POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY

PARLAMENTNÍ INSTITUT

DOKUMENTY EU

Posílení evropského systému kybernetické odolnosti

Informační podklad ke sdělení o posílení evropského systému kybernetické odolnosti a podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti

Obsah:

Podklad k dokumentu Rady č. 11013/16
prosinec 2016
zpracovala: Darina Šimková

AKTUÁLNÍ VYDÁNÍ:

Název: Posílení evropského systému kybernetické odolnosti
Zpracovala: Šimková, D.
Číslo: Podklad k dokumentu č. 11013/16
Datum: prosinec 2016

Klíčová slova:
Konkurenceschopnost; kybernetická bezpečnost; technická normalizace

ŘADA: DOKUMENTY EU

Typ řady: interní
První vydání řady: říjen 2004
Frekvence vydání řady: nepravidelná
Zaměření: Informační podklady k dokumentům EU projednávaným VEZ
Jazyk: CZ
Vydavatel: Kancelář Poslanecké sněmovny, Sněmovní 4, 118 26 Praha 1

PARLAMENTNÍ INSTITUT plní úkoly vědeckého, informačního a vzdělávacího střediska pro Poslaneckou sněmovnu, její orgány, poslance a Kancelář Poslanecké sněmovny, pro Senát, jeho orgány, senátory a Kancelář Senátu. Naše činnosti a produkty uvádíme níže.

Oddělení všeobecných studií	**STUDIE** Srovnávací studie Analytické studie	**ODPOVĚDI NA DOTAZ** Stručné odpovědi na dotazy členů Parlamentu	**VYBRANÁ TÉMATA** Studie zpracované k aktuálním problematikám	**MONITORING** Vybrané hospodářské měnové a sociální ukazatele	**MIGRACE** Přehled aktualit v oblasti migrace za vybrané období
	PŘEHLED SZBP Společná zahraniční a bezpečnostní politika EU	**EUROZÓNA+** Přehled ekonomických událostí v EU	**PODKLADY** pro zahraničně politická jednání	**PŘEDNÁŠKY** pro zahraniční delegace, PS, Senát	
Oddělení pro evropské záležitosti	**STANOVISKA** kompatibility nevládních návrhů zákonů s právem EU	**KONZULTACE** k předkládaným vládním návrhům zákonů	**DOKUMENTY EU** Výběr z aktů a dokumentů EU zaslaných PS	**ZPRÁVY** Aktuální agenda v Bruselu	**PODKLADY** pro jednání výboru na mezinárodní úrovni
Oddělení komunikace a vzdělávání	**INFORMAČNÍ STŘEDISKO** Informace o činnosti Poslanecké sněmovny a prohlídky budov	**ECPRD** Spolupráce s Evropským centrem pro parlamentní výzkum a dokumentaci	**PŘEDNÁŠKY** pro Poslaneckou sněmovnu, pro školy, veřejnost	**INFORMAČNÍ MATERIÁLY** o fungování Poslanecké sněmovny, o legislativním procesu	**ZÁPISY** ze schůzí, seminářů, přednášek, kulatých stolů

SDĚLENÍ

Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti
KOM(2016) 410 v konečném znění, kód Rady 11013/16

- **Právní základ:**
  Dokument informační povahy.

- **Datum zaslání Poslanecké sněmovně prostřednictvím VEZ:**
  11. 07. 2016

- **Procedura:**
  Není projednáváno legislativním postupem, jedná se o dokument nelegislativní povahy, který nepodléhá schválení v Radě a Evropském parlamentu. Procedura je ukončena jeho přijetím a předložením těmto institucím.

- **Předběžné stanovisko vlády (dle § 109a odst. 1 jednacího řádu PS):**
  Datované dnem 14. října 2016, doručené do výboru pro evropské záležitosti dne 26. října 2016 prostřednictvím systému ISAP.

- **Hodnocení z hlediska principu subsidiarity:**
  Hodnocení z hlediska principu subsidiarity se neuplatní, jedná se o dokument informační povahy.

- **Odůvodnění a předmět:**
  Sdělení popisuje opatření zaměřená na posílení evropského systému kybernetické odolnosti a na podporu konkurenceschopného a inovativního odvětví kybernetické bezpečnosti v Evropě, jak bylo uvedeno ve Strategii kybernetické bezpečnosti EU z roku 2013[1] a ve Strategii pro jednotný digitální trh[2].
  Dosavadní právní rámec v oblasti kybernetické bezpečnosti zahrnuje také směrnici o útocích na informační systémy[3] a směrnici o bezpečnosti sítí a informací,[4] jež má být členskými státy teprve implementována. Ze sdělení vyplývá, že navzdory některým pozitivním výsledkům činnosti EU v oblasti kybernetické bezpečnosti EU stále zůstává zranitelná vůči kybernetickým bezpečnostním incidentům.

---

[1] Společné Sdělení, Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor, JOIN/2013/01 v konečném znění, dostupné na: http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1476797849598&uri=CELEX:52013JC0001

[2] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Strategie pro jednotný digitální trh v Evropě, KOM(2015) 192 v konečném znění, dostupné na: http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1476708869729&uri=CELEX:52015DC0192

[3] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV, dostupná na: http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1476798075571&uri=CELEX:32013L0040

[4] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, dostupná na: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016L1148

- Obsah a dopad:

Sdělení se zabývá posílením spolupráce, znalostí a kapacity v rámci EU ve vztahu ke kybernetickým bezpečnostním incidentům, řešením problémů evropského jednotného trhu kybernetické bezpečnosti a rozvíjením průmyslových kapacit v oblasti kybernetické bezpečnosti.

Dosažení vyšší úrovně spolupráce, znalostí a kapacity

Komise ve sdělení vyzývá k užší spolupráci a sdílení informací napříč EU a ke zvýšení úrovně znalostí a kapacity, aby byla EU připravena na možné hrozby kybernetické bezpečnosti a uměla se lépe vypořádat s kybernetickými bezpečnostními incidenty. Svoji činnost k dosažení tohoto cíle Komise soustřeďuje okolo tří oblastí:

1) *Maximální využití mechanismů spolupráce podle směrnice o bezpečnosti sítí a informací a směřování k ENISA 2.0*

Komise má záměr předložit plán využívání mechanismů spolupráce podle směrnice o bezpečnosti sítí a informací včetně přeshraniční spolupráce, pokud se jedná o připravenost na rozsáhlý kybernetický bezpečnostní incident. Tento plán bude následně předložen skupině pro spolupráci, síti skupin CSIRT[5] a dalším subjektům v první polovině roku 2017.

Komise spolu s Evropskou agenturou pro bezpečnost sítí a informací (ENISA) a CERT-EU[6] dále podpoří vznik „informačního uzlu," který by orgánům EU a členským státům umožnil vyměňovat si příslušné informace. Na úrovni EU by také měla být zřízena poradní skupina na vysoké úrovni pro kybernetickou bezpečnost.

Komise do konce roku 2017 dokončí hodnocení agentury ENISA, které se bude zabývat potřebou změny nebo rozšíření jejího mandátu, s cílem v případě potřeby co nejdříve předložit návrh v tomto směru.

2) *Intenzivnější úsilí ve vzdělávání, odborné přípravě a cvičení v oblasti kybernetické bezpečnosti*

Komise ve sdělení zdůrazňuje význam dovedností a odborné přípravy jak při prevenci kybernetických bezpečnostním incidentů, tak v případě jejich řešení. Komise proto bude spolupracovat s členskými státy, agenturou ENISA, Evropskou službou pro vnější činnost (ESVČ) a dalšími subjekty při zřizování platformy pro odbornou přípravu v oblasti kybernetické bezpečnosti.

3) *Řešení meziodvětvových vzájemných závislostí a odolnosti klíčové veřejné síťové infrastruktury*

Komise po předchozím posouzení rizik kybernetických bezpečnostních incidentů s ohledem na vzájemnou provázanost různých odvětví zváží, zda jsou nutná další zvláštní pravidla a/nebo pokyny, pokud se jedná o připravenost na tato rizika. Komise se zaměří zejména na oblasti upravené směrnicí o bezpečnosti sítí a informací a přihlédne i k mezinárodnímu vývoji.
Na evropské úrovni se Komise zaměří na roli odvětvových středisek pro sdílení a analýzu informací (ISAC) a jejich spolupráci se sítí skupin CSIRT podle směrnice o bezpečnosti sítí a informací, dále s Evropským centrem pro boj proti kyberkriminalitě (EC3) při Europolu a s příslušnými donucovacími orgány.

[5] CSIRT (Computer Security Incident Response Team) jsou bezpečnostní týmy pro koordinaci řešení bezpečnostních incidentů v počítačových sítích.
[6] Skupina evropských orgánů, agentur a institucí pro reakci na počítačové hrozby.

Komise bude také usilovat o dobrovolná hlášení kybernetických krádeží obchodních tajemství prostřednictvím důvěryhodných kanálů.
V neposlední řadě hodlá Komise prozkoumat nezbytné právní a organizační podmínky, aby skupiny CSIRT mohly na požádání vnitrostátních regulačních orgánů ve spolupráci s vnitrostátními orgány pro kybernetickou bezpečnost provádět kontroly zranitelnosti veřejných sítí.

Řešení výzev, kterým čelí evropský jednotný trh kybernetické bezpečnosti

Sdělení také obsahuje několik iniciativ k řešení výzev jednotného trhu kybernetické bezpečnosti, jež mají vést k růstu průmyslových kapacit v oblasti kybernetické bezpečnosti. Komise ve sdělení uvádí, že trh s produkty a službami informačních a komunikačních technologií (IKT) v rámci EU je zeměpisně roztříštěný, což jednak ztěžuje hospodářskou soutěž a jednak omezuje výběr dostupných produktů a služeb pro podniky a občany.

Podpora rozvoje trhu s produkty a službami IKT

Komise uvádí následující oblasti, na které se dále zaměří za účelem podpory rozvoje trhu s produkty a službami IKT:

1) *Certifikace a označování*

Komise ve sdělení vyjadřuje svůj záměr nechat do konce roku 2016 vypracovat plán, který by mohl vést k přijetí návrhu evropského rámce pro certifikaci bezpečnosti informačních a komunikačních technologií do konce roku 2017. Certifikace by podle sdělení měla reflektovat mezinárodně uznávané normy a při jejím vývoji by měla probíhat spolupráce s mezinárodními partnery. Do postupu vytvoření tohoto rámce by měly být zapojeny také orgány veřejné správy, aby bylo možné používat společné specifikace při veřejných zakázkách a odkazovat na certifikaci.

Komise zároveň prozkoumá bezpečnost IKT v různých odvětvích infrastruktury a zjištěnými nedostatky se bude zabývat v rámci výše uvedeného evropského rámce pro certifikaci bezpečnosti informačních a komunikačních technologií.

2) *Zvýšení investic do kybernetické bezpečnosti v Evropě a podpora MSP*

Ze sdělení vyplývá, že na trhu EU existuje mnoho inovativních malých a středních podniků, které působí v oblasti kybernetické bezpečnosti, a to jak na specializovaných trzích (např. kryptografické systémy), tak na zavedených trzích (např. antivirové systémy). Tyto podniky však nemohou náležitě expandovat, neboť nemají dostatečné prostředky k financování svých aktivit.

Komise proto zdůrazňuje důležitost zvýšení povědomí malých a středních podniků o možnostech financování na evropské, vnitrostátní i regionální úrovni (např. prostřednictvím sítě Entreprise Europe Network). Komise bude dále ve spolupráci s Evropskou investiční bankou (EIB) a Evropským investičním fondem (EIF) usilovat o zlepšení jejich přístupu k financování, např. ve formě kapitálových a kvazikapitálových investic, půjček a záruk. Zvažováno je vytvoření platformy pro investice v oblasti kybernetické bezpečnosti v rámci Evropského fondu pro strategické investice (EFSI).
Komise se zabývá také možností rozvoje platformy pro inteligentní specializaci v kybernetické bezpečnosti a zavedení přístupu „bezpečnost už od návrhu“, podle něhož by požadavky na kybernetickou bezpečnost byly zahrnuty do všech návrhů s digitálním prvkem financovaných z fondů EU.

Vytvoření smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost

Komise v červenci 2016 zahájila smluvní partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost v rámci programu Horizont 2020 – rámcového programu EU pro výzkum a inovace pro období 2014-2020 - za účelem maximálního využití dostupných finančních prostředků. V prvním čtvrtletí roku 2017 zveřejní Komise výzvy k předkládání návrhů, které se týkají tohoto smluvního partnerství.

- Stanovisko vlády ČR:
  Vláda ČR sdělení Komise obecně vítá, staví se však rezervovaně k nově navrhovaným formátům informačního uzlu (information hub) a poradní skupiny na vysoké úrovni, neboť dle jejího názoru není jasně vymezen jejich účel. Vláda ČR má za to, že stávající Skupina pro spolupráci a síť CSIRT postačují jako platformy pro sdílení informací a koordinaci členských států a orgánů EU při zvyšování odolnosti vůči kybernetickým bezpečnostním incidentům. V této souvislosti vláda ČR preferuje soustředit se na zajištění účinného fungování Skupiny pro spolupráci a sítě CSIRT před zřizováním nových informační platforem a poradních skupin.

  Pokud se jedná o certifikaci, vláda ČR obecně volí princip technologické neutrality a upřednostňuje standardizaci před certifikací. Je však připravena podílet se na diskusích mezi Komisí a průmyslem týkajících se tohoto tématu.

  Dopad na rozpočet a právní řád

  Sdělení není legislativním aktem a nemá přímý dopad na rozpočet a právní řád ČR.

- Předpokládaný harmonogram projednávání v orgánech EU:
  Sdělení je nelegislativní dokument. Jeho projednávání v Evropském parlamentu je nyní v přípravné fázi. Příslušným k jeho projednání je výbor pro průmysl, výzkum a energetiku (ITRE). O stanovisko byl požádán také výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE), výbor pro vnitřní trh a ochranu spotřebitelů (IMCO) a výbor pro zahraniční věci (AFET). V Radě EU je dokument projednáván ve skupině přátel předsednictví pro kybernetické otázky.

- Projednávání ve výboru pro evropské záležitosti PS PČR:
  Výbor pro evropské záležitosti PS PČR projednal dokument dne 15. 12. 2016 a usnesením č. 331 přijal tyto závěry:

  Výbor pro evropské záležitosti:

  1. b e r e n a v ě d o m í sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti, KOM(2016) 410 v konečném znění, kód Rady 11013/16;

  2. p o d p o r u j e rámcovou pozici vlády ke sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti, KOM(2016) 410 v konečném znění, kód Rady 11013/16;

  3. s o u h l a s í se stanoviskem vlády, že členské státy mají primární úlohu v zajišťování své bezpečnosti a samy rozhodují o volbě prostředků zajišťujících jejich bezpečnostní zájmy při současném respektování potřeby koordinace reakcí na hrozby přicházející z kyberprostoru;

4. m á z a t o, že vzhledem k tomu, že členskými státy ještě nebyla implementována směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, je nyní předčasné přijímat další opatření pro využívání jí stanovených mechanismů spolupráce.