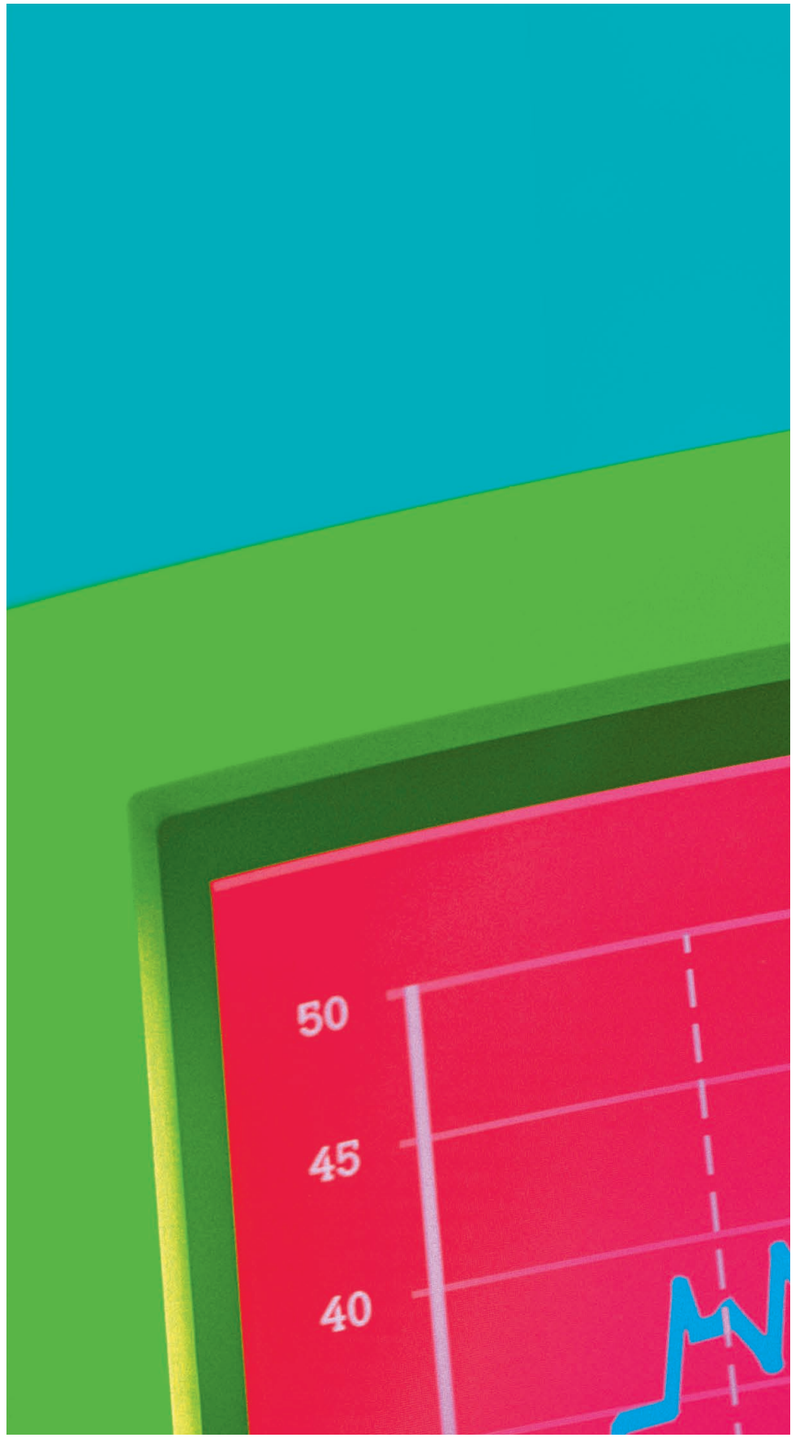
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
T 070 888 7 555
E info@govcert.nl
I www.govcert.nl



GOVCERT.NL

Trendrapport 2007

Cybercrime in trends en cijfers

GOVCERT.NL bouwt mee aan de e-overheid

GOVCERT.NL
is het Computer Emergency Response Team van en voor de Nederlandse overheid. Zij ondersteunt overheidsorganisaties in het voorkomen en afhandelen van ICT-gerelateerde veiligheidsincidenten, 24 uur per dag, 7 dagen per week. Advies en preventie, waarschuwing, incidentafhandeling en kennisdeling zijn hierbij sleutelwoorden.

GBO.OVERHEID
is de Gemeenschappelijke Beheer Organisatie waar GOVCERT.NL sinds 1 januari 2006 deel van uit maakt. Zij is verantwoordelijk voor beheer en verdere ontwikkeling van een aantal overheidsbrede ICT-voorzieningen.

Inhoud

GOVCERT.NL baseert haar adviezen en waarschuwingen op verschillende bronnen. Een groot aantal publieke en besloten internationale informatiebronnen en collega-CERT's leveren zicht op nieuwe kwetsbaarheden, dreigingen en misbruik. Deelnemers en partners waarmee GOVCERT.NL samenwerkt leveren informatie over individuele incidenten en vragen die leven bij de deelnemers. Daarnaast heeft GOVCERT.NL een eigen monitoringnetwerk, waarin sinds april 2006 actuele informatie over poortscans en aangeboden kwaadaardige programma's wordt verzameld en gepresenteerd.
Met behulp van deze bronnen is dit rapport samengesteld, waarbij feiten en concrete waarnemingen de basis vormen van de geschetste trends. Verwacht daarom geen schatting van de omvang van cybercrime in Nederland, gewoon omdat we hiervoor onvoldoende harde gegevens hebben. Er worden in dit rapport diverse voorbeelden aangehaald, waarvan op internet meer informatie te vinden is. De links naar deze informatie zijn gemakkelijk te vinden via de website van GOVCERT.NL: http://www.govcert.nl/trends.

Feiten en cijfers uit de praktijk onmisbaar

Zero days, spam, phishing, botnets. Het zijn voor veel mensen geen alledaagse termen. Maar het zijn wel degelijk alledaagse verschijnselen, waar veel organisaties en particuliere thuisgebruikers mee te maken hebben. Het zijn termen die direct gerelateerd zijn aan een fenomeen waar ik me -en velen met mij- al lange tijd zorgen over maak: internetcriminaliteit of cybercrime.

Cybercrime neemt in alle sectoren van de samenleving toe. Niet voor niets is in het coalitieakkoord dat in februari 2007 tot stand kwam, opgenomen dat de bestrijding hiervan daadkrachtig ter hand moet worden genomen. Naast de zegeningen van het internet -we hebben ook ambitieuze doelstellingen op het gebied van de elektronische dienstverlening geformuleerd- zijn er keerzijden aan de openheid en mogelijkheden van het wereldwijde web. En die moeten we heel serieus nemen.

In dit Trendrapport van GOVCERT.NL, het Computer Emergency Response Team van de Nederlandse overheid, wordt dit onverbloemd duidelijk. Ik ben bijzonder blij dat dit rapport er is: gebaseerd op feitelijke, dagelijkse waarnemingen van een operationele dienst die uitermate kundig is op het gebied van informatiebeveiliging.
Hier komt veel ervaring en informatie bij elkaar en het is goed dat die wordt gedeeld. GOVCERT.NL bestaat momenteel vijf jaar en heeft in die tijd een onmisbare bijdrage geleverd, zowel aan haar deelnemers als aan computergebruikers thuis en in het midden- en kleinbedrijf.

Het probleem cybercrime heeft te weinig urgentie bij burgers en bedrijven. Ondanks de omvang en het bereik is het een probleem dat veel mensen ervaren als ver van hun bed. Bewust of onbewust. Hoewel cybercrime vaak vrijwel onzichtbaar is, zijn de effecten enorm. Bewustwording is hierin het sleutelwoord. Praktische adviezen, nationale en internationale contacten en effectieve beveiligingsinstrumenten vormen onderdelen van de oplossing.
Ik hoop en verwacht dat dit Trendrapport met concrete cijfers en trends een rol speelt in die bewustwording.
Feiten helpen het zicht op het probleem te verbeteren. Daardoor kunnen we beter werken aan oplossingen.
Als we niets doen met dit soort heldere signalen, sluiten we onze ogen voor een ongewenste ontwikkeling.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
Ank Bijleveld-Schouten

1. De metamorfose van informatie

“Information wants to be free” zei Steward Brand tijdens de eerste “Hackers Conference” in 1984, de begindagen van het digitale tijdperk[1]. Met zijn uitspraak refereerde hij aan het feit dat informatie, vooral digitale informatie, zeer gemakkelijk te dupliceren en te verspreiden is. Tegelijkertijd wordt informatie steeds waardevoller en de behoefte aan het beschermen ervan steeds groter. Van dit spanningsveld was hij zich toen al zeer bewust.

Nu, bijna 25 jaar later, heeft de uitspraak van Steward Brand nog niets aan actualiteit ingeboet. Sterker nog, de tegenstellingen tussen de deelbaarheid van informatie aan de ene kant en de waarde van informatie aan de andere kant is alleen maar groter geworden. De uitspraak geeft hiermee kernachtig weer wat we signaleren in de veranderende plek van informatie in onze samenleving en de aantrekkingskracht die dit uitoefent op criminelen. In dit hoofdstuk belichten we kort enkele aspecten van informatie die we in de afgelopen jaren hebben zien veranderen:

- Informatie wordt mobieler en daarmee kwetsbaarder en moeilijker onder controle te houden;
- Informatie staat niet meer op zichzelf, ketens van informatie creëren afhankelijkheden en nieuwe kwetsbaarheden;
- Informatie wordt waardevoller en daarmee aantrekkelijker voor misbruik.

Als gevolg van de ontwikkelingen op deze vlakken groeit het risico dat informatie, ook uw en onze informatie, op onbedoelde manier wordt gebruikt, hetzij per ongeluk, hetzij als gevolg van kwade opzet. We hebben te maken met een veranderend dreigingsbeeld op het gebied van internetcriminaliteit.

1.1 Informatie wordt mobieler

De mens wordt wel een informavoor genoemd: we leven van informatie en die afhankelijkheid wordt steeds groter. Wat we de afgelopen jaren vooral hebben gezien, is dat mensen in toenemende mate behoefte hebben om informatie op elk moment ter beschikking te hebben. Denk daarbij aan USB-sticks om informatie te vervoeren, MP3-spelers om overal en altijd naar muziek te kunnen luisteren, en ook aan de diverse slimme apparaten die in omloop zijn: telefoons, gecombineerd met walkmans en browsers. Of PDA’s, die eigenlijk volwaardige kleine computers zijn. De markt voor dit soort mobiele apparatuur is in 2006 spectaculair gegroeid ten opzichte van 2005[2]. En terwijl het nog maar enkele jaren geleden heel normaal was om zonder navigatiecomputer en mobiele telefoon in de auto te stappen is dat nu bijna vreemd. Ook organisaties ontkomen er niet aan om een standpunt in te nemen over dergelijke mobiele datadragers en de mobiliteit van data in het algemeen. Enerzijds vragen werknemers om informatie en toegang tot systemen en netwerken waar en wanneer ze die nodig hebben, anderzijds hebben ook toeleveranciers en afnemers een groeiende informatiebehoefte. Voor een organisatie kan dit een verhoging van de productiviteit opleveren, maar het flexibel ontsluiten van informatie brengt op meerdere vlakken complexe vraagstukken met zich mee. Op het vlak van techniek, beleid en zeker informatiebeveiliging. Voor welke technieken kies je, moeten de gedragsregels worden aangepast, wat zijn de effecten op het informatiebeveiligingsbeleid?

We hebben te maken met een veranderend dreigingsbeeld in verband met cybercrime.

De introductie en verspreiding van mobiele datadragers draagt bij aan de vervaging van de grens tussen de eigen organisatie en de buitenwereld, net zoals die grens ook vervaagt op het moment dat mensen kunnen telewerken: informatie bevindt zich steeds vaker buiten wat traditioneel als “het eigen domein” wordt gezien. De controle die je over de informatie hebt zal dus verminderen. Een goed voorbeeld hiervan is de schokkende hoeveelheid mobiele apparatuur (mobiele telefoons, PDA’s, laptops) die mensen vergeten en ergens per ongeluk achterlaten. Uit een onderzoek van november 2006 blijkt dat in het gebied rondom Washington D.C. in de V.S. in zes maanden tijd ruim 8700 mobiele apparaten in taxi’s zijn achtergelaten![3]

Daarmee is ruim 8700 keer een schat aan informatie op straat komen te liggen. In Nederland hebben we recent een aantal spraakmakende incidenten meegemaakt die kenmerkend zijn voor de vervaging van de grens tussen de eigen organisatie en de buitenwereld[4]. De problematiek van mobiele datadragers is bij vrijwel alle deelnemers van GOVCERT.NL een “hot topic”, dat op alle niveaus speelt, zo maken we op uit de vragen die we krijgen.

Extra risico’s van mobiele apparatuur houden bijna alle deelnemers bezig.

Dit speelt niet alleen bij de overheid, maar ook bij het bedrijfsleven. In oktober 2006 heeft GOVCERT.NL een white paper voor haar deelnemers over dit onderwerp uitgebracht. Momenteel is er grote behoefte aan normen voor veilig gebruik van mobiele datadragers en “goedgekeurde” apparatuur. Om in dat laatste te voorzien loopt een onderzoek door het Nationaal Bureau Verbindingsbeveiliging (NBV) naar beveiligde USB-sticks voor gebruik met als “Departementaal Vertrouwelijk” geclassificeerde gegevens. Inmiddels is één stick al goedgekeurd, een tweede zal binnenkort volgen[5].

[1] Steward Brand heeft dit ook verder uitgewerkt in zijn boek “The Media Lab: Inventing the Future at MIT” uit 1987
[2] Gegevens van IDC: http://www.idc.com/getdoc.jsp?containerId=prUS20578607. Gegevens van Canalys: http://www.canalys.com/pr/2007/r2007024.htm
[3] “New survey reveals thousands of mobile devices left behind in major U.S. city taxi cabs”, 28 november 2006: http://www.pointsec.com/news/newsreleases/release.cfm?PressId=386
[4] Brief over veiligheidsincidenten van het ministerie van Defensie. http://www.mindef.nl/tekst/actueel/parlement/kamerbrieven/2006/2/20060609_briefveiligheidsincidenten.aspx
[5] Zie hiervoor de NBV-nieuwsbrief van december 2006: http://www.aivd.nl/contents/pages/70893/nieuwsbriefnbvdec.pdf

Het marktonderzoek dat het NBV vooraf heeft uitgevoerd toonde overigens aan dat veel producten lang niet de verwachtingen waar maken: van tien producten vielen direct al zeven producten af, een achtste bleek niet tijdig klaar te zijn. Thuiswerkers bij de overheid ontberen nog vaak faciliteiten om dit veilig te doen: vaak worden wel veilige verbindingen gebruikt, maar soms belanden documenten en dossiers op privécomputers van medewerkers. Op dit vlak vormen de kosten en regels voor thuiswerkplekken een belemmering en wordt meestal de verantwoordelijkheid bij de medewerkers gelegd. Incidenten die in de media zijn beschreven geven aan dat dit niet altijd een verstandige keuze is.

1.2 Informatie staat niet meer op zichzelf

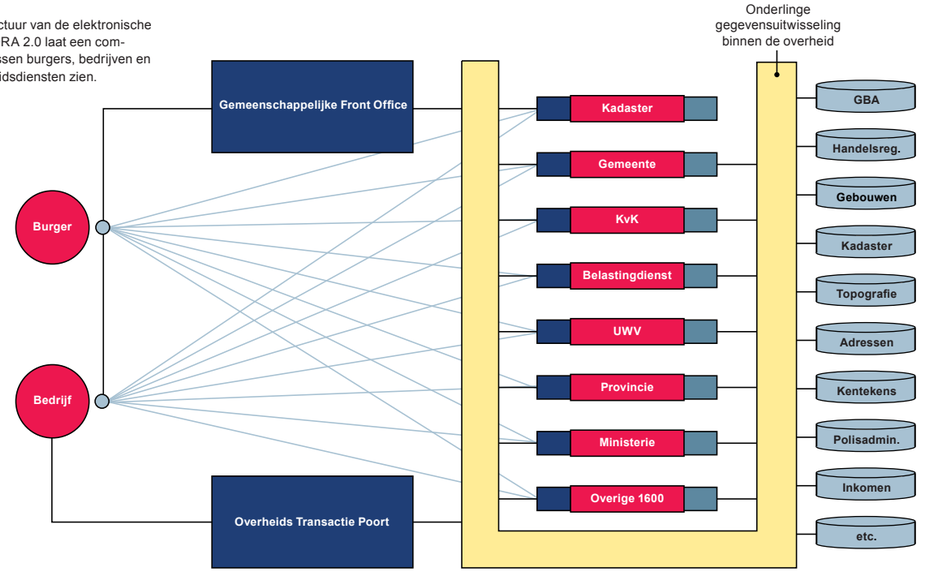
Het actieprogramma “Andere Overheid”[6] heeft tot doel de overheid te moderniseren, zodat zij beter in staat is grote maatschappelijke problemen adequaat aan te pakken. Deze moderniserings- en efficiëntieslag wordt voor een groot deel gerealiseerd door slim gebruik van ICT-middelen. Eén van de actielijnen van het programma is bijvoorbeeld het verbeteren van de overheidsdienstverlening aan de burger. Daaronder valt elektronische dienstverlening, waarbij specifiek is gesteld: “het kabinet streeft er naar dat in 2007 65% van de publieke dienstverlening (van rijk, provincies en gemeenten) plaats kan vinden via het internet.” Bekende projecten die voortkomen uit het actieprogramma zijn bijvoorbeeld DigiD[7] en de Persoonlijke Internet Pagina (PIP)[8], waar momenteel een pilot mee loopt. Uit onderzoek blijkt dat al 50% van de Nederlandse internetgebruikers gebruik maakt van elektronische dienstverlening van de overheid[9].

Volgens dit laatste onderzoek is de overheid goed op weg met het realiseren van deze doelstelling[10]. Maar wat zijn nu precies de consequenties van het elektronisch aanbieden van diensten aan burgers en bedrijven? Eén van de aandachtpunten is de koppeling van netwerken en databases. Als je de uitwisseling van informatie op een efficiënte manier wilt aanpakken zul je als overheidsorganisatie de gegevens die aangeleverd worden, (semi-)geautomatiseerd moeten opnemen in je processen. Dit brengt vanzelfsprekend extra risico’s met zich mee, omdat het gaat om informatie die van buiten komt en die in beginsel “niet te vertrouwen” is. De ontwikkeling van beveiligingsmaatregelen en afspraken tussen de partners in de verschillende procesketens is iets wat structurele aandacht verdient. Andersom betekent het aanbieden van elektronische diensten vaak het bundelen van informatie uit meerdere bronnen, zoals bijvoorbeeld de ontwikkeling van de eerder genoemde PIP laat zien. Naarmate bij een dienst meerdere aanbieders en ontvangers betrokken zijn, wordt het steeds belangrijker vast te leggen wie verantwoordelijk is voor welk deel van de informatie, en ook waar de oorspronkelijke informatie vastgelegd is.

De elektronische overheid vergt structurele aandacht voor informatiebeveiliging.

De manier waarop met autorisaties omgegaan wordt en de handhaving hiervan bij de toegang tot systemen is één van de fundamentele aandachtspunten. Zoals uit de schematische weergave in figuur 1-1[11] van de elektronische overheid blijkt, kunnen informatieketens complex zijn.

Figuur 1-1
De referentie architectuur van de elektronische overheid volgens NORA 2.0 laat een complexe uitwisseling tussen burgers, bedrijven en verschillende overheidsdiensten zien.



[6] http://www.andereoverheid.nl/AndereOverheid/Web/Het+Programma/
[7] http://www.digid.nl
[8] http://www.e-overheid.nl/atlas/overzichtskaarten/pip
[9] Overheidsdiensten via internet populair, CBS 18 april 2007: http://www.cbs.nl/nl-NL/menu/themas/bedrijven/publicaties/artikelen/archief/2007/2007-2173-wm.htm
[10] http://www.andereoverheid.nl/NR/rdonlyres/1EE4F67B-3D1C-436D-93FF-8B953F100924/12924/VoortgangsrapportageAndereOverheidapril2006.pdf
[11] Bron: http://www.e-overheid.nl/. Overgenomen onder de volgende voorwaarden: http://creativecommons.org/licenses/by-nc-sa/2.5/nl/

1.3 Informatie wordt waardevoller

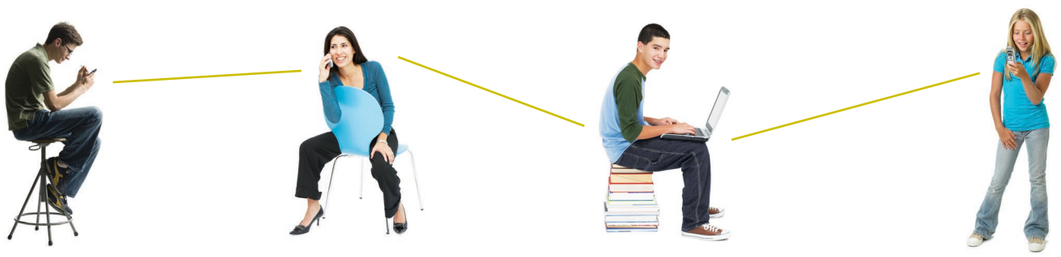
In toenemende mate laten mensen hun digitale gegevens achter bij overheden, winkels en dienstverleners. De databases die daarmee ontstaan bevatten veel en interessante informatie. Juist omdat we nu een heleboel zaken online kunnen regelen, wordt de informatie die benodigd is om die zaken te regelen waardevoller. Denk daarbij niet alleen aan informatie om overheidszaken te regelen maar ook aan informatie om bankzaken en verzekeringszaken te regelen. Criminelen worden hierdoor aangetrokken en het lukt hen daadwerkelijk financieel gewin te behalen en een lucratieve criminele organisatie op te zetten. Over de omvang van de schade door cybercrime circuleren verschillende schattingen, waarvan de betrouwbaarheid onbekend is. Zeker is dat het over enorme bedragen gaat.
Een ander kenmerk van online activiteiten is dat zij onafhankelijk zijn van waar de bezoeker zich fysiek bevindt. Of dat nu op kantoor of thuis of zelfs “in” een cyber café in Bangkok is.
Dit is een gegeven waar criminelen dankbaar gebruik van maken. Waardevolle informatie als inloggegevens van banken en betaalsystemen kunnen zij op grote schaal en op afstand stelen van nietsvermoedende computergebruikers. Daarna kunnen criminelen de gegevens misbruiken, ook weer op afstand. Voor het bemachtigen van hun buit, de digitale informatie, maken criminelen gebruik van kwaadaardige software, die ze per e-mail en via websites verspreiden. Ze bereiken hiermee grote groepen computergebruikers, waarvan altijd wel voldoende slachtoffers in de val trappen. Dit is een trend die al enkele jaren te zien is.
In het volgende hoofdstuk zullen we uitgebreid stil staan bij de methoden en middelen die op dit moment veel gebruikt worden.

1.4 De gevolgen

Zoals we hebben gezien zijn er meerdere redenen waarom internetcriminelen het op onze informatie gemunt hebben.

- De informatie wordt steeds mobieler en trekt zich minder aan van de grenzen van organisaties en netwerken.
- Tegelijkertijd wordt informatie waardevoller: er kan online, gemakkelijker en meer mee worden bereikt.
- Tenslotte is de informatie in grote hoeveelheden op afstand beschikbaar.

Daarmee is de aantrekkingskracht van digitale informatie wel erg groot geworden en dit heeft serieuze consequenties.
We moeten ons realiseren dat criminaliteit zich in snel tempo zal richten op de online activiteiten van mensen en overheid, die zich, sneller dan nu gebeurt, moeten wapenen tegen digitale misdaad. We moeten aandacht besteden aan de manier waarop we de informatie en systemen die we beheren beschermen.
Als overheid of bedrijf, als werknemer of werkgever maar ook als privégebruiker thuis en wellicht als opvoeder van kinderen. Zoals we in het volgende hoofdstuk zullen zien zijn de middelen die worden ingezet om onze informatie te stelen de afgelopen jaren gewijzigd. Dit betekent dat de verdedigingsmaatregelen waarmee we vertrouwd zijn niet in alle gevallen meer afdoende zijn.
We zullen andere of aanvullende maatregelen moeten nemen: op het werk en thuis. In hoofdstuk 3 zullen we in de vorm van een to do lijst een aantal mogelijke maatregelen beschrijven.



2. De feiten op een rij

Dit hoofdstuk beschrijft in het kort de methoden die internetcriminelen toepassen om geld te verdienen en de hulpmiddelen die ze daarbij gebruiken. Daarnaast gaan we in dit hoofdstuk dieper in op enkele belangrijke recente trends op het gebied van malware en middelen.

Zo zien we dat voor de infectie van machines meer en meer gebruik wordt gemaakt van zogenaamde zero-day exploits en zien we steeds vaker kleinschalige, gerichte aanvallen. Spam is tegenwoordig niet alleen vervelend, maar ook een risico. Tenslotte besteden we aandacht aan twee ontwikkelingen op het gebied van phishing: *phishing by proxy* en aanvallen op systemen die beschermd zijn met behulp van *two factor authentication*.

2.1 De malware-industrie

Centraal in de problematiek van cybercrime en malware staan bots en botnets. Je zou bots en botnets zelfs kunnen karakteriseren als de backbone, de infrastructuur van cybercrime. Een botnet is een verzameling van besmette computers die op afstand onder controle staan van internetcriminelen. De grootte van een botnet kan uiteenlopen van enkele tientallen tot enkele tienduizenden bots die tegelijkertijd online zijn en gebruikt kunnen worden voor criminele doeleinden[12]. Tabel 2-1 toont een viertal grote rechtzaken waarbij botnets een belangrijke rol hebben gespeeld. Opvallend in deze lijst is de snelle groei van de omvang van de gebruikte botnets. Dit toont aan dat internetcriminelen in staat zijn grootschalige botnets te creëren en te onderhouden. Criminelen en bendes steken veel tijd steken in het in de lucht houden van een botnet. Onder andere door de bots continu aan te passen zodat ze ongedetecteerd blijven. Overigens zijn dergelijke grote netwerken niet noodzakelijk voor de activiteiten waarvoor botnets gebruikt worden. Een botnet van enkele honderden bots is voldoende voor een effectieve spamrun en enkele duizenden bots is voldoende voor een DDoS-aanval. Voor het oogsten van gegevens van computers geldt wel hoe groter hoe beter.

Botnets vormen de infrastructuur voor cybercrime.

Botnets worden primair ingezet voor twee doeleinden: als hulpmiddel om crimineel geld te verdienen en als hulpmiddel om meer computers te besmetten en zo een botnet uit te breiden of nieuwe botnets te genereren. Om een beeld te schetsen van de mogelijkheden zullen we hier kort enkele voorbeelden benoemen[13]. Een botnet kan worden ingezet om op grote schaal e-mails te versturen, voor spam, scams of phishing. Verder kunnen bots worden gebruikt om gegevens te verzamelen van geïnfecteerde computers (harvesten of oogsten in jargon). Het gaat de criminelen om creditcard gegevens, maar ook om serienummers van spellen en andere software, inloggegevens en e-mailadressen.
Deze verzamelde gegevens worden daarna misbruikt of verhandeld. Tenslotte kunnen bots zich ook voordoen als legitieme gebruikers van websites. Zo kunnen bots worden ingezet om muisklikken op webadvertenties te genereren waarmee de eigenaar van de webpagina meer advertentie-inkomsten heeft: de zogenaamde klikfraude. Ook kunnen bots massaal worden ingezet om servers plat te leggen of, in geval van afpersing, hiermee te dreigen. Dit zijn de bekende DDoS-aanvallen.

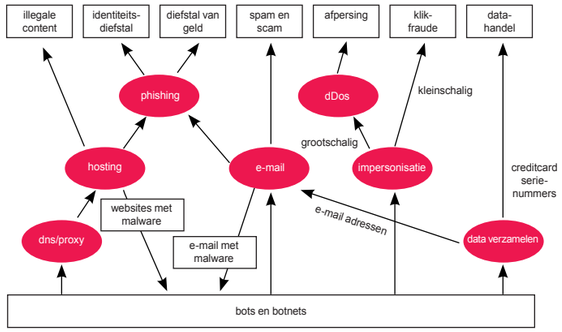
Bots zijn zeer veelzijdig en ontwikkelen zich snel.

Botnets worden ook ingezet voor de verspreiding van malware met als doel meer computers te besmetten die als bot kunnen worden ingezet. Vaak wordt dit gedaan door het versturen van e-mails. De e-mails bevatten bijlagen met malware of links naar websites die de computers van bezoekers besmetten.
Andere typen bots scannen de netwerken waarop de computer die ze geïnfecteerd hebben is aangesloten en vinden op deze manier meer gastheren die besmet kunnen worden.
In bedrijfsnetwerken worden computers op een uniforme manier geconfigureerd. Hierdoor is het erg waarschijnlijk dat er veel slachtoffers zijn die via dezelfde kwetsbare plek geïnfecteerd kunnen worden. Dit wordt in de praktijk waargenomen.

Zaak	Omvang botnet	Gebruikt voor
OM tegen hackersgroep 0x1fe (2005)	Volgens verklaring verdachten: 400 - 10.000	Onderbreken overheidssites regering.nl en overheid.nl
VS tegen Clark (2005)	20.000	Onderbreken van digitale diensten
VS tegen Anchetta (2006)	400.000	Onderbreken van digitale diensten
VS tegen Maxwell	625.000	Verspreiding van adware
OM tegen S.B en F.C. (2007, beroep loopt)	miljoenen	Het vastleggen van toetsaanslagen Fraude elektronisch bankieren Onderbreken van elektronische dienstverlening

Tabel 2-1
Gepubliceerde veroordelingen van internet criminelen die botnets inzetten voor afpersing en fraude. Bronnen: Rechtbank Rotterdam, US Department of Justice, Rechtbank Breda

[12] In de media verschijnen ook regelmatig berichten over botnets van enkele honderdduizenden tot meer dan een miljoen bots. Over het tellen en weergeven van botnetgroottes bestaan uiteenlopende meningen. Een verhelderende verhandeling hierover is gepresenteerd op de Usenix “HotBots” conferentie van 10 april 2007. “My Botnet is Bigger than Yours”: http://www.usenix.org/events/hotbots07/tech/full_papers/rajab/rajab.pdf
[13] Voor uitgebreide informatie over botnets verwijzen we u naar http://www.govcert.nl/trends



Figuur 2-1
Illegale activiteiten en de relatie met botnets

Belangrijk is te realiseren dat deze activiteiten niet per sé in één hand gehouden hoeven te worden. De beheerder van een botnet (de botherder) zal vaak delen van zijn botnet verhuren aan andere criminelen, die de bots gebruiken voor een aanval of spamrun. Ook de botherder zelf maakt gebruik van diensten van anderen, bijvoorbeeld om kennis over nieuwe exploits te verkrijgen. Er is sprake van een markt voor technologie en diensten. Het resterende gedeelte van dit hoofdstuk zullen we besteden aan enkele belangrijke recente ontwikkelingen op het gebied van malware, bots en botnets.

2.2 Gerichte aanvallen, zero-day-exploits en verminderde herkenning

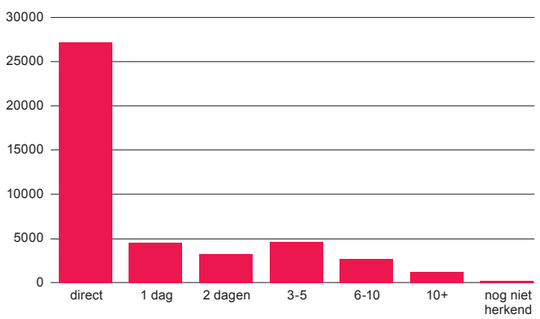
De tweede helft van 2006 liet een sterke toename zien in het misbruik van zero-day-exploits[14]. Opvallend was bijvoorbeeld malware die kwetsbaarheden in Microsoft Office producten misbruikte: Powerpoint, Word en Excel vielen allen ten prooi aan malware die veelal van Chinese origine leek te zijn[15]. Bijzonder was bovendien dat de malware werd ingezet in zeer kleinschalige, gerichte aanvallen: targeted attacks.

Office-bestanden met zero-day exploits vormen een groot risico voor gerichte aanvallen.

Zo'n gerichte aanval met behulp van een zero-day exploit deed zich in mei 2006 voor in het Amerikaanse Department of State, toen een medewerker een e-mail met bijlage ontving. Die bijlage, een Word-document, zou een toespraak bevatten uit het congres over een relevant onderwerp. In werkelijkheid bevatte het Word-document exploit-code voor een onbekende kwetsbaarheid in Microsoft Word, waarmee de computer van de medewerker geïnfecteerd werd[16]. Over de herkomst van deze aanval is niks bekend gemaakt. Door de malware op kleine schaal in te zetten, voorkomen internetcriminelen dat hun malware herkend wordt. Kleinschalige besmettingen vallen immers minder op dan grote uitbraken. Als gevolg hiervan duurt het vaak langer voordat anti-virus leveranciers updates maken. Veel malware die in omloop is, wordt dan ook (nog) niet herkend. Gegevens van het monitoringsysteem van GOVCERT.NL bevestigen dit. Figuur 2-2 bevat gegevens over de laatste 2000 bestanden die in 2006 door het monitoringsysteem zijn geanalyseerd. De figuur geeft weer hoeveel virusscanners bij de eerste scan een bepaalde malware herkenden.

Figuur 2-2
Van de in 2006 aangeboden unieke malware bestanden werd slechts 74% direct herkend (n=1942, resultaat bij gebruik van twee virusscanners). Installatie van een derde virus-scanner halverwege de meetperiode verbeterde dit naar 85% (figuur hieronder, n=1112).

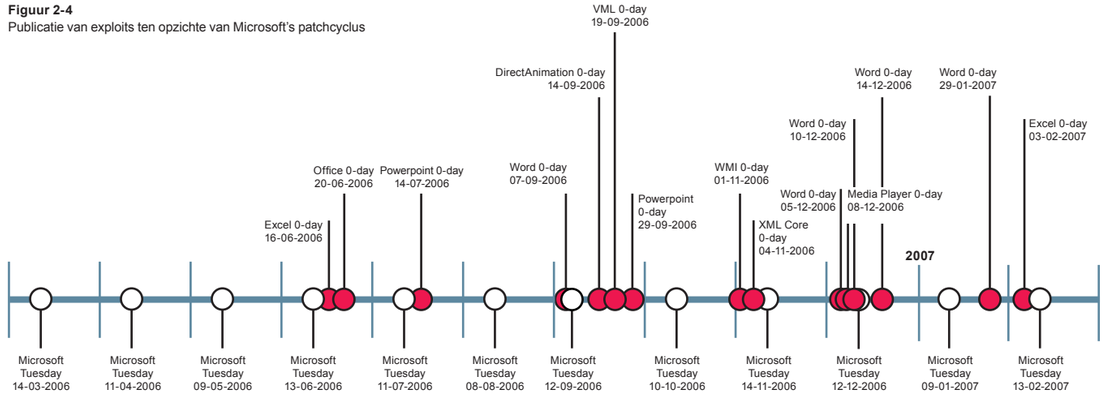
Malware die in eerste instantie niet herkend wordt heeft grote kans later wel herkend te worden, nadat de virusscanners worden voorzien van nieuwe updates. Na iedere update wordt de niet herkende malware opnieuw gescand en vaak is na een dag de juiste update geladen. Maar even vaak duurt dit drie tot vijf dagen. Voor een klein deel geldt dat het meer dan 10 dagen heeft geduurd voordat de malware werd herkend.



Figuur 2-3
Verstreken tijd tussen download van malware en herkenning door virusscanners (n=44112)

Ook is opvallend dat nieuwe kwetsbaarheden in Microsoft-producten in sommige gevallen vlak na de maandelijkse patch-dag van Microsoft bekend werden. Hierdoor duurt het vaak minimaal een maand voordat een patch beschikbaar komt die de betreffende kwetsbaarheid verhelpt. Figuur 2-4 geeft een overzicht van het bekend worden van ernstige zero-day kwetsbaarheden in relatie tot de maandelijkse patchdag van Microsoft[17]. Zero-day exploits bleven echter niet beperkt tot producten van Microsoft. Ook andere producten vielen ten prooi aan internet-criminelen.

Figuur 2-4
Publicatie van exploits ten opzichte van Microsoft's patchcyclus



Het risico van misbruik werd vergroot doordat technische details vaak openlijk gepubliceerd werden op mailinglijsten als Full Disclosure en Bugtraq[17] en op blogs. Berucht zijn inmiddels de "Month of …" initiatieven waarin een maand lang nieuwe kwetsbaarheden in een bepaald product of producten van een bepaalde leverancier bekend gemaakt worden. Zo hebben we de "Month of the Browser Bugs", "Month of the Kernel Bugs", "Month of the Apple Bugs" en "Month of the PHP Bugs" de revue zien passeren. Een "Month of the Oracle Bugs" werd op het laatste moment om onbekende reden afgeblazen. We verwachten de komende tijd meer van dit soort initiatieven te zien. Details over kwetsbaarheden verschijnen dus steeds vaker en steeds sneller publiekelijk op internet. Dit stelt internetcriminelen in staat om op eenvoudige wijze misbruik te maken van deze kwetsbaarheden. Exploit-archieven op internet tonen alle bekende exploits op overzichtelijke wijze en bieden de mogelijkheid om kant-en-klare exploits te downloaden en deze vervolgens voor eigen gewin in te zetten. Andere initiatieven maken misbruik van kwetsbaarheden nog eenvoudiger door de exploits in te bouwen in gebruikersvriendelijke software. Een bekend voorbeeld hiervan is het Metasploit framework. Hiermee kunnen zelfs ongetalenteerde kwaadwillenden eenvoudig kwetsbaarheden uitbuiten. Ondanks de grote dreiging van nieuwe kwetsbaarheden en exploits blijven oude virussen, of nieuwe virussen voor lang bekende kwetsbaarheden nog steeds effectief. Het monitoringsysteem van GOVCERT.NL registreert vaak jaren oude malware en ook Microsoft signaleert in haar halfjaarrapporten hardnekkig terugkerende virussen en wormen. Daarnaast is dit zichtbaar in de aan GOVCERT.NL gemelde incidenten. Een les is dat de dreiging van zero-day exploits de noodzaak van patchen van systemen niet wegneemt.

Nieuwe zero-day exploits voor Officeproducten worden vaak ingezet rond de maandelijkse patchdag van Microsoft.

Patchen en aandacht voor patchmanagement zijn nog steeds nodig.

2.3 Meer dan alleen vervelend

Het aandeel van spam in e-mail is in Nederland redelijk stabiel, maar het gaat om grote hoeveelheden berichten waar niemand om vraagt. Zie voor meer informatie over spam het kader "internetveiligheid". Veel van deze spam is redelijk onschuldig en verleidt de ontvanger de meest uiteenlopende producten aan te schaffen. Van palmbomen en barkrukken tot Viagra-pillen, het is het afgelopen jaar allemaal voorbij gekomen. Maar tussen deze onschuldige, zij het irritante, spamberichten bevinden zich in sommige gevallen ook minder onschuldige varianten. Denk bijvoorbeeld aan spamberichten voorzien van malware en spamberichten in de vorm van phishing en de combinatie. Internetcriminelen lijken voorlopig nog niet genoeg te krijgen van het versturen van grote hoeveelheden spam met malware. Zij spelen daarbij in op actuele gebeurtenissen en ontwikkelingen. Eind 2006 werd de Nuwar-worm in grote getale verspreid via e-mail-berichten met als titel "Happy New Year!" en "Warmest Wishes For New Year!". De storm die kort daarna over Europa raasde en openbaar vervoer en verkeer platlegde was vervolgens ook aanleiding voor een nieuwe worm storm. De toegenomen hoeveelheid spam met malware leidt tot meer infecties van computers. Deze computers maken na infectie mogelijk deel uit van een botnet dat vervolgens weer meer mogelijkheden tot het versturen van spam. Hierdoor ontstaat een vicieuze cirkel waarin meer spam leidt tot meer infecties wat weer leidt tot meer spam.

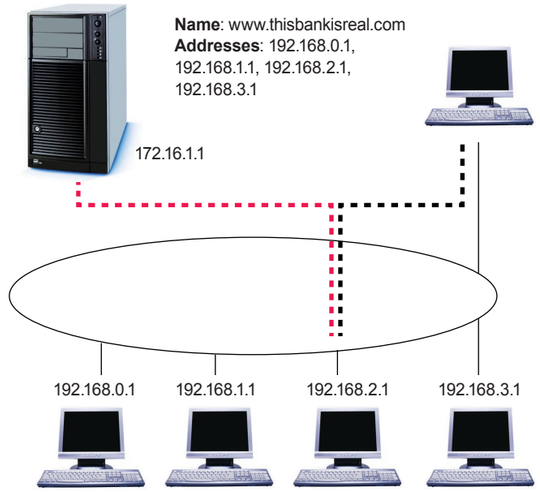
Spam is tegenwoordig niet alleen vervelend, maar vooral ook een risico.

[14] Messagelabs heeft hierover een specifiek rapport geschreven. Het rapport, uit maart 2007, is te vinden op: http://www.messagelabs.com/Threat_Watch/Intelligence_Reports
[15] Zie hiervoor bijvoorbeeld: MS Word Exploit Creation Tool, 4 april 2007: http://www.symantec.com/enterprise/security_response/weblog/2007/04/ms_word_exploit_creation_tool.html
[16] Het transcript van de verklaring over dit incident van Donald R. Reid, Senior Coordinator for Security Infrastructure, is te lezen op: http://www.state.gov/m/ds/rls/rm/83256.htm
[17] Zie ook het persbericht hierover: http://www.govcert.nl/news.html?it=139.

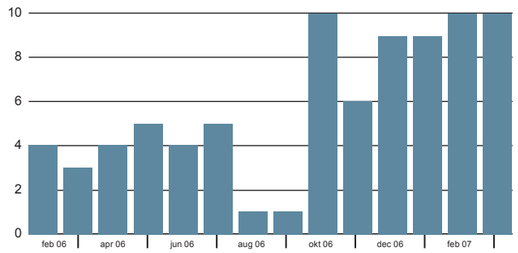
[18] Beide lijsten zijn beschikbaar via http://seclists.org/

2.4 Ontwikkelingen op het gebied van phishing

"Lieve Postbank klant", een niet-alledaagse begroeting van uw bank. En inderdaad, dit is de tekst van een phishing-aanval, gericht op Postbank klanten, door een phisher grof vertaald uit de oorspronkelijke tekst met een vertaalprogramma. Nederlandse banken zijn in toenemende mate een doelwit geworden voor phishers. Maatregelen die Nederlandse banken hebben genomen, maar banken in bijvoorbeeld de Verenigde Staten en Groot Brittanië niet, hebben ervoor gezorgd dat dit fenomeen in Nederland veel minder voorkwam. We zien nu dat internetcriminelen nieuwe manieren verzinnen om hun phishing-aanvallen succesvoller te laten zijn. En ook betere teksten in de e-mail gebruiken. Eén van de nieuwe technieken is er speciaal op gericht om de daadwerkelijke locatie van een phishing-site te verbergen en deze zo lang mogelijk in de lucht te houden. Bij deze techniek, phishing by proxy, worden bots ingezet als proxy-servers. Grote aantallen IP-adressen worden aan een phishing-URL gekoppeld en vormen zo een tussenstap in de toegang tot een phishing-website. Het laten blokkeren van dergelijke phishing-sites wordt hierdoor zeer complex. In sommige gevallen laat de phisher zijn volledige phishing-infrastructuur (DNS, webserver, proxy) op een botnet functioneren. Een andere belangrijke ontwikkeling op het gebied van phishing zijn man-in-the-middle phishing aanvallen.
Bij man-in-the-middle phishing positioneren internetcriminelen zich tussen de aangevallen klant en de bank. Authenticatiegegevens die de klant opgeeft worden direct doorgespeeld aan de bank. Deze manier van phishing maakt het mogelijk om ook toegang te krijgen tot websites als die beschermd zijn op basis van two factor authentication. Dergelijke phishing-aanvallen zijn nieuw: in de zomer van 2006 is Citibank er slachtoffer van geworden[19]. Dit was het eerst bekende technisch geslaagde geval van man-in-the-middle-phishing. Of er ook rekeninghouders gedupeerd zijn is niet naar buiten gebracht. In 2007 deed zich veel dichter bij huis een soortgelijk incident voor: phishers voerden een man-in-the-middle-aanval uit op ABN AMRO[20].



Figuur 2-5
Phishing by proxy



Figuur 2-6
Aantal phishing-incidenten waarbij GOVCERT.NL door Nederlandse banken is ingeschakeld.

Phishing

Wachtwoorden ontfutselen is eenvoudig geworden. Iedereen die een publieke dienst aanbiedt moet zich vandaag afvragen of gebruikersnaam en wachtwoord nog een voldoende basis van vertrouwen vormen. Voor steeds meer diensten worden maatregelen ingevoerd, zoals het gebruik van SSL, waarbij een digitaal certificaat de dienst identificeert aan de gebruiker. Een ander voorbeeld is de toepassing van persoonlijke en herkenbare inlogpagina's zoals bij yahoo.com. Nederlandse banken wapenen zich met two factor authentication, maar moeten blijven nadenken over volgende stappen en aanvullende maatregelen nemen.

[19] Citibank Phish Spoofs 2-Factor Authentication, 10 juli 2006: http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html
[20] Meer hierover op: https://www.abnamro.nl/nl/overabnamro/internetcriminaliteit.html?pos=hp_lb_20070412_criminaliteit

Nummer	Hits	Poortnummer	Gebruikt voor
1	225057	445	Microsoft SMB, Sasser-worm
2	209397	139	Microsoft NetBIOS, veel wormen
3	8961	135	Microsoft DCE, Blasterworm
4	3227	80	HTTP, websurfen
5	1202	5000	Windows UpnP, veel trojans
6	519	10000	Network Data Management Protocol, Cisco VPN
7	339	21	FTP
8	298	110	POP3 e-mail
9	230	143	IMAP e-mail
10	214	42	Host Name Server

Top 10 meest bevraagde communicatiepoorten (Bron: monitoringsysteem GOVCERT.NL, data van één sensor over de periode april 2007)

Nummer	Unieke IP-adressen	Land
1	4396	Frankrijk
2	3345	Verenigde Staten
3	2414	Zuid Korea
4	2367	Duitsland
5	2118	Spanje
6	1974	Ivoorkust
7	1947	Polen
8	1922	Verenigd Koninkrijk
9	1417	Taiwan
10	1225	Italië

Top 10 van landen waar de meeste aanvallen uit vandaan kwamen (Bron: monitoringsysteem GOVCERT.NL, over de periode april 2006 tot december 2006. Nederland staat op de veertiende plaats).

Nummer	Hits	URL
1	526	ftp://uid:pwd@spreadem.domein.info:21/spread.exe
2	303	ftp:// uid:pwd@world.domein.info:21/host.exe
3	200	ftp:// uid:pwd@203.121.x.x:8799/x.exe
4	146	ftp:// uid:pwd@166.104.x.x:2755/9.exe
5	138	ftp:// uid:pwd@163.17.x.x:2755/x.exe
6	125	ftp:// uid:pwd@82.x.x.x:5433/nice.exe
7	109	ftp:// uid:pwd@xman.domein.info:21/myhost.exe
8	97	ftp:// uid:pwd@203.121.x.x:2900/u.exe
9	80	ftp:// uid:pwd@ftpd.salvage.domein.info:21/salvage.exe
10	71	ftp:// uid:pwd@166.104.x.x:2755/2.exe

Top 10 van meest gebruikte downloadsites. FTP wordt het meest gebruikt voor het downloaden van malware. In deze tabel zijn gebruikersnamen en domeinen geanonimiseerd. (Bron: monitoringsysteem GOVCERT.NL, gegevens van één sensor over de periode van april 2006 – april 2007).

De data wordt op de webiste www.govcert.nl/trends beschikbaar gesteld.

"Er is sprake van een voortgaande innovatie, zoals de invoering van het Burgerservicenummer, de authenticatievoorziening DigiD, de informatie-uitwisseling tussen rijksinspectiediensten en de digitalisering van diensten en producten van de overheid.
Dit brengt met zich mee dat de informatiebeveiliging tijdig en pro-actief moet worden ingeregeld. Weerstand zal moeten worden overwonnen, spanning tussen ingezet beleid en de uitvoering zal zich gaan openbaren en de beveiliging van informatie zal weer veel aandacht krijgen omdat koppelingen worden gemaakt die tevoren niet waren te realiseren. Het noopt al met al tot een voortdurende alertheid, bewustzijn en scherpte."

Wilbert Vrouwenvelder, informatiebeveiliger bij het Ministerie van V&W

CERT/CC was established in 1988 as the first incident response team for the Internet. Our philosophy has always been a distributed approach to response where we try to motivate large organizations and countries to create CERTs, each one to tailor its services to the needs of the community it serves.
We know the advantages of international cooperation and sharing knowledge and expertise. During response activities, sharing and cooperation is essential to limiting damage and quickly responding to new attacks. At other times such as international conferences and meetings, teams share lessons learned so that each can benefit from the experience of the others. GOVCERT.NL is one of the organizations that supports us in this drive with innovative products such as CERT-in-a-Box and in actively participating in the international network of response teams.

Rich Pethia, Director, CERT/CC

"Het is belangrijk om zicht te houden op de risico's die je loopt. Het loont de moeite om met relatief lage investeringen te onderzoeken waar de belangrijkste risico's liggen die aangepakt moeten worden. Het is de verantwoordelijkheid van het management om hierover helderheid te creëren. Oogkleppen helpen alleen om een paard rustig te houden."

René van der Veen, informatiebeveiliger bij het Ministerie van VWS

"AusCERT has had a close working relationship with GOVCERT.NL from its establishment 5 years ago. We have been there to help provide support to its capability and operations internationally from the outset. In turn, within a short period of time, we gained much from our relationship with GOVCERT.NL, which has been effective in supporting the work of AusCERT in Australia on many occasions.Already, we regard GOVCERT.NL as one of the leading CERTs in Europe and the world and look forward to building closer ties with GOVCERT.NL over the next 5 years and beyond."

Graham Ingram, General manager AusCERT (Australische CERT)

"Banken investeren veel in de veiligheid van Internet. Zij lichten hun klanten intensief voor over maatregelen die klanten zelf kunnen en moeten nemen. De gezamenlijke banken hebben hiervoor ook een website ingericht: www.veiligbankieren.nl.
Het samenwerkingsverband met GOVCERT.NL ondersteunt de banken in de strijd tegen cybercrime. De initiatieven met GOVCERT.NL, het "Notice and Take Down" experiment en de samenwerking in het informatieknooppunt financiële dienstverlening, worden als bijzonder waardevol ervaren. De Nederlandse banken gaan ervan uit dat deze initiatieven worden gecontinueerd en zonodig uitgebreid."

Michael Samson, Nederlandse Vereniging van Banken

3. To do list

Beveiliging van informatie betekent het beschermen van geheimen, van identiteit, van privacy en van dierbare herinneringen. Criminaliteit verschuift naar het digitale domein, maar we zijn zelf nog gewend aan oude risico's en aanvallen. Het wordt tijd om mee te bewegen en de risico's die het digitale leven bedreigen in ogenschouw te nemen en het hoofd te bieden. GOVCERT.NL heeft voor u een 'to do-list' voor informatie-beveiliging gemaakt, met in het achterhoofd de belangrijkste punten die in dit trend rapport aan bod zijn gekomen. Deze lijst is vooral bedoeld als startpunt.

We moeten samen voorkomen dat criminelen bij bedrijven en overheden een voet aan de grond krijgen. Actief op zoek gaan naar de zwakke plekken. GOVCERT.NL ondersteunt daarbij met respons bij incidenten en het stimuleren van samenwerking en kennisdeling. om incidenten te voorkomen.

- ☐ Reality check voor uw informatiebeveiligingsbeleid: is het er al? Is het vastgesteld? Is het up-to-date? En is het ook bruikbaar?
- ☐ Maak een overzicht van uw meest waardevolle informatie. Geef prioriteit aan het beschermen van deze informatie.
- ☐ Inventariseer met wie u informatie uitwisselt: toeleveranciers, klanten, overheden en anderen. Welke afspraken heeft u gemaakt en welke maatregelen heeft u genomen zodat dit op een vertrouwde en betrouwbare manier gebeurt?
- ☐ Wie heeft toegang tot welke systemen en welke informatie? Zijn de autorisaties ook correct geïmplementeerd?
- ☐ Communiceer met de gebruikers van uw diensten over gebruiks-, beveiligings- en privacy-aspecten.
- ☐ Werk aan bewustzijn: voorzie uzelf, uw medewerkers, klanten en directie van de juiste kennis over informatie-beveiliging. Het risico van zaken als identiteitsdiefstal, phishing-aanvallen en aanvallen met zero-days kan hiermee aanzienlijk verminderd worden.
- ☐ Denk na of en hoe misbruik en fraude bij uw (online) diensten gedetecteerd kunnen worden.
- ☐ Hoe gaat u om met klanten die beweren slachtoffer te zijn van identiteitsdiefstal?
- ☐ Doe aangifte van beveiligingsincidenten.
- ☐ Bescherm u niet alleen tegen binnenkomende, maar ook tegen uitgaande dreigingen van bijvoorbeeld geïnfecteerde computers op het bedrijfsnetwerk. Laat uw firewalls, virusscanners en intrusion detection systemen en andere technische oplossingen niet alleen inkomende maar ook uitgaande datastromen controleren.
- ☐ Zorg ervoor dat de systemen in uw organisatie zoveel mogelijk up-to-date zijn voor wat betreft beveiligings-updates.
- ☐ Ga na welke maatregelen getroffen zijn tegen incidenten die uw eigen of ingehuurde medewerkers kunnen veroorzaken. Het alleen beschermen tegen dreigingen van buitenaf is onvoldoende.
- ☐ Controleer of er aanvullende maatregelen mogelijk zijn tegen virussen en wormen. Voorkom dat de virusscanner op de computers de enige kurk is waarop de bescherming drijft.

Internetveiligheid

OPTA, de toezichthouder op de post- en telecommarkt in Nederland, vindt internetveiligheid een belangrijk aandachtspunt. Internetveiligheid vergroot het vertrouwen van eindgebruikers in internet en e-mail. Hieronder geeft OPTA haar beeld op de huidige situatie.

OPTA richt zich op twee aspecten van internetveiligheid. Het eerste aspect is ongewenste, ongevraagde en in grote hoeveelheden verzonden berichten of spam. Het tweede aspect is de opkomst van ongewenste software die zonder toestemming van de eindgebruiker wordt geplaatst op computers. Consumenten en aanbieders van elektronische communicatienetwerken worden hiermee onnodig belast.

Spam in Nederland stabiel

Uit onderzoek door een marktpartij naar de groei van spam blijkt dat Hong Kong, Singapore en Australië aanzienlijk meer belaagd zijn dan in 2005. Anderzijds hebben Zwitserland, Canada en de Verenigde Staten juist aanzienlijk minder last gehad van spam. Nederland bleef met ongeveer 50% stabiel ten opzichte van 2005. Veruit de meeste spam in Nederland wordt verstuurd door middel van e-mail. Fax- en SMS-spam komen wel degelijk voor, maar dit staat in geen verhouding tot voornoemde e-mail spam. Spam via automatische oproepsystemen komt het minst voor.

Ongewenste software

Ongewenste software heeft voor eindgebruikers indringende consequenties. De programmatuur voert voor de eindgebruiker onopgemerkte handelingen uit in dienst van een derde.
OPTA onderscheidt de volgende verschijningsvormen:

- Spyware, software die gevoelige informatie van eindgebruikers verzamelt zoals bankgegevens;
- Adware, software die ervoor zorgt dat de eindgebruiker van tijd tot tijd wordt lastig gevallen met advertenties;
- Traditionele virussen die schade veroorzaken op de computer van de eindgebruiker;
- Moderne virussen waarmee de controle over de computer wordt overgedragen aan een derde, bijvoorbeeld door middel van een Trojaans paard.

De meest voorkomende manieren voor het verspreiden van malware zijn e-mail, internetsites en gratis software. Nederland heeft wereldwijd een groot aandeel in het hosten van websites die spyware pogen te installeren. In 2006 was de spyware afkomstig van met name China, de VS, Nederland en Frankrijk. De hoge notering van Nederland als verspreider van spyware is opvallend. In het verleden (2004) scoorde Nederland even hoog op de lijst van spamverspreidende landen. Het percentage adware wereldwijd op besmette computers wordt geschat op 59%[21].

Virussen en spam

Veelal worden de virusvarianten gebruikt voor het creëren van een botnet. Deze netwerken worden door internet-criminelen gebruikt o.a. voor het verzenden van spam. Het voordeel hiervan is dat de verzender anoniem blijft. Grotere spamorganisaties maken dus gebruik van malware voor het effectief verzenden van hun boodschappen. Betrouwbare statistische gegevens over dergelijke netwerken zijn niet voorhanden. Onderzoek door overheid en marktpartijen wijst uit dat het gaat om miljoenen geïnfecteerde computers.

[21] Bron: Webroot, state of spyware

Woordenlijst

Adware
Adware is een naam voor kleine programma's die (soms zonder dat u het merkt) op uw computer worden geïnstalleerd. Het zit vaak bij gratis software. Adware kan pop-up advertenties in beeld laten zien, maar wordt ook gebruikt om na te gaan waar u zoal in geïnteresseerd bent op het internet. Alle pagina's die u bezoekt, houdt het adware-programma bij. Deze informatie kan vervolgens periodiek worden opgestuurd naar een leverancier die deze informatie vervolgens weer gebruikt om u gerichte reclame te sturen.

Bot
Het woord 'bot' komt van robot. Een bot is een programma dat zelfstandig 'geautomatiseerd werk' kan uitvoeren. Een bot kan onschuldig zijn, zoals zoekmachines bots gebruiken om websites in kaart te brengen. Maar een bot wordt echter ook gebruikt om andere, meer kwaadaardige handelingen te kunnen uitvoeren op computers. Zo kan een bot volledig toegang krijgen tot informatie op uw computer of hem gebruiken in criminele acties tegen anderen.

Botnet
Als uw computer is geïnfecteerd met een bot, maakt deze vaak onderdeel uit van een grootschalig en wereldwijd botnetwerk. Dit netwerk noemt men ook wel een botnet. Een persoon kan een botnet vanuit een centraal punt op het internet besturen. De besturing vindt meestal plaats via IRC (Internet Relay Chat).

Denial of Service (DoS)
DoS houdt in dat een computer continu 'aangevallen' wordt door bijvoorbeeld e-mail of bepaald netwerkverkeer. Het gevolg is dat de computer vastloopt of geen diensten meer kan leveren aan gebruikers. Zo'n aanval kan ook door een groot aantal andere computers tegelijk gebeuren. Dat heet Distributed Denial of Service (DDoS).

Exploit
Met behulp van een exploit (een klein programma) kan een kwaadwillend persoon misbruik maken van een kwetsbaarheid in programma's of besturingssysteem. Exploits voor bekende kwetsbaarheden zijn soms ook makkelijk te vinden op het internet.

IP-adres
IP-adres = Internet Protocol-adres. Elke computer die is verbonden met het internet heeft een uniek IP-adres, dat gebruikt wordt voor het bepalen van bestemming en herkomst van netwerkverkeer. kwetsbaarheden zijn soms ook makkelijk te vinden.

IRC
IRC = Internet Relay Chat, de elektronische babbelbox van het internet. Door in te loggen op een IRC-server kunt u met meerdere mensen tegelijk, of met één netgebruiker apart, communiceren door getypte boodschappen uit te wisselen. IRC bestaat uit zogenoemde kanalen die ieder hun eigen onderwerp hebben zodat gerichte discussies kunnen plaatsvinden.

IRC-Bot
Zie ook Botnets.
Een IRC-bot is een programma geschreven om een PC automatisch te laten verbinden naar met IRC-server. Zo'n programma kan hierna worden aangestuurd door de IRC-server voor het uitvoeren van commando's.

Keylogger
Een keylogger is een programma dat bijhoudt welke toetsen een gebruiker aanslaat. Deze gegevens kunnen vervolgens via internet of per e-mail onopgemerkt verstuurd worden naar een kwaadwillende. Keyloggers zijn een verschijningsvorm van spyware.

Kwetsbaarheid (vulnerability)
Een kwetsbaarheid is een zwakke plek in software of hardware, over het algemeen veroorzaakt door een programmeerfout. Een kwetsbaarheid kan misbruikt worden (zie ook exploit) door een internetcrimineel om de software te laten crashen of om de acties uit te laten voeren zoals het verwijderen van bestanden of toegang verlenen tot een computer.

Man-in-the-middle aanval
Een aanval waarbij de aanvaller zich tussen een klant en een dienst bevindt. Hierbij doet hij zich richting de klant voor als de dienst en andersom. Als tussenpersoon kan de aanvaller nu uitgewisselde gegevens afluisteren en/of manipuleren.

Malware
Samentrekking van malicious (Engels voor kwaadaardig) en software. Verzamelnaam voor slechte software zoals: virussen, wormen, Trojaanse paarden, keyloggers, spyware, adware en bots.

Phishing
Phishing ("vissen"), is een verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan direct worden misbruikt voor het doen van bijvoorbeeld grote uitgaven (in het geval van creditcardnummers) of voor wat in het Engels "identity theft" wordt genoemd, het stelen van een identiteit. In dit geval zijn bijvoorbeeld gegevens als sofi-nummers, adressen en geboortedata nodig.

Poort (Port)
Een poort is een gedefinieerd communicatiekanaal op een computer. Aan beide zijden van het communicatiekanaal "luistert" een programma.

Poort scan
Een scan van de poorten van een computer om snel een indruk te krijgen van welke diensten een computer allemaal gebruik maakt. Op basis daarvan kan een aanvaller bepalen welk soort kwetsbaarheden gebruikt kunnen worden voor een aanval.

Scam
De term "scam" wordt vrij losjes gebruikt voor allerlei soorten frauduleuze handelingen die erop gericht zijn om geld van mensen afhandig te maken.

Spam
E-mail die in grote hoeveelheden en ongevraagd wordt verstuurd. De inhoud van het bericht is verschillend en loopt uiteen van reclame tot het verzoek voor een financiële bijdrage. Bij spam gaat het niet om de inhoud van het bericht, maar om het grote volume van e-mailberichten dat verzonden wordt.

Trojaans paard (Trojan horse)
Een programma dat vermomd is als een legaal, onschuldig programma, maar daarnaast ongewenste functies uitvoert. Die functies zijn bedoeld om bijvoorbeeld de maker of verspreider van het programma ongemerkt toegang te geven of om schade toe te brengen.

Two-factor authentication
Een manier van inloggen, waarbij gebruik gemaakt wordt van twee van de drie volgende aspecten: iets dat de gebruiker weet (een wachtwoord of pincode), iets wat hij of zij heeft (een codegenerator of lijst met eenmalige codes) of iets wat hij of zij is (biometrische kenmerken, zoals een scan van de iris of een vingerafdruk).

Virus
Een virus is een klein programma bedoeld om al dan niet stiekem dingen te doen met een systeem waar de eigenaar niet om gevraagd heeft of die u niet wilt. Soms blijft het bij 'onschuldige' pop-up schermpjes, maar vaak zijn virussen erg gevaarlijk. De instellingen van een computer kunnen compleet geruïneerd worden, of de computer kan misbruikt worden om bijvoorbeeld e-mail te sturen aan duizenden mensen of om privé-bestanden klakkeloos te verspreiden. Virussen zijn er in vele soorten en maten.

Worm
Een worm is een programma speciaal gemaakt om zichzelf te verspreiden naar zoveel mogelijk computers. Een worm verschilt van een virus; een virus heeft namelijk een bestand nodig om zichzelf te verspreiden en een worm niet. Een worm heeft niet altijd schadelijke gevolgen voor uw computer, maar kan de verbinding wel langzaam maken.

Zero-day exploit
Code die misbruik maakt van een tot dan toe onbekende kwetsbaarheid.

Zombie-computer
Als een computer geïnfecteerd is met een bot , dan wordt er ook wel gesproken over een zombie-computer. De geïnfecteerde computer vormt onderdeel van een botnet en staat als een 'zombie' ter beschikking van een internetcrimineel.

Colofon

Dit trendrapport is een uitgave van GOVCERT.NL en is gebaseerd op gegevens uit de periode april 2006 tot en met april 2007.

Uitgave
juni 2007

Oplage
500

Redactie
GOVCERT.NL

Vormgeving
Ontwerpstudio aan het werk, Haarlem