Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2000–2001

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 30

BRIEF VAN DE STAATSSECRETARIS VAN VERKEER EN WATERSTAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 juli 2001

Mede namens de Minister van Economische Zaken bied ik u de nota *Kwetsbaarheid op internet (KWINT)* aan. Deze nota is de uitwerking van een in *De Digitale Delta* toegezegde verkenning naar de kwetsbaarheden op internet.

In de nota worden ontwikkelingen geschetst met betrekking tot de maatschappelijke en economische betekenis van internet, risico's en kwetsbaarheden van (het gebruik van) internet geanalyseerd en maatregelen ter zake in een aantal landen aangehaald. Om het maatschappelijk en economisch belang van een goed functionerend internet te behartigen, worden tenslotte de rol van de overheid en een aantal concrete actielijnen beschreven. De actielijnen liggen onder meer op het terrein van voorlichting, stimulering van R&D, het stimuleren van effectief management van informatiebeveiliging in organisaties en het vergroten van het inzicht in de betrouw-baarheid van internet.

De nota hangt inmiddels ook samen met de Motie-Wijn c.s. (26 643, nr. 20) van maart jl. In deze motie komt de vraag naar voren in hoeverre de ICT-ontwikkelingen niet alleen gevolgen hebben voor de kwetsbaarheid van internet, de focus van KWINT, maar ook voor andere vitale infrastructuren zoals energie, financiële dienstverlening etc. In de motie wordt gevraagd een sectoroverschrijdend plan van aanpak inzake de bescherming van vitale infrastructuren op te stellen. Het Kabinet onderkent de noodzaak hiertoe. In september vindt overleg op politiek-bestuurlijk niveau hierover plaats, teneinde te bepalen wat een proportionele aanpak is.

Naast dit overleg over een brede aanpak, wordt de uitvoering van de maatregelen zoals genoemd in de nota KWINT op korte termijn ter hand genomen. Samen met de uitvoering van het Nationaal Continuïteitsplan

KST54719
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2001

Telecommunicatie (NACOTEL), beoogt dit te leiden tot een betrouwbare telecommunicatie-infrastructuur, als een van de vitale infrastructuren.

De Staatssecretaris van Verkeer en Waterstaat,
J. M. de Vries

BELEIDSNOTA KWETSBAARHEID OP INTERNET (KWINT)

INHOUDSOPGAVE

0. SAMENVATTING

Informatie en communicatietechnologie (ICT) in het algemeen en internet in het bijzonder vormen een steeds belangrijker schakel in de huidige samenleving. Internet kan zelfs beschouwd worden als één van de kritieke infrastructuren van een moderne samenleving als Nederland. Meer en meer maatschappelijk essentiële processen worden over internet afgehandeld, waardoor overheden, bedrijfsleven en individuele gebruikers steeds afhankelijker worden van een in redelijke mate betrouwbaar en veilig internet. Desondanks concludeerde de Europese Raad van Stockholm maart jl. dat in Europa de mogelijkheden die internet biedt nog onvoldoende worden benut. De Raad benadrukte hierbij het grote belang van het scheppen van voorwaarden die de veiligheid en betrouwbaarheid bevorderen.

De vele incidenten waar in de media blijk van wordt geven, laten eveneens zien dat de betrouwbaarheid van internet een duidelijke verbetering behoeft. Dit beeld is bevestigd door een onderzoek naar de aard en omvang van de kwetsbaarheid van internet in Nederland, dat al door het kabinet in *De Digitale Delta*[1] is aangekondigd. In de onderliggende nota wordt verslag van het in opdracht van VenW uitgevoerde onderzoek gedaan. Met deze kennis als achtergrond richt de nota zich op de wijze waarop de overheid vanuit haar maatschappelijke verantwoordelijkheid een bijdrage wil leveren aan de betrouwbaarheid van internet.

Uit het onderzoek naar de kwetsbaarheid van internet is naar voren gekomen dat het aantal incidenten dat inbreuk maakt op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie(systemen) de laatste jaren enorm is toegenomen. De opkomst van internet heeft de grenzen van voorheen losstaande informatiesystemen doen vervagen. Door het grote aantal onderlinge koppelingen vormen bedreigingen een steeds groter risico. Ook buitenlandse overheden hebben dit gevaar onderkend en nemen maatregelen die een bijdrage zouden moeten leveren aan een betrouwbaarder internet. Hieronder wordt aangegeven welke publiek-private aanpak van de kwetsbaarheid van internet in Nederland wordt voorgestaan.

Rol overheid

Gezien de wijze waarop internet tot stand is gekomen en functioneert, hebben in de visie van het kabinet internetgebruikers (zowel aanbieders als afnemers) en infrastructuuraanbieders de primaire verantwoordelijkheid voor het beveiligen en betrouwbaar maken van internet. Iedere partij dient voor zichzelf te beslissen welke maatregelen, procedures en producten noodzakelijk zijn om zijn systeem te beschermen. Dit geldt uiteraard ook voor de overheid als beheerder van haar eigen informatiesystemen.

De overheid zal de ontwikkelingen op internet in samenhang met de effectiviteit van het beleid nauwgezet monitoren. Wanneer de uitkomst daartoe aanleiding geeft kan bijtijds een verschuiving van een faciliterende naar een meer regelgevende rol plaatsvinden. Vooralsnog zal de overheid met betrekking tot haar inbreng bij het vergroten van de betrouwbaarheid van het internet terughoudend zijn met aanvullende regelgeving om de zich nog ontwikkelende markt niet onnodig te verstoren. Het kabinet ziet thans met name een rol voor zich weggelegd in het scheppen van de juiste randvoorwaarden die internetgebruikers faciliteren bij het invullen van hun verantwoordelijkheden op dit gebied.

Actielijnen

De beschreven actielijnen zijn een mix van activiteiten die al in meer of minder ver gevorderd stadium zijn opgepakt, waarover de Tweede Kamer al eerder is geïnformeerd, en van compleet nieuwe onderwerpen. Om een samenhangend en consistent beleidskader rond het thema internet-betrouwbaarheid te schetsen, worden beide beschreven.

Bij het vaststellen van de actielijnen zijn de volgende uitgangspunten gehanteerd:
- maatregelen mogen niet ten koste gaan van het innovatievermogen van internet;
- er moet rekening worden gehouden met de dynamische aard van de bedreigingen;
- er is een noodzaak tot (inter)nationale publiek-private samenwerking;
- het beheersbaar maken van de kwetsbaarheid van internet is het hoogst haalbare. Internet zal, in analogie met de openbare weg, altijd onveiligheden blijven hebben.

1. Voorlichting

Met voorlichting wordt beoogd de positie van de internetgebruiker, zowel bedrijfsleven als burger, te versterken door het bevorderen van zijn/haar bewustzijn en kennis van de veiligheidsrisico's die bij het gebruik van internet spelen en hoe met deze risico's kan worden omgegaan.
Een interdepartementale werkgroep bereidt een voorlichtingsactiviteit voor die in 2001 start en aansluit bij de campagne *Nederland gaat digitaal*. Rekening houdend met de verscheidenheid aan gebruikers wordt bekeken of de twee hoofddoelgroepen (burger en bedrijfsleven) nog nader moeten worden opgesplitst, wat de reikwijdte van de voorlichting moet zijn en via welke communicatiekanalen de voorlichting het beste kan plaatsvinden. Bij dit laatste aspect wordt nadrukkelijk de mogelijke rol van marktpartijen zoals brancheen gebruikersorganisaties meegenomen. De dynamiek van internet vereist een permanente verstrekking van informatie. Hoe deze aanhoudende informatievoorziening kan worden vormgegeven, is onderdeel van deze actielijn.

2. Research & Development

Doelstelling is om onderzoek naar en ontwikkeling van nieuwe informatiebeveiligingsmethoden en -hulpmiddelen te bevorderen. Het kabinet geeft hier invulling aan door het Nederlandse bedrijfsleven actiever trachten te betrekken bij Europese onderzoeksinitiatieven door middel van het verstrekken van informatie over deze initiatieven en ondersteuning te bieden bij het indienen van projectvoorstellen. Daarnaast zal structureel onderzoek sterker worden gestimuleerd, waarbij ook gekeken zal worden naar de mogelijkheden van (promotie)onderzoek bij universiteiten op het gebied van internet betrouwbaarheid en veiligheid.

3. Beveiligingsbeleid en -maatregelen binnen een organisatie

Deze actielijn is er op gericht de kwetsbaarheid op het niveau van individuele organisaties (bedrijven en overheden) te verminderen, door het stimuleren dat deze organisaties een effectief management van informatiebeveiliging voeren. In Nederland bestaat een leidraad voor beleid en implementatie van informatiebeveiliging, bekend als de *Code voor informatiebeveiliging*[2]. EZ en V&W zullen het gebruik van deze leidraad stimuleren door o.a. een grotere bekendheid te geven aan het bestaan en nut ervan. Tevens worden eventuele belemmeringen, die het

gebruik van de *Code* beperken, geïnventariseerd en wordt geholpen om deze zoveel mogelijk te elimineren.

4. Exclusiviteit van informatie

De Telecommunicatiewet (hoofdstuk 11) kent een inspanningsverplichting voor aanbieders van openbare telecommunicatienetwerken en -diensten ten aanzien van de beveiliging van netwerken en diensten ten behoeve van de vertrouwelijkheid van communicatie.
Daarnaast wordt, om de bekendheid van gebruikers met de versleutelingsmogelijkheden van communicatie te vergroten, in de actielijn «voorlichting» expliciet aandacht aan de beveiliging van vertrouwelijke informatie geschonken. Tenslotte kan de overheid het gebruik van cryptografie bevorderen middels haar eigen beveiligingsbeleid. Door de ontwikkeling van *e-government* kan de overheid een voorbeeldfunctie vervullen ten aanzien van het gebruik van effectieve cryptografische oplossingen en daarmee het vertrouwen in cryptografische producten verhogen.

5. Transparantie door kwaliteitsgegevens

Doelstelling van deze activiteit is om de marktwerking beter te laten functioneren door het vergroten van het inzicht in de aangeboden kwaliteit van dienstverlening door infrastructuuren dienstenaanbieders. Daarnaast kan het een beter (kwantitatief) inzicht geven in de beschikbaarheid van internet.
Infrastructuur- en dienstenaanbieders worden gestimuleerd om zelf, op vrijwillige basis, beschikbaarheids- en verkeersmetingen uit te voeren. Om dit proces te ondersteunen neemt V&W dit jaar het initiatief om in nauwe samenwerking met marktpartijen de totstandkoming van eenduidige en uniforme kwaliteitsindicatoren, meetmethoden en meetinstrumenten te stimuleren. In aanvulling daarop onderzoekt V&W of en hoe afspraken kunnen worden gemaakt met desbetreffende aanbieders om een beter beeld van de beschikbaarheid van internet te krijgen en mogelijke kritische infrastructuurdelen te identificeren.

6. Alarmering en incident response

Door BZK wordt een computer emergency response team (CERT) voor de rijksoverheid opgezet. Samen met V&W wordt onderzocht of en hoe vanuit een maatschappelijke verantwoordelijkheid deze CERT ook een waarschuwingsfunctie voor andere sectoren en burgers in Nederland kan invullen. Het snel en effectief waarschuwen van belanghebbenden ten aanzien van informatie-beveiligingsincidenten, zoals virussen en computerinbraken, kan de gevolgschade zoveel mogelijk beperken.

7. Integriteit van informatie

Het gaat hier om het waarborgen van de integriteit van informatie die elektronisch wordt gecommuniceerd of is opgeslagen. De integriteit van informatie is de zekerheid omtrent de identiteit van de persoon of organisatie waar de informatie van afkomstig is en de correctheid van de informatie zelf (niet gewijzigd of aangevuld). Trusted Third Parties (TTP) verlenen diensten waarmee de integriteit van elektronische informatie kan worden gewaarborgd.

De Europese richtlijn[3] voor elektronische handtekeningen verplicht dat een lidstaat een toezichtsysteem opzet om te waarborgen dat bepaalde TTP's, die immers een belangrijke vertrouwensdienst leveren, aan de eisen voldoen. Er is een wetsvoorstel, dat dit jaar aan de kamer wordt aangeboden, waarbij OPTA als toezichthouder wordt aangewezen. In

aanvulling daarop wordt de totstandkoming van een schema gestimuleerd waaronder TTP's zich kunnen laten certificeren. Dit is naar verwachting medio 2001 operationeel.

8. Cybercrime

Er worden maatregelen voorzien om burger, bedrijfsleven en overheid beter te beschermen door te bevorderen dat computercrimaliteit daadwerkelijk bestreden kan worden binnen een internationaal wettelijk en uitvoerbaar kader en met de daarvoor benodigde middelen. De belangrijkste maatregelen zijn het vergroten van de kennis van digitaal opsporen, het ontwikkelen van digitale opsporingsmiddelen en indien nodig het uitbreiden van de opsporingsbevoegdheden. Daarnaast is uitbreiding van de bureaus digitale expertise (BDE) bij de politie noodzakelijk. Op internationaal niveau bereidt de Raad van Europa het verdrag *Crime in Cyberspace* voor. Dit thema wordt in deze nota kort aangehaald en zal ook worden behandeld in de nota *Criminaliteitsbeheersing*, die de minister van Justitie dit jaar aan de Tweede Kamer aanbiedt.

Afstemming

Om uitwerking te geven aan voornoemde actielijnen, wordt een nationaal overleg voorzien waarin de betrokken departementen en private partijen zitting hebben. Hier zullen aan elkaar gerelateerde onderwerpen in hun samenhang worden behandeld.

1. INLEIDING

Informatie- en communicatietechnologie (ICT) dringt onmiskenbaar door, soms vertraagd en soms onverwacht snel, in de poriën van onze maatschappij. Internet is hiervan een voorbeeld. Het is een baanbrekend medium gebleken dat een nieuwe omgeving heeft gecreëerd waarin menselijke activiteiten ontplooid kunnen worden. Zowel het zakelijke als het particuliere gebruik is in een korte tijd gemeengoed geworden.

Desondanks is in de Europese Raad van Stockholm[4] vastgesteld dat het potentieel van internet in Europa nog niet ten volle wordt benut op belangrijke gebieden als openbare diensten, elektronische overheid en elektronische handel. De Raad wijst op het belang van netwerkbeveiliging, gegevensbescherming en privacy waardoor in vertrouwen gebruik kan worden gemaakt van nieuwe diensten. Het kabinet geeft in de nota *De Digitale Delta* eveneens aan dat een betrouwbare (tele)communicatie-infrastructuur een essentiële bouwsteen is van de informatiemaatschappij.

Incidenten als het «I love You»-virus, het platleggen van e-commerce websites en de wijzigingen van de website van de Nederlandse politie laten zien dat de veiligheid en betrouwbaarheid van dit medium de nodige zwakke plekken vertoont. Dergelijke incidenten hebben niet alleen bestanden, computers en netwerken beschadigd, maar hebben ook veel ongemak, productiviteitsverlies en verlies van vertrouwen veroorzaakt. De mogelijkheden die internet in potentie biedt, zouden wel eens beperkt kunnen worden door dit gebrek aan vertrouwen.

Het **doel van deze nota** is tweeledig:

- Het verschaffen van inzicht in de huidige toestand van de kwetsbaarheid van internet. Het is de rapportage van een onderzoek dat in *De Digitale Delta* is toegezegd: «Het ministerie van V&W gaat een verken-

ning uitvoeren naar de kwetsbaarheden en zwakheden op de ICT-infrastructuur waarbij speciaal aandacht wordt besteed aan de ontwikkelingen op het gebied van het internet.» In de nota *Netwerken in de Delta*[5] is deze verkenning eveneens aangekondigd.

- Het schetsen van de wijze waarop de overheid in samenwerking met de private sector het maatschappelijk en economisch belang van een goed functionerend internet wil behartigen. In deze nota wordt daartoe een aantal actielijnen gepresenteerd met als doel de betrouwbaarheid van het internet op een zo hoog mogelijk peil te brengen.

Door een tweetal organisaties is onderzoek[6] verricht naar de kwetsbaarheden op internet en zijn de activiteiten geïnventariseerd die ondernomen kunnen worden om internet beter te beveiligen. Resultaten van het onderzoek zijn verkregen op basis van een expert-analyse en een aantal workshops met deelnemers van zowel private als publieke partijen (zie bijlage B). Gedurende de expert-analyse is eveneens gekeken naar het beleid en de inspanningen die op dit gebied in het buitenland verricht worden.

De nota is als volgt opgezet. Allereerst komt in hoofdstuk 2 de reikwijdte van de nota aan de orde en wordt een begrippenkader rondom de kwetsbaarheid van internet geschetst. De ontwikkelingen op het gebied van internet en het belang van internet voor de maatschappij zijn onderwerpen die in hoofdstuk 3 behandeld worden. Hoofdstuk 4 gaat dieper in op de kwetsbaarheden op internet. In hoofdstuk 5 is aandacht voor internationale activiteiten op dit gebied en hoofdstuk 6 gaat dieper in op de rol van de overheid. Tenslotte staat hoofdstuk 7 stil bij de acties die het kabinet wil ondernemen om een bijdrage te leveren aan de betrouwbaarheid van internet. Een verklarende lijst van termen is weergegeven in bijlage C.

2. REIKWIJDTE

In het vorige hoofdstuk is gewezen op de kwetsbaarheid van internet en het belang van het vertrouwen van de gebruiker. Wat precies onder internet en de kwetsbaarheid van internet wordt verstaan, is onderwerp van respectievelijk paragraaf 2.1 en paragraaf 2.2. Paragraaf 2.3 geeft aan dat het bereiken van een in redelijke mate veilig en betrouwbaar internet niet voldoende is voor het vertrouwen in de informatiemaatschappij. Ingegaan wordt op de samenhang met de onderwerpen *computercriminaliteit*, *rechtszekerheid in de elektronische handel* en *privacy*.

2.1 Wat is internet?

Internet is de wereldwijde communicatie-infrastructuur die gebaseerd is op het Internet Protocol (IP). Dit protocol biedt de mogelijkheid om verschillende netwerken, mobiel en vast, op elkaar aan te sluiten en onderling gegevens uit te wisselen. De infrastructuur bestaat uit een verzameling van velerlei autonome netwerken inclusief de computers waartussen de informatie uitgewisseld wordt. Een wezenlijk kenmerk van deze infrastructuur is zijn open en internationale karakter. Landsgrenzen zijn grotendeels irrelevant geworden en er is niet langer sprake van een centraal gecontroleerde omgeving. Internet bestaat bij de gratie van samenwerking, zowel voor het beheer als voor de ontwikkeling ervan.

Internet verschilt in een belangrijk opzicht van de oudere generatie communicatienetwerken en de beveiliging dient daarop te worden afgestemd. In tegenstelling tot de meer traditionele telecommunicatienetwerken spelen toezicht en controle zich voornamelijk in de periferie af,

bij de gebruikers en de diensten. De kern van het netwerk is relatief eenvoudig en is bovenal bedoeld om informatie over te brengen. Het grootste gedeelte van de functionaliteit van internet bevindt zich aan de «rand» van het netwerk op de computers van de gebruikers.

Omdat de gebruikersomgeving een belangrijk onderdeel van internet vormt, wordt daar in de nota, naast het publieke internet, veel aandacht aan besteed. In deze omgeving moet de gebruiker in staat zijn om beveiligingstechnieken toe te passen, toegesneden op zijn behoeften. Dit impliceert dat de informatiesystemen van afnemers en aanbieders van internetdiensten bij deze nota worden betrokken.

2.2 Het begrip kwetsbaarheid

Bij informatiebeveiliging gaat men doorgaans uit van de klassieke betrouwbaarheidsaspecten *beschikbaarheid*, *integriteit en exclusiviteit*. Het begrip betrouwbaarheid wordt hier beschouwd als spiegelbeeld van kwetsbaarheid. De drie aspecten zijn als volgt omschreven:

Exclusiviteit (of Vertrouwelijkheid) Het beschermen van gevoelige informatie tegen onbevoegde kennisname.
Integriteit Het waarborgen van de correctheid (inclusief authenticiteit) en de volledigheid van informatie en computerprogrammatuur.
Beschikbaarheid Zekerstellen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers.

Alle drie de aspecten worden in de kwetsbaarheidsanalyse (zie hoofdstuk 4) meegenomen.

Internet kan beschouwd worden als één van de kritieke infrastructuren van een moderne samenleving als Nederland. Een kritieke infrastructuur wordt hier gedefinieerd als: *een systeem, zowel fysiek als virtueel, dat zo vitaal is voor een land dat het wegvallen hiervan een verzwakkende invloed heeft op het sociaal en economisch functioneren en de nationale veiligheid.*

De scope van deze nota beperkt zich tot internet, dus op potentiële kwetsbaarheden van andere kritieke sectoren, zoals energie, financiële dienstverlening, etc., wordt niet ingegaan. Wel is het zo dat er relaties cq. ketenafhankelijkheden met deze andere sectoren zijn. Dit is reeds onderkend bij het «jaar 2000 probleem», waarbij door het millenniumplatform onder leiding van de heer Timmer de problematiek rondom de millenniumbug werd opgepakt. Eén van de meest sprekende voorbeelden is de afhankelijkheid van de energiesector: zonder electriciteit geen internet.

De ketenafhankelijkheden tussen sectoren maken dat de aanpak van de kwetsbaarheid van internet (ICT) onvoldoende is. Vanuit de markt is aangegeven dat een sectoroverstijgende coördinatie, naar het voorbeeld van het milleniumprobleem, dan ook zeer nuttig kan zijn. De overheid wil bezien in hoeverre zo'n sectoroverstijgende coördinatie kan voorzien in een behoefte en welke meerwaarde het kan hebben bij de beheersing van kwetsbaarheden. Bij een positieve toets zal gekeken worden hoe één en ander op een effectieve en efficiënte wijze vorm kan worden gegeven.

2.3 Relatie met rechtszekerheid e-commerce, cybercriminaliteit en privacy

Naast de drie tamelijk objectieve betrouwbaarheidsaspecten *beschikbaarheid*, *integriteit* en *exclusiviteit* speelt de perceptie van de gebruiker een grote rol. Uiteindelijk is het *vertrouwen* van de consument één van de

grootste bepalende factoren bij de ontwikkeling van nieuwe diensten en toepassingen op internet. Dit vertrouwen ontstaat niet alleen door het gebruik van betrouwbare technische systemen, maar ook door de bijbehorende wettelijke en economische voorzieningen. Bij het bevorderen van het vertrouwen in internet moeten ook zaken als opsporing en vervolging van computercriminelen, privacy-aspecten en de rechtszekerheid ten aanzien van de elektronische handel geregeld worden.

Om met het laatste aspect te beginnen, de juridische erkenning van elektronische contracten en handtekeningen zijn net als procedures voor geschillenbeslechting thema's die in de nota *Wetgeving Elektronische Snelweg*[7] van Justitie uitgebreid aan bod komen. Inmiddels zijn over enkele van deze onderwerpen ook Europese richtlijnen verschenen en vindt implementatie plaats. In de onderliggende nota wordt op het thema *rechtszekerheid e-commerce* niet verder ingegaan.

De aanpak van internet-misbruik door middel van het rechtshandhavingssysteem komt in deze nota wel kort aan bod. Bij dit thema zal ook worden stilgestaan in het kader van de nota *Criminaliteitsbeheersing*, die dit jaar door de minister van Justitie aan de Tweede Kamer wordt aangeboden. Zodoende gaat de aandacht van deze nota primair uit naar de kwetsbaarheid van internet en minder naar de aanpak van computercriminaliteit.

Tenslotte maakt ook de beleving van *privacy* deel uit van het vertrouwen van de consument in internet. Het begip privacy beslaat bij het gebruik van internet in hoofdlijn twee aspecten. Het eerste aspect betreft de vertrouwelijkheid van persoonsgegevens en de inhoud van persoonlijke communicatie voor wat betreft het transport tussen verzender en ontvanger. Als zodanig maakt dit onderdeel uit van het algemene thema van de exclusiviteit van gegevensverkeer en de benodigde beveiligingsmaatregelen hiervoor (zie paragraaf 7.1.4).

Het andere aspect betreft de privaatrechtelijke verhouding tussen internetgebruiker en dienstenaanbieder. Het gaat hier om het verstrekken van en het gebruik van persoonsgegevens, wat buiten de scope van deze nota valt. Hierop heeft de Wet bescherming persoonsgegevens betrekking en is de Registratiekamer toezichthouder. Naast wetgeving bestaan beleidsopties voor het waarborgen van privacy hier bijvoorbeeld uit het bevorderen van gedragscodes, de transparantie van privacybeleid van dienstenaanbieders en het gebruik van Privacy Enhancing Technologies (PET).

3. ONTWIKKELING INTERNET

Veel bedrijven en organisaties uit allerlei sectoren van onze maatschappij zijn van internet afhankelijk geworden. Paragraaf 3.1 laat zien dat het belang van internet voor het bedrijfsleven, de overheid en de burger steeds groter wordt en dat de opkomst van nieuwe toepassingen sterk afhankelijk is van de betrouwbaarheid van internet. In paragraaf 3.2 wordt aandacht besteed aan de marktontwikkeling op internet. Hierin komt de ontwikkeling van het aantal en de diversiteit van de diensten en dienstenaanbieders op internet naar voren.

3.1 Maatschappelijke en economische betekenis internet

Internet geeft individuen en organisaties nieuwe mogelijkheden om te informeren, te communiceren en handel te drijven. Bijgevolg heeft internet in een kort tijdsbestek een enorm belangrijke plaats in de samenleving ingenomen. Uit een onderzoek van SMO[8] onder haar achterban bleek dat met name jongeren en jongvolwassenen (35 jaar of jonger) in

hun professionele bestaan niet meer zonder internet kunnen. Eén op de vier is er zelfs in economisch opzicht sterk van afhankelijk. Informatienetwerken in het algemeen en internet in het bijzonder vormen meer en meer de ruggengraat van de samenleving.

Naast de afhankelijkheid van e-mail, webbrowsing en file transfer valt een toenemende belangstelling waar te nemen voor multimedia-toepassingen en voor interactieve diensten zoals tele-educatie en e-commerce. Ook telewerken impliceert een veel grootschaliger toepassing van internet. De verwachting is dat inherent aan de populariteit van internet als wereldwijd communicatiemedium, diensten en activiteiten die nu nog hoofdzakelijk buiten internet worden afgewikkeld, zoals telefonie en omroep, geleidelijk hierin zullen worden opgenomen. Welke behoeftes in de toekomst uiteindelijk door middel van internet zullen worden ingevuld, hangt echter mede af van de betrouwbaarheid van internet.

Indiërs gebruiken internet bij inzamelingsacties voor aardbeving
Verschillende Indiase websites helpen bij de coördinatie van de inzameling van hulpgoederen voor het rampgebied in India. Inwoners van Gujarat maken gebruik van internet om hulpgoederen te verzamelen en de logistiek van de hulp te organiseren. De site zorgt onder meer voor online registratie van hulpdonaties en helpt bij het opsporen van vermiste familieleden. Tot afgelopen week was *Panjokutch* een gemeenschapswebsite die hielp bij gearrangeerde huwelijken, die informatie over banen gaf en die reisadvertenties toonde. Nu is de website een informatiecentrum voor hulp aan aardbevingslachtoffers en hun familie. De site www.kutchinfo.com geeft details over de behoeftes in verschillende getroffen dorpen.

Hulporganisaties wijzigen e-mailactie onder druk banken
6-2-2001 Geld voor de hulp aan India kan niet per e-mail worden gestort. De Samenwerkende Hulporganisaties (SHO) hebben na overleg met de Nederlandse Vereniging van Banken (NVB) besloten niet met internetmachtigingen te werken, maar met de traditionele acceptgiro. De hulporganisaties wilden aanvankelijk dat mensen via internet geld zouden storten, maar de NVB had hier moeite mee. Zij vindt het elektronisch machtigen nog niet veilig genoeg.
bron: www.cyberacties.nl

3.2 Marktontwikkeling

Het aanbod en de vraag naar capaciteit van infrastructuur is de afgelopen jaren explosief gestegen. De nota *Netwerken in Cijfers*[9] voorspelt meer dan een verdrievoudiging van het gebruik van ICT-netwerken in de periode 1998 tot en met 2002. De toename van het internetverkeer laat zich goed meten op de Amsterdam-Internet eXchange waar veel verkeer in Nederland samenkomt. Het internetverkeer blijkt zich hier elke 6 à 7 maanden te verdubbelen[10].

De spectaculaire vergroting van de transmissiecapaciteit tezamen met de opkomst van internet vormt een sterke drijvende kracht voor nieuwe diensten. De verschuiving van de meerwaarde van «eenvoudige transmissie» naar de productie en samenstelling van dienstenpakketten bewerkstelligt een toename van het aantal en de diversiteit van internetdiensten. E-mail, telewerken, virtual communities, e-commerce, gaming en de vele informatiediensten op internet zijn betrekkelijk nieuwe verschijnselen. Desondanks zijn ze niet meer weg te denken en SMO laat zien dat velen sterk afhankelijk van dergelijke diensten zijn geworden.

Wat voor de diensten geldt, geldt eveneens voor de dienstverleners. Ook de spelers die in het internetveld opereren, zijn de laatste jaren enorm in aantal en diversiteit toegenomen. Klassieke telecommunicatie-operators

kunnen al lang niet meer het totale proces van infrastructuurplanning en -bouw tot en met het leveren van alle denkbare diensten en dienstenpakketten volledig in eigen hand houden. Hierdoor ontstaan er veel kansen voor kleinschalige, gespecialiseerde bedrijven en initiatieven, dichtbij de klant. De opkomst van een bonte stoet van service providers, waaronder de Application Service Provider, laat deze trend duidelijk zien. De ASP is een goed voorbeeld van een dienstverlener waarbij de betrouwbaarheid van het internet een kritieke succesfactor wordt.

Application Service Provider (ASP)
De kerneigenschap van het concept is dat gebruikers op afstand toegang hebben tot applicaties, die op een centrale machine draaien. Zo kan bijvoorbeeld *Hotmail* als een ASP-dienst worden beschouwd. Daar waar ASPers bedrijfskritische applicaties aanbieden is de afhankelijkheid tussen de klant en de ASPer groot. Dat legt allerlei eisen op aan de ASPer zelf, maar zeker ook aan de beschikbaarheid en betrouwbaarheid van de telecommunicatie-infrastructuur.

Volgens TNO-onderzoek zijn de effecten van de opkomst van ASP voor de kwetsbaarheid van internet: 1. een toename van de behoefte aan beschikbaarheid van telecommunicatiediensten en 2. een toename van de behoefte aan bescherming van gegevens op het internet (integriteit en exclusiviteit). De kwetsbaarheid van internet en de veiligheid van bedrijfsgegevens zijn essentiële belemmeringen voor ASP.

De toename van de diversiteit en het aantal van diensten en dienstenaanbieders kan leiden tot een diffuus beeld van het aanbod. Voor potentiële afnemers kan het onduidelijk zijn wat van een dienst verwacht mag worden. Om het marktmechanisme optimaal te kunnen laten functioneren, is het van belang dat de kwaliteit en beschikbaarheid van (telecommunicatie)diensten in voldoende mate transparant is.

4. KWETSBAARHEDEN

Om de incidenten en verstoringen te kunnen aanpakken, is inzicht vereist in de kwetsbaarheden op internet. Het is echter op dit moment niet mogelijk gebleken om de kwetsbaarheden van een kwantitatieve basis te voorzien, niet in de laatste plaats omdat goede indicatoren en data nog niet of maar uiterst beperkt beschikbaar zijn of nauwelijks gemeten worden. Om deze reden is op basis van een expert-analyse een inschatting gemaakt van de belangrijkste kwetsbaarheden aan de hand van de kans van voorkomen en de impact hiervan. Hieruit is gebleken dat de zwakke plekken van internet talloos en zeer divers van aard zijn.

Dit hoofdstuk gaat dieper in op de kwetsbaarheden op internet. In paragraaf 4.1 worden de oorzaken van (ver)storingen toegelicht die ingrijpen op het functioneren en het gebruik van internet. Paragraaf 4.2 behandelt de resultaten van de kwetsbaarheidsanalyse en in paragraaf 4.3 komen de maatschappelijke en economische gevolgen van incidenten op internet aan bod. Tenslotte worden in paragraaf 4.4 enkele conclusies getrokken.

4.1 Oorzaken van (ver)storingen

Internet is in de jaren 60 ontstaan uit het door de Amerikaanse overheid opgerichte ARPANet. De leden van dit netwerk waren universiteiten en militaire instellingen die het netwerk gebruikten voor gezamenlijk onderzoek. In de tijd van het ARPANet was het netwerk klein en konden de leden elkaar vertrouwen. Als gevolg van dit vertrouwen besteedden de ontwerpers van TCP/IP (de basisprotocollen van internet) minder aandacht aan veiligheid. Er werd geen rekening gehouden met de mogelijkheid dat

internet wel eens zou kunnen uitgroeien tot een wereldwijde infrastructuur waarop honderden miljoenen gebruikers, met soms zeer uiteenlopende drijfveren, aangesloten zijn. Hierdoor bestaat er nog steeds een groot aantal opvallende gaten in de beveiliging van het netwerk.

Zwakheden in IP-protocollen vormen een duidelijke kwetsbaarheid van internet. Door het uitbuiten van deze zwakheden is het voor hackers in binnen- en buitenland mogelijk om (distributed) denial of service (DoS)-aanvallen (zoals die begin 2000 op CNN, Yahoo en E-Bay) te richten op routeringsapparatuur, specifieke organisaties en netwerken. Dergelijke aanvallen leiden tot het uitvallen van internetcommunicatie, wat voor flinke schade voor bedrijven en instellingen kan zorgen.

> **Hackers strike again. Washington Post, 9 februari 2000.**
> Een serie computer aanvallen heeft er voor gezorgd dat sinds maandag de toegang tot internet sites van Yahoo, E-bay, Amazon en CNN geblokkeerd is.
> http://www.washingtonpost.com/wp-dyn/articles/A30 882–2000Feb9.html

Naast het feit dat internet vanwege zijn geschiedenis een aantal inherente zwakheden kent, blijken veel organisaties geen of een slecht informatiebeveiligingsbeleid te voeren. Door het gebrek aan risicobewustzijn en doordat informatiebeveiliging dikwijls slechts als een kostenpost wordt beschouwd, waaraan geen directe baten verbonden zijn, heeft slechts een klein percentage van bedrijven een volledig uitgewerkt en geïmplementeerd beveiligingsplan.

Het is belangrijk te beseffen dat het installeren van firewalls – die hackers buiten de deur houden – onvoldoende is. Zorgvuldig veiligheidsbeheer betekent onder andere het dichten van beveiligingsgaten in het besturingssysteem en de applicaties. Ook het disciplineren van gebruikers om goede wachtwoorden – wachtwoorden die moeilijk te kraken zijn – te hanteren is een cruciaal onderdeel van het veiligheidsbeheer van organisaties. Verder wordt hier nog gewezen op het *insider*-risico. Insiders zouden verantwoordelijk zijn voor 40% tot 80% van de beveiligingsincidenten[11]. Het structureel aanpakken van informatiebeveiliging en het nemen van maatregelen om de niet-geaccepteerde risico's en de effecten daarvan te minimaliseren, is voor organisaties van groot belang.

Tenslotte worden ook de fabrikanten, die te weinig aandacht aan beveiliging schenken, vaak genoemd als een achterliggende oorzaak van een groot aantal incidenten. Een korte *time-to-market* kan ten koste gaan van de veiligheid en betrouwbaarheid, doordat minder tijd wordt vrijgemaakt voor het testen van de producten. Daar komt bij dat in een groot aantal producten beveiligingsopties standaard zijn uitgeschakeld of soms helemaal afwezig zijn.

4.2 Kwetsbaarheidsanalyse

In hoofdstuk 1 is reeds vermeld dat, ten behoeve van het vergroten van het inzicht in de problematiek, door de organisaties Stratix en TNO een inschatting is gemaakt van de belangrijkste kwetsbaarheden. Met betrekking tot deze analyse is gekeken naar de kans van optreden en de omvang van de schade. Het begrip kwetsbaarheid wordt aldus gerelateerd aan het risicobegrip (kans x schade). De analyse is gebaseerd op professionele kennis, jarenlange ervaring van deskundigen in het veld en de weinig beschikbare statistische gegevens over incidenten. Tabel 2 toont de resultaten van deze expert-analyse (zie bijlage C voor een verklarende lijst van termen).

Op de verticale as van de tabel is een indeling gemaakt in lagen. Een laag vertegenwoordigt bepaalde netwerkfuncties en iedere laag (afgezien van de twee onderste) maakt gebruik van de functies die de laag daaronder aanbiedt. De functies variëren van het transporteren van bits op de transmissielaag tot het uitwisselen van bijvoorbeeld een e-mail op de informatielaag.

Op de horizontale as is een indeling gemaakt in verantwoordelijkheidsgebieden. Incidenten kunnen ingrijpen op het beheergebied van één organisatie (2e kolom), maar het is ook mogelijk dat door ketenafhankelijkheden en -kwetsbaarheden meerdere organisaties getroffen worden (3e kolom). Tenslotte kunnen verstoringen een dusdanige omvang aannemen dat sprake is van bedreiging van vele organisaties en/of landen (zie laatste kolom).

Tabel 2. Overzicht van de belangrijkste kwetsbaarheden

Beheer Laag	Beheergebied één organisatie	Meer beheergebieden; Nationaal	Meer beheergebieden; Internationaal
Informatie	• **hackers, computercriminelen** • **DoS aanval, email- bommen** • **(persoons- en financieel-) vertrouwelijke gegevens slecht beveiligd**	• **(h)activisten, computer-criminelen** • **verlies vertrouwen in e-commerce, door fraude en slechte beveiliging vertrouwelijke gegevens**	• **macro-virusaanvallen** • **DoS aanval** • **verlies vertrouwen in e-commerce, door fraude en slechte beveiliging (vertrouwelijke) gegevens**
Generieke-applicaties		• DoS aanval of hack op belangrijke internet-componenten als DNS en TTP • verlies van vertrouwen in TTP • SpoFs bij conversiepunten internet-diensten naar/van mobiele diensten	• verlies van vertrouwen in TTP • integriteit root-servers
Netwerk	• ontbreken van een security policy, slechte firewalls • opleiding, training, tijd en middelen • uitval van belangrijke ISP's/ASP's en netwerken door DoS aanvallen of hacks	• uitval AMS-IX betekent uitval groot deel internetfaciliteiten Nederland • uitval van gedeelten van de Nederlandse internetbackbone	• uitval van internationale knooppunten
Transmissie		• schaarste local loop capaciteit • breuk glasvezelkabels door graven en natuurinvloeden • schaarste apparatuur/glasfiber, schaarste menskracht, vertraging graafrechten • schaarste aan verbindingen bij de ISP	• uitval internetbackbone (bv. zeekabels) • cross-connects zijn niet alle redundant/ dubbel uitgevoerd, waardoor SpoF • SPoFs in beheer- en besturings-systemen
Convergentie & Verweven-heid		• onbedoelde ketenafhankelijkheden in complexe netwerken waar het totaaloverzicht ontbreekt	• schaarste in netwerk kan leiden tot cascade-uitval • bekende gaten in COTS middelen

AMS-IX Amsterdam Internet eXchange
DoS Denial Of Service
ASP Application Service Provider
ISP Internet Service Provider
COTS Commercial Off The Shelf
SpoF Single Point of Failure
DNS Domain Name Server
TTP Trusted Third Party

De waardering van de kwetsbaarheden per laag is sterk afhankelijk van de betrokken partijen en het getroffen gebied. Er is niet duidelijk een laag aan te wijzen waar de belangrijkste kwetsbaarheden geconcentreerd zijn. Uit de risico-analyse blijkt dat op alle niveaus en voor alle gebieden er belangrijke kwetsbaarheden zijn, die niet veronachtzaamd kunnen worden.

Informatielaag

Op de informatielaag vormen hackers en andere computercriminelen een continue dreiging voor bedrijven en organisaties, die met hun beveiliging achterlopen op het bekend worden van nieuwe kwetsbaarheden. Slechte beveiligingsontwerpen en slecht geteste implementaties van besturingssystemen, databases, netwerkprogrammatuur, webservers en browsers geven de hacker aangrijpingspunten om in systemen en netwerken binnen te dringen.

Ook virussen zijn een grote bedreiging voor internetgebruikers. Per week worden tientallen zo niet honderden nieuwe virussen vanuit het internet op computersystemen losgelaten. Gemiddeld bevat één op de 1500 e-mailberichten een virus; voor gratis e-mailaccounts is dat één op de 500 e-mails. Het I-love-you virus heeft laten zien dat virussen in een zeer korte tijd enorme schade kunnen veroorzaken. Thuisgebruikers beginnen zich pas recent te wapenen door middel van anti-virusprogramma's.

Generieke applicatie- en de netwerklaag

In de generieke applicatie- en de netwerklaag kan de uitval van kritische internetcomponenten ernstige gevolgen met zich mee brengen. Zo steken er, ondanks de vermeende robuustheid van het internet, bij tijd en wijle berichten de kop op over het verlies van beschikbaarheid van (delen van) het internet, omdat steeds meer belangrijke onderdelen van het internet op enkele lokaties geconcentreerd zijn. Een goed voorbeeld is een artikel uit het wetenschapsblad Nature[12]. De conclusie van dit artikel is dat de grote mate van robuustheid ten opzichte van storingen in het netwerk gepaard gaat met een aanmerkelijke kwetsbaarheid ten opzichte van de vitale knooppunten. Het netwerk zou bij uitval van vitale knooppunten betrekkelijk snel uiteenvallen in eilanden die niet meer met elkaar kunnen communiceren.

> Op 24 augustus 2000 begaven tijdelijk vier van de dertien root-servers van internet het. De storing trad tegelijkertijd op in de servers van Network Solutions die de internet routering beheert. Het ging om een server bij Network Solutions in de Bay Area, en servers in Virginia, Californië en Tokio. De storing nam een uur in beslag; de angst dat er een hack was gepleegd was groot. De storing was het gevolg van de invoering van niet goed geteste programmatuur. (Wall Street Journal).
> In Europa staan rootservers in Stockholm en Londen. In juli 1997 waren zeven Europese root-servers vier uur uit de lucht ten gevolge van verkeerd installeren van een «domein name server (DNS) database» waardoor het Europese internet goeddeels plat ging. (Bron: Wayner 1997).

Transmissielaag en convergentie & verwevenheid

De transmissielaag verzorgt het «bittransport» voor de diensten van de netwerklaag. Door fouten in de uitvoering van meervoudige verbindingen en door acceptatie van enkelvoudige verbindingen ontstaan single point of failures (SPoF's). Tegelijkertijd treedt verwevenheid op, waarbij door één en hetzelfde transmissiemedium (bijv. glasvezel) alarmsignalen, controle- en stuursignalen, datatransport, mobiel en vast telefoonverkeer en betalingsverkeer gaan.

> Op 15/6/1999 ging om 08.00 uur een damwandplank gelijktijdig door 4 glasvezels van KPN Telecom in de haven van Groningen. Resultaat was dat de provincie Groningen en grote delen van Friesland en Drenthe tussen de 8 en 17 uur verstoken waren van mobiele en vaste telefonie, 1-1-2, alarmeringen, fax- en dataverkeer, geld- en pindiensten, internet. De mobiele telefoons van KPN concurrenten vielen ook uit omdat zij deels dezelfde infrastruc-

tuur gebruiken. Informatiediensten naar en van andere delen van Nederland en internet vielen uit.

Een andere verwevenheid ontstaat door het toenemend gebruik van commercial-off-the-shelf (COTS) apparatuur, programmatuur en diensten. Vroeger werd speciale apparatuur en programmatuur ontwikkeld voor toepassingen als monitoring en besturing, calamiteitendiensten en defensie-toepassingen. De inherente veiligheid kwam deels voort uit de kleinschaligheid en de onbekendheid bij derden met het gebruikte besturingssysteem en toepassingsprogrammatuur («security-by-obscurity»).

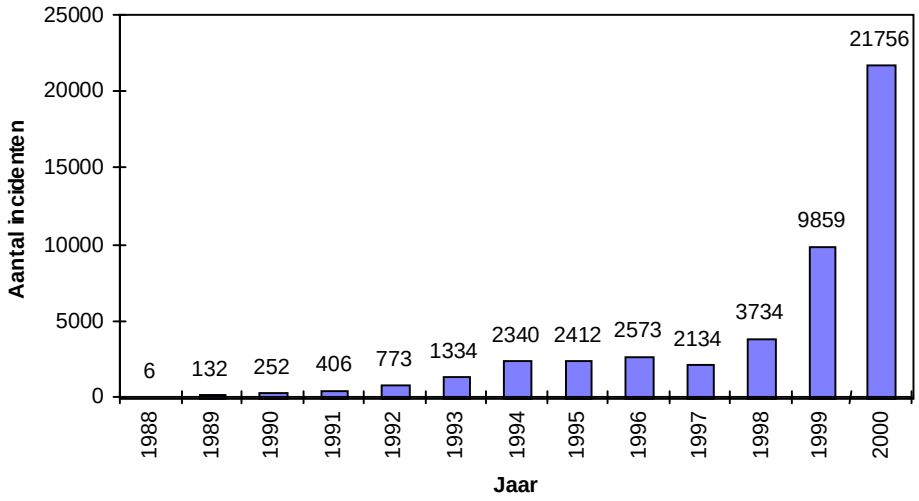
Tegenwoordig is het grootschalig gebruik van standaard of COTS-software erg in trek, hetgeen extra risico's met zich mee brengt. Het ontdekken van een beveiligingsgat in COTS-software heeft niet op slechts één organisatie betrekking, maar kan een hele markt duperen. Dat een incident als het I-love-you virus zoveel schade heeft kunnen aanrichten, is mede een gevolg van het feit dat het merendeel van de internetgebruikers hetzelfde e-mail programma op zijn computer heeft geïnstalleerd.

4.3 Maatschappelijke en economische gevolgen van kwetsbaarheden

De huidige en in de toekomst te verwachten omvang van de schade als gevolg van de in de vorige paragraaf beschreven kwetsbaarheden is op dit moment niet exact aan te geven. Wel zijn deskundigen het er wereldwijd over eens dat de kans op risicogedrag via internet zal toenemen. Dit alleen al door de reële verwachting dat het gebruik van internet en van toekomstige modernere ICT-innovaties sytematisch zal doorzetten. Tevens zullen grotere risico's ontstaan door bijvoorbeeld de toename van het volume van financiële transacties. Tenslotte is wegens de niet aflatende vraag om ook telewerkers en bedrijfsrelaties aan hetzelfde informatiesysteem te verbinden, steeds minder sprake van «gesloten» netwerken die niet van buitenaf benaderd kunnen worden. Hierdoor neemt het aantal mogelijkheden voor aanvallers om binnen te dringen nog eens toe.

Behalve de geluiden uit het veld laten ook de weinig beschikbare statistische gegevens zien dat de kwetsbaarheid van internet een steeds urgenter probleem wordt. In figuur 1 is de toename van het aantal gerapporteerde incidenten sinds de oprichting van het Computer Emergency Response Team Coordination Center (CERT/CC) afgebeeld. CERT/CC coördineert het bestrijden en het op korte termijn afhandelen van grootschalige computerinbraken, computervirussen en andere aanvallen op de op internet aangesloten computersystemen en netwerken. Dit centrum wordt mede gefinancierd door de Amerikaanse overheid en is verbonden aan het *Software Engineering Institute* dat beheerd wordt door de Carnegie Mellon University. Iedereen die een veiligheidsprobleem op internet heeft ondervonden, wordt aangemoedigd om dit (ook) bij CERT/CC te melden. Onder een incident wordt verstaan: «The act of violating an explicit or implied security policy». Zie bijlage C voor meer informatie over CERT/CC.

Figuur 1: Enkele CERT/CC statistieken over de jaren 1988 t/m 2000.



Enig inzicht in de economische schade als gevolg van misbruik is gewenst. De internationale accountancyorganisatie Price Waterhouse Coopers heeft berekend dat de schade als gevolg van het plegen van fraude via internet in 1998 wereldwijd ruim 33 miljard gulden bedroeg (terwijl volgens hetzelfde bureau de schade in 1996 nihil zou zijn). Werkgeversvereniging VNO-NCW schat de schade die het computervirus «I love you» in Nederland heeft aangericht op f 50 miljoen. Het verlies aan productiviteit en kosten die bedrijven maken om software te repareren zijn de grootste schadeposten[13].

Uit het vijfde jaarlijkse onderzoek[14] naar computerbeveiliging bij bedrijven dat de American Society for Industrial Security (ASIS) samen met Price Waterhouse Coopers heeft uitgevoerd, blijkt dat in 1999 bedrijven meer dan 45 miljard dollar hebben verloren als gevolg van informatiediefstal. Dergelijke berekeningen leggen naar verwachting nog maar een fractie van de werkelijk geleden schade bloot. Het is gebleken dat veel bedrijven – in verband met mogelijke imagoschade – niet bereid zijn aangifte te doen bij de justitiële autoriteiten.

Hackers breken in bij restaurant: witbier op

Den Haag – Zelf kan hij «nog net een e-mailtje versturen» maar de Haagse horeca-ondernemer Hans de Bruijn is wel overtuigd van de waarde van internet voor zijn bedrijven. Sinds vorige week is die prille liefde echter zeer bekoeld. Zijn restaurant De Eeuwige Jachtvelden aan het Plein werd toen waarschijnlijk het slachtoffer van «hackers». Normaal komen per dag ongeveer 120 tafelreserveringen binnen per e-mail. Klanten kunnen via de website van het restaurant het menu bekijken en een tafeltje bespreken. Vorige week donderdag, vrijdag en zaterdag kwam er echter geen enkele reservering binnen. Erger was dat op vrijdagavond om 19 uur, midden in het borreluur op het Plein, het witbier ineens op was. Iets wat normaal gesproken onmogelijk is. De leverancier van het bier kan de voorraadgegevens van De Eeuwige Jachtvelden zelf bekijken via het computersysteem en kan dus precies zien wanneer de voorraad aangevuld moet worden.

De Bruijn: «Een systeem dat altijd perfect heeft gewerkt. Ik wist meteen dat er iets niet klopte». Het bleek dat onbekenden hadden ingebroken in het computersysteem van De Eeuwige Jachtvelden. Reserveren via de website was onmogelijk gemaakt.

Verder bleek dat gedurende drie dagen de bestellingen voor de keuken zijn verstoord en voorraden niet zijn bijgehouden door het systeem. De Bruijn weet niet wat dit «misselijke geintje» zijn zaak heeft gekost. «Enkele duizenden guldens, schat ik. Het zijn de drukste dagen van de week». De ondernemer heeft «geen flauw idee» wie er achter de hacker-actie kan zitten. «Ik lees wel eens verhalen over die gastjes die hele avonden inbreken in de systemen van multinationals of bij het Pentagon ofzo. Zonder reden, gewoon voor de lol». De Bruijn bekijkt of hij de schade kan verhalen op de internetprovider, die zijn website hoort te beschermen. Hij verlangt niet terug naar het pre-internettijdperk, want zijn website levert hem veel gemak én nieuwe klanten op. «Laten we wel wezen; de tijd van de postduif is voorbij. Maar ik ben geschrokken hoe kwetsbaar al die dure elektronica blijkbaar is».
Bron: Haagsche Courant 23–08–2000

Maatschappelijke schade treedt vooral op in de sfeer van verlies van internetdiensten als email en het world wide web (www). Enerzijds kunnen particulieren geen gebruik meer maken van de informatiefunctie van internet en anderzijds kunnen organisaties, die in toenemende mate de verstrekking van informatie via het internet laten plaatsvinden, schade ondervinden.

Een goed voorbeeld van het gebruik van internet voor informatieverstrekking aan de bevolking is de publicatie van het rapport van de commissie Oosting over de vuurwerkramp in Enschede op de website van het ministerie van BZK. Op deze wijze wordt een groot publiek in staat gesteld op een relatief eenvoudige wijze toegang te krijgen tot wezenlijke informatie, hetgeen bevorderlijk wordt geacht voor de deelname aan politiek/maatschappelijke discussies. Tenslotte wordt in toenemende mate het gebruik van internet voor informatieverspreiding door hulpverlenende instanties gesignaleerd.

4.4 Conclusies

Uit vorige paragrafen is gebleken dat internet diverse vormen van kwetsbaarheden kent. Verschillende oorzaken liggen hieraan ten grondslag. Duidelijk is dat het open karakter van internet een grote rol speelt, maar ook dat het beveiligingsbeleid van veel organisaties en de betrouwbaarheid van producten vaak tekort schieten. Hackers en virussen vormen grote bedreigingen voor zowel organisationele als individuele internetgebruikers.

De verwachting is dat de maatschappelijke en economische gevolgen van een kwetsbaar internet steeds groter worden. Nieuwe toepassingen als transactie-diensten, telewerken en e-commerce zorgen voor een sterke groei van het internetgebruik, wat gepaard gaat met een groei van het aantal incidenten. Daar komt nog bij dat het toenemende gebruik van standaard producten ten koste van speciaal voor de klant ontworpen software, grotere risico's voor meerdere organisaties met zich mee brengt wanneer nieuwe gaten aan het licht komen.

Marktpartijen en overheid kunnen maatregelen nemen om de kwetsbaarheid op het internet te verminderen en daarmee het vertrouwen in het internet van bedrijfsleven en publiek te verhogen. Het volgende hoofdstuk laat zien dat de noodzaak om in te grijpen ook internationaal wordt onderkend.

5. INTERNATIONALE INITIATIEVEN

In verschillende landen en internationale organisaties zijn recent initiatieven genomen ten aanzien van de kwetsbaarheid van internet. In dit hoofdstuk worden een aantal opvallende beleidsontwikkelingen besproken van achtereenvolgens de Verenigde Staten, Duitsland, België, de Europese Commissie en de OESO.

5.1 Verenigde Staten

De activiteiten van de Verenigde Staten zijn niet zozeer gericht op de economische veiligheid, als wel op de nationale veiligheid en «information warfare». In 1996 werd President Clinton gealarmeerd door de gevolgen van enkele grootschalige stroomstoringen. De maatschappelijke verstoring was groot en plunderingen vonden plaats. Het besef dat de Amerikaanse samenleving niet alleen kwetsbaar zou kunnen zijn voor storingen en natuurgeweld, maar ook voor bijvoorbeeld terrorisme, bracht Clinton ertoe een onderzoekscommissie over *kritieke infrastructuren* in te stellen. Doelstelling van de *Presidents' Commission on Critical Infrastructure Protection* (PCCIP) is het analyseren van de afhankelijkheid en kwetsbaarheid van de samenleving en het opstellen van beleidsvoorstellen om de eventueel geconstateerde kwetsbaarheid te verminderen.

Een uitvloeisel van de commissie is het *National Infrastructure Protection Center* (NIPC), dat onderdeel vormt van het Ministerie van Justitie en gehuisvest is bij de FBI. Het NIPC fungeert als een landelijk, centraal bewakings- en alarmeringscentrum voor infrastructuurproblemen met een grote nadruk op ICT. Bij het NIPC werken ruim-80 FBI agenten en een twintigtal medewerkers van andere agencies. De reden dat het NIPC ondergebracht is bij de FBI is pragmatisch. Een deel van de FBI hield zich al bezig met dezelfde problematiek, een coördinatie en communicatiecentrum was al beschikbaar en op deze manier zou de informatieuitwisseling met de Federale opsporing gewaarborgd zijn.

Naar aanleiding van het snel groeiende aantal incidenten en de door de PCCIP geïdentificeerde kwetsbaarheid heeft de toenmalige President Clinton bij de State of the Union op 7 januari 2000 een *deltaplan*[15] gelanceerd voor de bescherming van informatiesystemen en infrastructuren van de samenleving van de Verenigde Staten. Hierin wordt veel aandacht besteed aan regelmatige en tijdige uitwisseling van informatie over indringers en aanvallers tussen civiele overheidsnetwerken, het netwerk van defensie en de informatieanalyse- en uitwisselingscentra van private organisaties (Information Sharing and Analysis Center, ISAC).

De *ISACs* zijn punten waar informatie over een ICT-incident vertrouwelijk kan worden gerapporteerd en verwerkt. Dergelijke rapporten kunnen leiden tot een waarschuwing aan alle deelnemers. Door anonimiseren kan men nooit achterhalen bij welke concurrent een incident plaatsvond. Momenteel is er al een ISAC voor banken en financiële instellingen, voor de telecommunicatie-industrie, voor energiebedrijven en één voor de IT-sector. Tijdens de uitbraak van het I-Love-you virus heeft de Financial Services ISAC, oftewel FS-ISAC uitstekend gewerkt. Het grote probleem was echter dat de verschillende ISACs geen onderling waarschuwingssysteem kennen en dat het NIPC traag reageerde.

5.2 Duitsland

In Duitsland is in 1991 het *Bundesamt für Sicherheit in der Informationstechnik* (BSI) opgericht. Het BSI, met circa 500 medewerkers, treedt actief naar buiten met preventie-informatie over een breed scala aan ICT-bedreigingen voor de overheid en het Duitse bedrijfsleven. Het geeft folders, CD's en website-informatie uit over de gevaren van onder andere internet. Daarnaast heeft het BSI de taak van Computer Emergency Response Team (BSI-CERT) voor de gehele Duitse overheid.

Na de plaagacties begin februari 2000 die in de Verenigde Staten (Yahoo, CNN, FBI), Nederland en ook in Duitsland systemen onbereikbaar maakten, heeft de Duitse minister van Binnenlandse Zaken Otto Schily de taakgroep *Sicheres Internet* (SI) in het leven geroepen.
Deelnemers zijn verschillende Bundesministeriums, maar ook het bedrijfsleven (banken, service providers) wordt erbij betrokken. Het eerste resultaat is een aanbevelingslijst met 15 beveiligingsmaatregelen gericht op eindgebruikers, internet providers, server providers en content providers.

Het Bundesministerium für Wirtschaft und Technologie, het BSI en het Bundesministerium des Innern hebben een publieks- en bedrijfsvoorlichtingswebsite[16] ingesteld op het gebied van internetbeveiliging *Sicherheit im Internet* (SiI). Doelstelling is het geven van betrouwbare informatie over recente incidenten op het internet (denial-of-service aanvallen, I-Love-You e.d.), over nationale ontwikkelingen, preventie tips en het bieden van een forum voor informatie-uitwisseling.

5.3 België

Naar aanleiding van het I-love-you virus begin mei 2000 richtte Minister Daems van Telecommunicatie samen met het bedrijfsleven een *virusmeldpunt* op, met de bedoeling ernstige virussen tijdig te detecteren en aan een breed publiek kenbaar te maken. Dit virusmeldpunt is gehuisvest bij het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT), de Belgische regelgever voor de postdiensten en de telecommunicatie, en zou als zeef moeten fungeren in de overvloed aan virusmeldingen. Hierdoor kunnen nepmeldingen van serieuze bedreigingen worden onderscheiden. Zo'n dertig specialisten testen bij het BIPT virusmeldingen op hun waarde[17]. In februari dit jaar werd de verkeersradio gebruikt om internetters te waarschuwen voor het Anna Kournikova virus.

5.4 Europese Commissie

De Europese Commissie is in december 1999 met het e-Europe-initiatief gestart met als doel de meest competitieve en dynamische economie in de wereld te worden. Voor de uitwerking van de hoofdlijn *een goedkoper, sneller en veiliger internet* van het actieplan e-Europe 2002[18] is het onderdeel *Veilige netwerken en overige onderwerpen van informatiebeveiliging* aangemerkt als een prioriteit. De Commissie bereidt een strategieplan voor, die specifiek gericht is op netwerkbeveiliging. Daarvan maakt onder andere deel uit het tot stand komen en samenwerken van CERT's; aandacht voor kwetsbaarheid en afhankelijkheid van op IP gebaseerde communicatie-infrastructuur (vast en mobiel); informatiebeveiliging en het ontwikkelen van standaarden.

Een andersoortige uitwerking van het actieplan e-Europe 2002 is de Mededeling over het verbeteren van de veiligheid van informatie-infrastructuren en het bestrijden van computercriminaliteit[19]. In de mededeling geeft de Commissie te kennen dat zij voornemens is een *EU-forum* op te richten waarin rechtshandhavingsinstanties, internet service providers,

telecommunicatie-exploitanten, organisaties op het gebied van burgerlijke vrijheden, consumentenorganisaties, gegevensbeschermingsinstanties en andere betrokken partijen samenkomen om het wederzijds begrip en de samenwerking op EU-niveau te verbeteren. Het forum zal het publiek wijzen op de gevaren van criminelen op internet, de beste beveiligingsmethoden bevorderen, zoeken naar doeltreffende instrumenten en procedures om computercriminaliteit te bestrijden, en de verdere ontwikkeling van systemen voor vroegtijdige waarschuwing en crisisbeheer bevorderen.

5.5 OESO

Om de internationale consensus en samenwerking tussen overheden en private sector te bewerkstelligen ten aanzien van de veiligheid van informatiesystemen, heeft de OESO een specialistische werkgroep opgericht. Hierin heeft de kwetsbaarheid van informatiesystemen recentelijk meer aandacht gekregen. De *Guidelines for the Security of Information Systems*[20] uit 1992, herzien in 1997, vormen een basis waarop genoemde samenwerking kan resulteren in een raamwerk voor de beveiliging van informatiesystemen. Ingegeven door het snel gegroeide belang van internet in de afgelopen jaren, het gedecentraliseerde en open karakter ervan, en de gebleken kwetsbaarheid, is een nieuwe herziening voorzien in 2001–2002. Hierin zal met betrekking tot kwetsbaarheid meer aandacht komen voor preventie, initiatieven uit de private sector en noodzakelijke standaarden. Een belangrijk element van deze activiteit zal zijn een discussie over de rol en verantwoordelijkheid van overheden in verhouding tot die van de private sector.

6. VISIE EN ROL OVERHEID

Voor het welzijn en de welvaart in Nederland wordt het essentieel geacht dat de mogelijkheden die internet biedt, zo goed mogelijk worden benut. In hoofdstuk 4 is echter gebleken dat internet vele verschillende vormen van kwetsbaarheden kent. Deze mogen niet worden veronachtzaamd. Ook buitenlandse overheden hebben de risico's onderkend en nemen maatregelen die een bijdrage zouden moeten leveren aan een betrouwbaarder internet. Dit hoofdstuk gaat in op de rol die de Nederlandse overheid voor zichzelf hierin ziet weggelegd en welke uitgangspunten worden gehanteerd voor de in het volgende hoofdstuk beschreven maatregelen.

6.1 Speelveld

Veel nationale overheden zijn, afgezien van de taak om hun eigen systemen te beschermen, nog zoekende naar hun rol inzake de kwetsbaarheid van het internet. Lopende discussies in EU en OESO, maar ook in ons land (o.a. Infodrome), getuigen hiervan. De mogelijke rol en sturingsinstrumenten van de overheid worden in deze gremia veelvuldig besproken, maar een eenduidig antwoord is nog niet geformuleerd. Een aantal kenmerken van internet ligt hieraan ten grondslag:

- ondanks dat de Amerikaanse defensie aan de wieg van het internet heeft gestaan, is de expansie van internet voornamelijk aangedreven door de private sector. Met name in het laatste decennium heeft het bedrijfsleven de ontwikkeling en het beheer van de diensten en onderliggende infrastructuur op zich genomen;
- standaardisatie is, aansluitend op het voorgaande kenmerk, een vorm van beheer. In het internetdomein is het standaardisatieproces overgelaten aan marktpartijen. Dit open standaardisatieproces is in hoge mate bepalend voor de wijze waarop het internet «bestuurd» wordt.

Overheden hebben hier, anders dan vroeger in de traditionele telecommunicatiewereld, weinig grip op;
- zoals reeds geschetst in paragraaf 3.2, zijn bij het leveren en afnemen van internetdiensten veel, diverse, partijen betrokken die dynamische onderlinge afhankelijkheidsrelaties onderhouden hetgeen centrale sturing bemoeilijkt.

Hieronder wordt ingegaan op de rollen zoals het kabinet deze momenteel voor zich ziet en wat van internetgebruikers en infrastructuuraanbieders wordt verwacht. Uiteraard zullen de internationale en maatschappelijke ontwikkelingen op dit vrij jonge beleidsterrein in de gaten worden gehouden en, waar opportuun, worden meegenomen in de verdere beleidsontwikkeling.

6.2 Rol

Gezien de wijze waarop internet tot stand is gekomen en functioneert, hebben in de visie van het kabinet internetgebruikers (zowel aanbieders als afnemers) en infrastructuuraanbieders de primaire verantwoordelijkheid voor het beveiligen en betrouwbaar maken van internet. Iedere partij dient voor zichzelf te beslissen welke maatregelen, procedures en producten noodzakelijk zijn om haar systeem te beschermen. Dit geldt uiteraard ook voor de overheid als beheerder van haar eigen informatiesystemen. Onlangs heeft minister Van Boxtel een nota[21] uitgebracht over de bescherming van de informatie-systemen van de overheid.

De overheid zal de ontwikkelingen op internet in samenhang met de effectiviteit van het beleid nauwgezet monitoren. Wanneer de uitkomst daartoe aanleiding geeft, kan bijtijds een verschuiving van een faciliterende naar een meer regelgevende rol plaatsvinden. Vooralsnog zal de overheid met betrekking tot haar inbreng bij het vergroten van de betrouwbaarheid van het internet, gezien de sterke dynamiek, de technische complexiteit en het grensoverschrijdende karakter van het vraagstuk, terughoudend zijn met aanvullende regelgeving om de zich nog ontwikkelende markt niet onnodig te verstoren. Het kabinet ziet thans met name een rol voor zich weggelegd in het scheppen van de juiste randvoorwaarden die internetgebruikers faciliteren bij het invullen van hun verantwoordelijkheden op dit gebied.

De actielijnen die invulling geven aan deze faciliterende rol van de overheid, staan beschreven in paragraaf 7.1. De rol kent de volgende elementen:
Voorlichting: gericht op het verhogen van de kennis van gebruikers;
Stimulering: gericht op de totstandkoming en het gebruik van ondersteunende voorzieningen, zoals informatiebeveiligingsmethoden- en hulpmiddelen, Trusted Third Parties en eenduidige en uniforme betrouwbaarheidsindicatoren.
Het bieden van voorzieningen: het voorzien in actuele informatie omtrent dreigingen, zoals virussen en het bieden van een tafel voor nationaal overleg.

Op dit nationaal overleg wordt in paragraaf 7.2 nader ingegaan. De in paragraaf 7.1 beschreven acties hebben namelijk alleen kans van slagen wanneer sprake is van een nauwe samenwerking tussen alle betrokken, publieke en private partijen. Tenslotte is de opsporing en vervolging van mensen die internet misbruiken en of strafbare feiten plegen via internet van groot belang. Op deze *handhavingsrol* wordt kort ingegaan aan het eind van paragraaf 7.1.

6.3 Uitgangspunten bij actielijnen

Dit hoofdstuk begon met een beschrijving van het speelveld, omdat dit bepalend is voor de mogelijke rol van de overheid, die zojuist is beschreven. Het hoofdstuk eindigt met een aantal uitgangspunten die zijn gehanteerd bij het vaststellen van de, in het volgende hoofdstuk uitgewerkte, actielijnen. De gehanteerde uitgangspunten worden hieronder belicht.

Behoud van innovatievermogen
De internet netwerkinfrastructuur is primair ontworpen voor het transport van gegevens naar gebruikers, zonder veel intelligentie (manipulatie van de gegevens, beveiligingsmechanismen) in het netwerk. De intelligentie zit met name aan de uiteinden van het internet, in de toepassingen bij de gebruikers. Dit verklaart het innovatievermogen en de stroom van nieuwe toepassingen van internetgebruik. Maatregelen om de kwetsbaarheid te verminderen moeten zo min mogelijk ten koste gaan van deze dynamiek en innovatievermogen om te voorkomen dat de uitwerking van de remedie erger is dan de kwaal die bestreden moet worden.

Rekening houden met dynamiek
Bedreigingen voor het functioneren van internet zijn dynamisch van aard. Het heeft geen zin om voor elke geconstateerde kwetsbaarheid een maatregel te verzinnen omdat deze kwetsbaarheden ten gevolge van de dynamische technologische ontwikkelingen veranderen in de tijd. Daarom is het van belang om maatregelen te nemen die het mogelijk maken om met deze dynamiek om te gaan en die zorgen voor een continue betrokkenheid en alertheid van belanghebbenden.

Noodzaak tot (inter)nationale samenwerking
Pas als er bij alle bedrijven en instellingen die in een netwerk samenwerken de juiste beveiligingsmaatregelen worden genomen, zal het geheel ook minder kwetsbaar worden. Daarnaast speelt samenwerking op internationaal niveau. Nederland kan het nationaal geregeld hebben, maar het nationale netwerk is direct verbonden aan de internationale netwerken. Mogelijke maatregelen moeten daarom breed, zowel in nationaal als internationaal verband, worden afgestemd.

Beheersbaar maken kwetsbaarheid internet hoogst haalbare
Internet zal, in analogie met de openbare weg, altijd onveiligheden blijven hebben. Ongelukken zijn nooit geheel te voorkomen. Geen enkele (private of publieke) partij kan een honderd procent veilig en betrouwbaar internet garanderen. Dat moet ook niet gesuggereerd worden. Het stelsel van maatregelen is er op gericht om, daar waar mogelijk, het manifest worden van kwetsbaarheden te voorkomen en daar waar dat niet mogelijk is, de risico's zoveel mogelijk beheersbaar te maken.

7. ACTIELIJNEN

Rekening houdend met de in het vorige hoofdstuk beschreven uitgangspunten, wordt in dit hoofdstuk ingegaan op de activiteiten die bijdragen aan het op een hoger peil brengen van de betrouwbaarheid van internet. Vanwege de vele partijen die betrokken zijn bij het vormgeven en implementeren van genoemde maatregelen, zal eveneens worden ingegaan op de wijze van (inter)nationale afstemming.

7.1 Overzicht van activiteiten

De hier beschreven activiteiten zijn een mix van activiteiten die al in meer of minder ver gevorderd stadium zijn opgepakt, en waarover de Tweede Kamer al eerder is geïnformeerd, en van compleet nieuwe onderwerpen. Om een samenhangend en consistent beleidskader rond het thema internetbetrouwbaarheid te schetsen, worden ook deze onderwerpen beschreven.

Bij elke activiteit is beschreven: het doel van de activiteit, de motivering waarom de activiteit bijdraagt aan het voorkomen c.q. beheersen van kwetsbaarheden en de uitvoering. Bij de uitvoering wordt aangegeven wat de overheid bij deze activiteit doet en wat van marktpartijen wordt verwacht. Indien aan een activiteit al uitvoering wordt gegeven, is daar kort de stand van zaken vermeld.

7.1.1 Voorlichting

Doel

Het versterken van de positie van de internetgebruiker, zowel bedrijfsleven als burger, door het bevorderen van bewustzijn en kennis van de veiligheidsrisico's die bij het gebruik van internet spelen en hoe met deze risico's kan worden omgegaan. Hiertoe dient objectieve en breed toegankelijke informatie beschikbaar te worden gesteld, rekening houdend met de verscheidenheid aan gebruikers (zowel consumenten als bedrijfsleven, zowel aspirant, beginnende als gevorderde internetgebruikers).

Motivering

Internetgebruikers hebben een belangrijke eigen verantwoordelijkheid voor het beveiligen van hun systemen c.q. communicatie. Kennis over de risico's en over welke maatregelen genomen kunnen worden om die te beheersen is een noodzakelijke randvoorwaarde voor internetgebruikers om zich bewust en met vertrouwen op de «elektronische snelweg» te kunnen begeven. Daarnaast wordt beoogd om de door diverse markt- en overheidspartijen, reeds in gang gezette voorlichtingsinitiatieven beter op elkaar af te stemmen. Daar waar informatie bij elkaar gebracht kan worden, zal de gebruiker efficiënter over meer informatie kunnen beschikken.

Uitvoering

In 2000 is er door V&W in samenwerking met EZ een marktonderzoek uitgevoerd en is er aansluitend een Ronde Tafelconferentie gehouden. Het doel was om een globale indruk te krijgen van de informatiebehoefte bij potentiële doelgroepen. Op basis van de verkregen inzichten bereidt een interdepartementale werkgroep inmiddels een voorlichtingsactiviteit voor die in 2001 zal starten en aan zal sluiten bij de campagne *Nederland gaat digitaal*. Rekening houdend met de verscheidenheid aan gebruikers wordt bekeken of de twee hoofddoelgroepen (burger en bedrijfsleven) nog nader moeten worden opgesplitst, wat de reikwijdte van de voorlichting moet zijn en via welke communicatiekanalen de voorlichting het beste kan plaatsvinden. Bij dit laatste aspect wordt nadrukkelijk de mogelijke rol van marktpartijen zoals branche- en gebruikersorganisaties meegenomen. De dynamiek van internet vereist een permanente verstrekking van informatie. Onderzocht wordt hoe deze aanhoudende informatievoorziening kan worden vormgegeven. Een web portal behoort hierbij tot één van de mogelijkheden.

7.1.2 Research & Development

Doel

Het bevorderen van onderzoek naar en ontwikkeling van nieuwe informatiebeveiligingsmethoden en -hulpmiddelen.

Motivering

De ontwikkeling en het op de markt brengen van een breed scala aan beveiligingsproducten draagt bij aan het tot stand komen van een veilige en betrouwbare informatie-infrastructuur en de ontwikkeling van de e-Society in het algemeen. Dit ondersteunt ook de Europese beleidsontwikkelingen zoals geformuleerd in het kader van het actieplan e-Europe. Maar ook de implementatie van nationaal beleid, zoals het stimuleren van het tot stand komen van TTP-diensten, is direct afhankelijk van het op de markt komen van goede en vooral ook gebruiksvriendelijke informatiebeveiligingsproducten. Nu de exportcontrole beperkingen op cryptografie binnen de Europese Unie en haar belangrijkste handelspartners buiten de Unie vorig jaar zijn vervallen, liggen hier ook meer kansen voor de ontwikkeling van Europese crypto-producten.

Uitvoering

Onderzoek op het gebied van internetbetrouwbaarheid heeft bij uitstek een internationale dimensie. De internetinfrastructuur reikt immers ver over onze landsgrenzen heen. Het is dus belangrijk dat Nederlandse bedrijven en onderzoeksinstellingen participeren in internationaal onderzoek. Het beleid is er daarom op gericht om, in samenwerking met Senter / EG-liaison, het Nederlandse bedrijfsleven en onderzoeksinstellingen actief te betrekken bij de ontwikkeling van toekomstige Europese onderzoeksprogramma's en de scoringskans op projecten onder bestaande Europese programma's te vergroten.
Dit laatste gebeurt onder andere door voorlichting te verstrekken over interessante projecten uit het lopende 5e Kaderprogramma (KP5) en door in te spelen op gunningscriteria voor toekenning van die projecten. Hierbij moet worden gedacht aan het faciliteren van de verspreiding van de onderzoeksresultaten die projecten opleveren en door te zorgen dat projectvoorstellen goed aansluiten bij het Nederlandse beleid op het gebied van «Trust and Confidence».

Voor wat betreft toekomstige onderzoeksprogramma's participeert Nederland actief in de discussies rondom de vormgeving van het 6e Kaderprogramma (KP6). Nederland benadrukt in die discussie het belang van het onderwerp «Trust and Confidence». Begin dit jaar is in het kader van KP6 met steun van ons land door de Europese Commissie een working party Trust & Confidence ingesteld. In deze werkgroep zullen de lidstaten met de Commissie afstemming plegen over de invulling en uitvoering van het deel van het kaderprogramma dat zich richt op veiligheid en betrouwbaarheid. Daarnaast organiseren V&W en EZ consultatiebijeenkomsten met de sector (bedrijven en onderzoeksinstellingen) over de vormgeving van KP6 en het onderdeel «Trust en Confidence» daarin.

Naast onderzoek op internationaal niveau, is ook nationaal onderzoek op het gebied van veiligheid en betrouwbaarheid belangrijk. Zonder een sterke nationale onderzoeksinfrastructuur op dit gebied, zou de Nederlandse bedrijven en kennisinstellingen de aansluiting met het buitenland missen. Er wordt in het kader van de – nationale – doelsubsidie, reeds enig onderzoek bij TNO verricht. Structureel onderzoek zal sterker worden gestimuleerd, waarbij ook gekeken zal worden naar de mogelijkheden van

(promotie-) onderzoek bij universiteiten op het gebied van internet betrouwbaarheid en veiligheid.

7.1.3 Beveiligingsbeleid en -maatregelen binnen een organisatie

Doel

Vermindering van de kwetsbaarheid op het niveau van individuele organisaties (bedrijven en overheden) door effectief management van informatiebeveiliging. Dit kan verwezenlijkt worden door te bevorderen dat een organisatie weloverwogen haar beveiligingsbehoeften bepaalt en vervolgens maatregelen implementeert die risico's tot een aanvaardbaar niveau reduceren.

Motivering

Een van de in paragraaf 4.1 genoemde oorzaken van verstoringen is dat veel organisaties geen of een beperkt veiligheidsbeleid voeren. Deze activiteit is er op gericht om dat te veranderen. Het behoud van beschikbaarheid, exclusiviteit en integriteit van informatie is essentieel voor zowel gebruikers als aanbieders van internetdiensten en -infrastructuur. Zij zijn potentieel kwetsbaar voor schending hiervan, hetgeen blijkt uit verschillende incidenten die optreden. Het preventief treffen van organisatorische- en technische maatregelen kan deze kwetsbaarheid verminderen.

Uitvoering

In Nederland bestaat een leidraad voor beleid en implementatie van informatiebeveiliging, bekend als *Code voor informatiebeveiliging*[22] en verkrijgbaar bij het Nederlands Normalisatie-instituut. De Code biedt een uitgebreide verzameling aandachtspunten voor een goede implementatie van informatiebeveiliging in het algemeen. In aanvulling daarop kunnen organisaties in Nederland op een juiste implementatie van beveiligingsmaatregelen gecertificeerd worden door een externe auditor op basis van een schema. Het gebruik van de Code en certificatie van organisaties hiertegen vindt momenteel nog slechts in beperkte mate plaats.

EZ en V&W zullen activiteiten ontplooien om de bekendheid en het nut van de Code breed onder de aandacht te brengen en het gebruik daarvan te stimuleren. Tevens worden eventuele belemmeringen, die het gebruik van de *Code* beperken, geïnventariseerd en wordt geholpen om deze zoveel mogelijk weg te halen. Hierbij zal ook meegenomen worden of de Code een nadere uitwerking behoeft voor internet gerelateerde risico's.

7.1.4 Exclusiviteit van informatie

Doel

Het bevorderen van de vertrouwelijkheid van berichten bij elektronische communicatie.

Motivering

Vertrouwelijkheid van communicatie heeft betrekking op het afschermen van de inhoud tegen kennisname door een derde. Het kabinet heeft voorgesteld om vertrouwelijke communicatie als een grondrecht te erkennen in de Grondwet. De Grondwet maakt met dit voorstel de bescherming van de vertrouwelijkheid van communicatie mede tot een zorg voor de overheid.

Uitvoering

De Telecommunicatiewet (hoofdstuk 11) kent reeds een inspanningsverplichting voor aanbieders van openbare telecommunicatienetwerken en -diensten ten aanzien van de beveiliging van netwerken en diensten ten behoeve van de bescherming van persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers. De invulling hiervan is afhankelijk van de afweging tussen veiligheidsrisico en beveiligingsniveau, rekening houdend met de stand der techniek en de kosten van uitvoering. Daarnaast hebben de betreffende aanbieders een informatieplicht richting consument ten aanzien van bijzondere risico's van betrokken diensten en netwerken.

Naast het scheppen van het regelgevend kader dient de overheid ook de overige randvoorwaarden die het belang van vertrouwelijke communicatie kunnen behartigen, in te vullen. Gebruikers kunnen, onafhankelijk van de beveiligingsmaatregelen van de operator én afhankelijk van hun eigen beveiligingsbehoefte, zelf hun berichten versleutelen. Versleutelde gegevens zijn alleen begrijpelijk voor de gesprekspartners. Hard- en software producten waarmee gegevens versleuteld worden, kunnen sinds de recente aanpassing van het exportcontrole beleid binnen de Europese Unie en haar belangrijke handelspartners makkelijker beschikbaar komen. Gebruikers zijn echter van het bestaan, het nut en de wijze van gebruik van deze producten vaak niet op de hoogte. Teneinde de bekendheid van gebruikers met de beveiligingsmogelijkheden te vergroten wordt in de actielijn «voorlichting» expliciet aandacht aan de beveiliging van vertrouwelijke informatie geschonken.

Tenslotte kan de overheid, met een mogelijke uitstraling naar private partijen, het gebruik van cryptografie bevorderen middels haar eigen beveiligingsbeleid. Door de ontwikkeling van *e-government* kan de overheid een voorbeeldfunctie vervullen ten aanzien van het gebruik van effectieve cryptografische oplossingen en daarmee het vertrouwen in cryptografische producten verhogen.

7.1.5 Transparantie door kwaliteitsgegevens

Doel

Deze activiteit is erop gericht om de marktwerking beter te laten functioneren door het vergroten van het inzicht in de aangeboden kwaliteit van dienstverlening door infrastructuuren dienstenaanbieders. Daarnaast kan het een beter (kwantitatief) inzicht geven in de beschikbaarheid van internet.

Motivering

In een situatie van een gedifferentieerde behoefte aan kwaliteit en het steeds afhankelijker worden voor de bedrijfsvoering en communicatie van externe netwerken, is het van belang om als afnemer informatie te hebben over aangeboden diensten. Dit geldt voor de hele keten, zowel voor eindgebruikers als voor infrastructuuraanbieders die via interconnectie diensten van elkaar afnemen. Infrastructuur- en dienstenaanbieders kunnen zich vervolgens onderscheiden in prijs/kwaliteitverhouding. Het marktmechanisme kan dan leiden tot kwaliteitscontracten waarin indicatoren zijn opgenomen die meetbaar zijn en kan op die manier bijdragen aan een betrouwbaarder internet. Uit het in opdracht van V&W uitgevoerde onderzoek naar de kwetsbaarheid van internet blijkt dat deze situatie echter in de praktijk nog niet bestaat. Het feit dat er geen structurele, uniforme meetresultaten van beschikbaarheidsindicatoren

voor handen zijn, leidt er bovendien toe dat er geen objectief beeld verkregen kan worden van de beschikbaarheid van het (Nederlandse deel) van internet. Een kwalitatieve inschatting is het hoogst haalbare gebleken, zoals verwoord in hoofdstuk 4 van deze nota.

Uitvoering

Infrastructuur- en dienstenaanbieders worden gestimuleerd om zelf, op vrijwillige basis, beschikbaarheids- en verkeersmetingen uit te voeren. Om dit proces te ondersteunen zal V&W dit jaar het initiatief nemen om in nauwe samenwerking met marktpartijen de totstandkoming van eenduidige en uniforme kwaliteitsindicatoren, meetmethoden en meetinstrumenten te stimuleren.
In aanvulling daarop wordt door V&W onderzocht of en hoe afspraken kunnen worden gemaakt met desbetreffende aanbieders omtrent de verwerking van meetgegevens en uitvoering van trendanalyses om op die manier een beter beeld van de beschikbaarheid van internet te krijgen en mogelijke kritische infrastructuurdelen te identificeren.

7.1.6 Alarmering en incident response

Doel

Het bijtijds tussen (inter)nationale belanghebbenden in een collaboratief netwerk[23] uitwisselen van meldingen en informatie omtrent dreigingen, kwetsbaarheden en tegenmaatregelen. Daarnaast kan het een beter (kwantitatief) inzicht geven in de aard en omvang van beveiligingsincidenten.

Motivering

Een effectieve en efficiënte wijze van informatieuitwisseling is er op gericht het effect van optredende informatiebeveiligingsincidenten, zoals virussen en computerinbraken, te beperken. Op deze manier kan worden omgegaan met de dynamiek van bedreigingen. Er wordt gezorgd voor een centraal punt waar beveiligingsincidenten kunnen worden gerapporteerd. Tevens kan dit centraal punt als filter dienen door alleen serieuze incidenten door te laten, waardoor de nu vaak optredende lawine aan niet gevalideerde, onbetrouwbare incidentmeldingen beter kan worden gekanaliseerd. Het feit dat aard en omvang van de beveiligingsincidenten in Nederland niet structureel wordt bijgehouden, leidt er bovendien toe dat er geen objectief beeld verkregen kan worden van de betrouwbaarheid van het (Nederlandse deel) van internet. Een kwalitatieve inschatting is het hoogst haalbare gebleken, zoals verwoord in hoofdstuk 4 van deze nota.

Uitvoering

Door BZK wordt een computer emergency response team (CERT) voor de rijksoverheid opgezet. Samen met V&W wordt onderzocht of en hoe vanuit een maatschappelijke verantwoordelijkheid deze CERT ook een waarschuwingsfunctie voor andere sectoren en burgers in Nederland kan vervullen. Randvoorwaarde voor succes is samenwerking en afspraken met buitenlandse CERT's, die veelal (semi)-overheidsorganisaties zijn, en de in Nederland bestaande private CERT's zoals die van KPN en Surfnet, die zich beperken tot waarschuwingen aan bij hun aangesloten gebruikers. Het exacte takenpakket van zo'n CERT moet nog worden ingevuld en tevens wordt nog bekeken hoe dat de CERT het beste organisatorisch kan worden vormgegeven. Taken waaraan gedacht wordt, zijn:
- het ontvangen, analyseren en classificeren van (desgewenst

anonieme) meldingen omtrent bestaande en verwachte dreigingen. Meldingen kunnen o.a. komen van incident response teams van branches, multinationals, internetproviders, gekwalificeerde (inter)nationale beveiligingsbedrijven, vanuit inlichtingen- en veiligheidsdiensten en nationale coördinatiecentra andere landen;
- het delen en verspreiden van informatie aan de bovengenoemde incident response teams zodat tijdig tegenmaatregelen genomen kunnen worden;
- alarmeren;
- coördinatie van de repressie van grootschaliger incidenten – opschalen van de coördinatiecapaciteit naar behoefte;
- het opstellen en up-to-date houden van draaiboeken en deze middels oefeningen geregeld testen;
- het bijhouden van statistieken opdat een beter beeld ontstaat van de aard en omvang van de kwetsbaarheid van internet.

Belang van branche/sector informatieuitwisselingscentra
Het is voor branches/sectoren van belang eigen informatieuitwisselingscentra op te richten en aangesloten te zijn op het collaboratieve netwerk opdat binnenkomende informatie effectief en efficiënt kan worden doorgegeven aan de aangesloten bedrijven en andere gebruikers. Daarnaast spelen zij ook een rol bij het doorgeven van gesignaleerde dreigingen aan het netwerk. Er is dus sprake van tweerichtingsverkeer. Het inrichten van dit soort sectorale/branchegewijze informatieuitwisselingscentra zal door de markt zelf moeten worden opgepakt.

7.1.7 Integriteit van informatie

Doel

Het bevorderen van de integriteit van informatie die elektronisch wordt gecommuniceerd of is opgeslagen. Onder integriteit van informatie wordt verstaan dat er zekerheid is omtrent de identiteit van de persoon of organisatie waar de informatie van afkomstig is en of deze informatie correct (niet gewijzigd of aangevuld) is. Dit kan bereikt worden door te zorgen voor een goed aanbod van Trusted Third Party (TTP) dienstverlening.

Motivering

Zoals in hoofdstuk 2 is aangegeven is integriteit één van de aspecten van informatiebeveiliging. Een Trusted Third Party (TTP) verleent diensten waarmee de integriteit van elektronische informatie kan worden gewaarborgd. Een TTP kan daarom gekarakteriseerd worden als een kritische internetcomponent.

Uitvoering

Het kabinet heeft reeds een TTP-beleid opgesteld dat is verwoord in de *Beleidsnotitie Nationaal TTP-project*[24]. Deze nota is in 1999 naar de Tweede Kamer verzonden. Daarnaast is in januari 2000 een Europese richtlijn[25] over elektronische handtekeningen gepubliceerd. In zowel de beleidsnotitie als de richtlijn zijn (gelijkwaardige) eisen opgesteld waaraan een betrouwbare TTP moet voldoen. Achterliggende gedachte is dat een TTP betrouwbaarheidsdiensten levert en dus zelf ook uiterst betrouwbaar moet zijn. Deze eisen hebben betrekking op organisatie, bedrijfsprocessen en techniek.

Eén van de eisen is gericht op de beschikbaarheid van TTP-dienstverlening om te voorkomen dat deze kritische internetcomponent uitvalt. In de beleidsnotitie is gesteld dat er een vrijwillig certificatieschema zal worden

opgesteld aan de hand waarvan getoetst kan worden of TTP's voldoen aan de gestelde eisen. Dit schema zal medio 2001 operationeel zijn.

Daarnaast stelt de richtlijn verplicht dat een lidstaat een toezichtsysteem opzet voor bepaalde, in de richtlijn genoemde, TTP's. Er is een wetsvoorstel waarbij OPTA als toezichthouder wordt aangewezen. Het verschil tussen certificatieschema en toezichthouder is dat het certificatieschema *vooraf* toetst of TTP's voldoen aan de eisen en daar een bewijs in de vorm van een certificaat voor afgeeft. De toezichthouder daarentegen toetst niet vooraf maar kan, bij op enig moment geconstateerde non-conformiteit aan de eisen, de TTP dwingen hieraan te voldoen of anders te stoppen met haar (als betrouwbaar gekwalificeerde) dienstverlening.

De overheid heeft, als grote marktpartij, een rol als *launching customer* voor TTP-dienstverleners. Binnen de overheid, onder regie van BZK, loopt een project *PKI-overheid*[26] dat deze rol invult.

In 2003 is een evaluatie voorzien van het TTP-beleid. Daarin zal worden gekeken naar de tot stand gekomen kwaliteit en vraag naar TTP-dienstverlening.

7.1.8 Cybercrime

Doel

Het beter beschermen van burger, bedrijfsleven en overheid door het bevorderen dat computercriminaliteit daadwerkelijk bestreden kan worden binnen een internationaal wettelijk en uitvoerbaar kader met de daarvoor benodigde middelen (kennis, capaciteit).

Motivering

Informatie- en Communicatie Techniek (ICT) maakt het mogelijk dat mensen gelijktijdig gebruik maken van ICT in netwerken en zodoende on-line met elkaar verbonden zijn. Een voorbeeld hiervan is het internet. Naast positieve effecten, zoals de ontwikkeling van e-commerce, zijn er echter ook schaduwkanten.

Ten eerste ontstaan er delicten die voorheen niet (op grote schaal) mogelijk waren: het aantasten van het goed functioneren van de informatiesystemen door het verspreiden van softwareprogramma's met een vernietigende werking (bijvoorbeeld virussen), het kraken van computersystemen ofbestanden (hacken), het plegen van denial-of-service attacks (het sturen van een zo groot aantal verzoeken om een website te openen dat het netwerk verstopt raakt en bezwijkt). Ten tweede faciliteert ICT bestaande delicten, bijvoorbeeld het plegen van vermogensdelicten (zoals creditcardfraude) en uitingsdelicten (zoals kinderpornografie en discriminatie).

Uitvoering

Alle opsporingsprocessen ondergaan momenteel de invloed van ICT-ontwikkelingen. Er komen steeds meer digitale sporen. Derhalve komt er steeds meer werk voor digitaal opsporingspecialisten. Digitale opsporing kan echter niet alleen op hen neerkomen. Politieambtenaren moeten tijdens hun gewone werkzaamheden kansen voor digitale opsporing kunnen herkennen en digitale sporen kunnen veiligstellen. De kennis bij de basiszorg van politie en bij de recherche is echter nog onvoldoende om op eigen kracht digitale sporen te kunnen ontdekken, interpreteren en veilig stellen.

De belangrijkste maatregel is het vergroten van de kennis van digitaal opsporen, het ontwikkelen van digitale opsporingsmiddelen en indien nodig het uitbreiden van de opsporingsbevoegdheden. Dit betekent niet dat elke opsporingsambtenaar in staat moet zijn tot een opsporingsonderzoek op het internet, maar wel dat elke opsporingsambtenaar zich bewust is van de mogelijke digitale misdrijven en kansen voor de opsporing.

Uitbreiding van de bureaus digitale expertise (BDE) bij de politie is noodzakelijk. Deze uitbreiding is gezien de concurrentie op de personeelsmarkt voor gekwalificeerd IT-personeel echter niet te realiseren zonder aanpassingen in het personeelsbeleid, met name op het gebied van salariëring en werving.

Ook op internationaal niveau wordt aandacht besteed aan de bestrijding van cybercrime. De Raad van Europa bereidt het verdrag «Crime in cyberspace» voor. Het verdrag beoogt een intensivering van de internationale samenwerking stelt en enkele materiële gedragingen (zoals het verspreiden van kinderporno) strafbaar.

In de Mededeling *De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden* van de Europese Commissie, worden enkele voorstellen gedaan om cybercrime effectiever te kunnen bestrijden. Het voorstel borduurt voort op het verdrag «Crime in Cyberspace». Voor de inhoud van het voorstel wordt verwezen naar hoofdstuk 5, waar hier reeds op is ingegaan.

In de nota *Criminaliteitsbeheersing* van de minister van Justitie, die dit jaar aan de Tweede Kamer wordt aangeboden, wordt ondermeer op de uitwerking van deze activiteit ingegaan.

7.2 Afstemming

Vanwege de vele partijen die betrokken zijn bij het vormgeven en implementeren van genoemde maatregelen, en door het internationale karakter van internet, is enigerlei wijze van (inter)nationale afstemming vereist.

7.2.1 Nationale afstemming

Er is meerdere malen aangegeven dat activiteiten in een nauwe publiek-private samenwerking moeten plaatsvinden. Om dit proces vorm te geven wordt een nationaal overleg voorzien waaraan de betrokken departementen en private partijen deelnemen. In dit overleg worden aan elkaar gerelateerde onderwerpen in hun samenhang behandeld. Het vervult daarmee een belangrijke schakel in de informatie-uitwisseling tussen betrokkenen. Uitwerking van de actielijnen kan nader vorm worden gegeven in (kleinere) samenwerkingsverbanden die rapporteren aan dit nationale overleg.

7.2.2 Internationale afstemming

Om recht te doen aan de grensoverschrijdende dimensie van de problematiek en om interactie te behouden tussen de nationale beleidslijn en de internationale ontwikkelingen, worden bilaterale contacten onderhouden en wordt deelgenomen aan initiatieven binnen Europese Commissie en OESO.

Een aspect dat met name internationaal aangekaart moet worden om groot effect te sorteren, is om de beschikbaarheid van producten op de markt te vergroten waarmee minder veiligheidsrisico's worden gelopen.

Vermindering van dit soort risico's kan bijvoorbeeld bereikt worden door te stimuleren dat producten worden geleverd waarin de beveiligingsopties standaard «aan» staan. Nationaal hebben leveranciers van producten, en brancheorganisaties zoals FENIT, uiteraard een eigen verantwoordelijkheid om dit soort producten op de markt te brengen.

BIJLAGE A

Referenties

[1] Ministeries van OCW, FIN, V&W, JUS, BZK en EZ, De Digitale Delta, Tweede Kamer, vergaderjaar 1998–1999, 26 643, nr. 1

[2] Nederlands Normalisatie Instituut (NNI), ministerie van Verkeer en Waterstaat, ministerie van Economische Zaken, Code voor Informatiebeveiliging, een leidraad voor Beleid en Implementatie, 2000

[3] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, Publicatieblad van de Europese Gemeenschappen L 13, 19 januari 2000

[4] Europese Raad van Stockholm, Conclusies van het voorzitterschap, Stockholm (24–03–2001) – Nr: 100/01, http://ue.eu.int/Newsroom/LoadDoc.cfm?MAX=1&DOC=!!!&BID=76&DID =65 821&GRP=33 14&LANG=3

[5] Ministerie van Verkeer en Waterstaat, Netwerken in de Delta, Tweede Kamer, vergaderjaar 1999–2000, 26 643, nr. 6

[6] Stratix / TNO, Kwetsbaarheid internet, Samen werken voor veilig internet verkeer, januari 2001

[7] Ministerie van Justitie, Wetgeving voor de elektronische snelweg, Tweede Kamer, vergaderjaar 1997–1998, 25 880, nrs 1–2

[8] Stichting Maatschappij en Onderneming, Informatieoorlog, Over de schaduwkanten van de informatiemaatschappij, december 2000

[9] Ministerie van Verkeer en Waterstaat, Netwerken in cijfers, Trendrapportage over ICT-infrastructuren 2000, mei 200

[10] Volume Amsterdam Internet Exchange Customers http://www.ams-ix.net/AMS-IX-klanten.cumu.html

[11] Computer Security Institute (2000) Computer Security Issues & Trends Vol VI No 1, Spring 2000 http://www.gosci.com

[12] Albert, R., Jeong, H. & Barabási, A.L., Error and attack tolerance of complex networks,Nature 27, juli 2000

[13] NU.NL, Werkgevers schatten schade virus op f 50 miljoen, http://nu.nl/document?n=11 390

[14] http://news.cnet.com/news/0–1003–200– 3314 544.html

[15] The White House, National Plan for Information Systems Protection, Defending America's Cyberspace, 2000

[16] http://www.sicherheit-im-Internet.de

[17] http://www.bipt.be/Pages/DUTCH/LIBRAI RI/Communic/virus.htm

[18] e-Europa 2002, Een informatiemaatschappij voor iedereen, Actieplan opgesteld door de Raad en de Europese Commissie voor de Europese Raad van Feira, 19–20 juni 200

[19] De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden, Mededeling van de Commissie aan de Raad, het Europees Parkement, het Economisch en Sociaal Comité en het Comité van de Regio's, COM (2000) 890

[20] OECD, Cryptography Policy Guidelines, 27 March 1997

[21] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Plan van aanpak virusbestrijding en informatiebeveiliging overheid, Tweede Kamer, vergaderjaar 2000–2001, 26 643, nr. 26

[22] Nederlands Normalisatie Instituut (NNI), ministerie van Verkeer en Waterstaat, ministerie van Economische Zaken, Code voor Informatiebeveiliging, een leidraad voor Beleid en Implementatie, 2000

[23] Een netwerk van actoren die vrijwillig samenwerken om beveiligingsincidenten te voorkomen, en daar waar dat niet mogelijk is, de gevolgen van dergelijke incidenten te beperken.

[24] Ministerie van Economische Zaken en Ministerie van Verkeer en Waterstaat, Beleidsnotitie Nationaal TTP-project, Tweede Kamer der Staten-Generaal, vergaderjaar 1998–1999, 26 581, nr.1

[25] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, Publicatieblad van de Europese Gemeenschappen L 13, 19 januari 2000

[26] www.pkioverheid.nl

BIJLAGE B

Lijst deelnemers workshops met deskundigen

Deelnemers workshops KWINT

1. Aanraad, Arjan	Ministerie van Defensie
2. Buys, Martin	Ministerie van Economische Zaken
3. Dijken, Pieter van	Shell Services International
4. Dulm, Maarten van	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
5. Eisner, Fred	Nederlandse Vereniging van Internetproviders (NLIP)
6. Graaf, Paul de	VNO-NCW
7. Haccou, Alexander	Vereniging ICT Nederland (KPN)
8. Hoedt, Celeste ten	BTG
9. Jansen, Ton	Safe Internet Foundation
10. Kamper, Tim de	Technische Universiteit Delft
11. Katus, Sergej	FENIT
12. Koole, Wibo	Consumentenbond
13. Kuiper, Renato	FENIT (CMG)
14. Leemans, Hans	Nederlandse Vereniging van Internetproviders (NLIP)
15. Meijkamp, Rens	Infodrome
16. Nasrullah, Mohammed	Ministerie van Verkeer en Waterstaat
17. Oosterhout, Arno	Ministerie van Justitie
18. Schuurman, Jacques	SURFNET/CERT-NL
19. Sonnemans, Ton	Nederlandse Vereniging van Banken
20. Temmerman, Danny de	Europese Commissie – DG Informatiemaatschappij
21. Timmermans, Jan	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
22. Vissers, Wim	FENIT (ADP Nederland B.V.)
23. Wehrmeijer, Job	VECAI

Verklarende lijst van termen

Amsterdam Internet eXchange (AMS-IX) is een plaats waar de netwerken van bijna alle internet providers in Nederland op aangesloten zijn en zowel nationaal als internationaal verkeer wordt uitgewisseld. De AMS-IX is het grootste internetknooppunt in Nederland.

Application Service Provider (ASP) is een aanbieder van applicaties, die op een centrale machine draaien, waar klanten op afstand gebruik van kunnen maken.

Cascade effect is het overslaan van uitval of verstoringen van een systeem op andere systemen die er aan gekoppeld zijn.

Commercial-off-the-shelf (COTS) software is software die ontwikkeld is voor een hele markt in plaats van voor individuele klanten.

Computer Emergency Response Team (CERT) is een team in dienst van een eigenaar van een informatiesysteem. Dergelijke teams assisteren bij het oplossen van beveiligingsinbreuken. Sommige grotere CERT's (als CERT-NL van SURFnet) hebben ook een belangrijke voorlichtingsfunctie en brengen zogenaamde *advisories* uit met waarschuwingen over recentelijk ontdekte softwaregaten en methoden waarop de problemen opgelost kunnen worden.

Computer Emergency Response Team Coordination Center (CERT/CC) is een belangrijk internet-beveiligingscentrum. Het is gehuisvest bij het Software Engineering Institute; een door de Amerikaanse overheid (ministerie van Defensie) gefinancierd onderzoeks- en ontwikkelingscentrum dat beheerd wordt door de Carnegie Mellon University in de VS. Aanvankelijk richtte CERT/CC zich bijna uitsluitend op het assisteren bij het oplossen van beveiligingsinbreuken. Later bestond het werk steeds meer uit het helpen opstarten van andere incident response teams, het coördineren van de inspanningen van teams bij de response op grootschalige incidenten, het opleiden van beveiligingsspecialisten, het onderzoeken en voorkomen van beveiligingslekken en het verbeteren van de «survivability» van grootschalige netwerken. Zie http://www.cert.org

Cross-connects zijn distributiepanelen waar transmissielijnen worden doorgelust.

Cyberterrorisme en -vandalisme. Cyberterrorisme is het plegen van gerichte aanvallen middels informatie-infrastructuren op (computersystemen van) vitale sectoren en organisaties als elektriciteitsbedrijven, luchthavens, banken, alarmcentrales en voedselfabrieken. Cybervandalisme is een mildere vorm van ICT-misbruik, zoals het onbereikbaar maken of inhoudelijk veranderen van internetpagina's.

Denial of Service (DoS). Het beperken of frustreren van de werking van een systeem, applicatie of netwerk in enige vorm.

Distributed Denial of Service (DoS). Het beperken of frustreren van de werking van één of meer netwerken, systemen, of toepassingen daarop door misbruik te maken van een groot aantal clientcomputers die door een «controller» er toe aangezet worden om massaal en gelijktijdig het aan te vallen netwerk, systeem of toepassing te benaderen.

Domain Name Server (DNS). Het internet kan zijn taken niet vervullen zonder ondersteunende diensten. Zo vindt de koppeling tussen het op

internet gebruikelijke IP-adres (een nummer) en de voor de gebruiker bekende naamgeving plaats middels een hiërarchisch georganiseerde dienst genaamd de Domain Name Server (DNS). De functionaliteit van deze dienst kan gezien worden als een telefoonboek. Diensten als het www, bestandsoverdracht en email zijn sterk afhankelijk van het correct functioneren van deze voorziening.

File transfer is het uitwisselen van bestanden.

Gaming is het spelen van computerspelletjes via internet.

Information Sharing Analysis Center (ISAC) is een centrum dat is opgericht door de private sector om informatie over beveiligingsincidenten binnen de sector te verzamelen, te analyseren en te verspreiden. Deze centra kunnen ook informatie met het NIPC uit de VS uitwisselen (zie paragraaf 5.1). In tegenstelling tot CERT's assisteren deze centra niet bij het oplossen van individuele beveiligingsinbreuken, maar fungeren zij slechts als informatieuitwisselingspunten over incidenten.

Internet Service Provider (ISP) is een organisatie die haar klanten toegang tot internet aanbiedt. De ISP onderhoudt hiertoe een of meer POP's, toegangspunten tot internet voor abonnees van de ISP. Naast het verlenen van toegang bieden veel ISP's tegenwoordig ook andere diensten aan. Voorbeelden zijn nieuwsdiensten, transactieoplossingen, entertainment-diensten, etc.

Kwetsbaarheid van de informatievoorziening is «de invloed van het manifest worden van bedreigingen op het functioneren van een informatiesysteem of een verantwoordelijkheidsgebied».

Kwetsbaarheid van de samenleving wordt in het rapport «Stroomloos» gedefinieerd als «de gevoeligheid van het maatschappelijk functioneren voor het uitvallen van bepaalde functies». De maatschappelijke veerkracht is hieraan gerelateerd: «verlaging van het behoeftepatroon in calamiteitensituaties en mogelijkheden om de normale situatie te herstellen».

Root server is een server op het hoogste niveau van het hiërarchische Domain Name System (zie DNS) en vormt derhalve een essentiële functie in internet's «adresboek».

Single Point of Failure is een enkelvoudig onderdeel van een systeem dat bij uitval de werking van het gehele systeem aantast.

Trusted Third Party verleent diensten waarmee de integriteit en/of vertrouwelijkheid van elektronische communicatie kan worden gewaarborgd. Zij speelt ook een rol bij het *on-line* valideren van elektronische handtekeningen.

Virtual communities zijn gemeenschappen van mensen die middels internet met elkaar in contact kunnen treden om informatie over wederzijdse interesses uit te wisselen.

Webbrowsing is het rondkijken (of surfen) op het world wide web.

World Wide Web (WWW). Het world wide web is evenals het «surfen» daarop inmiddels een ingeburgerd begrip. Protocol-technisch is de belangrijkste dienst die hieraan ten grondslag ligt het hypertext transfer protocol (http), dat zorg draagt voor het transport en het raadplegen van de webpagina's. In de loop der jaren is de functionaliteit van het web

uitgebreid met dynamische inhoud en uitgebreidere grafische opmaak (Java, ActiveX, flash etc.), dataobject-georiënteerde presentatie en uitwisseling (XML).