COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 6.6.2001
COM(2001)298 definitief

MEDEDELING VAN DE COMMISSIE AAN DE RAAD, HET EUROPEES PARLEMENT, HET ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak

MEDEDELING VAN DE COMMISSIE AAN DE RAAD, HET EUROPEES PARLEMENT, HET ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak

SAMENVATTING

I.

Veiligheid krijgt een steeds hogere prioriteit omdat communicatie en informatie sleutelfactoren voor de economische en maatschappelijke ontwikkeling zijn geworden. Via netwerken en informatiesystemen worden nu diensten geleverd en gegevens overgedragen op een schaal die tot voor enkele jaren nog voor onmogelijk werd gehouden. De beschikbaarheid is van kritiek belang voor andere infrastructuursystemen, zoals de drinkwater- en elektriciteitsvoorziening. Nu iedereen – bedrijfsleven, particulieren en overheden – gebruik wil maken van de mogelijkheden van communicatienetwerken, is de veiligheid van deze systemen een randvoorwaarde voor verdere groei geworden.

Tegen deze achtergrond is op de Europese Raad van Stockholm van 23 en 24 maart 2001 geconcludeerd dat *de Raad samen met de Commissie een allesomvattende strategie zal ontwikkelen voor de veiligheid van elektronische netwerken, inclusief praktische uitvoeringsmaatregelen. Een voorstel hiervoor dient nog vóór de Europese Raad van Göteborg te worden ingediend.* Deze mededeling moet worden gezien als het antwoord van de Europese Commissie op dit verzoek.

II.

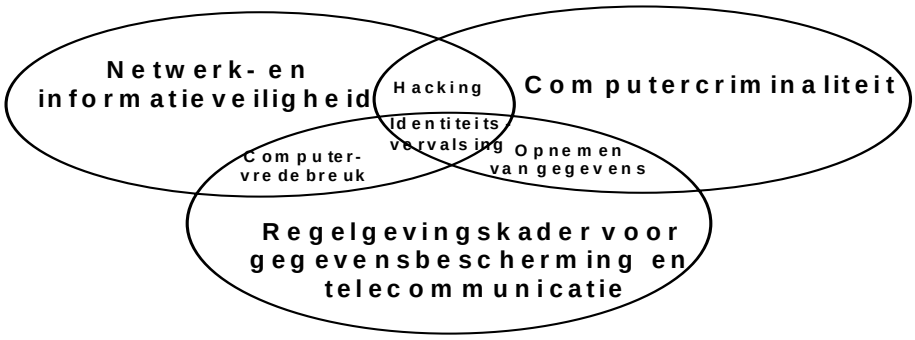
Juist nu de veiligheidsproblematiek voor de beleidsmakers een belangrijke uitdaging is geworden, blijkt het steeds moeilijker een adequaat beleid op dit punt te ontwikkelen. Communicatiediensten worden niet langer aangeboden door het staatstelecommunicatiebedrijf, maar, op basis van concurrentie en steeds meer op Europese en wereldwijde schaal, door een groot aantal particuliere exploitanten en dienstverleners. Netwerken convergeren: zij kunnen dezelfde diensten verlenen, worden steeds vaker onderling gekoppeld en maken deels gebruik van dezelfde infrastructuur.

Om een minimumniveau van veiligheid te garanderen, is er zowel op nationaal als op EU-niveau een omvangrijk corpus van wetgeving vastgesteld dat deel uitmaakt van het regelgevingskader voor telecommunicatie en gegevensbescherming. Deze wettelijke voorschriften moeten op doeltreffende wijze worden toegepast in een door grote veranderingen gekenmerkte omgeving. Zij dienen in de toekomst bovendien te evolueren, hetgeen nu al duidelijk wordt aan de hand van het voorstel voor een nieuw regelgevingskader voor elektronische communicatie of de toekomstige voorstellen ten aanzien van computercriminaliteit. Daarom moeten de beleidsmakers inzicht verwerven in de onderliggende veiligheidskwesties en hun rol bij de verhoging van de veiligheid.

Netwerk- en informatieveiligheid kan worden gezien als een goed dat op de markt wordt gekocht en verkocht en waarover afspraken worden gemaakt in de contractuele overeenkomsten tussen partijen. Meestal wordt er impliciet van uitgegaan dat er dankzij het prijsmechanisme een evenwicht zal ontstaan tussen de kosten van beveiliging en de specifieke

behoefte aan veiligheid. Niettemin is een groot aantal veiligheidsrisico's nog niet opgelost of bereiken de oplossingen daarvoor als gevolg van tekortkomingen in de marktwerking slechts langzaam de markt. **Met specifieke beleidsmaatregelen die deze tekortkomingen moeten ondervangen, kan de marktwerking en tegelijkertijd het functioneren van het regelgevingskader worden verbeterd.** Dergelijke maatregelen moeten deel uitmaken van een Europese aanpak teneinde ervoor te zorgen dat de interne markt voor dergelijke diensten gegarandeerd is, dat van gemeenschappelijk oplossingen kan worden geprofiteerd en dat effectief optreden op wereldwijd niveau mogelijk is.

De beleidsvoorstellen ten aanzien van netwerk- en informatieveiligheid dienen te worden gezien niet alleen tegen de achtergrond van de huidige wetgeving ten aanzien van telecommunicatie en gegevensbescherming. Met een beleid ten aanzien van netwerk- en informatieveiligheid wordt de ontbrekende schakel van dit beleidskader geleverd. Onderstaande afbeelding toont deze drie beleidsterreinen en illustreert aan de hand van enkele voorbeelden hoe deze met elkaar zijn verweven:



III.

Netwerk- en informatieveiligheid kan worden opgevat als de bestandheid van een netwerk of informatiesysteem met een gegeven mate van zekerheid tegen toevallige gebeurtenissen of opzettelijke handelingen waardoor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of overgedragen gegevens en de diensten die door of via het netwerk worden aangeboden, in gevaar worden gebracht. Deze veiligheidsrisico's kunnen als volgt worden ingedeeld:

- Elektronische communicatie kan worden onderschept en de gegevens kunnen worden gekopieerd of gewijzigd. Hierdoor kan schade ontstaan, hetzij door de inbreuk op de privacy van individuen of door misbruik te maken van de onderschepte gegevens.

- Ongeoorloofde toegang tot een computer of een computernetwerk wordt gewoonlijk verworven met de bedoeling om gegevens te kopiëren, wijzigen of vernietigen.

- Ontwrichtende aanvallen op het internet zijn gemeengoed worden en in de toekomst kan ook het telefoonnet kwetsbaarder worden.

- Kwaadaardige software, zoals virussen, kan computers onbruikbaar maken of gegevens vernietigen of wijzigen. Sommige recente virusaanvallen zijn uiterst destructief en kostbaar gebleken.

- Vervalsing van de identiteit van personen of entiteiten kan tot aanzienlijke schade leiden. Zo kunnen klanten kwaadaardige software van een betrouwbaar lijkende website downloaden, kunnen contractonderhandelingen worden afgebroken, en kunnen vertrouwelijke gegevens naar de verkeerde personen worden gestuurd.

- Een groot aantal veiligheidsincidenten is het gevolg van onvoorziene en onbedoelde gebeurtenissen zoals natuurrampen (overstromingen, stormen, aardbevingen), hardware- en softwarefouten, en menselijk falen.

IV.

De voorgestelde maatregelen:

- **Bewustmaking:** Er moet een op het publiek gerichte voorlichtings- en scholingscampagne worden gestart en de toepassing van praktijkcodes dient te worden bevorderd.

- **Een Europees waarschuwings- en informatiesysteem:** De lidstaten moeten hun computercalamiteitenteams (CERT's) versterken en de onderlinge coördinatie daarvan verbeteren. De Commissie zal samen met de lidstaten onderzoeken hoe de inzameling van gegevens, de analyse en de planning van preventieve maatregelen tegen de huidige en nieuwe veiligheidsrisico's het best kunnen worden georganiseerd.

- **Technologische ondersteuning:** Steun voor onderzoek en ontwikkeling op het gebied van veiligheid dient een hoofdthema van het zesde kaderprogramma te worden en te worden ingebed in een bredere strategie ter verhoging van de netwerk- en informatieveiligheid.

- **Steun voor marktgeoriënteerde standaardiserings- en certificeringswerkzaamheden:** De Europese normalisatie-instellingen wordt verzocht hun activiteiten op het gebied van interoperabiliteit in een stroomversnelling te brengen; de Commissie zal het gebruik van elektronische handtekeningen en de verdere ontwikkeling van IPv6 en IPSec blijven ondersteunen, en zal de behoefte aan een wetgevingsinitiatief op het gebied van de wederzijdse erkenning van certificaten peilen; de lidstaten dienen alle relevante veiligheidsnormen te evalueren.

- **Regelgevingskader**: De Commissie zal een inventarisatie maken van nationale maatregelen die in overeenstemming met het relevante Gemeenschapsrecht zijn getroffen. De lidstaten dienen het vrij verkeer van encryptieproducten te ondersteunen. De Commissie zal met wetgevingsvoorstellen ten aanzien van computercriminaliteit komen.

- **Veiligheid van toepassingen bij de overheid:** De lidstaten dienen in hun systemen voor elektronische overheid en elektronische aanbestedingen een doeltreffende en interoperabele veiligheidsoplossing in te bouwen. De lidstaten dienen een elektronische handtekening mogelijk te maken wanneer zij openbare diensten aanbieden. De Commissie zal de veiligheidseisen die zij aan haar informatie- en communicatiesystemen stelt verhogen.

- **Internationale samenwerking:** De Commissie zal de dialoog over netwerk- en informatieveiligheid met internationale organisaties en partners intensiveren.

V.

De volgende fase is dat de lidstaten en het Europees Parlement zich over dit raamwerk en de voorgestelde maatregelen gaan buigen. De Europese Raad van Göteborg van 15/16 juni kan wellicht de richting aangeven waarin dit beleid zich in de toekomst moet gaan ontwikkelen.

De Commissie stelt voor een uitvoerige discussie met de industrie, de gebruikers en de voor gegevensbescherming verantwoordelijke instanties te voeren over de praktische bijzonderheden betreffende de tenuitvoerlegging van de voorgestelde maatregelen. Reacties kunnen tot eind augustus 2001 worden toegezonden aan eeurope@cec.eu.int. Daarom dient deze mededeling te worden opgevat als een uitnodiging aan het adres van de belanghebbenden om reacties in te dienen zodat een definitieve en concrete reeks van maatregelen kan worden vastgesteld. Dit zou kunnen gebeuren in de vorm van een "roadmap", die voor eind 2001 klaar zou moeten zijn.

***

Netwerk- en informatieveiligheid:

Voorstel voor een Europese beleidsaanpak

Inhoud

1. Inleiding

De bezorgdheid over de veiligheid van elektronische netwerken en informatiesystemen is toegenomen vanwege de snelle groei van het aantal netwerkgebruikers en de omvang van hun transacties. De veiligheid is nu op het kritieke punt gekomen waarop deze een randvoorwaarde wordt voor de groei van het elektronisch handelsverkeer en het functioneren van de gehele economie. Diverse factoren hebben er samen toe geleid dat de veiligheid van informatie en communicatie boven aan de politieke agenda van de EU is komen te staan:

- De overheden zien inmiddels in dat de economie en de burgers zijn aangewezen op een goede werking van de communicatienetwerken met als gevolg dat zij hun beveiligingsvoorzieningen zijn gaan herzien.

- Het internet heeft voor wereldwijde connectiviteit gezorgd door miljoenen netwerken van uiteenlopende omvang, honderden miljoenen afzonderlijke PC's, alsmede een groeiend aantal andere apparaten zoals mobiele telefoons met elkaar te verbinden. Hierdoor zijn de kosten die moeten worden gemaakt om op afstand ongeoorloofde toegang te krijgen tot waardevolle economische informatie sterk gedaald.

- Via internet heeft een aantal virussen zich op grote schaal kunnen verspreiden en aanzienlijke schade kunnen aanrichten door informatie te vernietigen en de toegang tot netwerken onmogelijk te maken. Dergelijke veiligheidsproblemen blijven niet beperkt tot afzonderlijke landen, maar verspreiden zich snel over alle lidstaten.

- Op de Europese Raad van Lissabon en die van Santa Maria da Feira is de rol van het internet als gangmaker voor de productiviteit van de EU-economieën met de lancering van het actieplan *e*Europe 2002 erkend.

Tegen deze achtergrond is op de Europese Raad van Stockholm van 23 en 24 maart 2001 geconcludeerd dat *de Raad samen met de Commissie een allesomvattende strategie zal ontwikkelen voor de veiligheid van elektronische netwerken, inclusief praktische uitvoeringsmaatregelen. Een voorstel hiervoor dient nog vóór de Europese Raad van Göteborg te worden ingediend.* Deze mededeling moet worden gezien als het antwoord van de Europese Commissie op dit verzoek.

Een veranderende omgeving

Juist nu de veiligheidsproblematiek voor de beleidsmakers een belangrijke uitdaging is geworden, blijkt het steeds moeilijker een adequaat beleid op dit punt te ontwikkelen. Nog maar enkele jaren geleden was netwerkveiligheid vooral een zaak voor staatsmonopolies, die gespecialiseerde diensten aanboden op basis van openbare netwerken, met name het telefoonnet. Computersystemen werden alleen in grote organisaties beveiligd, voornamelijk door middel van toegangscontrole. Het formuleren van een veiligheidsbeleid was een relatief eenvoudige taak. In deze situatie is grote verandering gekomen als gevolg van de zeer diverse ontwikkelingen in de bredere context van de markt, waaronder de liberalisering, de convergentie en de mondialisering:

Eigendom en beheer van netwerken zijn nu meestal in particuliere handen. Communicatiediensten worden inmiddels op basis van concurrentie aangeboden, waarbij de beveiliging als een onderdeel van het aangeboden product wordt gezien. Niettemin is een

groot deel van de klanten zich nog steeds niet bewust van de veiligheidsrisico's die zij lopen bij het tot stand brengen van netwerkverbindingen, waardoor zij hun beslissingen op onvolledige informatie baseren.

Netwerken en informatiesystemen convergeren. Zij worden steeds vaker met elkaar verbonden en zij bieden hetzelfde soort, naadloos op elkaar aansluitende en gepersonaliseerde diensten. Tot op zekere hoogte delen zij ook dezelfde infrastructuur. De eindapparatuur (PC's, mobiele telefoons, enz.) speelt een steeds actievere rol in de netwerkarchitectuur en kan op verschillende netwerken worden aangesloten.

Netwerken zijn internationaal. Een aanzienlijk deel van de communicatie heeft vandaag de dag een grensoverschrijdend karakter of verloopt via derde landen (soms zonder dat de eindgebruiker dit beseft), zodat hiermee bij elke oplossing voor veiligheidsrisico's rekening moet worden gehouden. De meeste netwerken worden opgebouwd met behulp van in de handel verkrijgbare producten van internationale leveranciers. Beveiligingsproducten moeten compatibel zijn met internationale normen.

Politieke relevantie

Deze ontwikkelingen beperken de vrijheid van de overheden om het veiligheidsniveau bij de elektronische communicatie tussen hun burgers en bedrijven voor te schrijven. Maar dit betekent niet dat de rol van de overheid is uitgespeeld. Daarvoor zijn verschillende redenen:

In de eerste plaats **zijn er diverse wettelijke maatregelen van kracht die specifieke implicaties hebben voor de netwerk- en informatieveiligheid**. In het bijzonder is er het Europese regelgevingskader voor telecommunicatie en gegevensbescherming, waarin voorschriften zijn opgenomen die de exploitanten en dienstverleners verplichten het beveiligingsniveau af te stemmen op de betrokken risico's.

In de tweede plaats neemt de ongerustheid over de **nationale veiligheid** toe, aangezien informatiesystemen en communicatienetwerken een kritische factor zijn geworden voor de rest van de infrastructuur (bijv. de water- en elektriciteitsvoorziening) en de overige markten (bijv. de wereldwijde financiële markten).

Ten slotte zijn er redenen waarom de overheden maatregelen moeten treffen tegen **onvolkomenheden van de markt**. De marktprijzen zijn niet altijd een even nauwkeurige afspiegeling van de kosten en baten van investeringen in een betere netwerkbeveiliging en de aanbieders noch de gebruikers dragen altijd de consequenties van hun eigen gedrag. De controle over het netwerk is verdeeld over verschillende spelers en zwakke plekken in het ene systeem kunnen worden gebruikt om een aanval op het andere systeem uit te voeren. De complexiteit van netwerken maakt het de gebruikers moeilijk een goede inschatting van de mogelijke risico's te maken.

Het doel van deze mededeling is daarom aan te geven waar aanvullend of krachtiger ingrijpen van de overheid op Europees niveau of op nationaal niveau noodzakelijk is.

In **hoofdstuk 2** wordt het begrip netwerk- en informatieveiligheid gedefinieerd, worden de belangrijkste veiligheidsrisico's beschreven en worden de huidige oplossingen geëvalueerd. Hiermee wordt gepoogd het nodige inzicht in netwerk- en informatieveiligheid te bieden zodat de voorgestelde beleidsoplossingen kunnen worden begrepen. Het is niet de bedoeling een volledige technische beschrijving van de veiligheidsproblematiek te geven.

In **hoofdstuk 3** wordt een uiteenzetting gegeven van een Europese beleidsaanpak ter verbetering van de netwerk- en informatieveiligheid. Deze is gebaseerd op een analyse van de noodzaak om op de markt verkrijgbare oplossingen aan te vullen met beleidsmaatregelen. Er wordt een lijst gegeven van concrete beleidsmaatregelen, zoals de Europese Raad van Stockholm heeft gevraagd. De beleidsvoorstellen moeten worden gezien als een integrerend deel van het bestaande raamwerk voor elektronische communicatiediensten, gegevensbescherming en – recentelijk ook – computercriminaliteit.

2. Analyse van netwerk- en informatieveiligheidskwesties

2.1. Wat is netwerk- en informatieveiligheid?

Netwerken zijn systemen voor opslag, verwerking en doorgifte van gegevens. Zij omvatten transmissie-elementen (kabels, draadloze verbindingen, satellieten, routers, gateways, switches, enz.) en ondersteunende diensten (domeinnamensysteem met root server, nummeridentificatiedienst, authenticatiedienst, enz.) Gekoppeld aan die netwerken is een steeds gevarieerdere reeks toepassingen (e-mailsoftware, browsers, enz.) en eindapparatuur (telefoontoestellen, hostcomputers, PC's, mobiele telefoons, elektronische agenda's, huishoudelijke apparaten, industriële machines, enz.).

De aan netwerken en informatiesystemen gestelde algemene veiligheidseisen betreffen de volgende met elkaar samenhangende kenmerken:

i) **Beschikbaarheid:** dat wil zeggen dat de gegevens beschikbaar en de diensten operationeel moeten zijn, in weerwil van mogelijke storende gebeurtenissen zoals elektriciteitsstoringen, natuurrampen, ongevallen of aanvallen. Dit is met name essentieel wanneer netwerkstoringen in communicatienetwerken storingen in andere kritische netwerken, zoals het luchtverkeer of de elektriciteitsvoorziening, kunnen veroorzaken.

ii) **Authenticatie:** de bevestiging van de identiteit van entiteiten of gebruikers. Goede authenticatiemethodes zijn nodig voor een groot aantal applicaties en diensten zoals het on-line sluiten van een contract, de controle op de toegang tot bepaalde gegevens en diensten (bijv. bij telewerken), en de authenticatie van websites (bijv. bij internetbankieren). De authenticatie dient ook te voorzien in de mogelijkheid van anonimiteit, aangezien vele diensten niet de identiteit van de gebruiker hoeven te kennen, maar enkele een betrouwbare bevestiging wensen van bepaalde kenmerken (anonieme referenties), zoals de kredietwaardigheid.

iii) **Integriteit:** de zekerheid dat gegevens zijn verzonden, ontvangen of opgeslagen zonder verlies of wijziging van die gegevens. Dit is bijzonder belangrijk bij de authenticatie die plaatsvindt bij het sluiten van contracten of wanneer de nauwkeurigheid van de gegevens essentieel is (medische gegevens, industriële ontwerpen, enz.).

iv) **Vertrouwelijkheid:** de bescherming van overgedragen of opgeslagen gegevens tegen het onderscheppen of aftappen door onbevoegde personen. Vertrouwelijkheid is in het bijzonder nodig bij de overdracht van gevoelige informatie en is een van de voorwaarden voor authenticatie.

Alle gebeurtenissen die een bedreiging voor de veiligheid vormen moeten worden ondervangen, niet enkel die waarbij kwaad opzet in het spel is. Vanuit het standpunt van de gebruiker kunnen veiligheidsrisico's zoals milieurampen of menselijke fouten die de werking

van het netwerk verstoren, even kostbare gevolgen hebben als boos opzet. **Netwerk- en informatieveiligheid kan worden opgevat als de bestandheid van een netwerk of informatiesysteem met een gegeven mate van zekerheid tegen toevallige gebeurtenissen of opzettelijke handelingen waardoor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of overgedragen gegevens en de diensten die door of via het netwerk worden aangeboden, in gevaar worden gebracht.**

2.2. Veiligheidsrisico's

Bedrijven die op een netwerk zijn aangewezen voor de verkoop van hun producten of de organisatie van de bezorging ervan, kunnen door een "denial-of-service"-aanval worden lamgelegd. Persoonlijke en financiële informatie kan worden onderschept en misbruikt. De nationale veiligheid kan in gevaar worden gebracht. Deze voorbeelden geven een indruk van de risico's van een tekortschietende beveiliging. Er wordt onderscheid gemaakt tussen opzettelijke aanvallen (paragrafen 2.2.1 t/m 2.2.5) en onbedoelde gebeurtenissen (paragraaf 2.2.6). In deze paragrafen wordt beoogd een beschrijving te geven van de veiligheidsrisico's zodat in hoofdstuk 3 de grondslag kan worden gelegd voor een beleidskader ter verhoging van de veiligheid.

2.2.1. Onderscheppen van gegevensoverdracht

Elektronische communicatie kan worden onderschept en de gegevens kunnen worden gekopieerd of gewijzigd. Onderscheppen kan op verschillende manieren, onder meer door zich fysieke toegang te verschaffen tot de netwerkverbinding, bijvoorbeeld door het aftappen van draden of het inluisteren op radioverbindingen. De meest gevoelige punten voor het onderscheppen van netwerkverkeer zijn de netwerkbeheers- en –concentratiepunten, zoals routers, gateways, switches en netwerkbeheerservers.

Er dient onderscheid te worden gemaakt tussen het wederrechtelijk of met boos opzet onderscheppen van gegevensoverdracht en wettige onderscheppingsactiviteiten. In alle EU-lidstaten is het onderscheppen van gegevensoverdracht met het oog op de openbare veiligheid in bepaalde gevallen voor beperkte doeleinden toegestaan. Er bestaat een wettelijk kader op basis waarvan de politiediensten rechterlijke toestemming of , in het geval van twee lidstaten, een door een minister persoonlijk gegeven bevel kunnen krijgen op basis waarvan zij gegevensoverdracht mogen onderscheppen.

Mogelijke schade – Wederrechtelijke onderschepping kan schade veroorzaken als inbreuk wordt gemaakt op de privacy van natuurlijke personen of als de onderschepte informatie, zoals wachtwoorden en kredietkaartgegevens, voor commercieel gewin of sabotage wordt misbruikt. Dit risico wordt gezien als een van de grootste belemmeringen voor de popularisering van e-commerce in Europa.

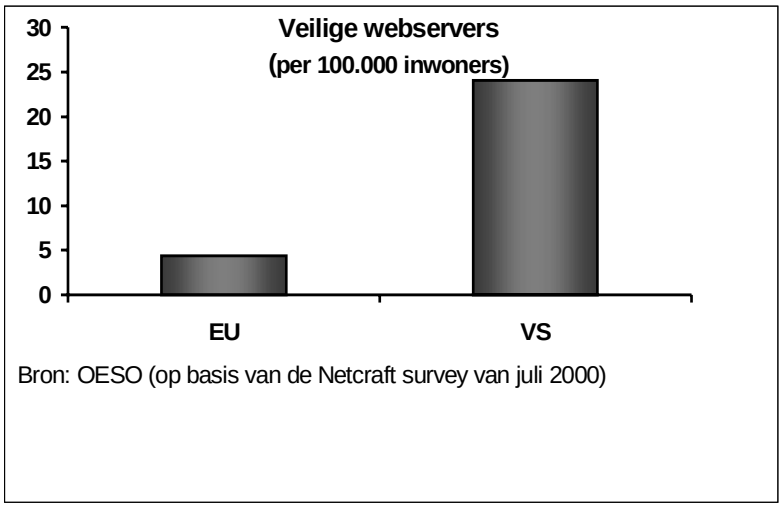
Mogelijke oplossingen – Zowel de **exploitanten** als de **gebruikers** kunnen zich beschermen, de eersten door hun netwerk te beveiligen conform de voorschriften van onder meer Richtlijn 97/66/EG[1], de tweeden door de gegevens die zij over het netwerk verzenden te encrypteren.

Voor de **exploitanten** is de bescherming van het netwerk tegen onderschepping van gegevens een complexe en kostbare aangelegenheid. In het verleden hebben telecommunicatie-exploitanten hun netwerken beveiligd door de fysieke toegang tot de installaties te controleren

[1] Richtlijn inzake gegevensbescherming in de telecommunicatiesector, PB L 24 van 30.1.1998.

en hun personeel richtsnoeren te geven. Het gegevensverkeer werd slechts zelden geëncrypteerd. Bij draadloze systemen moet er extra moeite worden gedaan om ervoor te zorgen dat de radiosignalen voldoende beveiligd zijn. De exploitanten van mobiele communicatiesystemen encrypteren het verkeer tussen de mobiele telefoon en het basisstation. De encryptiesterkte is in de meeste EU-landen minder dan technisch mogelijk is vanwege de eis dat wettige aftapping mogelijk dient te zijn. Om dezelfde redenen kan de encryptie vanuit het basisstation worden in- en uitgeschakeld zonder dat de gebruiker dit merkt.

De **gebruikers** kunnen zelf beslissen hun data- of spraaksignalen te encrypteren, onafhankelijk van de netwerkbeveilingsmaatregelen. Goed geëncrypteerde data kan alleen worden begrepen door de geautoriseerde ontvanger, zelfs wanneer deze wordt onderschept. Encryptiesoftware en –hardware is gemakkelijk verkrijgbaar voor bijna alle vormen van communicatie[2]. Een telefoongesprek of fax kan met speciale producten worden geëncrypteerd. E-mails kunnen worden geëncrypteerd met speciale software of met software die in een tekstverwerker of e-mail cliënt is geïntegreerd. Het probleem voor de gebruiker is dat wanneer hij e-mail-berichten of spraakcommunicatie encrypteert, de ontvanger deze moet kunnen begrijpen. De apparatuur of software moet interoperabel zijn. Voorts dient de ontvanger over de decryptiesleutel te beschikken, hetgeen inhoudt dat er een mechanisme moet bestaan voor de verzending en authenticatie van de sleutel. De kosten van encryptie zijn, zowel in termen van geld als van inspanning, hoog en de gebruikers beschikken vaak niet over voldoende informatie over de veiligheidsrisico's en –voordelen waardoor zij niet altijd een optimaal besluit nemen.



Bron: OESO (op basis van de Netcraft survey van juli 2000)

Een veelgebruikt beveiligingssysteem voor internet is de "Secure Socket Layer" (SSL). SSL encrypteert de communicatie tussen een webserver en een bladerprogramma aan de gebruikerszijde. In het verleden vormden de strenge exportbeperkingen van de VS een belemmerende factor voor de verspreiding van deze technologie, met name voor de krachtigste versie (128 bit). De Amerikaanse uitvoer-bepalingen zijn recentelijk evenwel herzien naar aanleiding van de versoepeling van de voorschriften van de Gemeenschap ten aanzien van de uitvoerbeperkingen voor goederen en technologie voor tweeërlei gebruik[3]. Uit statistische gegevens blijkt dat het aantal veilige webservers in Europa ver achterblijft bij dat in de VS (zie figuur).

De **exploitanten, gebruikers en producenten** worden geconfronteerd met het probleem dat er verschillende normen bestaan die niet interoperabel zijn. Voor de veilige verzending van e-

---

[2] Zie de mededeling van de Commissie "Zorgen voor veiligheid van en vertrouwen in elektronische communicatie" van 8 oktober 1997, COM (1997) 503 def.

[3] Verordening (EG) nr. 1334/2000 van de Raad tot instelling van een communautaire regeling voor controle op de uitvoer van producten en technologie voor tweeërlei gebruik, PB L 159 van 30.6.2000.

mail zijn er twee normen[4] die elkaar naar de kroon steken. De invloed van Europa op dit gebied is gering. Het resultaat is een overdaad van niet-Europese producten waarmee beide normen worden geïmplementeerd zodat de toegankelijkheid ervan voor de Europese gebruiker afhankelijk is van het beleid van de VS ten aanzien van de controle op de uitvoer. Omdat er twijfels bestaan omtrent de mate van veiligheid van een groot deel van deze producten (zie Echelon[5]), overwegen de regeringen van bepaalde EU-landen het gebruik van open source software om het vertrouwen in encryptieproducten te verhogen. Het bedoelde project verkeert evenwel nog in de proeffase[6], het wordt nog niet gecoördineerd en de marktkrachten zijn misschien wel sterker dan de inspanning van een afzonderlijke regering. Deze problematiek kan worden aangepakt door een totale evaluatie te maken van zowel de commerciële als de open source producten.

2.2.2. Ongeoorloofde toegang tot computers en computernetwerken

Ongeoorloofde toegang tot een computer of een computernetwerk wordt gewoonlijk verworven met de bedoeling om gegevens te kopiëren, wijzigen of vernietigen. Door deze handeling, die wordt aangeduid met de term computervredebreuk, bestaan verschillende methodes, waarbij onder meer gebruik kan worden gemaakt van inside informatie, woordenboekmethodes, brute kracht (profiterend van het feit dat mensen voorspelbare wachtwoorden gebruiken), sociale technieken (profiterend van het feit dat mensen de neiging hebben informatie te onthullen aan schijnbaar betrouwbare personen) en het onderscheppen van wachtwoorden. Vaak gebeurt dit van binnen uit de organisatie.

Mogelijke schade – Soms wordt computervredebreuk ingegeven door de intellectuele uitdaging en niet door geldelijk gewin. Maar door dat wat als een hinderlijke activiteit (dikwijls "hacking" genoemd) is begonnen, is de aandacht gevestigd op de kwetsbaarheid van informatienetwerken waardoor mensen met criminele of kwade bedoelingen ertoe zijn aangezet van deze zwakke plekken misbruik te maken. Particulieren hebben recht op bescherming tegen ongeoorloofde toegang tot hun persoonlijke informatie, waaronder hun financiële gegevens, bankrekeningen en medische dossiers. Voor de openbare sector en de industrie lopen de risico's uiteen van economische spionage tot mogelijke wijziging van interne of openbare gegevens, onder meer door de vervalsing van webpagina's.

Mogelijke oplossingen – De meest gangbare methodes om zichzelf tegen ongeoorloofde toegang te beschermen zijn wachtwoorden en firewalls. Deze bieden evenwel slechts beperkte bescherming en dienen te worden aangevuld met andere veiligheidsmaatregelen. Te denken valt bijvoorbeeld aan opsporing van aanvallen, detectie van inbraakpogingen en toegangsbeheer op applicatieniveau (bijv. met behulp van chipkaarten). De doeltreffendheid van deze beschermingsmaatregelen is afhankelijk van de mate waarin hun functionaliteit is afgestemd op de risico's die inherent zijn aan een bepaalde omgeving. Er dient een afweging te worden gemaakt tussen de door de netwerkbeveiliging veroorzaakte hinder en de voordelen van onbelemmerde toegang. Als gevolg van de snelle ontwikkelingen en de voortdurende nieuwe bedreigingen voor netwerken dienen de netwerkbeveiligingsmaatregelen voortdurend door onafhankelijke instanties te worden geëvalueerd. Zolang de gebruikers en aanbieders

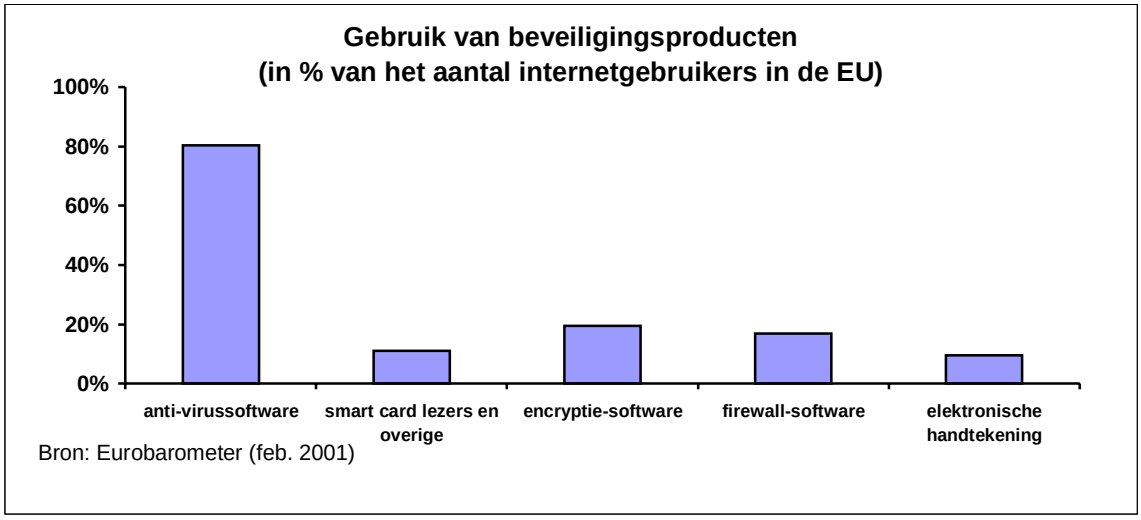
---

4 S-Mime (Secure Multiple Internet Mail Extensions) en OpenPGP (Pretty Good Privacy) zijn alle twee normen van de IETF (Internet Engineering Task Force).

5 Het Echelon-systeem wordt naar men zegt gebruikt voor het onderscheppen van het gewone e-mail-, fax-, telex- en telefoonverkeer via de wereldwijde telecommunicatienetwerken. Zie ook de activiteiten van de tijdelijke commissie van het Europees Parlement voor Echelon op http://www.europarl.eu.int/-committees/echelon_home.htm.

6 De Duitse regering financiert een op de OpenPGP-norm gebaseerd project met de naam GNUPG (http://www.gnupg.org).

niet geheel doordrongen zijn van de potentiële kwetsbaarheid van hun netwerk, blijft een aantal mogelijke oplossingen liggen. Een overzicht over de huidige marktpenetratie van



beveiligingsproducten wordt in voorgaand staafdiagram getoond (statistische gegevens afkomstig van een in februari 2001 verrichte enquête in het kader van de *e*Europe 2000 benchmarking-exercitie).

2.2.3. Netwerkontwrichting

Netwerken zijn inmiddels voor het grootste deel gedigitaliseerd en worden door computers bestuurd. In het verleden was een veelvuldige oorzaak van netwerkstoring een fout in het computersysteem waarmee het netwerk werd bestuurd. Aanvallen op netwerken waren dan ook vooral op deze computers gericht. Inmiddels worden de meest ontwrichtende aanvallen doorgaans gericht op de zwakke plekken van netwerkcomponenten (besturingssystemen, routers, switches, DNS-servers, enz.).

Terwijl ontwrichtende aanvallen op het telefoonnet in het verleden geen aanleiding voor grote bezorgdheid hebben gegeven, zijn aanvallen op internet tamelijk frequent. Dit komt doordat de besturingssignalen voor het telefoonnet gescheiden zijn van het netwerkverkeer en kunnen worden beschermd, terwijl het internet de gebruikers de mogelijkheid laat de centrale netwerkbeheerscomputers te bereiken. Maar ook het telefoonnet kan in de toekomst kwetsbaarder worden wanneer sleutelelementen van het internet in het telefoonnet worden geïntegreerd en wanneer het netwerkcontroleplan ook voor andere exploitanten toegankelijk wordt.

Aanvallen zijn op verschillende manieren mogelijk:

- **Aanvallen op DNS-servers:** Het internet is voor de werking afhankelijk van het domeinnamensysteem (DNS), waarmee gebruikersvriendelijke namen (bijv. www.europa.eu.int) in abstracte netwerkadressen (bijv. IP nr. 147.67.36.16) worden vertaald en omgekeerd. Als een deel van het DNS faalt, kunnen bepaalde websites niet meer worden gelokaliseerd en kan de bezorging van e-mail gedeeltelijk uitvallen. Storingen in de DNS-rootservers of andere topniveau-DNS-servers kunnen tot grootschalige ontwrichting leiden. Begin dit jaar zijn enkele zwakke plekken ontdekt in de software die op de meeste naamservers wordt gedraaid[7].

[7] Bron: CERT/CC (http://www.cert.org/advisories/CA-2001-02.html).

- **Aanvallen op routers:** De routering van het internetverkeer is sterk gedecentraliseerd. Elke router informeert periodiek andere nabijgelegen routers over de netwerken die hij kent en hoe deze kunnen worden bereikt. Een tekortkoming is dat deze informatie niet kan worden geverifieerd, aangezien het systeem zo is ontworpen dat elke router slechts een minimale kennis van de netwerktopologie bezit. Daarom kan elke router zichzelf aanbieden als het beste pad naar een willekeurige bestemming zodat deze het netwerkverkeer naar de betrokken bestemming kan onderscheppen, blokkeren of wijzigen.

- **Aanvallen door middel van flooding en denial-of-service:** Bij dit soort aanvallen wordt het netwerk ontwricht door het te overspoelen met kunstmatige berichten die legitieme toegang onmogelijk maken of beperken. Dit kan worden vergeleken met het blokkeren van faxapparaten door er herhaaldelijk lange berichten naar toe te sturen. Bij flooding attacks wordt geprobeerd webservers of de computers van ISP's (internet service providers) te overbelasten met automatisch gegenereerde berichten.

Mogelijke schade – Voor bepaalde websites met een hoog profiel kan de onderbreking van de dienst schade opleveren. Uit sommige studies is gebleken dat bij een recente aanval enkele honderden miljoen euro schade is veroorzaakt, nog afgezien van de niet te becijferen aantasting van de reputatie. Bedrijven zijn steeds afhankelijker van de beschikbaarheid van hun websites voor het zakendoen en met name bedrijven die op internet zijn aangewezen voor het "just-in-time"-voorraadbeheer, zijn bijzonder kwetsbaar.

Mogelijke oplossingen – Aanvallen op DNS-servers zijn in principe gemakkelijk te ondervangen door de DNS-protocollen uit te breiden, bijvoorbeeld met behulp van veilige DNS-uitbreidingen die op cryptografie met behulp van een openbare sleutel zijn gebaseerd. Dit impliceert evenwel de installatie van nieuwe software op client machines, hetgeen nog niet veel gebeurt. Ook dienen de administratieve procedures ter verhoging van het onderlinge vertrouwen dat DNS-domeinen in elkaar stellen, te worden verbeterd.

De bescherming van het routeringssysteem is veel moeilijker. Het internet werd zo ontworpen dat de routering zo flexibel mogelijk zou zijn, teneinde de kans op onderbreking van de dienst, mocht een deel van de netwerkinfrastructuur falen, zo klein mogelijk te houden. Het is onmogelijk om routeringsprotocollen te beveiligen, zeker op backbone routers.

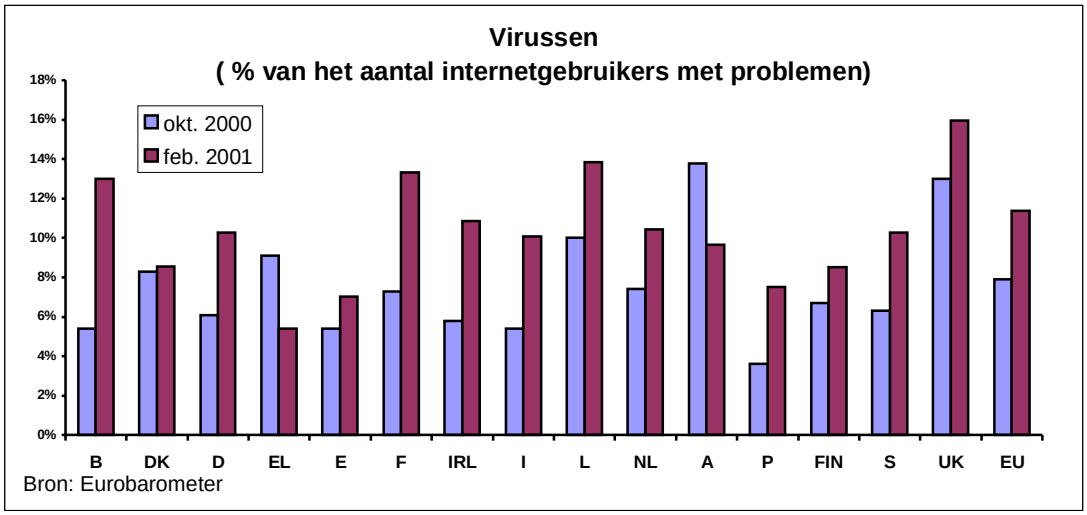
Het volume van de verzonden gegevens is zo groot dat gedetailleerde filtering niet mogelijk is, aangezien de netwerken door een dergelijke controle zouden komen stil te liggen. Daarom verrichten de netwerken alleen elementaire filter- en toegangscontrolefuncties, terwijl specifieke beveiligingsfuncties (bijv. authenticatie, integriteit, encryptie) naar de periferie van de netwerken worden verschoven, d.w.z. naar de randapparaten en netwerkservers die als eindpunten fungeren.

2.2.4. Kwaadaardige software waarmee gegevens worden gewijzigd of vernietigd

Computers hebben software nodig. Helaas kan software ook worden gebruikt om een computer onbruikbaar te maken of om gegevens te wissen of te veranderen. Zoals uit bovenstaande beschrijvingen blijkt, kan zoiets vérstrekkende gevolgen hebben als deze computer deel uitmaakt van de netwerkbesturing. Een virus is een voorbeeld van kwaadaardige software. Het is een programma dat zijn eigen code reproduceert door zichzelf aan andere programma's vast te hechten op een zodanig wijze dat ook de viruscode wordt uitgevoerd wanneer het besmette computerprogramma wordt gebruikt.

Er zijn nog verschillende andere soorten kwaadaardige software: sommige veroorzaken enkel schade op de computer waarnaar zij gekopieerd worden, terwijl andere zichzelf verspreiden naar andere computers in het netwerk. Er zijn bijvoorbeeld programma's (nogal dramatisch "logische bommen" genaamd) die inactief zijn totdat zij door een of andere gebeurtenis worden getriggerd, bijvoorbeeld het bereiken van een bepaalde datum (vaak vrijdag de 13e). Andere programma's wekken niet de indruk kwaadaardige effecten te beogen, maar ontketenen zodra zij worden geopend een doelbewuste aanval (en worden daarom "Trojaanse paarden" genoemd). Weer andere programma's ("wormen" genaamd) besmetten geen andere programma's, zoals een virus, maar maken kopieën van zichzelf, die op hun beurt weer nieuwe kopieën aanmaken en zo uiteindelijk het systeem overspoelen.

Mogelijke schade – Virussen kunnen uiterst destructief zijn, zoals is gebleken uit de hoge kosten als gevolg van enkele recente aanvallen (bijv. "I Love You", "Melissa" en "Kournikova"). Het volgende staafdiagram geeft een overzicht van de toename van het aantal virussen (uitgesplitst per lidstaat) waarmee intergebruikers in de EU tussen oktober 2000 en februari 2001 zijn geconfronteerd. Gemiddeld heeft ongeveer 11% van het aantal internetgebruikers in Europa thuis een virus op de PC opgelopen.



Bron: Eurobarometer

Mogelijke oplossingen – De belangrijkste verdediging is de anti-virussoftware, die in verschillende uitvoeringen verkrijgbaar is. Zo worden bekende virussen bijvoorbeeld opgespoord door virusscanners en desinfectieprogramma's. Hun belangrijkste tekortkoming is dat zij niet gemakkelijk nieuwe virussen kunnen detecteren, zelfs waneer zij regelmatig ge-update worden. Een ander voorbeeld van bescherming tegen virussen zijn de integriteitscontrolesystemen. Om een computer te besmetten moet een virus iets in het systeem veranderen. De integriteitscontrole moet dergelijke veranderingen detecteren, ook als zij door nog onbekende virussen worden veroorzaakt.

Ondanks tamelijk goed ontwikkelde beschermingsproducten zijn de problemen met kwaadaardige software alleen maar gegroeid. Daarvoor zijn twee hoofdredenen. In de eerste plaats biedt het open karakter van het internet aanvallers de mogelijkheid van elkaar te leren hoe zij methodes kunnen ontwikkelen om de beveiligingsmechanismen te omzeilen. In de tweede plaats wordt het internet steeds groter en bereikt het steeds meer gebruikers, waarvan een groot deel niet beseft dat zij voorzorgsmaatregelen behoren te nemen. De veiligheid is afhankelijk van de mate waarin het gebruik van beschermingssoftware ingang heeft gevonden.

2.2.5. Identiteitsvervalsing

Bij het tot stand brengen van een netwerkverbinding of het ontvangen van gegevens doet de gebruiker een bepaalde veronderstelling omtrent de identiteit van de persoon of entiteit aan de andere kant van de verbinding. Het netwerk biedt bepaalde indicatoren maar het grootste gevaar op een aanval komt van personen die de context kennen, insiders dus. Wanneer een gebruiker een telefoonnummer draait of een internetadres intypt, mag hij ervan uitgaan dat hij met de gekozen bestemming wordt verbonden. Bij een groot aantal toepassingen volstaat dit, maar niet bij belangrijke transacties in de commerciële, medische, financiële of formele sfeer, waarbij een hoger niveau van authenticatie, integriteit en vertrouwelijkheid is vereist.

Mogelijke schade – Vervalsing van de identiteit van personen of entiteiten kan op verschillende manieren tot schade leiden. Klanten kunnen kwaadaardige software downloaden van een website die zich als een vertrouwde bron voordoet. Zij kunnen vertrouwelijke informatie aan de verkeerde persoon prijsgeven. Identiteitsvervalsing kan tot het afbreken van contractonderhandelingen leiden, enz. Misschien wel het grootste gevaar schuilt in het feit dat het gebrek aan authenticatie vele bedrijven afschrikt. In diverse studies wordt bezorgdheid over de veiligheid aangewezen als de belangrijkste reden om geen zaken over internet te doen. Als de mensen er zeker van zouden kunnen zijn dat hun gesprekspartner inderdaad degene is voor wie hij zich uitgeeft, zou het vertrouwen in internettransacties toenemen.

Mogelijk oplossingen – Pogingen om tegelijk met de invoering van SSL authenticatie via netwerken mogelijk te maken, kunnen nu al tot een zekere mate van vertrouwen leiden. Bij virtuele particuliere netwerken (VPN's) worden SSL en IPSec gebruikt om communicatie over onveilige internetverbindingen en open kanalen mogelijk te maken met een redelijke mate van veiligheid. Deze oplossingen hebben evenwel slechts een beperkt nut aangezien zij gebaseerd zijn op elektronische certificaten en er geen garantie is dat deze certificaten niet vervalst zijn. Een derde partij, dikwijls "certificatie-instantie" of, zoals in de richtlijn inzake de elektronische handtekening[8], "certificatiedienstverlener" genoemd, kan een dergelijke garantie bieden. Bij de grootschalige introductie van deze oplossing doet zich een soortgelijk probleem voor als bij encryptie: de behoefte aan interoperabiliteit en sleutelbeheer. Bij VPN's is dit geen probleem aangezier er propriëtaire oplossingen kunnen worden ontwikkeld, maar voor openbare netwerken vormt dit een geweldig struikelblok.

De richtlijn inzake elektronische handtekeningen biedt een degelijkere rechtsgrondslag voor de waarborging van een gemakkelijkere manier van elektronische authenticatie in de EU. Het vormt een raamwerk op basis waarvan de markt zich in alle vrijheid kan ontwikkelen, maar dat tevens een stimulans biedt om veiligere handtekeningen te ontwikkelen die rechtsgeldigheid kunnen krijgen. Momenteel wordt de richtlijn in nationaal recht omgezet.

2.2.6. Omgevingsfactoren en onbedoelde gebeurtenissen

Een groot deel van de veiligheidsincidenten is het gevolg van onvoorziene en onbedoelde gebeurtenissen die veroorzaakt worden door:

- natuurrampen (bijv. stormen, overstromingen, branden, aardbevingen)
- derde partijen zonder contractuele relatie met de exploitant of gebruiker (bijv. onderbreking van de dienstverlening als gevolg van bouwwerkzaamheden)

[8] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, PB L 13 van 19.1.2000, blz.12.

- derde partijen met contractuele relatie met de exploitant of gebruiker (bijv. hardware- of softwarefouten in geleverde componenten of programma's)

- menselijk falen of gebrekkig beheer van de exploitant (met inbegrip van de service provider) of de gebruiker (bijv. problemen bij het netwerkbeheer, onjuiste installatie van software)

Mogelijke schade – Natuurrampen kunnen een netwerk onbruikbaar maken. Helaas zijn betrouwbare communicatielijnen nu juist onder deze omstandigheden het hardst nodig. Hardwarefouten en gebrekkige software kunnen systemen kwetsbaar maken waardoor directe ontwrichting optreedt of aanvallers de kans krijgen hiervan misbruik te maken. Gebrekkig beheer van de netwerkcapaciteit kan tot netwerkcongestie leiden waardoor de communicatiekanalen worden vertraagd of ontwricht.

In deze context is het de cruciale vraag hoe de aansprakelijkheid over de diverse partijen wordt verdeeld. In de meeste gevallen treft de gebruiker geen blaam maar heeft hij weinig of geen mogelijkheid tot verhaal.

Mogelijke oplossingen – De exploitanten van telecommunicatienetwerken zijn goed op de hoogte van de natuurlijke risico's. Zij hebben daarom redundantie in hun netwerken ingebouwd en de infrastructuur tegen deze risico's beschermd. De groeiende concurrentie zou evenwel een dubbel effect kunnen hebben op het gedrag van de exploitanten. Enerzijds zouden kostenoverwegingen de exploitanten ertoe kunnen aanzetten deze redundantie te verminderen en anderzijds zou de aanwezigheid van meer exploitanten op de markt als gevolg van de liberalisering de gebruikers de mogelijkheid kunnen bieden in geval van niet-beschikbaarheid van het netwerk op een andere exploitant over te schakelen (zoals bijvoorbeeld de vliegtuigpassagier die door een andere maatschappij wordt vervoerd als zijn vlucht geannuleerd wordt). Niettemin eist het Gemeenschapsrecht dat de lidstaten alle nodige maatregelen treffen om de kwetsbaarheid van openbare netwerken bij netwerkstoringen of natuurrampen te garanderen (zie de Interconnectierichtlijn 97/33/EG[9] en de Spraaktelefonierichtlijn 98/10/EG[10]). Over het geheel genomen is de kennis van het veiligheidsniveau als gevolg van het groeiende aantal onderling gekoppelde netwerken nog onvoldoende.

De concurrentie tussen de leveranciers van hardware en software moet de druk om de veiligheid van producten te verbeteren, opvoeren. Als drijfveer voor investeringen in veiligheid is de mededinging evenwel niet groot genoeg en veiligheid is niet altijd een doorslaggevende factor bij aankoopbeslissingen. Zwakke plekken in de beveiliging worden vaak pas ontdekt wanneer het kwaad al geschied is. De instandhouding van eerlijke concurrentie op de IT-markt zal de veiligheid evenwel ten goede komen.

Het risico van menselijk falen en beheersfouten kan worden verminderd door betere opleiding en bewustmakingsactiviteiten. Door een passend beveiligingsbeleid voor de onderneming te formuleren kan dit risico eveneens worden verminderd.

2.3. Nieuwe uitdagingen

Netwerk- en informatieveiligheid zal waarschijnlijk een sleutelfactor voor de ontwikkeling van de informatiemaatschappij worden, aangezien netwerken een steeds belangrijkere rol

---

9 PB L 199 van 26.7.1997.

10 PB L 101 van 1.4.1998.

gaan spelen in het economische en sociale leven. Daarbij dient aandacht te worden besteed aan twee aspecten: de steeds grotere potentiële schade en de nieuwe technologische ontwikkelingen.

i) Netwerken en informatiesystemen transporteren steeds meer **gevoelige gegevens en informatie met een economische waarde** waardoor de aantrekkelijkheid van een aanval op deze systemen groeit. Een dergelijke aanval kan op laag niveau plaatsvinden zodat deze geen gevolgen op nationale schaal zal hebben, zoals bij het inbreken in en wijzigen van een persoonlijke website of het herformatteren van een harde schijf door een virus. De ontwrichting kan echter ook op een veel kritischere schaal gebeuren, tot op het niveau van verstoring van uiterst gevoelige communicatie, grote stroomstoringen of misgelopen opdrachten door middel van denial-of-service-aanvallen of vertrouwelijkheidslekken

   De precieze omvang van de feitelijke en potentiële schade als gevolg van tekortkomingen in de veiligheid van netwerken is evenwel moeilijk te bepalen. Er bestaat geen systeem voor systematische rapportage en vele bedrijven maken geconstateerde aanvallen liever niet bekend uit vrees voor negatieve publiciteit. Concrete gegevens zijn dus schaars. De schade omvat niet alleen de directe kosten (inkomstenderving, verlies van waardevolle informatie, arbeidsloon van het personeel dat het netwerk dient te herstellen), maar ook de immateriële schade – in het bijzonder de aantasting van de reputatie – die moeilijk te kwantificeren is.

ii) **Netwerk- en informatieveiligheid is een dynamische kwestie.** Door het tempo van de technologische veranderingen worden wij voortdurend voor nieuwe uitdagingen geplaatst: de problemen van gisteren worden opgelost en de oplossingen van vandaag verliezen hun betekenis. De markt komt bijna dagelijks met nieuwe toepassingen, diensten en producten. Een deel van de ontwikkelingen zal een duidelijk nieuwe uitdaging vormen voor het veiligheidsbeleid van de particuliere en openbare sector.

   - Via netwerken zullen digitale objecten van uiteenlopende aard worden verzonden, zoals multimedia-objecten, programma's of mobiele agenten met een geïntegreerd veiligheidsbeleid. Het begrip beschikbaarheid, dat vandaag de dag nog wordt opgevat als de mogelijkheid om het netwerk te gebruiken, zal evolueren in de richting van geautoriseerd gebruik, bijvoorbeeld het recht om een videospel gedurende een bepaalde periode te gebruiken, het recht op één enkele kopie van een computerprogramma, enz.

   - In de toekomst zullen de exploitanten van IP-netwerken mogelijk de veiligheid willen verhogen door het netwerkverkeer permanent te controleren teneinde uitsluitend geautoriseerd verkeer door te laten. Dergelijke maatregelen dienen evenwel in overeenstemming te zijn met de relevante voorschriften inzake gegevensbescherming.

   - De gebruikers zullen overschakelen op permanente internetaansluitingen, die potentiële aanvallers meer houvast geven, de kwetsbaarheid van onbeschermde eindapparatuur verhogen en aanvallers ook meer mogelijkheden bieden om onopgemerkt te blijven.

   - Huisnetwerken waarop diverse apparaten zijn aangesloten zullen op grote schaal hun intrede doen, waardoor men zich blootstelt aan nieuwe aanvalsmogelijkheden

en de kwetsbaarheid van de gebruiker wordt verhoogd (door bijvoorbeeld alarminstallaties op afstand uit te schakelen).

- Als gevolg van de introductie op grote schaal van draadloze netwerken (bijv. draadloos aansluitnet, draadloze LAN's, 3G) kan doeltreffende encryptie van gegevens die via radiosignalen worden overgedragen, als een nieuwe uitdaging worden beschouwd. Derhalve wordt het steeds problematischer dat de wet een zwakke encryptie van deze signalen voorschrijft.

- Netwerken en informatiesystemen op basis van een combinatie van draadverbindingen en draadloze verbindingen zijn alom tegenwoordig en vormen een "intelligente omgeving", d.w.z. een geheel van zelfstandige functies dat beslissingen die vroeger door de gebruiker werden genomen, automatisch neemt en uitvoert. Het is nu zaak enerzijds te voorkomen dat de kwetsbaarheid hiervan op een onaanvaardbaar niveau komt te liggen en anderzijds te zorgen voor integratie van de veiligheid in de architectuur.

3. Een Europese beleidsaanpak

3.1. Noodzaak van een overheidsbeleid

De beveiliging van communicatienetwerken wordt steeds meer gezien als een prioriteit voor beleidsmakers, vooral met het oog op de bescherming van gegevens, die nodig is voor de goede werking van de economie, de nationale veiligheid, en de wens om de elektronische handel te bevorderen. Dit heeft geleid tot een aanzienlijk pakket van wettelijke voorschriften, die zijn opgenomen in de EU-richtlijnen inzake gegevensbescherming en het EU-regelgevingskader voor telecommunicatie (zie paragraaf 3.6). Deze maatregelen dienen evenwel te worden toegepast in een snel veranderende omgeving van nieuwe technologieën, geliberaliseerde markten, convergerende netwerken en mondialisering. Daar komt nog bij dat de markt om onderstaande redenen de neiging zal vertonen te weinig in beveiliging te investeren.

Netwerk- en informatieveiligheid kan worden gezien als een goed dat op de markt wordt gekocht en verkocht en waarover afspraken worden gemaakt in de contractuele overeenkomsten tussen partijen. De markt voor beveiligingsproducten is in de afgelopen jaren enorm gegroeid. Volgens sommige studies vertegenwoordigde de markt voor internetbeveiligingssoftware eind 1999 wereldwijd een waarde van 4,4 miljard dollar[11]. Uitgaande van een geraamde groei van 23% per jaar, zal dit bedrag in 2004 zijn opgelopen tot 8,3 miljard dollar. Verwacht wordt dat de markt voor beveiliging van elektronische communicatie in Europa zal groeien van 465 miljoen dollar in 2000 tot 5,3 miljard dollar in 2006[12], terwijl de omzet in de sector beveiliging van informatietechnologie zal toenemen van 490 miljoen in 1999 tot 2,74 miljard in 2006[13].

Meestal wordt er daarbij impliciet van uitgegaan dat de kosten van de beveiliging via het prijsmechanisme in evenwicht zullen worden gebracht met de specifieke beveiligingsbehoefte. Sommige gebruikers hebben behoefte aan een hoog niveau van veiligheid, terwijl andere genoegen nemen met een lager niveau – ofschoon de overheid natuurlijk een minimumbeveiligingsniveau kan voorschrijven. Hun voorkeuren komen dan tot

---

11 IDC : Internet security market forecast and analysis, 2000-2004 Report W23056, oktober 2000.

12 Frost & Sullivan: The European Internet communication security markets, rapport 3717, november 2000.

13 Frost & Sullivan: The European Internet communication security markets, rapport 3847, juli 2000.

uitdrukking in de prijs die zij bereid zijn voor de beveiligingsvoorzieningen te betalen. Niettemin is een groot aantal veiligheidsrisico's – zoals is gebleken uit de analyse van hoofdstuk 2 – nog niet opgelost of bereiken de oplossingen daarvoor als gevolg van tekortkomingen in de marktwerking slechts langzaam de markt.

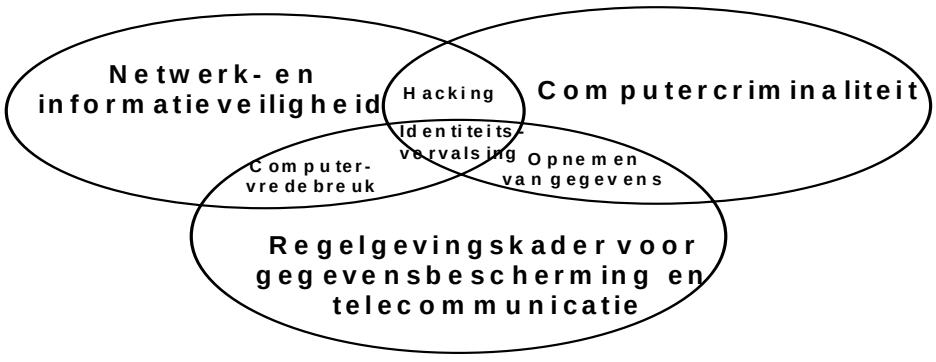
i) **Maatschappelijke kosten en baten:** Investeringen in een betere netwerkbeveiliging brengen maatschappelijke kosten en baten mee die niet voldoende in de marktprijzen tot uitdrukking komen. **Aan de kostenzijde** worden de marktspelers niet altijd verantwoordelijk gesteld voor de gevolgen van hun gedrag ten aanzien van veiligheid. Gebruikers en exploitanten van netwerken met een laag veiligheidsniveau dragen geen aansprakelijkheid jegens derden. Dit is hetzelfde als een roekeloze chauffeur die niet aansprakelijk wordt gesteld voor de kosten van de verkeersopstopping die ontstaat als gevolg van een door hem veroorzaakt ongeval. Evenzo zijn op het internet diverse aanvallen georganiseerd via de slecht beveiligde machines van relatief onvoorzichtige gebruikers. **De voordelen van beveiliging komen niet volledig tot uitdrukkin in de marktprijzen.** Wanneer exploitanten, leveranciers of service providers de veiligheid van hun producten verhogen komen de voordelen van deze investering niet alleen hun klanten ten goede, maar ook al degenen die direct of indirect bij elektronische communicatie zijn betrokken – in feite dus de gehele economie.

ii) **Asymmetrische informatie:** Netwerken worden steeds complexer en dringen door tot op een bredere markt van gebruiker waarvan een groot deel weinig inzicht heeft in de technologie of de potentiële gevaren ervan. Dit betekent dat de gebruikers niet terdege alle veiligheidsrisico's beseffen en dat een groot deel van de exploitanten, leveranciers en service providers ternauwernood in staat is het bestaan en de verspreiding van zwakke plekken te ontdekken. Een groot aantal nieuwe diensten, toepassingen en programma's biedt aantrekkelijke eigenschappen, maar verhoogt vaak tegelijkertijd de kwetsbaarheid van het netwerk (zo is het succes van het world wide web deels te danken aan de vele multimediatoepassingen die gemakkelijk gedownload kunnen worden, maar deze "plug-ins" vormen ook een aangrijpingspunt voor aanvallen). Terwijl de voordelen duidelijk zijn, zijn de risico's dit niet en de drijfveren voor de leveranciers om nieuwe mogelijkheden te introduceren zijn groter dan die om meer veiligheid te bieden.

iii) **Het dilemma van overheidsoptreden:** Steeds vaker schakelen exploitanten over op internetstandaards of koppelen zij hun netwerken op een of andere manier aan het internet. Het internet werd evenwel niet ontworpen met de veiligheid in het achterhoofd, maar werd juist ontwikkeld om de toegankelijkheid van informatie te waarborgen en de uitwisseling ervan te vergemakkelijken. Dit vormde de grondslag voor het succes. Het internet is uitgegroeid tot een wereldwijd netwerk van netwerken met een ongeëvenaarde rijkdom en diversiteit. Investeringen in beveiliging verdienen zichzelf alleen terug wanneer voldoende mensen meedoen. Derhalve is bij de ontwikkeling van oplossingen voor beveiligingsvraagstukken **samenwerking** onmisbaar. Maar samenwerking kan uitsluitend effect sorteren wanneer het aantal deelnemers een kritische massa bereikt, hetgeen moeilijk is aangezien gratis meeprofiteren mogelijk is. Interoperabiliteit tussen producten en diensten zal concurrentie tussen beveiligingsoplossingen mogelijk maken. De coördinatiekosten liggen evenwel hoog omdat soms wereldwijde oplossingen vereist zijn en sommige spelers geneigd zijn de markt propriëtaire oplossingen op te dringen. Aangezien bij een groot aantal producten en diensten nog steeds propriëtaire oplossingen worden gebruikt, is er geen voordeel te bereiken met het gebruik van veilige normen die alleen extra veiligheid bieden als iedereen deze aanbiedt.

Op grond van deze onvolkomenheden is met het regelgevingskader voor telecommunicatie en gegevensbescherming al voorzien in een wettelijke verplichting voor exploitanten en dienstverleners om een bepaalde mate van veiligheid van communicatie- en informatiesystemen te bieden. De kern van een Europees beleid inzake netwerk- en informatieveiligheid kan als volgt worden beschreven. In de eerste plaats dienen de wettelijke voorschriften op EU-niveau doeltreffend te worden toegepast. Hiervoor is een **gemeenschappelijk inzicht in de onderliggende veiligheidsproblematiek en de specifieke maatregelen die moeten worden getroffen** noodzakelijk. Het regelgevingskader dient in de toekomst voorts te evolueren, hetgeen nu al duidelijk wordt aan de hand van het voorstel voor een nieuw regelgevingskader voor elektronische communicatie of de toekomstige voorstellen ten aanzien van computercriminaliteit. In de tweede plaats moet op grond van bepaalde tekortkomingen van de markt moeten worden geconcludeerd dat de marktwerking alleen niet in staat is om voldoende investeringen in beveiligingstechnologie en –procedures te genereren. **De marktwerking kan met beleidsmaatregelen worden versterkt, waardoor tegelijkertijd de werking van het regelgevingskader kan worden verbeterd.** Ten slotte worden communicatie- en informatiediensten over de grenzen heen aangeboden. Daarom is een Europese beleidsaanpak noodzakelijk **teneinde ervoor te zorgen dat de interne markt voor dergelijke diensten gegarandeerd is, dat van gemeenschappelijk oplossingen kan worden geprofiteerd en dat effectief optreden op wereldwijd niveau mogelijk is.**

De voorgestelde beleidsmaatregelen ten aanzien van netwerk- en informatieveiligheid dienen te worden gezien niet alleen tegen de achtergrond van de huidige wetgeving ten aanzien van telecommunicatie en gegevensbescherming, maar ook in samenhang met het recentere beleid op het stuk van computercriminaliteit. De Commissie heeft onlangs een mededeling over computercriminaliteit[14] gepubliceerd, waarin onder meer de oprichting van een EU-Forum voor computercriminaliteit wordt aangekondigd, dat het wederzijds begrip en de onderlinge samenwerking tussen alle betrokkenen op EU-niveau dient te verbeteren. Met een beleid ten aanzien van netwerk- en informatieveiligheid wordt de ontbrekende schakel van dit beleidskader geleverd. Onderstaande afbeelding toont deze drie beleidsterreinen en illustreert aan de hand van enkele voorbeelden hoe deze met elkaar zijn verweven:



[14] De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden, COM (2000) 890, http://europa.eu.int/ISPO/eif/internetPoliciesSite/crime1.html.

3.2. Bewustmaking

Er zijn nog steeds te veel gebruikers (zowel in de particuliere als in de overheidssector) die niet op de hoogte zijn van de mogelijke risico's bij het gebruik van communicatienetwerken of van de oplossingen die daar nu al voor bestaan. De veiligheidsproblematiek is een complexe materie en de risico's zijn dikwijls moeilijk in te schatten, zelfs voor deskundigen. Gebrek aan informatie is een van de op de markt geconstateerde tekortkomingen, waarvoor het veiligheidsbeleid een oplossing dient aan te dragen. Het gevaar bestaat dat sommige gebruikers, ongerust over de vele berichten over de veiligheidsrisico's van computernetwerken, de elektronische handel gewoonweg gaan mijden. Anderen, die verstoken zijn gebleven van informatie of de gevaren onderschatten, kunnen te veel risico's gaan nemen. Sommige bedrijven hebben er belang bij de risico's te minimaliseren uit angst hun klanten kwijt te raken.

Paradoxaal genoeg is er op internet enorm veel informatie beschikbaar over netwerk- en informatieveiligheid en wordt er in computertijdschriften uitgebreid aandacht besteed aan dit onderwerp. Het probleem voor gebruikers is geschikte informatie te vinden die begrijpelijk en actueel is en aan hun specifieke behoeften beantwoordt. De automobielindustrie biedt een goed voorbeeld van hoe complexe veiligheidsspecificaties kunnen worden omgezet in een doorslaggevend verkoopargument. Ten slotte zijn de aanbieders van een openbaar toegankelijke telecommunicatiedienst op grond van de EU-wetgeving verplicht hun abonnees in te lichten over de bijzondere risico's van eventuele gaten in de netwerkbeveiliging en de maatregelen die daartegen mogelijk zijn, met inbegrip van de kosten daarvan (zie artikel 4 van Richtlijn 97/66/EG).

Het doel van een voorlichtingsinitiatief voor burgers, overheden en bedrijven is daarom toegankelijke, onafhankelijke en betrouwbare informatie over netwerk- en informatieveiligheid te bieden. Zodra de mensen goed zijn voorgelicht, zijn zij in staat hun eigen keuze te maken over het niveau van veiligheid waarmee zij zich tevreden stellen.

Voorgestelde maatregelen:

- De lidstaten dienen een voorlichtings- en scholingsactie te starten en de lopende activiteiten te moderniseren. Dit houdt in een voorlichtingscampagne in de massamedia en op de betrokken partijen afgestemde specifieke acties. Een weloverwogen en doeltreffende voorlichtingscampagne is niet goedkoop. Het opzetten van een campagne waarmee het publiek kan worden gewaarschuwd zonder paniek te zaaien en zonder potentiële hackers te stimuleren vereist zorgvuldige planning.

  De Europese Commissie zal de uitwisseling van beste praktijken bevorderen en zorgen voor een zekere mate van coördinatie van de verschillende nationale voorlichtingscampagnes in EU-verband, in het bijzonder wat betreft de inhoud van de te verstrekken informatie. Een portaalsite naar zowel nationale als Europese websites vormt een van de onderdelen van deze actie. Ook kan worden overwogen op deze portaalsites te verwijzen naar trusted websites van internationale partners.

- De lidstaten dienen de toepassing van de beste praktijk op het gebied van netwerkveiligheid op basis van bestaande instrumenten, zoals ISO/IEC 17799 (praktijkcode voor informatieveiligheidsbeheer: http://www.iso.ch), aan te moedigen. De aandacht moet vooral worden gericht op het midden- en kleinbedrijf. De Commissie zal de lidstaten daarbij steunen.

- De onderwijssystemen in de lidstaten dienen meer aandacht te schenken aan cursussen op het gebied van veiligheid. De ontwikkeling van onderwijsprogramma's op alle niveaus, bijvoorbeeld opleidingen inzake de veiligheidsrisico's van open netwerken en doeltreffende oplossingen daarvoor, dient te worden gestimuleerd zodat deze worden opgenomen in het computeronderwijs aan scholen.

  De leraren moeten op hun beurt worden voorgelicht over veiligheid in het kader van hun eigen opleiding. De Europese Commissie steunt in het kader van haar onderzoekprogramma de ontwikkeling van nieuwe modules voor leerprogramma's.

3.3. Een Europees waarschuwings- en informatiesysteem

Zelfs wanneer de gebruikers bekend zijn met de veiligheidsrisico's zullen zij op de hoogte moeten worden gehouden van nieuwe bedreigingen. Kwaadwillende aanvallers zullen welhaast zeker nieuwe manieren vinden om de modernste beveiligingssystemen te omzeilen. De industrie ontwikkelt continu nieuwe software-applicaties en -diensten die een betere kwaliteit van de dienstverlening bieden waardoor het internet aantrekkelijker wordt, maar daarmee creëren zij ongewild nieuwe zwakke plekken en risico's.

Zelfs ervaren netwerkbeheerders en beveiligingsdeskundigen worden dikwijls verrast door de originaliteit van sommige aanvallen. Daarom is een waarschuwingssysteem nodig waarmee alle gebruikers snel op de hoogte kunnen worden gebracht en dat als een bron van snelle en betrouwbare informatie kan dienen over de wijze waarop deze aanvallen kunnen worden afgeweerd. Voor het bedrijfsleven moet er een vertrouwelijk mechanisme komen voor de rapportage van aanvallen, zodat zij niet het gevaar lopen het vertrouwen van het publiek te verliezen. Tegelijkertijd dient een ruimer opgezette veiligheidsanalyse plaats te vinden waarbij vooruit wordt gekeken en in het kader waarvan bewijsmateriaal bijeengebracht wordt en de risico's binnen een bredere context kunnen worden geanalyseerd.

Op dit gebied wordt veel werk verzet door openbare en particuliere "computercalamiteitenteams" (Computer Emergency Response Teams: CERT's) of soortgelijke organisaties. In België bijvoorbeeld is een viruswaarschuwingssysteem opgezet dat Belgische burgers binnen twee uur op de hoogte stelt van een virusdreiging. De CERT's in de verschillende lidstaten gaan evenwel op uiteenlopende wijze te werk, wardoor de samenwerking complex is. De bestaande CERT's beschikken niet altijd over voldoende middelen en hun taken zijn vaak niet duidelijk omlijnd. Voor de wereldwijde coördinatie zorgt CERT/CC, dat gedeeltelijk door de Amerikaanse regering wordt gefinancierd en de CERT's in Europa zijn afhankelijk van de informatie die wordt vrijgegeven door CERT/CC en andere organisaties.

Als gevolg van deze complexe situatie is de Europese samenwerking tot dusver beperkt gebleven. Deze samenwerking is evenwel essentieel om ervoor te zorgen dat waarschuwingen via een systeem voor ogenblikkelijke uitwisseling van informatie snel door de gehele Unie worden verspreid, zodra zich in een van de landen de eerste tekenen van een aanval voordoen. Daarom is het dringend noodzakelijk de samenwerking met het CERT-systeem binnen de Europese Unie te verbeteren. Over een eerste stap in de richting van een betere samenwerking tussen openbare en particuliere sector wat betreft de afhankelijkheid van informatie-infrastructuren (waaronder de ontwikkeling van systemen voor vroegtijdige waarschuwing) en de verbetering van de samenwerking tussen de CERT's zijn afspraken gemaakt in het kader van het *e*Europe-actieplan.

Voorgestelde maatregelen:

- De lidstaten dienen hun CERT-systeem te herzien teneinde de uitrusting en deskundigheid van bestaande CERT's te verbeteren. Om de nationale inspanningen te steunen zal de Europese Commissie een concreet voorstel ontwikkelen ter verbetering van de samenwerking binnen de Europese Unie. Dit behelst onder meer voorstellen voor projecten in het kader van het TEN-Telecom-programma, die tot doeltreffende netwerkvorming moet leiden en de vaststelling van begeleidende maatregelen in het kader van het IST-programma ter bevordering van informatie-uitwisseling.
- Zodra het CERT-netwerk op EU-niveau een feit is, dient het te worden aangesloten op soortgelijke instrumenten in de rest van de wereld, zoals het voorgestelde G8-ongevalsrapportagesysteem.
- De Commissie stelt voor samen met de lidstaten te onderzoeken hoe de inzameling van gegevens, de analyse en de planning van preventieve maatregelen tegen de huidige en nieuwe veiligheidsrisico's het best kunnen worden georganiseerd. De organisatievorm van een eventuele structuur hiervoor dient nog te worden besproken met de lidstaten.

3.4. Technologische ondersteuning

Investeringen in netwerk- en informatieveiligheid zijn momenteel niet optimaal. Dit geldt zowel voor de toegepaste technologie als voor het onderzoek naar nieuwe oplossingen. Tegen de achtergrond van nieuwe technologieën die nieuwe risico's met zich meebrengen, is de continuïteit van het onderzoek van fundamenteel belang.

Netwerk- en informatieveiligheid is nu al een van de onderzoekthema's die in het programma Technologieën van de informatiemaatschappij (IST) van het vijfde kaderprogramma voor onderzoek van de EU (waarvoor in een periode van vier jaar 3,6 miljard euro zal worden uitgetrokken) is opgenomen. In de periode 2001/2002 zal in het kader hiervan ongeveer 30 miljoen euro worden besteed aan onderzoek in samenwerkingsverband op het gebied van voor de veiligheid relevante technologieën.

Het technisch onderzoek op het gebied van cryptografie verkeert in Europa in een gevorderd stadium. Het Belgische algoritme "Rijndael" heeft de Advanced Encryption Standard Competition van het Amerikaanse normalisatie-instituut (NIST) gewonnen. In het kader van het IST-project NESSIE (New European Schemes for Signature, Integrity and Encryption) is een grootscheepse prijsvraag gestart voor encryptie-algoritmes waarmee aan de eisen van nieuwe multimediatoepassingen, mobiele handel en chipkaarten kan worden voldaan.

Voorgestelde maatregelen:

- De Commissie stelt voor het thema veiligheid op te nemen in het komende zesde kaderprogramma, dat momenteel wordt behandeld door de Raad en het Parlement. Om optimaal gebruik te maken van de in dat verband gedane uitgaven, dient dit thema in een bredere strategie ter verhoging van de netwerk- en informatieveiligheid te worden ingebed. Bij het onderzoek in het kader van dit programma dient te worden ingegaan op de belangrijkste veiligheidsrisico's van de "volledig digitale" samenleving en op de noodzaak de rechten van het individu en de gemeenschap te beschermen. De nadruk zal worden gelegd op fundamentele beveiligingsmechanismen en de interoperabiliteit daarvan, dynamische beveiligingsprocessen, geavanceerde cryptografie, privacybeschermingstechnologieën, technologieën voor de behandeling van digitale activa en betrouwbaarheidstechnologieën ter ondersteuning van zakelijke en organisatorische functies in dynamische en mobiele systemen.

- De lidstaten moeten actief het gebruik van krachtige "pluggable"[15] encryptieproducten stimuleren. Veiligheidsoplossingen op basis van integreerbare encryptie dienen beschikbaar te zijn als alternatief voor de in de besturingssystemen opgenomen oplossingen.

3.5. Steun voor markgeoriënteerde standaardiserings- en certificeringswerkzaamheden

Oplossingen ter verhoging van de veiligheid zijn enkel effectief als deze door alle relevante marktspelers worden toegepast, bij voorkeur op basis van open internationale normen. Een van de grootste belemmeringen voor de popularisering van een groot aantal veiligheidssystemen, zoals de elektronische handtekening, is het gebrek aan interoperabiliteit van de diverse implementaties. Als twee gebruikers veilig met elkaar gegevens willen uitwisselen vanuit verschillende omgevingen, dient de interoperabiliteit gewaarborgd te zijn. Het gebruik van gestandaardiseerde protocollen en interfaces dient te worden gestimuleerd, onder meer door de toepassing van conformiteitstests, maar ook via "interoperabiliteits-bijeenkomsten". Open normen, bij voorkeur op basis van open source software, kunnen een bijdrage leveren tot een sneller herstel van fouten en een hogere transparantie.

Ook informatieveiligheidsevaluaties kunnen bijdragen tot het vertrouwen van de gebruiker. Het gebruik van gemeenschappelijke criteria is bevorderlijk geweest voor de toepassing in vele landen van wederzijdse erkenning als een beoordelingsmethode[16] en deze landen hebben met de VS en Canada afspraken gemaakt over wederzijdse erkenning van IT-veiligheidscertificaten.

Certificering van bedrijfsprocessen en systemen voor informatieveiligheidsbeheer wordt ondersteund door de Europese samenwerking op het gebied van de accreditering (EA)[17]. De erkenning van certificeringsinstanties verhoogt het vertrouwen in hun deskundigheid en onafhankelijkheid, waardoor de aanvaarding van door hen verleende certificaten in de gehele interne markt wordt bevorderd.

Naast certificering dienen er ook interoperabiliteitsproeven te worden verricht. Een voorbeeld van een dergelijke benadering is het European Electronic Signatures Standardisation Initiative (EESSI), dat zich bezighoudt met de ontwikkeling van door alle deelnemers aanvaarde oplossingen ter ondersteuning van de EU-richtlijn inzake elektronische handtekeningen. Andere voorbeelden zijn het chipkaartinitiatief in het kader van *e*Europe en de initiatieven op het gebied van de implementatie van de Public Key Infrastructure (PKI), die in het kader van het Programma voor uitwisseling van gegevens tussen overheden (IDA) van start zijn gegaan.

Het ontbreekt niet aan standaardiserings-activiteiten, maar een groot aantal concurrerende normen en specificaties heeft tot versnippering van de markt en niet-interoperabele oplossingen geleid. Daarom moeten de huidige standaardiserings- en certificeringsactiviteiten beter gecoördineerd worden, mede om het tempo waarin nieuwe oplossingen worden geïntroduceerd, te kunnen bijbenen. Door de harmonisatie van specificaties zal de interoperabiliteit toenemen en tegelijk een vlotte implementatie door de marktdeelnemers mogelijk worden.

---

[15] Met "pluggable" wordt bedoeld dat encryptiesoftware bovenop het besturingssysteem gemakkelijk kan worden geïnstalleerd en volledig operationeel worden gemaakt.

[16] Aanbeveling 95/144/EG van de Raad van 7 april 1995 inzake gemeenschappelijke veiligheidsbeoordelingscriteria voor informatietechnologie (in de meeste EU-lidstaten ten uitvoer gelegd).

[17] Europese samenwerking op het gebied van accreditering tussen accrediteringsinstanties uit 25 EU-, EVA- en kandidaat-lidstaten

Voorgestelde maatregelen:

- De Europese normalisatie-instellingen wordt verzocht het tempo van de activiteiten op het gebied van interoperabele en veilige producten en diensten op te voeren en hiervoor een ambitieus en vast tijdschema op te stellen. Waar nodig moeten de te bereiken resultaten en te volgen procedures in een nieuwe vorm worden gegoten om de werkzaamheden in een stroomversnelling te brengen, de samenwerking met vertegenwoordigers van de consumenten te verbeteren en de betrokkenheid van de marktspelers te verhogen.
- De Commissie zal het gebruik van elektronische handtekeningen, de implementatie van gebruikersvriendelijke interoperabele PKI-oplossingen en de verdere ontwikkeling van IPv6 en IPSec[18] (zoals gepland in het actieplan *e*Europe 2002), met name via de programma's IST en IDA, blijven ondersteunen.
- De lidstaten wordt verzocht het gebruik van certificerings- en accrediteringsprocedures te bevorderen op basis van algemeen aanvaarde Europese en internationale normen zodat de wederzijdse erkenning van certificaten wordt gestimuleerd. De Commissie zal nagaan of er behoefte aan bestaat om nog voor eind 2001 een regelgevingsinitiatief inzake wederzijdse erkenning van certificaten te nemen.
- De Europese marktspelers worden aangespoord om op actievere wijze deel te nemen aan Europese (CEN, Cenelec, ETSI) en internationale standaardiseringsactiviteiten (Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C)).
- De lidstaten dienen alle relevante beveiligingsnormen te evalueren. In samenwerking met de Commissie zouden prijsvragen kunnen worden georganiseerd voor de ontwikkeling van Europese encryptie- en beveiligingsoplossingen met de bedoeling een impuls te geven aan internationaal overeengekomen normen.

3.6. Wettelijk kader

Er bestaat diverse wetgeving die gevolgen heeft voor de veiligheid van communicatienetwerken en informatiesystemen. Het regelgevingskader voor telecommunicatie is daarvan het belangrijkste voorbeeld. Vanwege de convergentie van netwerken brengt de veiligheidsproblematiek regelgeving en regelgevingstradities uit verschillende sectoren nader bijeen. Het gaat hierbij om de **telecommunicatie** (alle communicatienetwerken), die enerzijds gereguleerd en anderzijds gedereguleerd wordt, de nog grotendeels niet reguleerde **computerindustrie**[19], het **internet**, dat tot dusver vooral op basis van een "laissez faire"-benadering heeft gefunctioneerd, en **elektronische handel**, waarvoor in toenemende mate specifieke regelgeving wordt vastgesteld. Wat betreft de veiligheidsvoorschriften in verband met de aansprakelijkheid jegens derden is de wetgeving inzake computercriminaliteit, elektronische handtekeningen, gegevensbescherming en uitvoerbepalingen relevant. Van de diverse bestaande regelingen zijn de gegevensbeschermingsrichtlijnen, het regelgevingskader voor telecommunicatie en verschillende regelgevingsinitiatieven in verband met computercriminaliteit in deze context bijzonder relevant.

---

[18] IPv6 is een internetprotocol waarbij het aantal mogelijke IP-adressen wordt verhoogd, de routering van berichten wordt geoptimaliseerd en de mogelijkheden voor introductie van IPSec worden verruimd. IPSec is een ander internetprotocol dat de vertrouwelijkheid moet waarborgen, ervoor moet zorgen dat datapakketten alleen door de ontvangende hostcomputer kunnen worden ingezien en authenticatie en integriteit moet bieden teneinde te garanderen dat de gegevens in een datapakket authentiek en van de oorspronkelijke afzender afkomstig zijn.

[19] Er bestaan veiligheidseisen voor elektrische componenten van een computer, maar niet voor de verwerking van gegevens door een computer.

Bescherming van de privacy is een belangrijke beleidsdoelstelling van de Europese Unie. De bescherming van de privacy wordt krachtens artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden[20] als een grondrecht beschouwd. De artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie[21] voorzien voorts in het recht op bescherming van gezins- en privéleven, huis en haard, communicatie en gegevens van persoonlijke aard.

Op grond van de gegevensbeschermingsrichtlijnen[22], in het bijzonder artikel 5 van de richtlijn Bescherming Telecommunicatiegegevens[23], zijn de lidstaten verplicht de vertrouwelijkheid voor openbare telecommunicatienetwerken en openbaar toegankelijke telecommunicatiediensten te garanderen. Met het oog op de toepassing in de praktijk van artikel 5 zijn de aanbieders van openbare diensten en netwerken op grond van artikel 4 van die richtlijn bovendien verplicht passende technische en organisatorische maatregelen te treffen om de veiligheid van hun diensten te waarborgen. Conform ditzelfde artikel dient bij deze maatregelen de mate van veiligheid te worden afgestemd op het risico, rekening houdende met de stand van de techniek en de kosten ervan. Dit betekent dat alle netwerkexploitanten wettelijk verplicht zijn het telecommunicatieverkeer te beschermen tegen wederrechtelijke onderschepping. Het pan-Europese karakter van diensten en de intensievere grensoverschrijdende concurrentie vergroten de noodzaak van harmonisatie van deze voorschriften.

Op grond van artikel 17 van de algemene gegevensbeschermingsrichtlijn 95/46/EG zijn de voor de verwerking verantwoordelijke organisaties verplicht maatregelen te treffen om een passend beveiligingsniveau te garanderen gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich brengen, in het bijzonder indien de verwerking doorzending van gegevens over een netwerk behelst. Zij dienen passende technische en organisatorische maatregelen te treffen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens via een netwerk behelst, en tegen enige andere vorm van onwettige verwerking. Deze voorschriften hebben gevolgen voor de veiligheidseisen die moeten worden gesteld aan netwerken en informatiesystemen die door die personen en organisaties worden gebruikt, zoals aanbieders van e-commerce diensten. Vanwege het pan-Europese karakter van diensten en de grotere grensoverschrijdende concurrentie groeit de behoefte om te specificeren met welke middelen aan deze voorschriften moet worden voldaan.

Het **EU-regelgevingskader voor telecommunicatiediensten** omvat diverse voorschriften ten aanzien van de “veiligheid van de netwerkexploitatie” (op te vatten als de beschikbaarheid van netwerken bij calamiteiten) en de “netwerkintegriteit” (de waarborging van de normale werking van gekoppelde netwerken)[24]. De Commissie heeft in juli 2000 voorstellen gedaan voor een nieuw regelgevingskader voor elektronische communicatiediensten (die nu

---

20 http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm#HD_NM_15

21 PB C 364 van 18.12.2000, http://ue.eu.int/df/default.asp?lang=nl.

22 Richtlijn 95/46/EG (PB L 281 van 23.11.1995) en Richtlijn 97/66/EG (PB L 24 van 30.1.1998) http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

23 “De lidstaten garanderen in hun nationale reglementering het vertrouwelijk karakter van oproepen via het openbare telecommunicatienetwerk en via algemeen beschikbare telecommunicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van gesprekken door anderen dan de gebruikers, indien de betrokken gebruikers daarmee niet hebben ingestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 14, lid 1.”

24 De Liberaliseringsrichtlijn 90/388/EG, de Interconnectierichtlijn 97/33/EG en de Spraaktelefonie-richtlijn 98/10/EG.

medebeslissingsprocedure doorlopen en dus ter behandeling bij het Europees Parlement en de Raad liggen). In deze voorstellen van de Commissie zijn de huidige voorschriften ten aanzien van netwerkveiligheid en –integriteit in essentie – zij het gewijzigd – overgenomen.

Het huidige regelgevingskader heeft, benevens op de specifieke thema's van elk van de genoemde teksten, dus ook betrekking op bepaalde aspecten van netwerken en informatiesystemen waarop in deze mededeling is ingegaan.

De **mededeling inzake computercriminaliteit** heeft geleid tot een discussie in de Europese Unie over de wijze waarop criminele activiteiten met behulp van computers en elektronische netwerken dienen te worden bestreden. De besprekingen tussen alle betrokken partijen zullen worden voortgezet in het kader van het EU-Forum, dat binnenkort zal worden opgericht zoals al is aangekondigd in de mededeling van de Commissie over computercriminaliteit. Het strafrecht van de lidstaten dient van toepassing te zijn op ongeoorloofde toegang tot computernetwerken, met inbegrip van de schending van de veiligheid van persoonlijke gegevens. Momenteel is er in de Europese Unie wat dit betreft geen sprake van enige convergentie van het strafrecht. Dit kan leiden tot problemen bij het onderzoek naar dit soort delicten en er gaat geen sterke afschrikkende werking van uit op degenen die hacking-plannen hebben of van zins zijn soortgelijke activiteiten te ontplooien. De harmonisatie van het strafrecht op het stuk van inbraak in computernetwerken is ook van belang om de gerechtelijke samenwerking tussen de lidstaten te vereenvoudigen.

De gerechtvaardigde ongerustheid over computercriminaliteit maakt een doeltreffende opsporing noodzakelijk. Dergelijke overwegingen van juridische aard mogen evenwel niet leiden tot oplossingen waarbij de juridische behoeften tot een verzwakking van de veiligheid van communicatie- en informatiesystemen leiden.

Voorgestelde maatregelen:

- Er dient een gemeenschappelijk inzicht te worden verworven in de juridische implicaties van de veiligheid van elektronische communicatie. Daartoe zal de Commissie een inventarisatie maken van nationale maatregelen die in overeenstemming met het relevante Gemeenschapsrecht zijn getroffen.

- De lidstaten en de Commissie dienen het vrij verkeer van encryptieproducten en –diensten te blijven steunen door middel van een verdere harmonisatie van de administratieve uitvoerprocedures en een verdere versoepeling van de uitvoerbeperkingen.

- De Commissie zal in het kader van titel VI van het Verdrag betreffende de Europese Unie een voorstel doen voor een regelgevingsinstrument dat gericht is op de convergentie van het nationale strafrecht op het stuk van computerdelicten zoals hacking en denial-of-service aanvallen.

3.7. Veiligheid van toepassingen bij de overheid

Het actieplan *e*Europe 2002 is erop gericht een meer doeltreffende en efficiënte interactie tussen burgers en overheden te stimuleren. Omdat een groot deel van de informatie-uitwisseling tussen burgers en overheden een persoonlijk of vertrouwelijk (medisch, financieel, juridisch, enz.) karakter heeft, is de beveiliging essentieel voor een geslaagde introductie. Bovendien maakt de ontwikkeling van de elektronische overheid overheidsdiensten enerzijds tot potentiële **modelvoorbeelden van doeltreffende veilige**

oplossingen en anderzijds tot marktspelers die de ontwikkelingen via hun aankoopbeleid richting kunnen geven.

Overheidsdiensten zouden zich niet tevreden moeten stellen met de aankoop van informatie- en communicatietechnologie die aan de veiligheidseisen voldoet, maar zouden ook een veiligheidscultuur binnen de organisatie moeten ontwikkelen. Dit kan worden bereikt door de ontwikkeling van een "veiligheidsbeleid van de organisatie", afgestemd op de behoeften van de instelling.

Voorgestelde maatregelen:

- De lidstaten dienen de toepassing van doeltreffende en interoperabele oplossingen voor de beveiliging van informatie te beschouwen als een randvoorwaarde voor activiteiten op het gebied van de elektronische overheid (e-government) en het elektronisch aankoopbeleid (e-procurement).

- De lidstaten dienen de bij het aanbieden van on-line overheidsdiensten het gebruik van de elektronische handtekening mogelijk te maken.

- In het kader van de "e-Commissie" dient de Commissie een reeks maatregelen te nemen zodat hogere veiligheidseisen kunnen worden gesteld aan haar informatie- en communicatiesystemen.

3.8. Internationale samenwerking

Communicatiesignalen overschrijden via netwerken grenzen in een fractie van een seconde, maar hetzelfde geldt voor de bijbehorende veiligheidsproblemen. Een netwerk is zo sterk als de zwakste schakel en Europa kan zichzelf niet isoleren van de rest van het wereldwijde netwerk. Daarom is voor de aanpak van de veiligheidsproblematiek internationale samenwerking vereist.

De Europese Commissie levert nu al een bijdrage aan de werkzaamheden van internationale fora, zoals de G8, de OESO en de VN. De particuliere sector pakt de veiligheidsproblematiek aan binnen hun eigen organisaties zoals de Global Business Dialogue (http://www.GBDe.org) en het Global Internet Project (http://www.GIP.org). Een permanente dialoog tussen deze organisaties is van essentieel belang voor wereldwijde veiligheid.

Voorgestelde maatregel:

- De Commissie zal een intensievere dialoog gaan voeren met internationale organisaties en partners op het gebied van netwerkveiligheid, in het bijzonder wat betreft de groeiende afhankelijkheid van elektronische netwerken.

4. Toekomstige stappen

In deze mededeling wordt de strategie geschetst voor het optreden op dit terrein. Het is niet meer dan een eerste stap, die nog geen definitief actieplan voor netwerkveiligheid in Europa biedt. Toch worden al suggesties gedaan die tot een raamwerk voor een gemeenschappelijke Europese benadering moeten leiden. De volgende fase is dat de lidstaten en het Europees Parlement zich over dit raamwerk en de voorgestelde maatregelen gaan buigen. De Europese Raad van Göteborg van 15/16 juni kan wellicht de richting aangeven waarin dit beleid zich in de toekomst moet gaan ontwikkelen.

De Commissie stelt voor een uitvoerige discussie met de industrie, de gebruikers en de voor gegevensbescherming verantwoordelijke instanties te voeren over de praktische bijzonderheden betreffende de tenuitvoerlegging van de voorgestelde maatregelen. Reacties kunnen tot eind augustus 2001 worden toegezonden aan eeurope@cec.eu.int. Daarom dient deze mededeling te worden opgevat als een uitnodiging aan het adres van de belanghebbenden om reacties in te dienen zodat een definitieve en concrete reeks van maatregelen kan worden vastgesteld. Dit zou kunnen gebeuren in de vorm van een "roadmap", die voor eind 2001 klaar zou moeten zijn.

***