



EVROPSKÁ
KOMISE

V Bruselu dne 30.5.2016
COM(2016) 363 final

2013/0027 (COD)

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU

podle čl. 294 odst. 6 Smlouvy o fungování Evropské unie

týkající se

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

(Text s významem pro EHP)

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU

podle čl. 294 odst. 6 Smlouvy o fungování Evropské unie

týkající se

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

(Text s významem pro EHP)

1. SOUVISLOSTI

Datum předání návrhu (COM(2013) 48 – 2013/0027 (COD))

Evropskému parlamentu a Radě:

7. 2. 2013

Datum vydání stanoviska Evropského hospodářského a sociálního výboru:

22. 5. 2013

Datum přijetí postoje Evropského parlamentu v prvním čtení:

13. 3. 2014

Datum přijetí postoje Rady:

17. 5. 2016

2. CÍL NÁVRHU KOMISE

Návrh za prvé vyžaduje, aby všechny členské státy zajistily alespoň minimální úroveň vnitrostátních kapacit, a to:

- zřízením příslušných orgánů pro bezpečnost sítí a informací,
- zřízením Skupin pro reakci na incidenty v oblasti počítačové bezpečnosti (CSIRT),
- přijetím vnitrostátních strategií bezpečnosti sítí a informací a vnitrostátních plánů spolupráce v této oblasti.

Za druhé by odpovědné vnitrostátní orgány měly spolupracovat v rámci sítě umožňující bezpečnou a efektivní spolupráci včetně koordinované výměny informací, jakož i odhalování a reakci na úrovni EU. Prostřednictvím této sítě by si členské státy měly vyměňovat informace a spolupracovat na potírání bezpečnostních hrozeb a incidentů na základě evropského plánu spolupráce v oblasti bezpečnosti sítí a informací. Aby bylo zajištěno řádné a včasné zapojení všech příslušných orgánů, návrh rovněž požaduje, aby byly donucovacím orgánům oznamovány incidenty trestní povahy a aby byl Europol zapojen do koordinačních mechanismů v rámci celé EU.

Za třetí je po vzoru rámcové směrnice o elektronických komunikacích cílem návrhu zajistit rozvoj kultury řízení rizik a sdílení informací mezi soukromým a veřejným sektorem. Společnosti z konkrétních klíčových odvětví a orgány veřejné správy budou mít povinnost posuzovat rizika, jimž čelí, a přijímat odpovídající a přiměřená opatření k zajištění bezpečnosti sítí a informací. Budou odpovědným orgánům povinně podávat zprávy o všech

incidentech, které vážně ohroží jejich sítě a informační systémy a které mají významný dopad na kontinuitu klíčových služeb a dodávek zboží.

3. PŘIPOMÍNKY K POSTOJI RADY

Rada ve svém postoji obecně schvaluje hlavní cíle návrhu Komise, tedy zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů. Provádí však řadu změn, pokud jde o způsoby dosažení tohoto cíle.

Vnitrostátní kapacity v oblasti kybernetické bezpečnosti

Na základě postoje Rady budou členské státy muset přijmout národní strategii pro bezpečnost sítí a informací, která stanoví strategické cíle a vhodná politická a regulační opatření v oblasti kybernetické bezpečnosti. Členské státy budou rovněž povinny určit příslušný vnitrostátní orgán pro provádění a prosazování směrnice, jakož i Skupiny pro reakci na incidenty v oblasti počítačové bezpečnosti (CSIRT) odpovědné za řešení incidentů a rizik.

Přestože postoj Rady členským státům neukládá, aby přijaly národní plán spolupráce pro bezpečnost sítí a informací, jak předpokládá původní návrh, lze tento postoj podpořit, jelikož některé aspekty plánu spolupráce jsou zachovány v ustanovení ohledně národní strategie pro bezpečnost sítí a informací.

Spolupráce mezi členskými státy

Na základě postoje Rady vytvoří směrnice „skupinu pro spolupráci“ složenou ze zástupců členských států, Komise a Agentury Evropské unie pro bezpečnost sítí a informací (ENISA), aby podporovala a usnadňovala strategickou spolupráci a výměnu informací mezi členskými státy. Směrnice rovněž vytvoří síť Skupin pro reakci na incidenty v oblasti počítačové bezpečnosti, nazývanou síť CSIRT, jež má podporovat rychlou a účinnou operativní spolupráci na konkrétních incidentech v oblasti kybernetické bezpečnosti a sdílení informací o rizicích.

Přestože se liší podstatně od přístupu použitého v původním návrhu, lze postoj Rady podpořit, neboť celkově odpovídá cíli zlepšení spolupráce mezi členskými státy.

Bezpečnostní požadavky a požadavky na oznamování incidentů pro provozovatele základních služeb

Na základě postoje Rady budou „provozovatelé základních služeb“ (pojem odpovídající „provozovatelům kritické infrastruktury“ v původním návrhu) povinni přijmout vhodná bezpečnostní opatření a oznamovat závažné incidenty příslušnému vnitrostátnímu orgánu. Rada však nepodpořila návrh, aby příslušné vnitrostátní orgány měly povinnost oznamovat incidenty trestní povahy donucovacím orgánům.

Podle původního návrhu se postoj Rady týká uvedených provozovatelů v oblasti energetiky, dopravy, bankovníctví, infrastruktury finančních trhů a zdravotnictví. Nicméně postoj Rady navíc zahrnuje také odvětví vodohospodářství a digitální infrastruktury.

Členské státy budou povinny určit tyto provozovatele na základě určitých kritérií, například zda jsou jejich služby zásadní pro zachování nejdůležitějších společenských či ekonomických činností. Ačkoli tento proces určení nebyl součástí původního návrhu, lze jej přijmout vzhledem k tomu, že členské státy mají povinnost předložit Komisi informace, které potřebuje k posouzení toho, zda členské státy používají k určení provozovatelů základních služeb jednotné postupy.

Orgány veřejné správy jako takové nejsou v postoji Rady zahrnuty. Pokud by však splnily kritéria stanovená podle článku 5, členské státy je budou muset určit jako provozovatele

základních služeb, jelikož provozovateli základních služeb mohou být veřejné i soukromé subjekty.

Bezpečnostní požadavky a požadavky na oznamování incidentů pro poskytovatele digitálních služeb

Na základě postoje Rady budou členské státy muset zajistit, aby poskytovatelé digitálních služeb přijali vhodná bezpečnostní opatření a oznamovali incidenty příslušnému orgánu. Postoj Rady zahrnuje online tržiště (odpovídající pojmu platformy pro elektronické obchodování v původním návrhu), služby cloud computingu a internetové vyhledávače. Ve srovnání s původním návrhem postoj Rady nezahrnuje:

- internetové platební brány – na ně se nyní vztahuje revidovaná směrnice o platebních službách,
- obchody s aplikacemi – ty je třeba chápat jako určitý druh online tržiště,
- sociální sítě – na základě politické dohody Rady s Evropským parlamentem.

Na základě postoje Rady byly Komisi uděleny prováděcí pravomoci pro stanovení procesních postupů nezbytných pro fungování skupiny pro spolupráci, jakož i pro upřesnění některých dalších prvků týkajících se poskytovatelů digitálních služeb, včetně formátů a postupů použitelných na oznamovací povinnosti těchto poskytovatelů.

Komise uvedené výsledky podporuje.

Po neformálních trojstranných jednáních ve dnech 14. října 2014, 11. listopadu 2014, 30. dubna 2015, 29. června 2015, 17. listopadu 2015 a 7. prosince 2015 dosáhly Evropský parlament a Rada ohledně tohoto znění předběžné politické dohody.

Rada tuto politickou dohodu potvrdila dne 18. prosince 2015. Dne 17. května 2016 přijala Rada postoj v prvním čtení.

4. ZÁVĚR

Komise podporuje výsledky interinstitucionálních jednání, a může proto přijmout postoj Rady v prvním čtení.