

V Bruseli 30. 5. 2016
COM(2016) 363 final

2013/0027 (COD)

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU

podľa článku 294 ods. 6 Zmluvy o fungovaní Európskej únie

o

**pozícii Rady k prijatiu smernice Európskeho parlamentu a Rady o opatreniach na
zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii**

(Text s významom pre EHP)

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU

podľa článku 294 ods. 6 Zmluvy o fungovaní Európskej únie

o

pozícii Rady k prijatiu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

(Text s významom pre EHP)

1. SÚVISLOSTI

Dátum predloženia návrhu Európskemu parlamentu a Rade
[COM(2013) 48 – 2013/0027(COD)] 7. 2. 2013

Dátum stanoviska Európskeho hospodárskeho a sociálneho výboru: 22. 5. 2013

Dátum pozície Európskeho parlamentu v prvom čítaní: 13. 3. 2014

Dátum prijatia pozície Rady: 17. 5. 2016

2. CIEĽ NÁVRHU KOMISIE

V prvom rade sa v návrhu vyžaduje, aby všetky členské štáty zabezpečili minimálnu úroveň vnútroštátnych spôsobilostí tým, že:

- ustanovia príslušné orgány pre bezpečnosti sietí a informácií;
- vytvoria jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT);
- prijmú vnútroštátnu stratégiu bezpečnosti sietí a informácií a vnútroštátny plán spolupráce v oblasti bezpečnosti sietí a informácií.

V druhom rade by príslušné vnútroštátne orgány mali spolupracovať v rámci siete, ktorá umožňuje bezpečnú a účinnú koordináciu vrátane koordinovanej výmeny informácií, ako aj zisťovania a reakcie na úrovni EÚ. Prostredníctvom tejto siete by si členské štáty mali vymieňať informácie a spolupracovať, aby na základe európskeho plánu spolupráce v oblasti bezpečnosti sietí a informácií odvrátili hrozby a incidenty v tejto oblasti. S cieľom zabezpečiť, aby sa všetky príslušné orgány náležite a včas zapojili, sa v návrhu takisto vyžaduje, aby sa orgánom presadzovania práva oznamovali incidenty trestnej povahy a aby bol Europol zapojený do koordinačných mechanizmov v rámci celej EÚ.

V treťom rade je podľa vzoru rámcovej smernice pre elektronické komunikácie cieľom návrhu zabezpečiť, aby sa vyvinula kultúra riadenia rizika a aby prebiehala výmena informácií medzi súkromným a verejným sektorom. Od spoločností v konkrétnych kritických odvetviach a od verejnej správy sa bude vyžadovať, aby posúdili riziká, ktorým čelia, a aby prijali vhodné a primerané opatrenia na zaistenie bezpečnosti sietí a informácií. Tieto subjekty

budú musieť oznamovať príslušným orgánom všetky incidenty, ktoré vážne ohrozujú ich siete a informačné systémy a majú značný vplyv na kontinuitu kritických služieb a dodávku tovaru.

3. PRIPOMIENKY K POZÍCII RADY

Celkovo Rada vo svojej pozícii podporuje hlavné ciele návrhu Komisie, t. j. zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov. Zavádza však niekoľko zmien, pokiaľ ide o spôsob dosiahnutia tohto cieľa.

Vnútroštátne spôsobilosti v oblasti kybernetickej bezpečnosti

Podľa pozície Rady sa od členských štátov bude vyžadovať, aby prijali vnútroštátne stratégie bezpečnosti sietí a informácií, ktorou sa stanovujú strategické ciele a vhodné politické a regulačné opatrenia v oblasti kybernetickej bezpečnosti. Členské štáty budú povinné určiť aj vnútroštátny príslušný orgán zodpovedný za vykonávanie a presadzovanie smernice, ako aj jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT) zodpovedné za riešenie incidentov a rizík.

Hoci Rada vo svojej pozícii od členských štátov nevyžaduje, aby prijali vnútroštátny plán spolupráce v oblasti bezpečnosti sietí a informácií, ako sa plánuje v pôvodnom návrhu, pozíciu možno podporiť, keďže niektoré aspekty plánu spolupráce sú v ustanovení o stratégii bezpečnosti sietí a informácií zachované.

Spolupráca medzi členskými štátmi

Podľa pozície Rady sa na základe smernice vytvorí „skupina pre spoluprácu“ zložená zo zástupcov členských štátov, Komisie a Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ďalej len „ENISA“) s cieľom podporovať a uľahčovať strategickú spoluprácu a výmenu informácií medzi členskými štátmi. Ďalej sa na základe smernice vytvorí sieť jednotiek pre riešenie počítačových incidentov, nazvaná sieť CSIRT, ktorá má podporovať rýchlu a účinnú operačnú spoluprácu pri konkrétnych incidentoch v oblasti kybernetickej bezpečnosti a výmenu informácií o rizikách.

Hoci sa podstatne líši od koncepcie načrtnutej v pôvodnom návrhu, pozíciu Rady možno podporiť, pretože celkovo zodpovedá cieľu zlepšiť spoluprácu medzi členskými štátmi.

Bezpečnostné požiadavky a požiadavky na oznamovanie incidentov platné pre prevádzkovateľov základných služieb

Podľa pozície Rady „prevádzkovatelia základných služieb“ (čo zodpovedá označeniu „prevádzkovatelia kritickej infraštruktúry“ v pôvodnom návrhu) budú povinní prijať vhodné bezpečnostné opatrenia a oznamovať závažné incidenty príslušným vnútroštátnym orgánom. Rada však nepodporila povinnosť vnútroštátnych príslušných orgánov oznamovať incidenty trestnej povahy orgánom presadzovania práva.

Vzhľadom na pôvodný návrh sa pozícia Rady vzťahovala na takýchto prevádzkovateľov v odvetviach energetiky, dopravy, bankovníctva, infraštruktúr finančných trhov a zdravotníctva. Avšak pozícia Rady okrem toho zahŕňa aj odvetvia vodohospodárstva a digitálnej infraštruktúry.

Členské štáty budú povinné identifikovať týchto prevádzkovateľov na základe určitých kritérií, napríklad či má služba zásadný význam z hľadiska zachovania najdôležitejších spoločenských alebo hospodárskych činností. Hoci tento proces identifikácie nebol súčasťou pôvodného návrhu, možno ho akceptovať vzhľadom na povinnosť členských štátov predkladať Komisii informácie, ktoré potrebuje na posúdenie toho, či členské štáty postupujú pri identifikácii poskytovateľov základných služieb jednotne.

Orgány verejnej správy ako také nie sú zahrnuté do pozície Rady. Ak by však spĺňali kritériá stanovené v článku 5, členské štáty ich budú musieť identifikovať ako prevádzkovateľov základných služieb, keďže prevádzkovatelia základných služieb môžu byť verejné alebo súkromné subjekty.

Bezpečnostné požiadavky a požiadavky na oznamovanie incidentov platné pre poskytovateľov digitálnych služieb

Podľa pozície Rady členské štáty budú musieť zabezpečiť, aby poskytovatelia digitálnych služieb prijali vhodné bezpečnostné opatrenia a oznamovali incidenty príslušnému orgánu. Pozícia Rady zahŕňa online trhoviská (zodpovedajúce pojmu platformy elektronického obchodu v pôvodnom návrhu), služby cloud computingu a online vyhľadávače. V porovnaní s pôvodným návrhom pozícia Rady nezahŕňa:

- internetové platobné portály – na ktoré sa teraz vzťahuje revidovaná smernica o platobných službách,
- obchody s aplikáciami – tie sa majú chápať ako určitý druh online trhoviska,
- sociálne siete – podľa politickej dohody Rady s Európskym parlamentom.

Na základe pozície Rady boli Komisii udelené vykonávacie právomoci na stanovenie procesných opatrení potrebných na fungovanie skupiny pre spoluprácu, ako aj pre spresnenie určitých ďalších prvkov týkajúcich sa poskytovateľov digitálnych služieb vrátane formátov a postupov uplatniteľných na požiadavky na oznamovanie platné pre poskytovateľov digitálnych služieb.

Komisia uvedené výsledky podporuje.

Po neformálnych trojstranných rokovaní, ktoré sa uskutočnili 14. októbra 2014, 11. novembra 2014, 30. apríla 2015, 29. júna 2015, 17. novembra 2015 a 7. decembra 2015, dosiahli Európsky parlament a Rada, predbežnú politickú dohodu, pokiaľ ide o toto znenie.

Rada túto politickú dohodu potvrdila 18. decembra 2015. Rada prijala pozíciu v prvom čítaní 17. mája 2016.

4. ZÁVER

Komisia podporuje výsledky medziinštitucionálnych rokovaní, a preto môže súhlasiť s pozíciou Rady v prvom čítaní.