Parlament České republiky
POSLANECKÁ SNĚMOVNA
2013
6. volební období

321.

USNESENÍ

výboru pro evropské záležitosti
ze 45. schůze konané dne 23. května 2013

k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úroveně bezpečnosti sítí a informací v Unii /kód dokumentu 6342/13, KOM(2013) 48 v konečném znění/

ke společnému sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Strategie kybernetické bezpečnosti Evropské unie – Otevřený, bezpečný a chráněný kyberprostor /kód dokumentu 6225/13, JOIN(2013) 1 v konečném znění/

Výbor pro evropské záležitosti po vyslechnutí informace ředitele Národního bezpečnostního úřadu Ing. Dušana Navrátila, po vyslechnutí zpravodajské zprávy posl. Viktora Paggio a po rozpravě

s c h v a l u j e stanovisko, které je přílohou tohoto usnesení.

Josef Šenfeld v. r.	Viktor Paggio v. r.	Jan Bauer v. r.
ověřovatel výboru	zpravodaj výboru	předseda výboru

Příloha I k usnesení č. 321

NÁVRH SMĚRNICE

Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii

KOM(2013) 48 v konečném znění, kód Rady 6342/13
Interinstitucionální spis 2013/0027/COD

SDĚLENÍ

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) 1 v konečném znění, kód Rady 6225/13

- **Právní základ:**
  Článek 114 Smlouvy o fungování Evropské unie (návrh směrnice).
  Dokument informační povahy (sdělení).

- **Datum zaslání Poslanecké sněmovně prostřednictvím VEZ:**
  13. 2. 2013

- **Datum projednání ve VEZ:**
  28. 2. 2013 (1. kolo)

- **Procedura:**
  Spolurozhodovací (návrh směrnice).
  Dokument nepodléhá hlasování v Radě (sdělení).

- **Předběžné stanovisko vlády (dle § 109a odst. 1 jednacího řádu PS):**
  Datované dnem 6. března 2013 (návrh směrnice), resp. 7. března 2013 (sdělení), doručené do výboru pro evropské záležitosti dne 8. dubna 2013 prostřednictvím systému ISAP.

- **Hodnocení z hlediska principu subsidiarity:**
  Návrh je v souladu s principem subsidiarity.

- **Odůvodnění a předmět:**

  Předkládané sdělení[1] spolu s návrhem směrnice mají za cíl *zajistit bezpečné a důvěryhodné digitální prostředí* a současně prosazovat i chránit základní práva a další hodnoty, na jejichž základech stojí EU. Internet, resp. kyberprostor mají v posledních dvou desetiletích nesmírný vliv na všechny složky společnosti. Aby zůstal kyberprostor otevřený a svobodný, musí být podle Komise zajištěna dostatečná bezpečnost a ochrana jeho uživatelů před zlovolnými aktivitami a zneužitím. V současné době je význam informačních a komunikačních technologií nezpochybnitelný jak pro fungování ekonomiky EU obecně, tak pro dokončení vnitřního trhu umožňujícího volný pohyb osob, zboží, služeb a kapitálu, tedy základního přínosu evropské ekonomické integrace. Je proto důležité zajistit odolnost a stabilitu sítí a informačních systémů.

  Podle výsledků veřejné konzultace[2] a následného hodnocení Komise dospěla k závěru, že současný digitální svět je zranitelný, incidenty v oblasti kybernetické bezpečnosti se množí a ekonomika EU je již postižena kyberkriminálními aktivitami. Svoboda na internetu si žádá bezpečnost a ochranu, *nedostatečná ochrana sítí a informací může ohrozit zcela zásadní služby* závislé na integritě sítí a informačních systémů. Přitom v členských státech EU panuje roztříštěnost různých přístupů, současný společný přístup na evropské úrovni založený na čistě dobrovolné bázi nezajistí dostatečnou ochranu před bezpečnostními incidenty a riziky. V EU v současnosti neexistuje účinný mechanismus pro spolupráci a sdílení informací o rizicích a případech narušení bezpečnosti sítí a informací mezi členskými státy.

  Ve společném sdělení Komise spolu s Vysokou představitelkou EU pro zahraniční věci a bezpečnostní politiku představuje strategii kybernetické bezpečnosti pro EU, která by měla vést k vytvoření „nejbezpečnějšího on-line prostředí na světě“[3]. Souběžně předkládaný návrh směrnice představuje hlavní opatření této strategie.

- **Obsah a dopad:**
  <u>*Sdělení - Strategie kybernetické bezpečnosti Evropské unie*</u>

  Sdělení popisuje vizi EU pro oblast kybernetické bezpečnosti. Objasňuje zásady, jimiž by se strategie měla řídit, definuje strategické priority, popisuje úlohy a povinnosti zúčastněných stran a obsahuje výčet opatření, která by měla být přijata.

  Zásady strategie kybernetické bezpečnosti v EU:
  - Základní hodnoty EU platí nejen v reálném, ale i v kybernetickém světě;
  - Ochrana základních práv, svobody projevu, osobních údajů a soukromí;
  - Bezpečný přístup pro všechny;
  - Demokratické a účinné mnohostranné řízení digitálního světa;
  - Společná odpovědnost za zajištění bezpečnosti.

  Pět strategických priorit vize EU:
  1) *Dosažení kybernetické odolnosti*
     - zvyšování informovanosti

[1] Společné sdělení Komise a Vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku.
[2] Internetová veřejná konzultace na téma „Zvyšování bezpečnosti sítí a informací v EU,“ která probíhala od července do října 2012.
[3] Viz sdělení, str. 3.

2) *Výrazné omezení kyberkriminality*
   - silné a účinné právní předpisy
   - posílení operační kapacity pro boj proti kyberkriminalitě
   - lepší koordinace na úrovni EU
3) *Rozvoj politiky a kapacit kybernetické obrany v souvislosti s rámcem společné bezpečnostní a obranné politiky EU (SBOP)*
4) *Rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost*
   - podpora jednotného trhu s produkty souvisejícími s kybernetickou bezpečností
   - podpora investic do výzkumu a vývoje a inovace
5) *Zavedení soudržné mezinárodní politiky EU týkající se kyberprostoru a podpora základních hodnot EU*
   - začlenění otázek kyberprostoru do vnějších vztahů a společné zahraniční a bezpečnostní politiky EU

Navrhovaná strategie by měla být realizována na více úrovních. Vhodným řešením není centralizovaný dohled EU, jelikož většinu opatření mohou nejlépe realizovat národní vlády. Současně je však nezbytná koordinace a společná reakce na evropské úrovni, jelikož povaha hrozeb a rizik není omezena hranicemi jednotlivých členských států. Nadto by společně s Komisí a Vysokou představitelkou EU pro zahraniční věci a bezpečnostní politiku měly členské státy prosazovat koordinovaná mezinárodní opatření.

Členské státy
Členské státy by měly mít vybudované struktury pro řešení kybernetické odolnosti, kyberkriminality a obrany a měly by dosáhnout požadované úrovně kapacity k řešení kybernetických incidentů. Ve svých strategiích kybernetické bezpečnosti by měly stanovit úlohy a povinnosti jednotlivých vnitrostátních subjektů. V neposlední řadě je třeba také podporovat sdílení informací vnitrostátních orgánů a soukromých subjektů.

EU
Relevantní agentury EU[4] by měly navzájem spolupracovat a společně s Komisí, skupinou CERT-EU[5] a členskými státy vytvářet kvalitní technické a odborné zázemí. Neformální způsoby spolupráce a koordinace by měly být doplněny také strukturálními vazbami (personální propojení). Komise by pak měla vymezit rámec spolupráce prostřednictvím sítě příslušných vnitrostátních orgánů pro bezpečnost sítí a informací, který by zahrnoval sdílení informací mezi těmito orgány a donucovacími orgány.

Mezinárodní úroveň
Komise, Vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku a členské státy by měly ve vzájemné spolupráci zajistit koordinovaná mezinárodní opatření v oblasti kybernetické bezpečnosti a současně prosazovat základní hodnoty EU a podporovat mírové, otevřené a transparentní využívání kybernetických technologií.

V souladu s návrhem víceletého finančního rámce EU na období 2014-2020 by financování strategie mělo probíhat z následujících zdrojů: nástroj pro propojení Evropy, Horizont 2020, Fond pro vnitřní bezpečnost, SZBP a vnější spolupráce.

[4] Tj. agentury, které působí v oblasti bezpečnosti sítí a informací, prosazování práva a obrany – **ENISA** (Evropská agentura pro bezpečnost sítí a informací), **Europol/EC3** (Evropský policejní úřad/Evropské centrum pro boj proti kyberkriminalitě) a **EDA** (Evropská obranná agentura).
[5] Skupina pro reakci na počítačové hrozby odpovědná za bezpečnost IT systémů orgánů, agentur a subjektů EU. Zřízena v roce 2012.

Návrh směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii

Předložený návrh směrnice představuje konkrétní opatření v rámci výše zmíněné Strategie kybernetické bezpečnosti Evropské unie, jejichž účelem je zajistit vysokou společnou úroveň bezpečnosti sítí a informací v rámci EU. Směrnice tak:

a) stanoví povinnosti členských států týkající se prevence a řešení rizik a bezpečnostních incidentů postihujících sítě a informační systémy a reakce na ně;
b) vytváří mechanismus spolupráce mezi členskými státy, který má zajistit její jednotné uplatňování v celé EU, včetně postupu pro koordinované a účinné řešení rizik a bezpečnostních incidentů postihujících sítě a informační systémy a reakce na ně;
c) stanoví bezpečnostní požadavky pro hospodářské subjekty a orgány veřejné správy.

Národní rámce pro bezpečnost sítí a informací

Podle čl. 5 návrhu by měl každý členský stát přijmout *národní strategii pro bezpečnost sítí a informací*, která vymezí strategické cíle a zákonná opatření k dosažení a udržení vysoké úrovně bezpečnosti. Strategie by měla vymezit:

- cíle a priority na základě aktuální analýzy rizik a incidentů;
- řídící rámec pro naplnění těchto cílů a priorit, včetně jasně vymezených pravomocí a odpovědnosti příslušných orgánů;
- opatření týkající se připravenosti, reakce a obnovy, včetně mechanismu spolupráce soukromého a veřejného sektoru;
- vzdělávací, informační a školicí programy;
- plány výzkumu a vývoje.

Součástí této strategie by měl být rovněž tzv. *národní plán spolupráce pro bezpečnost sítí a informací*.

Podle čl. 6 návrhu by pak měl každý členský stát jmenovat *orgán odpovědný za bezpečnost sítí a informačních systémů*, který bude vykonávat dohled nad uplatňováním této směrnice, v souladu s čl. 7 návrhu rovněž zřídit *skupinu pro reakci na počítačové hrozby (CERT)* odpovědnou za řešení incidentů a rizik. Tato skupina může být zřízena v rámci odpovědného orgánu, kterému bude také podřízena.

Spolupráce mezi odpovědnými orgány

Podle čl. 8 návrhu by měla být zřízena *síť pro spolupráci* na ochranu proti rizikům a incidentům narušujícím bezpečnost sítí a informačních systémů, která bude představovat stálé komunikační spojení mezi Komisí a odpovědnými orgány. Výměna citlivých a důvěrných informací uvnitř této sítě bude probíhat s pomocí *bezpečného systému pro sdílení informací*.

Prostřednictvím sítě pro spolupráci budou vydávána *včasná varování* ohledně rizik a incidentů, v rámci kterých sdělí odpovědné orgány či Komise veškeré relevantní informace, které by mohly být užitečné při jejich posuzování. Po vydání včasného varování posoudí odpovědné orgány veškeré dostupné informace a dohodnou se na *koordinované reakci* v souladu s tzv. *unijním plánem spolupráce v oblasti bezpečnosti sítí a informací*[6], který přijme Komise do jednoho roku od vstupu směrnice v platnost.

V rámci sítě pro spolupráci bude možná spolupráce také na mezinárodní úrovni, a to na základě mezinárodních dohod mezi Unií a třetími zeměmi či mezinárodními organizacemi.

[6] K obsahu tohoto plánu viz čl. 12 odst. 2 návrhu.

Bezpečnost sítí a informačních systémů orgánů veřejné správy a hospodářských subjektů
Podle čl. 14 návrhu by měly členské státy zajistit, aby jejich orgány veřejné správy a hospodářské subjekty přijaly *vhodná technická a organizační opatření k řízení bezpečnostních rizik*[7], jimž čelí jejich sítě a informační systémy, a aby *oznamovaly odpovědným orgánům veškeré incidenty* mající významný dopad na bezpečnost jimi poskytovaných základních služeb. V návaznosti na to musí členské státy zajistit, aby odpovědné orgány mohly plnění těchto povinností prosazovat. Odpovědné orgány by tak měly být oprávněny dávat orgánům veřejné správy a hospodářským subjektům závazné pokyny, požadovat od nich informace potřebné k posouzení bezpečnosti jejich sítí a informačních systémů či požadovat, aby se podrobily bezpečnostnímu auditu.

Čl. 18 upravuje podmínky pro výkon přenesené pravomoci Komise, na základě které může přijímat akty provádějící některá ustanovení tohoto návrhu (čl. 9, čl. 10, čl. 14). O výkonu této pravomoci musí pravidelně podávat zprávu Evropskému parlamentu a Radě, které mohou přenesení pravomoci kdykoli zrušit. Komisi je nápomocen Výbor pro bezpečnost sítí a informací.[8]

- **Stanovisko vlády ČR:**
  <u>*Sdělení - Strategie kybernetické bezpečnosti Evropské unie*</u>
  Vláda ČR předloženou strategii vítá a vnímá ji jako důkaz úsilí EU o zajištění bezpečnosti kyberprostoru. Navrhovaná opatření jsou podle ní plně v souladu se současnými aktivitami ČR v oblasti kybernetické bezpečnosti i s aktuálně navrhovaným zákonem o kybernetické bezpečnosti. Rovněž ideové zaměření dokumentu je plně v souladu s politikou ČR v této oblasti.

  <u>*Návrh směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii*</u>
  Vláda ČR předložený návrh vítá a z hlediska jeho obsahu je pro ni v zásadě přijatelný. K některým bodům směrnice však hodlá v průběhu projednávání uplatnit připomínky. Za nesprávnou či příliš rozsáhlou například považuje delegaci pravomocí na Komisi týkající se přijímání prováděcích předpisů k jednotlivým ustanovením směrnice, ať už v případě článku 9 odst. 2, či v případě článku 14 odst. 5. Podstatné výhrady má také například k čl. 15 návrhu, týkající se orgánu oprávněného provádět bezpečnostní audit (odst. 2), oznamování incidentů, které mají povahu trestných činů, donucovacím orgánům (odst. 4) či spolupráce odpovědných orgánů s úřady pro ochranu osobních údajů (odst. 5).
  Vláda ČR bude rovněž usilovat o prodloužení lhůty pro transpozici směrnice podle čl. 21 návrhu, a to nejméně o půl roku.

- **Předpokládaný harmonogram projednávání v orgánech EU:**
  Projednávání společného sdělení v Evropském parlamentu je v současné době v přípravné fázi. V případě návrhu směrnice je projednávání v současnosti ve fázi prvního čtení. V Radě EU již bylo zahájeno projednávání obou dokumentů.

[7] Tato opatření by měla být standardizována Komisí formou prováděcích aktů (čl. 16 návrhu).
[8] Ve smyslu čl. 3 nařízení Evropského parlamentu a Rady (EU) č. 182/2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (tzv. komitologické nařízení).

- **Závěr:**

  Výbor pro evropské záležitosti:

1. **v í t á** společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor;

2. **p o d p o r u j e** snahy Komise o zajištění bezpečnosti a ochrany kyberprostoru prostřednictvím koordinovaného přístupu na celoevropské, ale i mezinárodní úrovni;

3. **b e r e n a v ě d o m í** návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii;

4. **p o d p o r u j e** rámcovou pozici vlády ČR k tomuto dokumentu ze dne 6. března 2013;

5. **p o v a ž u j e** delegaci pravomocí na Komisi v rozsahu navrženém směrnicí za neopodstatněnou**;**

6. **n e s o u h l a s í** s dopadem opatření v čl. 14 odst. 1 a 2 návrhu směrnice na všechny evropské podniky vyjma mikropodniků a **j e p ř e s v ě d č e n ,** že by se opatření zde uvedená měla soustředit pouze na strategické podniky, jejichž fungování je nezbytné pro základní chod společnosti;

7. **ž á d á v l á d u Č R ,** aby při projednávání v orgánech EU prosazovala změny v textu návrhu směrnice, které jsou vyznačeny v příloze tohoto usnesení;

8. **z á r o v e ň ž á d á v l á d u Č R ,** aby jej informovala o dalším průběhu a výsledcích projednávání návrhu směrnice v orgánech EU;

9. **p o v ě ř u j e** předsedu výboru, aby o tomto usnesení informoval Evropskou komisi.

Josef Šenfeld v. r.	Viktor Paggio v. r.	Jan Bauer v. r.
ověřovatel výboru	zpravodaj výboru	předseda výboru

Příloha II k usnesení č. 321 **k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii (KOM(2013) 48 v konečném znění) a společnému sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů - Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor (JOIN(2013) 1 v konečném znění) ze dne 23. 5. 2013:**

K textu návrhu směrnice:

1) ***Preambule odst. 1:*** *„Sítě a informační systémy a služby hrají ve společnosti zcela zásadní roli. Jejich spolehlivost a bezpečnost je nezbytná pro hospodářskou činnost* ***~~a sociální blahobyt~~*** *a především pro fungování vnitřního trhu.“*

   Komentář: Sítě a informační systémy a služby pro sociální blahobyt nezbytné nejsou. Důkazem jsou země, kde panuje sociální blahobyt i bez fungujících sítí.

2) ***Preambule odst. 5:*** *„Tato směrnice by se měla vztahovat na* ***~~všechny~~ vybrané*** *sítě a informační systémy, aby byly pokryty všechny relevantní incidenty a rizika. Povinnosti orgánů veřejné správy …“*

   Komentář: Text není v souladu s paragrafovým zněním návrhu.

3) ***Preambule odst. 18:*** *„Na základě především vnitrostátních zkušeností s řešením krizí a ve spolupráci s agenturou ENISA by členské státy měly vypracovat evropský plán spolupráce v oblasti bezpečnosti sítí a informací, který by vymezil mechanismy spolupráce pro potírání rizik a incidentů.”*

   Komentář: Nejasné, doporučujeme konkretizovat, kdo evropský plán spolupráce vypracuje.

4) ***Kap. I, čl. 6:*** *„Každý členský stát Komisi neprodleně oznámí jmenování odpovědného orgánu****~~,~~ a*** *jeho úkoly* ***~~a jakékoliv změny s ním související~~****. Každý členský stát zveřejní jmenování příslušného odpovědného orgánu.“*

   Komentář: Nesplnitelné. Ohlašovat skutečně všechny změny nelze.