Stanovisko Evropského hospodářského a sociálního výboru ke sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“

KOM(2006) 251 v konečném znění

(2007/C 97/09)

Dne 31. května 2006 se Evropská komise, v souladu s článkem 262 Smlouvy o založení Evropského společenství, rozhodla konzultovat Evropský hospodářský a sociální výbor ve věci výše uvedené.

Specializovaná sekce Doprava, energetika, infrastruktura, informační společnost, kterou Výbor pověřil přípravou podkladů na toto téma, přijala stanovisko dne 11. ledna 2007. Zpravodajem byl pan PEZZINI.

Na 433. plenárním zasedání, které se konalo ve dnech 15. a 16. února 2007 (jednání ze dne 16. února 2007), přijal Evropský hospodářský a sociální výbor následující stanovisko 132 hlasy pro, 2 členové se zdrželi hlasování.

1. **Závěry a doporučení**

1.1 Výbor je přesvědčen, že problém informační bezpečnosti je předmětem rostoucího zájmu podniků, správy, veřejných orgánů, soukromých subjektů i jednotlivých občanů.

1.2 Výbor v zásadě souhlasí s analýzami a argumenty, které vyžadují novou strategii zvýšení zabezpečení sítí a informací proti útokům a vniknutím, která nemají zeměpisné hranice.

1.3 Výbor se domnívá, že vzhledem k šíři fenoménu a jeho důsledkům pro ekonomiku i soukromý život by Komise měla vynaložit větší úsilí na uskutečnění inovační a jasné strategie.

1.3.1 EHSV rovněž zdůrazňuje, že Komise nedávno předložila nové sdělení o informační bezpečnosti a že by v krátké době měl být vypracován nový dokument o stejném tématu. Výbor si vyhrazuje, že se v budoucnosti k tomuto tématu vyjádří podrobněji v samostatném stanovisku, které zohlední všechna sdělení.

1.4 Výbor zdůrazňuje, že aspekt informační bezpečnosti nemůže být jakkoli oddělován od posilování ochrany osobních dat a od ochrany svobod, což jsou práva zaručovaná Evropskou úmluvou o ochraně lidských práv.

1.5 EHSV si klade otázku, jaká je současná přidaná hodnota návrhu vzhledem k integrovanému přístupu přijatému v roce 2001, jehož cíl se shodoval s cílem uvedeným v tomto sdělení ([1]).

1.5.1 Dokument o posouzení dopadu ([2]), který tvoří přílohu k návrhu, obsahuje oproti situaci v roce 2001 několik zajímavých aktualizací, ale byl uveřejněn jen v jednom jazyce, a není tudíž přístupný mnoha evropským občanům, kteří formulují své závěry na základě oficiálního dokumentu publikovaném v různých jazycích Společenství.

1.6 Výbor se odvolává na závěry o informační společnosti přijaté v roce 2005 na světovém summitu v Tunisu, které byly dne 27. března 2006 podepsány Valným shromážděním OSN:

— nediskriminační přístup,

— podpora IKT jakožto nástroje míru,

— určení nástrojů na posílení demokracie, soudržnosti a řádné správy,

— prevence zneužití v rámci dodržování lidských práv ([3]).

1.7 Výbor zdůrazňuje, že dynamická a integrovaná strategie Společenství by se vedle dialogu, partnerství a posílení účasti mohla zabývat následujícími tématy:

— akce prevence,

— přechod od bezpečnosti k informačnímu pojištění ([4]),

— příprava jasného a uznávaného předpisového a sankčního rámce EU,

— posílení technické normalizace,

([1]) Viz stanovisko EHSV ke sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Bezpečnost sítí a informací – návrh evropského politického přístupu, Úř. věst. C 48, 21.2.2002, s. 33.

([2]) „Dokument o posouzení dopadu“ nemá stejnou hodnotu jako „strategický dokument“.

([3]) OSN 27.3.2006, doporučení č. 57 a 58. Závěrečný dokument z Tunisu č. 15.

([4]) Viz *Emerging technologies in the context of security* CCR – Institut pro ochranu a bezpečnost občana, sešit o strategickém výzkumu, září 2005, Evropská komise, http://serac.jrc.it.

— digitální identifikace uživatelů,

— zavedení evropských analýz a předvídání (*foresight*) informační bezpečnosti v podmínkách multimodálního sbližování technologií,

— posílení mechanismů posouzení rizik na evropské i národní úrovni,

— činnosti zaměřené na zamezení vzniku informačních monokultur,

— posílení koordinace Společenství na evropské a mezinárodní úrovni,

— zřízení bezpečnostního střediska IKT mezi generálními ředitelstvími *(ICT Security Focal Point),*

— vytvoření evropské sítě pro bezpečnost sítí a informací (*European Network and Information Security Network*),

— optimalizace role evropského výzkumu v informační bezpečnosti,

— zřízení „evropského dne bezpečného počítače“,

— organizování pilotních akcí Společenství k tématu informační bezpečnosti na školách různých druhů a stupňů.

1.8 EHSV se konečně domnívá, že v zájmu zajištění dynamické a integrované strategie Společenství by měly být vyčleněny přiměřené finanční dotace z rozpočtu a stanoveny výraznější koordinační iniciativy a akce na úrovni Společenství, které by v globálním kontextu byly schopny jednotně představovat Evropu.

2. **Odůvodnění**

2.1 Výzvy, které představuje bezpečnost informační společnosti, mají zásadní význam pro zajištění důvěry a spolehlivosti sítí a komunikačních služeb, což jsou kritické faktory rozvoje hospodářství a společnosti.

2.2 Sítě a informační systémy musí být chráněny, aby si udržely svoji konkurenční a obchodní schopnost, aby zabezpečily integritu a kontinuitu elektronické komunikace, aby předcházely podvodům a aby zaručily právní ochranu soukromého života.

2.3 Elektronická komunikace a služby, které s ní souvisí, představují nejširší úsek celého odvětví telekomunikací. V roce 2004 využívalo přibližně 90 % evropských podniků aktivně internet a 65 % z nich vytvořilo vlastní webové stránky, zatímco se odhaduje, že přibližně polovina evropského obyvatelstva pravidelně využívá internet a 25 % rodin soustavně využívá širokopásmové připojení ([5]).

2.4 Vzhledem k rychlému rozvoji investic představuje objem výdajů za bezpečnost jen 5 až 13 % veškerých investic do informačních technologií. Toto procento je očividně rozhodně příliš nízké. Nedávné studie prokázaly, že z průměrného počtu 30 protokolů, které sdílejí klíčové struktury, je 23 zranitelných před útoky více protokolů ([6]). Počet elektronických spamů ([7]), které jsou průměrně denně posílány, se odhaduje na 25 milionů a Výbor je proto potěšen návrhem, který Komise v této souvislosti nedávno předložila.

2.5 V oblasti počítačových virů ([8]) šel rychlý vývoj nejrůznějších červů („*worms*“) ([9]) a špionážních softwarů („*spyware*“) ([10]) ruku v ruce s velkým rozvojem systémů a sítí elektronické komunikace. Ty jsou stále více složitější a zároveň zranitelné, i v závislosti na sbližování multimédií a mobilních telefonů i systémů *GRID infoware* ([11]). Dalšími výzvami pro bezpečnost informační společnosti jsou případy vydírání, DdoS (*Distributed denials of service*), krádeže identity on-line, *phishing* ([12]), pirátství ([13]) a tak dále. Evropské společenství se již tímto problémem zabývalo ve svém sdělení z roku 2001 ([14]), ke kterému měl Výbor možnost se vyjádřit ([15]), a nyní navrhuje strategii se třemi druhy opatření:

— zvláštní bezpečnostní opatření,

([5]) *i2010: strategie pro bezpečnou informační společnost*. Generální ředitelství pro informační společnost a média, „Factsheet 8“ (červen 2006) http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

([6]) *Proceedings of the First International Conference on Availability, Reliability and Security* (ARES'06) – volume 00 ARES 2006 Editore: IEEE Computer Society.

([7]) Spam = nevyžádaná elektronická pošta obchodní povahy. Původní význam slova „spam“ je „*spiced pork and ham*“, což byl za druhé světové války určitý druh konzervy s masem v rosolu, která se – krom toho, že nebyla na příděl – stala hlavním zdrojem potravy amerických jednotek a obyvatel Anglie. Roky a roky takovéto diety jsou příčinou toho, že výraz nabyl záporného významu.

([8]) Počítačový virus je zvláštní typ programu, který patří do skupiny škodlivých softwarů („*malware*“) a který se dokáže sám šířit tím, že vytváří kopie sebe sama, obvykle aniž by to uživatel zaznamenal. Viry více či méně poškozují operační systém, který je hostí, ale i v nejlepším případě jsou spojené s určitým plýtváním zdroji (jako je RAM či CPU) a úbytkem místa na pevném disku (http://cs.wikipedia.org/wiki/Po %C4 %8D %C3 %ADta %C4 % 8Dov %C3 %BD_virus).

([9]) Červ je škodlivý software, který se velmi rychle šíří. „E-mailový červ“ podniká zničující útok na síť, sbírá veškeré e-mailové adresy uložené v místním programu (například MS OUtlook) a těm pak zasílá stovky e-mailů, které obsahují samotného červa v neviditelné příloze.

([10]) Špionážní software je program, který sleduje uživatelovo „surfování“ na internetu a instaluje se sám, aniž by o tom uživatel dostal zprávu nebo si toho byl vědom či s tím souhlasil a zkontroloval.

([11]) *GRID infoware* umožňuje sdílet, vybírat a přidávat široké spektrum zdrojů elektronického zpracování rozmístěných na určitém území (například superpočítač, počítačové bloky, systémy ukládání dat, zdroje dat, nástroje a osoby), které vydává za jednotný a samostatný zdroj pro řešení extrémně složitých výpočtů a zpracovával obzvláště intenzivní data.

([12]) *Phishing* v oblasti informačních technologií znamená podvodnou techniku používanou k získávání osobních a citlivých údajů za účelem krádeže identity prostřednictvím rozesílání falešných e-mailových zpráv vytvářených účelově tak, aby vypadaly jako pravé.

([13]) *Pirátství* je termín užívaný informačními „piráty“ k označení softwaru, kterému byla zcizena ochrana proti neautorizovanému pořizování děl a který je dán k dispozici ke stažení přes internet.

([14]) KOM(2001) 298 v konečném znění.

([15]) Viz poznámka pod čarou č. 1.

— předpisový rámec včetně ochrany dat a soukromí,

— boj proti počítačové trestné činnosti.

2.6 Vzhledem k neustálým změnám v nastavení, rozmanitosti síťových protokolů a nabízených a vyvíjených služeb, jakož i k nesmírné komplexnosti asynchronních útoků ([16]) představuje měření útoků na informační systémy a jejich určování a prevence v oblasti navzájem propojených systémů výzvu pro hledání vhodných řešení.

2.7 Nedostatečná viditelnost návratnosti investic do bezpečnosti a nedostatečné přebírání odpovědnosti na straně občanů – uživatelů jsou však bohužel příčinou podhodnocování rizik a poklesu pozornosti k rozvoji kultury bezpečnosti.

3. **Návrh Komise**

3.1 Svým sdělením o strategii pro bezpečnou informační společnost ([17]) Komise zamýšlí zlepšit informační bezpečnost, a to vytvořením dynamické a integrované strategie založené na:

a) lepším dialogu mezi orgány veřejné správy a Komisí prostřednictvím *benchmarkingu* národních politik a určení osvědčených postupů v bezpečné elektronické komunikaci;

b) intenzivnějším povědomí občanů a MSP o účinných bezpečnostních režimech, s aktivní stimulační rolí Komise a s větším zapojením Evropské agentury pro bezpečnost sítí a informací (ENISA);

c) dialogu o nástrojích a předpisech pro vyvážený vztah mezi bezpečností a základními právy včetně ochrany soukromí.

3.2 Z hlediska vývoje vhodného rámce pro sběr dat o narušování bezpečnosti, o úrovních důvěry uživatelů a o rozvoji odvětví bezpečnosti se mimoto ve sdělení stanovuje navázání partnerství důvěry ENISA:

a) s členskými státy,

b) se spotřebiteli a uživateli,

c) s odvětvím informační bezpečnosti,

d) se soukromým sektorem

prostřednictvím vytvoření mnohojazyčného portálu Společenství pro varování a sdílení informací za účelem strategického partnerství mezi soukromým sektorem, členskými státy a výzkumnými pracovníky.

3.2.1 Sdělení dále stanoví větší účast zúčastněných stran na zvyšování povědomí o potřebách a rizicích v oblasti bezpečnosti.

3.2.2 Pokud jde o mezinárodní spolupráci a spolupráci s třetími zeměmi, „celosvětový rozměr bezpečnosti sítí a informací vybízí Komisi k intenzivnější podpoře celosvětové spolupráce v otázkách bezpečnosti sítí a informací na mezinárodní úrovni a ve spolupráci s členskými státy“ ([18]), avšak v akcích dialogu, partnerství a posílení účasti se tato zmínka neobjevuje.

4. **Připomínky**

4.1 Výbor souhlasí s analýzou a s argumenty, které zdůvodňují integrovanou a dynamickou evropskou strategii pro bezpečnost sítí a informací, neboť otázku bezpečnosti považuje za zásadní pro povzbuzení příznivějšího postoje k IKT a zvýšení důvěry v ně. Postoj EHSV byl již popsán jinde v četných stanoviscích ([19]).

4.1.1 Výbor opět zdůrazňuje ([20]), že „internet a nové technologie jsou komunikace on-line (například mobilní telefony a palmtopy s internetovým připojením a multimediálními funkcemi, které nyní zaznamenávají prudký rozmach) zásadním způsobem důležité pro rozvoj znalostní ekonomiky, e-hospodářství a e-správy“.

([16]) Multivariate Statistical Analysis for Network Attacks Detection. Guangzhi Qu, Salim Hariri* – 2005 USA, Arizona
Internet Technology Laboratory, ECE Department, The University of Arizona, http://www.ece.arizona.edu/~hpdc
Mazin Yousif, Intel Corporation, USA – částečně financováno Intel Corporation IT R&D Council.

([17]) KOM(2006) 251 v konečném znění z 31.5.2006.

([18]) Viz KOM(251) 2006, předposlední odstavec kapitoly 3.

([19]) Viz následující dokumenty:
— stanovisko EHSV k *návrhu směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/ES*, Úř. věst. C 69, 21.3.2006, s. 16,
— stanovisko EHSV ke *sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: i2010 – evropská informační společnost pro růst a zaměstnanost*, Úř. věst. C 110, 9.5.2006, s. 83,
— stanovisko EHSV k *návrhu rozhodnutí Evropského parlamentu a Rady o založení víceletého programu Společenství pro podporu bezpečnějšího používání internetu a nových on-line technologií*, Úř. věst. C 157, 28.6.2005, s. 136,
— stanovisko EHSV ke sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Bezpečnost sítí a informací: návrh evropského politického přístupu, Úř. věst. C 48, 21.2.2002, s. 33.

([20]) Viz poznámka pod čarou č. 19 – třetí odrážka.

4.2 *Směrem k větší platnosti návrhů Komise*

4.2.1 Výbor se domnívá, že Komisí navržený přístup, který spočívá v tom, že tato integrovaná a dynamická strategie bude založena na otevřeném a participativním dialogu, partnerství a posílené účasti mnoha zúčastněných stran a zejména uživatelů, by mohl být dále rozšířen.

4.2.2 Tento postoj již byl zdůrazněn v předchozích stanoviscích: „má-li být program efektivní, musí přímo zahrnout všechny uživatele internetu. Uživatelé musí být poučeni a připraveni k potřebným opatřením a musí být seznámeni s prostředky, které je třeba použít, aby se chránili před zasíláním škodlivého a nevyžádaného obsahu, nebo aby byli zneužíváni k jeho dalšímu šíření. Podle názoru Výboru je jednou z priorit akčního plánu ve vztahu k informacím a odborné přípravě získat podporu uživatelů“ ([21]).

4.2.3 Zapojení uživatelů a občanů však podle názoru Výboru musí proběhnout tak, aby se sloučila nezbytná ochrana sítí a informací s občanskými svobodami a právem uživatelů na bezpečný přístup a dostupné ceny.

4.2.4 Je třeba zvážit, že snaha o informační bezpečnost představuje pro spotřebitele náklad i co do času stráveného odstraňováním nebo obcházením překážek. Podle Výboru by bylo nezbytné stanovit povinnost automatického vybavení všech počítačů ochranným antivirovým systémem, který by uživatel mohl nebo nemusel aktivovat sám, ale který by byl ve výrobku přítomen již od počátku.

4.3 *Směrem k dynamičtější a inovativnější strategii Společenství*

4.3.1 Kromě toho by si Unie podle Výboru měla vytyčit ctižádostivější cíle a přijmout inovační, integrovanou a dynamickou strategii s novými iniciativami. Například:

— mechanismy, které umožní digitální identifikaci jednotlivých uživatelů, kteří jsou příliš často nuceni opakovaně vkládat své vlastní anagrafické údaje;

— akce prostřednictvím ETSI ([22]), které by byly předpokladem bezpečného používání IKT a které by mohly nabídnout přesná a rychlá řešení definovaná jako společná prahová hodnota pro bezpečnost v celé Unii;

— akce zaměřené na prevenci, na základě integrace minimálních požadavků na bezpečnost v informačních systémech a na sítě a s pomocí pilotních akcí prostřednictvím kurzů o bezpečnosti organizovaných na školách všech druhů a stupňů;

— vytvoření jasného a uznávaného právního rámce na evropské úrovni. Tento rámec, uplatňovaný na informační technologie a na sítě, by umožnil přejít od informační bezpečnosti k informačnímu pojištění;

— posílení evropských a národních mechanismů posouzení rizik a zlepšení schopnosti uplatňovat právní předpisy za účelem odhalení počítačové kriminality v oblasti ochrany soukromí a uchovávání dat;

— činnosti zaměřené na zamezení vzniku informačních monokultur s výrobky a řešeními, které lze snázeji „napadnout“. Podpora diverzifikovaným plurikulturním inovacím zaměřeným na uskutečnění jednotného evropského informačního prostoru (SEIS – *Single European Information Space*).

4.3.2 Podle EHSV by bylo vhodné vytvoření bezpečnostního střediska IKT mezi generálními ředitelstvími (*ICT-Security Focal Point, inter DG*) ([23]). Středisko by umožnilo jednat:

— na úrovni útvarů Komise;

— na úrovni jednotlivých členských států prostřednictvím horizontálních řešení pro aspekty interoperability, řízení identity, ochrany soukromí, volného přístupu k informacím a službám, minimálních požadavků na bezpečnost;

— na mezinárodní úrovni s cílem zajistit, že EU bude v různých mezinárodních kontextech (jako je OSN, G8, OECD, ISO) vystupovat jednotně.

4.4 *Směrem k posíleným koordinačním akcím EU*

4.4.1 EHSV přikládá velkou důležitost také vytvoření evropské sítě pro bezpečnost sítí a informací, jejímž prostřednictvím bude možné podporovat průzkumy, studie a workshopy o bezpečnostních mechanismech a o jejich interoperabilitě, o moderní kryptografii a o ochraně soukromí.

4.4.2 EHSV se domnívá, že pro tuto delikátní oblast by bylo účelné optimalizovat roli evropského výzkumu účelným shrnutím obsahu:

— Evropského programu pro výzkum v oblasti bezpečnosti (ESRP) ([24]) začleněného do sedmého rámcového programu pro vědecký a technický rozvoj;

([21]) Viz poznámka pod čarou č. 19 – třetí odrážka.

([22]) ETSI, *European Telecomunications Standards Institute (Evropský institut pro normalizaci v telekomunikacích,)* viz zejména workshop ze 16. a 17. ledna 2006. ETSI mezi jiným vypracoval specifikace nezákonných zadržování (TS 102 232; 102 233; 102 234), přístupu k internetu Lan Wireless (TR 102 519) a elektronických podpisů a vyvinul bezpečnostní algoritmy pro GSM, GPRS a UMTS.

([23]) Tento *Focal Point inter DG* by mohl být financován v rámci priorit programu IST podprogramu „Spolupráce“ ze sedmého rámcového programu pro vědecký a technický rozvoj nebo z Evropského programu pro výzkum v oblasti bezpečnosti (ESRP).

([24]) Viz. 7RP – rámcový program EU pro RTD, podprogram „Spolupráce“, tematická priorita výzkum v oblasti bezpečnosti, financovaný částkou 135 mld. eur na období 2007-2013.

— programu Bezpečnější internet plus (*Safer internet plus*)

— a Evropského programu na ochranu kritické infrastruktury (EPCIP) ([25]).

4.4.3 K těmto návrhům by se mohlo připojit vyhlášení „evropského dne bezpečného počítače" podporovaného národními vzdělávacími kampaněmi ve školách a informačními kampaněmi pro spotřebitele o postupech při ochraně informací pomocí počítačů. Přirozeně také pomocí informací o technologickém pokroku zaznamenaném v široké a měnící se oblasti počítačů.

4.4.4 Výbor několikrát zdůrazňoval, že „vnímaná bezpečnost digitálních transakcí a důvěra v ně rozhoduje o rychlosti, s jakou budou firmy ve svých obchodech IKT využívat. Ochota zákazníků uvést číslo své kreditní karty na webové stránce je velkou měrou ovlivněna tím, jak bezpečný se jim tento úkon zdá" ([26]).

4.4.5 Výbor je přesvědčen, že vzhledem k obrovskému růstovému potenciálu odvětví je nezbytné jednak uplatňovat zvláštní politiku a jednak přizpůsobit stávající politiky novému vývoji. Je nezbytné spojit evropské iniciativy v oblasti informační bezpečnosti s integrovanou strategií odstraněním hranic mezi odvětvími a zaručením jednotného a bezpečného šíření IKT ve společnosti.

4.4.6 Podle Výboru jsou některé důležité strategie, jako například tato, uskutečňovány přehnaně pomalu, a to z důvodu, že členské státy kladou byrokratické a kulturní překážky nezbytným rozhodnutím, která musí být učiněna na úrovni Společenství.

4.4.7 Výbor je také toho názoru, že zdroje Společenství jsou nedostačující pro uskutečnění četných a naléhavých projektů, které by mohly dát konkrétní odpovědi na nové problémy globalizace pouze v případě, že budou uskutečněny na úrovni Společenství.

4.5 *Směrem k větší jistotě EU o ochraně spotřebitele*

4.5.1 Výbor si je vědom, že členské státy přijaly technická bezpečnostní opatření a zahájily postupy řízení bezpečnosti s ohledem na své vlastní potřeby a s tendencí zaměření na různé aspekty. I z tohoto důvodu je obtížné dát jednotnou a účinnou odpověď na problémy bezpečnosti. S výjimkou několika správních sítí neexistuje systematická přeshraniční spolupráci mezi členskými státy, i když je známo, že otázky bezpečnosti nemohou jednotlivé země řešit izolovaně.

4.5.2 Výbor upozorňuje mimo jiné na to, že Rada svým rámcovým rozhodnutím 2005/222 SVV zavedla systém spolupráce mezi soudními orgány a ostatními příslušnými orgány členských států, aby zajistila jejich soudržný přístup na základě sbližování jejich trestně-právních předpisů v oblasti následujících útoků proti informačním systémům:

— nezákonný přístup k informačním systémům,

— nezákonné zasahování do systémů prostřednictvím úmyslných činů zaměřených na závažné zpomalení nebo na přerušení fungování informačního systému,

— nezákonné zasahování do dat prostřednictvím úmyslných činů zaměřených na vymazání, narušení, poškození, padělání, odstranění nebo znepřístupnění dat v informačním systému,

— nabádání a podporování ke spoluúčasti na výše uvedených trestných činech.

4.5.3 Rozhodnutí mimoto udává kritéria pro stanovení odpovědnosti právnických osob a případné sankce, které by jim mohly být uloženy, pokud by za ně byly shledány odpovědnými ([27]).

4.5.4 V oblasti dialogu s orgány veřejné správy členských států Výbor podporuje návrh Komise, aby řečené orgány zahájily srovnávací analýzy svých vnitrostátních politik týkajících se bezpečnosti sítí a informačních systémů, včetně zvláštních politik ve veřejném sektoru. Toto doporučení je ostatně obsažené i ve stanovisku EHSV z roku 2001.

4.6 *Směrem k široce rozšířené kultuře bezpečnosti*

4.6.1 Pokud jde o zapojení odvětví informační bezpečnosti, musí toto odvětví v zájmu ochrany práv svých zákazníků na soukromí a na důvěrnost osobních údajů skutečně zaručit, že systémy materiálního dozoru nad svými instalacemi a nad kódováním sdělení budou v souladu s vývojem techniky ([28]).

([25]) KOM(2005) 576 ze dne 17.11.2005.
([26]) Viz poznámka pod čarou č. 19 – druhá odrážka.
([27]) Viz poznámka pod čarou č. 19 – čtvrtá odrážka.
([28]) Viz směrnice 97/66 ES o zacházením se soukromými údaji v odvětví telekomunikací (Úř. věst. L 24, 30.1.1998).

4.6.2 Co se týče akcí na zvyšování povědomí, Výbor považuje za zásadní, aby se vytvořila opravdová „kultura bezpečnosti" plně slučitelná s informační, sdělovací a názorovou svobodou. Na druhé straně připomíná, že četní uživatelé si nejsou vědomi všech rizik spojených s informačním pirátstvím, zatímco mnozí provozovatelé, prodejci či poskytovatelé služeb nejsou schopni posoudit existenci a rozsah zranitelných aspektů.

4.6.3 Je-li ochrana soukromí a osobních údajů prioritním cílem, pak mají také spotřebitelé právo na skutečně účinnou ochranu před nelegálním dokumentováním osobních profilů prostřednictvím špionážních softwarů (*spyware a web bugs*) nebo jiných metod. Rovněž by se měla učinit přítrž praktice *spamming* ([29]) (rozesílání obrovského množství nevyžádaných e-mailů), který je často výsledkem těchto zneužití. Za takovéto útoky platí jejich oběti určitou cenu ([30]).

4.7 *Směrem k silnější a aktivnější agentuře EU*

4.7.1 Výbor kladně hodnotí výraznější a posílenou roli Evropské agentury pro bezpečnost sítí a informací (ENISA) jak pro akce na zvyšování povědomí, tak i – a to především – pro informační kampaně a odbornou přípravu provozovatelů a uživatelů, což ostatně již uvedl ve svém nedávném stanovisku ([31]) k poskytování veřejných služeb v odvětví elektronických komunikací.

4.7.2 Konečně v souvislosti s akcemi navrženými k tématu posílení účasti všech skupin zúčastněných stran se zdá, že se tyto akce přísně řídí dodržováním zásady subsidiarity. Opravdu totiž spadají do působnosti členských států a soukromého sektoru, a to podle konkrétních odpovědností.

4.7.3 ENISA by měla mít možnost využívat přínosu poskytovaného evropskou sítí pro bezpečnost sítí a informací (*European Network and Information Security Network*) k organizování společných akcí, jakož i mnohojazyčného portálu Společenství pro varování a informační bezpečnost k získávání přizpůsobených a interaktivních informací, a to usnadněným stylem jazyka zejména pro jednotlivé uživatele různého věku a pro malé a střední podniky.

V Bruselu dne 16. února 2007.

předseda

Evropského hospodářského a sociálního výboru

Dimitris DIMITRIADIS

([29]) Francouzsky: pollu postage.

([30]) Viz stanoviska EHSV k tématům sítí elektronické komunikace (Úř. věst. C 123, 25.4.2001, str. 50), elektronického obchodování (Úř. věst. C 169, 16.6.1999, str. 36) a vlivu elektronického obchodování na jednotný trh (Úř. věst. C 123, 25.4.2001, str. 1).

([31]) Viz poznámka pod čarou č. 19 – první odrážka.