RADA EVROPSKÉ UNIE

Brusel 20. listopadu 2006 (OR. en)

15415/06

LIMITE

TELECOM 112
DATAPROTECT 43
JAI 609
CONSOM 121
RECH 317

ZPRÁVA

Odesílatel:	Pracovní skupina pro telekomunikace a informační společnost
Příjemce:	COREPER
Číslo návrhu Komise:	10248/06 TELECOM 56 DATAPROTECT 19 RECH 167 JAI 298 + ADD1 15379/06 TELECOM 111 DATAPROTECT 42 JAI 602 CONSOM 118 RECH 316
Předmět:	***PŘÍPRAVA ZASEDÁNÍ RADY VE SLOŽENÍ PRO DOPRAVU, TELEKOMUNIKACE A ENERGETIKU KONAJÍCÍHO SE VE DNECH 11. - 12. PROSINCE 2006*** Strategie pro bezpečnou informační společnost v Evropě - Návrh rozhodnutí Rady

1. Finské předsednictví Rady Evropské unie učinilo v druhé polovině roku 2006 bezpečnost sítí a informací[1] svou prioritou. Výroční konference o Evropské informační společnosti i2010, která se letos konala ve finském Espoo ve dnech 27. až 28. září 2006, se na tuto záležitost důkladně zaměřila, přičemž bezpečnost sítí a informací byla jedním ze tří jejích hlavních témat. Závěry předsednictví přijaté na závěr konference se konkrétně zabývají důvěrou a bezpečností ve „všudypřítomné informační společnosti".

[1] Připomíná se, že bezpečnost sítí a informací byla naposledy předmětem rozpravy na posledním zasedání Rady ve složení pro dopravu, telekomunikace a energetiku dne 8. června 2006 (na základě knihy předsednictví 9205/06). Ministři byli vyzváni k výměně názorů na hlavní politické priority v oblasti bezpečnosti sítí a informací, jež by EU měla v budoucnu při tvorbě politik zohlednit, a na nejvhodnější způsoby, jakými se lze s těmito novými výzvami vypořádat.
V budoucnu lze očekávat, že se nadcházející přezkum právního rámce pro elektronické komunikace bude bezpečností sítí a informací zabývat jako jedním ze svých cílů.

2. Sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a výboru regionů - Strategie pro bezpečnou informační společnost - „Dialog, partnerství a posílení účasti“ ze dne 31. května 2006 se zaměřilo na určení bezpečnostních výzev spojených s informačními systémy a sítěmi v EU a též na vymezení souhrnného a dynamického rámce pro politiku založeného na celistvém přístupu, který zohledňuje zájmy všech zúčastněných stran. Strategie v něm vymezená rozvíjí řadu politických orientací a specifických opatření, jež by měla Komise a členské státy zavést, ve vhodných případech ve spolupráci s Evropskou agenturu pro bezpečnost sítí a informací (ENISA), jakož i se všemi příslušnými zúčastněnými stranami. Sdělení rovněž bere na vědomí rozličné mezinárodní rozměry projednávaných otázek, čímž zdůrazňuje potřebu dbát o spolupráci na všech příslušných fórech.

3. Sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a výboru regionů „Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“)" ze dne 15. listopadu 2006 provádí bilanci dosud vyvinutého úsilí v boji proti těmto hrozbám a určuje další opatření, která mohou být na různých úrovních přijata (posílení právních předpisů Společenství, vynucování práva, spolupráce uvnitř členských států a mezi nimi, politický a hospodářský dialog se třetími zeměmi, iniciativy odvětví a činnosti spojené s vývojem a výzkumem).

4. Jako odpověď na tato sdělení předložilo předsednictví Pracovní skupině pro telekomunikace a informační společnost návrh usnesení Rady o strategii pro bezpečnou informační společnost v Evropě. Zněním návrhu rozhodnutí Rady se zabývala setkání této pracovní skupiny v říjnu a listopadu 2006. Pracovní skupina dospěla v zásadě ke shodě o znění tohoto návrhu. Jsou potvrzeny příslušné dalekosáhlé politické cíle, které se mají sledovat na úrovni EU, jakož i na úrovni členských států.

5. Znění návrhu v podobě vycházející z jednání pracovní skupiny je uvedeno v příloze k tomuto dokumentu. Delegace DK vznesla výhradu obecného parlamentního přezkumu, zatímco všechny delegace si ponechávají ke znění jazykové výhrady.

6. Výbor stálých zástupců se vyzývá, aby za účelem přijetí návrhu závěrů Radou přezkoumal uvedené nedořešené výhrady.

PŘÍLOHA

NÁVRH USNESENÍ RADY

O strategii pro bezpečnou informační společnost v Evropě

RADA EVROPSKÉ UNIE,

[PŘIJÍMÁ TOTO USNESENÍ A]

VÍTÁ

sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů nazvané Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“ ze dne 31. května 2006[2]

BERE NA VĚDOMÍ

sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů „Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“)“ ze dne 15. listopadu 2006.[3]

PŘIPOMÍNÁ

1. usnesení Rady ze dne 28. ledna 2002 o společném přístupu a konkrétních krocích v oblasti síťové a informační bezpečnosti[4];

---

[2] dokument 11190/06 [KOM(2006) 251 v konečném znění]
[3] dokument 10248/06 [KOM(2006) 251 v konečném znění]
[4] Úř. věst. C 43, 16.2.2002, s. 2.

2. usnesení Rady ze dne 18. února 2003 o evropském přístupu ke kultuře bezpečnosti sítí a informací[5];

3. závěry Rady ze zasedání konaného ve dnech 8. až 9. března 2004 na téma „Nevyžádaná sdělení pro účely přímého marketingu nebo spam“ a závěry Rady ze zasedání konaného ve dnech 9. až 10. prosince 2004 na téma „Boj proti spamu“.

4. závěry Evropské rady z března roku 2005 o oživení lisabonské strategie a závěry Evropské rady z března roku 2006, v nichž se Komise a členské státy vyzývají, aby důsledně prováděly novou strategii i2010;

5. ustanovení předpisového rámce Společenství pro elektronické komunikace[6], a zejména ustanovení týkají se bezpečnosti, soukromí a důvěrnosti komunikací, která přispěla k zajištění vysoké úrovně ochrany osobních údajů a soukromí, jakož i k integritě a bezpečnosti veřejných komunikačních sítí;

6. nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací (ENISA)[7];

7. Tuniskou agendu a tuniský závazek přijatý na Světovém summitu o informační společnosti (WSIS) zdůrazňující nutnost pokračovat v boji proti počítačové trestné činnosti a nevyžádané elektronické poště, ale zajistit přitom ochranu soukromí a svobodu projevu a ve spolupráci se všemi zúčastněnými stranami dále podporovat, rozvíjet a provádět celosvětovou kulturu počítačové bezpečnosti;

8. závěry předsednictví Výroční konference o Evropské informační společnosti (27. až 28. září 2006) „i2010 – směrem k všudypřítomné evropské informační společnosti“ ve finském Espoo;

---

5 Úř. věst. C 48, 28.2.2003, s. 1.

6 Směrnice 2002/58/ES (Směrnice o soukromí a elektronických komunikacích), 2002/20/ES (autorizační směrnice), 2002/22/ES (směrnice o univerzální službě).

7 Úř. věst. L 77, 13.3. 2004, s. 1.

PROTO ZDŮRAZŇUJE, ŽE:

1. naše společnost se rychle přibližuje nové fázi vývoje, směrem k všudypřítomné informační společnosti, ve které je stále více běžných činností občanů založeno na používání informačních a komunikačních technologií (ICT), jakož i elektronických komunikačních sítí; síťová a informační bezpečnost by měla být považována za základní prvek umožňující tento vývoj a jeho úspěch;

2. důvěra je životně důležitým prvkem pro úspěch nové informační společnosti; důvěra se též týká zkušeností koncových uživatelů a potřeby respektování jejich soukromí; proto by síťová a informační bezpečnost neměla být považována pouze za technickou záležitost;

3. bezpečnost sítí a informací musí být vnímána jako zásadní součást vytvoření evropského informačního prostoru v rámci iniciativy i2010, čímž přispěje k úspěchu oživené Lisabonské strategie; Informační a komunikační technologie jsou nezbytnou součástí inovace, hospodářského růstu a zaměstnanosti v rámci celého hospodářství;

4. nové technologie, které nás povedou k všudypřítomné informační společnosti se již vyvíjejí; nástup průkopnických technologií (jako jsou vysokorychlostní bezdrátové sítě, zařízení pro radiovou identifikaci, senzorové sítě) a obsahové inovační služby (jako je internetová televize (IPTV), internetové hlasové služby (VoIP), mobilní televize a jiné mobilní služby) vyžaduje dostatečnou úroveň bezpečnosti sítí a informací od samého počátku rozvojové fáze, aby dosáhly skutečné komerční hodnoty; brzké přijetí nových slibných inovací je pro rozvoj informační společnosti a konkurenceschopnosti Evropy velmi důležité; vládní orgány a podniky by měly co nejdříve přijmout bezpečné nově vznikající technologie a služby, aby urychlily jejich široké přijetí;

5. je pro EU strategicky významné, že evropský průmysl je jak náročným uživatelem síťových a bezpečnostních produktů a služeb, tak jejich konkurenceschopným dodavatelem; rozmanitost, otevřenost a interoperabilita jsou neoddělitelnými složkami bezpečnosti a je třeba je podporovat;

6. znalosti a dovednosti v oblasti bezpečnosti sítí a informací se musí též stát nedílnou součástí běžného života každého jednotlivce a zúčastněných subjektů ve společnosti; proběhla řada osvětových akcí jak na vnitrostátní úrovni tak na úrovni EU, ale v této oblasti je stále ještě zapotřebí vyvinou určité úsilí, zejména pokud jde o konečné uživatele a malé a střední podniky (SME); je třeba brát zvláštní ohled na uživatele se zvláštními potřebami nebo s nízkým povědomím o otázkách bezpečnosti sítí a informací; všechny zúčastněné subjekty by si měly být vědomy, že jsou součástí globálního bezpečnostního řetězce a měly by mít oprávnění, aby se takto mohly projevit; otázky bezpečnosti sítí a informací by měly být zohledňovány ve veškerém vzdělávání a školení týkajícího se informačních a komunikačních technologií;

7. zřízení agentury ENISA bylo důležitým pokrokem v úsilí EU čelit výzvám souvisejícím s bezpečností sítí a informací; rozsah, cíle, úkoly a délka působení agentury ENISA jsou definovány v nařízení (ES) č. 460/2004;

8. zdroje věnované výzkumu a vývoji (R&D) a inovaci jak na vnitrostátní úrovni tak na úrovni EU jsou jedním z klíčových prvků pro posílení úrovně bezpečnosti informací a sítí, pokud jde o nové systémy, aplikace a služby; měly by být posíleny snahy na úrovni EU v oblastech výzkumu a vývoje souvisejících s bezpečností, zejména prostřednictvím sedmého rámcového programu (FP7) a rámcového programu pro konkurenceschopnost a inovaci (CIP); úsilí by se mělo rovněž zaměřit na opatření pro šíření a podporu komerčního využití významných výsledků, včetně hodnocení jejich užitečnosti pro širší společnost; tím se zvýší schopnost evropských dodavatelů poskytovat bezpečnostní řešení, která splní specifické potřeby evropského trhu;

9. všudypřítomná informační společnost poskytuje nejen velké výhody, ale představuje rovněž významné výzvy, neboť vytváří nové oblasti potencionálních rizik; ohrožení bezpečnosti a soukromí, též prostřednictvím nezákonného zachycování a využívání údajů, jsou stále závažnější, cílenější a přesněji zaměřené na získání ekonomických výhod; nové reakce na vznikající a stávající hrozby by se proto měly vytvářet inovačním způsobem a měly by zahrnovat i otázky způsobené složitostí systému, omyly, náhodně nebo nejasnými pokyny; mělo by se povzbuzovat a dále propagovat zřízení a rozvoj vnitrostátních orgánů pro reakci na počítačové nouzové situace, zaměřené na různé účastníky a spolupráce mezi těmito orgány, jakož i s jinými příslušnými zúčastněnými subjekty;

10. zvláštní pozornost v rámci politiky EU bezpečnosti sítí a informací si zasluhuje normalizace výrobků, služeb a řídících systémů a vydávání osvědčení pro ně, zejména pokud tyto služby poskytují stávajícími orgány, jakožto způsob rozšiřování osvědčených postupů a profesionality v oblasti bezpečnosti sítí a informací; zejména nově vznikajícím technologiím, jako je RFID a mobilní televize, by prospělo včasné přijetí případných vznikajících otevřených a interoperabilních norem; mělo by se podpořit fungování evropských normalizačních subjektů v této oblasti;

11. při tom, jak elektronické sítě a informační systémy hrají stále důležitější úlohu v celkovém provozu kritické infrastruktury, jejich dostupnost a integrita se stávají nepostradatelnými pro správní orgány, podnikatelské subjekty a pro bezpečnost a kvalitu života občanů, jakož i pro celkové fungování společnosti;

12. Spolupráce a praktické přístupy jsou zapotřebí více než kdy jindy; různé zúčastněné subjekty by měly identifikovat a rozpoznat své příslušné úlohy, odpovědnosti a práva.

A PROTO VYZÝVÁ ČLENSKÉ STÁTY, ABY:

1. podpořily programy odborné přípravy a prováděly osvětu o otázkách bezpečnosti sítí a informací například tím, že zahájí informační kampaně o otázkách bezpečnosti sítí a informací, zaměřené na všechny občany/uživatele a hospodářská odvětví, zejména malé a střední podniky a konečné uživatele se zvláštními potřebami nebo nízkým povědomím; do roku 2008 by mohlo být vybráno společné datum dne evropské osvěty (například „Den bezpečnosti informací a sítí“), který by se každoročně a dobrovolně konal v každém členském státě;

2. posílily příspěvek k výzkumu a vývoji spojenému s bezpečností a zlepšily použitelnost a šíření významných výsledků; povzbudily vývoj inovačních partnerství za účelem podpořit růst evropského odvětví bezpečnosti informačních a komunikačních technologií a zvýšit brzké využívání technologií pro bezpečnost sítí a informací, čímž se jim dostane komerční podpory;

3. věnovaly náležitou pozornost potřebě zamezit novým a stávajících bezpečnostním hrozbám pro elektronické komunikační sítě, které rovněž zahrnují nedovolené zachycování a využívání údajů, potřebě rozpoznávat s nimi spojená rizika a řešit je a podpořit, ve vhodných případech ve spolupráci si agenturou ENISA, účinnou výměnu informací a spolupráci mezi příslušnými organizacemi a agenturami na vnitrostátní úrovni; zavázaly se bojovat proti spamu a špionážnímu a škodlivému softwaru, zejména prostřednictvím lepší spolupráce mezi příslušnými orgány na vnitrostátní i mezinárodní úrovni;

4. posílily svou vzájemnou spolupráci v rámci iniciativy i2010, za účelem určit účinné a inovační postupy pro zlepšení bezpečnosti sítí a informací a dobrovolné šíření znalostí těchto postupů v rámci EU;

5. povzbudily průběžné zlepšování vnitrostátních orgánů pro reakci na počítačové nouzové situace;

6. podpořily prostředí, které povzbuzuje poskytovatele služeb a provozovatele sítí k tomu, aby svým zákazníkům poskytovali spolehlivé služby a zajistili pružnost, jakož i možnost výběru pro spotřebitele, pokud jde o jejich bezpečnostní služby a řešení; povzbuzovaly provozovatele sítí a poskytovatele služeb, aby svým klientům zajišťovali odpovídající úroveň bezpečnosti sítí a informací, nebo to po nich ve vhodných případech požadovaly;

7. pokračovaly v strategických jednáních v rámci Skupiny na vysoké úrovni i2010, při zohlednění probíhajícího vývoje informační společnosti, a zajistily důsledný přístup mezi hledisky regulace, společné regulace, výzkumu a vývoje a eSprávy společně s komunikacemi a vzděláváním;

8. v souladu s akčním plánem eSprávy i2010 upravily zavádění řádných služeb eSprávy, podporovaly interoperabilní řešení správy identit a provedly všechny potřebné změny v uspořádání veřejného sektoru; vlády a veřejné správy by měly sloužit jako příklad osvědčených postupů a to tím, že podpoří bezpečné služby eSprávy pro všechny občany.

VÍTÁ ZÁMĚR KOMISE:

1. pokračovat ve vývoji souhrnné a dynamické strategie v rámci celé EU pro bezpečnost sítí a informací. Zvlášť významný je celistvý přístup navrhovaný Komisí;

2. zabývat se bezpečností sítí a informací jako jedním z cílů přezkumu předpisového rámce EU pro elektronické komunikace;

3. pokračovat ve své úloze v zájmu docílení lepšího povědomí o potřebě obecného politického odhodlání bojovat proti nevyžádané elektronické poště, spywaru a škodlivým programům; posílit dialog a spolupráci se třetími zeměmi, zejména prostřednictvím dohod se třetími zeměmi zahrnujícími otázku boje proti nevyžádané elektronické poště, spywaru a škodlivým programům;

4. posílit účast agentury ENISA na podpoře strategie pro bezpečnou informační společnost v Evropě uvedené v tomto usnesení, v souladu s cíly a úkoly stanovenými v nařízení o agentuře, jakož i prostřednictvím užší spolupráce a těsnějších pracovních vztahů s členskými státy a zúčastněnými subjekty;

5. v souvislosti s iniciativou i2010 vyvinout ve spolupráci s členskými státy a se všemi zúčastněnými subjekty, zejména s odborníky na statistiku a s odborníky členských států na bezpečnost informací, vhodné ukazatele pro průzkumy Společenství o aspektech týkajících se bezpečnosti a důvěry;

6. povzbudit členské státy k tomu, aby prostřednictvím vícestranného dialogu zúčastněných stran posoudily hospodářské, obchodní a společenské hybné síly s cílem vyvinout politiku specifickou pro odvětví informačních a komunikačních technologií za účelem zdokonalení bezpečnosti a odolnosti sítí a informačních systémů, jako potencionální příspěvek k plánovanému Evropskému programu na ochranu kritické infrastruktury;

7. pokračovat ve svém úsilí, koordinovaně s členskými státy, podpořit dialog s příslušnými mezinárodními partnery a organizacemi za účelem rozvoje celosvětové spolupráce týkající se bezpečnosti sítí a informací, zejména prováděním směrů činnosti WSIS a podáváním pravidelných zpráv Radě.

A VYZÝVÁ:

1. agenturu ENISA, aby pokračovala v úzké spolupráci s členskými státy, s Komisí a ostatními příslušnými zúčastněnými subjekty, za účelem splnění úkolů a cílů definovaných ve správním řádu agentury a napomáhala Komisi a členským státům v jejich snahách splnit požadavky bezpečnosti sítí a informací, čímž přispěje k provádění a dalšímu rozvoji nové strategie pro bezpečnou informační společnost v Evropě uvedené v tomto usnesení;

2. všechny zúčastněné subjekty, aby zlepšily bezpečnost programového vybavení a bezpečnost a odolnost sítí a informačních systémů v souladu se strategií pro bezpečnou informační společnost v Evropě, uvedené v tomto usnesení, a taktéž, aby se zapojily do strukturované rozpravy mezi více zúčastněnými stranami o tom, jak nejlépe použít stávající prostředky a správní nástroje;

3. výrobce, aby k bezpečnosti informací a sítí zaujali kladný přístup, s cílem vytvořit vyspělejší a bezpečnější výrobky a služby, a aby prostředky vložené do takových výrobků a služeb považovali za konkurenční výhodu;

4. výrobce a poskytovatele služeb, aby ve vhodných případech zohlednili při vývoji svých výrobků a služeb a při nasazení síťové infrastruktury, aplikací a programového vybavení požadavky na bezpečnost, soukromí a důvěrnost a aby zavedli řešení bezpečnosti a sledovali je;

5. zúčastněné strany, aby spolupracovali a vytvořili pokusná prostředí pro bezpečné zkoušky a pilotní provoz nových technologií a služeb; zúčastněné strany, aby si včas osvojily nové bezpečné technologie a služby po tom, co budou uvedeny na trh;

6. všechny zúčastněné strany, aby se zapojily do dalšího úsilí v boji proti spamu a jiným škodlivým praktikám online a aktivně spolupracovaly s příslušnými orgány na vnitrostátní a mezinárodní úrovni;

7. poskytovatele služeb a odvětví informačních a komunikačních technologií, aby se zaměřili na zdokonalování bezpečnosti, soukromí a užitkovosti výrobků, procesů a služeb s cílem zajistit jejich spolehlivost, předcházet a bránit krádežím identity a jiným útokům narušujícím soukromí;

8. provozovatele sítí, poskytovatele služeb a soukromý sektor, aby sdíleli a zaváděli osvědčené bezpečnostní postupy a aby v organizacích a podnicích pěstovali kulturu analýzy a řízení rizik tím, že podpoří vhodné programy odborné přípravy a vyvinou plánování pro případ nepředvídaných událostí, a též zpřístupní v rámci svých služeb bezpečnostní řešení pro své zákazníky.