EVROPSKÝ PARLAMENT 2009 - 2014

Dokument ze zasedání

A7-0167/2012

16. 5. 2012

ZPRÁVA

o ochraně kritické informační infrastruktury – „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti“
(2011/2284(INI))

Výbor pro průmysl, výzkum a energetiku

Zpravodaj: Ivailo Kalfin

PR_INI

OBSAH

Strana

NÁVRH USNESENÍ EVROPSKÉHO PARLAMENTU

o ochraně kritické informační infrastruktury – „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti“
(2011/2284(INI))

Evropský parlament,

– s ohledem na své usnesení ze dne 5. května 2010 nazvané „Nová digitální agenda pro Evropu: 2015.eu“[1],

– s ohledem na své usnesení ze dne 15. června 2010 nazvané „Řízení internetu: další kroky“[2],

– s ohledem na své usnesení ze dne 6. července 2011 nazvané „Evropské širokopásmové sítě: investice do digitálního růstu“[3],

– s ohledem na článek 48 jednacího řádu,

– s ohledem na zprávu Výboru pro průmysl, výzkum a energetiku a stanovisko Výboru pro občanské svobody, spravedlnost a vnitřní věci (A7-0167/2012),

A. vzhledem k tomu, že schopnost informačních a komunikačních technologií (IKT) podpořit hospodářství a společnost může být plně využita pouze tehdy, budou-li mít uživatelé důvěru v jejich bezpečnost a odolnost, a pokud budou v internetovém prostředí účinně vymáhány již existující právní předpisy v oblastech, jako jsou ochrana údajů a práva duševního vlastnictví;

B. vzhledem k tomu, že dopad internetu a informačních a komunikačních technologií (IKT) na různé aspekty života občanů sílí a že internet a IKT jsou zásadní hybnou silou sociální interakce, kulturního rozvoje a hospodářského růstu;

C. vzhledem k tomu, že bezpečnost IKT a internetu je komplexní otázkou, která má globální dopad v oblasti ekonomiky, sociálních věcí, technologie a vojenství, což vyžaduje jednoznačné vymezení a odlišení povinností a stabilní mechanismus mezinárodní spolupráce;

D. vzhledem k tomu, že stěžejním cílem Digitální agendy pro Evropu je zvýšení konkurenceschopnosti Evropy díky posílení IKT a vytvoření podmínek pro stabilně vysoký růst a pro pracovní místa založená na technologiích;

E. vzhledem k tomu, že soukromý sektor v minulém desetiletí investoval miliardy eur a je i nadále primárním investorem, vlastníkem a správcem produktů týkajících se bezpečnosti informací, opatření, služeb, aplikací a příslušné infrastruktury; vzhledem k tomu, že zapojení soukromých podniků by mělo být posíleno vhodnými politickými strategiemi na

[1] Úř. vìst. C 81E, 15.3.2011, s. 45.
[2] Úř. vìst C 236E, 12.8.2011, s. 33.
[3] Pøijaté texty, P7_TA(2011)0322.

podporu odolnosti infrastruktury, která je vlastněna nebo provozována veřejným či soukromým sektorem nebo v rámci partnerství veřejného a soukromého sektoru;

F. vzhledem k tomu, že podaří-li se dosáhnout vysoké úrovně bezpečnosti a odolnosti sítí, služeb a technologií IKT, zvýší se i konkurenceschopnost hospodářství EU, a to jak díky tomu, že se zlepší posuzování a řízení kybernetických rizik, tak tím, že hospodářství EU jako celek bude mít k dispozici robustnější informační infrastrukturu na podporu inovací a růstu, která vytvoří nové příležitosti pro zvyšování produktivity podniků;

G. vzhledem k tomu, že dostupné údaje o vymáhání práva v oblasti kybernetické trestné činnosti – patří sem počítačové útoky, ale také další druhy trestné činnosti on-line – svědčí o tom, že v různých evropských zemích dochází k jejímu výraznému nárůstu; vzhledem však k tomu, že orgány činné v trestním řízení ani skupiny CERT (skupiny pro reakci na počítačové hrozby) neposkytují v dostatečné míře statisticky reprezentativní údaje týkající se kybernetických útoků; tyto údaje budou v budoucnu vyžadovat lepší sumarizaci, díky níž budou policejní orgány moci tyto útoky důrazněji stíhat a která umožní, aby legislativní reakce na stále se vyvíjející kybernetické hrozby vycházely z relevantnějších informací;

H. vzhledem k tomu, že přiměřená míra bezpečnosti informací je zásadní pro výraznější rozmach internetových služeb;

I. vzhledem k tomu, že nedávné kybernetické incidenty, narušení a útoky proti informační infrastruktuře orgánů EU, průmyslu a členských států ukazují, že je nutno zavést robustní, inovativní a účinný systém ochrany kritické informační infrastruktury (CIIP), který bude založen na plné mezinárodní spolupráci a minimálních normách odolnosti platných v členských státech;

J. vzhledem k tomu, že rychlý rozvoj nových prvků v oblasti IKT, jako je např. cloud computing, vyžaduje, abychom věnovali velkou pozornost bezpečnosti, chceme-li plně využívat možností, které nové technologie skýtají;

K. vzhledem k tomu, že se Evropský parlament opakovaně zasazuje o uplatňování vysokých nároků na ochranu soukromí a údajů, neutralitu sítí a na ochranu práv duševního vlastnictví;

I. Opatření k posílení ochrany kritické informační infrastruktury na vnitrostátní a unijní úrovni

1. vítá, že členské státy provádějí evropský program na ochranu kritické informační infrastruktury a že byla zřízena výstražná informační síť kritické infrastruktury (CIWIN);

2. domnívá se, že snahy o ochranu kritických informačních infrastruktur nejen posílí celkovou bezpečnost občanů, ale zlepší také jejich pocit bezpečnosti a posílí jejich důvěru v opatření, která vláda přijímá na jejich ochranu;

3. bere na vědomí, že Komise zvažuje revizi směrnice Rady 2008/114/ES[1], a vyzývá, aby byly ještě před přijetím dalších opatření předloženy doklady o účinnosti a dopadu této směrnice; požaduje, aby se zvážilo rozšíření její působnosti, a to zejména na odvětví IKT a na finanční služby; dále žádá, aby byla pozornost věnována oblastem, jako je zdraví, systémy dodávek potravin a vody, jaderný výzkum a průmysl (pokud se na ně nevztahují zvláštní ustanovení); zastává názor, že tato odvětví by měla rovněž využívat výhod meziodvětvového přístupu, jaký se zaujímá v rámci výstražné informační sítě kritické infrastruktury (spočívající ve spolupráci, systému varování a výměně osvědčených postupů);

4. vyzdvihuje význam zavedení a zaručení trvalé integrace evropského výzkumu pro to, aby se zachovaly a dále vyvíjely evropské špičkové znalosti v oblasti ochrany kritických informačních infrastruktur;

5. s ohledem na propojenou, vysoce vzájemně závislou, citlivou, strategickou a zranitelnou povahu kritické informační infrastruktury na vnitrostátní úrovni a na úrovni EU vyzývá, aby byly pravidelně aktualizovány minimální standardy odolnosti, jejichž cílem je zajistit připravenost na narušení, incidenty, pokusy o destrukci či útoky (např. v důsledku nedostatečné odolnosti infrastruktury nebo nedostatečně zabezpečenými koncovými terminály) a odpovídající reakci;

6. zdůrazňuje význam norem a protokolů pro bezpečnost informací a vítá, že organizace CEN, CENELEC a ETSI byly v roce 2011 pověřeny vytvořením bezpečnostních norem;

7. očekává, že vlastníci a provozovatelé kritické informační infrastruktury umožní a v případě potřeby pomohou uživatelům uplatnit vhodné nástroje ochrany před poškozujícími útoky nebo narušeními, případně prostřednictvím lidského i automatizovaného dohledu;

8. podporuje spolupráci mezi veřejnými a soukromými subjekty na úrovni EU a rovněž jejich úsilí o vytvoření a provádění norem pro bezpečnost a odolnost vnitrostátní či celoevropské civilní – veřejné, soukromé nebo veřejně-soukromé – kritické informační infrastruktury;

9. zdůrazňuje význam celoevropských cvičení zaměřených na přípravu při rozsáhlých síťových bezpečnostních incidentech a význam vymezení jednotného souboru norem pro posuzování hrozeb;

10. vyzývá Komisi, aby ve spolupráci s členskými státy vyhodnotila provádění akčního plánu ochrany kritické informační infrastruktury; naléhavě žádá členské státy, aby vytvořily dobře fungující vnitrostátní/vládní skupiny CERT, vypracovaly vnitrostátní strategie v oblasti počítačové bezpečnosti, pořádaly pravidelné vnitrostátní a celoevropské simulace kybernetických incidentů, vypracovaly vnitrostátní krizové plány proti počítačovým útokům a přispěly k vytvoření evropského krizového plánu pro případy kybernetických incidentů do roku 2012;

[1] Úř. vist. L 345, 23.12.2008, s. 75.

11. doporučuje, aby byly pro všechny evropské kritické informační infrastruktury zavedeny bezpečnostní plány provozovatele nebo rovnocenná opatření a aby byli jmenováni styční bezpečnostní úředníci;

12. vítá probíhající revizi rámcového rozhodnutí Rady 2005/222/SVV[1] o útocích proti informačním systémům; připomíná, že je třeba koordinovat úsilí EU v boji proti rozsáhlým počítačovým útokům prostřednictvím zapojení agentury ENISA, skupin CERT v členských státech a kompetencí budoucích evropských skupin CERT;

13. domnívá se, že agentura ENISA může na evropské úrovni hrát klíčovou roli při ochraně kritické informační infrastruktury tím, že členským státům a orgánům a institucím EU bude poskytovat odborné technické poznatky a bude vypracovávat zprávy a analýzy bezpečnosti informačního systému na evropské a světové úrovni;

II. Další aktivity EU pro robustní bezpečnost na internetu

14. naléhavě vyzývá Evropskou agenturu pro bezpečnost sítí a informací (ENISA), aby koordinovala a prováděla každoroční akci EU – měsíc zvyšování povědomí o bezpečnosti internetu, díky níž se otázky bezpečnosti internetu dostanou do popředí zájmu členských států i občanů EU;

15. podporuje agenturu ENISA v plnění jejích povinností v oblasti bezpečnosti sítí a informací, a to v souladu s cíli digitální agendy, zejména pomocí pokynů a poradenství poskytovaných členským státům v otázce zajištění základních schopností pro jejich skupiny CERT, jakož i prostřednictvím podpory výměny osvědčených postupů prostřednictvím budování atmosféry důvěry; vyzývá agenturu, aby otázky týkající se vymezení podobných opatření v oblasti počítačové bezpečnosti pro soukromé vlastníky a provozovatele sítě a infrastruktury konzultovala s relevantními subjekty a aby Komisi a členským státům pomáhala při podpoře rozvoje a osvojování systémů certifikace v oblasti bezpečnosti informací, norem chování a postupů spolupráce mezi vnitrostátními a evropskými skupinami CERT a vlastníky a provozovateli infrastruktury, kdykoli a kdekoli to bude potřeba, a to prostřednictvím stanovení technologicky neutrálních společných minimálních požadavků;

16. vítá současný návrh revize mandátu agentury ENISA, zejména jeho rozšíření, jakož i rozšíření úkolů agentury; je přesvědčen, že úkolem agentury ENISA by mělo být nejen pomáhat členským státům prostřednictvím poskytování poradenství a analýz, ale také řídit řadu exekutivních úkolů na úrovni EU a ve spolupráci s protějšky v USA, pokud jde o prevenci a odhalování narušení sítě a bezpečnosti informací a rozvoj spolupráce mezi členskými státy; zdůrazňuje, že podle nařízení o ENISA by měly být agentuře uloženy další úkoly související s reakcí na internetové útoky, a to v takovém rozsahu, aby představovaly jednoznačný přínos nad rámec stávajících vnitrostátních mechanismů pro reakci;

17. vítá výsledky celoevropských cvičení v oblasti počítačové bezpečnosti, jež v roce 2010 a 2011 ENISA prováděla a monitorovala v celé Unii s cílem bylo pomoci členským státům při vypracovávání, údržbě a testování celoevropského pohotovostního plánu;

[1] Úř. vist. L 69, 16.3.2005, s. 67.

vyzývá agenturu ENISA, aby tato cvičení ponechala v programu své činnosti a aby vhodným způsobem postupně zapojovala relevantní soukromé subjekty s cílem zvýšit celkové evropské kapacity v oblasti bezpečnosti na internetu, a těší se na další mezinárodní spolupráci se stejně smýšlejícími partnery;

18. vyzývá členské státy, aby sestavily vnitrostátní plány pro případ krizových situací v kybernetickém prostoru, které by měly definovat příslušné kontaktní body a obsahovat ustanovení o pomoci, kontrole a nápravě v případě kybernetických narušení či útoků regionálního, vnitrostátního nebo přeshraničního významu a jiné klíčové prvky; podotýká, že členské státy by rovněž měly zavést vhodné koordinační mechanismy a struktury na vnitrostátní úrovni, což by přispělo ke zlepšení koordinace mezi příslušnými vnitrostátními orgány a k větší soudržnosti jejich činností;

19. doporučuje, aby Komise v rámci krizových plánů EU pro případy kybernetických incidentů navrhla závazná opatření pro lepší koordinaci technických a řídících funkcí mezi vnitrostátními a vládními skupinami CERT na úrovni EU;

20. vyzývá Komisi a členské státy, aby přijaly nezbytná opatření v zájmu ochrany kritické infrastruktury před počítačovými útoky a poskytly prostředky pro hermetické uzavření přístupu ke kritické infrastruktuře v případě, že přímý počítačový útok vážně ohrozí její řádné fungování;

21. očekává zřízení skupiny CERT EU, které bude klíčovým faktorem při prevenci a odhalování úmyslných a poškozujících počítačových útoků, namířených proti orgánům EU, při reakci na ně a při obnově po takových útocích;

22. doporučuje, aby Komise navrhla závazná opatření, která stanoví minimální standardy bezpečnosti a odolnosti a zlepší koordinaci mezi vnitrostátními skupinami pro reakci na počítačové hrozby (CERT);

23. vyzývá členské státy a orgány EU, aby zajistily existenci správně fungujících skupin CERT, jež na základě osvědčených postupů vymezí minimální funkce v oblasti bezpečnosti a odolnosti; poukazuje na to, že vnitrostátní skupiny CERT by měly být součástí účinné sítě, v jejímž rámci dochází k výměně relevantních informací v souladu s nezbytnými standardy důvěrnosti; požaduje, aby byla v každém členském státě vytvořena služba ochrany kritické informační infrastruktury, která bude k dispozici 24 hodin denně, 7 dní v týdnu, a aby byl vytvořen společný evropský protokol pro naléhavé situace, který by se používat pro komunikaci mezi vnitrostátními kontaktními místy;

24. zdůrazňuje, že budování důvěry a podpora spolupráce mezi členskými státy je zásadní pro ochranu údajů a vnitrostátních sítí a infrastruktury; vyzývá Komisi, aby navrhla společný postup pro nalezení a stanovení společného přístupu k řešení přeshraničních hrozeb IKT, přičemž se očekává, že členské státy poskytnou Komisi obecné informace o rizicích, hrozbách a zranitelných místech své kritické informační infrastruktury;

25. vítá iniciativu Komise, v níž se uvádí, že do roku 2013 bude vytvořen Evropský systém pro varování a sdílení informací;

26. vítá, že na základě iniciativy Komise byly otázky bezpečnosti internetu a ochrany kritické informační infrastruktury konzultovány s různými zainteresovanými stranami, jako je například Evropské partnerství veřejného a soukromého sektoru pro odolnost; bere na vědomí významné zapojení a odhodlání prodejců IKT v rámci tohoto úsilí; vybízí Komisi, aby vyvinula další úsilí na podporu akademické obce a sdružení uživatelů IKT, aby se ujímaly aktivnější role, a dále na podporu konstruktivního dialogu mezi větším počtem zainteresovaných stran, který by se věnoval otázkám kybernetické bezpečnosti; podporuje další rozvoj digitálního shromáždění jako rámce pro správu v oblasti ochrany kritické informační infrastruktury;

27. vítá práci, kterou doposud odvedlo Evropské fórum členských států, pokud jde o stanovení zvláštních kritérií pro jednotlivá odvětví, s jejichž pomocí by mohla být určena evropská kritická infrastruktura, se zaměřením na pevné a mobilní komunikace, a dále o projednávání zásad a pokynů EU pro odolnost a stabilitu internetu; těší se na to, že budování konsensu mezi členskými státy bude pokračovat, a v této souvislosti vybízí fórum, aby současný přístup zaměřený na fyzická aktiva rozšířilo o logickou infrastrukturu, jež bude v souvislosti s pokrokem v oblasti virtualizačních technologií a technologií „cloud“ nabývat na významu z hlediska účinnosti ochrany kritických internetových infrastruktur;

28. doporučuje Komisi, aby zahájila veřejnou celoevropskou iniciativu zaměřenou na vzdělávání a zvyšování povědomí koncových uživatelů – jak soukromých osob, tak podniků –, pokud jde o potenciální rizika internetu a nepřenosných i mobilních zařízení využívajících IKT na všech úrovních infrastrukturních řetězců, a na šíření bezpečnějšího individuálního chování na internetu; připomíná v tomto ohledu rizika spojená se zastaralým počítačovým vybavením a softwarem;

29. vyzývá členské státy, aby s podporou Komise posílily programy vzdělávání a odborné přípravy v oblasti bezpečnosti informací, určené pro vnitrostátní policejní a soudní orgány a příslušné agentury EU;

30. souhlasí s myšlenkou vytvoření evropských osnov pro akademické odborníky v oblasti bezpečnosti informací, neboť by to mělo pozitivní vliv na odbornost a připravenost EU s ohledem na neustále se vyvíjející kyberprostor a hrozby, kterým čelí;

31. vyjadřuje se ve prospěch podpory vzdělávání v oblasti kybernetické bezpečnosti (doktorandské studium, univerzitní přednáškové cykly, semináře, kurzy pro studenty atd.) a specializovaných školení o ochraně kritické informační infrastruktury;

32. vyzývá Komisi, aby do konce roku 2012 navrhla komplexní strategii bezpečnosti internetu pro Unii, která bude založena na jednoznačné terminologii; zastává názor, že cílem strategie bezpečnosti internetu by mělo být vytvoření kyberprostoru – podpořeného bezpečnou a odolnou infrastrukturou a otevřenými normami – který prostřednictvím volného toku informací přispívá k inovacím a prosperitě a zajišťuje důkladnou ochranu soukromí a dalších občanských svobod; domnívá se, že strategie by měla podrobně uvádět zásady, cíle, metody, nástroje a politiky (jak vnitřní, tak vnější) nezbytné pro zorganizování vnitrostátního a evropského úsilí a pro vytvoření minimálních standardů odolnosti pro členské státy, aby byla zajištěna bezpečná, kontinuální, robustní a odolná služba, ať v souvislosti s kritickou infrastrukturou, nebo obecným využíváním internetu;

33. zdůrazňuje, že Komisí připravovaná strategie bezpečnosti internetu by měla vycházet zejména z práce na ochraně kritické informační infrastruktury (CIIP) a měla by usilovat o ucelený a systematický přístup ke kybernetické bezpečnosti tím, že bude zahrnovat jak aktivní opatření, jako je zavedení minimálních norem pro bezpečnostní opatření nebo vzdělávání jednotlivých uživatelů, podniků a veřejných institucí, tak i reaktivní opatření, jako jsou sankce v rámci trestního, občanského a správního práva;

34. naléhavě žádá Komisi, aby navrhla účinný mechanismus pro koordinaci provádění strategie bezpečnosti na internetu a pro její pravidelnou aktualizaci; tento mechanismus by měl být podpořen dostatečnými správními, odbornými a finančními zdroji a jedním z jeho úkolů by mělo být pomáhat při utváření postojů EU ve vztazích s vnitřními i mezinárodními zainteresovanými subjekty v otázkách spojených s bezpečností na internetu;

35. vyzývá Komisi, aby navrhla rámec EU pro oznamování případů narušení bezpečnosti v kritických odvětvích, jako je energetika, doprava a dodávky vody a potravin, a rovněž v odvětví IKT a finančních služeb, přičemž cílem je zajistit, aby orgány členských států a uživatelé byli informováni o incidentech a útocích na internetu nebo narušení jeho fungování;

36. naléhavě žádá Komisi, aby zlepšila dostupnost statisticky reprezentativních údajů týkajících se nákladů počítačových útoků v EU, členských státech a průmyslu (zejména v odvětví finančních služeb a IKT), a to zvýšením kapacity shromažďování údajů Centra pro boj proti kyberkriminalitě, které by mělo být založeno v roce 2013, skupin CERT a dalších iniciativ Komise, jako je například Evropský systém pro varování a sdílení informací, aby bylo zajištěno systematické oznamování a sdílení údajů o počítačových útocích a dalších formách počítačové kriminality postihujících evropský průmysl a členské státy a aby bylo posíleno vymáhání práva;

37. podporuje blízký vztah a interakci mezi vnitrostátními soukromými sektory a agenturou ENISA s cílem napojit vnitrostátní/vládní skupiny CERT na vývoj Evropského systému pro varování a sdílení informací (EISAS);

38. zdůrazňuje, že primární hnací silou rozvoje a využívání technologií, které mají zvýšit bezpečnost internetu, je odvětví IKT; připomíná, že politiky EU nesmí bránit růstu evropské internetové ekonomiky a musí zahrnovat nezbytné pobídky, aby bylo možné v plném rozsahu využívat potenciál partnerství mezi podniky a partnerství veřejného a soukromého sektoru; doporučuje zvážit další pobídky pro odvětví IKT s cílem vypracovat solidnější plány bezpečnosti provozovatele v souladu se směrnicí 2008/114/ES;

39. vyzývá Komisi, aby předložila legislativní návrh na kriminalizaci dalších kybernetických útoků (tj. spear-phishing, internetové podvody atd.);

III. Mezinárodní spolupráce

40. připomíná, že mezinárodní spolupráce je hlavním nástrojem pro zavedení účinných opatření v oblasti kybernetické bezpečnosti; připouští, že EU v současnosti není trvale aktivně zapojena do procesů a dialogů, jež se v rámci mezinárodní spolupráce zaměřují na

kybernetickou bezpečnost; vyzývá Komisi a Evropskou službu pro vnější činnost (ESVČ), aby zahájily konstruktivní dialog se všemi stejně smýšlejícími zeměmi s cílem dospět ke konsensu a vytvořit programy zvyšování odolnosti internetu a kritické infrastruktury; domnívá se, že EU by zároveň měla zahrnovat otázky bezpečnosti internetu do rámce svých vnějších vztahů, a to trvale, mimo jiné tehdy, když navrhuje různé finanční nástroje nebo když přistupuje k mezinárodním dohodám, jejichž součástí je výměna a uchovávání citlivých údajů;

41. bere na vědomí pozitivní přínos Úmluvy Rady Evropy o kybernetické trestné činnosti, podepsané v Budapešti v roce 2001; poukazuje nicméně na to, že ESVČ by měla vyzvat k podpisu a ratifikaci úmluvy více zemí a měla by také rozvíjet dvoustranné a mnohostranné dohody o bezpečnosti a odolnosti internetu s podobně smýšlejícími mezinárodního partnery;

42. poukazuje na to, že různé mezinárodní a evropské orgány, subjekty a agentury a členské státy provádějí širokou škálu činností, které musí být koordinovány, aby nedocházelo k duplikaci, a za tímto účelem je vhodné zvážit jmenování úředníka odpovědného za koordinaci, případně určit koordinátora EU pro oblast kybernetické bezpečnosti;

43. zdůrazňuje, že strukturovaný dialog mezi hlavními aktéry a zákonodárci v EU a USA, kteří jsou zapojeni do projektu CIIP, má velký význam pro vzájemné porozumění a společný výklad a společné postoje v souvislosti s právními a správními rámci;

44. vítá, že na summitu EU-USA v listopadu 2010 byla zřízena pracovní skupina EU-USA pro kybernetickou bezpečnost a kyberkriminalitu, a podporuje její úsilí o zahrnutí otázek bezpečnosti na internetu do transatlantického politického dialogu; vítá, že Komise a vláda USA v rámci pracovní skupiny EU-USA spolu vypracovaly společný program a plán pro společná/synchronizovaná transkontinentální kybernetická cvičení v letech 2012–2013;

45. navrhuje, aby byl v rámci úsilí o společný konsensus, výklad a postoje zahájen strukturovaný dialog mezi tvůrci právních předpisů EU a USA o problematice internetu;

46. naléhavě vyzývá ESVČ a Komisi, aby na základě práce odvedené Evropským fórem členských států zajistily aktivní postavení v rámci příslušných mezinárodních fór, a to mimo jiné koordinací postojů členských států s cílem prosazovat hlavní hodnoty, cíle a politiky EU v oblasti bezpečnosti a odolnosti internetu; podotýká, že mezi tato fóra patří NATO, OSN (zejména prostřednictvím Mezinárodní telekomunikační unie a Fóra pro správu internetu), Internetové sdružení pro přidělování jmen a čísel, Úřad pro přidělování internetových čísel, OBSE, OECD a Světová banka;

47. vybízí Komisi a agenturu ENISA, aby se účastnily hlavních rozhovorů zúčastněných stran s cílem definovat technické a právní normy v kyberprostoru na mezinárodní úrovni;

48. pověřuje svého předsedu, aby předal toto usnesení Radě a Komisi.

VYSVĚTLUJÍCÍ PROHLÁŠENÍ

Úloha technologie v našich každodenních životech se stále zvětšuje ve všech svých aspektech – od komunikace po finančnictví a bankovnictví, od dopravy po energetiku, od kultury a zábavy po zdravotnictví.

Vzhledem ke stále většímu využívání internetu a počítačových technologií představuje bezpečnost internetu v současné době jednu z nejvyšších politických priorit pro Evropskou unii i zbytek světa. Strategie Evropa 2020 zahájená v roce 2010 začlenila mezi své stěžejní politiky Digitální agendu EU a stanovila ambiciózní cíle pro technologický rozvoj Evropské unie. Stále větší využívání a šíření inovativních IKT, jako jsou rychlé a superrychlé pevné a mobilní internetové a celulární sítě, inteligentní sítě, ale také internetové služby, jako je tzv. cloud computing a internet věcí, zcela závisí na jediném jednoduchém, ale zásadním aspektu – bezpečnosti, odolnosti a důvěře.

V prosinci 2006 Komise přijala sdělení o Evropském programu na ochranu kritické infrastruktury (EPCIP). Toto sdělení stanoví celkový rámec pro činnosti na ochranu kritické infrastruktury na úrovni EU. O dva roky později Rada přijala směrnicí 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Ve své první fázi se směrnice zaměřila na odvětví energetiky a dopravy. Zabývá se výhradně infrastrukturami, jejichž přerušení by mělo dopad na nejméně dva členské státy EU.

Směrnice 2008/114/ES určila odvětví IKT jako budoucí prioritní odvětví, ačkoli nebylo klasifikováno jako kritická infrastruktura. Nicméně Komise již od roku 2005 zdůrazňovala nutnost koordinovat úsilí zaměřené na budování důvěry v oblasti elektronických komunikací[1]. Za tímto účelem byla v roce 2006 přijata strategie pro bezpečnou informační společnost[2], jejíž hlavní prvky byly schváleny v usnesení Rady 2007/068/01.

V roce 2009 Komise přijala sdělení nazvané „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“[3]. V tomto sdělení Komise stanovila akční plán ochrany kritické informační infrastruktury, aby tak stimulovala a podpořila bezpečnost kritické informační infrastruktury jak na vnitrostátní úrovni, tak na úrovni Unie. Tento plán vymezuje zvláštní úkoly Komise, agentury ENISA, členských států a odvětví. Otázkou zvyšování bezpečnosti a odolnosti infrastruktur IKT se dále intenzivněji zabývá Digitální agenda pro Evropu[4] a související závěry Rady[5], návrh směrnice o útocích proti informačním systémům[6] a stejně tak návrh Komise týkající se nového mandátu pro posílenou a modernizovanou agenturu ENISA[7].

1 COM(2005)0229.
2 COM(2006)0251.
3 COM(2009)0149.
4 COM(2010)0245.
5 Závěry Rady ze dne 31. května 2010.
6 COM(2010)0517.
7 COM(2010)0521.

V březnu 2011 Komise vydala sdělení o ochraně kritické informační infrastruktury: „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti“[1]. V tomto dokumentu Komise vyhodnocuje výsledky provádění akčního plánu ochrany kritické informační infrastruktury od roku 2009 a popisuje další kroky, jež je třeba přijmout, přičemž klade důraz na mezinárodní spolupráci přesahující hranice EU.

Veškerý tento vývoj v rozsahu několika málo let, během nichž ještě nebylo vyčerpáno úsilí o posílení bezpečnosti kyberprostoru v Unii, ukazuje, že otázka bezpečnosti internetu je významná. Je zřejmé, že internet představuje kritickou infrastrukturu a že narušení internetu může vést k podstatným ztrátám a bezpečnostním rizikům, které mají dopad na velký počet evropských občanů a podniků. Rychlý rozvoj technologií navíc vyžaduje, aby prevence internetových útoků, nápravné reakce a odolnost globální sítě vycházely z komplexního, reakceschopného, flexibilního, inovativního a dlouhodobého rámce. Tento rámec musí zajišťovat účinnou interakci mezi vládami, podniky, jednotlivci a všemi dalšími zainteresovanými stranami. V neposlední řadě je zvýšená odolnost internetu možná pouze tehdy, pokud je zaveden účinný systém mezinárodní spolupráce a mezinárodních norem.

1 COM(2011)0163.

22. 3. 2012

STANOVISKO VÝBORU PRO OBČANSKÉ SVOBODY, SPRAVEDLNOST A VNITŘNÍ VĚCI

pro Výbor pro průmysl, výzkum a energetiku

k ochraně kritické informační infrastruktury. Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti
(2011/2284(INI))

Navrhovatelka: Ágnes Hankiss

NÁVRHY

Výbor pro občanské svobody, spravedlnost a vnitřní věci vyzývá Výbor pro průmysl, výzkum a energetiku jako příslušný výbor, aby do svého návrhu usnesení začlenil tyto návrhy:

1. domnívá se, že ochrana kritické informační infrastruktury vyžaduje interdisciplinární přístup, který musí zahrnovat významné aspekty občanských svobod, spravedlnosti a vnitřních věcí, jako je vnitřní bezpečnost, ochrana osobních údajů a právo na důvěrnost a soukromý život, čímž se posílí bezpečnost a zároveň budou dodržována základní práva;

2. připomíná, že ochrana kritické informační infrastruktury je začleněna do strategie vnitřní bezpečnosti Evropské unie v souvislosti se zvyšováním úrovně bezpečnosti pro občany a podniky v kybernetickém prostoru;

3. naléhavě žádá, aby bylo dokončeno určení evropské kritické infrastruktury a aby bylo průběžně aktualizováno pod dohledem Komise v souladu se směrnicí Rady 2008/114/ES[1] (směrnice o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu); zdůrazňuje rovněž potřebu co nejrychleji vytvořit výstražnou informační síť kritické infrastruktury na evropské úrovni; trvá na tom, že vzhledem k silné závislosti veřejných institucí, podniků a domácností na informačních a komunikačních technologiích by měla být směrnice Rady 2008/114/ES přezkoumána s cílem rovněž uznat toto odvětví jako klíčové;

4. vyzývá členské státy, aby vyvinuly vnitrostátní strategii a zajistily řádnou tvorbu politiky a regulační prostředí, komplexní postupy řízení rizik a náležitá přípravná opatření

[1] Úř. věst. L 345, 23.12.2008, s. 75.

a mechanismy; naléhavě vyzývá členské státy, které dosud neustanovily svou národní skupinu pro reakci na počítačové hrozby (CERT), aby tak včas učinily, v případě potřeby s pomocí Evropské agentury pro bezpečnost sítí a informací (ENISA);

5. zastává názor, že všechny rozsáhlé databáze pracující s citlivými osobními údaji, jako jsou databáze EU, vlád členských států a finančních a zdravotnických institucí, by měly být považovány za součást kritické informační infrastruktury, a měla by být zajištěna ochrana těchto údajů na základě nejvyšších možných standardů;

6. vyzývá Komisi a členské státy, aby přijaly nezbytná opatření na ochranu kritické infrastruktury před kybernetickými útoky a aby stanovily způsoby odříznutí přístupu ke kritické infrastruktuře v případě, že přímý kybernetický útok vážně ohrožuje její řádné fungování;

7. zdůrazňuje význam celoevropských cvičení zaměřených na přípravu při rozsáhlých síťových bezpečnostních incidentech a význam vymezení jednotného souboru norem pro posuzování hrozeb;

8. domnívá se, že agentura ENISA může na evropské úrovni hrát klíčovou roli při ochraně kritické informační infrastruktury tím, že členským státům a orgánům a institucím EU poskytne odborné technické znalosti, jakož i zprávy a analýzy bezpečnosti informačního systému na evropské a světové úrovni;

9. je přesvědčen, že je nezbytná spolupráce na mezinárodní úrovni přesahující hranice EU, jelikož povaha kybernetických hrozeb je globální a vyžaduje globální reakce, které jsou v souladu s ustanoveními mezinárodního práva; zdůrazňuje také, že jakékoliv mezinárodní dohody týkající se výměny citlivých údajů by měly zohlednit bezpečnost předávání a ukládání údajů;

10. zdůrazňuje, že Komisí připravovaná strategie bezpečnosti internetu by měla vycházet zejména z práce na ochraně kritické informační infrastruktury (CIIP) a usilovat o ucelený a systematický přístup ke kybernetické bezpečnosti tím, že bude zahrnovat jak aktivní opatření, jako je zavedení minimálních norem pro bezpečnostní opatření nebo vzdělávání jednotlivých uživatelů, podniků a veřejných institucí, tak i reaktivní opatření, jako jsou sankce v rámci trestního, občanského a správního práva;

11. je přesvědčen, že spolupráce v Evropské unii by měla být posílena a podpořena v prvé řadě mezi občanskými a vojenskými činiteli a také justičními a jinými příslušnými orgány v oblasti prevence, boje a trestání útoků na informační systémy, včetně policie a jiných donucovacích orgánů v členských státech, stejně jako specializovaných agentur na evropské úrovni, jako jsou Eurojust, Europol či ENISA;

12. zdůrazňuje význam intenzivní spolupráce mezi veřejným a soukromým sektorem, neboť různé silné stránky těchto sektorů by se měly vzájemně doplňovat a přispívat tak k úsilí vyvíjenému na ochranu infrastruktury, a tedy i životů a soukromí evropských občanů; vyzývá Komisi, aby zavedla Evropské partnerství mezi veřejným a soukromým sektorem pro odolnost, které by bylo zapojeno do práce agentury ENISA a Evropské vládní skupiny CERT;

13. poukazuje na to, že je potřeba, aby byly mnohé probíhající činnosti, které provádí různé mezinárodní a evropské orgány, subjekty a agentury a také členské státy, koordinovány s cílem zabránit zdvojení činností, a za tímto účelem je vhodné zvážit určení úředníka odpovědného za koordinaci, případně jmenovat koordinátora EU pro oblast kybernetické bezpečnosti;

14. domnívá se, že snahy o ochranu kritických informačních infrastruktur nejen posílí celkovou bezpečnost občanů, ale zlepší také to, jak vnímají bezpečnost, a posílí jejich důvěru v opatření, která vláda přijímá na jejich ochranu;

15. vyzdvihuje význam zavedení a zaručení trvalé integrace evropského výzkumu pro to, aby se zachovaly a dále vyvíjely evropské špičkové znalosti v oblasti ochrany kritických informačních infrastruktur;

16. zdůrazňuje význam aktivního plánu pro výzkum v oblasti kybernetické bezpečnosti;

17. vyjadřuje se ve prospěch podpory vzdělávání v oblasti kybernetické bezpečnosti (doktorandské studium, univerzitní cykly přednášek, semináře, kurzy pro studenty atd.) a specializovaných školení zaměřených na ochranu kritické informační infrastruktury;

18. podporuje blízký vztah a interakci mezi vnitrostátními soukromými sektory a agenturou ENISA s cílem napojit vnitrostátní/vládní skupiny CERT na vývoj Evropského systému pro varování a sdílení informací (EISAS);

19. zdůrazňuje význam společné evropské strategie pro kybernetickou bezpečnost a formulování harmonogramu pro její vymezení z hlediska potřebných činností a zdrojů;

20. zdůrazňuje význam strukturovaného dialogu mezi hlavními aktéry a zákonodárci v EU a USA, kteří jsou zapojeni do projektu CIIP, pro vzájemné porozumění, výklad i stanoviska v souvislosti s právními a správními rámci.

VÝSLEDEK KONEČNÉHO HLASOVÁNÍ VE VÝBORU

Datum přijetí	21.3.2012
Výsledek konečného hlasování	+: 45 –: 0 0: 2
Členové přítomní při konečném hlasování	Roberta Angelilli, Edit Bauer, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Rosario Crocetta, Frank Engel, Cornelia Ernst, Tanja Fajon, Kinga Göncz, Nathalie Griesbeck, Sylvie Guillaume, Anna Hedh, Salvatore Iacolino, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Juan Fernando López Aguilar, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu, Anthea McIntyre, Jan Mulder, Antigoni Papadopoulou, Judith Sargentini, Csaba Sógor, Renate Sommer, Rui Tavares, Kyriacos Triantaphyllides, Wim van de Camp, Renate Weber, Josef Weidenholzer, Cecilia Wikström
Náhradník(ci) přítomný(í) při konečném hlasování	Vilija Blinkevičiūtė, Andrew Henry William Brons, Michael Cashman, Anna Maria Corazza Bildt, Ana Gomes, Nadja Hirsch, Stanimir Ilchev, Iliana Malinova Iotova, Franziska Keller, Wolfgang Kreissl-Dörfler, Mariya Nedelcheva, Hubert Pirker, Zuzana Roithová, Kārlis Šadurskis
Náhradník(ci) (čl. 187 odst. 2) přítomný(í) při konečném hlasování	Luis de Grandes Pascual

VÝSLEDEK KONEČNÉHO HLASOVÁNÍ VE VÝBORU

Datum přijetí	8.5.2012
Výsledek konečného hlasování	+: 51 –: 7 0: 0
Členové přítomní při konečném hlasování	Amelia Andersdotter, Josefa Andrés Barea, Jean-Pierre Audy, Zigmantas Balčytis, Ivo Belet, Bendt Bendtsen, Jan Březina, Maria Da Graça Carvalho, Giles Chichester, Jürgen Creutzmann, Pilar del Castillo Vera, Dimitrios Droutsas, Adam Gierek, Norbert Glante, Robert Goebbels, András Gyürk, Fiona Hall, Edit Herczog, Kent Johansson, Romana Jordan, Krišjānis Kariņš, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Paul Rübig, Salvador Sedó i Alabart, Francisco Sosa Wagner, Konrad Szymański, Britta Thomsen, Evžen Tošenovský, Ioannis A. Tsoukalas, Claude Turmes, Marita Ulvskog, Vladimir Urutchev, Kathleen Van Brempt, Alejo Vidal-Quadras, Henri Weber
Náhradník(ci) přítomný(í) při konečném hlasování	Ioan Enciu, Françoise Grossetête, Takis Hadjigeorgiou, Roger Helmer, Jolanta Emilia Hibner, Bernd Lange, Werner Langen, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Inês Cristina Zuber
Náhradník(ci) (čl. 187 odst. 2) přítomný(í) při konečném hlasování	Anne E. Jensen, Nicole Kiil-Nielsen, Norica Nicolai