Stratix

Onderzoek inzake Artikel 11.3 Tw

Concept Dreigingsbeeld

Door Stratix Consulting

Hilversum, Februari 2007

Stratix

Samenvatting

Dit rapport is de neerslag van een onderzoek naar een wijze van invulling van de norm in Artikel 11 lid 3 van de Telecommunicatiewet. De tekst en de bijbehorende toelichting van het artikel geven onvoldoende duidelijkheid van de reikwijdte en het verband van de verplichtingen in artikel 11.3.

Artikel 11.3 legt aan aanbieders van openbare elektronische communicatiediensten en netwerken de verplichting op om in het belang van de bescherming van persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen te nemen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen dienen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te garanderen dat in verhouding staat tot het desbetreffende risico.

In het tweede lid van artikel 11.3 staat dat aanbieders er zorg voor moeten dragen dat de abonnees moeten worden geïnformeerd over de bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst en de beschikbare middelen waarmee de bedoelde risico's kunnen worden uitgesloten of verkleind en de kosten die daarmee gemoeid zijn.

Het College van OPTA wil een aanpak ontwikkelen die een invulling van deze norm bewerkstelligt met als leidend uitgangspunt daarbij de gevaren voor de persoonlijke levenssfeer van de eindgebruiker. Over deze aanpak en invulling van de norm wil het College in gesprek met de marktpartijen die de wetgever volgens de Memorie van Toelichting en Handelingen in ieder geval op het oog had bij dit artikel: *Internet Service Providers*.

Vóór de start van het gesprek met de marktpartijen wil het College zich eerst een beeld vormen van de dreigingen die recente technologische ontwikkelingen voor de consument meebrengt en wat op dit moment als een passend beveiligingsniveau kan worden gezien. Op gebieden waar bedreigingen bestaan en waar bovendien voor de hand liggende en passende maatregelen tegen deze dreigingen bestaan, kan het College de norm van het artikel nader invullen. De wijze waarop, allereerst via bewustwording en uiteindelijk mogelijk door middel van handhaving, zal onderwerp zijn van het te voeren gesprek met de marktpartijen.

Het College heeft aan Stratix Consulting verzocht een vijftal interviews te houden met experts van marktpartijen. Aan deze experts is een viertal hoofdvragen voorgelegd:

1. Wat zijn de dreigingen nu?
2. Wat zijn de dreigingen die opkomen?
3. Wat wordt daar nu aan gedaan?
4. Wat kan er aan gedaan worden?

Daarnaast is de marktpartijen gevraagd te reflecteren op de mogelijke rol van de overheid en OPTA, waaraan het toezicht op en de handhaving van dit artikel is opgedragen.

Dit rapport bevat de neerslag van de vijf interviews en een formulering van een concept-dreigingsbeeld voor OPTA, waarmee het gesprek met marktpartijen geopend kan worden.

Hiervoor zijn de volgende experts van vijf marktpartijen geïnterviewd:
1. NLnet Labs, Olaf Kolkman en Jaap Akkerhuis
2. SURFnet, Jacques Schuurman
3. CAIW, Hans van der Giessen
4. Xs4all, Scott McIntyre en Simon Hania
5. InterNLnet, Paul Theunissen

Gezien de gevoeligheid van veiligheid en beveiligingsvraagstukken is alle te interviewen experts vooraf aangeboden op basis van anonimiteit te worden geïnterviewd. Iedereen heeft niettemin ervoor gekozen om 'on the record' te spreken. Wel is volgens afspraak het concept-rapport vooraf ter correctie aan hen voorgelegd. Hierbij is in enkele gevallen gebruik gemaakt om nog aanvullingen te maken.

Voor de interviews is een vragenlijst opgesteld door Stratix Consulting in overleg met OPTA. Bij deze vragenlijst is in de voorbereiding bij een aantal vragen een lijst van potentiële antwoorden opgesteld, echter de vragen zijn aan de geïnterviewden open gesteld om tot 'spontane' en niet tot 'geholpen' antwoorden te komen bij de te interviewen partijen. De geïnterviewden bleken daarbij de dreigingen op Internet vooral in een breder (conceptueler) kader te benaderen.

Het aan de hand van de interviews op te stellen concept-dreigingsbeeld bestaat uit de te verwachten dreigingen, een inventarisatie van de mogelijke passende maatregelen die aanbieders of eindgebruikers tegen het betreffende risico reeds nemen of nog kunnen nemen, alsmede aanbevelingen voor een vervolgaanpak. De bevindingen zijn als volgt:

Concept-dreigingsbeeld

Een analyse van de interviews leidt tot het volgende concept-dreigingsbeeld op hoofdlijnen:
De belangrijkste dreigingen voor de persoonlijke levenssfeer worden nu veroorzaakt door de besmetting van apparatuur bij Internet gebruikers met 'malware' waarmee hun PC's door hen veelal onopgemerkt worden overgenomen. Deze zogenaamde 'Zombie-PC's' worden ingezet in 'botnets' om bijv. Spam te verspreiden of Distributed Denial of Service attacks uit te voeren. Bij dit instrumentele gebruik wordt niet zozeer de persoonlijke levenssfeer van de eigenaar bedreigd maar die van andere gebruikers. Wanneer de indringer een zeer breedbandige (glasvezel-) aansluiting detecteert worden ze soms zelfs als stiekeme file-hoster van illegale content (video, muziek, gekraakte software) gebruikt.

Een bijzondere nu opkomende variant van 'malware' is zogenaamde 'crimeware', waarbij het de inbreker te doen is om ongemerkt identiteitsgegevens te verzamelen, o.a. door gebruikersnamen en passwords te loggen (Key-logging) en stiekem screendumps te maken van activiteiten op sites voor elektronisch bankieren. Dit raakt duidelijk wel de persoonlijke levenssfeer. De aangekondigde overheidsplannen voor een 'Digitale Kluis', waarin zeer waardevolle en privacy gevoelige identiteitsinformatie wordt opgeslagen, maakt deze inbreuk in de persoonlijke levens

sfeer in de toekomst extra bedreigend. Het concentreren van zeer veel cruciale gegevens op één plaats voor alle Nederlanders maakt dit voor een identiteitsdief een belangrijk uniform doelwit.

De belangrijkste verspreidingsmethoden voor 'malware' en 'crimeware' zijn via e-mail verspreide virussen en geïnfecteerde webpaginas of screensavers waar door middel van Spam- en nieuwsberichten naar verwezen wordt, die de software om de PC over te nemen, installeren. Nieuw op Internet aangesloten PC's met het Windows XP besturingssysteem worden al binnen een paar minuten door 'portsweeps' (veelal uitgevoerd door overgenomen PC's) gevonden en besmet, vaak nog voordat de eerste 'security update' is geïnstalleerd.

Spam speelt dus nog steeds een aanzienlijke rol, is het niet voor het verspreiden van virussen zelf, dan is het wel voor het rondsturen van hyperlinks naar geïnfecteerde websites. Er wordt hierbij primair ingespeeld op de onoplettendheid van veel gebruikers bij het 'klikken' op allerlei links, vooral als die vertrouwd overkomen. 'Phishing' is daarbij een vergaande wijze van inspelen op die onoplettendheid, waarbij nepsites van vertrouwde partijen worden voorgeschoteld en er zo gepoogd wordt identiteitsgegevens te verzamelen en/of stiekem malware te installeren.

Statistische gegevens over dreigingen uit internationale bronnen bevestigen het beeld uit de interviews. Daarbij valt op dat in Nederland opgestelde servers in de Top-10 doelwitten staan van Denial of Service aanvallen. Omgerekend naar aanvallen per dag per inwoner komt Nederland zelfs kort achter de VS en het VK uit en ver voor andere landen.

Nieuwe bedreigingen zien de ISP's vooral voortkomen uit inbraken in accounts voor betaalde diensten zoals VoIP en downloaden/streamen van audio/visuele media. De drijfveer achter de bedreigingen is in toenemende mate crimineel van aard en direct gericht op geld uit accounts te verzamelen of aan elektronische accounts gekoppelde tegoeden toe te eigenen.

Met de groei in populariteit van nieuwe toepassingen, zoals het lezen van weblogs, beluisteren van muziek en bekijken van video's, wordt ook gepoogd deze applicaties te gebruiken voor de verspreiding van 'malware' en deceptie van de eindgebruiker.

ISP's kunnen maatregelen nemen tegen een deel van deze dreigingen, door enerzijds hun gebruikers goed voor te lichten over de risico's van Internet, vooral de gevolgen van onnadenkend klikgedrag, anderzijds zijn er een aantal infrastructurele maatregelen mogelijk. De belangrijkste zijn:

- Het niet naar andere netten routeren van verkeer vanaf IP-adresssen die niet tot de eigen reeksen behoren.
- Het niet routeren van inkomend verkeer van IP-blokken die niet officieel zijn uitgegeven
- Aanbieden van virus- en Spamfilters[1] voor inkomende en eventueel uitgaande e-mail
- Blokkeren van de meest voor inbraken op PC's misbruikte poortnummers
- Eindgebruikers adviseren om (personal) firewalls te installeren of activeren

[1] De basis is daarbij het gebruiken van black- en whitelists, geavanceerd filteren is het wegen van e-mail op typische Spamkenmerken.

Over de wenselijkheid van het introduceren van DNS Security Extensions (DNSSEC) zijn de meningen verdeeld. Dit protocol lost een aantal beveiligingsproblemen op, maar één geïnterviewde ziet een risico ontstaan doordat de omvangrijkere berichten van DNSSEC de effecten van een DNS-Amplification aanval[2] verergeren en een ander vind het iets minder urgent.

Veel misbruik kan voorkomen worden als alle partijen (vooral ook zakelijke gebruikers met eigen systemen) hun servers en netwerken goed configureren. Dat is echter regelmatig niet de praktijk. Internet beveiliging en veiligheid vereist dat de toepasselijke partijen (providers, eindgebruikers, software/hardware fabrikanten) zich ervan bewust zijn en met maatregelen reageren op bekende bedreigingen. De aanwezigheid van veel fabrikanten als Intel, Microsoft e.a. in een internationaal coördinerend forum als FIRST[3] maakt duidelijk dat zij hun rol wat dit betreft serieus nemen. Internationale organisaties van Internettechnici hebben de details om (tegen-) maatregelen goed te implementeren beschreven in verscheidene Best Current Practices (BCP) documenten. Daarnaast heeft een aantal veiligheidsdeskundigen van ISP's in Nederland zich verzameld in het Operationeel Incident Response Team Overleg (o-IRT-o), waar informatie wordt uitgewisseld over incidenten en maatregelen.

ISP's hebben een relatief beperkte invloed op het applicatiegebruik en klikgedrag van hun gebruikers en de mate van beveiliging van hun PC's. De meeste mogelijkheden om bedreigingen te beïnvloeden liggen bij de veiligheid van de eigen systemen en diensten. Het inzetten van speciale diagnostieke hulpmiddelen als 'honeypots', 'intrusion detection systems' en systemen om verkeer te bemonsteren op abnormale patronen die veiligheidsproblemen signaleren is vooral doorgevoerd bij de grootste ISP's. Vergaande oplossingen als een 'quarantainenet'[4], waarmee besmette of nieuwe PC's worden geïsoleerd tot ze voldoende beschermd zijn, zijn topologie en technologie afhankelijk. De specifieke oplossing van het Twentse bedrijf *Quarantainenet* wordt aangemerkt als prijzig en wordt selectief ingezet. Het concept quarantaine wordt echter als nuttig aangemerkt.

Een beperktere versie van het quarantainenet is de 'Walled Garden' om nieuwe apparatuur en gebruikers een authenticatieslag te maken voordat de dienstverlening definitief start. Pas daarna komt men op het publieke Internet terecht. Die scheiding van publiek en niet-publiek neemt toe met de nieuwe betaaldiensten als VoIP en IPTV. Met betrekking tot VoIP zijn er onder de geïnterviewden zowel implementaties gerealiseerd over het publieke Internet, naast afwikkeling van deze dienst over een apart niet publiek deel van het netwerk, waardoor er vermeden wordt dat het VoIP-deel in het modem rechtstreeks benaderd kan worden.

OPTA heeft tot slot geïnterviewden gevraagd op haar mogelijke rol te reflecteren. Diverse geïnterviewden hebben de indruk dat OPTA Artikel 11.3 Tw erg breed uitlegt. Één

[2] Een aanval, waarbij DNS-servers van derden worden misbruikt om een doelwit over te belasten.

[3] Forum of Incident Response and Security Teams, een in 1990 opgericht forum waarin coördinatie en communicatie tussen incident response teams plaats vindt.

[4] Het concept 'quarantainenet', betreft het detecteren en daarna isoleren van niet goed functionerende aangesloten systemen. Het Twentse bedrijf Quarantainenet levert een oplossing onder dezelfde naam.

geïnterviewde interpreteerde het eerste lid vooral als een eis dat een ISP zijn eigen systemen op orde moet hebben, zodat er niet snel op wordt ingebroken, of de gegevens van de systemen op straat komen te liggen, waardoor privacy of persoonlijke levenssfeer van hun abonnees in gevaar komt. Hij las het tweede lid vooral als een verplichting dat, mocht er toch zo'n inbreuk plaatsvinden, de ISP zijn gebruikers onmiddellijk en ter zake informeren over de (ernst van de) inbreuk en de mogelijke maatregelen om nadelige gevolgen tegen te gaan.

Dit is vermoedelijk een iets te beperkte interpretatie. Echter de hoofduitkomst van de vragen naar handhaving van Artikel 11.3 Tw door OPTA is dat ondervraagden niet inzien waarom die handhaving nu urgent is. Men vindt het onderwerp echter wel belangrijk. Zij zijn over het geheel terughoudend ten opzichte van het opleggen van verplichte maatregelen aan de bedrijfstak als geheel, zeker als die voorafgaan aan het opleggen van handhaving bij specifieke partijen die slecht hun zaken op orde hebben.

Als eerste stap is onder meer aangegeven dat het verstandig is dat OPTA het veld eens bij elkaar brengt. Daarbij zijn onder meer de volgende aanbevelingen afgegeven:

- OPTA zou als eerste activiteit kunnen gaan meelopen in het veld (bijvoorbeeld bezoeken van relevante bijeenkomsten van RIPE etc.), daarnaast de kennis te verrijken en de goede ontwikkelingen te benoemen.
- OPTA zou een blauwdruk kunnen maken met BCPs en dat onderhouden, daar moet dan een redactiecommissie voor worden opgezet die dat werk gaat doen. Dit zou men kunnen vragen aan het o-IRT-o, maar ook het ECP.NL[5] heeft een taak daarin. OPTA kan daar dan zijn wettelijk mandaat aan binden. Er speelt echter wel een representatievraagstuk, enkele grote marktpartijen zijn geen lid van voornoemde organisaties.
- In het vervolgtraject is het verstandig als OPTA een scherp onderscheid gaat maken tussen de begrippen *beveiliging* [Eng. security] en *veiligheid* [Eng. safety]. Politici hebben de neiging om beiden in de discussies op één hoop te gooien. ISP's kunnen de *beveiliging* van hun systemen en netwerken op orde hebben, maar hebben bij hun klanten vooral de mogelijkheden om de *veiligheid* te beïnvloeden.
- Veel geïnterviewden zien risico's bij een te formalistische aanpak van de handhaving. De wijze van introductie, oplegging, handhaving en kostenvergoeding die de overheid hanteert bij bijvoorbeeld aftappen, gegevensverstrekking en dataretentie nodigt volgens de ISP's niet in alle gevallen uit om de sector mee te krijgen. De belangen moeten duidelijk in lijn liggen. Er is een 'arms race' aan de gang waarbij dreigingen constant veranderen door de genomen tegenmaatregelen, hierdoor is er een risico dat OPTA 'altijd te laat reageert'. OPTA kan zich daarbij het best richten op maatregelen neergelegd in de al in internationale fora opgestelde Best Current Practices die zijn gebaseerd op open standaarden.

Geïnterviewden zien op het vlak van voorlichting aan eindgebruikers nog steeds een rol voor het Ministerie van EZ. Het is, gezien de penetratie van internettoegang, niet zo effectief daar de ISP's bij in te schakelen; beter kan materiaal huis-aan-huis worden verspreid, ondersteund door een campagne. Daarnaast kan OPTA de sector ook helpen door aanpassingen van de wetgeving bij de overheid te agenderen, waar die dreigingen onbedoeld bevordert. Een voorbeeld is het

[5] ECP.NL: Electronic Commerce Platform Nederland

afdichten van de Colportagewetgeving, zodat zaken als ‘Domaintasting’[6] niet ook in Nederland als praktijk worden geïntroduceerd na invoering van elektronische orderverwerking voor ‘.nl’ domeinnamen. ‘Domaintasting’ bemoeilijkt onder meer de opsporing van Spam-verzenders en ‘rogue websites’.

Door alle geïnterviewden is aangegeven dat zij op de hoogte gehouden willen worden en bereid zijn te participeren in vervolg discussies die OPTA wil entameren over Artikel 11.3 Tw.

[6] ‘Domaintasting’ is de praktijk dat partijen honderdduizenden domeinnamen enkele dagen uitproberen en dan retourneren.

Stratix

Inhoudsopgave

Stratix

1 Inleiding

OPTA heeft het voornemen de toepassing van artikel 11.3 van de Telecommunicatiewet (Tw) nader te onderzoeken, omdat internettechnologie een steeds grotere rol gaat spelen binnen de telecommunicatiemarkt en dit grote gevolgen kan hebben voor de persoonlijke levenssfeer (de privacy) van eindgebruikers.

Artikel 11.3 van de Tw luidt als volgt

Artikel 11.3

1. De in artikel 11.2 bedoelde aanbieders treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico.
2. De in artikel 11.2 bedoelde aanbieders dragen er zorg voor dat de abonnees worden geïnformeerd over:
   a. bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst;
   b. de eventuele middelen waarmee de onder a bedoelde risico's kunnen worden tegengegaan, voor zover het andere maatregelen betreft dan die welke de aanbieder op grond van het eerste lid gehouden is te treffen, alsmede een indicatie van de verwachte kosten.

Hierbij wordt verwezen naar het voorgaande artikel 11.2 Tw dat luidt:

Artikel 11.2

Onverminderd de Wet bescherming persoonsgegevens en het overigens bij of krachtens deze wet bepaalde dragen de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst zorg voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van zijn netwerk, onderscheidenlijk zijn dienst.

1.1 Reden onderzoek inzake Artikel 11.3 Tw

De wetstekst en de bijbehorende Memorie van toelichting van het artikel geven onvoldoende duidelijkheid over de reikwijdte en het verband van de verplichtingen in artikel 11.3, maar de opkomst van VoIP en het toenemend belang van datacommunicatie met behulp van het Internet Protocol maken dat de eindgebruikers steeds alert moeten zijn op de beveiligingsapparatuur en

software en dat de aanbieders daarbij, conform het artikel, steeds de persoonlijke levenssfeer moeten waarborgen, voor zover zij daartoe gehouden zijn.

Uit de toelichting en de handelingen van de Kamer kan worden afgeleid dat het oogmerk van de wetgever was om deze zaken in een later stadium te laten invullen. De formulering van het artikel, maakt het in principe ook een 'moving target'. Zowel de bedreigingen van de persoonlijke levenssfeer, als ook de stand van de techniek in de beveiliging ertegen en de daarmee gemoeide kosten veranderen in de dynamische omgeving, vooral qua applicaties, die het openbare Internet is.

OPTA wil een aanpak ontwikkelen die een invulling van deze norm[7] bewerkstelligt met als leidend uitgangspunt daarbij de gevaren voor de persoonlijke levenssfeer van de eindgebruiker. Hiervoor is het noodzakelijk dat het college zich eerst een beeld vormt van de dreigingen die recente technologische ontwikkelingen voor de consument meebrengt. Het college kan de norm nader invullen op gebieden waar dergelijke dreigingen bestaan en waar bovendien voor de hand liggende en passende maatregelen tegen de betreffende dreigingen bestaan.

Het college heeft daarbij het oogmerk om de (digitale) veiligheid van eindgebruikers te blijven garanderen door deze norm allereerst via bewustwording , stimulering, beleidsvorming en uiteindelijk, mocht dat noodzakelijk blijken, mogelijk door middel van handhaving te gaan gebruiken. Daarbij sluit hij niet uit dat men uiteindelijk beleidsregels zal opstellen om de norm nader in te vullen.

Het onderzoek is bedoeld om tot een concept-dreigingsbeeld te komen dat OPTA in een latere fase met een grotere groep vertegenwoordigers uit de markt wil bespreken en aan de verkregen inzichten aanpast. Afhankelijk van de uitkomsten daarvan kan het college daarna voorlichtingsacties definiëren, beleid opstellen en (in een later stadium) de gestelde normen handhaven, indien nodig.

Het op te stellen concept-dreigingsbeeld dient te bestaan uit de te verwachten dreigingen, een inventarisatie van de mogelijke passende maatregelen die aanbieders of eindgebruikers tegen het betreffende risico reeds nemen of nog kunnen nemen, alsmede aanbevelingen voor een vervolgaanpak.

1.2 Aanpak en geïnterviewden

Voor het opstellen van het concept-dreigingsbeeld is gekozen voor interviews met deskundigen uit de bedrijfstak.

Het College aan Stratix Consulting verzocht een vijftal interviews te houden met deskundigen van marktpartijen. Aan hen is een viertal hoofdvragen voorgelegd:

[7] OPTA hanteert hier het juridisch begrip 'norm' in de onderzoeksvraagstelling, de aanbieders zien dit als een verplichting.

1. Wat zijn de dreigingen nu?
2. Wat zijn de dreigingen die opkomen?
3. Wat wordt daar nu aan gedaan?
4. Wat kan er aan gedaan worden?

Daarnaast is de marktpartijen gevraagd te reflecteren op de mogelijke rol van de overheid en OPTA, waaraan het toezicht op en de handhaving van dit artikel is opgedragen.

Hiervoor zijn de volgende zeven experts van vijf marktpartijen geïnterviewd:

1. Olaf Kolkman, Directeur van NLnet Labs en lid van de Internet Architecture Board,
2. Jaap Akkerhuis, onderzoeker bij NLnet Labs en lid van de Security and Stability Advisory Committee (SSAC) van de Internet Corporation for Assigned Names and Numbers (ICANN).
3. Jacques Schuurman, account adviseur bij SURFnet en hoofd van het SURFnet-Computer Emergency Response Team (SURFnet-CERT)
4. Hans van der Giessen, directiesecretaris bij CAIW Holding
5. Scott McIntyre, Security Officer bij Xs4all en lid van het Steering Committee van het Forum of Incident Response and Security Teams (FIRST)
6. Simon Hania, Technisch Directeur bij Xs4all.
7. Paul Theunissen, Technisch Manager bij InterNLnet

Dit rapport bevat de neerslag van de vijf interviews en een formulering van een concept-dreigingsbeeld voor OPTA, waarmee het gesprek met marktpartijen geopend kan worden.

Gezien de gevoeligheid van veiligheid en beveiligingsvraagstukken is alle te interviewen experts vooraf aangeboden op basis van anonimiteit te worden geïnterviewd. Echter iedereen heeft ervoor gekozen om ‘on the record’ te spreken. Wel is het concept-rapport vooraf aan hen voorgelegd.

Voor de interviews is een vragenlijst opgesteld door Stratix Consulting in overleg met OPTA. Bij deze vragenlijst is in de voorbereiding bij een aantal vragen een lijst van potentiële antwoorden geformuleerd. Als techniek is echter gekozen om de vragen aan de geïnterviewden open te stellen om zo tot ‘spontane’ en niet tot ‘geholpen’ antwoorden te komen bij de te interviewen partijen. Dit heeft tot het effect geleid dat enkele geïnterviewden aanzienlijk abstracter over het dreigingsbeeld antwoorden dan anderen.

Wanneer potentiële antwoorden uit de voorbereiding / deskresearch niet werden genoemd dan werd daar aan het eind van de tweede groep vragen over dreigingen die opkomen alsnog naar gevraagd.

1.3 Inrichting rapport

De inrichting van het rapport is als volgt. In hoofdstuk 2, 3, 4 wordt op de hoofdvragen van de interviews ingegaan, in hoofdstuk 5 wordt gereflecteerd op de rol van OPTA en overheid en in hoofdstuk 6 worden conclusies en aanbevelingen samengevat. De hoofdstukken geven een

overzicht van de belangrijkste interviewuitkomsten en analyse van Stratix. In de bijlagen vindt u de gehanteerde vragenlijst en daarna wordt van iedere partij een gedetailleerd interviewverslag geleverd.

2 Wat zijn de dreigingen nu?

In dit hoofdstuk wordt in twee stappen beschreven wat de dreigingen zijn die nu spelen. Eerst wordt een beeld op hoofdlijnen geschetst van de bevindingen in de interviews. Daarna volgt een kort analytisch beeld van de huidige dreigingen op basis van die gesprekken en achtergrondkennis bij Stratix.

2.1 Bevindingen uit interviews op hoofdlijnen

In de gesprekken bleek dat diverse marktpartijen inderdaad het soort concrete dreigingen benoemde, die van tevoren werden verwacht. Echter een aantal van de geïnterviewde experts bleek de dreigingen op Internet aanzienlijk abstracter te benaderen. Wanneer providers of eindgebruikers op structurele schaal passende technische en organisatorische maatregelen nemen ten behoeve van de veiligheid en beveiliging, schakelen de partijen die de problemen veroorzaken namelijk al snel over op nieuwe varianten. De dreigingen zijn daardoor een ‘moving target’ en concrete passende maatregelen kunnen vooral worden gezien als het implementeren van aanbevelingen die genoemd staan in ‘Best Current Practices’ (BCP). Hierbij is BCP-38 meerdere keren als belangrijke aanbeveling, genoemd die ingaat op het beheersen van de communicatie die een net uitgaat (egress)

De interviews samenvattend kan worden gesteld dat de grootste dreiging op dit moment samenhangt met het kapen (overnemen) van computers, die daarna worden ingezet als ‘Zombie-PC’ in botnets ten behoeve van het verspreiden van Spam of gaan functioneren als ‘slave’ van een ‘master’, waarmee de kapers bijvoorbeeld een ‘Distributed Denial of Service attack’ uitvoeren. Ook zijn diverse methoden genoemd om gevoelige gegevens van gebruikerssessies te registreren en naar centrale verzamelpunten te sturen via ‘Key-logging’ of stiekeme ‘Screen dumps’. Eén van de geïnterviewden schatte op basis van gedrag en sporen die zij waarnemen op hun netwerk dat in Nederland ongeveer 200 duizend PC’s met logging software zijn geïnfecteerd. Dit is een groot risico voor identiteitsdiefstal, omdat de logger geïnstrueerd kan worden om screendumps door te sturen van opgevraagde webpagina’s van elektronisch bankieren, of de nieuw in te richten digitale kluizen van de Nederlandse overheid. Aanbieders van deze informatie (e.g. de website van de bank of de digitale kluis van de overheid) kunnen zich door het nemen van maatregelen aan de serverzijde niet beveiligen tegen gegevensdiefstal via screendumps. Men moet de privacy gevoelige gegevens nu eenmaal leesbaar maken voor de gebruiker op het scherm, die komt dan dus ook leesbaar in de screendump. De ISP heeft ook geen rol, in de dienst zelf die ziet een vertrouwelijke sessie tussen PC van de klant en de server.

Een ISP zou hier, als men zich laat informeren door de internationale security gemeenschap, mogelijk wel symptomen kunnen herkennen en daarvoor infrastructuur kunnen bouwen om sommige zaken te detecteren en af te stoppen, maar dit punt is een lastige balans tussen privacyinbreuk versus gedrag van de ISP die als een goede Internet citizen misbruik probeert te voorkomen. Keylogging en stiekem screendumps maken van notoir gevoelige websites zijn erg gerichte inbreuken. Het ontbreken van massaliteit maakt detectie bijzonder lastig.

Het overnemen van computers, of stiekem installeren van loggers gebeurt meestal door infectie met 'Malware' die via webpagina's door veel gebruikers ongezien of onbegrepen worden geïnstalleerd op hun PC, Spam zelf is, vooral met mailvirussen, ook nog steeds een grote verspreidingsbron van de software, waarmee PC's overgenomen kunnen worden.

Om 'Malware' te installeren zijn voortdurend partijen op Internet partijen actief met 'portsweeps'[8] (veelal uitgevoerd door besmette PC's) om onbeschermde nieuwe computers te detecteren die ze kunnen infecteren. Een nieuw geïnstalleerde PC met Windows XP, die nog niet op het niveau van Service Pack 2 is gebracht, is praktisch *binnen 2 minuten gecompromitteerd*, wanneer die PC op het open Internet wordt aangesloten. Dit is door één ISP bij proefnemingen geconstateerd en andere geïnterviewden gaven vergelijkbare tijden op. Enkele minuten is beduidend korter dan de tijd die nodig is om de Service Packs met betere beveiliging via Windows Update automatisch te laten installeren. Fabrikanten hebben op dit vlak een grote verantwoordelijkheid om zo up-to-date mogelijk uit te leveren en niet het retailkanaal vol te laten zitten met kwetsbare configuraties gezien de lange downloadtijd t.o.v. de infectietijd.

Alle geïnterviewden nemen bij de veroorzakers van de veiligheidsproblemen een toenemende criminalisering (en daarmee professionalisering) waar. Dit verandert de aard van de dreigingen. Voor een 'crimineel' is het onzichtbaar werken bij het overnemen van PC's namelijk van groter belang dan voor een 'vandaal'. Criminelen prefereren sluipende infecties van systemen bij eindgebruikers. De geïnfecteerde machines worden nu het grootste deel van de tijd slapend gehouden of er wordt slechts een beperkt deel van de capaciteit gebruikt. Hierdoor is detectie veel moeilijker.

2.2 Huidige dreigingen, een beeld

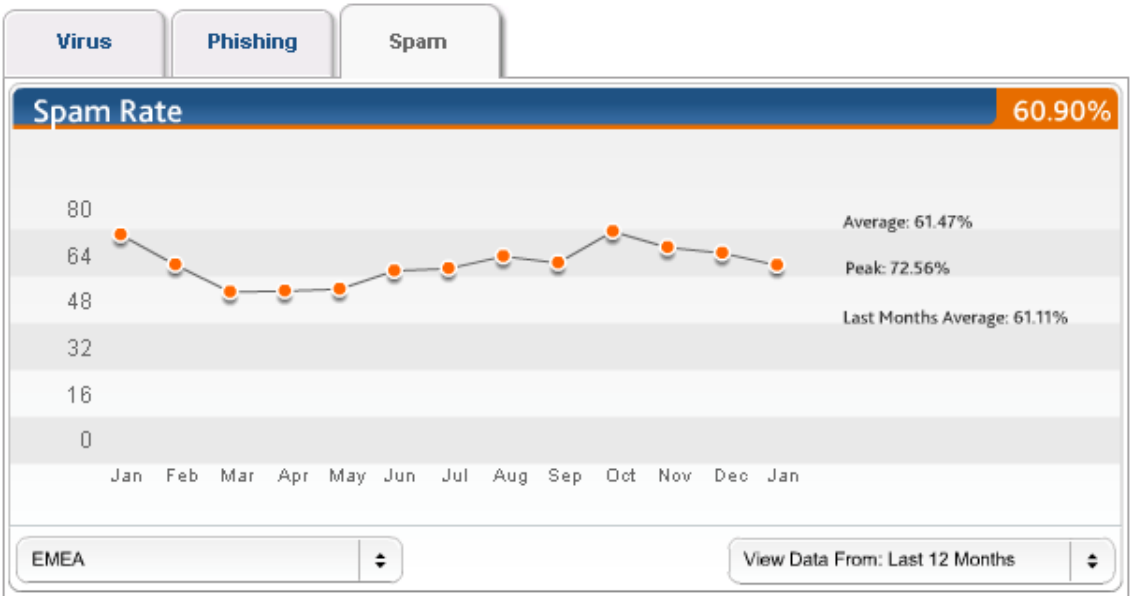
Over de huidige dreigingen kan men het snel eens worden. De verspreiding via Spam en 'rogue websites' van allerlei soorten virussen, vooral met het oogmerk botnets te vormen, die dan weer als deel van een vicieuze cirkel ingezet worden voor verdere verspreiding van deze *cyber-ellende*. Dit beeld wordt ook door openbare bronnen bevestigd. We nemen ze op de volgende pagina nog eens door.

2.2.1 Spam (incl. blogspam)

Spam is nog steeds een zeer fors probleem. Enkele dagen voor Kerst 2006 kwamen de berichten van ISP's in de media dat de mailsystemen al dagen een soort Kerststormloop van Spam moesten doorstaan en dat er grote storingen optraden[9]. Blogspam leek in 2005 even een serieus probleem te worden, echter het is nu vooral een irritatie. Veel populaire blogs hebben maatregelen getroffen ten aanzien van authenticatie, door een account te vereisen of het intypen van een code, weergegeven in grafische plaatjes. Op dit punt waren beperkte technische

[8] Een portsweep probeert vele ISP adressen uit op één poortnummer (bijv. port 135/tcp)
[9] ANP, 22 december 2006, Internetaanbieders in de problemen door spam

ingrepen op de blogsites effectief. Spam via e-mail domineert daardoor nog steeds deze dreigingsdiscussie. Figuur 1 toont het percentage Spam in de e-mail gemeten over de EMEA-regio door de e-mail filter service provider Messagelabs.



Bron: Messagelab.com Threat Watch

Figuur 1 *Spamstatistieken voor 2006 tonen piek in Oktober voor de EMEA-regio*

Messagelabs heeft veel zakelijke klanten, waardoor op consumenten georiënteerde ISP's aanzienlijk hogere volumes kunnen meten. Symantec, het grootste security software bedrijf, heeft een vergelijkbare dochter, Brightmail. Het bedrijf maakt halfjaarlijkse een uitgebreid Internet Security Threat Report[10] voor de gehele wereld. Het mat voor de eerste helft van 2006 een Spamgemiddelde van 54% van alle e-mail. Dit komt vrij goed overeen met de metingen van Messagelabs, waar het wereldgemiddelde een paar procent onder dat van de EMEA regio ligt.

Tabel 1 *Top-10 bronlanden van spam*[10]

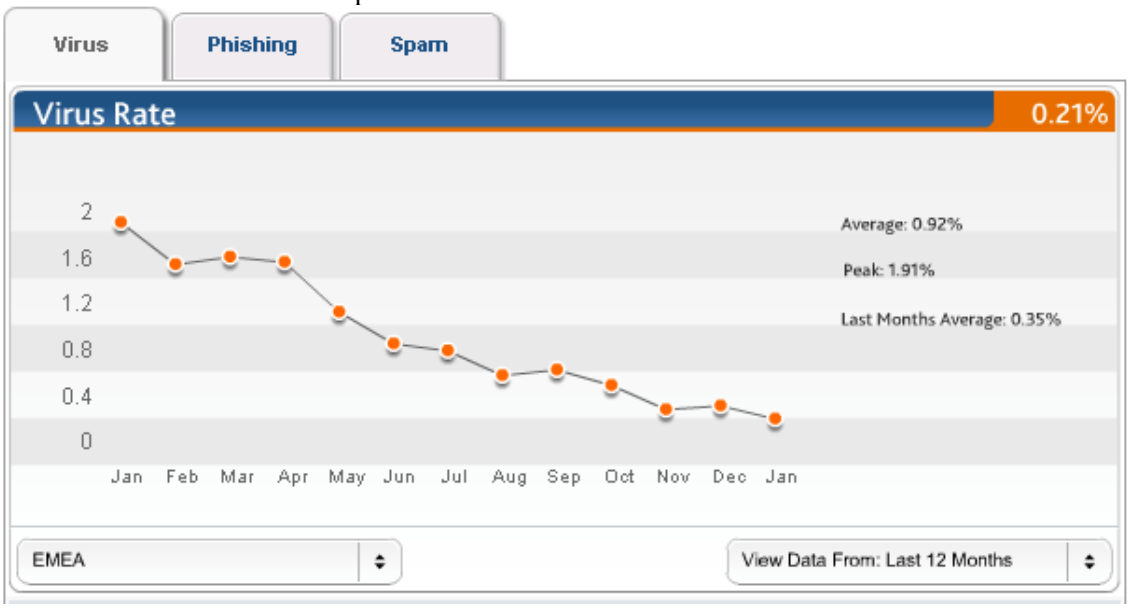
Land	Jan–Jun 2006	Jul–Dec 2005
VS	58%	56%
China	13%	12%
Canada	5%	7%
Zuid Korea	5%	9%
VK	4%	3%
Rest van de EU	4%	2%
België	4%	4%
Japan	3%	3%
Frankrijk	2%	2%
Polen	2%	n.b.

[10] Bron is de editie september 2006, die de 1e helft van 2006 beschrijft: http://www.symantec.com

Door het grootschalig gebruik van botnets liggen de meeste bronnen van spam in landen met veel breedbandaansluitingen. De VS is daardoor weer omhoog geschoten als fysieke bron van spam. Tabel 1 laat vooral een opvallend hoge positie van België zien. Nederland valt, net als de meeste Scandinavische landen in de categorie rest van de EU.

2.2.2 Virussen en wormen (mail, web, etc)

Wormen en virussen zijn een groot probleem, omdat ze PC's compromitteren en ze veranderen in Zombie PC's die deel gaan uitmaken van een botnet of de machine infecteren met logging software. De wormen zijn daarbij vaak ook dusdanig agressief met 'portsweeps' dat nieuwe machines die op Internet worden aangesloten al volledig 'dicht' moeten staan met personal firewalls. De meeste kunnen zich op meerdere wijzen verspreidden. Symantec maakt uit een studie van de 50 meest voorkomende op dat 98% zich via SMTP verspreiden kan. Het aantal dat wordt gedetecteerd in de virusscanners daalt echter trendmatig. Figuur 2 laat zien dat wormen en virussen steeds minder verspreid worden via massale uitbraken.



Bron: Messagelab.com Threat Watch

Figuur 2 *Virusstatistieken voor mailservers tonen sterk afnemende trend*

2.2.3 Zombie-PC's / botnets

Met wormen en virussen worden veel botnets gecreëerd. Het gemiddelde aantal actieve botnet computers dat Symantec in het eerste halfjaar van 2006 detecteerde bedroeg 4.696.903. Het gemiddelde aantal dat per dag actief was bedroeg echter 57.717. Het aantal actieve botnet computers stabiliseerde zich in de eerste helft van 2006 (zie Figuur 3). Uit het daggemiddelde en halfjaartotaal valt af te leiden dat de gemiddelde botnet computer niet veel meer dan 2 dagen actief is. Botnets worden beheerst door command-and-control servers. Symantec heeft in de eerste helft van 2006 er 6.337 gedetecteerd met zijn systemen, waarvan 42% zich in de Verenigde Staten bevonden.

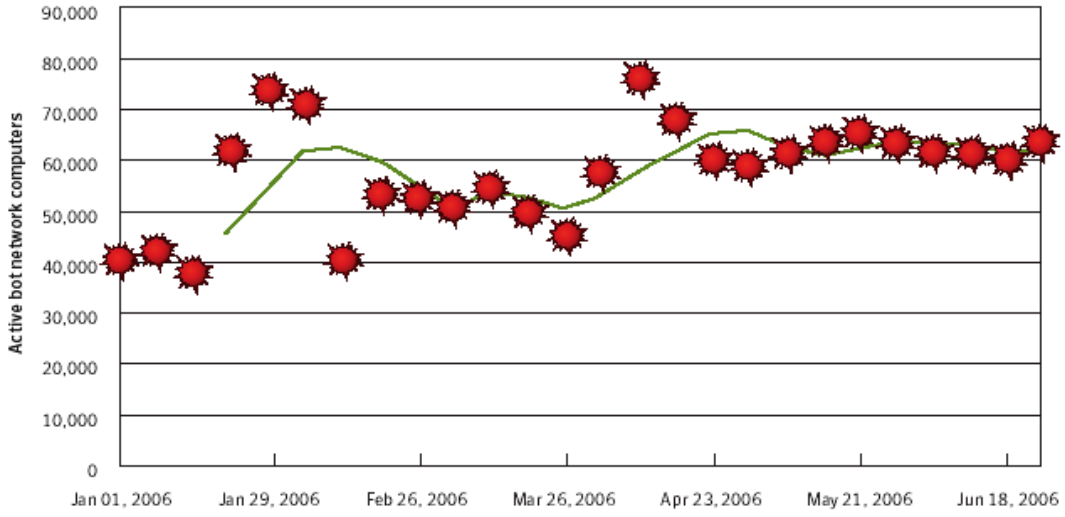


Figure 6. Active bot network computers per day
Source: Symantec Corporation

Figuur 3 *Gemiddeld aantal actieve botnetcomputers stabiliseert in 1H2006*

De verspreiding van actieve botnet computers dat door die 6.337 servers beheerst werd is afgebeeld in Figuur 4 en laat zien dat China de meeste geïnfecteerde PC's heeft. Ook Brazilië scoort zeer hoog. De oorzaak hiervan wordt meestal gezocht in het feit dat men in die landen massaal met illegale Microsoft Windows kopieën werkt, waar geen automatische security updates mee mogelijk zijn.

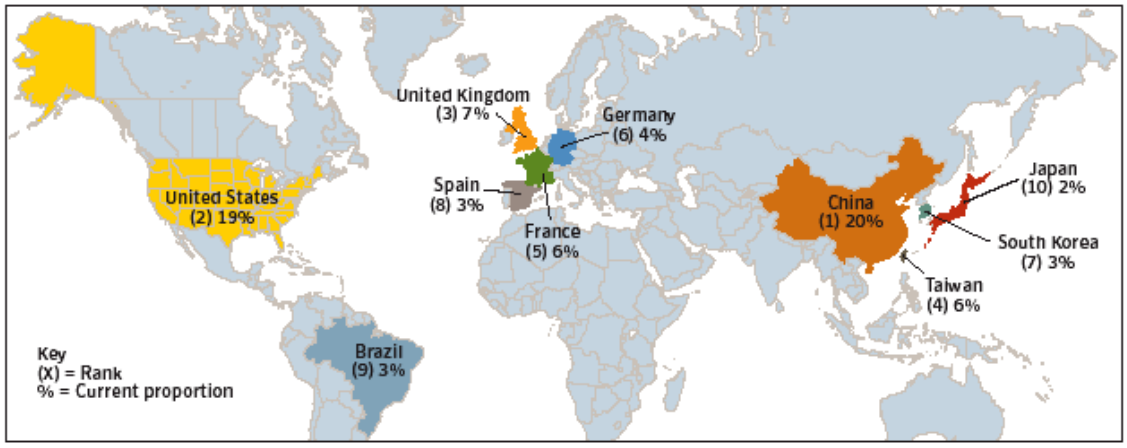
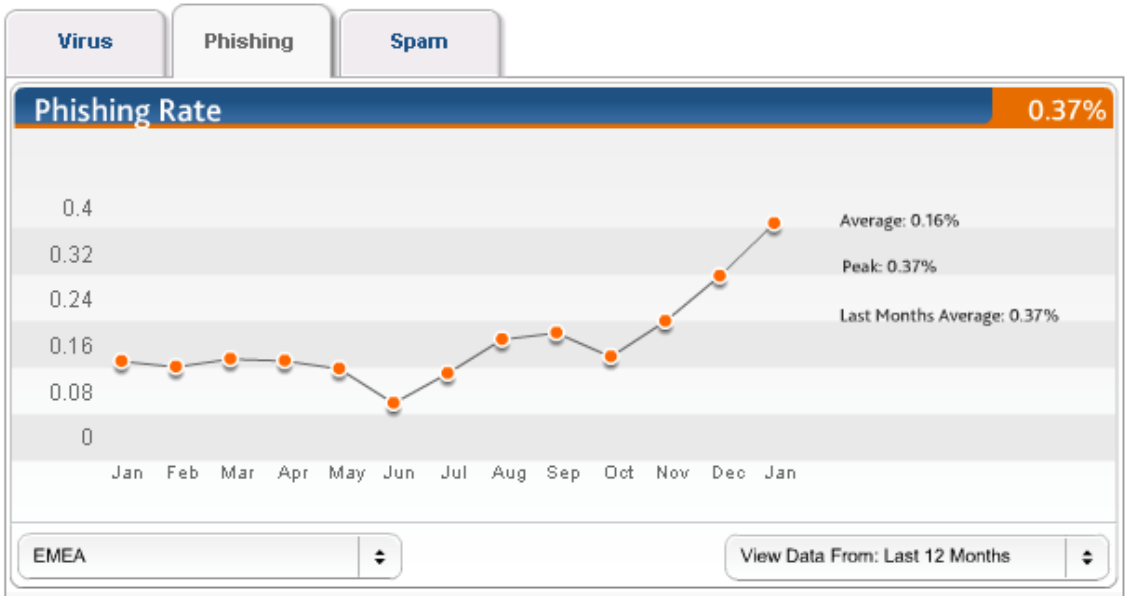


Figure 13. Top countries by bot-infected computers
Source: Symantec Corporation

Figuur 4 *Spreiding van actieve botnetcomputers over de wereld 1H2006, top-10 landen*

2.2.4 Phishing / Trojan sites

In tegenstelling tot de verminderende virusbesmetting en het zich stabiliserende spam percentage (dat wil niet zeggen dat de absolute mailflow stabiliseert) is Phishing sterk in opkomst. Dit wordt goed zichtbaar in de statistiek die is afgebeeld in Figuur 5.



Bron: Messagelab.com Threat Watch

Figuur 5 *Phishingstatistieken tonen sterke groei sinds de zomer.*

Phishing werkt veelal in combinatie met genepte websites om identiteitsgegevens informatie van bezoekers te ontfutselen. Vaak wordt er van de Trojaanse website ook nog software gedownload om gegevens te stelen of te loggen. Dit is de volgende categorie cyberrommel.

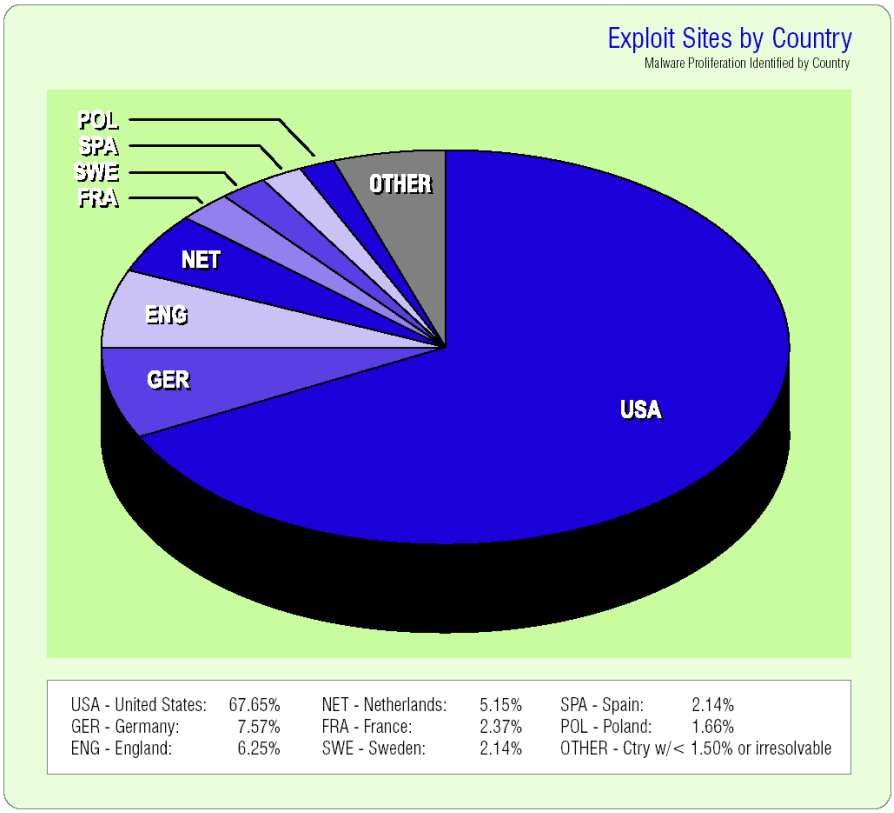
2.2.5 Malware

Een programma dat onzichtbaar wordt geïnstalleerd bij een bezoek aan een website, kan vele vormen aannemen en vervult meestal veel functies, de generieke naam hiervoor is *malware*. Kwantitatieve gegevens over de omvang van dit fenomeen zijn beperkt. Webroot, een leverancier van anti-spyware software, stelt in zijn kwartaalrapportage[11] dat het aantal nieuw gevonden traces in het tweede kwartaal ruim 10.000 bedroeg, wat het totaal op 144 duizend bracht. In het eerste kwartaal waren er ruim 14.000 nieuwe traces gevonden.

Een nog niet zo schadelijke versie van *malware* installeert bijvoorbeeld extra zoekbalken met advertenties of past de homepage voor de browser aan: *adware*. Echter veelal volgt het programma ook het browsegedrag van de gebruiker, welke privacygevoelige informatie wordt verstuurd naar een centrale site dan spreekt men vaak van *spyware*. Hoewel die naam vaak ook generiek wordt gebruikt. Verdergaande varianten worden ook wel aangeduid als *crimeware*. Hierbij is men uit op diefstal van allerlei identiteitsgegevens en worden bijv. de toetsenbord-aanslagen gelogd en doorgezonden (*system monitors* of *keyloggers*), of er worden screendumps

[11] State of Spyware: http://www.webroot.com/pdf/2006-q2-sos-US.pdf

gemaakt van de bezochte pagina's, doel is dan veelal om credit card en andere identiteitsgegevens te verzamelen. Een variant van malware die de afgelopen jaren veel problemen veroorzaakte is de *dialer*, die vaak ongemerkt het inbelnummer veranderde in een duur 090x nummer of een buitenlands nummer. Ook met een breedband PC wil dat nog wel succes hebben, omdat de telefoonlijn regelmatig aangesloten blijft op het modem voor het versturen van faxen.



Bron: Webroot: State of SpywareL Q2 2006

Figuur 6 *Webroot vindt dat ruim 5% van alle spyware uit Nederland komt*

Een groot deel van de malware en crimeware wordt geïnstalleerd bij bezoek van onbetrouwbare (*rogue)* websites. Er zijn over de opstellocaties van deze servers minder betrouwbare kwantitatieve gegevens voorhanden dan in de anti-virus en anti-spam activiteiten. Figuur 6 toont een meting van Webroot, die aangeeft dat in het tweede kwartaal van 2006 5,15% van alle spyware afkomstig was vanaf in Nederland opgestelde sites[12] en in het eerste kwartaal bedroeg het nog 7%. Naast verspreiding via websites wordt *malware* zelfs, zeer misleidend, verspreid bij programma's, die hun downloaders beloven juist hinderlijke adware te verwijderen.

2.2.6 Denial-of-Service aanvallen

Hoewel in de interviews wel genoemd als een serieus probleem, is de positie van Nederland in Symantec's top-10 van landen waarop de meeste Denial of Service attacks zijn gericht in de eerste helft van 2006 toch een verrassende (Figuur 7). Symantec constateerde een aantal van

[12] Een korrel zout lijkt aanbevolen: 1kw2006 waren China en de VS nog de grootste bronlanden en in 2kw2006 is alleen de VS voor dat percentage verantwoordelijk …

6110 DoS aanvallen per dag. Waarbij zij alleen naar het meest voorkomende type - zogenaamde SYN Flooding - telde. Ruim 1,1 miljoen aanvallen in een half jaar. In het VK en de VS loopt de aanvalslust op tot 11,2 DoS aanvallen per miljoen inwoners per dag, in Nederland is dat 7,6. De rest van de landen met veel DoS aanvallen kent aanzienlijk lagere aantallen.

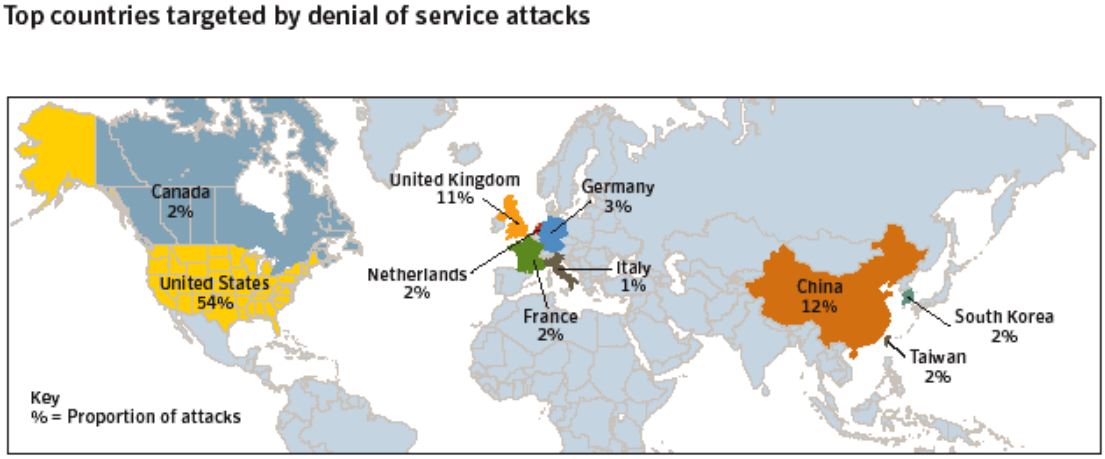


Figure 11. Top countries targeted by denial of service attacks
Source: Symantec Corporation

Figuur 7 *Nederland is een bovenproportioneel doelwit van Denial of Service aanvallen*

De meest gekozen doelwitten van Denial of Service aanvallen zijn volgens Symantec ISP's (38%) en Overheidssites (32%). Telecomoperators zijn met 8% van de aanvallen een minder gezocht doelwit.

2.2.7 Combinaties van deze dreigingen

Vooral bij crimeware en phishing, wordt tegenwoordig een praktijk geconstateerd waarbij indringers een combinatie van de hierboven beschreven dreigingen toepassen. Virussen verspreiden zich veelal met de technieken van een worm, zowel direct (via 'portsweeps' slecht beveiligde systemen zoeken) als via e-mail, rogue websites installeren soms software voor botnets en keyloggers, terwijl ze ook de techniek van een Trojaanse paard toepassen en aandacht proberen te trekken via hyperlinks in spam. De ene vorm van malware triggert dan de installatie van andere kwaadaardige software.

De algemene trend is dat de verspreiders bedoelingen steeds meer samenhangen met criminale activiteiten. Daarvoor worden de toegepaste technieken snel geavanceerder in 'subtiliteit', omdat bij het overnemen van een PC voor een botnet en andere criminele oogmerken onzichtbaarheid een oogmerk is, dit in tegenstelling tot het stimuleren van transacties via Spam 'advertenties'. Dit verklaart deels het krimpende percentage virussen via e-mail, kans op detectie bij die verspreidingswijze is veel groter. 'Onzichtbare' installatie via websites is attractiever, dit is veel minder zichtbaar voor de ISP's.

Enkele geïnterviewden maakten een nadrukkelijk onderscheid in het soort dreiging in relatie tot het oogmerk van artikel 11.3 Tw. Een aantal dreigingen, zoals het overnemen van een PC voor een botnet raakt eindgebruikers zelf amper. Het steeds meer werken met combinaties van

verspreidingswijzen en inbreuktechnieken, maakt het echter lastiger zo'n onderscheid in de praktijk tot leidraad van handelen te maken.

2.2.8 Schadelijke inhoud niet genoemd als dreiging persoonlijke levenssfeer

Wat tenslotte opvalt is het in Nederland onder de stortvloed van *rommel* verdampen van de *harmful content* discussie van rond de eeuwwisseling: het filteren van websites die bijv. ouders voor kinderen schadelijk of ongeschikt achten.

Wie de Europese discussies volgt, kan constateren dat men dit aspect vaak wel meeneemt, als men beleid bediscussieerd met betrekking tot inbreuk op de persoonlijke levenssfeer. Dit zal vermoedelijk deels met de Nederlandse cultuur van doen hebben, die bescherming hiertegen vooral als een eigen verantwoordelijkheid van eindgebruikers ziet.

3 Wat zijn de dreigingen die opkomen?

In dit hoofdstuk wordt in twee stappen beschreven wat de dreigingen zijn die nu spelen. Eerst wordt een beeld op hoofdlijnen geschetst van de bevindingen in de interviews. Daarna volgt een beeld van de opkomende dreigingen op basis van de gesprekken en analyse van Stratix.

3.1 Bevindingen uit interviews op hoofdlijnen

Bij de vraag naar de dreigingen die opkomen is extra aandacht besteed aan de dreigingen die Voice-over-IP introduceert, en dan vooral VoIP-diensten die (deels) over het publieke Internet lopen. De dreigingen bij VoIP worden door de hiermee actieve partijen vooral gerelateerd aan de geldstromen die met spraaktelefoondiensten zijn gemoeid en minder met SPIT (Spam over IP Telefonie). Het is dus vooral systeembeveiliging tegen fraude. Die kan alleen ten koste gaan van de provider, maar ook ten koste van eindgebruikers, die risico's lopen zoals het overnemen c.q. misbruiken van VoIP-accounts om bijv. dure gesprekken te voeren - "dialers in een nieuwe jas" - of het (pre-paid) conto in te pikken.

Geïnterviewden gaven ook aan dat de nieuwe betaalde videodiensten een doelwit kunnen worden. De mediaplayers (Windows Mediaplayer, Real Player, Flash Players en Quicktime) zijn door geen van de geïnterviewden zelf genoemd als nieuw voertuig voor het overbrengen van 'malware'. Tijdens het uitwerken van de interviews is aan deze dreiging door IT journalist Herbert Blankesteijn[13] aandacht besteed vanwege de eerste wormen die op deze wijze werden geïnstalleerd. Dit wordt door een geïnterviewde in reactie op het concept vooral als een voorbeeld gezien hoe een nieuwe (populaire) technologie weer nieuwe dreigingen met zich meebrengt. Het probleem is volgens hem niet een zwakte in de videocodecs/system zelf, maar het misbruiken van een *feature* van dit soort software. Veel videosystemen vervoeren extra tags of hyperlinks bij het signaal, een nuttige aanvulling indien correct gebruikt. Het probleem is dat kwaadwillenden dit soort functies, waarbij gebruikers gewend raken om ze aan te klikken, zoeken om voor hun eigen doeleinden in te zetten.

Hoewel niet concreet genoemd, bevestigde dit wel de meer conceptuele antwoorden van geïnterviewden, waar opkomende dreigingen vandaan komen: "Alle zaken waar zonder veel na te denken op geklikt wordt door gebruikers, zijn doelwit om besmettingen van de apparatuur van eindgebruikers te realiseren" en "het gaat de veroorzakers primair om geld" zijn als belangrijkste abstracte principes aangegeven voor de wijze waarop dreigingen werken en de drijfveer van de bedreigers. De drijfveer 'geld' zorgt er ook voor dat geïnterviewde ISP's veel aandacht besteden aan de door henzelf geïntroduceerde nieuwe betaalde diensten (VoIP, video etc.). Op dat punt kunnen zij de veiligheid ook veel sterker beïnvloeden.

Identiteitsdiefstal is door enkele als opkomende dreiging benoemd, door andere al als bestaande dreiging. In Nederland is dit fenomeen nog niet zo sterk ontwikkeld. Credit Cards worden niet

[13] Herbert Blankesteijn, *Video wordt bron van virussen*, 4 december 2006, BNR Nieuwsradio, http://www.hccmagazine.nl/index.cfm?fuseaction=home.showColumns&id=50445

zoveel gebruikt, en het werken met PIN-calculators bij elektronisch bankieren remt phishing. Dat zou echter sterk kunnen veranderen, wanneer de Nederlandse overheid haar beleid om te komen tot één centrale digitale kluis doorzet, met zeer veel privacy gevoelige gegevens gekoppeld aan het Burger Service Nummer. Dan wordt juist het verspreiden van logging malware ten behoeve van identiteitsdiefstal pas echt lucratief, want er is dan één homogeen doelwit ontstaan.

Tenslotte is in het interview met NLnet Labs 'domaintasting' genoemd als nieuwe bedreiging. Dit is een praktijk waarbij marktpartijen in één klap honderdduizenden tot een miljoen domeinnamen aanvragen. Zij implementeren die namen dan op eigen servers en bekijken ze op hun aantrekkingskracht voor verkeer (bijv. van typefouten), om na enkele dagen de minder aantrekkelijke namen terug te leveren. Dit drijft op slim misbruik van de elektronische colportage wetgeving, waardoor ook domeinnamen op zicht kunnen worden verkregen, 'geproefd' en binnen de wettelijke spijttermijn teruggedraaid. De praktijk is ook erg attractief voor 'hit and run' uitbaters van Spam en 'Rogue websites' vol met spy- en malware, omdat ze er veel onzichtbaarder mee worden. Een kwaadwillende levert dan na enkele dagen de domeinnaam weer in en de transactie verdwijnt uit de boeken zonder veel controle.

Hoewel niet alle partijen alle in de voorbereiding bedachte potentiële antwoorden opnoemden bij de huidige en toekomstige dreigingen is geconstateerd dat enkele partijen spontaan praktisch de gehele lijst uit de voorbereiding opsomden en bij navraag ook voorbeelden konden geven. De enige dreiging die nooit door een geïnterviewde is genoemd is Domeinnaamdiefstal, het ontfutselen van iemands domeinnaam bij een registrar. Een praktijk vergelijkbaar met *slamming* op het telefoonnet.

3.2 Een beeld van de opkomende dreigingen

Bij de opkomende dreigingen is door een aantal geïnterviewden deels uitgegaan van wat abstractere concepten op welk gedragingen er vooral worden ingespeeld. Dat leidt tot: "alle toepassingen waar redelijk onnadenkend op geklikt kan worden" en "alle zaken waar geldstromen mee gemoeid zijn". Het geven van een beeld van opkomende dreigingen is lastig. De risico's zijn vooral gekoppeld aan populaire nieuwe toepassingen en die waar geldstromen aan verbonden zijn. Het vraagstuk vereist zo een dubbele inschatting: welke opkomende toepassingen hebben zowel een groot potentieel in adoptie als een grote kwetsbaarheid, die geëxploiteerd kan worden door vindingrijke kwaadwillenden.

3.2.1 ISP's kijken vooral naar fraude betaalde diensten

Bij de voorbereiding was een lijstje met kandidaat antwoorden genoteerd: SPIT, SPIM, Advertentiefraude, ID en (Game) persona diefstal, Crimeware, DNS-vervuiling en name hijacking. *Crimeware* is mede naar aanleiding van de interviews als een van de huidige dreigingen aangemerkt en al besproken.

De interviews maakten duidelijk dat men zich vooral zorgen maakt om de dreiging van fraude bij de nieuwe betaalde diensten als VoIP-telefonie en Video en bijvoorbeeld minder over nieuwe vormen van Spam. Spam lijkt vooral te gedijen in 'gratis' en 'niet-interactieve'

omgevingen, waarbij het moeilijk is de bron op te sporen. Dit is de gezamenlijke noemer van e-mail, nieuwsgroepen en weblogs die vooral door Spam getroffen zijn. SMS-spam is daarentegen vrij succesvol bestreden door mobiele operators, omdat men door de onderlinge verrekening de verzenders snel opspoorde. In meer interactieve toepassingen zijn dreigingen anders. Gebruikers kunnen de sessie direct beëindigen / wegklikken of de toegang blokkeren c.q. tot de buddylist laten beperken. SPIM en SPIT zijn daardoor een kleiner risico.

Bij de DNS-dreigingen kunnen berichten die speelde rond de diverse trucs om een cache te vervuilen (ook wel als *cache poissoning*) en zo bijv. een domain name (tijdelijk) te hijacken als enigszins journalistieke hype worden aangemerkt. *Domaintasting* wordt als een groter risico gezien. DNS Amplification aanvallen zijn al gemeld in het vorige hoofdstuk als huidige dreiging, en het risico van vergroting van de impact is gemeld bij de veel grotere DNSSEC berichten. Het argument van grotere berichten gaat echter ook op voor IPv6 Resource Records en de NAPTR records die voor ENUM gebruikt gaan worden[14]. De oorzaak van de dreiging is dat veel DNS servers nog 'open resolvers' zijn en niet alleen de lokale clients tot hun systeem toelaten. Dit is vergelijkbaar met de *SMTP-open relay,* een wijze van configureren die initieel massaal werd geëxploiteerd door Spammers. Dichtzetten voor niet-lokale verzoeken om recursie[15] is dus de eerste tegenmaatregel. Hierbij zal ook een groot aantal hosters en zakelijke eindgebruikers met DNS-servers geadviseerd moeten worden.

De groep geïnterviewden deskundigen zijn vooral actief op het terrein van netwerken en core-infrastructure systemen. Dit heeft mogelijk geleid tot enige selectiviteit: zaken als *advertentie-fraude* en diefstal van *virtuele waarden* of een *persona* met een hoge spelwaarde zijn meer problemen voor marktpartijen als Google, Marktplaats/eBay of multiplayer speluitbaters dan voor Nederlandse ISP's. Het gaat tot nu toe echter ook meer om diensten die in EU jargon als 'diensten voor de informatiesamenleving' worden aangemerkt en niet zozeer als 'communicatie-diensten', bij sommige 'spelen' is echter chat zo ongeveer het hoofdelement van het spel. Google Talk en Skype zijn ook voorbeelden van communicatiediensten. Artikel 11.3 Tw koppelt qua toezicht o.a. aan het begrip openbare elektronische communicatiedienst. Het is niet duidelijk of dit begrip zich ook uitstrekt tot Usenet, mailinglists, Internet Relay Chat, profiel-sites, blogs, MSN, of zelfs MUD- & MOO-spelen[16] als *World of Warcraft* en de 3D-chat-omgeving *Second Life,* die allen ook deels als communicatiedienst kunnen worden aangemerkt. Een aanzienlijk deel van deze diensten wordt bovendien door derde partijen geleverd en niet door ISP's. Hier ontstaat een afbakeningsvraag: "wat is nog een elektronische communicatie-dienst en valt een aanbieder onder artikel 11.3 Tw als die vanuit het buitenland Nederlandse gebruikers bedient?"

---

[14] Voor een uitleg zie: http://www.securiteam.com/securityreviews/5GP0L00I0W.html

[15] Opzoeken van domeinnamen door clients gebeurd meestal recursief met een verzoek aan een nabije DNS-server (van bedrijf of ISP) om de look up van de domeinnaam op Internet uit te voeren. Een server die verzoeken vanuit het hele Internet toelaat is een potentieel relais voor een DDoS-aanval

[16] Multi-User Dungeon, een online rollenspel met *hack & slash* Fantasy-figuren en sociale chatrooms, en MUD Object Oriented, MUD waarin (ervaren) gebruikers, Wizards en Guru's, nieuwe zaken kunnen programmeren. World of Warcraft is een grafische MUD, Second Life is een grafische MOO.

OPTA zal moeten afbakenen, welke dreigingen op Internet en diensten zij op dit punt nog tot haar werkterrein rekent en waar zij bijv. het CBP een meer geëigende toezichthoudende instantie acht en hoe zij extra-territoriale kwesties adresseert. Er zijn nog meer marktbewegingen die een afbakeningsvraag oproepen: Rabo Mobiel combineert nu elektronisch bankieren met communicatie- en Internetdiensten. Banken en verzekeraars hebben ook al een eigen security overlegstructuur (zie SURFnet interview).

3.2.2 SPIT vraagstuk lijkt al geadresseerd voor VoIP volledig uitrolt

Bij het opstellen van de vragenlijst waren extra vragen toegevoegd ten aanzien van VoIP security. Mede vanwege de snel groeiende vraag naar VoIP. De grootschalige partijen met een VoIP aanbod (KPN, Priority Telecom en kabelexploitanten) werken in Nederland tot nu toe vooral via het Media Gateway Control Protocol in afgeschermde domeinen. SIP is een techniek die pas recent werd geïntroduceerd en dan veelal nog in afgeschermde omgevingen (zie ook [17]).

Een beperkt aantal partijen, vooral ISP's en VoIP Service Providers (VSP's) zijn net als het geïnterviewde XS4all al actief met SIP platforms op Internet. Hun schaal is relatief klein. SPIT is in de huidige markt dus nog geen groot vraagstuk. Een zoektocht door diverse security sites op Internet bevestigt het beeld dat SPIT wereldwijd tot nu toe een schaars voorkomend fenomeen is. Het lijkt dat in ieder geval te blijven zolang er betaald moet worden voor een gesprek. Overigens houd het maken van kosten per gesprek ongevraagde telefonische telemarketing nu ook niet tegen.

Er is echter een ontwikkeling onderweg naar VoIP Peering, waarbij met gesloten beurzen verkeer wordt uitgewisseld. Daardoor neemt de SPIT dreiging op termijn mogelijk toe. Een aantal partijen die zich bezighoudt met VoIP en VoIP Peering (Kayote Networks, XConnect en Siemens) trekken op dit moment in de IETF SIPPING werkgroep de standaardisatie voor SPIT preventie[18]. De eerste twee zijn leveranciers van de *SIP Exchange*, het peering platform dat de kabelsector in Nederland heeft opgericht, terwijl Siemens in Nederland de VoIP-platforms levert aan zowel een aantal grote kabelmaatschappijen als KPN. Met drie in Nederland leidende leveranciers, die de internationale standaardisatie trekken voor maatregelen tegen SPIT, lijkt de SPIT-dreiging voor de komende tijd afdoende geadresseerd en is de fraudedreiging voorlopig relevanter.

3.2.3 Dreiging sociale inbreuken in de levenssfeer en privacy

Op één opmerking van een geïnterviewde over digitaal pesten op Internet na, zijn sociale dreigingen die leiden tot inbreuken in de persoonlijke levenssfeer niet genoemd. Dit speelt zich ook veelal buiten het zicht van ISP's af. Soms wordt het zichtbaar, als bijvoorbeeld een shockblog na een negatieve publicatie plotseling een *Denial-of-Service* aanval voor zijn kiezen krijgt en de server uit de lucht gaat.

[17] *IP interconnectie,* Rapport voor OPTA, Stratix Consulting, Januari 2007
[18] http://tools.ietf.org/wg/sipping/draft-schwartz-sipping-spit-saml-01.txt

Telefonie operators zijn al jaren bekend met *plaagggevallen*. Zij werden, nadat automatisering de telefonie in de jaren vijftig anonimiseerde, geconfronteerd met *hijgers* en *zwijgers (telefonische belaging?)*. Daarop zijn toen technische maatregelen genomen in de centrales (vangschakeling en later de politieprinter) om de opsporing en vervolging te ondersteunen. Belagen op Internet is ook gekoppeld aan schijnbare anonimiteit en impersonatie. Het geijkte voorbeeld bij impersonatie is een volwassene die zich als een leeftijdsgenootje van een kind voordoet. Dit wordt vaak met een 'onveilig Internet' geassocieerd.

De groepskarakteristieken van veel internettoepassingen introduceren vaak onverwachte dreigingen. In het verleden werden mailinglists misbruikt om bijv. een niet geliefd persoon te overstelpen met e-mail (mailbom), IRC-kanalen worden ook nu nog ingezet om bijv. botnets te besturen. Een aantal spelen heeft ook 'waarde' gekregen, waardoor er in avatars en spelattributen wordt gehandeld en identiteitsdiefstal voor dat spel lonend wordt. Bij vrijwel elke groepsapplicatie kan er door groepsdynamiek bedreigend 'gedrag' ontstaan. Bij caféruzies komt echter ook de politie langs en niet de Keuringsdienst van Waren. Veel sociale inbreuk dreigingen zal men meer met *veiligheid* associëren dan met *beveiliging*. Het gaat ook veelal buiten ISP's om. Het lijkt daarom verstandig voor OPTA om op dit punt de reikwijdte van artikel 11.3 Tw nader af te bakenen tot beveiliging en te bevorderen dat veiligheidsdreigingen in het justitiële domein worden geadresseerd.

4 Wat wordt daar nu aan gedaan en wat kan er aan gedaan worden?

In dit hoofdstuk wordt beschreven wat er nu door marktpartijen aan wordt gedaan en wat er aan gedaan kan worden. Eerst wordt een beeld op hoofdlijnen geschetst van de bevindingen in de interviews. Daarna volgt een analyse van wat er nu aan gedaan wordt en vervolgens wat er aan gedaan kan worden met uitsplitsingen per soort partij.

4.1 Bevindingen uit interviews op hoofdlijnen

In de praktijk nemen alle geïnterviewden maatregelen tegen de verspreiding van Spam en virussen via e-mail. Daarvoor heeft men systemen voor inkomende mail filtering (ingress), maar men scant en filtert ook uitgaande mail die via de eigen systemen wordt gerouteerd. Ook de implementatie van BCP-38[19]: ingress- en egress filtering van pakketverkeer met IP-adressen uit andere dan eigen reeksen wordt algemeen als maatregel genoemd.

Ook het blokkeren van poorten komt algemeen voor, er is echter een aanzienlijk verschil in aanpak tussen ISP's die alleen de meest gevaarlijke poorten (NETBIOS, Back Orrifice) voor alle klanten blokkeren en ISP's, die op die wijze ook of alleen maar de uitgaande e-mailpoorten (poort 25) afstoppen en zo de inzet van Zombie-PC's voor Spam verspreiding onmogelijk maken. Keuzes hangen samen met de aard en kennisniveau van het klantenbestand dat de ISP heeft. Bovendien heeft een aantal ISP's ook een doelbewuste commerciële positionering met open toegang en geen rem op het draaien van servers bij klanten.

Alleen de twee grootste geïnterviewde ISP's (SURFnet en Xs4all) geven aan speciale systemen voor detectie van besmettingspogingen ('honeypots') en bemonstering van verkeer ('flowanalyse', 'sensornetwerken') te hebben om afwijkende patronen die behoren bij misbruik te kunnen zien. De twee kleinere ISP's hebben minder geautomatiseerde bewaking. Dit heeft duidelijk met schaal en kosten te maken.

InterNLnet, draait voor een klantengroep het Quarantainenet uit Twente. Dit is een systeem dat ook bij een aantal universiteiten is geïnstalleerd, waarbij nieuwe en besmette PC's in een afgeschermd domein van het netwerk worden geplaatst en daarmee gedwongen om de systeembeveiliging eerst op niveau te brengen. Pas daarna kan men weer Internet gebruiken. Deze oplossing is niet alleen ingrijpend en daardoor vooral geschikt voor domeinen zoals universiteiten en hogescholen, die ook andere relaties met de netwerkgebruikers hebben, maar ook nogal prijzig.

CAIW past een 'walled garden' techniek toe waarbij gebruikers van nog niet eerder gesignaleerde kabel(koop)modems, al dan niet voorzien van VoIP, zich eerst nader moeten identificeren voor ze volledige toegang krijgen; al gaat het daarbij vooral om het voorkomen van misbruik van de diensten van CAIW zelf en niet zozeer om het tijdelijk afgescheiden

[19] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000

houden van nieuwe PC's etc. die voor het eerst worden aangesloten op Internet in de woning van de gebruiker.

Er is op gewezen dat een aantal nieuwe technieken om tot meer veiligheid te komen technologisch klaar zijn. DNSSEC is in 'early deployment' voor certificatie van IP adresblokken en voor 'routing security' bestaan er prototypes. Met deze technieken kan men vermijden dat Spammers of rogue hosters met een net communiceren vanuit loszwervende adresblokken of 'fake' domeinen gebruiken. Echter de uptake (deployment) moet nog van de grond komen. Wat dan vooral inhoudt dat veel 'zaken om een nieuw protocol heen' nog moeten worden geregeld. Hierin kan de overheid als eindgebruiker van Internet een voorbeeldrol nemen, door nieuwe veilige protocollen en technieken zelf in de eerste groep te implementeren.

In een aantal gevallen loopt implementatie van nieuwe technieken en beveiligde protocollen op tegen structurele zakelijke problemen. 'Secure Routing' zorgt er bijv. ook voor dat een ISP laat zien met wie men 'peert', welke routing policy er wordt gehanteerd etc.

Er zijn in de industrie al een aantal organisaties die uitgebreid aanbevelingen doen, welke dreigingen er opspelen (bijv. Computer Emergency Response Teams) en welke tegenmaatregelen er kunnen worden geïmplementeerd en welke verstandig zijn. De laatste gebeurt veelal in de Best Current Practices documenten die via de IETF worden verspreid of op RIPE meetings besproken.

Tenslotte is uit de gesprekken gebleken dat een aantal geïnterviewden c.q. hun marktpartijen 1 keer per 2 maanden bij elkaar komt voor het *operationele Incident Response Team overleg* (o-IRT-o). Er is ook een telefoonnoodlijst voor onderlinge coördinatie bij grote incidenten. CAIW gaf aan dat die lijst, voor zover hen bekend, los staat van het o-IRT-o.

Op een aantal aspecten is aangegeven dat er steeds meer (semi-) besloten domeinen ontstaan met groepen marktpartijen, die zich deels afscheiden van het publieke internet en binnen een domein hun eigen niveaus van veiligheid hanteren. Waarbij ISP's meer of minder open zijn in de wijze van transport van hun verkeer van en naar hun eindgebruikers. Een voorbeeld is VoIP-verkeer: CAIW en InterNLnet vervoeren het in een besloten deel vanaf hun aansluiting. Xs4all daarentegen levert VoIP over het publieke deel van het Internet. Dat laatste verwachten CAIW en InterNLnet op termijn te zullen gaan bieden voor softphones.

Het ontstaat van 'clusters', 'clubs' of 'subgroepen met een hogere onderlinge graad van vertrouwen' is een trend die ook geldt voor veiligheid en beveiliging in het algemeen. Mobiele providers zijn met hun IP verkeer gesloten. Volledige openheid is verleden tijd. Fora zoals de o-ITR-o zijn selectief in de uitnodiging van deelnemende experts.

Een geïnterviewde duidde deze werkwijzen aan als een uitvloeisel van het 'meritocratisch principe' dat op Internet gebruikelijk is. Hierbij wordt vooral gekeken naar het niveau van de inbreng (bijdragen en kennis van zaken) en effectiviteit in de onderlinge openheid en externe vertrouwelijkheid over wat er wordt uitgewisseld over dreigingen. Deze principes kunnen

mogelijk botsen met de uitgangspunten, die een regelgever (moet) hanteren, waarbij men gewend is niet op effectiviteit maar op efficiëntie te sturen en men gedwongen is om iedereen te horen en aan tafel te noden. Hierbij werd wel in de feedbackronde het commentaar gegeven (door een andere ISP) dat ook het meritocratisch principe niet zuiver wordt toegepast. Men heeft de neiging om andere ISP's niet te informeren over de resultaten.

4.2 Wat wordt er nu aan gedaan, een beeld

De bevindingen van de interviews met de beveiligingsspecialisten geven een goed beeld van wat er nu aan gedaan wordt. Hierbij moet echter worden opgemerkt dat gesproken is met deskundigen die bij bedrijven werken met een goede naam op dit vlak. Er is echter een groep aanbieders op de markt die meer gericht is op marketing en minder bekend staat om de kwaliteit van hun beveiligingsinspanningen. Internetdienstverlening is een sterk gesegmenteerde markt. De wijze van aanpak van veiligheid en beveiliging is deels een concurrentieaspect. De volgende alinea's schetsen het beeld.

Aan de providerzijde

- Het scannen van e-mail op spam en virussen is tegenwoordig onderdeel van het standaard-aanbod. Kwaliteit en niveau van deze dienstverlening kan echter variëren. Niet iedereen filtert bijvoorbeeld al de uitgaande (*egress*) e-mail. Update beleid en gekozen blocklist databases beïnvloeden de prestaties.
- Waar de geïnterviewden Best Current Practices implementeren ten aanzien van het routeren van IP verkeer (anti-spoofing maatregelen, blokkeren van verkeer van ongeregistreerde blokken) geld dit nog niet voor alle marktpartijen. Dat kan zowel door configuratiefouten komen als door IT-staf met een matig kennisniveau.
- Het blokkeren van een aantal poortnummers die veel misbruikt worden is gemeengoed, er zijn echter verschillen in benadering welke poorten men op generieke basis dicht zet. Sommige ISP's differentiëren zich in de markt door toe te staan dat gebruikers zelf servers mogen draaien en minimaliseren port blocking.
- ISP's hanteren vrijwel allen informatiepagina's voor gebruikers over hoe zij zich kunnen beveiligen en hoe bijv. hun anti-spam maatregelen werken. De voorlichting en kennis bij helpdesks varieert echter sterk tussen providers. Advies over anti-spyware maatregelen is ook veel minder te vinden

Andere maatregelen variëren sterk tussen providers, en zijn vooral gericht op detectie en monitoring van het verkeer op anomaliën.

- aan de gebruikerszijde

Publieke ISP's werken zelf niet met filterende firewalls. Eindgebruikers kunnen het best zelf personal firewalls op PC's te installeren. De meeste Ethernet en WiFi breedbandrouters bevatten slechts rudimentaire firewall functies, en de USB-breedbandmodems vereisen zeker een personal firewall om enigszins veilig te werken.

Anti-spyware software en een regelmatig updatende virusscanner zijn ook praktisch een must. In sommige gevallen wordt dit soort software met een PC meegeleverd, of stelt een ISP dit ook

beschikbaar als onderdeel van het abonnement of bij speciale acties. Microsoft probeert steeds meer deze functionaliteit ook mee te leveren als onderdeel van het besturingssysteem. Echter pas sinds Windows XP service pack 2 staan veel beveiligingsfuncties in default aan met automatische updates.

Bij bedrijven is het vaak verstandiger als men separate hardware firewalls installeert en als men eigen mailsystemen heeft zijn ook eigen spam-filters en mail-virusscanners verstandig. Dit kan men zowel zelf installeren op de eigen servers, hiervoor een appliance aanschaffen of de mail bij een ISP dan wel een gespecialiseerde mail service provider laten filteren en controleren.

Tenslotte kunnen eindgebruikers leren hun gedrag aan te passen en niet te snel op allerlei links klikken of zonder veel na te denken akkoord te geven om zaken te installeren.

◊ door anderen

De Nederlandse overheid heeft tegenwoordig met GOVCERT een kenniscentrum, waarvan vertegenwoordigers lid zijn van het o-IRT-o. Men beheert ook de website http://www.waarschuwingsdienst.nl/ een informatiepunt over internet beveiliging. Daarnaast initieert EZ al een aantal jaren diverse campagnes (o.a. Surf op Safe) in het voorlichtende domein.

Fabrikanten van hardware en software nemen vooral de laatste jaren steeds meer initiatieven op het terrein van security. Hierbij komt de grootste last op de schouders van Microsoft, dat pas vrij recent een koers is ingeslagen om systemen bij uitlevering default al zoveel mogelijk ‘dicht’ te zetten. Hoe dit allemaal met het nieuwe Vista gaat uitpakken moet 2007 leren.

Het automatiseren van patch-procedures is tegenwoordig bij veel applicaties een normale gedragslijn geworden. Volgens Symantec is de responstijd bij Microsoft en Red Hat (Linux) tegenwoordig teruggelopen tot ca. twee weken. Exploits worden soms echter al enkele uren na bekendmaking misbruikt. Er kan echter nog veel meer inspanning worden geleverd.

Op het terrein van IP hardware en op serverniveau zijn security patches en updates praktisch niet geautomatiseerd en hebben de beheerders een veel grotere verantwoordelijkheid om zelf bij de tijd te blijven qua security kennis. Hiervoor worden cursussen en trainingen gegeven door zowel fabrikanten als gespecialiseerde bureaus.

4.3 Wat kan er aan gedaan worden

Er is door geïnterviewden gesignaleerd dat er in toenemende mate afgrenzingen en afscherming ontstaat op het Internet. Cruciale systemen en applicaties worden vaak wel met internet technologie gerealiseerd, maar soms in een bijna volledig separate omgeving neergezet. Er ontstaan daardoor deels parallelle domeinen. Wat dan nodig is, is een zorgvuldige balans te vinden in de openheid binnen clusters van vertrouwde partijen en openheid naar andere delen van het Internet. Op het Internet loopt men tegen de meeste beveiligingsproblemen op, maar het is voor innovatie essentieel om niet met een dichtgetimmerde omgeving te moeten werken.

In het begin van de 19e eeuw is de stoommachine vele decennia een wetenschappelijk niet volledig doorgrond en daardoor onveilig apparaat geweest. Machines ontploften toen regelmatig en er vielen slachtoffers. Dat is toen met o.a. het Stoomwezen als toezicht en vele soorten meters volledig dichtgetimmerd, waardoor aan het eind van de eeuw stoomtechniek niet meer competitief in schaal kon worden verkleind.

Met deze waarschuwing in het achterhoofd volgen toch enige aanbevelingen over wat er aan gedaan kan worden:

◊ aan de providerzijde

ISP's kunnen een aantal basismaatregelen nemen waarmee men Best Current Practices implementeert. De belangrijkste zijn:

- Routeringsmaatregelen (ingress/egress) voor IP verkeer.
- Aanbieden van virus- en Spamfilters[20] voor zowel inkomende als uitgaande e-mail
- Blokkeren van de meest voor inbraken op PC's misbruikte poortnummers
- Eindgebruikers adviseren om (personal) firewalls te installeren of activeren

Deze verzameling maatregelen zou men heden ten dage als een minimum kunnen aanmerken.

Men kan dit ook aanvullen met informatie over anti-spyware en anti-virussoftware, aangezien niet alle personal firewall bundels dit soort dreigingen al volledig meenemen.

Additioneel kan men in de infrastructuur detectie en monitoringssystemen installeren. Bijv. honeypots, en intrusion detection sensornetten. Systemen die bijv. netflow analyseren of ingrepen die quarantaine mogelijk maken van geïnfecteerde machines, vereisen echter veel van de infrastructuur, er komen ook aanzienlijke kosten bij kijken. Het creëren van voldoende redundantie en back-up is ook niet voor alle systemen voor elke ISP of hostingbedrijf betaalbaar.

Wat opvalt is dat in de consumentenmarkt er toch maar weinig ISP's zijn die hun klanten de mogelijkheid bieden om bijv. gegevens op te slaan in safe back-up voorzieningen. Er zijn op Internet ook een paar partijen die bijv. een probe test op een PC doen om te controleren hoe goed de firewall dicht staat met een portscan, maar er wordt door weinigen naar verwezen.

◊ aan de gebruikerszijde

Gebruikers kunnen hun systemen zo configureren dat ze automatisch security updates ontvangen. Daarnaast is een regelmatig bezoek bij een site die controleert door middel van port-scans verstandig. Er zijn ook sites die aanbieden om bijv. adware te detecteren, echter hier moet men erg goed oppassen, omdat een aantal van deze partijen, juist meer adware en spyware installeren.

Er is veel gedrag dat kan verbeteren dit vereist echter intensieve voorlichting. Bijv. het bewust worden van de instelling van browsers om het lekken van privacy gegevens te voorkomen. Ook

[20] De basis is daarbij het gebruiken van black- en whitelists, geavanceerd filteren is het wegen van e-mail op typische Spamkenmerken.

bevatten moderne besturingssystemen functies om bijv. directories te versleutelen, wat vooral handig is als meerdere personen een machine gebruiken.

Het meer werken met versleuteling en maken van backups is ook een evergreen. Echter het meest effectief is toch gedragsaanpassing en zich regelmatig op de hoogte houden over nieuwe beveiligingsproblemen die zich voordoen.

◊ door anderen

Overheden en leveranciers kunnen hun huidige activiteiten intensiveren. Het lijkt daarbij vooral ook voor leveranciers raadzaam om het financieren van fundamentele Research & Development ten aanzien van de oorzaken van het veiligheidsprobleem niet over het hoofd te zien.

5 Reflecties op de rol van OPTA en de overheid

Aan de geïnterviewden is gevraagd om zich uit te spreken over de rol van OPTA en de overheid in deze materie. Eerst worden die opmerkingen uit de interviews op hoofdlijnen geschetst. Daarna volgt een aantal observaties van Stratix op dit punt.

5.1 Bevinding uit de interviews op hoofdlijnen

Met betrekking tot de urgentie van de handhaving van de beveiligingsbepaling in de Tw zijn de reacties vrij eensluidend: velen geven aan dat OPTA zich beter eerst kan richten op een adviserende en voorlichtende rol en niet moet starten met een eigen lijstje *Best Current Practices* voor Nederlandse ISP's te gaan formuleren.

Er bleek bij veel geïnterviewden een behoefte te bestaan om n.a.v. de uitnodigingsbrief voor het interview, hun eigen visie te geven op wat artikel 11.3 Tw naar hun idee inhield voor de branche en de rol van de overheid en OPTA als toezichthouder / handhaver. De visies varieerden sterk, maar waren in hoofdlijnen veel terughoudender dan OPTA in uitleg van de reikwijdte van dit artikel.

De meest beperkte uitleg kwam van InterNLnet. Naar zijn idee betekende Artikel 11.3 lid 1 Tw vooral dat ISP's hun eigen systemen op orde moeten hebben, zodat er niet snel op wordt ingebroken, of de gegevens van hun systemen op straat komen te liggen, waardoor privacy of persoonlijke levenssfeer van hun abonnees in gevaar komt. Artikel 11.3 lid 2 zou dan gelezen kunnen worden als de taak dat, mocht er toch zo'n inbreuk plaatsvinden, dan moet de ISP zijn gebruikers onmiddellijk en ter zake informeren over de (ernst van de) inbreuk en de mogelijke maatregelen om nadelige gevolgen tegen te gaan.

Door meerdere geïnterviewden werd ook genoemd dat men, waar het *beveiliging* betreft, ook een rol ziet voor het Ministerie van EZ in het voorlichtende domein en vooral ook de leveranciers van hardware, besturingssystemen en applicatiesoftware. CAIW gaf daarbij bijvoorbeeld aan dat de overheid met de huidige gebruiksschaal voorlichtende boekjes over veilig internet huis-aan-huis kan verspreiden. OPTA werd niet in de voorlichtende rol genoemd.

Op verzoek van OPTA is aan alle geïnterviewden een volgend 'scenario' ter beoordeling voorgelegd:

> OPTA adviseert eerst maatregelen, en als het probleem blijft bestaan kan zij maatregelen aan aanbieders, als ultimum remedium, aan specifieke partijen verplicht stellen.

Vrijwel alle geïnterviewden hadden moeite met het tweede deel, waarbij het voor enkelen de vraag was of dit scenario inhield dat er eerst industriebrede maatregelen moeten worden vastgesteld en verplicht opgelegd, voordat die aan specifieke partijen verplicht kunnen worden gesteld. Daarbij werd door meerderen aangegeven dat men bang is dat OPTA achter de feiten zal gaan aanlopen wanneer men *Best Current Practices* in algemene zin voor Nederland wil formaliseren.

Wat betreft de invulling van begrippen maakte Xs4all een relevante opmerking. Zij wensen een scherp onderscheid te maken tussen de begrippen *beveiliging* [Eng. security] en *veiligheid* [Eng. [safety]. Politici hebben de neiging om beiden in de discussies op één hoop te gooien. ISP's kunnen vooral de *beveiliging* van hun eigen netwerk en diensten beïnvloeden en over *veiligheid* slechts voorlichten en hulpmiddelen facultatief ter beschikking stellen.

Een aanzienlijk aantal gaf ook aan dat hun kernactiviteit het leveren van (open) toegang tot het Internet is en dat zij vooral daaraan hun maatregelen koppelen. Bijvoorbeeld wel het veilig configureren c.q. bij de start in quarantaine zetten van breedbandmodems. Geïnterviewden stopten echter bij dit scheidingsvlak en zien het niet als hun taak dit door te trekken tot het controleren van configuraties van PC's van gebruikers. Voor dienstverlening op dat niveau werd aangegeven dat gespecialiseerde ISP's in de markt zijn.

Xs4all merkte op dat zij een duidelijk andere benadering van Internet heeft dan de gedachten van de Consumentenbond over de rol van ISP's[21].. Xs4all ziet Internet niet als iets wat iemand consumeert, maar wat men gezamenlijk maakt, daarbij is dan ook van belang hoe men zich gedraagt. Zij zijn van mening dat OPTA eerst zou moeten uitzoeken wie er allemaal actief zijn in de keten, en pas daarna bepalen wie wat zou moeten doen.

CAIW gaf aan dat men voor een effectieve introductie van maatregelen het beste kan zorgen dat de belangen sporen met die van ISPs: internet dient een prettig product voor de eindgebruiker te zijn en moet dus relatief veilig en niet al te schadelijk voor de persoonlijke levenssfeer zijn. De wijze waarop de overheid nu vaak enigszins gerelateerde maatregelen introduceert, oplegt, handhaaft en de wijze waarop de daaraan verbonden kosten worden vergoed nodigt niet bepaald uit om de sector mee te krijgen, ook niet op andere terreinen. Overheid en het toezicht zouden zich naar hun idee het best kunnen richten op die punten waar de industrie dat niet uit zichzelf doet. Een ISP die zijn dienst probeert aan de man te brengen gaat bijvoorbeeld bij verkoop niet in detail alle risico's opsommen, behalve als het (en dan nog in beperkte mate) min of meer afgedwongen wordt (zoals nu de bijsluiters in de financiële wereld).

Ook SURFnet gaf aan dat een uitkomst waarbij gebruikers bang worden gemaakt niet verstandig is. OPTA zou een blauwdruk kunnen maken met BCPs en dat onderhouden, daar moet dan een redactiecommissie voor worden opgezet die dat werk gaat doen. Dit zou men kunnen vragen aan het o-IRT-o, maar ook het ECP.NL[22] heeft een taak daarin. SURFnet ziet wel een voordeel dat OPTA met een mandaat kan opereren.

[21] http://www.consumentenbond.nl/nieuws/nieuws/Archief/2006/5847620?ticket=nietlid
Cit.: De Consumentenbond vindt daarom dat de industrie zelf veiligheidsnormen moet opstellen; de overheid stelt bedrijven die zich daar niet aan houden aansprakelijk, zodat gedupeerden een compensatie kunnen krijgen.

[22] ECP.NL: Electronic Commerce Platform Nederland

NLnet Labs geeft aan dat OPTA als eerste stap het beste kan in het veld kan gaan meelopen, kennis te verrijken en goede ontwikkelingen te benoemen, daarbij wijst men naar de wijze waarop in Zweden/PTS de verschillende clubs bij elkaar heeft laten komen. De geïnterviewden kunnen echter niet uit de voeten met het begrip 'passende maatregelen'. Daarvoor is het teveel een 'arms race' en veranderen de dreigingen constant.

Door NLnet Labs is tenslotte opgemerkt dat in Nederland enkele marktpartijen lobbyen om elektronische orderverwerking voor '.nl' domeinnamen mogelijk te maken. Onder de huidige Colportagewetgeving heeft elektronische orderverwerking sterk negatieve gevolgen voor bijv. de opsporing van Spam en 'rogue websites' met malware, omdat dan ook hier 'gratis' domeinen kunnen worden 'geproefd'. OPTA kan als passende maatregel bij de overheid agenderen om de wetgeving op dit vlak in Nederland zodanig aan te laten passen, dat dergelijke juridische opportunistische sluiproutes vooraf legaal kunnen worden gestopt.

Xs4all zou graag zien dat SIDN in deze discussie wordt betrokken. veel van de Spam en ".nl" problemen die optreden op het terrein van security/safety online zijn daadwerkelijk te beheersen door SIDN. Over de huidige prestaties heerst grote ontvredenheid. Mogelijkerwijs kan OPTA op dit punt meer betekenen door hen aan te moedigen?

5.2 Rol van OPTA en de overheid, onze observaties

Het is duidelijk dat veel van de geïnterviewden een erg terughoudende rol bepleiten van OPTA. Echter wat ook uit het onderzoek naar voren komt, is het bestaan van al een redelijke consensus over een aantal Best Current Practices.

Het lijkt gezien deze twee elementen vooral verstandig dat OPTA een discussie op gang brengt en zich daarbij te concentreren op zaken die gericht zijn op de beveiliging van systemen en netwerken ten behoeve van dienstverlening. Veel van de veiligheidsvragen zijn beter te adresseren door EZ (voorlichting) of door het justitiële apparaat. Het laatste geldt vooral voor bescherming tegen storend gedrag van andere Internet gebruikers.

Daarbij moet niet uit het oog worden verloren dat Internet een steeds belangrijkere plaats in de samenleving inneemt, maar technologisch nog volop in ontwikkeling is. In een recente voordracht bij Google [video] - "A New Way to look at Networking"[23] - gaf Internet Pionier Van Jacobson een zeer interessante ander perspectief op de veiligheidsvragen. Hij tekende aan dat het telefoonnet en ook TCP/IP gebaseerd zijn op *conversatie*, terwijl 99% van het huidige Internetverkeer gericht is op *disseminatie* van informatie en software. In dat geval is het beveiligen van verbindingen niet zo effectief, en zou het veel verstandiger zijn om datgene te beveiligen en authenticeren waar werkelijk naar wordt gevraagd: *informatie*. Die moet dan beveiligd en gedistribueerd redundant worden gemaakt.

Zo'n transitie van conversatie naar disseminatie als ontwerpprincipe vereist een forse slag, echter veel van de nieuwe, op disseminatie gerichte infrastructuur is al in delen gerealiseerd in

[23] http://video.google.com/videoplay?docid=-6972678839686672840

moderne peer-to-peer applicaties. Er is een argument te maken om fundamenteel onderzoek naar de security vragen te bevorderen en niet te snel om operationele redenen het *Stoomwezen* van de 21e eeuw op te richten, omdat vrij fundamentele technische vragen nog niet zo goed doorgrond zijn.

6 Afsluitende opmerkingen

6.1 Conclusies

De belangrijkste problemen die er nu zijn hebben betrekking op botnets en het overnemen van computers via virussen en malware. Hiervoor wordt Spam echter nog steeds op grote schaal als verspreidingswijze ingezet. Phishing is daarnaast een snel groeiend probleem.

Een vergelijking met enige internationale rapporten met kwantitatieve gegevens ondersteunen de beelden die geschetst zijn door de geïnterviewden. Daarbij valt op dat in Nederland opgestelde systemen een bovenproportioneel deel van de Denial-of-Service aanvallen in de wereld te verwerken krijgt. Ook is Nederland een bovenproportioneel groot bronland van websites waarmee Spyware en andere Malware wordt verspreid.

ISP's kunnen maatregelen nemen tegen een deel van deze dreigingen, door enerzijds hun gebruikers goed voor te lichten over de risico's van Internet, vooral de gevolgen van onnadenkend klikgedrag, anderzijds zijn er een aantal infrastructurele maatregelen mogelijk. De belangrijkste zijn:

- Het niet naar andere netten routeren van verkeer vanaf IP-adresssen die niet tot de eigen reeksen behoren.
- Het niet routeren van inkomend verkeer van IP-blokken die niet officieel zijn uitgegeven
- Aanbieden van virus- en Spamfilters voor inkomende en uitgaande e-mail
- Blokkeren van de meest voor inbraken op PC's misbruikte poortnummers
- Eindgebruikers adviseren om (personal) firewalls te installeren of activeren

Wat betreft opkomende dreigingen blijken veel geïnterviewden vooral te kijken naar de fraude risico's van de nieuwe betaalde diensten. SPIM en SPIT spelen geen grote rol.

De introductie van DNSSEC blijkt omstreden. Er zijn veel voorstanders, maar XS4all ziet met deze techniek het risico van DNS-Amplification aanvallen vergroot worden, omdat DNSSEC berichten een aanzienlijk grotere omvang hebben.

Gezien de genoemde zaken in de interviews is er echter voldoende overeenstemming om een basisniveau te geven van minimummaatregelen die elke ISP zal en kan implementeren. Hierbij moet wel de opmerking van CAIW in de gaten worden gehouden, dat veel van dit lijstje de beïnvloedbare infrastructuur betreft (*beveiliging*) en niet zozeer de *veiligheid* van de eindgebruiker. Dat laatste lijkt echter vaak meer de politiek en wetgever te drijven.

De hoofduitkomst van de vragen naar handhaving van Artikel 11.3 Tw door OPTA is dat ondervraagden niet inzien waarom die handhaving nu urgent is. Men vindt het onderwerp zelf echter wel belangrijk. Zij zijn over het geheel terughoudend ten opzichte van het opleggen van verplichte maatregelen aan de bedrijfstak als geheel, zeker als die voorafgaan aan het opleggen van handhaving bij specifieke partijen die nu slecht hun zaken op orde hebben.

6.2 Aanbevelingen

Als eerste stap is onder meer aangegeven dat het verstandig is dat OPTA het veld eens bij elkaar brengt. Daarbij zijn onder meer de volgende aanbevelingen afgegeven:

- OPTA zou als eerste activiteit kunnen gaan meelopen in het veld (bijvoorbeeld bezoeken van relevante bijeenkomsten van RIPE etc.), daarnaast de kennis te verrijken en de goede ontwikkelingen te benoemen.

- OPTA zou een blauwdruk kunnen maken met BCPs en dat onderhouden, daar moet dan een redactiecommissie voor worden opgezet die dat werk gaat doen. Dit zou men kunnen vragen aan het o-IRT-o, maar ook het ECP.NL[24] heeft een taak daarin. OPTA kan daar dan zijn wettelijk mandaat aan binden. Er speelt echter wel een representatievraagstuk, enkele grote marktpartijen zijn geen lid van voornoemde organisaties. Er zijn wel wat opmerkingen te maken bij het meritocratisch model, als het om de huidige informatieverspreiding gaat. Dit is een aardig discussiepunt voor de eerste gespreksronde.

- In het vervolgtraject is het verstandig als OPTA een scherp onderscheid gaat maken tussen de begrippen *beveiliging* [Eng. security] en *veiligheid* [Eng. safety]. Politici hebben de neiging om beiden in de discussies op één hoop te gooien. ISP's kunnen de *beveiliging* van hun systemen en netwerken op orde hebben, maar hebben bij hun klanten vooral de mogelijkheden om de *veiligheid* te beïnvloeden. Bij het onderwerp *veiligheid* spelen bijv. ook fabrikanten een grote rol.

- Veel geïnterviewden zien risico's bij een te formalistische aanpak van de handhaving. De wijze van introductie, oplegging, handhaving en kostenvergoeding die de overheid hanteert bij bijvoorbeeld aftappen, gegevensverstrekking en dataretentie nodigt volgens de ISP's niet in alle gevallen uit om de sector mee te krijgen. De belangen moeten duidelijk in lijn liggen. Er is een 'arms race' aan de gang waarbij dreigingen constant veranderen door de genomen tegenmaatregelen, hierdoor is er een risico dat OPTA 'altijd te laat reageert'. OPTA kan zich daarbij het best richten op maatregelen neergelegd in de al in internationale fora opgestelde Best Current Practices die zijn gebaseerd op open standaarden.

Geïnterviewden zien op het vlak van voorlichting aan eindgebruikers nog steeds een rol voor het Ministerie van EZ. Men acht het, gezien de penetratie van internettoegang, niet zo effectief daar de ISP's bij in te schakelen; beter kan materiaal huis-aan-huis worden verspreid, ondersteund door een campagne.

Wij bevelen OPTA aan zich, mede vanwege het groeiende phishing probleem te concentreren op een discussie met partijen aan de aanbodzijde: HW/SW-fabrikanten, ontwikkelaars van grote elektronische communicatie diensten met financiële en privacygevoelige gegevens (banken, verzekeraars, rijks- en gemeentelijke overheden), SIDN en ISP's.

[24] ECP.NL: Electronic Commerce Platform Nederland

OPTA kan met de sector ook nagaan of er een verband bestaat tussen de door internationale security bedrijven gemeten bovenproportionele blootstelling van in Nederland opgestelde systemen aan Denial-of-Service aanvallen en het ook geconstateerde bovenproportionele aantal sites met Spyware. Daarbij moet worden opgemerkt dat Nederland ook al jaren een bovenproportioneel aantal Internet Hosts kent.

Daarnaast kan OPTA de sector ook helpen door aanpassingen van de wetgeving bij de overheid te agenderen, waar die een dreiging onbedoeld bevordert. Een voorbeeld is het afdichten van de Colportagewetgeving, zodat zaken als 'Domaintasting'[25] niet ook in Nederland als praktijk worden geïntroduceerd na invoering van elektronische orderverwerking voor '.nl' domeinnamen. 'Domaintasting' bemoeilijkt onder meer de opsporing van Spam-verzenders en 'rogue websites'. Omdat dit ook OPTA's eigen opsporingstaak t.a.v. SPAM raakt, lijkt ons een agenderende rol hier zeker op zijn plaats.

[25] 'Domaintasting' is de praktijk dat partijen honderdduizenden domeinnamen enkele dagen uitproberen en dan retourneren.

Annex A Vragenlijst

Hieronder volgt de vragenlijst zoals die gehanteerd is in de gesprekken. De vragen zijn in open vorm gepresenteerd aan de geïnterviewden. Dat betekent dat er bij vragen om dreigingen te benoemen, gezocht is naar wat in interview en survey technieken aangeduid wordt als 'spontaan genoemde antwoorden'. De interviewer hanteerde een vragenlijst met daarop als steun wel een shortlist van potentiële antwoorden die men kon geven bij de specifieke vragen. Deze potentiële antwoorden zijn opgesomd achter een ruit: ◊.

I Beschrijving van de geïnterviewde partij 5:00

1 Bij wat voor soort organisatie werkt u?
2 Wat zijn de hoofdactiviteiten van uw organisatie?
3 Wat zijn de belangrijkste primaire processen van uw organisatie of uw markt?
4 Beschrijft u de omvang van uw organisatie?
5 Wat is de positie van de partij:
   - ◊ Eindgebruiker
   - ◊ Operator
   - ◊ Fabrikant / Ontwikkelaar van software
   - ◊ Anders, ……
6 Welke (soort) organisaties acht u vergelijkbaar met u?

II Wat zijn de dreigingen nu? 10:00

7 Kunt u aangeven wat u nu als de belangrijkste dreigingen ziet (meerdere mogelijk)?
   - ◊ Spam (incl. blogSpam)
   - ◊ Virussen en worms (mail, web, etc)
   - ◊ Trojan sites / Phishing
   - ◊ Spyware / malware / keyloggers
   - ◊ Zombie-PC's
   - ◊ DDoS-attacks
   - ◊ Domeinnaamdiefstal (bij registrar)
   - ◊ ...
   - ◊ Combinaties van deze dreigingen

8 Zou u de genoemde bedreigingen in ernst kunnen ranken?
9 Als we nog nader ingaan op de genoemde bedreigingen kunt u aangeven wat u van elke dreiging het meest ernstige aspect acht?
   - ◊ Spam (incl. blogSpam)? …….
   - ◊ Virussen en worms (mail, web, etc)? …….
   - ◊ Trojan sites / Phishing? …….
   - ◊ Spyware / malware / keyloggers? …….
   - ◊ Zombie-PC's? …….

- ◊ DDoS-attacks? …….
- ◊ Domeinnaamdiefstal (bij registrar)? …….
- ◊ Overige genoemde? ...
- ◊ Combinaties van deze dreigingen? …….

III Wat zijn de dreigingen die opkomen? 30:00

[spontaan]

10 Kunt u aangeven welke dreigingen u ziet opkomen? [meerdere mogelijk]

◊ SPIT (Spam over IP Telephony)
◊ SPIM (Spam over Instant Messaging)
◊ Ad-fraud
◊ ID en (Game) persona theft
◊ Crimeware
◊ DNS-vervuiling en hijacking (op systemen)
◊ ...

11 Wat acht u daarbij de belangrijkste kwetsbaarheden en dreigingen?

[geholpen vragen, indien niet genoemd]

12 Nederland schakelt nu snel over op VoIP, welke risico's loopt men naar uw idee met deze toepassing via het Internet?
13 Levert het verder technisch uiteenrafelen van VoIP extra dreigingen op?
14 Groeien er nieuwe dreigingen door populaire applicaties als Instant Messaging?
15 Hoe moeten we de rol van ENUM en VoIP zien in het licht van kwestbaarheden?
16 Zijn er al kwetsbaarheden aan te geven in de combinatie DNS/ENUM voor VoIP?
17 Kent u gevallen uit uw praktijk van:
- ◊ DNS cache pollution en sessie hijacking?
- ◊ (grootschalig) ID diefstal en impersonatie?
- ◊ Advertentie-fraude?
- ◊
- ◊ ...

18 Hoe schat u de groei van deze dreigingen in?

IV Wat wordt daar nu aan gedaan? 45:00

a. aan de providerzijde

19 Heeft u voorbeelden van maatregelen die een provider neemt om dreigingen in te tomen?
- ◊ Spamfilters (ingress/egress)
- ◊ mail virus check
- ◊ deep packet inspection, blocklists, port-blocking, DNS-filter, proxies, human challengers etc., …

b. aan de gebruikerszijde

20 Heeft u voorbeelden van maatregelen die een gebruiker kan nemen om dreigingen in te tomen?

- ◊ personal firewalls van diverse kwaliteitsniveaus
- ◊ virusscanners etc. [door ISP gedistribueerd?]
- ◊ …

c. door anderen

21 Wat doen anderen (overheden, leveranciers) nu al?

Overheden

- ◊ GOVcert
- ◊ EZ
- ◊ etc: bewustwording consumenten
- ◊ samenbrengen kennis
- ◊ …

Producenten

- ◊ bijvoorbeeld Microsoft: security updates
- ◊ firewall default aanzetten
- ◊ etc.
- ◊ …

V Wat kan er aan gedaan worden? 60:00

d. aan de providerzijde

22 Welke acties of middelen kunnen door een provider worden ingezet om dreigingen te verminderen of vroeg te onderkennen?

- ◊ Quarantaine-netten
- ◊ Honeypots,
- ◊ Intrustion Detection Sensornetten
- ◊ Safe back-up voorzieningen
- ◊ Computer 'wasserette'
- ◊ ...

23 Welke acties zijn grotendeels al met bestaande middelen of beperkte investering uitvoerbaar?

24 Welke maatregelen zou u als absoluut minimum zien?

e. aan de gebruikerszijde

25 Welke acties kunnen er aan de gebruikerszijde worden uitgevoerd om dreiging te verminderen?

- ◊ Vergaande automatisering security-updates
- ◊ Routinematige port-attack scan

- ◊ Cookie-scans & privacy-lekken scans
- ◊ Versleutelde directories en [Extra] beveiligde data-opslag
- ◊ ...

26 Kan een ISP hierbij helpen?

27 Welke maatregelen zou u als absoluut minimum zien?

f. door anderen

28 Wat kunnen anderen (overheden, producenten) doen om dreigingen in te tomen?

Overheden

- ◊ GOVcert
- ◊ EZ
- ◊ etc: bewustwording consumenten
- ◊ samenbrengen kennis
- ◊ …

Producenten

- ◊ bijvoorbeeld Microsoft: security updates
- ◊ firewall default aanzetten
- ◊ etc.
- ◊ …

29 Kan betere voorlichting (zo ja: door wie?) voor ISP's helpen om ISP's hun systemen op orde te laten houden/brengen?

30 Kan verscherpt toezicht helpen om ISP's hun systemen op orde te laten houden/brengen?

VI OPTA/Overheid 0:75

31 Hoe urgent acht u handhaving van de beveiligingsbepaling in de Tw?

32 Welke maatregelen zou u dan verwachten van de overheid?

33 Van wie zou u deze verwachten?

34 Scenario: OPTA adviseert eerst maatregelen, en als het probleem blijft bestaan kan zij maatregelen aan aanbieders, als ultimum remedium, aan specifieke partijen verplicht stellen. Zou u dat scenario positief beoordelen?

35 Hoe zou u (anders) willen dat OPTA invulling geeft aan begrippen als "voldoende beveiliging" en "passende maatregelen" ex 11.3 Tw?

VII Afsluitende opmerkingen 80:00

36 Bent u bereid deel te nemen aan een eventueel vervolg op dit onderzoek?

37 Heeft u een vraag of onderwerp gemist?

38 Wie zouden wij volgens u nog moeten interviewen over dit onderwerp?

Einde 85:00

Annex B Interview NLnet Labs

http://www.nlnetlabs.nl
Het interview is vanwege de achtergrond extra ingegaan op vraagstukken die spelen rond DNS.

Olaf Kolkman is directeur bij NLnet Labs en daarnaast lid van de Internet Archtitecture Board (IAB) en is medevoorzitter van de DNS Extensions Workgroup van de Internet Engineering Task Force (IETF).
Jaap Akkerhuis is onderzoeker bij NLnet Labs en daarnaast lid van de Security and Stability Advisory Committee van de Internet Corporation for Assigned Names & Numbers (ICANN).

NLnet Labs heeft geen bezwaar tegen vermelding met naam en toenaam.

I Beschrijving van de geïnterviewde partij

Stichting NLnet Labs bestaat sinds 2000. Het is een volledig met privaat geld van stichting NLnet gefinancierd laboratorium, deze stichting was de grootaandeelhouder tot in de tweede helft van de jaren negentig van Nederlands eerste Internetprovider NLnet en beheert de opbrengsten sinds de verkoop van NLnet aan het Amerikaanse UUnet / MCI Worldcom. De stichting NLnet Labs werkt onder een charter met een financieel commitment tot 2015.

In de statuten van NLnet labs staat dat het moet werken aan open source en open standaarden ontwikkeling t.b.v. het Internet. Het kennisveld van NLnet Labs beslaat de terreinen *core-netwerken* en *core protocollen* met name het *Domain Name System (DNS)*.

Dit is men aan het verbreden naar het werkveld *addressing & routing*, waarbij men onderzoek doet naar het exploderen van de routingtabellen op het Internet en de schaalbaarheid. Fast memory in routers is te traag en de eisen aan centrale processorcapaciteit groeit sneller dan Moore's Law, waardoor de eenheidskostprijs van routers omhoog schiet. Een rem op zowel IPv6 introductie als nieuwe diensten.

De achtergrond van het NLnet Labs team is het DNS, men adviseert TopLevelDomains en is actief op het gebied van security vraagstukken. ENISA, deels ICANN.

NLnet Labs heeft met 'Name Server Daemon' (NSD) een *authoritative (only) server* ontwikkeld als alternatief voor de oorspronkelijk vrijwel overal op Internet gebruikte DNS software BIND[26]. Komend jaar wordt gestart met een *recursive resolver (unbound)*. De software van NLnet Labs draait nu bij een aantal Top Level Domains (o.a. .nl, .de en .se) en bij de G-, K- en L-rootservers. Een deel van de ontwikkelde code wordt gebruikt in UltraDNS.

Vergelijkbaar met NLnet Labs is het Internet Software Consortium (ISC), de ontwikkelaar van BIND in Californië. Vanwege het charter geeft NLnet Labs alle ontwikkelde software weg. Wel

[26] Berkely Internet Naming Daemon

heeft men voor enkele partijen support contracten. Maar die heeft men liever niet. Het bedrijf prefereert kennisoverdracht.

Een ander bedrijf dat enige overeenkomsten heeft is PowerDNS, dat ook een eigen implementatie van DNS heeft ontwikkeld. PowerDNS probeert echter als bedrijf te opereren en te leven van de support op hun implementaties en functioneert dus niet zozeer als een non-profit onderzoeks- en ontwikkellab zoals NLnet Labs en ISC.

Reactie op uitnodigingsbrief voor het interview

Bij de start van het Interview werd aangegeven n.a.v. de introductiebrief en het daarin beschreven Artikel 11.3 Tw, dat de uitleg die OPTA beoogt te geven aan dit artikel hen een behoorlijke oprekking van het begrip leek.

NSD ondersteund de implementatie van DNSSEC (Domain Name System Security Extensions, zie RFC 2035 en 4035), de nieuwe beveiligde versie van het DNS protocol. De status van deze implementatie hangt van de gebruiker en implementatie af. Men is nog bezig de diagnostiek te verbeteren. Technologisch staat DNSSEC nog in de kinderschoenen, wat betekent dat het protocol af is en de software gereed, echter de markt moet het nog implementeren.

Overheden zouden hierbij een rol kunnen spelen, maar dan vooral als de zakelijke groot-gebruiker, die zij zijn op Internet voor de vele overheidssites en mailservers. D.w.z. als voorbeeldpartij die in aanbestedingen DNSSEC implementaties eist etc. Dat is in Nederland nog niet zo doorgedrongen. In de VS is DNSSEC nu een vereiste bij federale aanbestedingen via FICA /FIMS. Ook Post & Telestyrelsen bevordert nu de implementatie van deze veilige techniek.

II Wat zijn de dreigingen nu?

a. Belangrijkste dreigingen

De belangrijkste dreigingen zijn nu:

- Bots en bad traffic
- Overdrijving van de dreiging, op de loop gaan met oplossingen zonder probleem
- Het kernprobleem end-to-end, iedereen kan services ‘deployen’ op internet, maar dus ook ongewenst verkeer
- De oplossing is risico spreiding door (verdergaande) distributie van resources en software-variatie, daardoor slagen nu DDoS-aanvallen op root-servers niet meer.

Best Current Practices beschrijven hoe men zich met configuratie kan wapenen tegen dreigingen, deze komen voort uit discussies die worden gevoerd in de RIPE[27] community. Daar

[27] Resaux Internet Protocol Europeènne

kan men op inhaken. BCP-38 (gericht op ingress/egress van IP verkeer) is een goed voorbeeld daarvan. BCP-84 behandelt de implementatie van uRPF[28]

De grondoorzaak van bad traffic ligt in besturingssystemen en applicaties die niet goed beveiligd zijn. Er is nu een document in draft[29] over dit vraagstuk, van een IAB workshop.
Dit leidt tot:
- Overgenomen dozen
- Spam
- Virusdistributie
- Zonder toestemming "hosten"

De enige manier om dit te keren is het beveiligingsniveau aan de edge op te krikken.

Een tweede groep dreigingen is de inherente beveiliging van de protocollen (die vaak nog ontbreekt). Hier speelt:
- DNS SEC als opvolger van DNS
- Routing security

DNSSEC is protocoltechnisch klaar , maar de uptake (deployment) moet nog komen. Dit vereist o.a. (Authenticatie) Key-signing.
Ook routering is erg kwetsbaar. Zodra iemand op de grote routers zit (core) dan kan er van alles. De twee voorgestelde oplossingen security oriented-Border Gateway Protocol (so-BGP) en s-BGP, secure BGP zijn niet 'je van het'. Wie deze protocollen aanzet, lekt zijn policies naar andere partijen. Een partij laat dan namelijk zien met wie men peert en welke routing policies men hanteert. Dit is een business probleem en staat brede implementatie in de weg.

- Misbruik van 'zwevende' adresblokken

Er is certificatie van (IP-) adresblokken mogelijk bij de RIPE database. Dat kun je gebruiken om je zone/peering te authenticeren en zo kun je de rondzwevende blokken, die veel door Spammers en Rogue servers worden gebruikt uit je routeringstabel vewijderen. Dit vereist het annonceren van adresreeksen. Het adresblok certificatie 'circus' bevindt zich in een prototype fase.

- Domaintasting

Dit is een praktijk die nu vooral optreed in het '.com' domein. Men registreert 1 miljoen domeinnamen in één klap, registreert alle namen op een paar nameservers, zet advertenties (leidt tot inkomsten) en/ of software op de sites en bekijkt dan welke domeinnamen veel verkeer blijken aan te trekken. Die houdt men en de rest levert men binnen de wettelijke termijn voor elektronische orderafwikkeling (in NL is dat een window van 12 dagen) terug aan de domain name registrar. De schaal voor deze praktijk is een open invitatie voor 'hit-and-run' taktieken van bulletproof hosters om ongezien te opereren (bij teruglevering binnen de termijn vervallen de registratierecords en veelal ook de logs). Het is een hele activiteitentak geworden. Er worden zelfs conferenties over georganiseerd.

[28] Unicast Reverse Path Forwarding, een feature op routers om het bronadres te controleren
[29] http://tools.ietf.org/html/draft-iab-iwout-report

b. Ranking en ernst van bedreiging

Het overnemen van hosts/stacks/applicaties en die dan gecontroleerd dingen laten doen acht men het meest ernstig. Dit moet je uiteindelijk actief opsporen in strafrechtelijke zin. Belangrijk hierbij is dat er binnen de overheid één specialistische club is met de kennis.

III Wat zijn de dreigingen die opkomen?

In de vorige paragraaf is 'domaintasting' genoemd als praktijk in het '.com-domein'. Een aantal marktpartijen lobbyen bij SIDN om ook elektronische orderverwerking in Nederland in te voeren. Nu zorgt de eis om papieren contracten met klanten te hebben nog voor een rem. Dan gaat echter ook hier de Colportagewet voor elektronische levering (tot 14 dagen op zicht met recht op retour) gelden. Het .nl-domein is nu het grootste TopLevelDomain dat nog geen elektronische orderverwerking kent. Men vermoedt dat de partijen die lobbyen het oog hebben laten vallen op 'domaintasting'. OPTA zou zich sterk kunnen maken voor aanpassing van de wetgeving, zodat deze juridische sluiproute kan worden afgesloten.

Wat betreft ENUM (dat draait op DNS-servers) zou men al vanaf de start kunnen gaan werken met DNSSEC.

Men acht het een grote bedreiging dat het end-to-end karakter van Internet dreigt te worden doorbroken, dit is juist de motor van de innovatie.

IV/V Wat wordt daar nu aan gedaan en wat kan er aan gedaan worden?

Genoemd wordt honeypot netwerken (die zijn gericht op detecteren van poging tot overname van PC's)
NLnet is van mening dat je er niet iets tegen kan doen door te beginnen met reguleren en ziet vooral een taak in voorlichting voor de overheid, o.a. aan de eindgebruikers zoals bij Surf-op-Safe.
Ook adviseert men zoveel mogelijk open standaarden te implementeren, zodat een provider zelf de regie houdt over wat er gebeurd.
Daarnaast achten zij het vooral van belang de 'meat space enforcement' te versterken tegen cybercrime. Misschien is het een idee om als een kapstok de vervolging te starten van enkele notoire criminele gevallen en miscreanten [Ed. dus meer strafrecht lijn dan regulering]

Technisch is er duidelijk sprake van 'arms races'. Genoemd worden activiteiten van de IAB en IETF, echter er bestaat niet zoiets als het Evil bit protocol.

NLnet Labs is van mening dat een normale ISP klanten niet kan forceren tot implementaties.

VI OPTA/Overheid

NLnet Labs is van mening dat de urgentie niet bij handhaving van de beveiligingsbepaling in de Tw ligt. Wel kan men ISP's bewuster maken van het bestaan van Best Current Practices. Hierbij wordt nogmaals gerefereerd naar BCP-38 (ingress/egress beheersen van het IP verkeer op het eigen netwerk), daarbij is het probleem wel dat prudente handelingen van een ISP vooral de buren (ook die in de Cariben) bevoordelen.

Men vindt dat er geen 'Internet Police' moet worden opgetuigd en dat OPTA dat ook niet in de handhaving moet gaan proberen te worden. Internet moet het vooral hebben van principes van de 'goed burgerschap' en het aanspreken van de buren.

Hiervoor ziet men de volgende route: probeer als eerste stap de volgende zaken te doen:
- Loop mee in het veld (bijv. RIPE meetings bezoeken)
- Verrijk de kennis
- Benoem goede ontwikkelingen

Men ziet het geschetste scenario voorbij de rol van adviseren voor OPTA niet zitten. En adviseert OPTA vooral om te zorgen dat na de eerste stap de verschillende groepen bij elkaar komen. Hierbij wordt als voorbeeld de aanpak in Zweden genoemd van PTS[30]. De wetgever stelde daar eisen t.a.v. access / universele dienst op na met technische Internet experts te hebben gesproken. Er wordt ten aanzien van het meelopen in de bestaande organisaties gewezen op de activiteiten van Thomas de Haan (DGET) en in Zweden naar de rol die Patrick Fältström[31] daar speelt.

Men weet niet snel aan te geven wat onder 'passende maatregelen' volgens artikel 11.3 Tw moet worden verstaan.
- het is een 'arms race'
- kenmerk is het constant veranderen, 'formele actie is vermoedelijk altijd te laat'
- richt de zaak op implementatie van open standaarden, dan is duidelijk waarover men het heeft en is het makkelijker te weten waar de gaten zitten.

VII Afsluitende opmerkingen

Men wil graag op de hoogte worden gehouden van een eventueel vervolg

[30] Post & Telestyrelsen
[31] Zweedse medewerker van Cisco, die zich intensief met safety en security zaken bezighoudt in Europa en ook één van de drijvende krachten is achter ontwikkelingen van o.a. ENUM

Stratix

Annex C Interview SURFnet

http://www.surfnet.nl

Jacques Schuurman is account adviseur bij SURFnet en hoofd van het SURFnet-Computer Emergency Response Team.

Jacques Schuurman heeft geen bezwaar gemaakt tegen vermelding met naam en toenaam.

I Beschrijving van de geïnterviewde partij

Jacques Schuurman werkt sinds 1998 bij SURFnet, zijn achtergrond is informatica en daarvoor was hij actief in netwerkbeheer op het Campusnetwerk en de Centrale Rekendienst van de Vrije Universiteit. Sinds 1999 is hij het hoofd van SURFnet-CERT.

SURFnet is de aanbieder van netwerkdiensten aan het hoger onderwijs en onderzoek. Het gebruikt daar sinds 1989 het Internet Protocol voor. SURFnet is vanwege zijn doelgroep een besloten netwerk (niet-openbaar in de zin van de Tw). De klanten zijn de instellingen, de gebruikerspopulatie omvat de medewerkers en studenten van die instellingen. De SURFnet organisatie telt 62 werknemers.

Vergelijkbare organisaties zijn te vinden buiten Nederland, de zogenaamde National Research & Education Networks.

Reactie op uitnodigingsbrief voor het interview

- geen specifieke opmerkingen

II Wat zijn de dreigingen nu?

De belangrijkste dreigingen nu komen voort uit het feit dat gebruikers *always on* zijn. Hierdoor kunnen niet alleen machines worden gekaapt, gebruikers merken het niet meer. De kaping werkt op de achtergrond.
Het gevolg is “rotzooi”.

- Gebruik als robots door de kaper
- Deelhosting (illegale) bestanden op de gekaapte machine(s)

Dat laatste gebeurt veelal diep verborgen in de directory-boomstructuur (is men dan strafrechtelijk aansprakelijk, bewijslast? vervolgbaar?).
Typisch gevonden materiaal op die plaatsen zijn auteursrechtelijk beschermd materiaal zoals films, of strafrechtelijk verboden materiaal zoals kinderporno.

De tweede belangrijke dreiging is Identity Theft

- dit is mogelijk door het uit allerlei contexten genereren en bij elkaar harken van een persoonsprofiel: plots wordt er van je Credit Card een betaling afgeschreven voor autoverhuur …

De derde grote bedreiging zijn de vormen van Social Engineering. Hier rekent Schuurman ook de vele varianten van Phishing en deceptie van schijnbaar vertrouwde partijen, waaronder trucs met wormvirussen die zich vooral via het adresboek verspreiden naar relaties en daardoor veel succes hadden.

Als ranking kan men stellen dat de individueel gerichte acties (ID diefstal) voor de persoon erger zijn. Echter vanuit de continuïteit van Internet is technische overname [door scriptkiddies] veel erger.

Impersonatie kan zijns inziens worden gezien als een duidelijke rechtshandeling. Of de identiteitsdief wordt er financieel beter van, of hij wil zijn doelwit er per sé slechter van laten worden (bijv. reputatie besmeuren).

Bij bedrijven is de dreiging meer een instrument (afpersing). Echter de consument is kwetsbaarder.

III Wat zijn de dreigingen die opkomen?

De gekaapte machines en bandbreedte zijn steeds meer handelswaar. 500 machines worden voor 50ct per stuk aangeboden met een pluk bandbreedte. Het totale volume verhandelde machines wordt echter steeds grootschaliger en de partijen erachter worden steeds crimineler. De tijd van de puber is geweest. De grootste dreiging is de professionalisering.

Schuurman ziet geen grote risico's voor VoIP tot nu toe. Bij goede VoIP implementaties zijn er over internet veelal geen betalingen, voor diefstal van (pre-paid) accounts is VoIP nu nog te exotisch. Het beeld van Schuurman is dat VoIP nu vooral grootschalig wordt uitgerold als onderdeel van een bundel.

Hij ziet een belangrijker probleem na de grootschalige migratie naar VoIP in de risico's die dan ontstaan als IP plat gaat. Dan is er opeens geen out-of-band[32] meer! Telefonie is nog steeds bedrijfskritisch.

Wat betreft risico's voor Routing Engineering en DNS vervuiling ziet Schuurman niet zo grote dreigingen. DNSSEC is 'hartstikke deployable', maar niemand doet het. Dan is het kennelijk nog niet nodig. Toen ooit de root-servers werden aangevallen gingen A t/m F eruit, maar bleven de hogere letters tot en met K in de lucht.

[32] Veel private computernetwerken en industriële apparatuur worden nu op afstand beheerd door bij storing via modemlijnen in te bellen.

IV/V Wat wordt daar nu aan gedaan en wat kan er aan gedaan worden?

Als tegenactie tegen cyberellende zoals bijvoorbeeld identiteitsdiefstal, zeg maar de afdeling contraspionage, zijn er door een internationale groep CERTs ca. 10 machines neergezet die continu observeren maar zelf geen verkeer aantrekken. Als zo'n machine dan toch geraakt wordt vanaf een kennelijk geïnfecteerde machine, is boven elke twijfel vastgesteld dat die machine daadwerkelijk geïnfecteerd is.

Een andere belangrijke trend is naar zijn indruk dat providers meer en meer netwerk "wolken" voor zichzelf willen houden en die afschermen van het open Internet (o.a. bij VoIP is dit goed zichtbaar). Het oude "ideaal" van één groot open Internet keert niet terug. Die opmerking plaatst hij vooral in het licht van organisatie. D.w.z. de fundamentele architectuur houdt wel de principes aan van end-to-end, maar providers schermen delen af.

End-to-End beveiliging is uiteindelijk waar de zaak naar toe moet gaan. Dat betekent dat gebruikers zelf de parameters moeten stellen hoe veilig zij willen opereren. Diegenen die niet weten hoe ze dat moeten doen kunnen geassisteerd worden door mensen die het wel weten. Je krijgt dan twee hoofdmodellen, de minimalistische provider of juist de partij die zich richt op "maximale assistentie" (voorbeeld SimPC, beheert en bewaakt tot op de desktop).

De wetgever heeft een taak, het gaat hier om regeling van gedragingen in een openbare ruimte. Dat is ook buiten Internet een vanzelfsprekende taak van de wetgever.

Internet bestaat materieel wel als gekoppelde privé ruimtes, maar maatschappelijk wordt dat niet zo ervaren. "Als twee mensen elkaar in de V&D de hersens staan in te slaan, dan heeft het OM gewoon jurisdictie, ook al is een winkel geen openbaar terrein. Men kan ook gen rechercheurs buiten houden, het gaat erom dat burgers zich op individueel niveau beschermd weten door de overheid.

Maatregelen van providers zijn er in verschillende soorten.
- Organisatorisch & juridisch kunnen zij veel gedrag regelen in de gebruikersoveenkomst
- Men moet dan wel het gedrag monitoren, pro-actief optreden bij normoverschrijding
- Het is wel nodig dat er beter wordt gereageerd op rechtshulpverzoeken (overheidsinstanties)

Operationeel Incident Response Team Overleg (o-IRT-o)
- Door SURFnet zijn samen met GOVCERT de statuten geschreven van de o-IRT-o:
  - Zij komen 1 keer per 2 maanden bij elkaar
  - Er is een telefoonlijst voor spoedgevallen
  - Men deelt met elkaar de trends en de bedreigingen die zijn gezien
  - Het is een besloten overleg met een geheimhoudingsverklaring
- Voorbeeld: het o-IRT-o gaat bijeen geroepen worden voor de Tweede Kamer verkiezingen (elektronisch stemmen over internet)

Voor SURFnet geldt nu in de richting van eindgebruikers, dat zij veel advies aan instellingen geven. Zij kijken op verzoek ook wel eens naar poorten etc.

Monitoring
SURFnet heeft voor monitoring twee soorten systemen actief:
1. Het Intrusion Detection System Semantisch
2. Verkeersgegevens (flow) analyse Syntactisch

Voor het IDS wordt aan een aangesloten instelling een USB-stick uitgedeeld, waarmee een pc die vanaf de stick kan booten met de applicatie direct kan gaan werken. Inbraakpogingen / besmettingspogingen worden door het apparaat dan meteen doorgestuurd naar een centraal systeem voor de registratie, simulatie (van de kwetsbaarheid) en analyse.

Voor de flowanalyse wordt Netflow data uit de routers gehaald om bijv. portsweeps te zien. Hierbij wordt met een bemonstering van 1:100 pakketten geadministreerd bij welke flow dat pakket hoort. De flowanalyse is een speciaal zelfontwikkeld systeem deels in een Europees project. De Netflow data worden op de Borderrouters[33] opgepakt. Het wordt nu naar alle NRENs uitgebreid.

In de centrale verwerkingssystemen voor de flowanalyse zitten profielen en alarmdrempels. Er worden nu meer dan 3000 flows per seconde geanalyseerd. Men herkent dan praktisch in real-time als bijvoorbeeld een PC op port 25 Spam gaat versturen. Er is met deze patroonherkenning real time alarmering van security problemen in het Netwerk Operations Center (dat bij SURFnet een 24x7 bewaking heeft).

Wat betreft organisatorisch overleg tegen dreigingen constateert Schuurman dat er al landen zijn die een goed functionerend overleg hebben. Echter hoe groter het land, des te kleiner is de kans dat dit al is gebeurd.

Voor de overheid ziet hij bij bedreigingen vooral een rol in *voorlichting* en *herhaling van voorlichting*. ISP's kunnen daarbij helpen, vooral met instrumenten waarmee zij hun eigen machines op orde kunnen houden. Hier speelt vaak de kwestbaarheid van automatisering (verwaarloosde systemen).

De Rol van ISP's gezamenlijk moet een duidelijke strategie in de markt zijn.
Bij elke ISP past een eigen niveau van voorlichting
- een soort bijsluiter heeft wel eenzelfde vorm
- vermijd intussen echter stemmingmakerij
- bangmaken helpt niet

VI OPTA/Overheid

Handhaving van de beveiligingsbepaling in de Tw acht Schuurman niet urgent, maar wel belangrijk. Hij ziet een omgekeerde trap: de mogelijkheid van handhaven is een basisvoorwaarde, maar daarbovenop komt de invulling van de voorlichtingstaak.

[33] Machines aan de rand van een domein van een ISP, hier wordt IP peering en transit op aangesloten

Men moet er vanuit gaan dat gebruikers geen kennis hebben, maar wel praten met de ISP. Het is daarbij van belang dat ze wel goed worden voorgelicht, maar niet bang gemaakt.

Het scenario dat OPTA schetst om eerst maatregelen te adviseren en als het probleem blijft bestaan verplichtingen te stellen beoordeelt hij niet positief.

Hij stelt voor dat OPTA zich richt op het maken van een blauwdruk met Best Current Practices en dat gaat onderhouden. Dat betekent dat er een redactiecommissie moet komen die dat werk gaat doen. Het o-IRT-o kan gevraagd worden. Echter ook ECP.nl zal een soort taak daarin moeten hebben. Het voordeel van OPTA is dat zij wel een mandaat heeft. Maar dat niet moet brengen.

VII Afsluitende opmerkingen

Schuurman is bereid deel te nemen aan een eventueel vervolg op dit onderzoek.

Potentieel relevante personen/partijen:
- GOVCERT
- Martijn v.d. Heijden, KPN-CERT
- Bankenwereld // Verzekeraars, die hebben ook een intern productclubje. Contact bijv. Wim Hafkamp, Rabobank
- Multinationals, met hoofdzetels in Nederland, hun diensten worden concreet bedreigd

Annex D Interview CAIW

http://www.caiw.nl

Hans van der Giessen is directiesecretaris bij CAIW Holding. Hij is eerder, als bestuurslid bij de toenmalige branchevereniging NLIP, nauw betrokken geweest bij de opstelling van het protocol voor het aftappen van internet en is nu op persoonlijke titel bestuurslid van de Stichting NBIP.

Hans van der Giessen heeft geen bezwaar gemaakt tegen vermelding met naam en toenaam.

I Beschrijving van de geïnterviewde partij

Hans van der Giessen is directiesecretaris van CAIW Holding uit Naaldwijk. CAIW zet onder het merk CAIWAY, verschillende diensten (radio en televisie, internettoegang, vaste telefonie en zakelijke diensten en verbindingen) in de markt, hoofdzakelijk over het eigen kabelnet en netwerken van andere exploitanten.
CAIW Holding opereert onder de Regeling CAIW, een samenwerkingsverband van de gemeenten Westland en Midden-Delfland. CAIW Holding heeft drie werkmaatschappijen: CAIW Netwerken, CAIW Diensten en CAIW Media.

CAIW heeft de afgelopen jaren een aantal kabelnetten buiten het oorspronkelijke werkgebied overgenomen; als grootste het net van ONS CAI in Schiedam medio 2006. Het bedrijf levert nu aan zo'n 150 duizend huishoudens radio en televisie.

CAIW, die in 1995 commercieel kabelinternet introduceerde, levert nu breedband kabelinternet aan ca. 65.000 abonnees. Naast levering via het eigen netwerk gebeurt dit ook via netwerken van andere exploitanten. Sinds medio 2006 wordt grootschalig vaste telefonie op basis van VoIP aangeboden; er zijn nu ca. 15.000 abonnees. Op dit moment benadert men primair de kabelinternetabonnees.

CAIW heeft ca. 150 werknemers.

CAIW geeft aan het begin van het interview aan dat het primaire proces is het aanbieden van diensten aan klanten. CAIW is niet in het leven geroepen voor het geven van voorlichting, het meewerken aan onderzoek van de overheid of het geven van assistentie bij opsporing.

CAIW ziet de kabelexploitanten UPC, Essent, Casema, Delta e.d. als vergelijkbare bedrijven (al zijn er grote verschillen in de schaalgrootte). CAIW heeft bij wijze van proef een nieuwbouwwijk in Naaldwijk volledig verglaasd. Daar wordt nu ook TV over IP geleverd.

Reactie op uitnodigingsbrief voor het interview

Van belang is volgens Van der Giessen het vraagstuk wat veiligheid nu precies is.

- Klanten koppelen willens en gedeeltelijk ook wetens apparatuur die zij niet volledig doorgronden aan een wereldwijd netwerk; CAIW verschaft hen daar slechts toegang toe.
- Voorlichting is hier wezenlijk; want hoewel dit gedrag lastig is voor de klant en voor de provider wil de klant niet anders.
- De helpdesk is eigenlijk gericht op toegang maar levert vaak een hele hoop algemene computersupport (waaronder op het vlak van veiligheid en beveiliging) eromheen.
- Bij het artikel 11.3 Tw denkt hij primair aan
  - 'veilig Internet' waaronder het wel eens eerder geopperde 'PC rijbewijs';
  - 'kinderen & Internet'

II Wat zijn de dreigingen nu?

Een belangrijke dreiging is er voor een nieuwe PC met bijvoorbeeld Windows XP Home Edition. Voordat Service Pack 2 erop staat is hij al overgenomen.

- virussen, wormen, trojans, dialers[34], phishing, spam & pharming[35], ongewenste berichten tot aan PC Distributed Denial of Service attacks.
- Dreiging is het kunnen misbruiken van diensten waarop iemand anders zich heeft geabonneerd, gebruik van diensten zonder wachtwoord (telefoon, internet) gebeurt, maar je ziet het niet zo snel.
  - Bestrijding is daarbij een probleem omdat CAIW niet kan verhinderen dat klanten zelf identificerende gegevens uit handen geven.

Bij de vraag naar een ranking worden virussen en wormen als de meest voorkomende zaken aangemerkt, maar de schade is nu vaak beperkt

- plaagvirussen zorgen voor veel dataverkeer
- pharming (overname via DNS) is van belang
- bijna alle problemen die leiden tot financiële schade en inbreuk op de persoonlijke levenssfeer komen nu voort uit Phishing.

Veelal onbedoeld misbruik (bijvoorbeeld vanuit een overgenomen PC) leidt tot klachten van andere aangeslotenen en vanuit andere internetproviders. Dat probleem is soms alleen maar op te lossen door de aansluiting van de klant te blokkeren. Dit gebeurt uiteraard pas na tevergeefs bellen en mailen.

Een evenzeer ernstig probleem in de persoonlijke levenssfeer is pesten of (seksueel getinte) intimidatie, zoals dat bijvoorbeeld kan spelen binnen een schoolgemeenschap.

[34] Ook bij kabelmodems werkt dit vaak, klanten laten de modempoort van de PC aangesloten zitten op het netwerk van KPN.

[35] Dit is een term voor het misleiden van de eindgebruiker door internetadressen onmerkbaar te laten verwijzen naar nagebootste sites.

III Wat zijn de dreigingen die opkomen?

De dreigingen die er nu zijn blijven nog wel even in stand. Een bijzonder punt van aandacht is wel de nieuwe, deels nog niet ontdekte, speelruimte die VoIP-, SIP- en ENUM- implementaties geven. Ook verspreiding via peer-2-peer neemt toe; echter de hoofdmoot is nog steeds verspreiding via e-mail.

De problematiek neemt toe, waar aanvallen eerst gericht waren op Microsoft software moeten nu ook Linux en OSX (Apple) regelmatig security updates uitbrengen. Het probleem is dan vaak de interpretatielaag over de applicaties.

Technische maatregelen in kabelmodems en routers garanderen op zich geen afdoende beveiliging. In de begindagen van kabelinternet bij CAIW is eens een lijst met accountgegevens in de openbaarheid gebracht. De beveiliging (procesmatig en technisch) van de persoonlijke levenssfeer van de eindgebruiker loopt vaak parallel aan de beveiliging van de dienstverlening van de aanbieder, die zich inspant om onbetaalde toegang tot betaalde dienstverlening te voorkomen. Zo wordt er vor de extra pakketten van digitale televisie een moeilijk na te maken smartcard gebruikt.

Bij VoIP via kabelmodems is het van het grootste belang dat men gebeld kan worden en kan bellen. Dit is kritischer dan beschikbaarheid van internettoegang. Eén uurtje uit de lucht kan niet. Er is mede daarom een logische scheiding tussen netwerken gerealiseerd; die heeft er in geresulteerd dat het telefoondeel niet toegankelijk is vanaf het publieke internet. Maar bij het aanbieden van ‘softphones’ (telefonie via de microfoon en de speakers van de PC) als product vervalt deze mogelijkheid. Het risico voor de eindgebruiker is dat iemand anders voor hoge gesprekskosten kan zorgen. En de eindgebruiker zal dat risico neer willen leggen bij de provider.

ENUM, in essentie de mogelijkheid om via telefoon en internet “altijd dichtbij” te zijn onder één nummer, heeft uiteraard de belangstelling vanuit marketingorganisaties, zelfs reeds voor aanbieders technisch actief werden. De mogelijkheden zijn nog niet allemaal ontdekt. De doorsnee eindgebruiker overziet de mogelijkheden niet en is ook nauwelijks in staat om via een ‘self service’ pagina de juiste instellingen te doen om bijvoorbeeld telemarketeering te voorkomen.

Van der Giessen signaleert dat de belangstelling vooral uitgaat naar het deel waar geld mee te verdienen is. Dat zijn dan:

- dure nummers bellen
- dure content afnemen

op kosten van iemand anders.

IV/V Wat wordt daar nu aan gedaan en wat kan er aan gedaan worden?

CAIW participeert niet in het o-IRT-o (zoals aangegeven door SURFnet is dit een besloten groep op invitatie).

Op het gebied van VoIP zijn de maatregelen vrij passief en niet intrusief, door de scheiding van verkeer waardoor VoIP toestellen niet via het publieke internet te benaderen zijn. Virusfiltering kan de klant niet uitzetten, behalve op speciaal verzoek. Spam kan worden gecategoriseerd in verschillende klassen: doorlaten, markeren, blokkeren, wegzetten.
Mail-relay wordt gesignaleerd, uitgaand verkeer wordt op egress gefilterd, ook wordt port 25 uitgaand geblokkeerd (tegen misbruik) en een stuk voorlichting gegeven.

De draadloze routers (WiFi) die veel klanten onbedoeld open hebben staan, zijn nu verder een bron van risico. CAIW heeft geen Quarantainenet, voor de applicatielaag, echter wel een ‘walled garden’ voor het randapparaat (dat over het gedeelde kabelmedium werkt). Sinds zij hun model koopmodems voeren is er een afgeschermde omgeving gecreëerd waar een modem de eerste keer terechtkomt en zich identificeert. Pas als de abonnee relaties en het nieuwe apparaat bekend zijn is de klant aangesloten en wordt de ‘walled garden’ verlaten..

Van der Giessen ziet vooral ook een rol voor de leveranciers van software.

Hij ziet echter, gezien de druk van consumentenorganisaties op ISPs toch liever dat OPTA het voortouw neemt. CAIW hanteert nog steeds onder meer de bij de NLIP ontwikkelde codes:
- geen direct marketing door derden
- goed netwerkbeheer
- hoofdstuk 1: IP adressen die niet van jezelf zijn blokkeren

ISP’s dienen geen misbruik te maken van hun positie (Direct Marketing geruchten circuleren in de markt over enkele ISP’s, die klantgegevens aan derden leverden). Er dient een bijzondere aandacht te worden gegeven aan dat aspect in de overeenkomsten met klanten.
De rol van de overheid ziet van der Giessen toch meer bewustmakend en voorlichtend. Daarbij denkt hij dat consumentenbewustmaking primair iets is voor de overheid, zoals EZ.

Wat verdere verantwoordelijkheden van consumenten betreft denkt hij over Internet toch meer in de lijn van de wegenverkeerswet, daar geldt ook dat je een helm op moet voor de bromfiets.

De kosten voor het filteren van spam en virussen draagt de consument in wezen zelf.

VI OPTA/Overheid

Hij acht een veilig netwerk een zaak van goed ondernemerschap. Echter, de wijze waarop de overheid nu vaak enigszins gerelateerde maatregelen introduceert, oplegt, handhaaft en de wijze waarop de daaraan verbonden kosten worden vergoed nodigt niet bepaald uit om de sector mee te krijgen, ook niet op andere terreinen.

OPTA zoekt nu met een vraag naar de rol voor handhaving Artikel 11.3 Tw, maar er staat in de krant[36] in zoveel woorden toe de uitspraak dat ze gaat handhaven. Het lijkt hem verstandig om dit proces niet te starten met uitgesproken meningen. OPTA zou er het best voor kunnen zorgen dat belangen sporen: een veilig product, prettig voor de eindgebruiker, niet schadelijk voor de persoonlijke levenssfeer.

De rol van de overheid en het toezicht ziet hij dan vooral voor de punten waar de industrie dat niet zelf gaat doen. Een ISP gaat niet aan een klant in detail alle risico's opsommen, wanneer hij een aansluiting probeert te verkopen, behalve als het moet (zoals nu in beperkte mate bij financieringen), d.w.z. min of meer afgedwongen.

VII Afsluitende opmerkingen

Van der Giessen geeft aan bereid te zijn deel te nemen aan een eventueel vervolg op dit onderzoek.

Wat hij in de vraagstelling had gemist is wat hij bij het openingsstatement inbracht over de rol van een ISP / operator in de bedrijfstak en de betekenissen van veiligheid en beveiliging.

Hij zou bij deze discussie graag ook fabrikanten en leveranciers betrokken zien worden, hun rol is nu onderbelicht.

[36] AD Den Haag, 27 okt. 2006, artikel n.a.v. Consumentenbond symposium Internetveiligheid 26 okt.

Stratix

Annex E Interview Xs4all

http://www.xs4all.nl

Scott McIntyre, Security Officer bij Xs4all en lid van het Steering Committee van het Forum of Incident Response and Security Teams (FIRST)
Simon Hania, Technisch Directeur bij Xs4all.

Scott en Simon hadden geen bezwaar gemaakt tegen openbaarmaking

I Beschrijving van de geïnterviewde partij

Xs4all is een ISP die ook telefonie en video levert. De aandelen zijn in handen van KPN. Het bedrijf had eind september 390 duizend klanten, waarvan 262 duizend met breedband.

XS4all ziet zich in de eerste plaats als een Network Service Provider. Men is de afgelopen jaren verandert naar een service op Internet die levert over netwerken van derden en bundels verkoopt. Het bedrijf is een Fixed en Mobile Virtual Network Operator, men levert support via de helpdesk.

Het product is een continue levering van gebruiksrecht. Men heeft als doel kwalitatief hoogwaardig te zijn en als de beste provider bekend te zijn. Daarbij mikt men er op eindklanten zoveel mogelijk eigen verantwoordelijkheid te geven, de keuze is voor de contractant, men probeert zo lang mogelijk die ondergrens te handhaven.

Reactie op uitnodigingsbrief voor het interview

Xs4all wijst er vooraf op, dat in de artikeltekst de begrippen *veiligheid* en *beveiliging* worden gebruikt. In het Nederlands wordt dat vaak door elkaar gebruikt. In het Engels is een scherper onderscheid tussen *safety* en *security* Men is benieuwd naar de termen die in de Europese tekst zijn vervat. Wat betreft het begrip ‘veiligheid’ een ‘stalker’ kan ook een naar gevoel oproepen.

Xs4all observeert een volstrekt eenzijdige attitude bij de consumentenbod (A. Sixma).

- Internet is niet iets wat je consumeert, maar wat je gezamenlijk maakt. Dan is hoe je je gedraagt ook van belang
- Wat niet wordt beantwoord is: Wie zijn er allemaal actief in de keten? En dan wie moet wat doen? En als OPTA wat doet, is dat naar de (providers) telecomsector, wie richt zich daarbij dan tot de klant.

II Wat zijn de dreigingen nu?

Privacy is de belangrijkste dreiging, er is meer en meer risico voor informatiegegevens.
Informatie die van/over je gaat, die komt beschikbaar

Sociale dreigingen, werkwijzen om die data aan je te onttrekken
- social engineering (mens naar mens)
- phishing
- iedere vorm van 'malware', cracks verkocht via p2p methoden.

Praktisch voorbeeld:
- Een Australische bank is recent aangevallen met een DDoS aanval.
- Tegelijk ging eer een mail uit: "having problems","please use other site". Daar trapt vrijwel iedereen in.
- Dit is georganiseerde misdaad, vroeger was het meer scriptkiddies en daarvoor hackers.

Vage convergentie, het risico en de dreiging is dat dit ideeën en de mentaliteit van de telefoon en videowereld op het net brengt.
- Caller ID op telefonie, dit is opener bij VoIP.
- De klant kan niet goed zien hoe de dienst jouw telefoonnummers afhandelt, o.a. impersonatie risico met caller ID.

Mobiliteit: PDA's, organisers, mobiele telefoons, Bluetooth, WiFi-drivers, HP/Dell/Gateway. Dit komt niet van Microsoft, dus geen update. Men kan een trojan installeren 'Phone home'.

Bij Sony en Nokia betekent een upgrade: koop een nieuw toestel. Een SW/HW probleem.
Software is perfect, maar het zit vol met programmacode in *C*. Dat betekent altijd wel buffer overflows. De opleiding en achtergrond dekken dit niet.

Rest: gewoon het gebruikelijke:
- geen update = niet beveiligd
- Slammer worm kan werken op oude embedded software
- Door dial-up naar breedband is dit hard gepakt, geen upgrade.

Wanneer iemand met kaal Windows XP bij Xs4all op het net komt, dan duurt het 11 seconden voordat iemand je IP-adres raakt.

Landen met VDSL en glas bieden meer upstream, dit betekent in de praktijk dat de dreiging toeneemt.

De grote meerderheid van 'Malware' gaat nu naar Botnet controllers.

Internet / breedband technologie is een commodity geworden. Dit heeft vreemde effecten.
- Beschouw het functionaliteitsniveau van auto's met Internet, bijv. een content management systeem. Veel scholen hebben bij Xs4all nu site@school. Dat is uiteindelijk op PHP gebouwd. Daarin zat diep in de code iets mis en toen midden in de zomer tijdens de Israël / Libanon oorlog een 'defacing wedstrijdje' uitbrak, werd via "Google" met de juiste zoektermen voor het PHP-programma een hele rij servers gevonden en gedefaced. Scholen waren midden in de zomer echter gesloten, docenten onbereikbaar, toen is er een hele rij sites maar uit de lucht gehaald, omdat ze gekraakt werden …
- Deze casus geeft een gevoel van onveiligheid. Het is echter

  - Een software engineering probleem
  - Een beveiligingsprobleem
  - Een veiligheidsprobleem

- Type goedkeuring is onzin het is geen gesloten systeem, maar open
  - Dus moet je ook daar nu een verbetercyclus implementeren
  - Service providers inschakelen
  - Relatief onbezorgd software updaten.

Omdat de software monocultuur minder extreem is bij mobiel dan bij de PC valt dit minder op. Maar essentieel is dat de dynamiek te groot is.

- E-government, het vertrouwen van mensen is laag in DigiD, Burger Service Nummer etc. Er zijn ca. 200.000 mensen in Nederland met Trojan's en keyloggers op hun PC, schat Xs4all uit metingen. Van deze mensen kan de digitale identiteit worden ontvreemd zonder dat er één veiligheidsinbreuk aan de serverzijde bij de overheid is gemaakt, simpelweg door screendumps als ze ingelogd zijn in hun 'Digitale Kluis'. Dit feit wordt door de overheid tot nu toe straal genegeerd.

- Meer financieel gemotiveerde misdaden, meer diensten
  - Microbetalingen
  - Telecomfraude, de schade blijft nog beperkt
  - Maar meer geld wordt gekoppeld aan meer diensten

- Het maatschappelijke risico is voor arme mensen, die werken met oudere spullen en kunnen zich vaak geen nieuwe upgrade veroorloven. Die kosten meer dan de oude versies, wel/geen PC-privé, iedereen die niet betaalt ontvangt geen upgrades.

- Uit de statistieken van bezoeken vanuit Azië valt goed te zien dat er erg veel "US/English" versies worden gebruikt. Dat zijn vrijwel zeker illegale kopieën
  - Dat betekent dat (automatische) patching daar dus niet werkt
  - N.B. dit is geen pleidooi voor software upgrades

III Wat zijn de dreigingen die opkomen?

Een deel van de nog opkomende dreigingen is in de vorige paragraaf al benoemd.
Een belangrijke trend is de verschuiving naar mensen die zelf iets doen. D.w.z. geen zichzelf vermenigvuldigende wormen meer. Gedrag wordt steeds belangrijker.

Schrijvers van kwaadaardige software worden steeds beter. Ze leren van eerdere versies. Er wordt steeds meer slapende software geproduceerd.
De Sony-rootkit dit jaar was het echte probleem, voor een legitiem doel werd veiligheid compromitterende software misbruikt.

Het verschil met de auto is dat niet iedereen aan de auto gaat knutselen, maar iedereen sleutelt wel aan de PC.

Het VoIP risico is vooral een vraag hoe open dit wordt neergezet in de markt.
- Elke real-world implementatie is in Nederland redelijk dicht getimmerd.
- Xs4all heeft vanwege de aftapeisen een veel centralere server implementatie neer moeten zetten met een minder open peer-2-peer karakter
- Bij VoIP en publiek ENUM is de operational excellence nog een vraag. SIDN is geen Ams-IX of COIN. Of zij een kritische high-performance kunnen runnen is de vraag.
- Je ziet nu een situatie ontstaan van server federation, groepen marktpartijen die elkaars gegevens vertrouwen.
- Het gebruik van Instant Messaging is alsof men met blinddoek op en de neus dicht in het café gaat staan praten.
- Na IM komt de MySpace en de Flash content, alles wat populair wordt, wordt riskant als vehikel om Keyloggers en screendump software stiekem te installeren.

Alle dreigingen blijven op de achtergrond aanwezig. Nieuwe zaken komen erbij, en het wordt slimmer. De groei is exponentieel of meer dan exponentieel. Spam wordt nog steeds in technische zin verder gepersonaliseerd, daardoor moeilijker tegen te houden. De zwakke schakel is de mens. 'AfpersSpam'. Er zijn nu enkele tientallen miljoen gecompromitteerde bots for relayeren van Spam.

Bots zijn gericht op veel duurdere zaken, tienduizenden beheersen valt op. Daarom is richting nodig. Dit wordt nu aangeduid met SpearPhishing of Spearspam. Men mag dan verwachten dat je gericht op de bedrijfsleiding aanvalt.
- een curieuze handel door spionage
- mensen verstrikt met bijv. blackberry

IV/V Wat wordt daar nu aan gedaan en wat kan er aan gedaan worden?

Wanneer Xs4all merkt dat klanten problemen hebben, dan komt het Incident Response Team in actie. Liaisons naar bijv. o-IRT-o / FIRST / E-CoAT[37] / CERT.
Je kunt niet iedereen in zo'n groep zetten. Doel is te bepalen wat het "IP-adres" is en waar het vandaan komt. Om dat goed waar te nemen dien je eigenlijk op een US exchange te staan en daarvandaan naar Nederland te kijken, wie welk IP-adres gekregen heeft van RIPE.

De Ams-IX is zo groot, dat het een supernova en zwart gat tegelijk is. Ook Cisco, Juniper, Siemens etc. zouden bij de discussie moeten worden getrokken.

De kernfilosofie is nu een 'Goede Netbuurman' te zijn, Security en Privacy verantwoordelijken overleggen intern met een voorspelling en tactisch overleg en aansturing op operationeel niveau.

Xs4all heeft een voorlichtingspagina.

[37] European Cooperation of Abuse fighting Teams, http://www.e-coat.org/

Voor al zijn klanten en mini-hosters als klanten ziet Xs4all ca. 10 tot 12 DDoS aanvallen per dag passeren. Security maatregelen zijn nodig om dat te kunnen voorstellen. Er is een geautomatiseerd systeem voor netflow sampling dat alarmen voedt.

Het verkeersniveau in de core is vele tientallen Gigabit/s, daarmee wordt het een balanceeract.
De vraag moet niet alleen zijn, wat er aan gedaan kan worden, maar wat wil men eraan doen.
- Deep packet inspection?
- Alles willen zien, of daar minder ver ingaan.

Van de WBP mag vrij veel, die wet zegt vooral "zeg wat je zegt en doe wat doet". De discussie zou moeten zijn of het wel verstandig is om dit soort taken bij een ISP neer te leggen.

Bij Ericsson is een apparaat te koop voor €60k, waarmee men Skype kan uitzetten, wil OPTA een represieve ISP geforceerd door de overheid, zoals in Italië?
Packet Cleaning, na deep packet inspection, weggooien. Het is een heel makkelijke geroepen, in technische interpretatie, maar het gaat een hellend vlak op. Het is niet zozeer de vraag wat er wel/niet kan, maar het probleem is het beleid eromheen.

Internet = een publieke ruimte in privaat bezit.

Xs4all verwacht van OPTA niet zozeer handhaving maar discussies en openheid. Een interoperabiliteitsverplichting inzetten in formulering. Niet "filter port x of 4" maar:
- zo werken wij
- zo richten wij in

Als je dat niet vind dan bouw je consumentenbond-net

Informeren is het partijen/klanten kunnen laten kiezen iets in of uit te schakelen
Uitgaande mail-servers staan bij Xs4all op virus scanners, voor klanten die dat niet willen is er een scan-loos net. "If you're not part of the solution, you're part of the problem".
Sommige zaken worden op minimumniveau uitgevoerd.
- Vrijheid komt met verantwoordelijkheid

Portnummer 135, 137/udp (oud), 139 (NETBIOS) en 445 zijn echter dicht gezet, om de meerderheid van de wormen af te stoppen maar dat doet bijna iedere ISP als "good behaviour" om de achtergrondruis en risico's voor klanten te beperken. Xs4all zou portblokkades het liefst per klant instellen, maar dat is nog te duur / onmogelijk.

OPTA verwacht nu veel meer de discussie op de agenda te zetten. In plaats van regelgever naar beleidsvoorbereider. Er is echter ook behoefte aan een organisatie die deze rol in internationale fora voert.

VI OPTA/Overheid

Handhaving van de beveiligingsbepaling in de Tw acht Xs4all totaal irrelevant. Eerst dient helder te zijn wat je te handhaven hebt.

In reactie op de vraag naar maatregelen die verwacht werden van de overheid kwam de reactie: “Thou sould not try to impose”. OPTA zou medestandersr moeten kweken, een autoriteit op dit vraagstuk worden. Xs4all geeft aan dat Internet in zijn aard een meritocratie is:

- Wie het weet moet het zeggen, niet
- Wie de macht heeft moet het zeggen.

Het regelgevend kader komt uit een geheel andere hoek.
Xs4all ziet vooral een vruchtbare rol OPTA als autoriteit die niet als regelgever optreed maar als aanjager.
Op de vraag van wie men maatregelen zou verwachten, wordt verwezen naar de Finse regulator [Ed. Ficora] die wel dingen bereiken, hoewel er twijfels zijn over de inhoud van de maatregelen. Bij het door OPTA geschetste scenario merkt Xs4all op dat dit kan als het ‘last resort’ is. Het risico is dat men niet op basis van goede adviezen werkt en toch gaat afdwingen na slecht bediscussiëren De meritocratie moet kunnen werken. Dat wil zeggen standpunten moeten voortkomen uit inhoud / gezag in deze kwesties.

OPTA zou het beste invulling kunnen geven door gemeenschappelijke doelstellingen neer te zetten i.p.v. maatregelen te formeel invoeren. Bijv. het verlagen van een bepaald type fraude leidt tot meer opengezette deuren dan gesloten. Security is niet bedoeld en werkt niet als een poldermodel, wanneer er ook al een vrij goed draaiende meritocratie is.

In de feedback ronde zijn op dit punt enkele extra opmerkingen toegevoegd:

a. XS4all ziet geen rol voor OPTA in de IETF, dat is vooral een plek voor Internet Engineers en niet zozeer voor telecom regulators. Het kan als ongepast worden ervaren om hier te starten en door aanwezigheid onwelwillendheid vs Nederland kweken bij de Internet Security gemeenschap. Mogelijk zijn bezoeken aan RIPE of NANOG[38], wel gepast, maar dan vooral als toehoorder en om over zaken te leren en niet om wensen of mandaten te uiten.
b. XS4all acht het creëren van Bluepints en BCP’s een zaak om vooral te laten bij mensen voor wie dit werkelijk een taak is. OPTA kan het best werk van FIRST, IETF, NANOG en dergelijke organisatie overnemen, en eventueel vertalen in Nederlands, als referentie. Het lijkt hen niet gepast voor Nederlandse regelgevers om te proberen het Internet vorm te geven, omdat OPTA hiervoor niet een rol of mandaat lijkt te hebben en Nederland maar een klein stukje is. Wel kan het gepast zijn om de BCP’s e.d. die gemaakt zijn te nemen en hen te “mappen” met Nederlandse wet- en regelgeving. D.w.z. als er bijv. een BCP is die refereert naar een bepaalde vorm van data privacy, dan kan OPTA de link aangeven met de wet in Nederland die hetzelfde onderwerp adresseert.
c. OPTA / SIDN relatie. Er is op dit punt mogelijk geen directe relatie, echter veel van de Spam en “.nl” problemen die optreden op het terrein van security/safety online zijn daadwerkelijk te beheersen door SIDN, echter Xs4all ervaart dat SIDN op dit moment EXTREEM zwak handelt op deze bedreigingen. “Ze zijn traag, niet co-operatief en niet “up-to-date” m.b.t. de potentiële rol die een Registrar kan vervullen met betrekking tot

[38] North American Network Operator Group, een regelmatige conferentie van ISP’s over operationele vraagstukken, wordt ook veel door niet-Amerikaanse organisaties bijgewoond.

Internet beveiliging en veiligheid. Mogelijkerwijs kan OPTA op dit punt meer betekenen door hen aan te moedigen?"

VII Afsluitende opmerkingen

Er is aangegeven dat Xs4all bereid is om deel te nemen aan een eventueel vervolg.

Bij de feedback op het concept gaf Xs4all aan een andere visie te hebben op de wenselijkheid voor DNSSEC. Dit protocol lost inderdaad enkele veiligheidsproblemen op, maar de veel grotere berichten die terug worden gestuurd bij het opvragen van een domeinnaam maakt de impact van een aanval via DNS-Amplification veel groter, omdat overbelasting bij zo'n aanval eerder optreedt. DNS-Amplification is een aanval, waarbij domeinnaamservers van derden worden misbruikt om een groot aantal verzoeken tegelijk vanuit de gehele wereld te sturen naar de DNS-servers van het doelwit en die onbereikbaar te maken door overbelasting. Servers van het doelwit worden bij uitval van de DNS onbereikbaar via hun domeinnaam[39].

[39] DNS Amplification is onder meer ingezet in combinatie met een phishing-aanval, waarbij eindgebruikers via Spam werd gemeld dat de servers van een elektronische banksite onder 'domeinnaam x' tijdelijk uit de lucht was, en of ze zo vriendelijk wilden zijn op een andere site (de phishing-site) in te loggen. Wat velen prompt deden, want zij constateerden dat de bank inderdaad onbereikbaar was...

Stratix

Annex F Interview InterNLnet

http://www.internl.net

Paul Theunissen, Technisch Manager

Paul Theunissen heeft geen bezwaar gemaakt tegen vermelding met naam en toenaam.

I Beschrijving van de geïnterviewde partij

InterNLnet is een 11 jaar oude ISP die ooit als filiaal van NLnet in Nijmegen startte voor internetdiensten. Daarna zijn de aandelen in handen gebracht van de Stichting InterNLnet, terwijl NLnet werd verkocht aan UUnet en daarna MCI Worldcom. MCI is uitgekocht en de aandelen zijn nu 100% in handen van de stichting.

Recent is het bedrijf gegroeid vanwege de rol als provider voor Xtra Media Services (XMS) / Glasvezel Netwerk Exploitatie Maatschappij (GNEM), bedrijven van VolkerWesselsStevin die een glasvezelnet aanleggen voor woningcorporaties in enkele steden.
Het bedrijf levert de billing & supportdesk voor het aansluitproces. InterNLnet heeft een belang in XMS en diensten. Het is ook na de verkoop van HCCnet aan KPN nog deels betrokken bij enkele diensten.

InterNlnet is begonnen met inbeltoegang, het bedrijf levert nu veel DSL. Doelgroepen worden ook bedient. O.a. SURFsnel ADSL en Academie Kabel in Groningen. Via de wholesale relatie met BBned worden ook diensten aangeboden over Citynet in Amsterdam

Als Internet services levert het bedrijf: access, hosting, telefonie (VoIP), VISP diensten voor andere partijen en mailplatforms. De bedrijfsomvang is ca. 60 man / 46 FTE.

Als middelgrote provider ziet het als vergelijkbare partijen Concepts ICT, Unet, en kan men vrij snel schakelen. InterNlnet richt zich daarbij commercieel gezien op de professionele eindgebruiker.

Reactie op uitnodigingsbrief voor het interview

Theunissen geeft in de loop van het interview aan dat hij “Internet dreigingen” een discutabele benaming vind. Vrijwel alle bedreigingen zijn aan PC’s, PDA’s, de pijp is niet zozeer het probleem. Aanhakend op de door de Consumentenbond gemaakte vergelijking van “een auto koop je ook niet zonder gordels” ziet Theunissen deze vergelijking met de automobielindustrie niet op gaan. De meeste Internetdreigingen zijn min of meer vormen van computervredebreuk (een strafbaar feit!). Het kan niet zo zijn dat de deze verantwoordelijkheden op het bordje van de Internetindustrie wordt geschoven. De automobielindustrie is ook niet verantwoordelijk voor

strafbaar gedrag op de wegen. Strafbare feiten onderbrengen in het civiele aansprakelijkheidsrecht zou een eigenaardig fenomeen zijn..

Hij las het artikel 11.3 als volgt:
Een ISP wordt geacht maatregelen te nemen dat persoonsgegevens niet op straat liggen, evenals de inhoud van de mailbox, gesprekken niet afluisterbaar mochten zijn. Hij zag het als een inspanningsverplichtingen. De ISP draagt de verantwoordelijkheid voor die systemen die ook daadwerkelijk in zijn beheer zijn. Verder is een mogelijkheid dat de ISP middelen beschikbaar stelt waarmee de eindgebruiker zijn verantwoordelijkheden kan nemen (bv de optie op het instellen van een bellimiet om de belkosten in de hand te houden).

Het is zeker juist dat er extra diensten zijn, maar in het verleden zijn er ook nooit maatregelen opgelegd aan fabrikanten van floppy disks ten aanzien van de virussen.

II Wat zijn de dreigingen nu?

Als belangrijkste dreigingen ziet men:
- Virussen, trojans, botjes, (rootkits)
- Spam verspreiding is naar hun indruk nog steeds de meest voorkomende reden om trojans en virussen op eindgebruikers PC's te installeren
- Phishing komt op, met als duidelijk doel geld afhandig te maken.
- Spyware acht men meer marketing gericht.
- Phishing ziet men zowel in relatie tot keyloggers, spyware als websites defacing en DNS aanvallen
- DDoS zijn wel risico's maar frequentie niet zo hoog (wel potentieel grote impact)
- IRC betreft vooral clubjes tegen elkaar.
- Bij dreigingen naar routers en DNS zijn de aanvallers gericht op systemen die beheerd worden door professionele beheerders, die zullen sneller en adequater acteren

Het versturen van spam is thans de grootste motivator om PC's van eindgebruikers te voorzien van botjes en rootkits maar phishing komt op en heeft een grotere impact.

III Wat zijn de dreigingen die opkomen?

- Spam over VoIP, Caller ID spoofing, misbruik van SIP accountgegevens
- Bijv. SIP accountgegevens kraken om gesprekken te initiëren naar vast/mobiel/servicenr's.
- Bij VoIP leveren wij nu een voorgeconfigureerde ATA[40], dat houdt je niet vol. Op den duur zullen we ook de SIP accountgegevens los moeten verstrekken zodat deze direct in VOIP telefoons geconfigureerd kunnen worden. Dan is het hebben van een username/password combinatie al genoeg om te kunnen bellen.

[40] Analog Terminal Adapter

De uiteindelijke motivator = geld. Alle dreigingen zonder geld zijn veel incidenteler (pesten is ook verstaan als deel van dreigingen). Maar wat politieker gesteld: de hoofdmoot is toch vooral criminaliteit.

De vraag is voor Theunissen wat OPTA wil handhaven, dat is de vraag die komt na het vaststellen van verantwoordelijkheden.

Theunissen ziet geen duidelijke nieuwe motivator? Is Spam over? IM wel nieuw maar meer van hetzelfde. Andere applicatie, iets andere gaatjes.
ENUM is DNS in een ander jasje. De vanzelfsprekendheid is?

Theunissen schat het lastig in om te voorspellen hoe hard de groei gaat. Vooral voor Phishing en aanvallen op SIP credentials vermoedt hij een sterke groei. Op belgedrag staan bij hem wel bellimieten ingeregeld.

IV/V Wat wordt daar nu aan gedaan en wat kan er aan gedaan worden?

Theunissen geeft aan dat zijn hoofddoel is om te zorgen dat zijn gebruikers zo weinig mogelijk kattekwaad uithalen.

- hij zorgt er voor dat IP Spoofen niet kan
- er geen virussen de wereld in gaan (uitgaande mail-relay / virusscanner)
    - er staat echter bij InterNLnet geen poort 25 dicht (bij voorbaat)
    - er worden wel maatregelen genomen als er relay servers staan / detectie
- er wordt adequaat gereageerd op alle meldingen van vermeend misbruik op het InterNLnet netwerk (van het dichtzetten van poorten tot volledige afsluiting van abonnees)

Inkomende faciliteiten:

- viruschecken kost geld (licenties Kaspersky gaan per gebruiker)
- Spamfilter is gratis
- Veel is open source dus grotendeels zelf gemaakt

Inkomende faciliteiten zijn facultatief. InterNLnet wil niet voor de eindgebruiker bepalen wat goed of fout is, InterNLnet wil wel faciliteren zodat de eindgebruiker deze keuze (makkelijker) kan maken.

Het belangrijkste bij de dreigingen is het acteren op iedere melding van misbruik / bron van fout verkeer. De dreigingen moeten bij de bron worden aangepakt/voorkomen.

InterNLnet draait ook het Quarantainenet, echter alleen voor de SURFsnel abonnees. Quarantainenet draait op IP niveau, een honeypot detecteert, bij besmetting en dan wordt de browser omgerouteerd naar een pagina waar de PC dan geïsoleerd updates van viruscheckers etc. kan downloaden.

Hij acht dit nu nog wel redelijk effectief, maar misschien dat detectie door honeypots steeds lastiger wordt door snel wisselende fingerprints. De oplossing van Quarantainenet is niet goed-koop. InterNLnet heeft het voor SURFsnel, maar het is geen verplicht onderdeel voor alle aansluitingen.

Service pack 2 en een Quarantaine is een vorm van dienstverlening. Maar vraag dit niet van een klant, neem wel de maatregelen maar blijf facultatief. Het is wat anders bij misbruik, maar misbruik valt onder de algemene voorwaarden.

Iemand die bij Inter NLnet een transparante open verbinding wil krijgt dat. NETBIOS poort staat nog open, het punt is een principe overboord te gooien. Het internet bestaat bij de gratie van open transport. Het is een moeilijk beheerspunt maar klachten kunnen nog goed afgehandeld worden op de helpdesk en dus kiezen we nog steeds voor individuele maatregelen.

Theunissen toont een deel van overzichten die hij heeft gemaakt met grondige netwerkanalyse. Er worden niet de lichtste systemen ingezet en maatregelen genomen, ook wordt er veel verzameld, maar het zijn geen continue monitoring systemen zoals SURFnet en Xs4all die hebben staan.

Theunissen is van mening dat er heel veel verantwoordelijkheid bij eindgebruiker moet liggen. Eindgebruikers blijven downloaden en zolang besturingssystemen niet veilig zijn, blijven zij een prooi. Groot deel van de verantwoordelijkheid ligt dan wellicht bij de fabrikanten van besturingssystemen.

Hij acht voorlichting wel een taak voor een ISP, maar dan dergelijk informatie op iedere website van een ISP terug te vinden zijn. Dus men moet niet alleen proberen het werkend te krijgen, maar het ook draaiend te houden.

VI OPTA/Overheid

Theunissen ziet meer in formele criminele handhaving. Veel van wat nu binnenkomt op machines heeft alle kenmerken van Computer vredebreuk. Dit brengt het veel meer in het justitiële domein, hij ziet zich echter al naar een politiebureau stappen voor een aangifte van een virus.

Hij begrijpt dat er een handhavingsprobleem is met het terughalen van de bron. Maar er dient goed gekeken te worden naar de verantwoordelijkheden in de hele keten. Zeer veel ook bij fabrikanten en eindgebruikers. Bij een ISP kan wel gekeken worden maar toegespitst op de dienstverlening van die ISP. D.w.z. Netwerk administratie en eigen diensten in hoofdzaak.

De rol van de overheid zou dan vooral staan gedefinieerd op computervredebreuk.

Stratix

Theunissen beoordeelt het scenario van OPTA niet positief. Want dit is precies het gevaren van Internet, eigenlijk gevaren van besturingssystemen, tot onderdeel van de ISP diensten verklaren terwijl deze daar eigenlijk los van staan.

OPTA moet begrijpen dat een ISP niet de hele keten kan controleren. Het internet is een open netwerk, een verzameling van nodes, en slechts een klein stukje valt in het domein van een ISP..

VII Afsluitende opmerkingen

Geen verdere opmerkingen