevat informatie over technieken die internetcriminelen gebruiken, de impact daarvan op de Nederlandse eindgebruikers, overheid en bedrijfsleven en doet aanbevelingen over de verbetering van informatiebeveiliging.

GOVCERT.NL baseert haar adviezen en waarschuwingen op verschillende bronnen. Een groot aantal publieke en besloten internationale informatiebronnen en contacten met collega-CERT's geven zicht op nieuwe kwetsbaarheden, dreigingen en vormen van misbruik. GOVCERT.NL schenkt daarbij veel aandacht aan het verifiëren van haar bronnen.

De deelnemers en partners, waarmee GOVCERT.NL samenwerkt, leveren informatie over incidenten en over oplossingen en ontwikkelingen. Daarnaast heeft GOVCERT.NL sinds april 2006 een eigen monitoringnetwerk, waarin actuele informatie over aanvallen en aangeboden kwaadaardige programma's wordt verzameld en gepresenteerd. Met behulp van deze bronnen is dit rapport samengesteld, waarbij feiten en concrete waarnemingen in de periode april 2008 tot april 2009 de basis vormen van de beschreven trends. Verwacht echter geen schatting van de omvang van internetcriminaliteit in Nederland, simpelweg omdat hiervoor niet voldoende harde gegevens op één plaats beschikbaar zijn. Bij het publiceren van een Trendrapport, in het bijzonder op het gebied van cybercrime, moet je afwegen welke zaken wel en welke niet op te nemen. Openheid en transparantie zijn belangrijk: inzicht kan leiden tot betere bescherming. Anderzijds kan te veel informatie schadelijk zijn: inzicht kan leiden tot extra kwetsbaarheid. Vooral op het gebied van technische details en zeer recente ontwikkelingen hebben wij terughoudendheid betracht.

In dit rapport halen wij diverse voorbeelden aan waarover op internet soms meer informatie te vinden is. De links hiernaar vindt u in dit rapport en ook op de website van GOVCERT.NL: [www.govcert.nl/trends](http://www.govcert.nl/trends).

## De belangrijkste trends in cybercrime

Dit Trendrapport geeft een overzicht van de ontwikkelingen in cybercrime in het afgelopen jaar. Hieronder vatten wij de belangrijkste gesignaleerde trends kort samen.

### **Internetveiligheid, een blijvend punt van zorg**

Hoewel stappen vooruit worden gezet in de bestrijding van cybercrime, signaleren wij helaas vooral trends die – als geheel – wijzen op een verslechtering van de situatie op het gebied van internetveiligheid. De internetinfrastructuur blijkt kwetsbaar en netwerkverkeer van besmette computers neemt toe.

### **Eindgebruikers blijven kwetsbaar**

Internetcriminelen kunnen nog steeds met relatief gemak de computers van thuisgebruikers overnemen. Zij bereiken dit door misbruik te maken van lekken in software of de angst van gebruikers, zoals we hebben gezien bij de snelle groei van nep-antivirus. De overgenomen computers worden op grote schaal gebruikt voor illegale activiteiten. Internetcriminelen stelen persoonlijke informatie en maken de gebruikers geld afhandig. We zien dit ook terug in de internationaal toegenomen fraude met internetbankieren.

### **Verlies van persoonsgegevens op internet vormt een structureel probleem**

Mensen laten bewust en onbewust veel informatie over zichzelf achter op internet. De mate waarin persoonlijke informatie gekoppeld kan worden, ook als je een redelijke inspanning verricht om bijvoorbeeld privé en zakelijk gescheiden te houden, wordt vaak onderschat. Met deze informatie worden social engineeringaanvallen op zowel organisaties als privé-personen uitgevoerd.

### **Zwakheden maken de infrastructuur van het internet kwetsbaar**

In het afgelopen jaar zijn nieuwe zwakheden ontdekt in de fundamenteën van het internet. Kwaadwillenden kunnen deze zwakheden misbruiken om gebruikers ongemerkt naar een kwaadaardige website te leiden of om websites onbereikbaar te maken. Als dergelijk misbruik op grote schaal voorkomt, kunnen essentiële diensten geschaad worden en kan het vertrouwen in internet afnemen.

### **De veroudering van cryptografie wordt onderschat**

Goede cryptografie is van essentieel belang voor de integriteit en vertrouwelijkheid van informatie. Er wordt te weinig rekening mee gehouden dat cryptografie snel verouderd, mede omdat aanvalstechnieken steeds verbeteren.

### **Bij verschuiving van toepassingen naar het web, verschuift de dreiging mee**

Computertoepassingen verplaatsen zich van desktops naar het web en we zien tegelijkertijd een snelle groei van mobiel internet. Daardoor zijn mensen meer online en zetten zij ook meer gevoelige informatie online. Toepassingen op internet worden daarmee een interessanter doelwit. Kwetsbaarheden in browsers en plug-ins zijn daarbij belangrijke aanvalsvectoren.

### **Kwetsbare software blijft de achilleshiel van informatiebeveiliging**

Kwetsbaarheden in software komen op grote schaal voor. Gebruikers en IT-afdelingen besteden als gevolg veel tijd aan het up-to-date houden van hun computersystemen. Daarom maken steeds meer softwareleveranciers beveiliging een integraal onderdeel van hun ontwikkelcyclus. Ook bevat software vaker automatische updatemechanismen, wat in de praktijk tot meer up-to-date software leidt. Als geheel staat de zorg voor veiliger software echter nog in de kinderschoenen, waardoor kwetsbaarheden in software voorlopig de belangrijkste aanvalsvector voor internetcriminelen blijven.

### **Hactivisme is een vast onderdeel van ideologische conflicten geworden**

Diverse incidenten in de sfeer van hactivisme en digitale oorlogsvoering geven aan dat conflicten van ideologische aard voortaan ten minste een cybercomponent hebben. DDoS-aanvallen, defacement en cyberspionage zijn daarvan enkele voorbeelden.

### **De security community werkt intensiever samen**

Intensieve internationale samenwerking neemt toe. Dat is gebleken bij de Conficker-casus. Conficker is malware die op grote schaal en wereldwijd machines heeft geïnfecteerd. Om de gevolgen van Conficker te beperken is er wereldwijd door verschillende partijen intensief samengewerkt (waaronder in de Conficker working group). Mede hierdoor zijn de gevolgen van het Conficker-virus relatief beperkt geweest.

### **Bestrijding en opsporing boeken belangrijke successen**

Het afgelopen jaar zijn belangrijke successen geboekt in de bestrijding en opsporing van cybercrime. In Nederland springen enkele zaken in het oog waarbij het Team High Tech Crime (onderdeel van het KLPD) effectief heeft samengewerkt met diverse opsporingsdiensten in het buitenland. Dit werpt zijn vruchten af: internetcriminelen worden vaker opgepakt en berecht. Opsporing en berechting zijn een effectief wapen tegen cybercrime. Het spamverbod in Nederland en de handhaving hiervan door OPTA heeft geleid tot een daling met 85% vanuit Nederland verstuurde spam, in vergelijking met 2004.



## Inhoud



<b>1</b>	<b>Het afgelopen jaar</b>	<b>8</b>
1.1	Informatiebeveiliging bij de overheid	8
1.2	Groei van de elektronische overheid	9
1.3	Het internet wordt de computer	9
1.4	De uitdaging	11
<b>2</b>	<b>Barsten in het fundament van het internet</b>	<b>12</b>
2.1	Internet is niet meer wat het geweest is	12
2.2	Kwetsbare protocollen: niet nieuw, maar wel urgenter	12
2.3	Cryptografie: aan de basis van informatiebeveiliging	16
<b>3</b>	<b>Internetcriminaliteit en innovatie</b>	<b>20</b>
3.1	Internet is het nieuwe besturingssysteem	20
3.2	Money makes the world go around	23
3.3	Macht en ideologie als drijfveer	26
3.4	Deanonimisatie – minder privacy	28
3.5	De status van internetveiligheid	30
<b>4</b>	<b>Incident response, toezicht en opsporing</b>	<b>32</b>
4.1	Botnets	33
4.2	Phishing	33
4.3	Spam	35
<b>5</b>	<b>Aanbevelingen</b>	<b>37</b>
5.1	Basismaatregelen blijven belangrijk	37
5.2	Specifieke aanbevelingen naar aanleiding van trends	37
	<b>Woordenlijst</b>	<b>39</b>
	<b>Over GOVCERT.NL</b>	<b>42</b>

# 1 Het afgelopen jaar

Het nieuws in het afgelopen jaar werd vooral beheerst door de kredietcrisis. Wereldwijd hebben economieën – mensen, bedrijven en overheden – financiële schade opgelopen. De gevolgen worden gevoeld in vrijwel alle lagen en sectoren van de maatschappij. De veranderde economische omstandigheden hebben ook invloed op informatiebeveiliging: qua budgetten, maar ook omdat andere omstandigheden andere dreigingen met zich mee brengen.

Hoewel als onderdeel van slinkende ICT-budgetten ook informatiebeveiligingsbudgetten kritisch bekeken worden, lijkt het erop dat bedrijven op dit vlak weinig extra risico willen accepteren. Uit onderzoeken komt bijvoorbeeld naar voren dat maar 10% van de onderzochte bedrijven hun securitybudget verlagen<sup>1</sup>. In alle andere gevallen blijft het budget gelijk of groeit het zelfs: security blijft belangrijk en is geen post om op te bezuinigen. Uit de onderzoeken blijkt ook dat dit waarschijnlijk niet ondanks maar dankzij de economische teruggang is. Daarbij wordt onder andere gewezen op de vergrote interne dreiging zoals van (ex-) medewerkers die uit frustratie systemen onklaar maken en informatie stelen.

In dit hoofdstuk beschrijven we verder de hoofdlijnen en ontwikkelingen op overheids- en ICT-gebied in het afgelopen jaar, die relevant zijn voor informatiebeveiliging.

## 1.1 Informatiebeveiliging bij de overheid

Ook overheden blijven in deze economisch onzekere tijden groot belang hechten aan informatiebeveiliging. Zo heeft president Obama vanwege het grote belang van internet voor de Amerikaanse economie uitgebreid de activiteiten op het gebied van cybersecurity laten doorlichten<sup>2</sup>. Resultaat van deze review is onder andere dat president Obama heeft besloten zelf een cybersecuritycoördinator te benoemen<sup>3</sup>. Deze coördinator moet onder andere zorgen voor een geïntegreerd overheidsbeleid voor cybersecurity en moet een reactie coördineren bij een groot cyberincident of een zware cyberaanval. De coördinator is lid van de Nationale Veiligheidsstaf. Het onderzoek laat verder zien dat een grotere inspanning nodig is in het onderwijs en op het gebied van publieke bewustwording over risico's en dat het delen van informatie tussen overheid, private sectoren en (internationale) samenwerkingspartners noodzakelijk is.

In Nederland besloot de ministerraad dat elk departement een Chief Information Officer (CIO) aanstelt. De CIO is verantwoordelijk voor een strategie inzake informatievoorziening van het eigen departement en zorgt voor de verbinding tussen het primaire proces en ICT. Bij de directie Bedrijfsvoering Rijksoverheid, onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, is een directeur informatiseringbeleid Rijk benoemd. Deze 'Rijks-CIO' gaat richting geven aan de manier waarop ICT binnen de overheid wordt ingezet. Onder de verantwoordelijkheid van de CIO's valt uiteraard ook informatiebeveiliging. Adviserend aan de CIO's is een rijksbrede commissie, subcommissie informatiebeveiliging, aangesteld waarin informatiebeveiligingsfunctionarissen van alle ministeries plaatshebben.

<sup>1</sup> De onderzoeken van CA, Infosecurity Europe en Finjan zijn op dit punt in overeenstemming met elkaar. Informatie uit de onderzoeken is te vinden op [www.ca.com/us/products/collateral.aspx?cid=203706](http://www.ca.com/us/products/collateral.aspx?cid=203706), [www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1389](http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1389) en [www.finjan.com/Pressrelease.aspx?id=2140&PressLan=2139&lan=3](http://www.finjan.com/Pressrelease.aspx?id=2140&PressLan=2139&lan=3)

<sup>2</sup> Het rapport is te downloaden op [www.whitehouse.gov/asset.aspx?AssetId=1732](http://www.whitehouse.gov/asset.aspx?AssetId=1732)

<sup>3</sup> De toespraak waarin Obama de positie van de cybersecuritycoördinator aankondigt, is integraal online geplaatst: [www.whitehouse.gov/the\\_press\\_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/](http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/)

## 1.2 Groei van de elektronische overheid

Nu de overheid haar dienstverlening naar burgers steeds verder digitaliseert en integreert, nemen de risico's op misbruik van overheids- en burgergegevens ook toe. Daarbij geldt: hoe complexer een systeem is, hoe groter de kans op misbruik is.

Voorbeelden van complexe systemen die in 2008 sterk onder de aandacht waren, zijn de digitale dossiers. Zo kennen we onder meer het Elektronisch Patiënten Dossier (EPD), het Elektronisch Kind Dossier (EKD) en het Digitale Klant Dossier (DKD). Al deze dossiers hebben gemeenschappelijk dat ze gegevens van verschillende organisaties samenbrengen en delen. De risico's die dat met zich meebrengt, zoals het ongewenst inzien van gegevens, leiden tot hoge eisen aan de informatiebeveiliging. De authenticatie van gebruikers, toegangsbeheer tot persoonlijke gegevens en het loggen wie welke gegevens heeft gewijzigd en ingezien, zijn daarbij belangrijke aspecten.

Tegen het EPD bestaat overigens onder de Nederlandse bevolking momenteel een weerstand die groter is dan aanvankelijk verwacht. Medio maart 2009 waren er ongeveer 438.000 bezwaren ontvangen door het Informatiepunt BSN in de Zorg en Landelijk EPD<sup>4</sup>. Ook onder artsen is het aantal gemaakte bezwaren aanzienlijk. Uit een enquête van het blad Medisch Contact bleek dat 31% van de ondervraagde artsen bezwaar had ingediend<sup>5</sup>. Uit ander onderzoek is gebleken dat 70% vertrouwen heeft in de betrouwbaarheid van de uitwisseling van medische gegevens<sup>6</sup>.

Om meer focus en samenhang te krijgen in het ontwikkelen en in gebruik nemen van bouwstenen van de e-overheid, hebben rijk, provincies, gemeenten en waterschappen afspraken gemaakt in het Nationaal Uitvoerings Programma Dienstverlening en e-Overheid (NUP)<sup>7</sup>. Het intensievere gebruik roept echter ook nieuwe vragen op. Deze vragen gaan, als het gaat om beveiliging, vooral over de risico's van het gebruik van internet voor de kernactiviteiten van een overheidsorganisatie. De eisen die een overheid aan een infrastructuur stelt, zijn namelijk anders van aard dan de eisen van de meeste bedrijven, en sommige risico's kunnen niet simpelweg worden geclassificeerd als bedrijfsrisico. Wanneer de overheid en bedrijven intensiever gebruikmaken van internet, wordt het ook steeds belangrijker dat het internet goed functioneert.

## 1.3 Het internet wordt de computer

Het afgelopen jaar hebben we een verdere groei gezien van toepassingen op het web. Diensten en sociale interactie spelen zich meer en meer op het web af. Waar informatie en informatiesystemen zich bevinden wordt daarbij steeds minder duidelijk. Hier wordt ook wel gesproken over cloud computing. Het web biedt goede mogelijkheden voor het delen en combineren van informatie uit verschillende bronnen. De complexiteit neemt dan echter ook toe: het wordt minder inzichtelijk waar de informatie vandaan komt, of de informatie juist is en wie de eigenaar ervan is. Door de openheid van internet is het moeilijk vertrouwelijke informatie ook echt vertrouwelijk te houden.

<sup>4</sup> Zie hiervoor de 'Voortgangsrapportage Elektronische Patiëntendossier' op [www.minvws.nl/kamerstukken/meva/2009/voortgangsrapportage-elektronisch-patientendossier.asp](http://www.minvws.nl/kamerstukken/meva/2009/voortgangsrapportage-elektronisch-patientendossier.asp)

<sup>5</sup> Meer over het onderzoek is te lezen op [medischcontact.artsennet.nl/tijdschrift/archief/Tijdschriftartikel/Te-vroeg-voor-landelijk-EPD.htm](http://medischcontact.artsennet.nl/tijdschrift/archief/Tijdschriftartikel/Te-vroeg-voor-landelijk-EPD.htm)

<sup>6</sup> [www.npcf.nl/uploads/files/eindrapport\\_epd\\_tns\\_nipo\\_npcf.pdf](http://www.npcf.nl/uploads/files/eindrapport_epd_tns_nipo_npcf.pdf)

<sup>7</sup> [www.e-overheid.nl/sites/nup](http://www.e-overheid.nl/sites/nup)

Google wordt een steeds dominantere partij voor (webgebaseerde) toepassingen en kan in potentie de plaats innemen die Microsoft traditioneel had. Google search is voor 95% van de Nederlanders de meest gebruikte zoekmachine<sup>8</sup> en Google biedt daarnaast ook e-mail, een agenda, kantoortoepassingen in de vorm van Google Docs, kaarten, instant messaging, video's, fotobewerking en zelfs een persoonlijk patiëntendossier. Dit alles is toegankelijk vanuit elke browser, waaronder die van Google zelf. Ook Microsoft, Apple en vele andere leveranciers bieden steeds meer toepassingen aan op het web die voorheen alleen op de eigen PC konden worden gebruikt. Door het groeiende gebruik van deze webdiensten, worden ze een steeds aantrekkelijker doelwit voor internetcriminelen: er is steeds meer informatie te vinden en de webdiensten kunnen centraal worden aangevallen.

Een ander voorbeeld van de toenemende verschuiving naar webtoepassingen zijn sociale netwerken. Begin dit jaar sprak een Hyves-medewerker van 7 miljoen Hyves-profielen van geregistreerde Nederlanders, waarvan er ongeveer 5 miljoen in de maand ervoor actief waren geweest<sup>9</sup>. Daarnaast is Twitter een in het oog springende netwerkdienst, met een spectaculaire bezoekersgroei van honderden procenten in het afgelopen jaar<sup>10</sup>. Het gebruik van Twitter door kiezers tijdens de Amerikaanse verkiezingen vorig jaar sprak tot de verbeelding, maar ook overheden zelf twitteren. In Nederland is minister Verhagen waarschijnlijk de bekendste 'overheidstwitteraar'; ruim 14 duizend mensen volgen zijn tweets.

Een steeds groter deel van onze levens speelt zich af op sociale netwerksites. Daarmee is het afgelopen jaar zonder twijfel ook het jaar geweest van verdere vervaging tussen de online en offline wereld. Onze online en offline levens, zakelijk en privé, gaan vloeiend in elkaar over.



<sup>8)</sup> [www.checkit.nl/nationalesearchenginemonitor.html](http://www.checkit.nl/nationalesearchenginemonitor.html)

<sup>9)</sup> 'Hyves statistieken en leugens;-)' door Yme Bosma op [www.yme.nl/ymerce/2009/01/08/hyves-statistieken-en-leugens/](http://www.yme.nl/ymerce/2009/01/08/hyves-statistieken-en-leugens/)

<sup>10)</sup> [blog.nielsen.com/nielsenwire/online\\_mobile/twitters-tweet-smell-of-success/](http://blog.nielsen.com/nielsenwire/online_mobile/twitters-tweet-smell-of-success/) en [blog.compete.com/2009/03/13/twitter-search/](http://blog.compete.com/2009/03/13/twitter-search/)

## 1.4 De uitdaging

Door het centraal beschikbaar komen van informatie en informatiesystemen op internet, nemen de risico's van misbruik en diefstal ervan toe. Daarnaast wordt de afhankelijkheid van de internetinfrastructuur en de gegevens die er zijn opgeslagen, maar ook van de informatiesystemen die deze informatie bewerken, steeds groter.

De uitdaging is om de openheid en toegankelijkheid van de internettechnologie te benutten, en deze tegelijkertijd zo veilig mogelijk te maken en te houden. Het is vooral belangrijk de informatiebeveiligingsaspecten goed te analyseren. Niet om mogelijkheden te mijden of te verbieden, maar om optimaal, veilig gebruik mogelijk te maken. Dit type diensten is immers niet de toekomst: ze zijn er nu en worden nu gebruikt. We moeten er verantwoord mee omgaan.

De overheid speelt hierbij een belangrijke rol. Overheden zijn namelijk niet alleen verantwoordelijk voor een gedegen informatiebeveiliging van de eigen systemen, processen en informatie, maar spelen ook een belangrijke rol als het gaat om de vitale infrastructuur, privacybescherming en economische stabiliteit van een land. De overheid kan het zeker niet alleen. Er zal met diverse partijen samengewerkt moeten worden om te zorgen dat zowel de infrastructuur als de informatie en de informatiesystemen aan de veiligheidseisen voldoen. De bovengenoemde ontwikkelingen worden verder uitgewerkt in de volgende hoofdstukken. In hoofdstuk 2 zullen we de vraag "Is het internet stuk?" beantwoorden. In hoofdstuk 3 gaan we dieper in op de verschuiving van toepassingen naar het internet en wat dit betekent voor kwaadaardige activiteiten op internet. Daarnaast beschrijven we fenomenen uit het afgelopen jaar, zoals nep-antivirus en Conficker. Ten slotte besteden we in hoofdstuk 4 ruim aandacht aan enkele opvallende successen die geboekt zijn bij de bestrijding van kwaadaardige activiteiten op internet.

## 2 Barsten in het fundament van het internet

Internet is in het dagelijks leven zo belangrijk geworden, dat veel mensen en organisaties niet meer zonder kunnen. Daarom is het van groot belang dat de basale infrastructuur van internet goed werkt. Afgelopen jaar is echter gebleken dat we daar niet zomaar van uit kunnen gaan.

Dit hoofdstuk gaat over de kwetsbaarheid van de infrastructuur van internet en belangrijke en urgente verbeteringen die nodig zijn om de beveiliging van internet als infrastructuur te verhogen.

### 2.1 Internet is niet meer wat het geweest is

Van een infrastructuur met zo'n groot maatschappelijk en economisch belang mag je verwachten dat het in alle opzichten betrouwbaar is. Helaas is dit bij het internet niet het geval.

Het internet is ooit ontworpen als militair netwerk, bedoeld om robuust en veerkrachtig te zijn, zodat het ook blijft werken als delen van het netwerk uitvallen. Bij het ontwerp is te weinig aandacht geschonken aan de integriteit van de informatie die nodig is om het netwerk goed te beheren, waardoor de fundamentele beperkingen op deze gebieden hebben. Doordat het gebruik van internet elk jaar intensiveert en onze afhankelijkheid ervan steeds verder toeneemt, worden deze beperkingen in de fundamentele steeds nijpender. Zo werden in enkele communicatieprotocollen en cryptografische standaarden zwakheden ontdekt die grote impact kunnen hebben op de betrouwbaarheid van het internet. In de media is uitgebreid aandacht besteed aan deze ontdekkingen en sommige gingen zelfs zo ver om te stellen dat het internet 'stuk' was.

*“Van een infrastructuur met zo'n groot maatschappelijk en economisch belang mag je verwachten dat het in alle opzichten betrouwbaar is. Helaas is dit bij het internet niet altijd het geval”*

Hoewel dit laatste zeker niet het geval is, leiden deze incidenten wel tot een belangrijke constatering: de fundamentele van het internet sluiten niet aan bij de eisen die het moderne gebruik ervan stelt. Waar we lange tijd de fundamentele van het internet als een (bijna saai) gegeven hebben beschouwd, staan ze nu weer volop in de spotlights. Er moet nu actie worden ondernomen om te zorgen dat de fundamentele wel kunnen voldoen aan de eisen en dit in de toekomst ook blijven doen. Gezien de omvang van het internet en de versnipperde verantwoordelijkheden is dit een moeilijke opgave.

### 2.2 Kwetsbare protocollen: niet nieuw, maar wel urgenter

Het afgelopen jaar is er veel aandacht geweest voor kwetsbaarheden in protocollen (de talen die computers met elkaar spreken) die van fundamenteel belang zijn voor een goede werking van het internet: TCP, DNS en BGP. Deze protocollen zorgen ervoor dat computers elkaar op internet op een zo efficiënt mogelijke manier weten te vinden. Over de kwetsbaarheid in TCP, waarover het Zweedse bedrijf Outpost24 in oktober 2008 naar buiten trad, zijn de precieze details nog niet publiek<sup>11</sup>. Het gaat in elk geval om een Denial of Service-kwetsbaarheid, waarbij het mogelijk is een andere computer onbereikbaar te maken door het versturen van een beperkt aantal netwerkberichten<sup>12</sup>. Op een netwerk als het internet, waar zoveel computers met elkaar verbonden zijn, kan de impact hiervan enorm zijn.

<sup>11</sup> De Finse overheids-CERT CERT-FI heeft de coördinatie rondom deze kwetsbaarheid in handen.

Verwacht wordt dat in de loop van 2009 meer details bekend zullen worden.

Zie voor meer informatie ook [www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html](http://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html).

<sup>12</sup> Een interview met Robert Lee, CEO van Outpost24, over de kwetsbaarheid is te beluisteren op [debeveiligingsupdate.nl/2008/09/30/de-beveiligingsupdate-3-socketstress](http://debeveiligingsupdate.nl/2008/09/30/de-beveiligingsupdate-3-socketstress)

De kwetsbaarheden in DNS en BGP vertonen overeenkomsten. Succesvolle uitbuiting van de daarin ontdekte kwetsbaarheden zou ertoe kunnen leiden dat het netwerkverkeer tussen computers wordt omgeleid, afgeluisterd of gemanipuleerd. Iemand die een verbinding probeert te maken met de website van zijn bank of van de overheid kan in zo'n geval bijvoorbeeld ongemerkt doorgestuurd worden naar een nep-website, waarna zijn inloggegevens afgegeven worden aan de internetcrimineel.

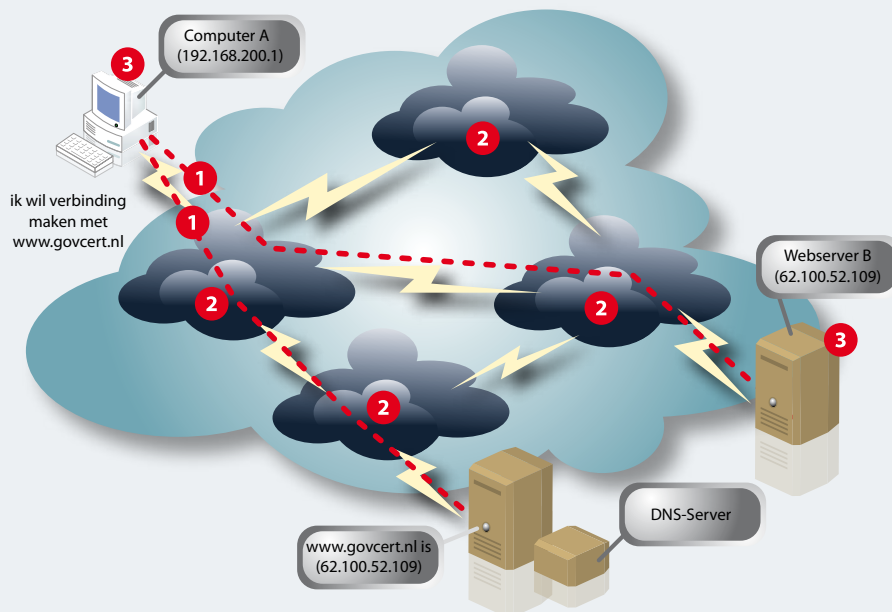
De ontdekte kwetsbaarheden zijn ernstig, vooral omdat ze door het fundamentele karakter van de protocollen raken aan de basis van het internet. De gevolgen ervan kunnen dan ook groot zijn. Maar toch komen deze kwetsbaarheden, ondanks de grote media-aandacht, niet helemaal als een verrassing. Dat de genoemde protocollen kwetsbaarheden bevatten – die in de praktijk ook worden uitgebuit – is al langer bekend. In het geval van DNS is er zelfs al ruim tien jaar een veilig alternatief, maar dat wordt zelden gebruikt. Ook voor BGP zijn er

### BGP, TCP en DNS, wat zijn dat eigenlijk?

TCP en DNS zijn geen bekenden van de meeste internetgebruikers. Terwijl de meeste mensen gehoord hebben van HTTP, ligt de bekendheid van DNS en TCP al een stuk lager. BGP is helemaal een grote onbekende. Toch is diepgaande kennis van deze protocollen niet nodig om hun relevantie op waarde te kunnen schatten.

Het internet is niet één groot netwerk, maar een netwerk van netwerken. Grote en kleine netwerken communiceren met elkaar en vormen zo het internet. Alle computers op internet hebben een IP-adres. Dit is een uniek nummer (een netwerkadres) waarmee de computer te bereiken is. Omdat mensen makkelijker omgaan met namen dan met nummers is het DNS (Domain Name System) bedacht. DNS koppelt namen aan IP-adressen. Als je bijvoorbeeld een verbinding wilt maken met `www.govcert.nl`, dan zorgt een DNS-server voor de vertaling van `www.govcert.nl` naar het IP-adres van die computer (1).

Met behulp van BGP (Border Gateway Protocol) wordt bepaald welke route het beste is om, via tussenliggende netwerken, van computer A naar computer B te komen (2). TCP (Transmission Control Protocol) ten slotte, verzorgt de daadwerkelijke verbinding tussen twee computers (3).



Figuur 2-1 Samenhang tussen BGP, DNS en TCP

alternatieven, maar die worden slechts langzaam of helemaal niet in gebruik genomen. Het probleem is dat de eigenaren van netwerken wel de kosten van deze aanpassingen dragen, maar ze hebben er zelf op de korte termijn weinig voordeel bij<sup>13</sup>.

*“De toegenomen afhankelijkheid van internet maakt dat we deze kwetsbaarheden met grote urgentie moeten verhelpen”*

De media-aandacht voor het vraagstuk of het internet stuk is, is deels terecht. Hoewel kwetsbaarheden in TCP, DNS en BGP niet nieuw zijn, is het gemak waarmee de aanvallen kunnen worden ingezet veel groter geworden. Al vele jaren wordt ervoor gewaarschuwd dat de basisprotocollen waarop internet draait niet veilig zijn<sup>14</sup>. De toegenomen afhankelijkheid van het internet, voor zowel het bedrijfsleven als de overheid en als voor de samenleving als geheel, maakt dat we deze kwetsbaarheden met grote urgentie moeten verhelpen.

### **2.2.1 BGP: Border Gateway Protocol**

Het BGP-protocol dat de routing van berichtverkeer op internet tussen computers regelt bevat kwetsbaarheden omdat het protocol werkt op basis van vertrouwen. Hiermee kan netwerkverkeer zowel bewust (door kwaadwillenden) als onbewust (door menselijke fouten) naar een andere computer worden omgeleid. Bij een geslaagde aanval kan al het omgeleide netwerkverkeer bekeken en, in sommige gevallen, aangepast worden<sup>15</sup>. Dit alles zonder dat het voor de gebruiker altijd duidelijk is dat het verkeer omgeleid is geweest.

Een bekend voorbeeld hiervan is het per ongeluk kapen van een deel van het netwerk van YouTube door Pakistan Telecom in februari 2008<sup>16</sup>. Hierdoor was YouTube enige tijd niet bereikbaar. Het kapen gebeurt ook met opzet, bijvoorbeeld om tijdelijk een netwerk ‘te hebben’ om van daaruit spam te kunnen versturen<sup>17</sup>. De complexiteit van het internet zorgt er overigens voor dat een dergelijke aanval niet per se wereldwijde gevolgen hoeft te hebben.

Voor BGP zijn enkele veilige alternatieven beschikbaar, die nog niet in gebruik zijn. Dit komt voornamelijk doordat zo’n alternatief pas echt waarde heeft als iedereen het gebruikt. Ook zijn er best practices die de risico’s van het gebruik van BGP verminderen, zoals het filteren van bepaalde routeringsberichten door ISP’s. Deze best practices worden wel in praktijk gebracht, maar lang niet door alle netwerkproviders. Ze zijn vaak kostbaar, tijdrovend en complex om in te voeren en zijn vooral van belang voor het internet als geheel en slechts van marginaal belang voor de netwerkbeheerder zelf. Arbor Networks concludeert in haar “Worldwide Infrastructure Security Report 2008”<sup>18</sup> dat de staat van beveiliging van routing op het internet met name door de groei en toegenomen complexiteit, in de afgelopen 10 jaar achteruit is gegaan.

<sup>13</sup> Er is overigens behoorlijk wat beweging op dit vlak. Er zijn meerdere samenwerkingsverbanden die onderzoeken welke mogelijkheden er zijn om het DNS-systeem te verbeteren en hoe dit op een praktische wijze aan te pakken is.

<sup>14</sup> [www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf](http://www.cs.columbia.edu/~smb/papers/acsac-ipext.pdf) en [www.nap.edu/openbook.php?record\\_id=6161](http://www.nap.edu/openbook.php?record_id=6161)

<sup>15</sup> Een en ander is uiteraard afhankelijk van het gebruik van versleuteling op het netwerkverkeer.

<sup>16</sup> RIPE heeft hiervan een case study gemaakt die te zien is op [www.ripe.net/news/study-youtube-hijacking.html](http://www.ripe.net/news/study-youtube-hijacking.html)

<sup>17</sup> Anirudh Ramachandran en Nick Feamster hebben dit overtuigend aangetoond in hun paper “Understanding the NetworkLevel Behavior of Spammers” uit 2006, te lezen op [www.cc.gatech.edu/~avr/publications/p396-ramachandran-sigcomm06.pdf](http://www.cc.gatech.edu/~avr/publications/p396-ramachandran-sigcomm06.pdf)

<sup>18</sup> Verkrijgbaar (na registratie) via [www.arbornetworks.com/report](http://www.arbornetworks.com/report)

## De aanval op BGP

In augustus 2008 presenteerden Alex Pilosov en Anton Kapela op DefCon een Man in the Middle-aanval met behulp van BGP<sup>19</sup>. Hun aanval maakt op slimme wijze gebruik van een aantal 'normale' eigenschappen van BGP. Cruciaal is dat BGP werkt op basis van vertrouwen. Elk netwerk op internet (in jargon een Autonomous System (AS) dat geïdentificeerd wordt met een AS-nummer) stuurt aankondigingen de wereld in over de IP-adressen die zich in het eigen netwerk bevinden en andere IP-adressen die, met het netwerk als tussenstap, bereikt kunnen worden. Op basis van deze aankondigingen kunnen routers beslissen wat de beste route is die netwerkverkeer kan nemen.

De aanval van Pilosov en Kapela bestaat uit twee delen. In het eerste deel wordt het verkeer voor een bepaald netwerk gekaapt. Dit is, door de aard van BGP, niet ingewikkeld. Moeilijker is het, om het gekaapte verkeer weer verder te routeren. Normaal gesproken werkt dit niet, omdat – als gevolg van de kaping – het netwerkverkeer juist niet meer naar het oorspronkelijke doel gerouteerd kan worden. In dit geval is vooraf een route gepland naar het gekaapte netwerk. Deze route, inclusief alle routers die daarin een rol spelen, werd gedocumenteerd. Tijdens de aanval is gebruikgemaakt van AS path prepending om de gedocumenteerde routers de kaping te laten negeren. Omdat deze routers niet van de kaping wisten, konden zij alsnog worden gebruikt om het gekaapte verkeer door te sturen naar het oorspronkelijke doelnetwerk. Ook werd de Time-to-live (TTL) van netwerkpakketten gemanipuleerd, waardoor de systemen van de aanval in een netwerktrace onzichtbaar werden.

### 2.2.2 DNS: Domain Name System

Halverwege 2008 maakte onderzoeker Dan Kaminsky bekend dat hij een nieuwe aanvalstechniek op DNS had ontdekt. De aanvalstechniek, een combinatie van twee bekende zwakheden in dit systeem, stelt kwaadwillenden in staat om bepaalde DNS-servers te vervuilen met foutieve informatie (cache poisoning). Op het moment dat een DNS-server dergelijke vervuilde informatie bevat, kan een aangesloten gebruiker ongemerkt op een andere website terecht komen dan waar hij om gevraagd heeft (bijvoorbeeld een nepsite voor internetbankieren)<sup>20</sup>.

Door een gecoördineerde actie van leveranciers van DNS-producten zijn aanpassingen doorgevoerd waardoor het moeilijker is geworden DNS aan te vallen. Maar een fundamenteel betere oplossing is het gebruiken van Domain Name System Security Extensions (DNSSEC), een specificatie die al sinds eind jaren '90 beschikbaar is. Via DNSSEC plaatst een eigenaar van een domein een digitale handtekening bij de domeininformatie, waardoor deze informatie op juistheid geverifieerd kan worden.

Vanaf eind 2008 kiezen steeds meer partijen voor DNSSEC. Zo zijn in de Verenigde Staten alle overheden verplicht om voor het einde van 2009 DNSSEC te ondersteunen. Ook verschillende registries die verantwoordelijk zijn voor de landendomeinen, ondersteunen DNSSEC: zoals Zweden, Bulgarije en Tsjechië. De registry van Nederland, de Stichting Internet Domeinregistratie Nederland (SIDN), heeft plannen om ondersteuning van DNSSEC voor het .nl-domein in 2009 te gaan inrichten. In Nederland is vanuit de overheid nog geen uitspraak gedaan over het gebruik van DNSSEC. Een klein onderzoek van GOVCERT.NL in april 2009 onder 466 overheidsorganisaties<sup>21</sup> wees uit dat DNSSEC door geen van de onderzochte overheidsorganisaties wordt ondersteund.

<sup>19)</sup> [eng.5ninesdata.com/~tkapela/iphd-2.ppt](http://eng.5ninesdata.com/~tkapela/iphd-2.ppt)

<sup>20)</sup> Meer informatie over "De Kaminsky Code" is te lezen in de factsheet die GOVCERT.NL hierover heeft uitgebracht. Deze factsheet bevat ook tips om de kwetsbaarheid op te lossen en is te lezen op [www.govcert.nl/download.html?f=118](http://www.govcert.nl/download.html?f=118)

<sup>21)</sup> GOVCERT.NL heeft de nameservers onderzocht van de 13 ministeries, 12 provincies en 441 gemeenten

Naast de kwetsbaarheid van Kaminsky was er het afgelopen jaar ook weer aandacht voor DNS Amplification. Deze techniek, die al in 2006 uitgebreid werd beschreven, maakt het mogelijk om een Distributed Denial-of-Service (DDoS)-aanval uit te voeren door misbruik te maken van DNS-servers. De aanval is erop gebaseerd dat een kleine DNS-vraag soms een zeer groot antwoord kan hebben. Door de DNS-vraag te versturen met als afzender de aan te vallen computer, kun je deze computer onbereikbaar maken.

### Recursieve en autoritatieve DNS-servers

Tot voor kort was de veronderstelling dat DNS Amplification-aanvallen alleen mogelijk waren richting recursieve DNS-servers die normaal gesproken, maar lang niet altijd, alleen op een lokaal netwerk bereikbaar zijn. Hierdoor is misbruik in de praktijk relatief moeilijk. Nu is echter een variant op deze techniek bekendgemaakt, waardoor ook autoritatieve (niet-recursieve) DNS-servers kunnen worden ingezet voor het uitvoeren van een DDoS-aanval. Bij deze variant vraagt een kwaadwillende een autoritatieve DNS-server naar alle bekende DNS root servers. Aangezien de lijst met DNS root servers lang is, biedt de grootte van het antwoord voldoende mogelijkheden om een DDoS-aanval uit te voeren. Via IP-spoofing is het dan mogelijk om een willekeurig IP-adres te overstelpen met DNS-antwoorden.

### 2.3 Cryptografie: aan de basis van informatiebeveiliging

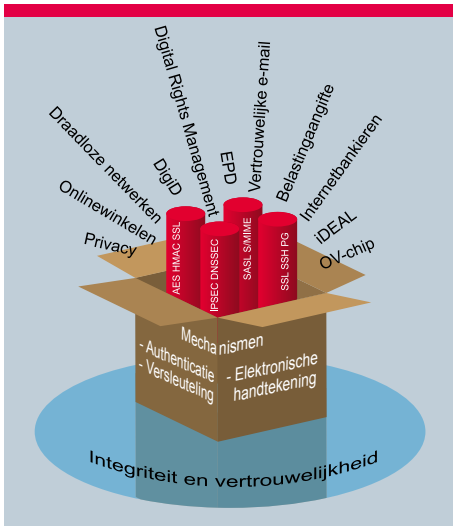
In dit deel van het hoofdstuk besteden we aandacht aan een opvallende serie kwetsbaarheden en incidenten die te maken hebben met cryptografie. Cryptografie is van belang voor het garanderen van vertrouwelijkheid en de integriteit van informatie en daarmee cruciaal voor informatiebeveiliging en voor veel zaken die wij in ons dagelijks leven doen. Cryptografie is een wiskundig vakgebied, waar kleine fouten grote gevolgen kunnen hebben. Het is ook een vakgebied dat continu in ontwikkeling is, zowel als het gaat om het ontwerpen van nieuwe

algoritmen als om het ontdekken van zwakke plekken in bestaande algoritmen en het bedenken van nieuwe aanvallen en aanvalscenario's.

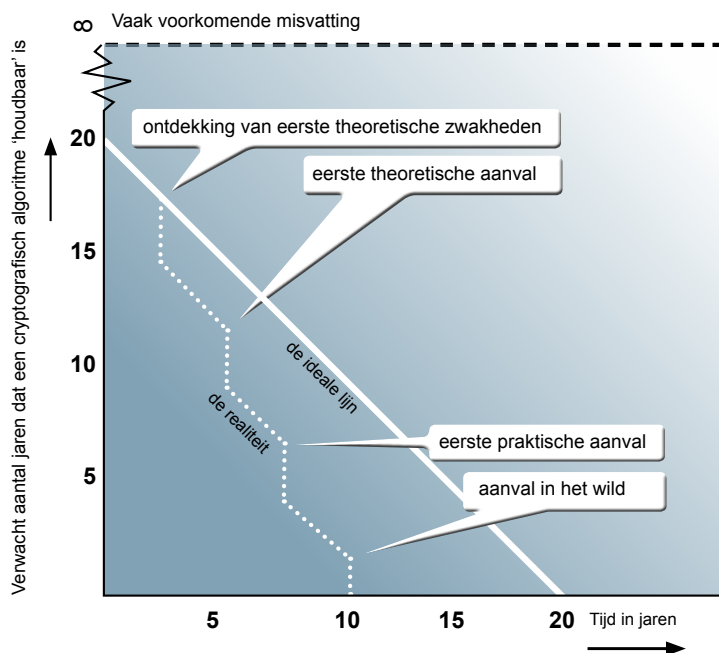
De kwetsbaarheden en incidenten die we hieronder behandelen gaan niet alleen over zwakke algoritmen zoals in de gebeurtenissen rondom de Mifare-chip, waarover we vorig jaar uitgebreid hebben bericht. Want zelfs als de keuze wordt gemaakt voor robuuste versleuteling, is succes niet gegarandeerd. Versleuteling is een technische oplossing, die zijn werk alleen goed kan doen als deze regelmatig geëvalueerd wordt en goed gebruikt wordt, zowel in technische als in organisatorische zin.

De Nederlandse overheid is zich hiervan bewust. Recent nog, bij de presentatie van de nieuwe rijksпас, benadrukte de heer Welling, voorzitter van de stuurgroep Rijksпас dat de pas niet eeuwig houdbaar zal zijn: "De pas zal een keer gekraakt worden, dat weten we."<sup>22</sup> Dit realisme is belangrijk: je moet ervan uit gaan dat elk cryptografisch algoritme zwakheden bevat, die op een moment in de toekomst ontdekt zullen worden. Daar bovenop komt de steeds

toenemende rekenkracht van computers. Deze twee factoren zorgen ervoor dat elk cryptografisch algoritme beperkt houdbaar is. In figuur 2-2 is dit grafisch weergegeven. Dit, en de organisatorische aspecten rondom cryptografie, komen in de nu volgende paragrafen aan bod.



<sup>22</sup> www.pm.nl/index.php?page=verbeterde-rijksпас-klaar-voor-gebruik



Figuur 2-2 De verjaring van cryptografie

### 2.3.1 MD5: het tijdig vervangen van verouderde cryptografie

Rond kerst 2008 werd door de Nederlandse onderzoeker Benne de Weger een opzienbarende aanval vertoond op de Public Key Infrastructure (PKI) die gebruikt wordt voor certificaten van beveiligde websites, door de onderzoekers de 'Internet PKI' genoemd<sup>23</sup>. Het is de naam voor het geheel aan SSL-certificaten, hun eigenaren en de organisaties die de certificaten verstrekken, Certificate Authorities (CA's).

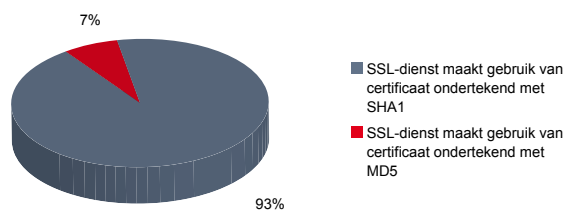
De aanval bouwde voort op vele jaren van onderzoek naar de zwakheden van de hashfunctie MD5: al in 2004 werd gewaarschuwd dat de bruikbaarheid van MD5 voor bepaalde toepassingen ten einde liep<sup>24</sup>. Met de nieuwe aanval waren de onderzoekers in staat om een certificaat te maken waarbij ze de handtekening van de CA van een ander certificaat gebruikten om hun eigen certificaat een geldige status te geven. De aanval was mogelijk omdat de MD5-hashwaarde van hun eigen certificaat identiek was aan de hashwaarde van het andere certificaat (hash collision).

Met het overzetten van de handtekening van de CA naar hun frauduleuze certificaat hadden de aanvallers een certificaat in handen waarmee ze nieuwe certificaten konden ondertekenen die door elke browser vertrouwd zouden worden. Nieuwe certificaten voor elk gewenst domein ter wereld, ook bestaande domeinen van andere partijen. Kwaadwillenden hebben hiermee de mogelijkheid zich voor te doen als een ander.

<sup>23</sup> Een beschrijving van het onderzoek is te vinden op [www.win.tue.nl/hashclash/rogue-ca/](http://www.win.tue.nl/hashclash/rogue-ca/). GOVCERT.NL heeft over dit onderwerp een factsheet gepubliceerd op [www.govcert.nl/download.html?f=122](http://www.govcert.nl/download.html?f=122)

<sup>24</sup> [eprint.iacr.org/2004/264.pdf](http://eprint.iacr.org/2004/264.pdf)

De getoonde aanval toont aan dat problemen rondom de uitgifte van certificaten in een deel van de PKI verstrekende gevolgen kunnen hebben voor de gehele PKI. De controles die CA's uitvoeren bij de uitgifte van een nieuw certificaat, bedoeld om zekerheid te bieden over de aanvragende partij, zijn soms triviaal. De aanval toont verder aan dat zelfs de CA's te lang gebruik blijven maken van verouderde cryptografische algoritmen.



Figuur 2-3  
Gebruik van SSL-certificaten door de onderzochte organisaties (n=163)

Het belang van de PKI is groot: het wordt onder andere gebruikt voor internetbankieren, onlinewinkelen en soms voor het vertrouwelijke berichtenverkeer van de overheid met haar burgers en tussen overheden onderling. Het is daarom zeer verontrustend dat een dergelijke aanval kon slagen.

Naar aanleiding van deze aanval heeft GOVCERT.NL een kort onderzoek uitgevoerd naar het gebruik van SSL-certificaten op de websites van een aantal Nederlandse overheidsorganisaties<sup>25</sup>. Uit dit onderzoek blijkt dat nog slechts 11 organisaties gebruikmaken van een certificaat dat ondertekend is met MD5 (zie figuur 2-3). Deze certificaten hebben nog geen kwetsbaarheden tot gevolg, maar moeten wel op korte termijn worden vervangen.

### 2.3.2 Debian OpenSSL: een kleine beslissing met grote gevolgen

Een ander incident met een fundamentele cryptografische toepassing op internet betrof OpenSSL. OpenSSL wordt onder andere gebruikt voor het maken van cryptografische sleutels. In mei 2008 bleek dat OpenSSL geen willekeurige getallen meer kon genereren waardoor sleutels gemaakt met OpenSSL als gevolg hiervan zeer zwak en feitelijk waardeeloos waren. Versleutelde sessies op basis van deze sleutels konden worden afgeluisterd.

De zwakheid bleek het gevolg van de beslissing die een programmeur bijna twee jaar eerder had gemaakt. Een deel van de code van OpenSSL veroorzaakte namelijk waarschuwingen bij het gebruik van een analysetool voor geheugenlekken en corruptie. De programmeur besloot toen om bepaalde delen van de code te verwijderen die niet relevant leken en die de waarschuwing veroorzaakten. Pas ruim anderhalf jaar later bleek dat deze code bedoeld was om willekeurige getallen te genereren.

Anderhalf jaar lang heeft er dus een zeer ernstige zwakheid gezeten in de implementatie van een cryptografisch algoritme van een vaak gebruikt besturingssysteem. Ondanks dat het een open source product was, en de broncode dus voor iedereen is in te zien, heeft het lang geduurd voordat het probleem werd gevonden. De consequentie was dat iedereen die in die anderhalf jaar cryptografisch sleutel materiaal had gegenereerd op basis van die zwakke versie van OpenSSL, de sleutels opnieuw moest genereren. Een kleine verkeerde beslissing van een programmeur heeft in dit geval dus zeer verstrekende gevolgen gehad voor de veiligheid van vele systemen wereldwijd, en het oplossen van het probleem heeft wereldwijd veel geld gekost.

<sup>25</sup>) GOVCERT.NL heeft de primaire webservers onderzocht van de 13 ministeries, 12 provincies en 441 gemeenten

### 2.3.3 WPA/TKIP: draadloze beveiliging verder ontrafeld

De laatste opvallende ontwikkeling op het gebied van versleuteling is een kwetsbaarheid in de beveiliging van draadloze netwerken die in november 2008 werd aangetoond. Het gaat om een kwetsbaarheid in het Temporal Key Integrity Protocol (TKIP), gebruikt voor de beveiliging van draadloze netwerken in Wi-Fi Protected Access (WPA) en als optie in WPA2<sup>26</sup>. Dit incident toont ook aan dat het van belang is om cryptografische oplossingen op regelmatige basis te herzien. Concreet is deze aanval het eerste signaal dat het verstandig is om op korte termijn af te stappen van TKIP voor beveiliging van draadloze netwerken en gebruik te gaan maken van AES-versleuteling als optie in WPA2.

Onderzoekers toonden met hun aanval aan dat ze erin geslaagd waren om de versleuteling van een draadloos netwerk te doorbreken, zelfs als dit beveiligd is met WPA met TKIP<sup>27</sup>. TKIP werd tot dan toe beschouwd als behoorlijk robuust, ook al was het destijds geïntroduceerd als 'lapmiddel' voor het zeer kwetsbare WEP. De onderzoekers doorbraken overigens maar een deel van de beveiliging en hun aanval is alleen mogelijk onder bepaalde omstandigheden. Toch wordt hun onderzoek gezien als een doorbraak: het is de eerste keer dat een dergelijke aanval op TKIP geslaagd is.

<sup>26</sup>) Een algemene inleiding op draadloze beveiliging is te lezen in het factsheet van GOVCERT.NL over dit onderwerp op [www.govcert.nl/download.html?f=101](http://www.govcert.nl/download.html?f=101)

<sup>27</sup>) Het onderzoek is te lezen op [dl.aircrack-ng.org/breakingwepandwpa.pdf](http://dl.aircrack-ng.org/breakingwepandwpa.pdf). Een begrijpelijke uitleg ervan is te lezen op [radajo.blogspot.com/2008/11/wpatkip-chopchop-attack.html](http://radajo.blogspot.com/2008/11/wpatkip-chopchop-attack.html) en [arstechnica.com/security/news/2008/11/wpa-cracked.ars](http://arstechnica.com/security/news/2008/11/wpa-cracked.ars)

## 3 Internetcriminaliteit en innovatie

In hoofdstuk 2 is ingegaan op een aantal in het oog springende kwetsbaarheden van het internet. In dit hoofdstuk geven we inzicht in de staat van internetcriminaliteit halverwege 2009. We doen dit aan de hand van ontwikkelingen die samenhangen met algemene ontwikkelingen op ICT-gebied en aan de hand van specifieke voorbeelden van internetcriminaliteit. We sluiten dit hoofdstuk af met een blik op de status van de veiligheid van het internet en zaken die het internet juist veiliger kunnen maken.

### 3.1 Internet is het nieuwe besturingssysteem

Meer en meer computertoepassingen verschuiven naar het web. De eerste pogingen, eind jaren '90, om computerprogramma's via het internet aan te bieden, waren niet succesvol. Computergebruikers hadden onvoldoende bandbreedte en de beschikbare internettechnologieën waren nog te beperkt. In de afgelopen vijf jaar heeft deze verschuiving alsnog vaart gekregen. Na toepassingen als e-mail zijn nu ook tekstverwerking, foto- en video-bewerking en relatiebeheer online beschikbaar.

#### 3.1.1 Cloud computing: donkere wolken boven het nieuwe walhalla

Het afgelopen jaar kreeg de verschuiving van applicaties naar het web meer momentum.

'Cloud Computing' heeft in dit kader veel aandacht gekregen: het internet als een wolk waarin allerlei diensten beschikbaar zijn, inclusief virtualisatie, rekenkracht en opslag. Deze diensten bieden groot gebruikersgemak: zelf geen software meer installeren, gegevens die altijd en overal te benaderen zijn en goede samenwerkingsmogelijkheden. Voor het geboden gemak moeten gebruikers echter ook een stuk zekerheid over hun veiligheid inleveren.

Een van de voordelen van cloud computing – gegevens die altijd en overal zijn te benaderen – is namelijk ook een risico. Als een onlinedienst een kwetsbaarheid bevat, dan kan iedereen deze via internet proberen uit te buiten. Bij een geslaagde aanval heeft een aanvaller ongeautoriseerd toegang tot gegevens en kan deze kopiëren, aanpassen of verwijderen. Maar ook zonder kwetsbaarheden is onlineinformatie niet altijd even goed beschermd. Toegang tot de informatie is meestal alleen afgeschermd met een gebruikersnaam en wachtwoord, relatief gemakkelijk te omzeilen met behulp van bijvoorbeeld een wachtwoord-resetmechanisme.

Verder schuilt een risico in de gebruiksvoorwaarden van onlinediensten. Bijna alle aanbieders houden zich het recht voor de voorwaarden eenzijdig te wijzigen. Vooral bij zakelijke toepassingen is dat een risico. Sommige voorwaarden bevatten bepalingen waarmee de dienstaanbieder een gebruikslicentie wordt verleend<sup>28</sup> op alle online geplaatste informatie. Hiermee verliest de gebruiker voor een deel de controle over wat er met zijn informatie gebeurt. Ook in de beschikbaarheid van de diensten schuilt een risico. In geval van een probleem bij de aanbieder kan een gebruiker niet bij zijn documenten, zonder dat daarvoor een alternatief is. Dienstverleners bieden soms ook betaalde versies van hun diensten aan, waarbij een hogere beschikbaarheid wordt gegarandeerd. Soms kunnen documenten lokaal gesynchroniseerd worden en offline bewerkt.

De genoemde risico's maken het gebruik van cloud computing-diensten door bedrijven of overheden op dit moment alleen in bepaalde gevallen opportuun. Wel zien we dat de

20

*“Onlinediensten bieden groot gemak, maar gebruikers geven daarvoor een stuk zekerheid over hun veiligheid op”*

<sup>28</sup>) [www.google.com/accounts/TOS?hl=nl](http://www.google.com/accounts/TOS?hl=nl)

aanbieders van cloud computing-diensten momenteel bezig zijn hun dienstverlening en beveiliging verder te professionaliseren. Dat betekent dat in de toekomst dergelijke diensten voor voornamelijk kleinere bedrijven al interessanter en veiliger kunnen zijn dan wanneer ze hiervoor zelf een computeromgeving moeten beheren.

### 3.1.2 Aanvallen verschuiven verder van besturingssysteem naar browsers

Zoals we eerder constateerden, bestaan steeds meer applicaties alleen nog in de browser en op internet (bijvoorbeeld Gmail, Google docs, Apple's MobileMe). Er vindt, kortom, een verschuiving plaats van desktopapplicaties naar webapplicaties. Google bracht een compleet nieuwe browser uit, Chrome, die gebaseerd is op het concept dat een browser kleine onafhankelijke programma's moet kunnen draaien. Webapplicaties worden namelijk steeds complexer en vragen meer van zowel de website als de browser. Toenemende complexiteit betekent vrijwel altijd ook een toename in kwetsbaarheden en aanvalsmogelijkheden. Met een browser die up-to-date is, kun je de bedreiging maar voor een deel wegnemen. Niet alleen in de browser zelf kunnen namelijk kwetsbaarheden zitten, maar ook in alle plug-ins, toolbars, scripts en andere uitbreidingen die je als eindgebruiker aan je browser kunt toevoegen. Sommige daarvan, zoals de plug-ins van Adobe voor het weergeven van PDF's of Flash, zijn zo gangbaar dat ze in vrijwel alle browsers aanwezig zijn. In deze plug-ins hebben het afgelopen jaar meerdere kwetsbaarheden gezeten die ook misbruikt zijn door aanvallers. Veilig surfen wordt hiermee een zeer complexe aangelegenheid. Het is de gezamenlijke verantwoordelijkheid van browser- en plugin-ontwikkelaars, webapplicatie-aanbieders en gebruikers om dat doel te bereiken.

### 3.1.3 De sociale kant van het net én van internetcriminelen

Nieuwe communicatietoepassingen schieten uit de grond en maken soms een stormachtige groei door. Facebook bijvoorbeeld heeft meer dan 175 miljoen actieve gebruikers. Als een toepassing eenmaal genoeg gebruikers heeft, wordt deze ook aantrekkelijk voor misbruik door internetcriminelen. Vorig jaar schreven we in ons Trendrapport al dat sociale netwerken zoals Hyves en instant messaging zoals MSN actief werden misbruikt. In het afgelopen jaar zagen we ook nepprofielen opduiken op LinkedIn, waarmee malware werd verspreid<sup>29</sup>.

De nieuwste trend op dit gebied is Twitter: de microblog waar gebruikers in berichtjes van maximaal 140 tekens laten weten wat ze aan het doen zijn. Ook Twitter werd op verschillende manieren misbruikt door cybercriminelen: via speciaal daarvoor aangemaakte profielen verspreidden ze berichtjes met links naar kwaadaardige websites<sup>30</sup>. Twitter werd ook gebruikt voor identiteitsdiefstal van sterren en zelfs president Obama, doordat anderen via hun accounts berichten plaatsten<sup>31</sup>. Recent is ook een phishing-aanval gericht op Twittergebruikers aan het licht gekomen<sup>32</sup>. Het ernstigste incident voor Twitter was de diefstal van de toegangsgegevens van een beheerder<sup>33</sup>.

Gezien het tempo waarmee internetcriminelen nieuwe succesvolle communicatiemediën en -diensten misbruiken voor hun doeleinden, kan worden gesteld dat elk succesvol online communicatiemedium (uiteindelijk) door internetcriminelen zal worden misbruikt.

*“Ieder succesvol  
online communicatiemedium  
zal uiteindelijk misbruikt  
worden door  
internetcriminelen”*

<sup>29</sup>) [www.avertlabs.com/research/blog/index.php/2009/01/06/rogue-linkedin-profiles-lead-to-malware/](http://www.avertlabs.com/research/blog/index.php/2009/01/06/rogue-linkedin-profiles-lead-to-malware/)

<sup>30</sup>) [www.f-secure.com/weblog/archives/00001633.html](http://www.f-secure.com/weblog/archives/00001633.html)

<sup>31</sup>) [blog.twitter.com/2009/01/monday-morning-madness.html](http://blog.twitter.com/2009/01/monday-morning-madness.html) en  
[www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124900](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9124900)

<sup>32</sup>) [blog.twitter.com/2009/01/gone-phishing.html](http://blog.twitter.com/2009/01/gone-phishing.html)

<sup>33</sup>) [blog.twitter.com/2009/04/unauthorized-access-update-on-security.html](http://blog.twitter.com/2009/04/unauthorized-access-update-on-security.html)

### 3.1.4 Internet gaat mobiel: altijd en overal online

Het aantal mobiele telefoons met internet stijgt nog steeds fors en ook het gebruik neemt steeds meer toe: 15% van de Nederlandse huishoudens zou inmiddels mobiel internetten<sup>34</sup> en op Europees niveau ligt dat percentage ongeveer gelijk<sup>35</sup>. Tegelijkertijd worden mobiele telefoons steeds krachtiger: het zijn kleine computers.

Hoewel de doorbraak van mobiel internet al enkele jaren wordt voorspeld, lijkt een aantal parallele ontwikkelingen nu de weg te plaveien voor echt bruikbaar mobiel internet. Zo zien we de verschuiving van applicaties naar het web, de beschikbaarheid van nieuwe mobiele platformen zoals Apple's iPhone en Google's Android en een snelle groei in nieuwe functionaliteit die specifiek voor deze platformen is gemaakt. Een gevolg hiervan is dat er miljoenen apparaten in gebruik zijn die de functionaliteit en complexiteit van computers hebben en continu met internet verbonden zijn. Hierdoor worden deze apparaten een doelwit voor internetcriminelen.

Over het algemeen heeft een mobiele internetter weinig mogelijkheden om zijn mobieltje te configureren. Het updaten en dus zo veilig mogelijk houden van software is in de meeste gevallen nog minder gemakkelijk dan bij een 'gewone' computer. Hierdoor rust er een grote verantwoordelijkheid voor een veilig mobiel internet op de schouders van softwareleveranciers en telecomproviders.

Al minstens 10 jaar wordt voorspeld dat er aanvallen zullen plaatsvinden op mobiele platformen, maar tot nu toe is dit beperkt gebleven. Een van de mogelijke redenen hiervoor is de grote diversiteit aan mobiele platformen, waardoor aanvallen meestal een beperkt bereik zullen hebben. Een andere belangrijke reden is het gebrek aan een financiële drijfveer voor criminelen. Het gebruik van mobiele platformen voor financiële dienstverlening, zoals internetbankieren en betalen, is nog beperkt. In januari is overigens in Indonesië, waar wel veel mensen betalen met behulp van hun mobiele telefoon, malware aangetroffen die mobiele platformen aanviel en daarbij geld over probeerde te maken<sup>36</sup>. Als we verder kijken naar Azië, waar mobiele telefoons al veel langer worden gebruikt als primaire computer, dan zien we dat malware ook daar nog geen groot probleem is. Spam lijkt daar momenteel het grootste probleem<sup>37</sup>.

De komende jaren verwachten wij een stijging van het aantal aanvallen op mobiele telefoons, als gevolg van de groei van mobiele toepassingen, waaronder financiële.

<sup>34</sup> [www.molblog.nl/bericht/Onderzoek-gebruik-internet-op-mobiele-telefoon-stijgt/](http://www.molblog.nl/bericht/Onderzoek-gebruik-internet-op-mobiele-telefoon-stijgt/)

<sup>35</sup> [europa.eu/rapid/pressReleasesAction.do?reference=IP/09/473&language=NL](http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/473&language=NL)

<sup>36</sup> [www.viruslist.com/en/weblog?weblogid=208187621](http://www.viruslist.com/en/weblog?weblogid=208187621)

<sup>37</sup> [whatjapanthinks.com/2009/05/14/mobile-spam-very-discomforting-for-three-in-five-japanese/](http://whatjapanthinks.com/2009/05/14/mobile-spam-very-discomforting-for-three-in-five-japanese/) en [whatjapanthinks.com/2008/05/12/cell-phone-spam-daily-plague-for-almost-one-in-three-japanese/](http://whatjapanthinks.com/2008/05/12/cell-phone-spam-daily-plague-for-almost-one-in-three-japanese/)

## 3.2 Money makes the world go around

### 3.2.1 Conficker: malware is slimmer dan ooit!

Veel malware die we de afgelopen jaren gezien hebben werd verspreid via e-mail en vooral via websites, waarbij de infectie plaatsvindt door misbruik te maken van lekken in browsers en kantoortoepassingen als Word en Excel. Conficker toonde afgelopen jaar aan dat wormen<sup>38</sup> nog steeds geen gepasseerd station zijn. Conficker is zeer actieve malware, die gebruikmaakt van verschillende geavanceerde technieken om maximaal succes te boeken. De worm werd in eerste instantie bekend omdat het misbruik maakt van een ernstige kwetsbaarheid in Windows die Microsoft in oktober 2008 had verholpen met een update (zie kader). Conficker maakt misbruik van de kwetsbaarheid door op afstand systemen te infecteren en zich zo binnen een netwerk te verspreiden. Daarnaast maakt Conficker ook gebruik van andere verspreidingsmethoden.

#### Microsoft update MS08-067: niet zomaar een update

Op donderdag 23 oktober bracht Microsoft een patch uit voor een ernstige kwetsbaarheid in alle versies van Windows. Bijzonder is dat deze patch buiten de reguliere patch-cyclus om werd uitgebracht omdat Microsoft de kwetsbaarheid als bijzonder ernstig inschatte en omdat kwaadwillenden de kwetsbaarheid al actief uitbuiten. GOVCERT.NL heeft haar deelnemers hierover direct telefonisch ingelicht.

De kwetsbaarheid bevindt zich in de 'Windows Server' service en kan worden misbruikt om op het aangevallen systeem code te laten uitvoeren met SYSTEM-rechten. Een aanvaller heeft het systeem hiermee volledig onder controle.

Misbruik vindt plaats met malafide 'Remote Procedure Calls' (RPC) over SMB (Server Message Blocks). SMB maakt het mogelijk om via het netwerk toegang te krijgen tot bestanden en printers op andere systemen. De kwetsbaarheid kan alleen misbruikt worden via de poorten 139/tcp (NetBIOS) en 445/tcp (CIFS).

Binnen twee uur na het beschikbaar komen van de Microsoft-update werd op internet al programmacode te koop aangeboden om de kwetsbaarheid te misbruiken. In de dagen daaropvolgend verschenen dergelijke programma's ook op publieke websites als Milw0rm en SecurityFocus.

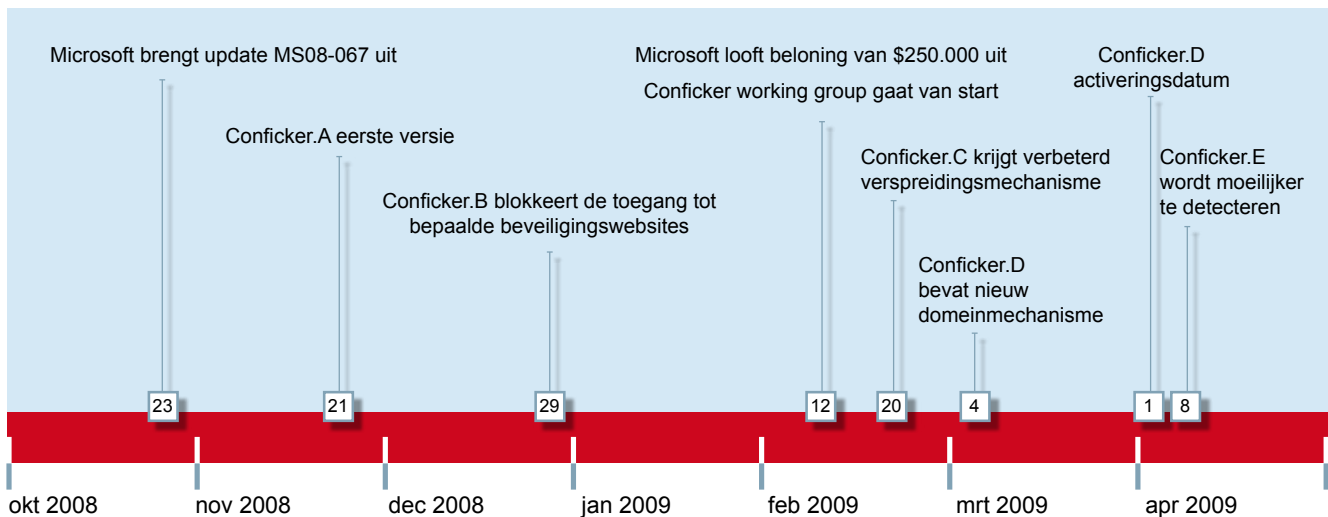
Al langer weten we dat internetcriminelen zeer actief werken aan het beschermen van hun infrastructuur. Diverse technieken als obfuscatie en fast-flux, zijn in eerdere trendrapporten van GOVCERT.NL aan bod gekomen. De mensen achter Conficker gaan hierin echter weer een stap verder. Zo wordt voor de aansturing van het botnet gebruikgemaakt van dynamische domeinnamen, waardoor het erg moeilijk is om het botnet onschadelijk te maken. Beveiligingsonderzoekers zijn er in november 2008 achter gekomen hoe Conficker de 250 verschillende domeinnamen per dag genereerde en konden hiermee voorspellen welke domeinnamen in de toekomst gebruikt zouden gaan worden. Door deze domeinen van tevoren te registreren ontstond de mogelijkheid om delen van het botnet over te nemen of onschadelijk te maken. In reactie hierop werd Conficker aangepast.

<sup>38)</sup> Traditioneel wordt de term 'worm' gebruikt voor malware die zichzelf zonder tussenkomst van de gebruiker verspreidt van computer naar computer. De term is tegenwoordig wat misleidend, omdat veel malware bestaat uit meerdere componenten en vrij simpel aangepast kan worden. Termen als virus, worm en trojan hebben hierdoor eigenlijk hun onderscheidend vermogen verloren.

De derde variant van Conficker, Conficker C, kiest elke dag uit 50 duizend verschillende domeinnamen, waarmee de tactiek van het van tevoren registreren van alle mogelijke domeinnamen op slag onhaalbaar werd. De verwachte activering van deze nieuwe variant, op 1 april 2009, genereerde een mediahype. De datum was eigenlijk alleen relevant omdat op die dag de werking van Conficker zou veranderen. Op het gebruik en het doel van Conficker – zaken die de daadwerkelijke impact bepalen – heeft dit geen invloed.

De wereldwijde samenwerking in de security community in de strijd tegen Conficker is voor een groot deel te volgen op de website van de *Conficker working group*<sup>39</sup>. Vooral deelname van organisaties als ICANN is een positieve ontwikkeling. Een dreiging als Conficker kan niet door slechts één organisatie worden aangepakt.

In een poging om de makers van de Conficker-worm te achterhalen, loofde Microsoft in februari 2009 een bedrag van \$ 250.000 uit voor informatie die zou leiden tot het arresteren en vervolgen van de makers van de worm. Tot op dit moment heeft dit nog niet tot een succesvolle vervolging geleid. De belangrijkste gebeurtenissen rondom Conficker zijn weergegeven in figuur 3-1.



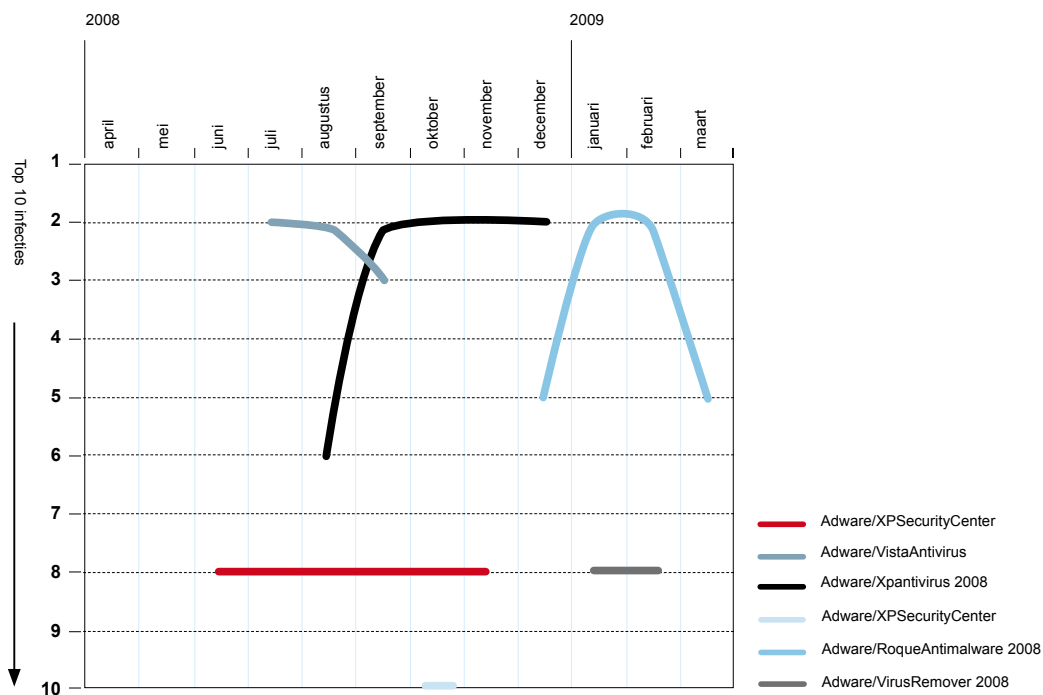
Figuur 3-1 Tijdlijn Conficker

### 3.2.2 Nep-antivirus maakt misbruik door social engineering

In 2008 hebben we een explosieve groei gezien van nep-antivirussoftware. Dit is kwaadaardige software die zich vermomt als een antivirusprogramma of antispywareprogramma. Nep-antivirus is geen nieuw fenomeen; al vanaf het jaar 2000 waren er gevallen bekend van spyware die als antispyware aangeprezen werd. In 2008 kwam het zelfs tot formele klachten en een rechterlijk bevel tegen enkele makers<sup>40</sup>. In figuur 3-2 staat een overzicht van de positie van nep-antivirusprogramma's in de top tien van malware in Nederland, zoals gevonden door de onlinedienst ActiveScan van Panda. In de grafiek is zichtbaar dat nep-antivirusprogramma's vanaf juni 2008 in de top tien verschijnen en dat verschillende nep-antivirusprogramma's elkaar in de loop van de tijd opvolgen.

<sup>39)</sup> [www.confickerworkinggroup.org](http://www.confickerworkinggroup.org)

<sup>40)</sup> [www2.ftc.gov/opa/2008/12/winssoftware.shtm](http://www2.ftc.gov/opa/2008/12/winssoftware.shtm)



Figuur 3-2. Positie van nep-antivirusprogramma's in de top 10 van malware in Nederland (bron:Panda)

In tegenstelling tot de eerdere scams is de huidige nep-antivirus niet alleen een scam waarvoor je betaalt, maar vooral een agressief soort malware. Het nepproduct maakt misbruik van de angst van internetters en buit hun beveiligingsbewustzijn uit. Uiteindelijk worden gebruikers verleid om tegen betaling malware op hun computer te installeren. Uit een computerinbraak bij een bedrijf dat nep-antivirus verspreidde, is gebleken dat er wel \$ 158.000 per week aan de verspreiding werd verdiend<sup>41</sup>. Daarom zijn er ook honderden verschillende varianten in omloop onder uiteenlopende, professioneel klinkende namen: WinFixer, WinAntivirus en XP Antivirus. Zelfs voor de Mac is er nep-antivirus in omloop!

### Hoe werkt een nep-antivirus-'aanval'?

Tijdens het internetten krijgen computergebruikers een melding dat op hun computer ongewenste software staat. Deze melding – in de vorm van een pop-up of een banner die lijkt op een echt Windows-venster – is echter onjuist en alleen bedoeld om gebruikers bang te maken en te verleiden nep-antivirussoftware te installeren. Als de gebruiker op de pop-up of banner klikt, wordt er malware geïnstalleerd.

De malware is overigens zo gemaakt dat deze in alle opzichten op echte antivirussoftware lijkt: een mooie interface, iconen in de system tray en de mogelijkheid om een scan uit te voeren van je systeem. Als de nietsvermoedende gebruiker zo'n scan laat uitvoeren, worden er uiteraard veel infecties op de computer gevonden. Infecties die er helemaal niet zijn. De nep-software meldt dan dat het gehele pakket moet worden aangeschaft om de infecties te kunnen verwijderen. Helaas gaan heel veel gebruikers hierop in.

<sup>41)</sup> [www.nytimes.com/2008/10/30/technology/internet/30virus.html?\\_r=1](http://www.nytimes.com/2008/10/30/technology/internet/30virus.html?_r=1)

### 3.2.3 Klassieke aanvallen op banken

Omdat bij een aanval in de financiële sector vaak direct financieel voordeel te behalen valt, is deze sector voor aanvallers erg aantrekkelijk. In Nederland worden er nauwelijks cijfers gepubliceerd over verliezen van onlinebankieren als gevolg van internetcriminaliteit. In Engeland publiceert APACS deze cijfers wel. Het verlies is daar in 2008, ondanks de maatregelen die daar zijn genomen om onlinebankieren beter te beveiligen, met 132% gestegen tot £ 52.5 miljoen in vergelijking met 2007<sup>42</sup>. Hierbij is een verschuiving opgemerkt van phishing-aanvallen naar aanvallen gebaseerd op malware. Bij deze aanvallen worden zowel klantcomputers als interne banksystemen aangevallen.

In Nederland zijn dit jaar voor het eerst wel de verliezen als gevolg van skimmen bekend gemaakt. In 2008 is door de Nederlandse banken € 31 miljoen verlies geleden door skimmen. Hoewel dit op het totaalbedrag van € 75 miljard bij 1,7 miljard keer pinnen een klein percentage is, laat de omvang wel zien dat het lucratief is en hoe professioneel deze criminelen zijn<sup>43</sup>.

Via interne systemen van de banken is in potentie veel meer geld te halen. Zo is in 2009 bij een gecoördineerde wereldwijde aanval op geldautomaten \$ 9 miljoen buitgemaakt. Bij deze aanval is gebruikgemaakt van gestolen gegevens uit een intern banksysteem. Wij verwachten dat er in de toekomst meer van dergelijke combinatieaanvallen zullen plaatsvinden.

#### Aanval op Heartland Payment Systems met grote gevolgen

De aanval op de interne systemen van Heartland Payment Systems was, vanwege de omvang, het meest opmerkelijke incident in de financiële sector van het afgelopen jaar. Heartland verwerkte de transacties van meer dan 250.000 bedrijven. Op 20 januari 2009 heeft dit bedrijf een inbreuk op haar systemen bekendgemaakt. In de Verenigde Staten zijn bedrijven verplicht inbreuk op informatiesystemen te melden. Heartland heeft hier zelfs een speciale website voor opgezet. Hoewel Heartland voldeed aan de beveiligingsnorm voor financiële instellingen (PCI-DSS) hebben aanvallers de gelegenheid gekregen malafide software op de systemen van Heartland te installeren, waarmee de gegevens van tientallen miljoenen actieve kaarten en kaarthouders is buitgemaakt.

## 3.3 Macht en ideologie als drijfveer

In ons vorige Trendrapport hebben we uitgebreid aandacht besteed aan gerichte aanvallen en aanvallen met een ideologische of politieke motivatie. Het afgelopen jaar zijn er meer van dergelijke aanvallen voorgekomen, waarvan we de belangrijkste hierna toelichten.

### 3.3.1 Gerichte aanvallen blijven plaatsvinden

Eind maart 2009 verschenen in de media berichten over een spionagenetwerk dat computers bespioneerd heeft in meer dan 100 landen. Het bleek te gaan om een netwerk genaamd GhostNet, vernoemd naar een van de soorten malware die gebruikt is om computers te infecteren: 'Gh0st Rat'. Het gepubliceerde onderzoek over GhostNet is uitvoerig, goed onderbouwd en geeft inzicht in digitale aanvallen die vermoedelijk vanuit China werden geregistreerd. In figuur 3-3 staat de verspreiding van de GhostNet-infecties zoals deze geconstateerd zijn door de Information Warfare Monitor.

<sup>42</sup> [www.apacs.org.uk/09\\_03\\_19.htm](http://www.apacs.org.uk/09_03_19.htm)

<sup>43</sup> [www.nvb.nl/index.php?p=290495](http://www.nvb.nl/index.php?p=290495)



Figuur 3-3 Verspreiding van GhostNet infecties (bron: Information Warfare Monitor)

### GhostNet

Via gerichte e-mails met daaraan geïnficeerde Word- en PDF-bestanden, infecteerden kwaadwillenden pc's van belangrijke personen. Hoe zo'n aanval in elkaar steekt, is beschreven in Trendrapport 2008 van GOVCERT.NL. Van geïnficeerde pc's werd informatie verzameld door documenten van de geïnficeerde systemen te kopiëren en door via webcams en microfoons gesprekken af te luisteren. De onderzoekers zijn via geïnficeerde pc's de controlservers van het botnet op het spoor gekomen. Via deze controlservers, die zich in China bevonden, hebben zij veel meer geïnficeerde pc's en de aard van de verzamelde informatie in kaart gebracht. Het botnet bestond uit ten minste 1295 geïnficeerde computers in 103 landen. Het overgrote deel van de infecties heeft plaatsgevonden in Zuid-oost Azië. Het vermoeden van de onderzoekers dat de Chinese overheid betrokken is, is gebaseerd op het feit dat de Chinese overheid op een bepaald moment een reactie gaf, klaarblijkelijk naar aanleiding van een door GhostNet onderschepte mail vanuit Tibet.

### 3.3.2 Ideologisch gedreven aanvallen (hacktivisme) blijven actueel

Na de cyberaanval vanuit Rusland op Estland op ongeveer 300 websites in april 2008 was Rusland in augustus van dat jaar opnieuw betrokken bij een cyberaanval. Ditmaal viel de aanval samen met de (fysieke) oorlog tussen Rusland en Georgië. Door de aanval waren Georgische overheids- en commerciële websites niet bereikbaar of werd de inhoud ongewenst veranderd (defacement). Georgië werd bij het afslaan van de cyberaanval geholpen door Polen en securityspecialisten van de CERT in Estland. Voor zover bekend, werd de aanval niet door de Russische overheid uitgevoerd, maar omdat zij het ook niet heeft gestopt wordt ze beschuldigd van het geven van passieve steun<sup>44</sup>.

Naast deze cyberoorlog speelde zich ook een elektronisch conflict af tussen Israël en Hamas. Aanhangers van beide kampen werd opgeroepen malware te installeren waarmee websites van de tegenstander konden worden platgelegd. In Palestina wordt dit ook wel de Elektronische Intifada genoemd<sup>45</sup>.

<sup>44)</sup> [www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report](http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report) en [ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html](http://ddanchev.blogspot.com/2008/08/whos-behind-georgia-cyber-attacks.html)

<sup>45)</sup> [latimesblogs.latimes.com/babylonbeyond/2008/10/iran-hamas-offi.html](http://latimesblogs.latimes.com/babylonbeyond/2008/10/iran-hamas-offi.html)

Naast de voornoemde twee incidenten zijn er ook andere aanvallen geweest. Uit dit type incidenten concluderen wij dat elk ideologisch conflict in de toekomst een cybercomponent zal hebben.

*“Ieder ideologisch conflict zal voortaan een cybercomponent hebben”*

In Nederland hebben we ook te maken gehad met hacktivisme. In augustus 2008 vond een mass defacement plaats, specifiek gericht op websites in Nederland. De defacements vonden plaats in reactie op de film Fitna. De homepage van naar schatting meer dan 18.000 websites werden beklad met religieus-ideologische leuzen.

### 3.4 Deanonimisatie – minder privacy

Een onderwerp dat de afgelopen jaren veelvuldig onder de aandacht is geweest, is de veranderende beleving en interpretatie van het begrip privacy. Enerzijds zien we dat internetgebruikers op vrijwillige basis veel persoonlijke informatie over zichzelf op internet plaatsen en daarmee gevoelig worden voor misbruik. Anderzijds zien we ophef over incidenten waarbij persoonlijke informatie onvrijwillig wordt prijsgegeven.

#### 3.4.1 Onvrijwillig verlies van privacy

Veel persoonlijke informatie wordt door internetcriminelen buitgemaakt of komt op andere manieren in handen van derden. Vaak gebeurt dit door het infecteren van computers van eindgebruikers met kwaadaardige software die persoonlijke gegevens achterhaalt. In 2008 is het percentage trojans dat persoonlijke gegevens probeert te achterhalen, gebaseerd op blokkades door Scansafe, gestegen van 6% naar 14%<sup>46</sup>.

Maar vaak ook komt persoonlijke informatie in handen van derden door centrale computersystemen die onvoldoende beveiligd zijn, waardoor de gegevens van de ene gebruiker in te zien zijn door een andere gebruiker. Soms is op een website, waar informatie van verschillende personen is samengebracht, het aanpassen van een volgnummer in een URL voldoende om de gegevens van een ander in te zien. Een aanvaller kan zo de persoonlijke gegevens van meerdere gebruikers achterhalen. Voorbeelden van dit soort aanvallen zijn het lekken van privacygevoelige gegevens via de website van OV-fiets<sup>47</sup> en Mijnpolitiebureau.nl<sup>48</sup>. Overigens is niet bekend of er daadwerkelijk misbruik is gemaakt van de gegevens die in deze gevallen gelekt zijn.

Een hele andere vorm van het vrijkomen van persoonlijke gegevens is als dit met opzet door derden wordt gedaan. De website stopkindersex.com is daar een voorbeeld van: op deze website werden de persoonlijke gegevens van veroordeelden van misbruik met kinderen getoond, waaronder adresgegevens en foto's. Door het hosten van de website in het buitenland werd de Nederlandse wetgeving, die dit niet toelaat, omzeild.

Voorbeelden als Google Streetview en stopkindersex geven aan dat zaken die op kleine schaal acceptabel zijn – mensen praten over een veroordeelde in hun omgeving, mensen maken foto's en delen die met anderen – door hun grote bereik en volume ineens nieuwe vragen kunnen oproepen en voor ongemak kunnen zorgen.

<sup>46</sup> [www.scansafe.com/\\_\\_\\_data/assets/pdf\\_file/11635/agtr\\_2008.pdf](http://www.scansafe.com/___data/assets/pdf_file/11635/agtr_2008.pdf)

<sup>47</sup> [webwereld.nl/nieuws/56621/ov-site-lekt-privacygevoelige-data.html](http://webwereld.nl/nieuws/56621/ov-site-lekt-privacygevoelige-data.html)

<sup>48</sup> [www.security.nl/artikel/28096/Politie\\_dicht\\_lekken\\_flitsfoto](http://www.security.nl/artikel/28096/Politie_dicht_lekken_flitsfoto)

## Google Streetview

Google Streetview is een aanvulling op Google Maps. Voor Google Streetview worden overal ter wereld vanaf een rijdende auto met '360-graden camera's' grote aantallen foto's gemaakt op straat, inclusief omgeving en toevallige passanten. De meeste foto's zijn onschuldig, maar er zijn ook privacygevoelige beelden: een man die net een seksshop verlaat en iemand die wordt gearresteerd. Voor publicatie worden de foto's bewerkt zodat gezichten onherkenbaar zijn en Google reageert wel snel op meldingen en verwijdert de foto's – inmiddels al enkele honderden – maar is blijkbaar niet in staat om privacyschendingen te voorkomen. In Engeland is de auto van Google die de opnames maakt al uit het dorp Broughton geweerd. De bewoners willen niet dat zij of hun eigendommen worden gefotografeerd. De belangengroep Privacy International heeft stappen ondernomen om Google StreetView van internet te halen.

### 3.4.2 Vrijwillig verlies van privacy

Naast het zonder toestemming gebruiken van informatie van anderen, plaatsen mensen zelf ook steeds meer informatie online. Jongeren – trots op wat ze doen en schijnbaar zonder schaamte – worden ook wel de 'Say everything'-generatie<sup>49</sup> genoemd. Ze plaatsen van alles online over zichzelf en anderen; van telefoonnummers tot dagboeken en zelfs hun eigen blootfoto's. Het vervelende voor hen is dat het internet eigenlijk niks vergeet en dat kan, tot zelfs jaren later, ongewenste gevolgen hebben. Ouders spelen een belangrijke rol in het bewustmaken van hun kinderen van dergelijke risico's. Ze worden hierbij geholpen door websites als Mijn Kind Online<sup>50</sup>, Digivaardig & Digibewust<sup>51</sup> en Waarschuwingsdienst.nl.

Zelfs als je zelf voorzichtig bent met het plaatsen van persoonlijke informatie op internet door beperkt informatie te delen en op verschillende sociale netwerken verschillende identiteiten aan te nemen, kan deze informatie aan elkaar gekoppeld worden<sup>52</sup>. Dit koppelen kan bijvoorbeeld op basis van foto's, metagegevens uit de foto's, relaties of taalgebruik en gaat dus veel verder dan het simpelweg koppelen van e-mailadressen of gebruikersnamen. Foto's kunnen ook informatie geven over waar iemand zich bevindt. Het zijn forensische technieken die gebruikt worden om misdrijven op te lossen, maar die ook door kwaadwillenden gebruikt kunnen worden als informatiebron bij social engineering.

Aanvallers maken ook gebruik van het gedeeltelijk overlappen van sociale netwerken door zich als iemand voor te doen die in het ene netwerk wel aanwezig is en in het andere niet. Omdat het netwerk en de relaties hun vertrouwen biedt, is dit een mooie uitvalsbasis voor social engineeringaanvallen.

Gebruikers realiseren zich vaak ook niet dat de organisaties achter de sociale netwerken ook informatie verzamelen over het netwerkgedrag van een gebruiker: hoe vaak en hoe lang ben je online, met wie ben je verbonden, hoe vaak en met wie wissel je berichten uit, en waarover? Waarvoor deze informatie gebruikt wordt, is vaak alleen summier terug te vinden in gebruikersvoorwaarden of privacybeleid.

Al deze ontwikkelingen kunnen leiden tot een snel verminderende privacy waarbij de gemiddelde internetgebruiker weinig besef heeft van de risico's die kleven aan het deelnemen aan

<sup>49</sup> [nymag.com/news/features/27341/](http://nymag.com/news/features/27341/)

<sup>50</sup> [www.ouders.nl/](http://www.ouders.nl/) en [www.mijnkindonline.nl/](http://www.mijnkindonline.nl/)

<sup>51</sup> [www.digivaardigdigibewust.nl/](http://www.digivaardigdigibewust.nl/) en [www.watchyourspace.nl/](http://www.watchyourspace.nl/)

<sup>52</sup> [www.cs.utexas.edu/~shmat/shmat\\_oak09.pdf](http://www.cs.utexas.edu/~shmat/shmat_oak09.pdf)

sociale netwerken. Vooral door identiteitsdiefstal/fraude zijn de gevaren groot wanneer men onbezonnen met deze nieuwe mogelijkheden omgaat.

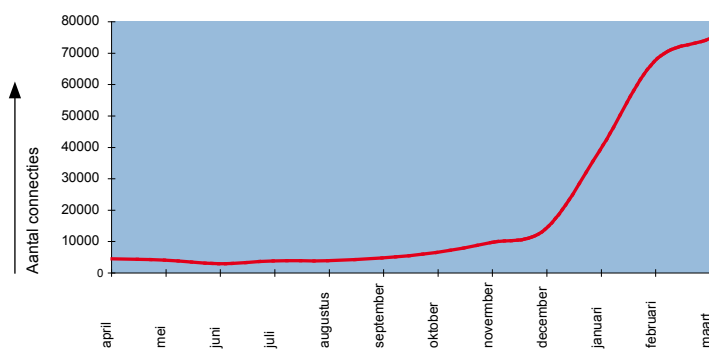
### 3.5 De status van internetveiligheid

Internetveiligheid is een zeer complex onderwerp dat niet beperkt is tot de landsgrenzen. Wereldwijd spelen veel publieke en private partijen een rol op dit vlak. Deze complexiteit maakt het erg moeilijk om 'internetveiligheid' te meten. Bepalen welke indicatoren je wilt gebruiken voor internetveiligheid is een lastige taak. Nog lastiger is het daarna verzamelen en aggregeren van de gegevens, die vaak over veel partijen verspreid zijn.

#### 3.5.1 Kwaadaardig netwerkverkeer

Een voorbeeld hiervan is de mate waarin computers van eindgebruikers in Nederland besmet zijn. Nederlandse ISP's kunnen hier inzicht in verschaffen, maar een andere manier is om te kijken naar de hoeveelheid kwaadaardig netwerkverkeer dat in andere netwerken gesignaleerd wordt met als herkomst Nederland. ShadowServer is een partij die dergelijke informatie bijhoudt voor honderden netwerken wereldwijd.

In figuur 3-4 is een analyse te zien van een van de sets gegevens van ShadowServer, namelijk die van gesignaleerd netwerkverkeer van besmette IP-adressen in Nederland. Het blijkt dat het door ShadowServer waargenomen verkeer vanaf besmette IP-adressen in Nederland in het afgelopen jaar sterk is gestegen. Bij een dergelijke grafiek hoort een nuance: Shadow-



Server aggregereert gegevens uit honderden netwerken, maar dekt daarmee maar een beperkt deel van het internet af. Als deze gegevens naast die van een andere partij gelegd zouden worden, is de overlap waarschijnlijk erg klein. Een dergelijke grafiek geeft dus geen compleet beeld.

Figuur 3-4 Aantal infecties in Nederland (bron: ShadowServer)

Omgekeerd zien wij in Nederland uiteraard ook kwaadaardig verkeer uit het buitenland. In de tabel 'Meest voorkomende landen' is de top tien te zien van landen waaruit het monitoringsysteem van GOVCERT.NL het meeste kwaadaardige verkeer te verwerken heeft gekregen.

#### Meest voorkomende landen

Unieke IP-adressen

Duitsland	13824
Rusland	12715
Verenigde Staten	11788
Zuid-Korea	5766
Taiwan	5721
Japan	5635
China	5501
Verenigd Koninkrijk	5310
Italië	5153
Brazilië	5047

#### 3.5.2 De kwetsbaarheid van software

Kwaadaardig netwerkverkeer zoals beschreven in de vorige paragraaf ontstaat natuurlijk niet zomaar. Hiervoor moet een computer besmet zijn en om dat te bereiken maken internetcriminelen gebruik van social engineering, maar ook van lekken in software. We beschreven hierboven al de manier waarop de Conficker-worm misbruik maakt van lekken in Windows en dat browsers ook nog steeds zeer gewilde doelwitten zijn.

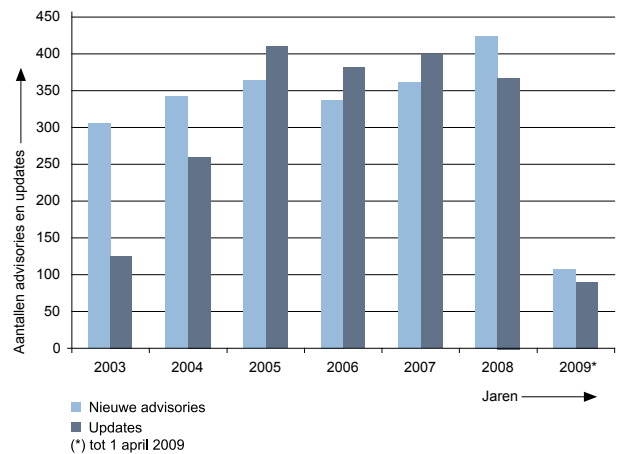
De omvang van dit probleem van kwetsbare software is behoorlijk. Een van de diensten die GOVCERT.NL aan haar deelnemers levert, is advies over nieuwe en bestaande kwetsbaarheden in software. GOVCERT.NL licht haar deel-

nemers in over nieuwe kwetsbaarheden en biedt bij elke kwetsbaarheid een korte analyse van de technische impact. In figuur 3-5 is bijvoorbeeld te zien dat GOVCERT.NL al zes jaar lang ruim 300 nieuwe advisories per jaar heeft verstuurd aan haar deelnemers. Elke advisory heeft voor de ontvangende deelnemer consequenties: er moet een risico-inschatting worden gemaakt, tests worden uitgevoerd en de patch moet worden geïnstalleerd. Afhankelijk van het systeem handmatig of automatisch, enkele malen of honderden keren. Dit kost veel tijd en veel geld.

Voor thuisgebruikers is de situatie niet veel beter. Door de grote verscheidenheid aan programma's die de meeste mensen op hun computer hebben staan is het up-to-date houden ervan een behoorlijke klus. Op pagina 42 is in de figuur te zien dat GOVCERT.NL via Waarschuwingsdienst.nl een behoorlijk aantal waarschuwingen publiceert voor nieuwe kwetsbaarheden in de meest gebruikte consumentproducten.

Leveranciers van IT-producten hebben zich traditioneel nooit veel zorgen hoeven te maken over de kwaliteit van hun producten in relatie tot informatiebeveiliging. Aansprakelijkheid voor fouten in een geleverd product wordt gewoonlijk uitgesloten in het End User License Agreement (EULA), het contract tussen de leverancier en de gebruiker. De Europese Commissie heeft een 'digitale agenda' opgesteld voor de consumentenrechten van morgen<sup>53</sup>. Licentieverlening moet de consument dan dezelfde basisrechten garanderen als wanneer hij een product koopt. Gelukkig maken sommige softwareleveranciers beveiliging meer en meer een integraal onderdeel van hun ontwikkelcyclus.

De snelheid waarmee gebruikers software up-to-date houden, is een interessant onderzoek. Dit kan veel softwareproducten helpen veiliger te worden<sup>54</sup>. Op basis van grote hoeveelheden data die bij Google zijn verzameld, is gekeken naar verschillende populaire browsers. De manieren waarop deze browsers bijgewerkt worden, lopen uiteen van het downloaden en installeren van updates door de gebruiker van de website van producenten tot volledig automatisch zonder enige gebruikerinteractie. Uit het onderzoek blijkt dat volledig automatisch bijgewerkte software veel meer up-to-date is: 97% na 3 weken. Updates waarbij de gebruiker zelf initiatief moet ondernemen, werden in slechts 24% van de gevallen geïnstalleerd in dezelfde periode. Als softwareproducenten dit onderzoek serieus nemen en toepassen kan dit leiden tot een snelle verbetering in de kwetsbaarheid van software, met name bij thuisgebruikers. In het bedrijfsleven, en vooral in technische installaties, blijft patchen een dure en soms risicovolle aangelegenheid.



Figuur 3-5 Aantal advisories en updates van GOVCERT.NL

<sup>53</sup> [europa.eu/rapid/pressReleasesAction.do?reference=IP/09/702&format=HTML&aged=0&language=NL&guiLanguage=en](http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/702&format=HTML&aged=0&language=NL&guiLanguage=en)

<sup>54</sup> [www.techzoom.net/publications/silent-updates/](http://www.techzoom.net/publications/silent-updates/)

## 4 Incident response, toezicht en opsporing

De kwetsbaarheden en aanvalsmethoden die we in de voorgaande hoofdstukken hebben beschreven, onderstrepen het belang van het onderwerp internetveiligheid. Aan dit onderwerp zit niet alleen een preventieve kant in de vorm van veilige software, veilig gebruik en veilig gedrag. Er zit ook een repressieve kant aan, die onder andere bestaat uit het oplossen van incidenten en het opsporen en vervolgen van daders.

In dit hoofdstuk belichten we een aantal ontwikkelingen die zich op het repressieve vlak hebben voorgedaan in het afgelopen jaar. Zo hebben we enkele opvallende successen gezien in de opsporing, vervolging en berechting van internetcriminelen, maar zien we ook verhoogde activiteit van partijen als registries en zelfs de Internet Corporation for Assigned Names and Numbers (ICANN), die in het verleden meestal geen actieve rol speelden bij het bestrijden van internetcriminaliteit.

In de meeste gevallen zijn de successen voor een belangrijk deel te danken aan goede internationale samenwerking tussen verschillende organisaties. Ook extra aandacht in de vorm van opleidingen, zoals dat nu gebeurt in Nederland bij politie en justitie, is van belang<sup>55</sup>. Het grenzeloze en anonieme karakter van internet maakt deze intensieve internationale samenwerking tot een absolute noodzaak. Door de samenwerking is de internetcriminaliteit een eerste slag toegebracht. Hiermee is een stap in de goede richting gezet in het bestrijden ervan.

*“Het grenzeloze en anonieme karakter van internet maakt intensieve internationale samenwerking tot een absolute noodzaak”*

Alvorens dieper op een aantal ontwikkelingen in te gaan, lichten we twee opvallende zaken aangaande computervredebreuk uit het afgelopen jaar toe. Deze hebben betrekking op journalisten die zich ongeautoriseerd toegang verleenden tot informatie uit mailboxen. Een journalist van Revu kreeg toegang tot de gegevens uit de privé-mailbox van staatssecretaris van Defensie, De Vries. Hij beroept zich hierbij op landsbelang. Een journalist mag echter geen strafbare feiten plegen, ook niet om aan te tonen dat er sprake is van een misstand<sup>56</sup>. Een journalist van Voetbal International kreeg toegang tot de gegevens uit de mailbox van ex-voorzitter van Ajax, John Jaakke. Voetbal International heeft afstand genomen van de actie van de journalist en hem op non-actief gezet<sup>57</sup>. De journalist is ook vervolgd en heeft inmiddels een taakstraf gekregen<sup>58</sup>.

De voorbeelden die we in dit hoofdstuk aanhalen zullen eerst ingaan op een van de gereedschappen van internetcriminelen: botnets. Daarna zullen we aandacht besteden aan twee uitingsvormen: phishing en spam.

<sup>55</sup> [www.om.nl/actueel/toespraken/@149577/procureur-generaal\\_3/](http://www.om.nl/actueel/toespraken/@149577/procureur-generaal_3/)

<sup>56</sup> [blog.iusmentis.com/2008/12/19/de-journalistieke-hack-van-revu/](http://blog.iusmentis.com/2008/12/19/de-journalistieke-hack-van-revu/)

<sup>57</sup> [headlines.nos.nl/forum.php/list\\_messages/11987](http://headlines.nos.nl/forum.php/list_messages/11987)

<sup>58</sup> [www.parool.nl/parool/nl/13/AJAX/article/detail/246576/2009/06/05/Ajaxhacker-krijgt-taakstraf.dhtml](http://www.parool.nl/parool/nl/13/AJAX/article/detail/246576/2009/06/05/Ajaxhacker-krijgt-taakstraf.dhtml)

## 4.1 Botnets

Botnets fungeren als infrastructuur voor veel vormen van internetcriminaliteit. Dat is dan ook de reden dat internetcriminelen er hard aan werken om ze te beschermen. We hebben dit in hoofdstuk 3 toegelicht aan de hand van Conficker. Om dezelfde reden hebben botnets ook de speciale aandacht van CERT's, opsporingsdiensten en internet serviceproviders (ISP's). Er wordt intensief informatie gedeeld over haarden van besmetting en *Command and Control* (C&C) servers<sup>59</sup>. In het ideale geval worden C&C-servers onschadelijk gemaakt en eindgebruikers door hun ISP ingelicht.

Het is lastig om de mensen achter de botnets te pakken te krijgen, maar dankzij intensievere internationale samenwerking tussen opsporingsdiensten komt hierin verbetering. Een goed voorbeeld is de succesvolle samenwerking van het Team High Tech Crime (onderdeel van het KLPD) en de FBI in de zomer van 2008, met als resultaat de aanhouding van twee verdachten in de zaak van het 'Sneker botnet'. Wereldwijd maakten ongeveer 100.000 computers onderdeel uit van dit botnet, waarvan ongeveer 1100 in Nederland. Toen de beheerder uit Sneek het botnet met behulp van een Braziliaanse tussenpersoon wilde verkopen, is hij opgepakt. Hij zal in Nederland worden vervolgd voor computervredebreuk<sup>60</sup>. De Braziliaan is aangeklaagd in New Orleans en wacht een gevangenisstraf van maximaal 5 jaar en een geldboete van minimaal \$ 250.000<sup>61</sup>. Bijzonder in deze zaak was dat gebruikers van besmette computers een bericht ontvingen van het KLPD met instructies hoe de besmetting ongedaan te maken en hoe aangifte te doen, iets wat wereldwijd nog nooit gedaan was<sup>62</sup>.

### 4.1.1 Spamproviders aangepakt

Dat het aanpakken van botnets zeker effect heeft, werd duidelijk in november 2008 toen de Amerikaanse webhoster McColo door zijn upstream providers werd afgesloten van internet, iets dat drie maanden eerder ook gebeurde met netwerkprovider Atrivo<sup>63</sup>. McColo was ISP voor veel spammers en het spamvolume daalde hierdoor wereldwijd tijdelijk met 75%! McColo werd beschuldigd van het bieden van de gelegenheid voor het ontplooiën van criminele activiteiten<sup>64</sup>. Het afsluiten van een provider om deze reden was nog nooit eerder gebeurd. Via McColo werden botnets aangestuurd die verantwoordelijk waren voor het versturen van grote hoeveelheden spam. Door deze sluiting zijn het Szribi en Rustock botnet (tijdelijk) zonder aansturing geweest. Enige tijd later werd het netwerk van McColo weer aangesloten op internet, ditmaal via een upstream provider in Zweden<sup>65</sup>. Dit duurde slechts enkele uren, maar dit was lang genoeg voor internetcriminelen om delen van de botnets weer onder controle te krijgen.

## 4.2 Phishing

Een andere, bekendere, vorm van internetcriminaliteit is phishing. Al sinds februari 2006 werkt GOVCERT.NL met Nederlandse banken samen bij het bestrijden van phishing, daar waar private initiatieven geen resultaat leveren. Bij de Notice and Take Down (NTD)-dienst worden, na een melding van een bank, de webserver van de internetcriminelen door GOVCERT.NL opgespoord en wordt ervoor gezorgd dat phishing-sites uit de lucht worden gehaald. Hierbij wordt internationaal samengewerkt met CERT's en ISP's.

<sup>59</sup> Bij 'traditionele' botnets worden de bots aangestuurd door middel van een centrale computer, die ook wel Command and Control server wordt genoemd.

<sup>60</sup> [www.om.nl/@148582/19-jarige\\_hacker/](http://www.om.nl/@148582/19-jarige_hacker/)

<sup>61</sup> [www.usdoj.gov/opa/pr/2008/August/08-crm-739.html](http://www.usdoj.gov/opa/pr/2008/August/08-crm-739.html)

<sup>62</sup> [www.om.nl/@148583/klpd\\_informeert/](http://www.om.nl/@148583/klpd_informeert/)

<sup>63</sup> [asert.arboretworks.com/2008/08/atrivointercage-called-out-as-us-rbn/](http://asert.arboretworks.com/2008/08/atrivointercage-called-out-as-us-rbn/)

<sup>64</sup> [www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658_pf.html)

<sup>65</sup> [arstechnica.com/security/news/2008/11/mccolo-reconnect-highlights-network-security-gap.ars](http://arstechnica.com/security/news/2008/11/mccolo-reconnect-highlights-network-security-gap.ars)



Een andere in het oog springende zaak is de veroordeling van een phisher, in mei 2009, in het kader van phishingaanvallen op enkele Amerikaanse bedrijven<sup>68</sup>. Een Roemeen, een van 38 aangeklaagden, was eind 2007 door Roemenië uitgeleverd aan de Verenigde Staten waar hij nu veroordeeld is tot 50 maanden gevangenisstraf.

### 4.3 Spam

Spam is voor de meeste computergebruikers waarschijnlijk het meest zichtbare 'probleem'. Elk medium wordt vroeg of laat ontdekt door spammers, zoals e-mail, SMS, MSN en Twitter. Kwalitatief goede spamfilters helpen het probleem hanteerbaar te houden, maar ook het installeren en beheren van een spamfilter kost tijd en geld. Het versturen van spam is inmiddels in veel landen, waaronder Nederland, verboden. Spam sturen aan natuurlijke personen is in Nederland al vijf jaar verboden. OPTA houdt daar vanaf 2004 toezicht op. Het versturen van spam vanuit Nederland is sinds die tijd met 85% afgenomen. Vanaf 1 oktober 2009 is ook het versturen van spam aan bedrijven verboden<sup>69</sup>.

*“Het versturen van spam vanuit Nederland is sinds 2004 met 85% afgenomen”*

Toezicht op de naleving van het spamverbod is in Nederland de verantwoordelijkheid van OPTA. OPTA werkt hiervoor intensief samen met andere partijen, zowel nationaal als internationaal. Via het meldpunt spamklacht.nl heeft OPTA in 2008 ruim 12.000 klachten over spam ontvangen, ten opzichte van 19.000 in het jaar ervoor<sup>70</sup>.

Om spam aan te pakken kan OPTA waarschuwingen geven en boetes opleggen. In april 2008 heeft OPTA een boete van 510.000 euro opgelegd voor het versturen van spam nadat eerder een waarschuwing was gegeven<sup>71</sup>. Later in 2008 is ook nog een boete van 10.000 euro opgelegd voor het versturen van spam via SMS<sup>72</sup> en een boete van ruim 100.000 euro voor het plaatsen van software die ad- en malware verspreiden op computers van eindgebruikers<sup>73</sup>.

Deze boetes vallen in het niet bij de enorme boetes die in Amerika worden opgelegd. Facebook kreeg in november 2008 een schadevergoeding van \$ 873 miljoen toegewezen in de zaak tegen het bedrijf Atlantis Blue Capital dat spam had verstuurd naar Facebook-gebruikers<sup>74</sup>. Deze boete was weer meer dan de \$ 234 miljoen die een half jaar eerder aan MySpace was toegewezen. Van deze bedragen zal overigens naar alle waarschijnlijkheid maar een klein deel betaald kunnen worden, ondanks dat spam versturen een lucratieve bezigheid is.

Naast het uitdelen van boetes wordt er ook op andere fronten tegen spam gevochten. Spam wordt veelal verstuurd door bots in botnets, en voor de verkoop van producten zijn ook websites nodig. De bijbehorende domeinen moeten uiteindelijk ergens geregistreerd zijn en door het aanpakken van deze domeinen kan spam ook effectief worden tegengewerkt. De botnets, de geregistreerde domeinen en de gehoste websites zijn allemaal punten in de keten waarop spam kan worden aangepakt.

<sup>68</sup>) [www.usdoj.gov/usao/ct/Press2009/20090330-2.html](http://www.usdoj.gov/usao/ct/Press2009/20090330-2.html)

<sup>69</sup>) [www.spamklacht.nl/asp/nieuws/id/57](http://www.spamklacht.nl/asp/nieuws/id/57)

<sup>70</sup>) [www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2926](http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2926)

<sup>71</sup>) [www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2584](http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2584)

<sup>72</sup>) [www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2743](http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2743)

<sup>73</sup>) [www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2776](http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2776)

<sup>74</sup>) [blog.facebook.com/blog.php?post=40218392130](http://blog.facebook.com/blog.php?post=40218392130)

#### 4.3.1 De rol van registries

De betrokkenheid van registries bij het bestrijden van internetcriminaliteit heeft in het verleden nog wel eens te wensen overgelaten, maar dat is iets dat nu lijkt te veranderen. Naast de in hoofdstuk 3 genoemde Conficker Working Group, waaraan ICANN deelneemt, zijn er ook andere positieve ontwikkelingen op dit vlak.

In oktober 2008 besloot ICANN om de organisatie EstDomains te deaccrediteren. EstDomains was een organisatie waarvan eerder in de media bekend was gemaakt dat zij de registrar waren voor ruim een kwart miljoen domeinen, waarvan tienduizenden gebruikt werden voor het versturen spam en het verspreiden van malware<sup>75</sup>. Een waarschuwing gevolgd door daadwerkelijke deaccreditatie, is een zwaar middel dat nu wordt ingezet. In andere gevallen hebben registrars, na een waarschuwing van ICANN, actie ondernomen om de situatie op de door hen geregistreerde domeinen te verbeteren.

Uit een rapportage van project Knuj0n uit februari 2009 blijkt dat meer dan 83% van de illegale activiteiten plaatsvinden op domeinen van maar een tiental registrars<sup>76</sup>. Hoogstwaarschijnlijk is dit omdat domeinen bij deze registrars relatief veilig zijn tegen verzoeken van buitenaf om malafide domeinen op te heffen. Deaccreditatie van deze registrars kan een goed middel zijn om de situatie te verbeteren, maar kan ook ongewenste bijeffecten hebben. Als er geen digitale 'vrijplaatsen' meer zijn waar spammers hun domeinen in bulk kunnen registreren, is de verwachting dat ze hun domeinen zullen verspreiden over veel verschillende registrars. Hierdoor wordt het weer complexer om het probleem aan te pakken.

<sup>75</sup>) Onderzoek van de Washington Post: [voices.washingtonpost.com/securityfix/2008/09/estdomains.html](http://voices.washingtonpost.com/securityfix/2008/09/estdomains.html) en [voices.washingtonpost.com/securityfix/2008/09/estdomains\\_a\\_sordid\\_history\\_an.html](http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html)

<sup>76</sup>) [www.knujon.com/registrars/](http://www.knujon.com/registrars/)

## 5 Aanbevelingen

Aan het begin van dit Trendrapport hebben wij de belangrijkste trends genoemd op het gebied van cybercrime en ICT-dreigingen. Deze trends hebben wij in de voorgaande hoofdstukken voorzien van verdieping en onderbouwing. We kunnen het echter niet houden bij signaleren alleen. GOVCERT.NL doet de volgende aanbevelingen.

### 5.1 Basismaatregelen blijven belangrijk

Het beeld dat zich in dit Trendrapport vormt, is dat de ontwikkelingen in cybercrime voor een deel voortbouwen op eerdere ontwikkelingen. De basismaatregelen die eindgebruikers en beheerders moeten treffen om zichzelf en hun omgeving te beschermen tegen cybercrime zijn dan ook niet substantieel veranderd. In het Trendrapport dat GOVCERT.NL in 2008 uitgaf, hebben wij deze basismaatregelen uitgebreid beschreven. In essentie komen deze neer op het volgende:

#### **Basismaatregelen voor eindgebruikers**

- Zorg ervoor dat het besturingssysteem, programma's en ook uw netwerkapparatuur (zoals routers) up-to-date zijn.
- Gebruik een up-to-date virusscanner en een personal firewall.
- Wees u bewust van online risico's en vraag uzelf altijd kritisch af of e-mails, hyperlinks of websites wel betrouwbaar zijn.
- Zorg ervoor dat u op de hoogte bent van dreigingen en updates, bijvoorbeeld via de Waarschuwingsdienst.nl.

#### **Basismaatregelen voor beheerders**

- Beveilig de computers van eindgebruikers door goede updatemechanismen.
- Zorg voor netwerkbeveiliging via ten minste een firewall en een (e-mail)virusscanner.
- Informeer gebruikers over risico's, train ze en geef ze de juiste hulpmiddelen.
- Bewaak de beveiliging van de website van uw organisatie, want deze is een gewilde prooi voor internetcriminelen om te bekladden (defacement) of om malware mee te verspreiden. Let op kwetsbaarheden, monitor ongeautoriseerde wijzigingen en bescherm de methoden waarmee de site geupdate wordt.
- Wees alert op dreigingen van binnenuit.

### 5.2 Specifieke aanbevelingen naar aanleiding van trends

In deze paragraaf staan een aantal specifieke aanbevelingen naar aanleiding van de gesignaleerde trends.

#### **Cryptografie periodiek evalueren**

Voor diensten die gebruikmaken van cryptografie moet periodiek geëvalueerd worden of deze nog voldoet voor die dienst. Hierbij dient bij voorkeur van gestandaardiseerde algoritmen gebruikgemaakt te worden. Organisaties moeten deze evaluatie in hun procedures opnemen en de verantwoordelijkheid beleggen binnen de organisatie. Indien MD5 nog wordt gebruikt: faseer het gebruik van MD5 op korte termijn uit.

#### **Voer DNSSEC in voor een veiliger internet infrastructuur**

Om kwetsbaarheden van DNS te ondervangen, moet ook vanuit de overheid meer aandacht komen voor een snelle invoering van DNSSEC. Met de invoering van DNSSEC wordt een veiliger infrastructuur van internet gerealiseerd. De Nederlandse overheid zou het voorbeeld van andere landen kunnen volgen om een deadline te stellen aan de invoering van DNSSEC voor domeinen van de overheid.

### **Automatisch patchen werkt beter**

Softwareleveranciers moeten ervoor zorgen dat eindgebruikers met zo min mogelijk moeite hun software kunnen voorzien van beveiligingsupdates. Automatisch updaten zorgt voor minder kwetsbare software. Dit geldt voor de traditionele besturingssystemen en zeker ook voor mobiele platformen!

### **Veilig ontwikkelen is de sleutel naar veilige producten**

Om de kwetsbaarheden in software te verminderen zouden organisaties meer aandacht moeten besteden aan een veilige ontwikkelcyclus. Hieronder vallen onder meer opleidingen voor ontwikkelaars voor veilig ontwikkelen, tools en reviews die code op kwetsbaarheden toetsen en geautomatiseerde regressietesten.

### **Samenwerking loont**

Door intensief samen te werken, informatie te delen en voorbereid te zijn op nieuwe incidenten – onder meer door afspraken te maken en regelmatig te oefenen – kunnen de gevolgen van aanvallen in de toekomst worden beperkt.

### **Blijf werken aan bewustwording**

De overheid en marktpartijen vervullen een belangrijke rol in het blijvend informeren van eindgebruikers over risico's. Er moet terugkerende aandacht voor zijn. Bewustwordingscampagnes binnen bedrijven moeten bij voorkeur de koppeling maken met het gedrag van mensen thuis. Gebruikers moeten sneller proactief op de hoogte worden gesteld van actuele dreigingen en de maatregelen die zij hiertegen kunnen nemen.

### **Bescherm privacy op internet**

Het is van groot belang dat vooral jonge gebruikers leren wat de risico's zijn van het gebruik van sociale netwerken. Campagnes die gericht zijn op zowel kinderen, ouderen als leraren kunnen hieraan bijdragen. Aanbieders van sociale netwerken zullen jongeren moeten beschermen in hetgeen zij publiekelijk over zichzelf kunnen delen. Ook binnen organisaties moet meer aandacht komen voor de risico's van sociale netwerken.

### **Webdiensten dienen adequaat beveiligd te worden**

Aanbieders van webdiensten moeten hun diensten adequaat beveiligen, de beveiliging monitoren en snel reageren wanneer er kwetsbaarheden worden ontdekt. Dit geldt ook voor het digitaal beschikbaar stellen van dossiers op internet. Eindgebruikers moeten zelf zorgen dat ze in een veilige omgeving werken en de aanbieders kunnen daar nog meer de aandacht op vestigen en handreikingen doen.

# Woordenlijst

## Android

Een open source besturingssysteem ontworpen door Google. Android is voornamelijk ontworpen voor mobiele telefoons.

## Autonomous System (AS)

De naam voor een netwerk dat deel uitmaakt van het internet en dat intern een eigen routeringsbeleid heeft.

## 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 netwerk-routes 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 door een persoon centraal bestuurd kunnen worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit.

## Command and Control server (C&C)

Vaak worden bots in een botnet aangestuurd door een centrale computer die ook wel Command and Control server wordt genoemd.

## Cache poisoning

Cache poisoning is de benaming voor een bepaald type aanval op een DNS-server, waarvoor de lokale opslag (de 'cache') van een DNS-server met opzet wordt vervuild (vergiftigd) met onjuiste gegevens. Een dergelijke aanval wordt gebruikt om mensen naar kwaadaardige websites te leiden.

## 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.

## Certificate Authority (CA)

Een certificate authority is een entiteit die de bevoegdheid heeft om digitale certificaten te verlenen. Een certificate authority heeft alleen autoriteit binnen de PKI waarin hij opereert. Zo is het goed mogelijk om binnen een bedrijf een eigen PKI op te zetten met een eigen CA.

## Chief Information Officer (CIO)

De Chief Information Officer is de Engelse benaming van de positie die in het Nederlands wel hoofd informatisering of hoofd informatietechnologie heet.

## Cloud computing

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

## Conficker

Een recente malware die ook wel 'Downadup' of 'Kiddo' wordt genoemd. Hij maakt misbruik van een kwetsbaarheid in Windows waarvoor op 15 oktober 2008 een patch is uitgebracht door Microsoft.

## 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.

## 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'.

## 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.

## DNS amplification

DNS amplification (versterking) is de benaming van een type DoS-aanval waarbij gebruik wordt gemaakt van DNS-servers. De aanval is erop gebaseerd dat een DNS-server soms een zeer groot antwoord kan geven op een kleine DNS-vraag.

## EULA (End-User License Agreement)

Overeenkomst tussen een eindgebruiker en de softwareproducent.

## Fast-flux

Een DNS-techniek die gebruikt wordt door botnets, die bedoeld is om systemen (bijvoorbeeld de Command and Control server) te beschermen tegen uitschakeling.

## Hacktivism

Ideologisch gemotiveerde hack-activiteiten, vaak in georganiseerd verband.

## Hash

Een hash is een verkorte tekenreeks die berekend is op basis van een set gegevens. Hoewel een hash in theorie geen unieke waarde is, zijn hashfuncties zo ontworpen dat hashes in de praktijk kunnen worden gebruikt om gegevens uniek mee te duiden.

## IP-spoofing

Spoofen betekent 'je voordoen als een ander', meestal in kwaadaardige zin. Bij IP-spoofing wordt het IP-adres van een andere computer gebruikt, hetzij om de herkomst van netwerkverkeer te maskeren, hetzij om de computer zich daadwerkelijk als een andere computer voor te laten doen.

### **Internet Service Provider (ISP)**

Leverancier van internetdiensten, vaak simpelweg aangeduid als 'provider'. De geleverde diensten kunnen zowel betrekking hebben op de internetverbinding zelf als diensten die men op het internet kan gebruiken.

### **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.

### **Man-in-the-middle-aanval**

Aanval waarbij de aanvaller zich tussen twee partijen bevindt, bijvoorbeeld een internetwinkel en een klant. Hierbij doet de aanvaller zich richting de klant voor als de winkel en andersom. Als tussenpersoon kan de aanvaller uitgewisselde gegevens afluisteren en/of manipuleren.

### **MD5**

MD5 (Message Digest Algorithm 5) is een verouderde 128-bit cryptografische hashfunctie.

### **Mifare-chip**

De Mifare Classic is een chip van het bedrijf NXP Semiconductors, die veelal gebruikt wordt in contactloze chipkaarten, zoals de Nederlandse OV-chipkaart.

### **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 phishing sites.

### **Obfuscatie**

In het algemeen: versluiting. Deze term wordt gebruikt om de interne werking van malware te versluiten voor onderzoekers of onzichtbaar te maken voor virusscanners.

### **OpenSSL**

OpenSSL is de naam van de verzameling open source hulpprogramma's op basis van de SSL- en TLS-protocollen die gebruikt worden voor integriteit en vertrouwelijkheid van informatie.

### **Patch**

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

### **Payment Card Industry - Data Security Standard (PCI-DSS)**

PCI-DSS is een beveiligingsstandaard die specifiek gemaakt is voor bedrijven die creditcardbetalingen verwerken. De standaard omvat naast technische ook organisatorische maatregelen.

### **Phishing**

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

### **Plug-in**

Een programma of script dat tot doel heeft om een ander programma uit te breiden, maar dat niet zelfstandig kan draaien.

### **Public Key Infrastructure (PKI)**

Een Public Key Infrastructure is een verzameling organisatorische en technische middelen waarmee je op een betrouwbare manier een aantal zaken kunt regelen, zoals het versleutelen en ondertekenen van informatie en het vaststellen van de identiteit van een andere partij.

### **Registrar**

Een organisatie die, namens eindgebruikers, internetdomeinnamen registreert bij een domeinnaam registry, een database met domeinnamen. De registry voor Nederland wordt beheerd door de Stichting Internet Domeinregistratie Nederland (SIDN). Alle domeinen worden uiteindelijk gebaseerd op een aantal 'top level domains', die toegekend worden door ICANN (Internet Corporation for Assigned Names and Numbers).

### **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.

### **SSL-certificaat**

Een SSL-certificaat is een bestand dat fungeert als digitale identificatie van een persoon of systeem. Het bevat tevens PKI-sleutels om gegevens tijdens transport te versleutelen. Een bekende toepassing van SSL-certificaten zijn de met HTTPS beveiligde websites.

### **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.

### **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.

### **Targeted attack**

Een gerichte aanval op een specifieke organisatie, bedrijfstak of persoon.

### **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.

### **Temporal Key Integrity Protocol (TKIP)**

Een verouderd beveiligingsprotocol voor draadloze netwerken, oorspronkelijk ontworpen ter vervanging van WEP.

**Trojan**

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

**Upstream provider**

Upstream provider is een term voor een (grote) leverancier voor internetdiensten die toegang verleent voor kleinere providers tot het internet.

**Wired Equivalent Privacy (WEP)**

Een verouderde beveiligingsstandaard voor draadloze netwerken.

**Wi-Fi Protected Access (WPA)**

Een verouderde beveiligingsstandaard voor draadloze netwerken, die gebruikmaakt van TKIP. WPA is inmiddels vervangen door de meer omvattende standaard WPA2.

## Over GOVCERT.NL

GOVCERT.NL is sinds 2002 het Computer Emergency Response Team voor de overheid en heeft als taak het voorkomen en afhandelen van ICT-gerelateerde incidenten voor haar deelnemers. Er zijn 62 deelnemers: alle ministeries, diverse gemeenten en provincies, zbo's en agentschappen, Hoge Colleges van Staat en tevens bedrijven in de vitale sector.

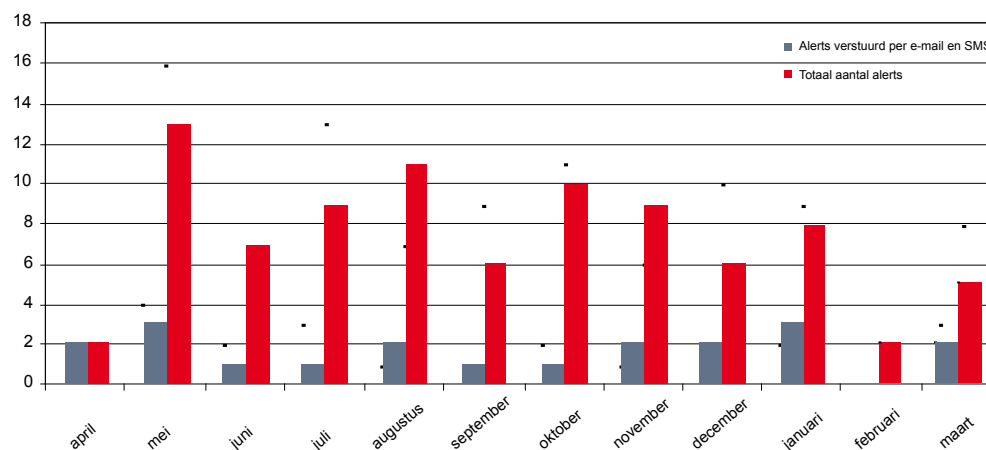
### Analyse incidenten

Incidenttype	%
Request for Assistance	30%
Malware	20%
Kwetsbaarheid	9%
Overig	9%
Phishing	7%
Hacking	5%
Defacement	3%
Publicatie vertrouwelijke gegevens	3%
DoS	3%
Spam versturen	3%
Gerichte aanval	3%
Persoonsgegevens	2%
Beheerfout	2%
Bedreiging	1%
Oplichting	0%
Social engineering	0%

Incident response, advies & preventie, kennisdeling en waarschuwen zijn de kerntaken van GOVCERT.NL. De securityspecialisten zijn 24 uur per dag, 7 dagen per week beschikbaar voor bijstand tijdens incidenten. Er wordt een follow-the-sun waakdienst gedraaid van 09.00 tot 21.00 uur, waarna collega-securityspecialisten in Australië en de VS het stokje overnemen. Tijdens de waakdiensten worden duizenden bronnen continu gemonitord, met het doel om vroegtijdig ontwikkelingen, dreigingen en incidenten te ontdekken.

GOVCERT.NL werkt nauw samen met andere organisaties, waaronder ISP's, opsporingsdiensten en de vitale sectoren. Daarnaast is zij onderdeel van een internationale community van CERT's en andere overheidsdiensten. Immers, internet en ook internetcriminaliteit kent geen grenzen. Internationale samenwerking is dan ook essentieel. GOVCERT.NL draait mee in (inter)nationale rampenoefeningen, ontwikkelt tools om het detecteren van dreigingen en malware te versnellen en ontwikkelt kennisproducten als white papers en factsheets.

Waarschuwingsdienst.nl is een instrument van GOVCERT.NL om de computergebruiker thuis en binnen het MKB te bereiken. Via e-mail, sms en [www.waarschuwingsdienst.nl](http://www.waarschuwingsdienst.nl) worden zij gewaarschuwd voor dreigingen vanaf het internet en ontvangen informatie over veilig internetten.



Alerts gepubliceerd via [Waarschuwingsdienst.nl](http://Waarschuwingsdienst.nl)

Zie voor meer informatie over GOVCERT.NL en Waarschuwingsdienst.nl ook [www.govcert.nl/jaaroverzicht2008](http://www.govcert.nl/jaaroverzicht2008)

## Colofon

GOVCERT.NL bedankt de volgende organisaties voor het verstrekken van aanvullende gegevens:

- The ShadowServer Foundation ([www.shadowserver.org](http://www.shadowserver.org)) voor het verstrekken van informatie over bots in Nederland.
- Panda ([www.pandasecurity.com](http://www.pandasecurity.com)) voor het verstrekken van informatie over detectie van nep-antivirus in Nederland.
- Het Information Warfare Monitor initiatief (128.100.171.10) voor het verstrekken van informatie over wereldwijde infecties in het GhostNet netwerk.

### **Verantwoording illustraties:**

De illustratie op pagina 10 is een gedeelte van de 'Web Trend Map 4' en is gebruikt met toestemming van Information Architects Japan ([informationarchitects.jp](http://informationarchitects.jp))

### **Gebruik:**

*(Naamsvermelding-Niet-commercieel-Gelijk delen 3.0 Nederland)*

U mag dit werk kopiëren, verspreiden en doorgeven en afgeleide werken maken onder de voorwaarden zoals beschreven in de licentie op [creativecommons.org/licenses/by-nc-sa/3.0/nl/](http://creativecommons.org/licenses/by-nc-sa/3.0/nl/)

Uitgave: juni 2009

Oplage: 750

Redactie: GOVCERT.NL

Vormgeving: NewCase

Druk: Koninklijke Broese & Peereboom b.v.

Elektronische versie: [www.govcert.nl/trends](http://www.govcert.nl/trends)

Wilhelmina van Pruisenweg 104  
2595 AN Den Haag

Postbus 84011  
2508 AA Den Haag

T 070 888 7 555

E [info@govcert.nl](mailto:info@govcert.nl)

I [www.govcert.nl](http://www.govcert.nl)



GOVCERT.NL bouwt mee aan de e-overheid