I

(Usnesení, doporučení a stanoviska)

USNESENÍ

RADA

USNESENÍ RADY

ze dne 18. prosince 2009

o společném evropském přístupu k bezpečnosti sítí a informací

(2009/C 321/01)

RADA EVROPSKÉ UNIE,

I. S OHLEDEM NA:

1. sdělení Komise ze dne 31. května 2006 nazvané „Strategie pro bezpečnou informační společnost“, jež navrhuje proces dialogu, partnerství a posílení účasti se zapojením členských států a zúčastněných stran ze soukromého sektoru;

2. sdělení Komise ze dne 12. prosince 2006 o „Evropském programu na ochranu kritické infrastruktury“, jehož cílem je zlepšit ochranu kritických infrastruktur v EU a vytvořit rámec EU týkající se ochrany kritických infrastruktur;

3. směrnici Rady ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu;

4. usnesení Rady ze dne 22. března 2007 o strategii pro bezpečnou informační společnost v Evropě;

5. závěry Rady ze zasedání ve dnech 19. a 20. dubna 2007 o Evropském programu na ochranu kritické infrastruktury;

6. sdělení Komise ze dne 30. března 2009 o ochraně kritické informační infrastruktury;

7. probíhající debatu, zahrnující příslušnou veřejnou konzultaci, o budoucnosti Evropské agentury pro bezpečnost sítí a informací (ENISA) a o její úloze při ochraně kritických informačních infrastruktur;

8. závěry předsednictví o ochraně kritických informačních infrastruktur, které jsou výsledkem ministerské konference v Tallinu konané ve dnech 27. a 28. dubna 2009;

9. lisabonské cíle v oblasti konkurenceschopnosti a růstu a probíhající práci na přezkumu Lisabonské strategie;

10. bezpečnostní opatření navržená při přezkumu předpisového rámce pro elektronické komunikace, sítě a služby;

11. s cílem zajistit účinnou budoucí politiku v oblasti bezpečnosti sítí a informací toto usnesení vychází z předpokladu, že dosud nebylo dosaženo žádných závěrů ohledně změn, které je třeba provést v nařízení o agentuře ENISA. Vzhledem k tomu, že Komise v současnosti provádí přezkum budoucí politiky v oblasti bezpečnosti sítí a informací, by tímto usnesením neměl být před zveřejněním výsledků Komise dotčen jakýkoliv výsledek tohoto přezkumu v souvislosti se změnami nařízení o agentuře ENISA.

II. BEROUC NA VĚDOMÍ, ŽE:

1. vzhledem k významu elektronických komunikací, infrastruktur a služeb jakožto základu hospodářských a společenských činností přispívá bezpečnost sítí a informací k důležitým hodnotám a cílům společnosti, jako je demokracie, soukromí, hospodářský růst, svobodný pohyb myšlenek a hospodářská a politická stabilita;

2. systémy, infrastruktury a služby informačních a komunikačních technologií, včetně internetu, mají pro společnost zásadní význam a jejich narušení může způsobit nesmírnou hospodářskou škodu, z čehož jasně vyplývá důležitost opatření na zvýšení ochrany a odolnosti zaměřených na zajištění nepřetržitosti kritických služeb;

3. riziko bezpečnostních událostí podlamuje důvěru uživatelů. Vážná narušení sítí a informačních systémů by mohla mít závažný hospodářský a společenský dopad, avšak i každodenní problémy a obtíže mohou narušit důvěru veřejnosti v technologie, sítě a služby;

4. oblast hrozeb se vyvíjí a roste, čímž se zvyšuje potřeba poskytnout koncovým uživatelům, podnikům a vládám takové infrastruktury elektronických komunikací, jež budou ze své podstaty robustní a odolné, a určit správné pobídky pro poskytovatele za účelem včasného dosažení tohoto cíle;

5. je třeba posílit bezpečnost sítí a informací a začlenit ji do všech oblastí politik i složek společnosti a zabývat se problémem zajištění dostatečných dovedností, a to prostřednictvím opatření na vnitrostátní i evropské úrovni a zvyšováním povědomí o informačních a komunikačních technologiích mezi uživateli;

6. dokončení vnitřního trhu a jeho fungování bude vyžadovat, aby se vlastníci sítí a poskytovatelé služeb zapojili do přeshraniční spolupráce, neboť možná narušení v jednom členském státě mohou rovněž zasáhnout další členské státy a EU jako celek;

7. nové způsoby využívání, jako je „cloud computing“ a software jako služba, ještě více zdůrazňují význam bezpečnosti sítí a informací;

8. bezpečnost sítí a informací má vést k tomu, aby všechny strany ve všech složkách společnosti mohly důvěřovat informačním systémům, a proto je nutný meziodvětvový a přeshraniční přístup;

9. vzhledem k narůstajícímu používání informačních a komunikačních technologií ve společnosti je bezpečnost sítí a informací nezbytným předpokladem pro spolehlivé, bezpečné a zajištěné poskytování veřejných služeb, jako je e-Government;

10. ENISA může stavět na důležité úloze, kterou již v oblasti bezpečnosti sítí a informací zastává.

III. ZDŮRAZŇUJE, ŽE:

1. je nutná vysoká úroveň bezpečnosti sítí a informací v EU za účelem podpory:

   a) svobod a práv občanů, včetně práva na soukromí;

   b) účinné společnosti, pokud jde o kvalitu zpracování informací;

   c) výnosnosti a růstu obchodu a průmyslu;

   d) důvěry občanů a organizací ve zpracování informací a v systémy informačních a komunikačních technologií;

2. odvětví informačních a komunikačních technologií má pro většinu složek společnosti zásadní význam, a z tohoto důvodu je bezpečnost sítí a informací oblastí, za niž nesou společnou odpovědnost všechny zúčastněné strany, včetně provozovatelů, poskytovatelů služeb, poskytovatelů hardwaru a softwaru, konečných uživatelů, veřejných subjektů a vlád jednotlivých zemí.

IV. UZNÁVÁ:

1. význam aktivního a znalého evropského společenství pro bezpečnost sítí a informací, jež přispívá k posílené spolupráci mezi členskými státy a soukromým sektorem;

2. výhody případného harmonizovaného používání mezinárodních bezpečnostních norem v celé EU pro účely bezpečnosti sítí a informací;

3. potřebu společného evropského přístupu k bezpečnosti sítí a informací na mezinárodní scéně, neboť jde o celosvětový problém;

4. význam, který má pro členské státy a orgány EU dostupnost spolehlivých statistických údajů o stavu bezpečnosti sítí a informací v Evropě;

5. potřebu lepší informovanosti všech zúčastněných strana a potřebu poskytnout jim nástroje pro řízení rizika;

6. význam, který má zintenzivnění snah členských států o zvýšení informovanosti, výměnu osvědčených postupů a vytvoření pokynů pro členské státy;

7. význam modelů za účasti více stran, jako jsou partnerství veřejného a soukromého sektoru, založených na dlouhodobém modelu postupu zdola nahoru pro účely zmírnění zjištěných rizik, pokud tento přístup přináší přidanou hodnotou a napomáhá k zajištění vysoké míry odolnosti sítí;

8. zásadní úlohu, kterou zastávají poskytovatelé při poskytování robustních a odolných infrastruktur elektronických komunikací společnosti;

9. užitečnost cvičení pořádaných v Evropě v oblasti bezpečnosti sítí a informací, která mohou přinést cenné poznatky provozovatelům sítí a poskytovatelům služeb, jakož i vládám;

10. skutečnost, že skupiny pro reakci na počítačové hrozby (CERT) na vnitrostátní či vládní úrovni nebo jiné mechanismy odezvy, jež reagují na hrozby a řeší zranitelná místa, mohou přispět k vysoké míře odolnosti a schopnosti sítí a informačních systémů odolávat narušením a napravovat je;

11. význam prozkoumání strategických účinků, rizik a perspektiv, pokud jde o zřízení skupin CERT pro účely orgánů EU, a zvážení případné budoucí role, kterou má mít ENISA v této záležitosti;

12. práci, kterou ENISA dosud v oblasti bezpečnosti sítí a informací vykonala, a potřebu tuto agenturu dále rozvíjet, aby se stala účinným orgánem, jež pro evropskou bezpečnost sítí a informací znamená jasný přínos.

V. ZDŮRAZŇUJE, ŽE:

1. pro řešení stávajících i budoucích problémů má zásadní význam posílená a celostní evropská strategie pro bezpečnost sítí a informací, v níž bude jasně vymezena úloha Evropské komise, členských států a agentury ENISA;

2. po odpovídající konzultaci a analýze by se v rámci legislativního procesu měla zvážit modernizace a posílení agentury ENISA, a to prostřednictvím mandátu zajišťujícího pružnost a dohled ze strany členských států a Komise, jakož i účinnou roli stran zastupujících soukromý sektor. Její mandát by měl zohlednit předpisový rámec pro elektronické komunikace, sítě a služby, měl by být v souladu s cíli uvedenými v lisabonské agendě a měl by zahrnovat cíle týkající se výzkumu, inovací, konkurenceschopnosti, hospodářského růstu a zajištění důvěry;

3. ENISA by mohla podpořit rozvoj politiky i prováděcí úlohy Komise a členských států, zejména pokud jde o překonání rozdílů mezi technologií a politikou, a měla by úzce spolupracovat s členskými státy a dalšími zúčastněnými stranami s cílem zajistit, aby její činnosti byly v souladu s prioritami EU;

4. ENISA by v rámci revidovaného mandátu měla sloužit jako odborné středisko EU v záležitostech spojených s bezpečností sítí a informací v EU. Orgány EU by proto při vypracovávání a provádění politik, které mohou mít na tuto oblast dopad, měly žádat o její stanovisko a v co největší míře je zohlednit;

5. ENISA by rovněž mohla být na základě žádosti nápomocna členským státům při zlepšování jejich vlastních schopností v oblasti bezpečnosti sítí a informací, jakož i schopnosti zvládat bezpečnostní události.

VI. VYZÝVÁ ČLENSKÉ STÁTY, ABY:

1. nadále usilovaly o zvýšení důvěry koncových uživatelů informačních a komunikačních technologií prostřednictvím informačních kampaní;

2. pořádaly vnitrostátní cvičení a/nebo se účastnily pravidelných evropských cvičení v oblasti bezpečnosti sítí a informací a vzaly přitom na vědomí, že vzhledem ke složitosti této oblasti a zapojení soukromého sektoru je nutné rozsáhlé plánování. ENISA by mohla být v tomto ohledu členským státům na žádost nápomocna. Rozsah a zeměpisný rozměr cvičení by se měly postupně přirozeně vyvíjet a měly by být založeny na zjištěných rizicích;

3. zřídily skupiny pro reakci na počítačové hrozby, pokud tyto kapacity dosud nevytvořily, a posílily spolupráci mezi vnitrostátními skupinami CERT na evropské úrovni. ENISA by mohla být v tomto ohledu členským státům nápomocna;

4. zvýšily úsilí, pokud jde o programy vzdělávání, odborné přípravy a programy výzkumu v oblasti bezpečnosti sítí a informací s cílem zajistit dostupnost potřebných technických dovedností a odborníků v EU a zvýšit odbornost těch, kteří jsou do této oblasti zapojeni;

5. postupovaly společně v případě přeshraničních událostí a zvýšily tak svou schopnost reagovat náležitým způsobem, což vyžaduje zintenzivnění dialogu mezi zúčastněnými aktéry s rozhodovací pravomocí, zejména v otázkách důvěrnosti.

VII. VYZÝVÁ KOMISI, ABY:

1. podle potřeby podpořila členské státy při provádění tohoto usnesení;

2. pravidelně informovala Evropský parlament a Radu o iniciativách v oblasti bezpečnosti sítí a informací prováděných na úrovni EU;

3. ve spolupráci s agenturou ENISA zahájila kampaň na zvýšení informovanosti veřejnosti a soukromého sektoru v Evropě o významu náležitého řízení rizik v oblasti bezpečnosti sítí a informací;

4. ve spolupráci s členskými státy pokračovala v určování pobídek pro poskytovatele infrastruktur elektronických komunikací, aby tito poskytovatelé mohli koncovým uživatelům, podnikům a vládám dodávat standardní robustní a odolné infrastruktury;

5. ve spolupráci s členskými státy vyvíjela metody, jež umožní provádět na úrovni EU srovnatelné vyhodnocování socioekonomických dopadů bezpečnostních událostí a účinnosti preventivních opatření;

6. podpořila a zlepšila modely za účasti více stran, jež musí prokázat jasnou přidanou hodnotu, která bude přínosem pro koncové uživatele a průmysl;

7. předložila celostní strategii v oblasti bezpečnosti sítí a informací, [1] včetně návrhů týkajících se posíleného a pružného mandátu agentury ENISA, jakož i posíleného dohledu členských států a Komise;

8. ve spolupráci s členskými státy provedla analýzu skupin pro reakci na počítačové hrozby s cílem určit, v kterých oblastech je zapotřebí další spolupráce;

9. i nadále zkoumala možnosti společného nebo interoperabilního přístupu orgánů EU při pořizování bezpečných systémů a služeb informačních a komunikačních technologií.

VIII. VYZÝVÁ AGENTURU ENISA, ABY:

1. nadále aktivně podporovala členské státy, Evropskou komisi a další zúčastněné strany při provádění evropských politik bezpečnosti sítí a informací a akčního plánu v oblasti ochrany kritické informační infrastruktury;

2. společně s členskými státy, Komisí a statistickými orgány pracovala na vytvoření rámce statistických údajů o stavu bezpečnosti sítí a informací v Evropě.

IX. VYZÝVÁ ZÚČASTNĚNÉ STRANY, ABY:

1. zintenzívnily úsilí o zvýšení úrovně bezpečnosti sítí a informací, zejména pokud jde o dodávání spolehlivých a důvěryhodných produktů a služeb vyznačujících se jednoduchým používáním;

2. uživatele řádně informovaly o bezpečnostních rizicích spojených s produkty a službami a o tom, jak se před nimi mohou chránit;

3. přijaly všechna odpovídající technická a organizační opatření pro zajištění nepřetržitosti, integrity a důvěrnosti sítí a služeb elektronických komunikací;

4. nadále pracovaly na standardizaci bezpečnosti sítí a informací s cílem nalézt harmonizovaná a interoperabilní řešení;

5. se společně s členskými státy účastnily cvičení, jež jim umožní náležitě reagovat na mimořádné události.

---

[1] Komise navrhuje doplnit slovo „případně“.