COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN

Brussel, 31.5.2006
COM(2006) 251 definitief

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

Een strategie voor een veilige informatiemaatschappij – "Dialoog, partnerschap en empowerment"

{SEC(2006) 656}

INHOUD

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

Een strategie voor een veilige informatiemaatschappij – "Dialoog, partnerschap en empowerment"

1. INLEIDING

In de mededeling "i2010 – Een Europese informatiemaatschappij voor groei en werkgelegenheid" [1] is de aandacht gevestigd op het belang van netwerk- en informatieveiligheid voor de realisatie van een grote Europese informatieruimte. Beschikbaarheid, betrouwbaarheid en beveiliging van netwerken en informatiesystemen spelen in de economie en de samenleving een steeds grotere rol.

Het doel van deze mededeling is de strategie van de Europese Commissie, die in 2001 in de "Mededeling over netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak"[2] is ontvouwd, een nieuwe impuls te geven. In de onderhavige mededeling wordt de stand van zaken met betrekking tot de beveiliging van de informatiemaatschappij opgemaakt en wordt bepaald welke aanvullende stappen nodig zijn om de netwerk- en informatieveiligheid te verbeteren.

Het is de bedoeling om, voortbouwend op de ervaringen van de lidstaten en de Europese Gemeenschap, in Europa tot een dynamische, algemene strategie te komen die op een veiligheidscultuur is gebaseerd en op **dialoog, partnerschap en empowerment** berust.

De Europese Gemeenschap heeft een drieledige benadering ontwikkeld voor de aanpak van veiligheidsrisico's in de informatiemaatschappij: specifieke netwerk- en informatie-beveiligingsmaatregelen, een regelgevingskader voor elektronische communicatie (met inbegrip van regels inzake privacy- en gegevensbescherming) en bestrijding van computercriminaliteit. Ofschoon deze drie aspecten tot op zekere hoogte afzonderlijk kunnen worden ontwikkeld, noopt hun onderlinge samenhang tot een gecoördineerde strategie. In deze mededeling wordt een dergelijke strategie ontvouwd. Voorts biedt zij een raamwerk voor de ontwikkeling van een samenhangende benadering voor netwerk- en informatieveiligheid.

In de mededeling uit 2001 is netwerk- en informatieveiligheid gedefinieerd 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"*. In de afgelopen jaren heeft de Europese Gemeenschap een aantal maatregelen getroffen om de netwerk- en informatieveiligheid te verhogen.

---

[1] COM(2005) 229 def. van 1.6.2005.

[2] COM(2001) 298 def. van 6.6.2001.

Het regelgevingskader voor elektronische communicatie, dat momenteel wordt herzien, omvat een aantal voor de veiligheid relevante voorschriften. In het bijzonder zijn aanbieders van openbare elektronische communicatiediensten volgens de Richtlijn betreffende privacy en elektronische communicatie [3] ertoe verplicht hun diensten te beveiligen. Ook zijn er voorschriften tegen spam[4] en spyware[5] vastgesteld.

Betrouwbaarheid en beveiliging spelen een belangrijke rol in de onderzoek- en ontwikkelingsprogramma's van de Europese Gemeenschap. In het zesde kaderprogramma is dit het thema van allerlei projecten. Het veiligheidsgerelateerd onderzoek wordt bij het zevende kaderprogramma nog uitgebreid met een Europees programma voor veiligheidsonderzoek (ESRP)[6]. Bovendien wordt in het kader van het programma Safer Internet Plus steun gegeven aan netwerkprojecten en uitwisseling van beste praktijken om de overdracht van schadelijke inhoud via informatienetwerken te bestrijden.

Om een antwoord te vinden op de veiligheidsrisico's heeft de Europese Gemeenschap in 2004 besloten het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) op te richten. Het ENISA draagt bij tot de ontwikkeling van een cultuur van netwerk- en informatiebeveiliging waarvan burgers, consumenten, ondernemingen en openbare instellingen in de gehele Europese Unie (EU) profijt hebben.

De EU speelt ook een actieve rol binnen internationale fora die zich met deze thematiek bezighouden, zoals de OESO, de Raad van Europa en de VN. Op de Wereldtop over de informatiemaatschappij in Tunis heeft de EU een forse bijdrage geleverd aan de discussie over de beschikbaarheid, betrouwbaarheid en beveiliging van netwerken en informatie. In de Tunis-agenda[7], die samen met de Verbintenis van Tunis de door de wereldleiders aanvaarde blauwdruk voor de toekomst van de beleidsdiscussie over de wereldwijde informatiemaatschappij vormt, wordt aangedrongen op voortzetting van de strijd tegen computercriminaliteit en spam, evenwel zonder dat dit ten koste van de privacy en de vrijheid van meningsuiting mag gaan. Voorts dient een gemeenschappelijk inzicht te worden gekweekt in internetveiligheidskwesties en moet er beter worden samengewerkt om de inzameling en de verspreiding van veiligheidsgerelateerde informatie, alsmede de onderlinge uitwisseling van goede praktijken over maatregelen tegen de veiligheidsrisico's tussen alle stakeholders te bevorderen.

2. NAAR EEN VEILIGERE INFORMATIEMAATSCHAPPIJ: DE VOORNAAMSTE UITDAGINGEN

Ondanks de inspanningen in internationaal, Europees en nationaal verband blijft de veiligheid een probleempunt.

In de eerste plaats worden aanvallen op informatiesystemen steeds vaker ingegeven door winstbejag in plaats van vandalisme. Gegevens worden illegaal onderschept, meer en meer

---

3 Richtlijn 2002/58/EG.

4 Ongevraagde commerciële berichten.

5 Spyware is spionagesoftware die geïnstalleerd wordt zonder dat de gebruiker daarvan op de hoogte is gesteld, daarvoor toestemming heeft verleend of daarop invloed heeft.

6 In het kader van de Voorbereidende actie voor veiligheidsonderzoek worden in de periode 2004-2006 voorbereidingen voor het ESPR getroffen.

7 *Naar een wereldwijd partnerschap in de informatiemaatschappij: Follow-up van de Tunis-fase van de Wereldtop over de informatiemaatschappij (WSIS)*, COM(2006) 181 def. van 27.4.2006.

zonder dat de gebruiker daar weet van heeft, terwijl de variatie in malware[8]-programma's steeds groter wordt. Spam is een goed voorbeeld van deze ontwikkelingen: spam wordt gebruikt als drager voor de overdracht van virussen en voor frauduleuze en criminele activiteiten, zoals spyware, phishing[9] en andere vormen van malware. De wijde verspreiding ervan is steeds vaker te danken aan botnets[10], d.w.z. netwerken van gekaapte servers en pc's die zonder medeweten van hun eigenaars gebruikt worden voor de verzending van spam.

De steeds grote populariteit van mobiele toestellen (zoals 3G-telefoons, draagbare videospelletjes, enz.) en dienstverlening via mobiele netwerken zorgt voor nieuwe problemen, aangezien de op IP gebaseerde diensten zich in hoog tempo ontwikkelen. Uiteindelijk zouden zij wel eens een aantrekkelijker kanaal voor aanvallen kunnen blijken dan pc's, die doorgaans al redelijk goed beveiligd zijn. Alle nieuwe communicatieplatforms en informatiesystemen bieden immers onvermijdelijk nieuwe mogelijkheden voor mensen met kwade bedoelingen.

Een andere belangrijke ontwikkeling is de opkomst van "omgevingsintelligentie", waardoor op computer- en netwerktechnologie steunende intelligente elementen overal in onze omgeving doordringen (zoals RFID[11], IPv6 en sensornetwerken). Door dit soort bouwstenen onderling te koppelen en in netwerken op te nemen ontstaan er in het leven van alledag tal van nieuwe mogelijkheden. Maar er ontstaan ook nieuwe veiligheids- en privacyrisico's. Ofschoon gemeenschappelijke platforms en applicaties de compatibiliteit en acceptatie van informatie- en communicatietechnologie (ICT) verhogen, kunnen zij ook risico's opleveren. Hoe meer er van confectiesoftware gebruik wordt gemaakt, des te groter het effect wanneer beveiligingslekken worden misbruikt of er storingen optreden. Door een zekere "monocultuur" op het gebied van besturingssystemen en toepassingen worden de groei en de verspreiding van veiligheidsbedreigingen zoals malware en virussen in de hand gewerkt. **Diversificatie, openheid en interoperabiliteit zijn onmisbare ingrediënten voor een goede beveiliging en moeten daarom worden gestimuleerd.**

De relevantie van de ICT-sector voor de Europese economie en voor de Europese samenleving in haar geheel staat buiten kijf. De ICT is een kritische component van de innovatie die verantwoordelijk is voor bijna 40% van de productiviteitsstijging. Bovendien neemt deze uiterst innovatieve sector meer dan een kwart van al het O&O in Europa voor zijn rekening en fungeert hij als motor voor de economische groei en de werkgelegenheid in de gehele economie. Steeds meer Europeanen leven in een echte, op informatie gebaseerde maatschappij waarin het gebruik van ICT een hoge vlucht heeft genomen en een spilfunctie vervult in het sociaal en economisch intermenselijk verkeer. Volgens Eurostat maakte 89% van de EU-bedrijven in 2004 actief gebruik van internet, terwijl ongeveer 50% van de consumenten nog recentelijk van internet gebruik had gemaakt[12].

Een lek in de netwerk- en informatiebeveiliging kan een effect hebben dat uitstijgt boven de economische dimensie. Algemeen wordt gevreesd dat veiligheidsproblemen de gebruiker ontmoedigen en een negatief effect hebben op de acceptatie van ICT, terwijl beschikbaarheid,

---

8 Malware is een synoniem van "kwaadaardige" software.

9 Phishing is een vorm van internetfraude waarbij waardevolle informatie zoals kredietkaartgegevens, bankrekeningnummers, gebruikeridentificaties en paswoorden aan de gebruiker worden ontfutseld.

10 Botnets zijn netwerken van bots: applicaties die in opdracht van een op een ander systeem draaiend programma op de machine van het slachtoffer allerlei taken uitvoeren en die ongemerkt op die machine zijn geïnstalleerd.

11 Identificatie met behulp van radiogolven (Radio Frequency Identification).

12 Eurostat, *Internetactiviteiten in de Europese Unie*, 40/2005.

betrouwbaarheid en veiligheid randvoorwaarden zijn voor het garanderen van de fundamentele rechten in de online-omgeving.

Omdat netwerken steeds vaker met elkaar zijn gekoppeld, worden andere kritische infrastructuurvoorzieningen (zoals het vervoers- en het elektriciteitsnet) eveneens meer en meer afhankelijk van de goede werking van de bijbehorende informatiesystemen.

De risico's worden in Europa nog steeds onderschat, zowel door bedrijven als door particulieren. Daar zijn verschillende redenen voor. Voor bedrijven is de belangrijkste de slechte zichtbaarheid van de winst op investeringen in beveiliging. Voor particulieren komt het vooral omdat zij zich niet bewust zijn van hun rol in de totale veiligheidsketen.

Vanwege de alomtegenwoordigheid van ICT en informatiesystemen, is netwerk- en informatieveiligheid een taak voor iedereen:

- **Overheidsinstellingen** moeten hun systemen beveiligen, niet alleen om publieke-sectorinformatie te beschermen maar ook om anderen het goede voorbeeld te geven.

- **Bedrijven** moeten netwerk- en informatieveiligheid meer gaan zien als een productiemiddel en concurrentievoordeel dan als een kostenpost.

- **Particulieren** dienen te beseffen dat hun computersysteem thuis een kritische rol speelt in de totale "veiligheidsketen".

Om de geschetste problemen het hoofd te bieden hebben alle betrokkenen betrouwbare informatie nodig over incidenten en trends op het gebied van informatieveiligheid. Betrouwbare en complete gegevens over incidenten zijn evenwel moeilijk te verkrijgen. Daarvoor zijn allerlei redenen, variërend van de snelheid waarmee dergelijke incidenten zich soms aandienen tot de geringe bereidheid van bepaalde organisaties om er ruchtbaarheid aan te geven. Toch is **verbetering van ons inzicht in de problematiek** een van de hoekstenen van de ontwikkeling van een veiligheidscultuur.

Het is belangrijk dat bewustmakingscampagnes die de veiligheidsrisico's onder de aandacht moeten brengen, niet het vertrouwen van de consument en de gebruiker ondermijnen door alleen op de negatieve aspecten van beveiliging te wijzen. Waar mogelijk **moet netwerk- en informatieveiligheid worden gepresenteerd als een aanwinst en een niet te missen kans** in plaats van als een risico- en kostenfactor. Netwerk- en informatieveiligheid dient te worden gezien als een middel om het vertrouwen van de consument te winnen, als een concurrentievoordeel voor bedrijven die informatiesystemen gebruiken en als een uiting van de dienstkwaliteit voor zowel openbare als particuliere dienstverleners.

De grootste uitdaging voor de beleidsmakers is om tot een totaalaanpak te komen. Bij een dergelijke aanpak moet de eigen rol van de diverse belanghebbenden op waarde worden geschat. Daarbij moet er worden gezorgd voor een goede coördinatie van overheidsbeleid en wettelijke bepalingen met directe of indirecte gevolgen voor de netwerk- en informatieveiligheid. De liberalisering, deregulering en convergentie hebben ertoe geleid dat hier tal van spelers bij betrokken moeten worden, hetgeen de zaak er niet eenvoudiger op maakt. Het ENISA kan een belangrijke bijdrage aan deze doelstelling leveren. Het zou kunnen fungeren als een centrum voor het poolen van informatie, voor samenwerking tussen alle betrokkenen en voor uitwisseling van aan te bevelen praktijken, zowel binnen Europa als

met de rest van de wereld, teneinde een bijdrage te leveren aan het concurrentievermogen van onze ICT-industrie en aan de goede werking van de interne markt.

3. NAAR EEN DYNAMISCHE BENADERING GERICHT OP EEN VEILIGE INFORMATIEMAATSCHAPPIJ

Een veilige informatiemaatschappij steunt op **uitgebreide netwerk- en informatieveiligheid** en een alom gevolgde **veiligheidscultuur**. Daarom doet de Europese Commissie een voorstel voor een **dynamische en geïntegreerde benadering** waarbij alle spelers worden betrokken en die gebaseerd is op **dialoog, partnerschap en empowerment**. Omdat de openbare en de particuliere sector elkaar aanvullen als het op het creëren van een veiligheidscultuur aankomt, dienen de beleidsinitiatieven op dit terrein te worden gebaseerd op een **open en inclusieve dialoog tussen diverse partijen**.

Deze benadering en de bijbehorende acties dienen ter aanvulling en verrijking van het plan van de Commissie om de ontwikkeling van een compleet en dynamisch beleidskader in 2006 voort te zetten door:

(1) de ontwikkelingen ten aanzien van spam en andere dreigingen, zoals spyware en andere vormen van malware, in een speciale mededeling hierover aan de orde te stellen;

(2) voorstellen te doen om de samenwerking tussen handhavingsautoriteiten te verbeteren en nieuwe vormen van internetcriminaliteit die de werking van kritische infrastructuurnetwerken ondermijnen, aan te pakken. Dit onderwerp zal aan bod komen in een specifieke mededeling over internetcriminaliteit.

Deze beleidsinitiatieven vormen tevens een aanvulling op de activiteiten die worden gepland om de doelstellingen te realiseren van het Groenboek van de Commissie betreffende een Europees programma voor de bescherming van kritieke infrastructuur (EPCIP)[13], dat op verzoek van de Raad van december 2004 is opgesteld. Dit groenboek zal waarschijnlijk in een actieplan resulteren waarbij een overkoepelende benadering voor bescherming van kritieke infrastructuur wordt gecombineerd met een sectorspecifiek beleid, onder meer voor de ICT-sector. Het sectorspecifieke beleid voor de ICT-sector moet door middel van een **dialoog tussen diverse partijen** de relevante economische, zakelijke en maatschappelijke factoren onderzoeken om de veiligheid te verhogen en netwerken en informatiesystemen robuuster te maken.

Bovendien zal bij de herziening van het regelgevingskader voor elektronische communicatie in 2006 ook rekening worden gehouden met aspecten die tot een betere netwerk- en informatieveiligheid kunnen leiden, zoals technische en organisatorische maatregelen die dienstverleners moeten nemen, een meldplicht voor veiligheidsincidenten, alsmede specifieke instrumenten en sancties voor wanneer de verplichtingen niet worden nagekomen.

Het is vooral aan de particuliere sector om eindgebruikers oplossingen, diensten en beveiligingsproducten aan te bieden. Daarom is het van strategisch belang dat **de Europese industrie zich enerzijds als veeleisende gebruiker** van beveiligingsproducten en -diensten

[13] COM(2005) 576 def. van 17.11.2005.

opstelt en **anderzijds als concurrerende leverancier** van netwerk- en informatiebeveiligingsproducten.

Nationale overheden moeten een inventaris van beste praktijken kunnen maken en deze in de beleidsontwikkeling kunnen opnemen. Daarnaast moeten zij laten zien dat het hun ernst is met deze beleidsdoelstellingen door hun eigen informatiesystemen op veilige wijze te beheren. Voor overheidsinstellingen in de lidstaten en op EU-niveau is er een belangrijke taak weggelegd bij de voorlichting van de gebruikers zodat die zelf een bijdrage kunnen leveren aan hun eigen veiligheid en beveiliging. Prioriteit moet worden verleend aan voorlichting over netwerk- en informatieveiligheidskwesties en het via speciale webportaals voor e-veiligheid tijdig verstrekken van nuttige informatie over dreigingen, risicofactoren, waarschuwingen en beste praktijken. Een belangrijk doel van het ENISA zou daarom kunnen zijn een onderzoek te doen naar de haalbaarheid van de **oprichting van een Europees meertalig informatie-uitwisselings- en waarschuwingssysteem** door uitbreiding en bundeling van bestaande en geplande nationale publieke en particuliere initiatieven.

De mondiale dimensie van netwerk- en informatieveiligheid stelt de Commissie voor de uitdaging om de **wereldwijde samenwerking op het gebied van netwerk- en informatieveiligheid**, zowel in internationaal verband als wat betreft de coördinatie met de lidstaten, beter te promoten. Zij zal zich daartoe met name richten op de uitvoering van de Tunis-agenda, die is vastgesteld op de Wereldtop over de informatiemaatschappij (WSIS) in november 2005.

Ten slotte zal O&O, vooral in EU-verband, helpen nieuwe en innovatieve partnerschappen te ontwikkelen om de groei van de Europese ICT-industrie in het algemeen en de Europese ICT-beveiligingsindustrie in het bijzonder een impuls te geven. De Commissie zal daarom trachten voor voldoende financiële middelen te zorgen voor het onderzoek naar netwerk- en informatieveiligheid en betrouwbaarheidstechnologie in het bestek van het zevende EU-kaderprogramma.

3.1. Dialoog

3.1.1. *Als een eerste stap ter verbetering van de dialoog tussen overheden stelt de Commissie voor* ***het nationaal beleid ten aanzien van netwerk- en informatieveiligheid****, waaronder het specifiek voor de overheidssector bestemde beveiligingsbeleid, te* ***benchmarken****. Daarmee kunnen de meeste efficiënte praktijken worden opgespoord, waardoor deze in de EU ook breder kunnen worden toegepast en overheidsinstellingen zich tot motor voor de verspreiding van beste praktijken op beveiligingsgebied kunnen ontwikkelen. Zo zouden de activiteiten op het gebied van elektronische identificatie in het recente actieplan voor de elektronische overheid in dit verband een belangrijke rol kunnen spelen.*

Bij een goede opzet zal een dergelijke benchmarking-operatie duidelijk maken wat de **beste praktijken zijn om het MKB en de bevolking ervan te doordringen** dat zij zelf ook iets moeten doen aan hun specifieke problemen, behoeften en capaciteiten ten aanzien van netwerk- en informatieveiligheid. Op het ENISA moet een beroep worden gedaan om in deze dialoog en bij de consolidatie en uitwisseling van beste praktijken een actieve rol te spelen.

3.1.2. *De* ***diverse partijen moeten een gestructureerd debat gaan voeren*** *over de beste manier om bestaande hulpmiddelen en wetgevingsinstrumenten te gebruiken om een*

goed maatschappelijk evenwicht te vinden tussen beveiliging enerzijds en grondrechten, zoals het recht op privacy, anderzijds. De geplande conferentie "i2010 - Naar een alomtegenwoordige Europese informatiemaatschappij", die door het aanstaande Finse Voorzitterschap zal worden georganiseerd, en de raadpleging over de gevolgen van RFID voor veiligheid en privacy in het kader van een onlangs door de Commissie gestarte bredere raadpleging, zullen een bijdrage aan dit debat leveren. Bovendien zal de Commissie een tweetal activiteiten organiseren:

- een evenement voor het bedrijfsleven dat de industrie ertoe moet bewegen een doeltreffende aanpak te volgen voor de invoering van een veiligheidscultuur in de **industrie**;

- een seminar over manieren om de alertheid op beveiligingsproblemen te verhogen en het vertrouwen van **eindgebruikers** in het gebruik van elektronische netwerken en informatiesystemen op te vijzelen.

3.2. Partnerschap

3.2.1. Voor een doeltreffende beleidsvorming dient een goed inzicht te worden verworven in de aard en omvang van de uitdagingen. Daarvoor zijn betrouwbare en actuele statistische en economische gegevens nodig, niet alleen met betrekking tot netwerk- en informatieveiligheidsincidenten en het vertrouwen van de consument en de gebruiker, maar ook over de omvang van en de trends in de ICT-beveiligingsindustrie in Europa. De Commissie is voornemens het ENISA te vragen ***met de lidstaten en de betrokken partijen tot een partnerschap van vertrouwen te komen*** *teneinde een* ***raamwerk voor de inzameling van gegevens*** *te creëren, met inbegrip van de procedures en mechanismen voor de inzameling en analyse van gegevens over veiligheidsincidenten en consumentenvertrouwen in Europa.*

Tegelijkertijd zal de Commissie vanwege de sterke versnippering en het specifieke karakter van de EU-markt een beroep doen op de lidstaten, de particuliere sector en de onderzoekswereld om **een strategisch partnerschap op te richten.** Dit moet ervoor zorgen dat er gegevens beschikbaar worden gesteld over de ICT-beveiligingsindustrie en over de nieuwe markttrends voor producten en diensten.

3.2.2. Om Europa beter in staat te stellen op netwerkveiligheidsrisico's te reageren, zal de Commissie het ENISA vragen te onderzoeken of het haalbaar is een ***Europees informatie-uitwisselings- en waarschuwingssysteem*** *op te zetten dat doeltreffend kan reageren op bestaande en nieuwe bedreigingen voor elektronische netwerken. Een van de eisen die aan een dergelijk systeem moeten worden gesteld is het opzetten van een* ***meertalig EU-webportaal****, dat op maat gesneden informatie over dreigingen, risico's en waarschuwingen verschaft.*

3.3. Empowerment

Eigen verantwoordelijkheid is voor elke belangengroep een randvoorwaarde om alert te blijven op beveiligingsbehoeften en -risico's.

*3.3.1. Daarom verzoekt de Commissie de **lidstaten**:*

- actief deel te nemen aan de voorgestelde benchmarking-operatie voor het nationale beleid ten aanzien van netwerk- en informatieveiligheid;

- in nauwe samenwerking met het ENISA voorlichting te geven over de voordelen van doeltreffende beveiligingstechnieken, -praktijen en -gedrag;

- de uitrol van e-overheidsdiensten te stimuleren om goede beveiligingspraktijken onder de aandacht te brengen en te promoten en die vervolgens naar andere sectoren uit te breiden;

- te stimuleren dat in de onderwijsprogramma's voor het hoger onderwijs meer aandacht wordt geschonken aan de ontwikkeling van netwerk- en informatiebeveiligingsprogramma's.

3.3.2. *De Commissie verzoekt de **particuliere sector** voorts:*

- duidelijk vast te leggen wat de verantwoordelijkheden van software-ontwikkelaars en internetaanbieders zijn voor wat betreft het garanderen van een adequaat en controleerbaar niveau van beveiliging. In dit verband moet er steun worden verleend voor gestandaardiseerde processen om onderling overeengekomen beveiligingsnormen en beste praktijken in acht te kunnen nemen;

- verscheidenheid, openheid, interoperabiliteit, bruikbaarheid en concurrentie te promoten als drijvende krachten voor beveiliging en de uitrol van beveiligingsproducten, -processen en -diensten te stimuleren om identiteitsroof en andere aanvallen met inbreuk op de privacy te bestrijden;

- goede beveiligingspraktijken voor netwerkexploitanten, dienstverleners en kleine en middelgrote ondernemingen te verspreiden om een basisniveau van beveiliging en bedrijfscontinuïteit te bieden;

- opleidingsprogramma's onder de aandacht van het bedrijfsleven te brengen, in het bijzonder het MKB, om de kennis en bedrevenheid van werknemers te verbeteren die nodig zijn om beveiligingsmaatregelen doeltreffend te kunnen toepassen;

- te streven naar betaalbare oplossingen voor de certificering van beveiligingsproducten, -processen en -diensten (met name gelet op de privacy);

- de verzekeringssector te betrekken bij de ontwikkeling van geschikte risicobeheersingsinstrumenten waarmee ICT-gerelateerde risico's kunnen worden aangepakt en waarmee de risicobeheersingscultuur in organisaties en bedrijven (in het bijzonder het MKB) wordt gestimuleerd.

4. CONCLUSIES

Voor het opsporen en oplossen van beveiligingsrisico's voor informatiesystemen en netwerken in de EU moet op de volledige inzet van alle betrokkenen kunnen worden gerekend. Met de in deze mededeling geschetste beleidsbenadering wordt getracht dit te bereiken door

een **krachtdadig gemeenschappelijk optreden van de diverse betrokken partijen**. Dit houdt in dat op wederzijdse belangen wordt voortgebouwd, de taken van elkeen duidelijk worden omschreven en een dynamisch raamwerk wordt gecreëerd om de doeltreffendheid van de beleidsontwikkeling door de overheden en initiatieven van de particuliere sector te promoten.

De Commissie zal medio 2007 aan de Raad en het Parlement verslag uitbrengen over de gestarte activiteiten, de voorlopige bevindingen en de stand van zaken voor de afzonderlijke initiatieven, bijv. die van het ENISA, de lidstaten en de particuliere sector. Zo nodig zal de Commissie met een voorstel komen voor een aanbeveling inzake netwerk- en informatieveiligheid.