EURÓPSKA
KOMISIA

V Bruseli 7. 2. 2013
COM(2013) 48 final

2013/0027 (COD)

Návrh

SMERNICA EURÓPSKEHO PARLAMENTU A RADY

o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii

{SWD(2013) 31 final}
{SWD(2013) 32 final}

DÔVODOVÁ SPRÁVA

Cieľom navrhovanej smernice je zabezpečiť vysokú úroveň bezpečnosti sietí a informácií (NIS). To znamená zvyšovať bezpečnosť internetu a súkromných sietí a informačných systémov, na ktorých je založené fungovanie našich spoločností a ekonomík. Dosiahne sa to tým, že od členských štátov sa bude požadovať, aby zvýšili svoju pripravenosť a zlepšili vzájomnú spoluprácu, a od prevádzkovateľov kritickej infraštruktúry, ako sú prevádzkovatelia v oblasti energetiky, dopravy a hlavní poskytovatelia služieb informačnej spoločnosti (platformy elektronického obchodu, sociálne siete), ako aj od verejnej správy sa bude požadovať, aby prijali príslušné opatrenia na riadenie bezpečnostných rizík a podávali správy o závažných incidentoch príslušným vnútroštátnym orgánom.

Tento návrh sa predkladá v súvislosti so spoločným oznámením Komisie a vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku o európskej stratégii kybernetickej bezpečnosti. Cieľom stratégie je zabezpečiť dôveryhodné a bezpečné digitálne prostredie, pričom je treba podporovať a ochraňovať základné práva a iné kľúčové hodnoty EÚ. Tento návrh je hlavnou akciou uvedenej stratégie. Ďalšie akcie v rámci stratégie v tejto oblasti sa zameriavajú na zvyšovanie povedomia, rozvoj vnútorného trhu s produktmi a službami kybernetickej bezpečnosti a podporovanie investícií v oblasti výskumu a vývoja. K týmto činnostiam pribudnú ďalšie, ktoré budú zamerané na zintenzívnenie boja proti kybernetickej kriminalite a budovanie medzinárodnej politiky pre kybernetickú bezpečnosť EÚ.

1.1. Dôvody a ciele návrhu

Bezpečnosť sietí a informácií je čoraz dôležitejšia pre naše hospodárstvo a spoločnosť. Je tiež dôležitým predpokladom na vytvorenie spoľahlivého prostredia pre celosvetový obchod so službami. Informačné systémy môžu byť však ovplyvnené bezpečnostnými incidentmi, ako sú napríklad ľudské chyby, prírodné udalosti, technické poruchy alebo škodlivé útoky. Tieto incidenty sú čoraz väčšieho rozsahu, vyskytujú sa častejšie a sú komplexnejšie. Komisia prostredníctvom verejných konzultácií na internete na tému „Zvýšenie bezpečnosti sietí a informácií v EÚ“[1] zistila, že 57 % respondentov malo počas minulého roka skúsenosť s incidentmi v oblasti bezpečnosti sietí a informácií, ktoré mali vážny vplyv na ich činnosti. Nedostatočná bezpečnosť sietí a informácií môže v závislosti od integrity sietí a informačných systémov ohroziť dôležité služby. To môže zastaviť chod podnikov, spôsobiť značné finančné straty pre hospodárstvo EÚ a negatívne ovplyvniť životné podmienky v spoločnosti.

Okrem toho digitálne informačné systémy, a najmä internet, ako komunikačné nástroje bez hraníc, sú v členských štátoch navzájom prepojené a hrajú významnú úlohu pri uľahčení pohybu tovaru, služieb a osôb cez hranice. Značné narušenie týchto systémov v jednom členskom štáte môže ovplyvniť aj ďalšie členské štáty a EÚ ako celok Preto je pre dokončenie jednotného digitálneho trhu a riadne fungovanie vnútorného trhu nevyhnutná odolnosť a stabilita sietí a informačných systémov. Pravdepodobnosť a častý výskyt incidentov, ako aj neschopnosť zabezpečiť efektívnu ochranu tiež narúša dôveru verejnosti v sieťové a informačné služby. Napríklad v prieskume Eurobarometra o kybernetickej bezpečnosti v roku 2012 sa zistilo, že 38 % používateľov internetu v EÚ má obavy o bezpečnosť platieb cez internet a zmenilo svoje návyky z dôvodu obáv v súvislosti s otázkami bezpečnosti. U 18 % používateľov je menšia pravdepodobnosť, že budú nakupovať prostredníctvom internetu, a u

[1] Verejná konzultácia na internete na tému „Zvýšenie bezpečnosti sietí a informácií v EÚ“ prebiehala od 23. júla do 15. októbra 2012.

15 % používateľov je menšia pravdepodobnosť, že využijú služby elektronického bankovníctva[2].

Súčasná situácia v EÚ, ktorá doposiaľ odrážala čisto dobrovoľný prístup, neposkytuje v celej EÚ dostatočnú ochranu proti incidentom a rizikám v oblasti bezpečnosti sietí a informácií. Existujúce kapacity a mechanizmy v oblasti bezpečnosti sietí a informácií sú jednoducho nepostačujúce na to, aby držali krok s rýchlo sa meniacim prostredím hrozieb a aby vo všetkých členských štátoch zabezpečovali vysokú spoločnú úroveň ochrany.

Napriek podniknutým iniciatívam je v členských štátoch rôzna úroveň spôsobilosti a pripravenosti, čo vedie k roztrieštеným prístupom v rámci celej EÚ. Keďže sú siete a systémy navzájom prepojené, tie členské štáty, ktoré nemajú dostatočnú úroveň ochrany, oslabujú celkovú bezpečnosť sietí a informácií EÚ. Táto situácia bráni aj vytváraniu dôvery medzi partnermi, ktorá je základným predpokladom spolupráce a vzájomnej výmeny informácií. V dôsledku toho existuje spolupráca len medzi malým počtom členských štátov, ktoré majú vysokú úroveň spôsobilosti.

Preto v súčasnosti neexistuje na úrovni EÚ žiadny účinný mechanizmus pre účinnú spoluprácu a dôvernú výmenu informácií o incidentoch a rizikách v oblasti bezpečnosti sietí a informácií medzi členskými štátmi. Toto môže mať za následok nekoordinované zásahy regulačných orgánov, nesúvisiace stratégie a rôznorodé normy, čo povedie k nedostatočnej ochrane sietí a informácií v EÚ. Vzniknúť môžu aj prekážky na vnútornom trhu prinášajúce tým spoločnostiam, ktoré vykonávajú svoju činnosť vo viac než jednom členskom štáte, náklady na zabezpečenie súladu.

[2] Eurobarometer 390/2012

Nakoniec subjekty, ktoré riadia kritickú infraštruktúru alebo poskytujú služby nevyhnutné pre fungovanie našich spoločností, nie sú primerane zaviazané prijímať opatrenia na riadenie rizík ani vymieňať si informácie s príslušnými orgánmi. Na jednej strane chýbajú preto podnikom účinné stimuly na riadenie závažných rizík vrátane vyhodnotenia rizika a prijatie primeraných opatrení na zabezpečenie bezpečnosti sietí a informácií. Na druhej strane informácie o veľkej časti incidentov sa nedostanú k príslušným orgánom a zostanú nepovšimnuté. Informácie o incidentoch sú však nevyhnutné na to, aby mohli verejné orgány reagovať, prijať primerané opatrenia na zníženie rizika a stanoviť primerané strategické priority v oblasti bezpečnosti sietí a informácií.

Podľa súčasného regulačného rámca sa vyžaduje iba od telekomunikačných spoločností, aby prijali opatrenia na riadenie rizík a podávali správy o závažných incidentoch. Mnohé iné odvetvia však taktiež využívajú informačné a komunikačné technológie (IKT) na sprostredkovanie informácií, a preto by sa mali tiež zaujímať o bezpečnosť sietí a informácií. Obzvlášť zraniteľných je niekoľko špecifických infraštruktúr a poskytovateľov služieb, a to vzhľadom na ich vysokú závislosť na správnom fungovaní sietí a informačných systémov. Tieto odvetvia hrajú pri poskytovaní kľúčových podporných služieb pre naše hospodárstvo a spoločnosť dôležitú úlohu a bezpečnosť ich systémov je obzvlášť dôležitá pre fungovanie vnútorného trhu. Do týchto odvetví patrí bankovníctvo, burza cenných papierov, výroba, prenos a distribúcia energie, doprava (letecká, železničná, námorná), zdravotníctvo, internetové služby a verejná správa.

Preto sú potrebné viditeľné zmeny, pokiaľ ide o spôsob, akým sa v EÚ zaobchádza s bezpečnosťou sietí a informácií. Na vytvorenie rovnakých podmienok pre všetkých a odstránenie existujúcich legislatívnych medzier sú potrebné regulačné povinnosti. V záujme riešenia týchto problémov a zvýšenia úrovne bezpečnosti sietí a informácií v Európskej únii sú ciele navrhovanej smernice tieto:

V prvom rade sa v návrhu vyžaduje, aby všetky členské štáty zabezpečili zavedenie minimálnej úrovne vnútroštátnej spôsobilosti tým, že určia príslušné orgány zodpovedné za bezpečnosť sietí a informácií, vytvoria tímy reakcie na núdzové počítačové situácie (CERT) v oblasti bezpečnosti sietí a informácií a prijmú vnútroštátne stratégie a plány 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.

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

1.2. Všeobecný kontext

Už v roku 2001 Komisia vo svojom oznámení o bezpečnosti sietí a informácií: Návrh na európsky politický prístup opísala rastúci význam bezpečnosti sietí a informácií[3]. Po ňom

[3] KOM(2001) 298.

nasledovalo v roku 2006 prijatie stratégie pre bezpečnú informačnú spoločnosť[4] s cieľom rozvíjať v Európe kultúru bezpečnosti sietí a informácií. Jej hlavné prvky boli schválené v uznesení Rady[5].

Komisia 30. marca 2009 ďalej prijala oznámenie o ochrane kritických informačných infraštruktúr (CIIP)[6], ktoré je zamerané na ochranu Európy pred narušeniami kybernetickej bezpečnosti prostredníctvom zvyšovania bezpečnosti. Oznámením sa začal akčný plán na podporu členských štátov v ich snahe o zabezpečenie prevencie a reakcie. Akčný plán bol schválený v záveroch predsedníctva ministerskej konferencie o CIIP v Taline v roku 2009. Rada prijala dňa 18. decembra 2009 rezolúciu o „spoločnom európskom prístupe k bezpečnosti sietí a informácií“[7].

V Digitálnej agende pre Európu[8] (DAE), ktorá bola prijatá v máji 2010, a v súvisiacich záveroch Rady[9] sa zdôraznilo spoločné porozumenie, že dôvera a bezpečnosť sú základné predpoklady pre široké využívanie IKT, a tým aj pre dosiahnutie cieľov stratégie Európa 2020[10] týkajúcich sa „inteligentného rastu“. V kapitole o dôvere a bezpečnosti sa v agende DAE kladie dôraz na potrebu, aby všetky zúčastnené strany spojili svoje sily v holistickom úsilí a zabezpečovali odolnosť a bezpečnosť infraštruktúry IKT tým, že sa zamerajú na prevenciu, pripravenosť a informovanosť a budú vyvíjať účinné a koordinované bezpečnostné mechanizmy. Najmä kľúčové opatrenie č. 6 Digitálnej agendy pre Európu si vyžaduje opatrenia zamerané na posilnenie a vysokú úroveň politiky v oblasti bezpečnosti sietí a informácií.

Vo svojom oznámení o CIIP z marca 2011 o ochrane kritických informačných infraštruktúr „Dosiahnuté ciele a ďalšie kroky: na ceste ku globálnej kybernetickej bezpečnosti“[11], Komisia zvážila výsledky dosiahnuté od prijatia akčného plánu CIIP v roku 2009, pričom dospela k záveru, že realizácia plánu preukázala, že pri riešení výziev bezpečnosti a odolnosti nie je postačujúci len národný prístup a že Európa by mala pokračovať vo svojom úsilí o vybudovanie uceleného a spoločného prístupu v rámci celej EÚ. V oznámení o CIIP z roku 2011 Komisia uviedla niekoľko opatrení, pričom vyzvala členské štáty, aby zabezpečili spôsobilosť na zabezpečenie bezpečnosti sietí a informácií a cezhraničnú spoluprácu. Väčšina týchto opatrení mala byť ukončená do roku 2012, neboli však ešte vykonané.

Rada Európskej únie vo svojich záveroch o CIIP z 27. mája 2011 zdôraznila naliehavú potrebu zabezpečiť, aby boli systémy a siete IKT bezpečné a odolné proti všetkým možným narušeniam, náhodným alebo úmyselným, aby sa v rámci EÚ vytvorili kapacity s vysokou úrovňou pripravenosti, bezpečnosti a odolnosti, aby sa zvýšila odborná spôsobilosť, čo by Európe umožnilo čeliť problémom v oblasti ochrany sietí a informačných infraštruktúr, a aby sa podporila spolupráca medzi členskými štátmi prostredníctvom vytvorenia mechanizmov spolupráce na riešenie incidentov medzi členskými štátmi.

---

4 KOM(2006) 251 http://www.cc.cec/sg_vista/cgi-bin/repository/getdoc/COMM_PDF_COM_2006_0251_F_SK_ACTE.pdf.

5 2007/068/01.

6 KOM(2009) 149.

7 2009/C 321/01.

8 COM(2010) 245.

9 Závery Rady z 31. mája 2010 o Digitálnej agende pre Európu (10130/10).

10 COM (2010) 2020 a Závery Európskej rady z 25. a 26. marca 2010 (EUCO 7/10).

11 COM(2011) 163.

1.3. Existujúce ustanovenia Európskej únie a medzinárodné ustanovenia v tejto oblasti

V súlade s nariadením (ES) č. 460/2004 Európske spoločenstvo zriadilo v roku 2004 Európsku agentúru pre bezpečnosť sietí a informácií (ENISA)[12], aby prispievala k zabezpečovaniu vysokej úrovne bezpečnosti sietí a informácií a rozvoju jej kultúry v rámci EÚ. Dňa 30. septembra 2010 bol prijatý návrh na modernizáciu mandátu agentúry ENISA[13], ktorý je predmetom diskusie v Rade a Európskom parlamente. Na základe revidovaného regulačného rámca pre elektronické komunikácie[14], ktorý je v platnosti od novembra 2009, majú poskytovatelia elektronických komunikačných služieb povinnosť zaviesť bezpečnostné opatrenia[15]. Táto povinnosť mala byť na vnútroštátnej úrovni transponovaná do mája 2011.

Všetci účastníci trhu, ktorí sú prevádzkovateľmi údajov (napríklad banky alebo nemocnice), sú podľa regulačného rámca na ochranu údajov[16] povinní zaviesť bezpečnostné opatrenia na ochranu osobných údajov. Na základe návrhu všeobecného nariadenia o ochrane údajov predloženého Komisiou v roku 2012[17] by prevádzkovatelia údajov mali tiež hlásiť nepovolený prístup k osobným údajom národným dozorným orgánom. To znamená, že napríklad narušenie bezpečnosti sietí a informácií, ktoré má vplyv na poskytovanie služieb bez toho, aby ohrozilo osobné údaje (napríklad výpadok v oblasti informačných a komunikačných technológií v elektrárni, ktorý má za následok výpadok dodávky elektrického prúdu) by nemuselo byť oznámené.

Podľa smernice 2008/114 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu sa v Európskom programe na ochranu kritickej infraštruktúry (EPCIP)[18] stanovuje celkový „ zastrešujúci“ prístup k ochrane kritickej infraštruktúry v EÚ. Ciele programu EPCIP sú v plnej miere v súlade s týmto návrhom a smernica by sa mala uplatňovať bez toho, aby bola dotknutá smernica 2008/114. Program EPCIP nezaväzuje účastníkov trhu, aby podávali správy o závažnom porušení bezpečnosti, ani nestanovuje pre členské štáty mechanizmy na spoluprácu pre prípad incidentov a na reakciu na ne.

Spoluzákonodarcovia v súčasnosti rokujú o návrhu smernice o útokoch proti informačným systémom[19], ktorý sa zameriava na harmonizáciu kriminalizácie určitých spôsobov správania. Vzťahuje sa len na kriminalizáciu určitých spôsobov správania a nezaoberá sa prevenciou rizík bezpečnosti sietí a informácií ani incidentov v tejto oblasti ani reakciou na takéto incidenty či zmiernenie ich vplyvu. Súčasná smernica by sa mala uplatňovať bez toho, aby bola dotknutá smernica o útokoch proti informačným systémom.

Komisia prijala dňa 28. marca 2012 oznámenie o zriadení Európskeho centra boja proti kybernetickej kriminalite (EC3)[20]. Toto centrum, ktoré bolo zriadené 11. januára 2013, je súčasťou Európskeho policajného úradu (Europol) a funguje ako kontaktné miesto v boji proti kybernetickej kriminalite v EÚ. Centrum EC3 má šíriť odborné poznatky v oblasti

---

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:SK:HTML.

13 COM(2010) 521.

14 Pozri http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Články 13a a 13b rámcovej smernice.

16 Smernica 2002/58 z 12. júla 2002.

17 COM(2012) 11.

18 KOM(2006) 786 http://www.cc.cec/sg_vista/cgi-bin/repository/getdoc/COMM_PDF_COM_2006_0786_F_SK_ACTE.pdf.

19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:sk:PDF.

20 COM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:SK:PDF.

kybernetickej kriminality s cieľom podporovať členské štáty pri budovaní kapacít, poskytovať členským štátom podporu pri vyšetrovaní kybernetickej kriminality a v úzkej spolupráci s Eurojustom sa stať spoločným hlasom európskych vyšetrovateľov kybernetickej kriminality v oblasti presadzovania práva a súdnictva.

Európske inštitúcie, agentúry a orgány zostavili svoj vlastný tím reakcie na núdzové počítačové situácie, tzv. CERT-EÚ.

Na medzinárodnej úrovni pracuje Európska únia na kybernetickej bezpečnosti tak na bilaterálnej, ako aj multilaterálnej úrovni. Samit EÚ – USA 2010[21] zaznamenal zriadenie pracovnej skupiny EÚ – USA pre kybernetickú bezpečnosť a kybernetickú kriminalitu. EÚ je činná aj v iných príslušných multilaterálnych fórach, ako je Organizácia pre hospodársku spoluprácu a rozvoj (OECD), Valné zhromaždenie Organizácie Spojených národov (VZ OSN), Medzinárodná telekomunikačná únia (ITU), Organizácia pre bezpečnosť a spoluprácu v Európe (OBSE), svetový samit o informačnej spoločnosti a Fórum o riadení internetu.

2. VÝSLEDKY KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

2.1. Konzultácie so zainteresovanými stranami a využitie odborných znalostí

Verejná konzultácia na internete na tému „Zvýšenie bezpečnosti sietí a informácií v EÚ“ prebiehala od 23. júla do 15. októbra 2012. Komisii bolo celkovo doručených 160 vyplnených dotazníkov online.

Hlavným výsledkom bolo, že zainteresované strany preukázali všeobecnú podporu, čo sa týka potreby zlepšenia bezpečnosti sietí a informácií v rámci celej EÚ. Napríklad: 82,8 % respondentov vyjadrilo názor, že vlády v EÚ by mali vyvinúť viac úsilia na zabezpečenie vyššej úrovne bezpečnosti sietí a informácií. 82,8 % respondentov zastávalo názor, že používatelia informácií a systémov nemajú vedomosti o existujúcich hrozbách a incidentoch v oblasti bezpečnosti sietí a informácií; 66,3 % respondentov by v zásade podporovalo zavedenie regulačných požiadaviek na riadenie rizík bezpečnosti sietí a informácií a 84,8 % respondentov uviedlo, že takéto požiadavky by mali byť stanovené na úrovni EÚ. Mnohí respondenti sa domnievali, že by bolo potrebné prijať požiadavky v oblasti bezpečnosti sietí a informácií najmä v týchto sektoroch: bankovníctvo a financie (91,1 %), energetika (89,4 %), doprava (81,7 %), zdravotníctvo (89,4 %), internetové služby (89,1 %) a verejná správa (87,5 %). Respondenti takisto uviedli, že ak by sa zaviedla požiadavka hlásiť narušenie bezpečnosti sietí a informácií príslušnému vnútroštátnemu orgánu, malo by sa tak stanoviť na úrovni EÚ (65,1 %) a potvrdili, že by sa mala vzťahovať aj na verejnú správu (93,5 %). Nakoniec respondenti uviedli, že požiadavka na realizáciu riadenia rizík v oblasti bezpečnosti sietí a informácií s ohľadom na najnovší technologický vývoj by pre nich nepredstavovala žiadne významné dodatočné náklady (63,4 %) a že ani požiadavka, aby oznamovali narušenia bezpečnosti, by pre nich nepredstavovala žiadne významné dodatočné náklady (72,3 %).

V niektorých príslušných zloženiach Rady sa uskutočnili konzultácie s členskými štátmi v rámci Európskeho fóra pre členské štáty (EFMS) na konferencii o kybernetickej bezpečnosti, ktorú zorganizovala Komisia a Európska služba pre vonkajšiu činnosť 6. júla 2012, a na vyhradených bilaterálnych stretnutiach zvolaných na žiadosť jednotlivých členských štátov.

[21] http://europa.eu/rapid/press-release_MEMO-10-597_sk.htm

Rozhovory so súkromným sektorom sa uskutočnili aj v rámci Európskeho verejno-súkromného partnerstva pre odolnosť[22] a prostredníctvom bilaterálnych stretnutí. Čo sa týka verejného sektora, Komisia viedla rozhovory s agentúrou ENISA a tímom CERT pre EÚ.

2.2. Posúdenie vplyvu

Komisia uskutočnila posúdenie vplyvu troch možností politiky:

Možnosť č. 1: Pokračovať obvyklým spôsobom (základný scenár): zachovanie súčasného prístupu.

Možnosť č. 2: Regulačný prístup, ktorého súčasťou je legislatívny návrh na vytvorenie spoločného právneho rámca EÚ v oblasti bezpečnosti sietí a informácií, pokiaľ ide o kapacity členských štátov, mechanizmy na spoluprácu na úrovni EÚ a požiadavky na kľúčových účastníkov trhu zo súkromnej sféry a na verejnú správu.

Možnosť č. 3: Zmiešaný prístup, ktorý spája dobrovoľné iniciatívy v oblasti bezpečnosti sietí a informácií, pokiaľ ide o kapacity členských štátov, a mechanizmy na spoluprácu na úrovni EÚ s právnymi požiadavkami na kľúčových účastníkov trhu zo súkromnej sféry a na verejnú správu.

Komisia dospela k záveru, že najvýraznejší pozitívny vplyv by mala možnosť č. 2, pretože by značne zlepšila ochranu spotrebiteľov, podnikov a verejnej správy EÚ proti incidentom v oblasti bezpečnosti sietí a informácií. Najmä povinnosti uložené členským štátom by zabezpečili zodpovedajúcu pripravenosť na vnútroštátnej úrovni a prispeli by k atmosfére vzájomnej dôvery, ktorá je základnou podmienkou pre účinnú spoluprácu na úrovni EÚ. Vytváranie mechanizmov spolupráce na úrovni EÚ prostredníctvom siete by prinieslo súdržnú a koordinovanú prevenciu a reakciu na cezhraničné incidenty a riziká v oblasti bezpečnosti sietí a informácií. Zavedenie požiadaviek na realizáciu riadenia rizík v oblasti bezpečnosti sietí a informácií pre orgány verejnej správy a kľúčových účastníkov trhu zo súkromnej sféry by bolo silným podnetom na účinné riadenie bezpečnostných rizík. Povinné oznamovanie incidentov v oblasti bezpečnosti sietí a informácií, ktoré majú významný vplyv, by zlepšilo schopnosť reagovať na incidenty a podporovať transparentnosť. Okrem toho, keď si EÚ spraví poriadok doma, môže rozšíriť svoj medzinárodný dosah a stať sa ešte dôveryhodnejším partnerom na spoluprácu na bilaterálnej a multilaterálnej úrovni. EÚ by tým mala aj lepšiu pozíciu pri podpore základných práv a kľúčových hodnôt EÚ v zahraničí.

Kvantitatívne hodnotenie ukázalo, že možnosť č. 2 by nepredstavovala pre členské štáty neprimeranú záťaž. Náklady v súkromnom sektore by boli takisto obmedzené, pretože mnohé príslušné subjekty už musia dodržiavať existujúce bezpečnostné požiadavky (konkrétne prevádzkovatelia údajov majú povinnosť prijať technické a organizačné opatrenia na zabezpečenie osobných údajov vrátane opatrení v oblasti bezpečnosti sietí a informácií). Zohľadňujú sa aj súčasné výdavky na bezpečnosť v súkromnom sektore.

V tomto návrhu sú dodržané zásady uznané najmä Chartou základných práv Európskej únie, právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastniť majetok, právo na účinný opravný prostriedok pred súdom a právo na vypočutie. Táto smernica sa musí vykonávať v súlade s týmito právami a zásadami.

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

3. PRÁVNE PRVKY NÁVRHU

3.1. Právny základ

Európska únia je oprávnená prijímať opatrenia s cieľom vytvoriť vnútorný trh alebo zabezpečiť jeho fungovanie v súlade s príslušnými ustanoveniami zmlúv (článok 26 Zmluvy o fungovaní Európskej únie – ZFEÚ). Podľa článku 114 ZFEÚ môže EÚ prijímať „opatrenia na *aproximáciu ustanovení zákonov, iných právnych predpisov a správnych opatrení členských štátov*, ktoré smerujú k vytváraniu a fungovaniu vnútorného trhu".

Ako je uvedené vyššie, siete a informačné systémy zohrávajú dôležitú úlohu pri uľahčovaní cezhraničného pohybu tovaru, služieb a osôb. Často sú navzájom prepojené a internet má globálny charakter. Vzhľadom na tento skutočne nadnárodný rozmer, narušenie v jednom členskom štáte môže mať vplyv aj na ďalšie členské štáty a EÚ ako celok. Preto je pre riadne fungovanie vnútorného trhu nevyhnutná odolnosť a stabilita sietí a informačných systémov.

Zákonodarca Spoločenstva už uznal potrebu harmonizovať pravidlá v oblasti bezpečnosti sietí a informácií, aby sa zabezpečil rozvoj vnútorného trhu. Najmä to bol prípad nariadenia 460/2004 o zriadení agentúry ENISA[23], ktoré sa zakladá na článku 114 ZFEÚ.

Rozdiely vyplývajúce z nerovnomerných vnútroštátnych spôsobilostí a politík v oblasti bezpečnosti sietí a informácií, ako aj z úrovne ochrany v členských štátoch, viedli k vzniku prekážok vnútorného trhu a zdôvodnili opatrenia EÚ.

3.2. Subsidiarita

Zásahy na úrovni EÚ v oblasti bezpečnosti sietí a informácií sú odôvodnené zásadou subsidiarity.

V prvom rade, vzhľadom na cezhraničnú povahu bezpečnosti sietí a informácií by nezasahovanie zo strany EÚ viedlo k situácii, v ktorej by každý členský štát konal samostatne, bez ohľadu na vzájomnú závislosť sietí a informačných systémov v EÚ. Primeraná úroveň koordinácie medzi členskými štátmi by zabezpečila, aby boli riziká v oblasti bezpečnosti sietí a informácií v cezhraničnom kontexte, v ktorom vznikajú, správne riadené. Rozdiely v nariadeniach v oblasti bezpečnosti sietí a informácií sú obmedzujúce pre spoločnosti, ktoré chcú podnikať vo viacerých krajinách, ako aj pre dosiahnutie celkových úspor z rozsahu.

V druhom rade sú regulačné povinnosti na úrovni EÚ potrebné na vytvorenie rovnakých podmienok pre všetkých a na odstránenie legislatívnych medzier. V dôsledku čisto dobrovoľného prístupu existuje spolupráca len medzi malým počtom členských štátov, ktoré majú vysokú úroveň kapacít. V záujme zapojenia všetkých členských štátov je potrebné zabezpečiť, aby mali všetky požadovanú minimálnu úroveň spôsobilostí. Opatrenia prijaté vládami v oblasti bezpečnosti sietí a informácií musia byť vo vzájomnom súlade a musia byť koordinované, aby zabránili dôsledkom incidentov v oblasti bezpečnosti sietí a informácií alebo aby ich minimalizovali. Príslušné orgány a Komisia budú v rámci siete a prostredníctvom výmeny osvedčených postupov a stáleho zapojenia agentúry ENISA spolupracovať v záujme jednotného vykonávania smernice v celej EÚ. Okrem toho, zosúladený postup v oblasti bezpečnosti sietí a informácií môže mať výrazne pozitívny vplyv na účinnú ochranu základných práv a konkrétne práva na ochranu osobných údajov a súkromia. Preto by opatrenia na úrovni EÚ zlepšili účinnosť existujúcich národných politík a uľahčili ich rozvoj.

Navrhované opatrenia sú opodstatnené aj z dôvodu proporcionality. Požiadavky na členské štáty sú stanovené na minimálnu úroveň, ktorá je potrebná na dosiahnutie primeranej

[23] Nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií (Ú. v. EÚ L 077 13.3.2004, s. 1).

pripravenosti, aby umožnila spoluprácu založenú na dôvere. To tiež umožní členským štátom, aby riadne zohľadnili svoje vnútroštátne špecifiká a zabezpečili, aby boli spoločné zásady EÚ uplatňované primeraným spôsobom. Vďaka širokému rozsahu pôsobnosti budú môcť členské štáty vykonávať smernicu s ohľadom na skutočné riziká, ktorým čelia a ktoré majú uvedené vo svojej vnútroštátnej stratégii pre bezpečnosť sietí a informácií. Požiadavky na realizáciu cieľa riadenia rizík sú zamerané len na kritické subjekty a zahŕňajú opatrenia, ktoré sú primerané riziku. Vo verejnej konzultácii sa zdôraznil význam zabezpečenia bezpečnosti týchto subjektov. Požiadavky na podávanie správ by sa týkali iba incidentov s významným vplyvom. Ako bolo už uvedené, opatrenia by nepredstavovali neprimerané náklady, keďže od mnohých z týchto subjektov ako prevádzkovateľov sa podľa súčasných pravidiel o ochrane údajov už vyžaduje, aby zabezpečovali ochranu osobných údajov.

Aby sa na malých prevádzkovateľov, najmä na malé a stredné podniky, nekládla neprimeraná záťaž, požiadavky sú primerané riziku, ktoré predstavuje daná sieť alebo informačný systém, a nemali by sa uplatňovať na mikropodniky. V prvom rade subjekty, na ktoré sa tieto povinnosti vzťahujú, budú musieť identifikovať riziká a budú sa musieť rozhodnúť, aké opatrenia prijmú na zmiernenie týchto rizík.

Vzhľadom na cezhraničné aspekty incidentov a rizík v oblasti bezpečnosti sietí a informácií možno uvedené ciele lepšie dosiahnuť na úrovni EÚ než na úrovni jednotlivých členských štátov. EÚ preto môže prijímať opatrenia v súlade so zásadou subsidiarity, ako je stanovená v článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality navrhovaná smernica neprekračuje rámec toho, čo je nevyhnutné na dosiahnutie týchto cieľov.

V záujme dosiahnutia cieľov by Komisia mala byť splnomocnená prijímať delegované akty v súlade s článkom 290 Zmluvy o fungovaní Európskej únie s cieľom doplniť alebo zmeniť a doplniť určité nepodstatné prvky základného aktu. Cieľom návrhu Komisie je podporiť aj uplatňovanie proporcionality pri zavádzaní povinností uložených súkromným a verejným subjektom.

S cieľom zabezpečiť jednotné podmienky na vykonávanie základného aktu, Komisia by mala mať v súlade s článkom 291 Zmluvy o fungovaní Európskej únie právomoc prijímať vykonávacie akty.

Vzhľadom najmä na veľký rozsah pôsobnosti navrhovanej smernice, na skutočnosť, že sa v nej riešia značne regulované oblasti, a na právne povinnosti vyplývajúce z jej kapitoly IV, k oznámeniu o transpozičných opatreniach by mali byť pripojené vysvetľujúce dokumenty. V súlade so spoločným politickým vyhlásením členských štátov a Komisie k vysvetľujúcim dokumentom z 28. septembra 2011 sa členské štáty zaviazali, že v odôvodnených prípadoch pripoja k oznámeniu o transpozičných opatreniach jeden alebo viacero dokumentov vysvetľujúcich súvislosť medzi zložkami smernice a zodpovedajúcimi časťami vnútroštátnych transpozičných nástrojov. Pokiaľ ide o túto smernicu, zákonodarca považuje prenos takýchto dokumentov za opodstatnený.

4. VPLYV NA ROZPOČET

Spolupráca a výmena informácií medzi členskými štátmi by mala byť podporovaná bezpečnou infraštruktúrou. Návrh bude mať vplyv na rozpočet EÚ len v prípade, ak sa členské štáty rozhodnú zmeniť existujúcu infraštruktúru (napríklad sTESTA) a poveria Komisiu, aby túto zmenu implementovala do viacročného finančného rámca (VFR) na roky 2014 – 2020. Odhadujú sa jednorazové náklady vo výške 1 250 000 EUR, ktoré by boli pokryté v rozpočte EÚ, rozpočtový riadok 09.03.02 (na podporu prepojenia a interoperability vnútroštátnych elektronických verejných služieb, ako aj prístupu k takýmto službám – kapitola 09.03, Nástroj na prepojenie Európy CEF — telekomunikačné siete)

pod podmienkou, že v rámci nástroja CEF budú dostupné dostatočné finančné prostriedky. Členské štáty sa môžu prípadne podieľať na jednorazových nákladoch v súvislosti so zmenou existujúcej infraštruktúry, alebo sa môžu rozhodnúť vytvoriť novú infraštruktúru a niesť náklady, ktoré sa odhadujú približne na 10 miliónov EUR ročne.

2013/0027 (COD)

Návrh

SMERNICA EURÓPSKEHO PARLAMENTU A RADY

o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE ,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po predložení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[1],

po porade s európskym dozorným úradníkom pre ochranu údajov,

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) Siete a informačné systémy a služby hrajú v spoločnosti základnú úlohu. Ich spoľahlivosť a bezpečnosť sú nevyhnutné pre ekonomické činnosti a sociálne zabezpečenie a najmä pre fungovanie vnútorného trhu.

(2) Rozsah a frekvencia úmyselných alebo náhodných bezpečnostných incidentov sa zvyšuje a predstavuje významnú hrozbu pre fungovanie sietí a informačných systémov. Takéto incidenty môžu zabraňovať napredovaniu ekonomických činností, spôsobovať značné finančné straty, narúšať dôveru používateľa a spôsobovať značné škody v hospodárstve Únie.

(3) Digitálne informačné systémy, a najmä internet, ako komunikačné nástroje bez hraníc hrajú významnú úlohu pri uľahčení pohybu tovaru, služieb a osôb cez hranice. Z dôvodu tohto nadnárodného charakteru môže vážne narušenie týchto systémov v jednom členskom štáte ovplyvniť aj ďalšie členské štáty a Úniu ako celok. Preto je na riadne fungovanie vnútorného trhu nevyhnutná odolnosť a stabilita sietí a informačných systémov.

(4) Na úrovni Únie by sa mal vytvoriť mechanizmus spolupráce, ktorý by umožnil výmenu informácií a koordinovanú činnosť, pokiaľ ide o zisťovanie a reakciu v súvislosti s bezpečnosťou sietí a informácií. Aby bol takýto mechanizmus účinný a týkal sa viacerých strán, členské štáty musia mať minimálne spôsobilosti a stratégiu, ktoré by na ich území zabezpečili vysokú úroveň bezpečnosti sietí a informácií. Minimálne bezpečnostné požiadavky by sa mali uplatňovať aj na verejnú správu a prevádzkovateľov kritickej informačnej infraštruktúry s cieľom podporovať kultúru riadenia rizika a zabezpečovať oznamovanie najzávažnejších incidentov.

(5) S cieľom pokryť všetky príslušné incidenty a riziká by sa mala táto smernica uplatňovať na všetky siete a informačné systémy. Povinnosti, ktoré má verejná správa a účastníci trhu, by sa však nemali uplatňovať na podniky poskytujúce verejné

[1] Ú. v. EÚ C […], […], s. […].

komunikačné siete alebo verejne dostupné elektronické komunikačné služby v zmysle smernice Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica)[2], na ktoré sa vzťahujú osobitné požiadavky, pokiaľ ide o bezpečnosť a integritu, ktoré sú stanovené v článku 13a uvedenej smernice, a nemali by sa uplatňovať ani na poskytovateľov dôveryhodných služieb.

(6) Existujúce spôsobilosti nie sú postačujúce na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii. V členských štátoch je rôzna úroveň pripravenosti, čo vedie k roztrieštеným prístupom v Únii. Toto má za následok rozdielnu úroveň ochrany spotrebiteľov a podnikov a narúša celkovú úroveň bezpečnosti sietí a informácií v rámci Únie. Nedostatok spoločných minimálnych požiadaviek na verejnú správu a účastníkov trhu na druhej strane znemožňuje, aby sa na úrovni Únie vytvoril spoločný a účinný mechanizmus spolupráce.

(7) Účinné reagovanie na výzvy, pokiaľ ide o bezpečnosť sietí a informačných systémov, si preto vyžaduje spoločný prístup na úrovni Únie, ktorý by pokryl spoločné požiadavky na budovanie minimálnych kapacít a plánovanie, výmenu informácií a koordináciu činností, a spoločné minimálne bezpečnostné požiadavky pre všetkých zainteresovaných účastníkov trhu a verejnú správu.

(8) Ustanovenia tejto smernice by sa mali uplatňovať bez toho, aby bola dotknutá možnosť členských štátov prijať potrebné opatrenia na zabezpečenie ochrany svojich základných bezpečnostných záujmov, chrániť verejný poriadok a verejnú bezpečnosť a povoliť vyšetrovanie a odhaľovanie trestných činov, ako aj prenasledovanie ich páchateľov. V súlade s článkom 346 ZFEÚ žiaden členský štát nie je povinný poskytovať informácie, ktorých sprístupnenie odporuje podľa jeho názoru základným záujmom jeho bezpečnosti.

(9) S cieľom dosiahnuť a udržiavať spoločnú vysokú úroveň bezpečnosti sietí a informačných systémov by mal mať každý členský štát vnútroštátnu stratégiu pre bezpečnosť sietí a informácií, v ktorej by boli vymedzené strategické ciele a konkrétne opatrenia, ktoré sa majú v rámci tejto politiky vykonať. Na vnútroštátnej úrovni je treba vytvoriť plány spolupráce v oblasti bezpečnosti sietí a informácií, ktoré by boli v súlade so základnými požiadavkami, s cieľom dosiahnuť úroveň možností reakcie, ktoré v prípade incidentov umožnia účinnú a efektívnu spoluprácu ako na vnútroštátnej úrovni, tak aj na úrovni Únie.

(10) S cieľom umožniť účinné vykonávanie ustanovení prijatých podľa tejto smernice by sa mal v každom členskom štáte zriadiť alebo určiť orgán, ktorý bude zodpovedný za koordináciu otázok v oblasti bezpečnosti sietí a informácií a ktorý bude pôsobiť ako ústredný bod pre cezhraničnú spoluprácu na úrovni Únie. Tieto orgány by mali dostať primerané technické, finančné a ľudské zdroje, aby mohli efektívnym a účinným spôsobom vykonávať úlohy, ktoré im budú pridelené, a tak dosahovať ciele tejto smernice.

(11) Všetky členské štáty by mali mať primerané vybavenie, pokiaľ ide o technické a organizačné kapacity, aby mohli predchádzať incidentom a rizikám v oblasti sietí a informačných systémov, odhaľovať ich, reagovať na ne a zmierňovať ich. Preto by sa mali vo všetkých členských štátoch založiť dobre fungujúce tímy reakcie na núdzové počítačové situácie, ktoré budú dodržiavať základné požiadavky, aby sa zaručili

[2] Ú. v. ES L 108, 24.4.2002, s. 33.

účinné a zlučiteľné kapacity na riešenie incidentov a rizík a aby sa na úrovni Únie zabezpečila efektívna spolupráca.

(12) Na základe značného pokroku, ktorý sa dosiahol v rámci Európskeho fóra členských štátov (ďalej len „EFMS“) pri podpore diskusií o osvedčených postupoch a ich výmen, vrátane vytvorenia zásad pre spoluprácu v európskej kybernetickej kríze, členské štáty a Komisia by mali vytvoriť sieť, ktorá by im umožnila stálu komunikáciu a podporila ich vzájomnú spoluprácu. Tento bezpečný a účinný mechanizmus spolupráce by mal umožniť štruktúrovanú a koordinovanú výmenu informácií, ako aj zisťovanie a reakciu na úrovni Únie.

(13) Európska agentúra pre bezpečnosť sietí a informácií (ďalej len „ENISA“) by mala pomáhať členským štátom a Komisii tým, že poskytne svoje odborné znalosti a poradenstvo a bude uľahčovať výmenu osvedčených postupov. Predovšetkým pri uplatňovaní tejto smernice by sa Komisia mala radiť s agentúrou ENISA. V záujme zabezpečenia účinného a včasného informovania členských štátov a Komisie by malo v rámci siete spolupráce prebiehať včasné varovanie pred incidentmi a rizikami. S cieľom budovať kapacity a šíriť vedomosti medzi členskými štátmi by sieť spolupráce mala slúžiť aj ako nástroj na výmenu osvedčených postupov a pritom pomáhať svojim členom pri budovaní kapacít, riadiť organizovanie partnerských hodnotení a cvičení v oblasti bezpečnosti sietí a informácií.

(14) Mal by sa zaviesť bezpečný systém výmeny informácií, aby sa v rámci siete spolupráce umožnila výmena citlivých a dôverných informácií. Bez toho, aby bola dotknutá povinnosť členských štátov oznamovať sieti spolupráce incidenty a riziká, ktoré sa týkajú celej Únie, prístup k dôverným informáciám z iných členských štátov by sa mal udeľovať členským štátom iba po preukázaní, že ich technické, finančné a ľudské zdroje a procesy, ako aj ich komunikačná infraštruktúra, zaručujú ich účinnú, efektívnu a bezpečnú účasť v sieti.

(15) Keďže väčšinu sietí a informačných systémov prevádzkujú súkromní operátori, je nevyhnutná spolupráca medzi verejným a súkromným sektorom. Účastníci trhu by mali byť povzbudzovaní, aby sa s cieľom zabezpečiť bezpečnosť sietí a informácií snažili aj o vytvorenie svojich vlastných neformálnych mechanizmov spolupráce. Mali by spolupracovať aj s verejným sektorom a vymieňať si informácie a osvedčené postupy výmenou za prevádzkovú podporu v prípade incidentov.

(16) S cieľom zabezpečiť transparentnosť a riadne informovať občanov EÚ a účastníkov trhu, príslušné orgány by mali zriadiť spoločnú internetovú stránku, na ktorej by uverejňovali informácie o incidentoch a rizikách, ktoré nemajú dôverný charakter.

(17) Ak sa informácie považujú v súlade s pravidlami Únie a vnútroštátnymi pravidlami o obchodnom tajomstve za dôverné, pri výkone činností a plnení cieľov stanovených v tejto smernici je dôvernosť týchto informácií zaručená.

(18) Najmä na základe vnútroštátnych skúseností v oblasti krízového riadenia a v spolupráci s agentúrou ENISA, Komisia a členské štáty by mali vypracovať plán spolupráce, pokiaľ ide o bezpečnosť sietí a informácií v Únii, v ktorom by boli vymedzené mechanizmy spolupráce v rámci boja proti rizikám a incidentom. Tento plán by mal byť náležite zohľadnený v súvislosti so zasielaním včasného varovania v rámci siete spolupráce.

(19) Zasielanie včasného varovania v rámci siete by sa malo vyžadovať len v prípade, ak rozsah a závažnosť predmetného incidentu alebo rizika sú alebo by sa mohli stať tak významné, že je potrebné informovanie alebo koordinácia reakcie na úrovni Únie.

Včasné varovanie by malo byť preto obmedzené na skutočné alebo potenciálne incidenty alebo riziká, ktoré sa rýchlo rozširujú, presahujú možnosti reakcie na vnútroštátnej úrovni alebo ovplyvňujú viac než jeden členský štát. S cieľom umožniť riadne hodnotenie by sa všetky informácie, ktoré sú relevantné pre posúdenie rizika alebo incidentu, mali oznamovať sieti spolupráce.

(20) Po prijatí včasného varovania a jeho posúdení by sa príslušné orgány mali v rámci plánu spolupráce, pokiaľ ide o bezpečnosť sietí a informácií v Únii, dohodnúť na koordinovanej reakcii. Príslušné orgány, ako aj Komisia, by mali byť informované o opatreniach prijatých na vnútroštátnej úrovni v dôsledku koordinovanej reakcie.

(21) Vzhľadom na globálny charakter problémov bezpečnosti sietí a informácií je potrebná užšia medzinárodná spolupráca s cieľom zlepšiť bezpečnostné normy a výmenu informácií a presadzovať spoločný globálny prístup k otázke bezpečnosti sietí a informácií.

(22) Zodpovednosť za zabezpečenie bezpečnosti sietí a informácií spočíva vo veľkej miere na verejnej správe a účastníkoch trhu. Kultúra riadenia rizika vrátane hodnotenia rizika a vykonávania bezpečnostných opatrení, ktoré sú primerané rizikám, by sa mala podporovať a rozvíjať prostredníctvom vhodných právnych požiadaviek a dobrovoľných priemyselných postupov. Vytvorenie rovnakých podmienok pre všetkých je tiež nevyhnutné na účinné fungovanie siete spolupráce v záujme zabezpečenia účinnej spolupráce všetkých členských štátov.

(23) V smernici 2002/21/ES sa vyžaduje, aby podniky poskytujúce verejné elektronické komunikačné siete alebo verejne dostupné elektronické komunikačné služby prijali primerané opatrenia na ochranu svojej integrity a bezpečnosti, a zavádzajú sa v nej požiadavky na oznamovanie v prípade narušenia bezpečnosti a straty integrity. V smernici Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách)[3] sa vyžaduje od poskytovateľov verejne dostupných elektronických komunikačných služieb, aby v záujme zabezpečenia bezpečnosti svojich služieb prijali primerané technické a organizačné opatrenia.

(24) Tieto povinnosti by sa mali rozšíriť nad rámec sektora elektronických komunikácií k hlavným poskytovateľom služieb informačnej spoločnosti, ako sú vymedzené v smernici Európskeho parlamentu a Rady 98/34/ES z 22. júna 1998 o postupe pri poskytovaní informácií v oblasti technických noriem a predpisov, ako aj pravidiel služieb informačnej spoločnosti[4], ktoré podporujú nadväzujúce služby informačnej spoločnosti alebo činnosti online, ako napríklad platformy elektronického obchodu, internetové platobné portály, sociálne siete, vyhľadávače, služby cloud computing, obchody s aplikáciami. Narušenie týchto služieb informačnej spoločnosti zabraňuje tomu, aby sa mohli poskytovať iné služby informačnej spoločnosti, ktoré sú na nich ako hlavných vstupoch závislé. Tvorcovia softvéru a výrobcovia hardvéru nie sú poskytovateľmi služieb informačnej spoločnosti, a preto sú vylúčení. Tieto povinnosti by sa mali rozšíriť aj na verejné správy a prevádzkovateľov kritickej infraštruktúry, ktorá vo veľkej miere závisí od informačných a komunikačných technológií a je nevyhnutná na udržanie dôležitých ekonomických alebo spoločenských funkcií, ako je elektrická energia a plyn, doprava, úverové inštitúcie, burzy cenných papierov a

[3] Ú. v. ES L 201, 31.7.2002, s. 37.
[4] Ú. v. ES L 204, 21.7.1998, s. 37.

zdravotníctvo. Narušenie týchto sietí a informačných systémov by mohlo mať vplyv na vnútorný trh.

(25) Technické a organizačné opatrenia, ktoré má prijímať verejná správa a účastníci trhu, by nemali vyžadovať, aby bol konkrétny produkt komerčnej informačnej a komunikačnej technológie navrhnutý, vyvinutý alebo vyrobený konkrétnym spôsobom.

(26) Verejné správy a účastníci trhu by mali zabezpečiť bezpečnosť sietí a systémov, ktoré sú pod ich správou. To by mali byť predovšetkým súkromné siete a systémy, ktoré spravujú buď ich interní pracovníci IT alebo externí dodávatelia. Povinnosti zabezpečenia a povinnosti informovať by sa mali týkať príslušných účastníkov trhu a verejných správ bez ohľadu na to, či vykonávajú údržbu svojich sietí a informačných systémov interne alebo prostredníctvom externého dodávateľa.

(27) S cieľom vyhnúť sa neprimeranému finančnému a administratívnemu zaťaženiu malých hospodárskych subjektov a používateľov by mali byť požiadavky primerané riziku, ktoré predstavuje sieť alebo konkrétny informačný systém, berúc do úvahy najnovší vývin v oblasti. Tieto opatrenia by sa nemali týkať mikropodnikov.

(28) Príslušné orgány by mali venovať náležitú pozornosť zachovaniu neformálnych a dôveryhodných kanálov na výmenu informácií medzi účastníkmi trhu a verejným a súkromným sektorom. Pri uverejňovaní incidentov oznámených príslušným orgánom by sa mala v primeranej miere udržiavať rovnováha medzi záujmom verejnosti mať informácie o hrozbách a možnými rizikami poškodenia obchodu a dobrej povesti verejných správ a účastníkov trhu, ktorí incidenty oznámia. Pri vykonávaní povinnosti oznamovania by príslušné orgány mali venovať osobitnú pozornosť potrebe, aby sa pred zavedením príslušných bezpečnostných opatrení zachovali informácie o zraniteľných miestach výrobku v prísnej tajnosti.

(29) Príslušné orgány by mali mať prostriedky nevyhnutné na plnenie svojich úloh vrátane právomocí získavať potrebné informácie od účastníkov trhu a verejnej správy, aby mohli posúdiť úroveň bezpečnosti sietí a informačných systémov, ako aj spoľahlivé a komplexné údaje o konkrétnych incidentoch, ktoré majú vplyv na fungovanie sietí a informačných systémov.

(30) V mnohých prípadoch je príčinou incidentu trestná činnosť. Trestný charakter incidentov možno predpokladať aj v prípade, ak od začiatku nie sú k dispozícii dostatočne jasné dôkazy. V tejto súvislosti by mala vhodná spolupráca medzi príslušnými orgánmi a orgánmi presadzovania práva tvoriť súčasť účinnej a komplexnej reakcie na hrozby bezpečnostných incidentov. Najmä podpora chráneného, bezpečného a odolnejšieho prostredia si vyžaduje systematické oznamovanie incidentov, v prípade ktorých existuje podozrenie na závažnú trestnú činnosť, orgánom presadzovania práva. Incidenty, ktoré majú charakter závažnej trestnej činnosti, by sa mali posudzovať v kontexte právnych predpisov EÚ o kybernetickej kriminalite.

(31) V dôsledku incidentov sú v mnohých prípadoch ohrozené osobné údaje. V tejto súvislosti by mali príslušné orgány a orgány na ochranu údajov navzájom spolupracovať a vymieňať si informácie o všetkých súvisiacich veciach s cieľom riešiť prípady nepovoleného prístupu k osobným údajom následkom incidentov. Členské štáty zavedú povinnosť oznamovať bezpečnostné incidenty spôsobom, ktorý minimalizuje administratívne zaťaženie v prípade, ak bezpečnostný incident predstavuje zároveň aj porušenie ochrany osobných údajov v súlade s nariadením

Európskeho parlamentu a Rady o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov a o voľnom pohybe takýchto údajov[5]. Európska agentúra pre bezpečnosť sietí a informácií (ENISA) by v spolupráci s príslušnými orgánmi a orgánmi na ochranu údajov mohla pomôcť tým, že vytvorí mechanizmy na výmenu informácií a vypracuje vzorové formuláre, a tak nebude potrebné používať na oznamovanie dva formuláre. Takýto jednotný vzorový dokument by uľahčil oznamovanie incidentov, ktorými sa porušuje ochrana osobných údajov, a tým by sa zmiernilo administratívne zaťaženie podnikov a verejnej správy.

(32) Normalizácia bezpečnostných požiadaviek je proces riadený trhom. V záujme zabezpečenia zosúladeného uplatňovania bezpečnostných noriem by členské štáty mali podporovať plnenie špecifických noriem alebo súlad s nimi, aby sa na úrovni Únie zabezpečil vysoký stupeň bezpečnosti. V tejto súvislosti bude možno potrebné navrhnúť harmonizované normy, čo by sa malo uskutočniť v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES a ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES[6].

(33) Komisia by mala robiť pravidelné preskúmanie tejto smernice, najmä s ohľadom na stanovenie potreby zmeny na základe meniacich sa technologických a trhových podmienok.

(34) S cieľom umožniť riadne fungovanie siete spolupráce by právomoc prijímať akty v súlade s článkom 290 Zmluvy o fungovaní Európskej únie mala byť prenesená na Komisiu, pokiaľ ide o vymedzenie kritérií, ktoré musia byť splnené, aby mohol byť členský štát oprávnený zúčastniť sa na bezpečnom systéme výmeny informácií, ďalšiu špecifikáciu udalostí, na podnet ktorých sa zasiela včasné varovanie, ako aj vymedzenie podmienok, za ktorých sa od účastníkov trhu a verejnej správy vyžaduje, aby oznamovali incidenty.

(35) Je osobitne dôležité, aby Komisia počas svojich prípravných prác uskutočňovala náležité konzultácie aj na expertnej úrovni. Pri príprave a vypracúvaní delegovaných aktov by Komisia mala zabezpečiť súbežné, včasné a vhodné postúpenie príslušných dokumentov Európskemu parlamentu a Rade.

(36) V záujme zabezpečenia jednotných podmienok na vykonávanie tejto smernice by mali byť vykonávacie právomoci prenesené na Komisiu, čo sa týka spolupráce medzi príslušnými orgánmi a Komisiou v rámci siete spolupráce, prístupu k bezpečnému systému výmeny informácií, plánu spolupráce, pokiaľ ide o bezpečnosť sietí a informácií na úrovni Únie, formátov a postupov, ktoré možno využiť na informovanie verejnosti o incidentoch, a noriem a/alebo technických špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informácií. Tieto právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa stanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie[7].

---

5 SEC(2012) 72 final

6 Ú. v. EÚ L 316, 14.11.2012, s. 12.

7 Ú. v. EÚ L 55, 28.2.2011, s. 13.

(37) Pri uplatňovaní tejto smernice by Komisia mala podľa potreby spolupracovať s príslušnými výbormi v danom sektore a príslušnými orgánmi založenými na úrovni EÚ, najmä v oblasti energetiky, dopravy a zdravotníctva.

(38) Informácie, ktoré príslušný orgán považuje za dôverné podľa predpisov Únie a vnútroštátnych predpisov o obchodnom tajomstve, by mali byť vymieňané s Komisiou a inými príslušnými orgánmi len v prípade, ak je takáto výmena nevyhnutná v záujme uplatňovania ustanovení tejto smernice. Informácie, ktoré sú predmetom výmeny, by sa mali obmedziť na informácie relevantné a primerané účelu takejto výmeny.

(39) Pri výmene informácii o rizikách a incidentoch v rámci siete spolupráce a dodržiavaní požiadaviek oznamovať incidenty vnútroštátnym príslušným orgánom sa môže vyžadovať spracovanie osobných údajov. Takéto spracovanie osobných údajov je potrebné v záujme plnenia cieľov verejného záujmu, ktoré sú sledované v tejto smernici, a tým je v súlade s článkom 7 smernice 95/46/ES legitímne. Nepredstavuje v súvislosti s týmito legitímnymi cieľmi neprimeraný a neúnosný zásah, ktorý by narušil samotnú podstatu práva na ochranu osobných údajov, ktoré je zaručené v článku 8 Charty základných práv. Pri uplatňovaní tejto smernice by sa malo primerane uplatňovať nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie[8]. V prípade spracúvania údajov inštitúciami a orgánmi Únie, takéto spracúvanie by na účely uplatňovania tejto smernice malo byť v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov.

(40) Keďže ciele tejto smernice, a to zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii, nie je možné uspokojivo dosiahnuť na úrovni jednotlivých členských štátov, a preto ich možno z dôvodu rozsahu a účinku tohto nariadenia lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity, ako sa uvádza v článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku neprekračuje táto smernica rámec nutný na dosiahnutie týchto cieľov.

(41) V tejto smernici sú dodržané základné práva a zásady uznané najmä Chartou základných práv Európskej únie, právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastniť majetok, právo na účinný opravný prostriedok pred súdom a právo na vypočutie. Táto smernica sa musí vykonávať v súlade s týmito právami a zásadami.

PRIJALI TÚTO SMERNICU:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet a rozsah pôsobnosti

1. V tejto smernici sa stanovujú opatrenia na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii.

2. S týmto cieľom sa v tejto smernici:

[8] Ú. v. ES L 145, 31.5.2001, s. 43.

a) stanovujú pre všetky členské štáty povinnosti, ktoré sa týkajú prevencie rizík a incidentov, ktoré majú vplyv na siete a informačné systémy, ich riešenia a reakcie na ne;

b) zavádza mechanizmus spolupráce medzi členskými štátmi s cieľom zabezpečiť jednotné uplatňovanie tejto smernice v rámci Únie a v prípade potreby koordinovanú a efektívnu a reakciu na riziká a incidenty, ktoré postihli siete a informačné systémy;

c) stanovujú bezpečnostné požiadavky pre účastníkov trhu a verejné správy.

3. Bezpečnostné požiadavky stanovené v článku 14 sa nevzťahujú na podniky, ktoré poskytujú verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby v zmysle smernice 2002/21/ES, ktoré sa riadia osobitnými požiadavkami, pokiaľ ide o bezpečnosť a integritu podľa článkov 13a a 13b uvedenej smernice, ani na poskytovateľov dôveryhodných služieb.

4. Táto smernica sa nedotýka právnych predpisov EÚ o kybernetickej kriminalite ani smernice Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu[9].

5. Táto smernica sa nedotýka ani smernice Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov[10], ani smernice Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcej sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií, ani nariadenia Európskeho parlamentu a Rady o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov a o voľnom pohybe takýchto údajov[11].

6. Výmena informácií v rámci siete spolupráce podľa kapitoly III a oznamovanie incidentov v oblasti bezpečnosti sietí a informácií v zmysle článku 14 si môže vyžadovať spracovanie osobných údajov. Členský štát povoľuje takéto spracovanie údajov, ktoré je potrebné v záujme plnenia cieľov verejného záujmu sledovaných v tejto smernici, podľa článku 7 smernice 95/46/EHS a smernice 2002/58/ES, v zmysle ich uplatnenia vo vnútroštátnych právnych predpisoch.

Článok 2

Minimálna harmonizácia

Členským štátom sa nebude brániť v prijímaní alebo zachovaní ustanovení, ktoré zabezpečujú vyššiu úroveň bezpečnosti, bez toho, aby boli dotknuté ich povinnosti v súlade s právom Únie.

Článok 3

Vymedzenie pojmov

Na účely tejto smernice sa uplatňuje toto vymedzenie pojmov:

(1) „siete a informačné systémy“ znamenajú:

a) elektronickú komunikačnú sieť v zmysle smernice 2002/21/ES, a

[9] Ú. v. EÚ L 345, 23.12.2008, s. 75.
[10] Ú. v. ES L 281, 23.11.1995, s. 31.
[11] SEC(2012) 72 final.

b) každé zariadenie alebo skupinu vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú na základe programu automatické spracúvanie počítačových údajov, ako aj

c) počítačové údaje, ktoré sú uložené, spracúvané, opätovne získavané alebo prenášané prostredníctvom prvkov uvedených v písm. a) a b) na účely ich spracovávania, používania, ochrany a udržiavania,

(2) „bezpečnosť“ znamená schopnosť siete alebo informačného systému odolávať na určitom stupni spoľahlivosti náhodným udalostiam alebo zlomyseľnému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov alebo súvisiacich služieb poskytovaných prostredníctvom tejto siete a informačného systému alebo prístupných prostredníctvom tejto siete a informačného systému;

(3) „riziko“ znamená každú okolnosť alebo udalosť, ktorá má prípadný nepriaznivý vplyv na bezpečnosť;

(4) „incident“ znamená každú okolnosť alebo udalosť, ktorá má konkrétny nepriaznivý vplyv na bezpečnosť;

(5) „služby informačnej spoločnosti“ znamenajú služby v zmysle článku 1 ods. 2 smernice 98/34/ES;

(6) „plán spolupráce v oblasti bezpečnosti sietí a informácií“ znamená plán, ktorým sa vytvára rámec pre organizačné úlohy, zodpovednosť a postupy na zachovanie alebo obnovu prevádzky sietí a informačných systémov v prípade rizika alebo incidentu, ktoré majú vplyv na tieto siete a informácie;

(7) „riešenie incidentov“ znamená všetky postupy na podporu analýzy, monitorovania a reakcie na incident;

(8) „účastník trhu“ znamená:

a) poskytovateľ služieb informačnej spoločnosti, ktoré umožňujú poskytovanie ďalších služieb informačnej spoločnosti, ktorých neúplný zoznam je uvedený v prílohe II,

b) prevádzkovateľ kritickej infraštruktúry, ktorá má zásadný význam z hľadiska zachovania dôležitých ekonomických a spoločenských činností v oblasti energetiky, dopravy, bankovníctva, burzy cenných papierov a zdravotníctva, ktorých neúplný zoznam je uvedený v prílohe II,

(9) „norma“ znamená normu, ako je uvedená v nariadení (EÚ) č. 1025/2012;

(10) „špecifikácia“ znamená špecifikáciu, ako je uvedená v nariadení (EÚ) č. 1025/2012;

(11) „poskytovateľ dôveryhodných služieb“ je každá fyzická alebo právnická osoba, ktorá poskytuje elektronické služby, a to vytváranie, potvrdzovanie, overovanie, spracovávanie a uchovávanie elektronických podpisov, elektronických pečatí, elektronických časových pečiatok, elektronických dokumentov; elektronické doručovacie služby, autentifikáciu webových lokalít a elektronických certifikátov vrátane certifikátov elektronických podpisov a elektronických pečatí.

KAPITOLA II

VNÚTROŠTÁTNE RÁMCE PRE BEZPEČNOSŤ SIETÍ A INFORMÁCIÍ

Článok 4

Princíp

Členské štáty zabezpečujú v súlade s touto smernicou na svojom území vysoký stupeň bezpečnosti sietí a informačných systémov.

Článok 5

Vnútroštátna stratégia pre bezpečnosť sietí a informácií a vnútroštátny plán spolupráce v oblasti bezpečnosti sietí a informácií

1. Každý členský štát prijme vnútroštátnu stratégiu pre bezpečnosť sietí a informácií, v ktorej budú vymedzené strategické ciele a konkrétne politické a regulačné opatrenia na dosiahnutie a udržanie vysokej úrovne bezpečnosti sietí a informácií. Vnútroštátna stratégia pre bezpečnosť sietí a informácií sa zaoberá najmä týmito otázkami:

a) vymedzenie cieľov a priorít stratégie založenej na aktuálnej analýze rizík a incidentov;

b) rámec riadenia na dosiahnutie cieľov a priorít stratégie vrátane jasného vymedzenia úloh a zodpovedností vládnych orgánov a ďalších príslušných subjektov;

c) identifikácia všeobecných opatrení, pokiaľ ide o pripravenosť, reakciu a obnovu vrátane mechanizmov spolupráce medzi verejným a súkromným sektorom;

d) predstavenie vzdelávacích programov, programov na zvyšovanie informovanosti a programov v oblasti odbornej prípravy;

e) výskum a vývoj plánov a opis toho, ako tieto plány odrážajú stanovené priority.

2. Súčasť vnútroštátnej stratégie pre bezpečnosť sietí a informácií tvorí vnútroštátny plán spolupráce v oblasti bezpečnosti sietí a informácií, ktorý spĺňa prinajmenšom tieto požiadavky:

a) plán na hodnotenie rizika na účely identifikácie rizík a hodnotenia vplyvu potenciálnych incidentov;

b) vymedzenie úloh a zodpovedností jednotlivých subjektov zainteresovaných v realizácii plánu;

c) vymedzenie procesov spolupráce a komunikácie, ktorými sa zabezpečí prevencia, zisťovanie, reakcia, náprava a obnova a ktoré sú upravené podľa stupňa pohotovosti;

d) harmonogram cvičení a odbornej prípravy v oblasti bezpečnosti sietí a informácií, ktorých cieľom bude vylepšiť, preskúmať a testovať tento plán. Získané skúsenosti budú zaznamenané do aktualizácií plánu.

3. Vnútroštátna stratégia pre bezpečnosť sietí a informácií a vnútroštátny plán spolupráce v oblasti bezpečnosti sietí a informácií sa oznamujú Komisii do jedného mesiaca po ich prijatí.

Článok 6

Príslušný vnútroštátny orgán pre oblasť bezpečnosti sietí a informačných systémov

4. Každý členský štát určí príslušný vnútroštátny orgán pre oblasť bezpečnosti sietí a informačných systémov (ďalej len „príslušný orgán“).

5. Príslušné orgány monitorujú uplatňovanie tejto smernice na vnútroštátnej úrovni a prispievajú k jej jednotnému uplatňovaniu v celej Únii.

6. Členské štáty zabezpečia, aby príslušné orgány mali primerané technické, finančné a ľudské zdroje, aby mohli účinným a efektívnym spôsobom vykonávať úlohy, ktoré im budú pridelené, a tak dosahovať ciele tejto smernice. Členské štáty zabezpečia prostredníctvom siete uvedenej v článku 8 účinnú, efektívnu a bezpečnú spoluprácu príslušných orgánov.

7. Členské štáty zabezpečia, aby príslušné orgány dostali od verejných správ a účastníkov trhu oznámenia o incidentoch, ako je uvedené v článku 14 ods. 2, a aby mali právomoci na vykonávanie a presadzovania práva, ako je stanovené v článku 15.

8. V prípade potreby sa príslušné orgány radia s príslušnými vnútroštátnymi orgánmi presadzovania práva a orgánmi na ochranu údajov a spolupracujú s nimi.

9. Každý členský štát bezodkladne oznámi Komisii názov príslušného orgánu, jeho úlohy a každú ďalšiu zmenu vykonanú v súvislosti s jeho ustanovením. Každý členský štát zverejní ustanovenie príslušného orgánu.

Článok 7

Tímy reakcie na núdzové počítačové situácie

1. Každý členský štát zostaví tím reakcie na núdzové počítačové situácie (ďalej len „CERT“), ktorý bude zodpovedný za riešenie incidentov a rizík podľa presne stanoveného postupu v súlade s požiadavkami stanovenými v bode 1 prílohy I. Tím CERT môže byť vytvorený v rámci príslušného orgánu.

2. Členské štáty zabezpečia, aby tímy CERT mali primerané technické, finančné a ľudské zdroje na to, aby mohli účinne vykonávať svoje úlohy stanovené v bode 2 prílohy I.

3. Členské štáty zabezpečia, aby tímy CERT využívali na vnútroštátnej úrovni bezpečnú a odolnú komunikačnú a informačnú infraštruktúru, ktorá je zlučiteľná a interoperabilná s bezpečným systémom výmeny informácií, na ktorý sa odkazuje v článku 9.

4. Členské štáty informujú Komisiu o zdrojoch a mandáte tímov CERT, ako aj o ich postupe pri riešení incidentov.

5. Tím CERT vykonáva svoju činnosť pod dohľadom príslušného orgánu, ktorý pravidelne skúma primeranosť jeho zdrojov, jeho mandát a účinnosť jeho postupu pri riešení problémov.

KAPITOLA III

SPOLUPRÁCA MEDZI PRÍSLUŠNÝMI ORGÁNMI

Článok 8

Sieť spolupráce

1. Príslušné orgány a Komisia vytvoria sieť („sieť spolupráce“) s cieľom spolupracovať v boji proti rizikám a incidentom, ktoré postihujú siete a informačné systémy.

2. Sieť spolupráce zabezpečí medzi Komisiou a príslušnými orgánmi stálu komunikáciu. Na požiadanie pomáha v sieti spolupráce aj Európska agentúra pre bezpečnosť sietí a informácií (ďalej len „ENISA“) tým, že poskytuje svoje odborné znalosti a poradenstvo.

3. V rámci siete spolupráce príslušné orgány:

   a) zasielajú včasné varovanie o rizikách a incidentoch v súlade s článkom 10;

   b) zabezpečujú koordinovanú reakciu v súlade s článkom 11;

   c) pravidelne zverejňujú na spoločnej webovej lokalite informácie, ktoré nemajú dôverný charakter, o aktuálnych včasných varovaniach a koordinovanej reakcii;

   d) na žiadosť jedného členského štátu alebo Komisie vedú spoločnú diskusiu a posudzujú jednu alebo viaceré vnútroštátne stratégie pre bezpečnosť sietí a informácií a vnútroštátne plány spolupráce v oblasti bezpečnosti sietí a informácií uvedené v článku 5, v rozsahu pôsobnosti tejto smernice;

   e) na žiadosť členského štátu alebo Komisie vedú spoločnú diskusiu o účinnosti tímov CERT, a to najmä pri cvičeniach v oblasti bezpečnosti sietí a informácií na úrovni Únie, a posudzujú ju;

   f) spolupracujú a vymieňajú si informácie o všetkých súvisiacich veciach s Európskym centrom boja proti kybernetickej kriminalite, ktoré je zriadené v rámci Europolu, a s ostatnými príslušnými európskymi orgánmi, najmä čo sa týka ochrany údajov, energetiky, dopravy, bankovníctva, burzy cenných papierov a zdravotníctva;

   g) vymieňajú si informácie a osvedčené postupy medzi sebou navzájom a s Komisiou, a navzájom si pomáhajú pri budovaní kapacít v oblasti bezpečnosti sietí a informácií;

   h) organizujú pravidelné partnerské preskúmania schopností a pripravenosti;

   i) organizujú cvičenia v oblasti bezpečnosti sietí a informácií na úrovni Únie a podľa potreby sa zúčastňujú na medzinárodných cvičeniach v tejto oblasti.

4. Komisia prostredníctvom vykonávacích aktov stanoví potrebné metódy s cieľom uľahčiť spoluprácu medzi príslušnými orgánmi a Komisiou uvedenou v odsekoch 2 a 3. Tieto vykonávacie akty sa prijmú v súlade s poradným postupom uvedeným v článku 19 ods. 2.

Článok 9

Bezpečný systém výmeny informácií

1. Výmena citlivých a dôverných informácií sa v rámci siete spolupráce uskutočňuje prostredníctvom bezpečnej infraštruktúry.

2. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 18 týkajúce sa vymedzenia kritérií, ktoré musia byť splnené, aby mohol byť členský štát oprávnený zúčastniť sa na bezpečnom systéme výmeny informácií systému, pokiaľ ide o:

   a) dostupnosť bezpečnej a odolnej komunikačnej a informačnej infraštruktúry na vnútroštátnej úrovni, ktorá je zlučiteľná a interoperabilná s bezpečnou infraštruktúrou siete spolupráce v súlade s článkom 7 ods. 3, a

b) existenciu primeraných technických, finančných a ľudských zdrojov a postupov pre ich príslušný orgán a tím CERT, ktoré by umožnili účinnú, efektívnu a bezpečnú účasť na bezpečnom systéme výmeny informácií v súlade s článkom 6 ods. 3, článkom 7 ods. 2 a článkom 7 ods. 3.

3. Komisia prijme prostredníctvom vykonávacích aktov rozhodnutia o prístupe členských štátov k tejto bezpečnej infraštruktúre, v súlade s kritériami uvedenými v odsekoch 2 a 3. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania podľa článku 19 ods. 3.

Článok 10

Včasné varovanie

1. Príslušné orgány alebo Komisia zasielajú v rámci siete spolupráce včasné varovania v súvislosti s tými rizikami a incidentmi, ktoré spĺňajú aspoň jednu z týchto podmienok:

a) ich rozsah sa rýchlo sa zväčšuje alebo sa môže rýchlo zväčšovať;

b) presahujú, alebo môžu presiahnuť možnosti reakcie na vnútroštátnej úrovni;

c) ovplyvňujú alebo môžu ovplyvniť viac ako jeden členský štát.

2. Prostredníctvom včasného varovania príslušné orgány a Komisia poskytujú všetky relevantné informácie, ktoré majú k dispozícii a ktoré môžu byť užitočné pre hodnotenie rizika alebo incidentu.

3. Na žiadosť členského štátu alebo na základe vlastného podnetu môže Komisia požiadať členský štát, aby poskytol všetky príslušné informácie o konkrétnom riziku alebo incidente.

4. Ak v prípade rizika alebo incidentu podliehajúceho včasnému varovaniu existuje podozrenie z trestného činu, príslušné orgány alebo Komisia informujú Európske centrum boja proti kybernetickej kriminalite, ktoré je zriadené v rámci Europolu.

5. Komisia je oprávnená prijímať delegované akty v súlade s článkom 18, pokiaľ ide o podrobnejšie určenie rizika a incidentov, v prípade ktorých je potrebné zasielať včasné varovanie uvedené v odseku 1.

Článok 11

Koordinovaná reakcia

1. Na základe včasného varovania uvedeného v článku 10 sa príslušné orgány po tom, ako zhodnotia príslušné informácie, dohodnú na koordinovanej reakcii v súlade s plánom spolupráce v oblasti bezpečnosti sietí a informácií na úrovni Únie, ktorý je uvedený v článku 12.

2. V rámci siete spolupráce sa v dôsledku koordinovanej reakcie oznamujú rôzne opatrenia prijaté na vnútroštátnej úrovni.

Článok 12

Plán spolupráce v oblasti bezpečnosti sietí a informácií na úrovni Únie

1. Komisia je oprávnená prostredníctvom vykonávacích aktov prijať plán spolupráce v oblasti bezpečnosti sietí a informácií na úrovni Únie. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 19 ods. 3.

2. Plán spolupráce v oblasti bezpečnosti sietí a informácií na úrovni Únie zabezpečuje:

a) na účely článku 10:

– vymedzenie formátu a postupov na zhromažďovanie a výmenu zlučiteľných a porovnateľných informácií o rizikách a incidentoch príslušnými orgánmi,

– vymedzenie postupov a kritérií na hodnotenie rizika a incidentov prostredníctvom siete spolupráce;

b) postupy, ktoré sa majú dodržiavať pri koordinovanej reakcii podľa článku 11, vrátane vymedzenia úloh a zodpovedností, ako aj postupov spolupráce;

c) harmonogram cvičení a odbornej prípravy v oblasti bezpečnosti sietí a informácií, ktorých cieľom bude vylepšiť, preskúmať a testovať tento plán;

d) program na prenos poznatkov medzi členskými štátmi v súvislosti s budovaním kapacít a partnerským učením;

e) program na zvyšovanie informovanosti a odbornú prípravu v členských štátoch.

3. Plán spolupráce v oblasti bezpečnosti sietí a informácií na úrovni Únie sa prijme najneskôr jeden rok po nadobudnutí účinnosti tejto smernice a pravidelne sa reviduje.

Článok 13

Medzinárodná spolupráca

Bez toho, aby bola dotknutá možnosť neformálne spolupracovať na medzinárodnej úrovni v rámci siete spolupráce, Únia môže uzatvárať medzinárodné dohody s tretími krajinami alebo medzinárodnými organizáciami, a tým umožniť ich účasť na niektorých činnostiach siete spolupráce a takúto účasť zorganizovať. V takýchto dohodách sa berie do úvahy potreba zabezpečenia primeranej ochrany osobných údajov, ktoré sú zasielané v rámci siete spolupráce.

KAPITOLA IV

BEZPEČNOSŤ SIETÍ A INFORMAČNÝCH SYSTÉMOV VEREJNEJ SPRÁVY A ÚČASTNÍKOV TRHU

Článok 14

Bezpečnostné požiadavky a oznamovanie incidentov

1. Členské štáty zabezpečia, aby verejná správa a účastníci trhu prijali primerané technické a organizačné opatrenia na riadenie rizík spojených s bezpečnosťou sietí a informačných systémov, ktoré riadia a využívajú vo svojej prevádzke. S ohľadom na najnovší technologický vývoj tieto opatrenia zaručujú takú úroveň bezpečnosti, ktorá zodpovedá miere daného rizika. Opatrenia sa prijímajú najmä s cieľom zabrániť a minimalizovať vplyv incidentov ovplyvňujúcich ich siete a informačný systém na základné služby, ktoré poskytujú, a tak zabezpečiť kontinuitu služieb podporovaných týmito sieťami a informačnými systémami.

2. Členské štáty zabezpečia, aby verejná správa a účastníci trhu oznamovali príslušnému orgánu incidenty, ktoré majú významný vplyv na bezpečnosť základných služieb, ktoré poskytujú.

3. Požiadavky uvedené v odsekoch 1 a 2 sa týkajú všetkých účastníkov trhu, ktorí poskytujú služby v rámci Európskej únie.

4. Príslušný orgán môže informovať verejnosť alebo žiadať, aby tak urobila verejná správa a účastníci trhu, ak usúdi, že zverejnenie incidentu je vo verejnom záujme. Príslušný orgán raz ročne predkladá sieti spolupráce súhrnnú správu o prijatých oznámeniach a o krokoch, ktoré urobil v súlade s týmto odsekom.

5. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 18, pokiaľ ide o vymedzenie okolností, za akých sa vyžaduje od verejnej správy a účastníkov trhu, aby oznamovali incidenty.

6. Na základe delegovaných aktov prijatých podľa odseku 5 môžu príslušné orgány prijať usmernenia a v prípade potreby vydať pokyny týkajúce sa okolností, za akých sa vyžaduje od verejnej správy a účastníkov trhu, aby oznamovali incidenty.

7. Komisia je oprávnená prostredníctvom vykonávacích aktov zaviesť formát a postupy uplatniteľné na účely odseku 2. Tieto vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 19 ods. 3.

8. Odseky 1 a 2 sa nevzťahujú na mikropodniky, ako je vymedzené v odporúčaní Komisie 2003/361/ES zo 6. mája 2003 o vymedzení mikropodnikov a malých a stredných podnikov[12].

Článok 15

Vykonávanie a presadzovanie

1. Členské štáty zabezpečia, aby príslušné orgány mali všetky právomoci potrebné na vyšetrovanie prípadov, ak verejná správa alebo účastníci trhu nedodržiavajú svoje povinnosti podľa článku 14, a ich dôsledkov na bezpečnosť sietí a informačných systémov.

2. Členské štáty zabezpečia, aby príslušné orgány mali právomoc vyžadovať od účastníkov trhu a verejnej správy:

   a) aby poskytovali informácie potrebné na posúdenie bezpečnosti svojich sietí a informačných systémov, vrátane dokumentovaných bezpečnostných politík;

   b) aby sa podrobili bezpečnostnému auditu, ktorý vykoná kvalifikovaný nezávislý orgán alebo vnútroštátny orgán, a sprístupnili jeho výsledky príslušnému orgánu.

3. Členské štáty zabezpečia, aby príslušné orgány mali právomoc vydávať pre účastníkov trhu a verejnú správu záväzné pokyny.

4. Príslušné orgány informujú orgány presadzovania práva o podozrení na závažné incidenty trestnej povahy.

5. Príslušné orgány úzko spolupracujú s orgánmi na ochranu osobných údajov pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov.

6. Členské štáty zabezpečia, aby povinnosti uložené verejným správam a účastníkom trhu na základe tejto kapitoly mohli byť predmetom súdneho preskúmania.

[12] Ú. v. ES L 124, 20.5.2003, s. 36.

Článok 16

Normalizácia

1. S cieľom zabezpečiť zosúladené vykonávanie článku 14 ods. 1 členské štáty podporujú používanie noriem a/alebo špecifikácií, ktoré sú príslušné pre bezpečnosť sietí a informácií.

2. Komisia vypracuje prostredníctvom vykonávacích aktov zoznam noriem uvedených v odseku 1. Zoznam sa uverejňuje v *Úradnom vestníku Európskej únie* .

KAPITOLA V

ZÁVEREČNÉ USTANOVENIA

Článok 17

Sankcie

1. Členské štáty stanovia pravidlá ukladania sankcií za porušenie vnútroštátnych ustanovení prijatých podľa tejto smernice a vykonajú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Tieto sankcie musia byť účinné, primerané a odradzujúce. Členské štáty oznámia tieto ustanovenia Komisii najneskôr do dátumu transpozície tejto smernice a bezodkladne jej oznámia všetky následné zmeny a doplnenia, ktoré majú na ne vplyv.

2. Členské štáty zabezpečujú, aby v prípade bezpečnostného incidentu, ktorý zahŕňa osobné údaje, plánované sankcie zodpovedali sankciám stanoveným v nariadení Európskeho parlamentu a Rady o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov a o voľnom pohybe takýchto údajov[13].

Článok 18

Vykonávanie delegovania právomoci

1. Právomoc prijímať delegované akty sa Komisii udeľuje za podmienok stanovených v tomto článku.

2. Komisii sa udeľuje právomoc prijímať delegované akty uvedené v článku 9 ods. 2, článku 10 ods. 5 a článku 14 ods. 5. Komisia predloží správu týkajúcu sa delegovania právomoci najneskôr deväť mesiacov pred uplynutím päťročného obdobia. Delegovanie právomoci sa automaticky predlžuje na rovnako dlhé obdobia, pokiaľ Európsky parlament alebo Rada nevznesú voči takémuto predĺženiu námietku najneskôr tri mesiace pred koncom každého obdobia.

3. Delegovanie právomocí uvedené v článku 9 ods. 2, článku 10 ods. 5 a článku 14 ods. 5 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomocí v ňom uvedených. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom stanovený. Nemá vplyv na platnosť žiadneho z delegovaných aktov, ktoré už nadobudli účinnosť.

4. Komisia oznamuje delegovaný akt Európskemu parlamentu a Rade súčasne, a to hneď po jeho prijatí.

---

[13] SEC(2012) 72 final

5. Delegovaný akt prijatý podľa článku 9 ods. 2, článku 10 ods. 5 a článku 14 ods. 5 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu parlamentu a Rade, alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

Článok 19

Postup výboru

1. Komisii bude pomáhať výbor (Výbor pre bezpečnosť sietí a informácií). Uvedeným výborom je výbor v zmysle nariadenia (EÚ) č. 182/2011.
2. Keď sa odkazuje na tento odsek, uplatňuje sa článok 4 nariadenia (EÚ) č. 182/2011.
3. Keď sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

Článok 20

Preskúmanie

Komisia pravidelne skúma funkčnosť tejto smernice a podáva správu Európskemu parlamentu a Rade. Prvá správa sa predkladá najneskôr tri roky po dátume transpozície, na ktorú sa odkazuje v článku 21. Na tento účel môže Komisia požadovať od členských štátov, aby bez zbytočného odkladu poskytli informácie.

Článok 21

Transpozícia

1. Členské štáty prijmú a uverejnia najneskôr do [jeden a pol roka od dátumu prijatia] zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou. Komisii bezodkladne oznámia znenie týchto opatrení.

   Tieto opatrenia uplatňujú od [jeden a pol roka od dátumu prijatia].

   Po prijatí týchto opatrení členskými štátmi sa v opatreniach nachádza odkaz na túto smernicu alebo je takýto odkaz uvedený pri príležitosti ich úradného uverejnenia. Podrobnosti o odkaze upravia členské štáty.
2. Členské štáty oznámia Komisii znenie hlavných ustanovení vnútroštátnych právnych predpisov, ktoré prijmú v oblasti pôsobnosti tejto smernice.

Článok 22

Nadobudnutie účinnosti

Táto smernica nadobúda účinnosť [dvadsiatym] dňom po jej uverejnení v *Úradnom vestníku Európskej únie*.

Článok 23

Adresáti

Táto smernica je určená členským štátom.

V Bruseli

Za Európsky parlament
predseda

Za Radu
predseda

PRÍLOHA I

Požiadavky týkajúce sa Tímu reakcie na núdzové počítačové situácie (CERT) a jeho úlohy

Požiadavky na tím CERT a jeho úlohy sú primerane a jasne vymedzené a podporované vnútroštátnymi politikami a/alebo právnymi prepismi. Zahŕňajú tieto prvky:

(1) Požiadavky na tím CERT

a) Tím CERT zabezpečuje, aby v jeho komunikačných službách neboli takzvané slabé miesta zlyhania a aby jeho služby boli čo možno najdostupnejšie, a má niekoľko spôsobov, ktorými môže kontaktovať ostatných a ktorými oni môžu kontaktovať jeho. Okrem toho sú komunikačné kanály jasne vymedzené a zainteresované strany, ako aj spolupracujúci partneri, sú o nich dobre informovaní.

b) Tím CERT vykonáva a riadi bezpečnostné opatrenia s cieľom zabezpečiť dôvernosť, integritu, dostupnosť a pravosť informácií, ktoré získava a spracováva.

c) Kancelárie tímu CERT a podporné informačné systémy sú umiestnené na bezpečných miestach.

d) Vytvorí sa systém riadenia kvality služieb s cieľom nadviazať na činnosť tímu CERT a zabezpečiť stály proces zlepšovania. Tento systém bude založený na jasne vymedzenej metrike, ktorá obsahuje stupne formálnych služieb a kľúčové ukazovatele výkonu.

e) Zabezpečenie kontinuity činnosti:

- tím CERT má zavedený vhodný systém riadenia a zasielania žiadostí v záujme jednoduchšieho odovzdávania,
- tím CERT má primeraný počet pracovníkov, aby sa zabezpečila jeho stála dostupnosť,
- tím CERT využíva infraštruktúru, kontinuita ktorej je zabezpečená. V tejto súvislosti sa pre tím CERT vytvoria záložné systémy a záložný pracovný priestor, aby sa zabezpečil trvalý prístup ku komunikačným prostriedkom.

(2) Úlohy tímu CERT

a) Úlohy tímu CERT sú prinajmenšom tieto:

- monitorovanie incidentov na vnútroštátnej úrovni,
- zasielanie včasného varovania, vyhlasovanie pohotovosti, oznamovanie a šírenie informácií príslušným zainteresovaným stranám o rizikách a incidentoch,
- reagovanie na incidenty,
- zabezpečenie dynamickej analýzy rizika a incidentov a získavanie informácií o situácii,
- budovanie rozsiahleho verejného povedomia o rizikách spojených s aktivitami vykonávanými online,
- organizovanie kampaní v oblasti bezpečnosti sietí a informácií.

b) Tím CERT nadviaže spoluprácu so súkromným sektorom.

c) V záujme uľahčenia spolupráce tím CERT podporuje prijímanie a využívanie spoločných alebo štandardizovaných postupov v oblasti:

– riešenia incidentov a rizík,

– klasifikácie incidentov, rizík a informácií,

– taxonómie na metriku,

– formátov na výmenu informácií o rizikách, incidentoch, ako aj pravidiel na pomenovanie systémov.

PRÍLOHA II

Zoznam účastníkov trhu

uvedených v článku 3 ods. 8 písm. a):

1. platformy elektronického obchodu;

2. internetové platobné portály;

3. sociálne siete;

4. vyhľadávače;

5. služby cloud computing;

6. obchody s aplikáciami;

uvedených v článku 3 ods. 8 písm. b):

1. energetika

- dodávatelia elektrickej energie a plynu,
- prevádzkovatelia distribučnej sústavy elektrickej energie a/alebo plynu a maloobchodní predajcovia pre konečných spotrebiteľov,
- prevádzkovatelia prepravnej siete zemného plynu, prevádzkovatelia skladovacích zariadení a zariadení LNG,
- prevádzkovatelia prenosovej sústavy elektrickej energie,
- ropovody a zariadenia na skladovanie ropy,
- prevádzkovatelia na trhu s elektrickou energiou a zemným plynom,
- prevádzkovatelia zariadení na spracovanie, rafináciu a úpravu ropy a zemného plynu;

2. doprava

- leteckí dopravcovia (nákladná a osobná letecká doprava),
- námorní dopravcovia (spoločnosti poskytujúce námornú a pobrežnú osobnú vodnú dopravu a spoločnosti poskytujúce námornú a pobrežnú nákladnú vodnú dopravu),
- železnice (manažéri infraštruktúry, integrované spoločnosti a prevádzkovatelia železničnej dopravy),
- letiská,
- prístavy,
- prevádzkovatelia kontroly riadenia dopravy,
- pomocné logistické služby a) uskladňovanie a skladovanie, b) manipulácia s nákladom a c) ďalšie podporné činnosti v doprave);

3. bankovníctvo: úverové inštitúcie v súlade s článkom 4 ods. 1 smernice 2006/48/ES;

4. infraštruktúry finančných trhov: burzy cenných papierov, klíringové ústavy s centrálnymi protistranami;

5. sektor zdravotníctva: zdravotnícke zariadenia (vrátane nemocníc a súkromných kliník) a iné subjekty poskytujúce zdravotnú starostlivosť.

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

1.2. Príslušné oblasti politiky v rámci ABM/ABB

1.3. Druh návrhu/iniciatívy

1.4. Ciele

1.5. Dôvody návrhu/iniciatívy

1.6. Trvanie akcie a jej finančného vplyvu

1.7. Plánovaný spôsob hospodárenia

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa kontroly a predkladania správ

2.2. Systémy riadenia a kontroly

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

3.2.2. Odhadovaný vplyv na operačné rozpočtové prostriedky

3.2.3. Odhadovaný vplyv na administratívne rozpočtové prostriedky

3.2.4. Súlad s platným viacročným finančným rámcom

3.2.5. Účasť tretích strán na financovaní

3.3. Odhadovaný vplyv na príjmy

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii.

1.2. Príslušné oblasti politiky v rámci ABM/ABB[37]

- 09 – komunikačné siete, obsah a technológie

1.3. Druh návrhu/iniciatívy

☒ Návrh/iniciatíva sa týka **novej akcie**

☐ Návrh/iniciatíva sa týka **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu**[38]

☐ Návrh/iniciatíva sa týka **predĺženia trvania existujúcej akcie**

☐ Návrh/iniciatíva sa týka **akcie presmerovanej na novú akciu**

1.4. Ciele

1.4.1. Viacročné strategické ciele Komisie, ktoré sú predmetom návrhu/iniciatívy

Cieľom navrhovanej smernice je zabezpečiť vysokú úroveň bezpečnosti sietí a informácií v EÚ.

1.4.2. Konkrétne ciele a príslušné činnosti v rámci ABM/ABB

V návrhu sa stanovujú opatrenia na zabezpečenie vysokej úrovne bezpečnosti sietí a informačných systémov v Únii.

Konkrétnymi cieľmi sú:

1. Zaviesť minimálnu úroveň bezpečnosti sietí a informácií v členských štátoch, a tým zvýšiť celkovú úroveň pripravenosti a reakcie.

2. Zlepšiť spoluprácu v oblasti bezpečnosti sietí a informácií na úrovni EÚ v záujme efektívneho boja proti cezhraničným incidentom a hrozbám. Zavedie sa bezpečný systém výmeny informácií, aby sa medzi príslušnými orgánmi umožnila výmena citlivých a dôverných informácií.

3. Vytvoriť kultúru riadenia rizika a zlepšiť výmenu informácií medzi súkromným a verejným sektorom.

Príslušné činnosti v rámci ABM/ABB

Smernica sa týka subjektov (spoločností a organizácií vrátane malých a stredných podnikov) v mnohých sektoroch (energetika, doprava, úverové inštitúcie a burzy cenných papierov, zdravotníctvo) a sprostredkovateľov základných internetových služieb, ako aj verejnej správy. Rieši súvislosti s problémami s presadzovaním práva a ochranou údajov, ako aj aspekty bezpečnosti sietí a informácií v medzinárodných vzťahoch.

- 09 – komunikačné siete, obsah a technológie

- 02 – podniky

- 32 – energetika

[37] ABM: riadenie podľa činností – ABB: zostavovanie rozpočtu podľa činností.

[38] Podľa článku 49 ods. 6 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

- 06 – mobilita a doprava

- 17 – zdravie a ochrana spotrebiteľa

- 18 – vnútorné záležitosti

- 19 –vonkajšie vzťahy,

- 33 – spravodlivosť

- 12 – vnútorný trh

1.4.3. Očakávané výsledky a vplyv

Uveďte, aký vplyv by mal mať návrh/iniciatíva na príjemcov/cieľové skupiny.

Značne by sa zvýšila ochrana spotrebiteľov, podnikateľov a vlád v EÚ proti incidentom, hrozbám a rizikám v oblasti bezpečnosti sietí a informácií.

Ďalšie podrobnosti možno nájsť v oddiele 8.2 (Vplyv možnosti č. 2 – Regulačný prístup) posúdenie vplyvu pracovného dokumentu útvarov Komisie, ktorý je pripojený k tomuto legislatívnemu návrhu.

1.4.4. Ukazovatele výsledkov a vplyvu

Uveďte ukazovatele, pomocou ktorých je možné sledovať realizáciu návrhu/iniciatívy.

Ukazovatele na monitorovanie a hodnotenie možno nájsť v oddiele 10 Posúdenie vplyvu.

1.5. Dôvody návrhu/iniciatívy

1.5.1. Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte

Každý členský štát musí mať:

– vnútroštátnu stratégiu v oblasti bezpečnosti sietí a informácií,

– plán spolupráce v oblasti bezpečnosti sietí a informácií,

– príslušný vnútroštátny orgán v oblasti bezpečnosti sietí a informácií, a

– tím reakcie na núdzové počítačové situácie (CERT).

Členské štáty musia na úrovni EÚ spolupracovať prostredníctvom siete.

Od verejnej správy a kľúčových účastníkov trhu zo súkromnej sféry sa vyžaduje, aby realizovali riadenie rizík v oblasti bezpečnosti sietí a informácií a aby oznamovali príslušným orgánom v oblasti bezpečnosti sietí a informácií incidenty s významným vplyvom.

1.5.2. Prínos zapojenia Európskej únie

Vzhľadom na cezhraničnú povahu bezpečnosti sietí a informácií sú rozdiely v príslušných právnych predpisoch a politikách obmedzujúce pre spoločnosti, ktoré vykonávajú svoju činnosť vo viacerých krajinách, ako aj pre dosiahnutie celkových úspor z rozsahu. Nedostatočné zasahovanie na úrovni EÚ by viedlo k situácii, keď by bez ohľadu na vzájomné prepojenia medzi sieťami a informačnými systémami každý členský štát konal samostatne.

Stanovené ciele možno preto lepšie dosiahnuť prostredníctvom akcie na úrovni EÚ, a nie na úrovni jednotlivých členských štátov.

1.5.3. Poznatky získané z podobných skúseností v minulosti

Návrh vychádza z analýzy, v ktorej sa uvádza, že na vytvorenie rovnakých podmienok pre všetkých a na uzatvorenie niektorých legislatívnych medzier sú potrebné regulačné

povinnosti. V dôsledku čisto dobrovoľného prístupu existuje v tejto oblasti spolupráca len medzi malým počtom členských štátov, ktoré majú vysokú úroveň spôsobilostí.

1.5.4. Zlučiteľnosť a možná synergia s inými finančnými nástrojmi

Návrh je v plnom rozsahu v súlade s Digitálnou agendou pre Európu, a tým aj so stratégiou Európa 2020. Je v súlade aj s regulačným rámcom pre elektronické komunikácie EÚ, smernicou EÚ o európskych kritických infraštruktúrach a smernicou EÚ o ochrane údajov, a tento rámec a smernice dopĺňa.

Tento návrh je priložený k oznámeniu Komisie a vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku o európskej stratégii kybernetickej bezpečnosti a tvorí jeho nevyhnutnú súčasť.

1.6. Trvanie akcie a jej finančného vplyvu

– ☐ Návrh/iniciatíva s **obmedzeným trvaním**

– ☐ Návrh/iniciatíva je v platnosti od [DD/MM]RRRR do [DD/MM]RRRR,

– ☐ Finančný vplyv trvá od RRRR do RRRR

– ☒ Návrh/iniciatíva s **neobmedzeným trvaním**

– Lehota na transpozíciu smernice začne bezprostredne po jej prijatí (predbežne v roku 2015) a bude trvať 18 mesiacov. Vykonávanie smernice sa však začne po jej prijatí a jeho súčasťou bude vytvorenie bezpečnej infraštruktúry, ktorá bude podporovať spoluprácu medzi členskými štátmi,

– a potom bude vykonávanie postupovať v plnom rozsahu.

1.7. Plánovaný spôsob hospodárenia[39]

– ☒ **Priame centralizované hospodárenie** na úrovni Komisie

– ☒ **Nepriame centralizované hospodárenie** s delegovaním úloh súvisiacich s plnením rozpočtu na:

– ☐výkonné agentúry

– ☒ subjekty zriadené spoločenstvami[40]

– ☐ národné verejnoprávne subjekty/subjekty poverené vykonávaním verejnej služby

– ☐ osoby poverené realizáciou osobitných akcií podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte v zmysle článku 49 nariadenia o rozpočtových pravidlách

– ☐ **Zdieľané hospodárenie** s členskými štátmi,

– ☐ **Decentralizované hospodárenie** s tretími krajinami

– ☐ **Spoločné hospodárenie** s medzinárodnými organizáciami vrátane Európskej vesmírnej agentúry.

V prípade viacerých spôsobov hospodárenia uveďte v oddiele „Poznámky“ presnejšie vysvetlenie.

Poznámky:
Agentúra ENISA, decentralizovaná agentúra založená Spoločenstvom, môže na základe svojho mandátu pomáhať členským štátom a Komisii pri vykonávaní tejto smernice tým, že sa prerozdelia zdroje, ktoré boli podľa VFR 2014 – 2020 plánované pre túto agentúru.

[39] Vysvetlenie spôsobov hospodárenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovej stránke BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Podľa článku 185 nariadenia o rozpočtových pravidlách.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa kontroly a predkladania správ

Uveďte časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Komisia bude pravidelne skúmať funkčnosť tejto smernice a podávať správy Európskemu parlamentu a Rade.

Komisia bude taktiež hodnotiť správnu transpozíciu tejto smernice členskými štátmi.

Návrh na zriadenie nástroja CEF ďalej poskytuje možnosť vykonať hodnotenie metód realizácie projektov, ako aj vplyvu ich realizácie s cieľom posúdiť, či boli dosiahnuté ciele vrátane cieľov týkajúcich sa ochrany životného prostredia.

2.2. Systémy riadenia a kontroly

2.2.1. Zistené riziká

– oneskorenia v realizácii projektu pri budovaní bezpečnej infraštruktúry

2.2.2. Plánované metódy kontroly

Dohody a rozhodnutia o vykonávaní činnosti v rámci nástroja CEF zabezpečia dohľad a finančnú kontrolu zo strany Komisie alebo zástupcu splnomocneného Komisiou, ako aj prostredníctvom auditov vykonávaných Dvorom audítorov a kontrol na mieste vykonávaných Európskym úradom pre boj proti podvodom (OLAF).

2.2.3. Náklady a prínosy kontrol a pravdepodobná miera neplnenia

Kontroly ex-ante a ex-post na základe rizika a možnosť vykonania auditu na mieste zabezpečia, aby boli náklady na kontroly primerané.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uveďte existujúce alebo plánované preventívne a ochranné opatrenia.

Komisia prijme vhodné opatrenia na zabezpečenie toho, aby pri vykonávaní akcie financovanej v rámci tejto smernice, boli finančné záujmy Únie chránené prostredníctvom preventívnych opatrení proti podvodom, korupcii a každej inej nezákonnej činnosti účinnými kontrolami, a aby v prípade zistenia nezrovnalostí boli vrátené nesprávne vyplatené sumy, a aby sa v prípade potreby uplatnili účinné, primerané a odradzujúce sankcie.

Komisia alebo jej zástupcovia a Dvor audítorov majú právomoc na základe kontrol dokumentov a kontrol na mieste vykonať audit u všetkých príjemcov grantov, dodávateľov a subdodávateľov, ktorým boli v rámci tohto programu poskytnuté finančné prostriedky Únie.

Európsky úrad pre boj proti podvodom (OLAF) môže vykonávať kontroly na mieste, kontroly hospodárskych subjektov, ktorých sa takéto financovanie priamo alebo nepriamo týka, a to v súlade s postupmi podľa nariadenia (Euratom, ES) č. 2185/96 v záujme zistenia, či v súvislosti s dohodou alebo rozhodnutím o grante alebo zmluvou týkajúcou sa financovania Úniou nedošlo k podvodu, korupcii alebo inému protiprávnemu konaniu, ktoré poškodzuje finančné záujmy Únie.

Bez toho, aby boli dotknuté vyššie uvedené odseky platí, že dohody o spolupráci s tretími krajinami a medzinárodnými organizáciami, dohody o grante, rozhodnutia

o grante a zmluvy, ktoré budú výsledkom vykonávania tohto nariadenia, udeľujú Komisii, Dvoru audítorov a úradu OLAF výslovné právo na vykonávanie takýchto auditov, kontrol a kontrol na mieste.

Nástroj CEF zabezpečuje, aby zmluvy o grante a verejné obstarávanie bolo založené na štandardných modeloch, ktoré stanovia všeobecne uplatniteľné opatrenia proti podvodom.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

- Existujúce rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo [Názov……..……...……]	DRP/NRP (41)	krajín EZVO[42]	kandidátskych krajín[43]	tretích krajín	v zmysle článku 18 ods. 1 písm. aa) nariadenia o rozpočtových pravidlách
	09 03 02 podporovať vzájomné prepojenie a interoperabilitu vnútroštátnych verejných služieb online, ako aj prístup do takýchto sietí	DRP	NIE	NIE	NIE	NIE

- Požadované nové rozpočtové riadky (neuplatňuje sa)

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo [Názov……..]	DRP/NRP	krajín EZVO	kandidátskych krajín	tretích krajín	v zmysle článku 18 ods. 1 písm. aa) nariadenia o rozpočtových pravidlách
	[XX.YY.YY.YY]		ÁNO/ NIE	ÁNO/NIE	ÁNO/ NIE	ÁNO/NIE

41 DRP = diferencované rozpočtové prostriedky / NRP = nediferencované rozpočtové prostriedky.

42 EZVO: Európske združenie voľného obchodu.

43 Kandidátske krajiny a prípadne potenciálne kandidátske krajiny západného Balkánu.

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca:	1	Inteligentný a inkluzívny rast

GR <…….>			2015* [44]	Rok **2016**	Rok **2017**	Rok **2018**	Nasledujúce roky (2019 – 2021) a ďalšie			**SPOLU**
• Operačné rozpočtové prostriedky										
09 03 02	Záväzky	(1)	1.250**	0.000						**1.250**
	Platby	(2)	0.750	0.250	0.250					**1.250**
Administratívne rozpočtové prostriedky financované z balíka prostriedkov určených na realizáciu špecifických programov[45]			**0.000**							**0.000**
Číslo rozpočtového riadka		(3)	**0.000**							**0.000**
Rozpočtové prostriedky pre GR <….> SPOLU	Záväzky	=1+1a +3	1.250	0.000						**1.250**
	Platby	=2+2a +3	0.750	0.250	0.250					**1.250**

• Operačné rozpočtové prostriedky SPOLU	Záväzky	(4)	1.250	0.000						**1.250**
	Platby	(5)	0.750	0.250	0.250					**1.250**
• Administratívne rozpočtové prostriedky financované z balíka prostriedkov určených na realizáciu špecifických		(6)	**0.000**							

[44] Rok N je rokom, v ktorom sa návrh/iniciatíva začína realizovať.

[45] Technická a/alebo administratívna pomoc a výdavky určené na financovanie realizácie programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

programov SPOLU										
Rozpočtové prostriedky OKRUHU 1 viacročného finančného rámca **SPOLU**	Záväzky	=4+ 6	1.250	0.000						**1.250**
	Platby	=5+ 6	0.750	0.250	0.250					**1.250**

* Presné časové nastavenie bude závisieť od dátumu prijatia návrhu zákonodarným orgánom (t. j. ak bude smernica schválená v priebehu roku 2014, prispôsobenie existujúcej infraštruktúry by sa malo začať v roku 2015, inak o rok neskôr).

** Ak sa členské štáty rozhodnú používať existujúcu infraštruktúru a pokryť jednorazové náklady na jej úpravu v rozpočte EÚ, ako sa vysvetľuje v bodoch 1.4.3 a 1.7, náklady na prispôsobovanie siete v záujme podpory spolupráce medzi členskými štátmi podľa kapitoly III smernice (včasné varovanie, koordinovaná reakcia atď.) sa odhadujú na 1 250 000 EUR. Táto suma je o niečo vyššia ako suma uvedená v posúdení vplyvu („približne 1 milión EUR“), keďže je založená na presnejšom odhade potrebných stavebných prvkov takejto infraštruktúry. Potrebné stavebné prvky a náklady s nimi súvisiace sú založené na odhadoch Spoločného výskumného centra a jeho skúsenostiach s vytváraním podobných systémov pre iné oblasti, ako je verejné zdravotníctvo, a zahŕňali by: systém včasného varovania a oznamovania pre bezpečnosť sietí a informácií (275 000 EUR), platformu na výmenu informácií (400 000 EUR), systém včasného varovania a reakcie (275 000 EUR), situačné stredisko (300 000 EUR) v celkovej výške 1 250 000 EUR. V pripravovanej štúdii uskutočniteľnosti podľa osobitnej zmluvy SMART 2012/0010 sa očakáva podrobnejší plán: „Štúdia uskutočniteľnosti a prípravné činnosti na realizáciu európskeho systému včasného varovania a reakcie proti kybernetickým útokom a narušeniam“.

Ak má návrh/iniciatíva vplyv na viaceré okruhy:

• Operačné rozpočtové prostriedky SPOLU	Záväzky	(4)	0.000	0.000						
	Platby	(5)	0.000	0.000						
• Administratívne rozpočtové prostriedky financované z balíka prostriedkov určených na realizáciu špecifických programov SPOLU		(6)	**0.000**	**0.000**						
Rozpočtové prostriedky OKRUHOV 1 až 4 viacročného finančného rámca **SPOLU** (referenčná suma)	Záväzky	=4+ 6	1.250	0.000						1.250
	Platby	=5+ 6	0.750	0.250	0.250					1.250

Okruh viacročného finančného rámca	**5**	„Administratívne výdavky“

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Nasledujúce roky (2019 – 2021) a ďalšie			**SPOLU**
GR:CNECT									
• Ľudské zdroje		0.572	0.572	0.572	0.572	0.572	0.572	**0.572**	**4.004**
• Ostatné administratívne výdavky		0.318	0.118	0.318	0.118	0.318	0.118	**0.118**	**1.426**
GR pre komunikačné siete, obsah a technológie **SPOLU**	Rozpočtové prostriedky	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

Rozpočtové prostriedky OKRUHU 5 viacročného finančného rámca **SPOLU**	(Záväzky spolu = Platby spolu)	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		Rok **2015**[46]	Rok **2016**	Rok **2017**	Rok **2018**	Nasledujúce roky (2019 – 2021) a ďalšie			**SPOLU**
Rozpočtové prostriedky OKRUHOV 1 až 5 viacročného finančného rámca **SPOLU**	Záväzky	2.140	0.690	0.890	0.690	0.890	0.690	0.690	**6.680**
	Platby	1.640	0.940	1.140	0.690	0.890	0.690	0.690	**6.680**

[46] Rok N je rokom, v ktorom sa návrh/iniciatíva začína uskutočňovať.

3.2.2. Odhadovaný vplyv na operačné rozpočtové prostriedky

– ☐ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov.

– ☑ Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

– viazané rozpočtové prostriedky v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Uveďte ciele a výstupy ⇩			Rok **2015***		Rok **2016**		Rok **2017**		Rok **2018**		Nasledujúce roky (2019 – 2021) a ďalšie						**SPOLU**	
	VÝSTUPY																	
	Druh[47]	Priemerné náklady	Počet výstupov	Náklady	Počet výstupov	Náklady	Počet výstupov	Náklady	Počet výstupov	Náklady	Počet výstupov	Náklady	v	Náklady	Počet výstupov	Náklady	Počet výstupov spolu	Náklady spolu
KONKRÉTNY CIEĽ č. 2[48] Bezpečný systém výmeny informácií																		
Výstup	Upraviť infraštruktúru																	
Konkrétny cieľ č. 2 medzisúčet			1	1.250**													1	1.250
NÁKLADY SPOLU				1.250														1.250

47 Výstupy znamenajú dodané produkty a služby (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

48 Ako je uvedené v bode 1.4.2. „Konkrétny cieľ (ciele)...“

* Presné časové nastavenie bude závisieť od dátumu prijatia návrhu zákonodarným orgánom (t. j. ak bude smernica schválená v priebehu roku 2014, prispôsobenie existujúcej infraštruktúry by sa malo začať v roku 2015, inak o rok neskôr).

** Pozri bod 3.2.1.

3.2.3. Odhadovaný vplyv na administratívne rozpočtové prostriedky

3.2.3.1. Zhrnutie

– ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov.

– ☑ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Rok **2015**[49]	Rok **2016**	Rok **2017**	Rok **2018**	Nasledujúce roky (2019 – 2021) a ďalšie			**SPOLU**
OKRUH 5 viacročného finančného rámca								
Ľudské zdroje	0.572	0.572	0.572	0.572	0.572	0.572	0.572	**4.004**
Ostatné administratívne výdavky	0.318	0.118	0.318	0.118	0.318	0.118	0.118	**1.426**
OKRUH č. 5 viacročného finančného rámca medzisúčet	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**
Mimo OKRUHU 5 [50]viacročného finančného rámca								
Ľudské zdroje	0.000	0.000						**0.000**
Ostatné administratívne výdavky								
Mimo OKRUHU 5 viacročného finančného rámca medzisúčet	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**
SPOLU	0.890	0.690	0.890	0.690	0.890	0.690	0.690	**5.430**

Požadované administratívne rozpočtové prostriedky budú pokryté z rozpočtových prostriedkov GR pre komunikačné siete, obsah a technológie (GR CNECT), ktoré sú už pridelené na riadenie akcie a/alebo sú presunuté v rámci GR, v prípade potreby spolu s ďalšími rozpočtovými prostriedkami, ktoré sa môžu poskytnúť riadiacemu GR v rámci ročného postupu prideľovania rozpočtových prostriedkov a vzhľadom na existujúce rozpočtové obmedzenia.

[49] Rok N je rokom, v ktorom sa návrh/iniciatíva začína uskutočňovať.

[50] Technická a/alebo administratívna pomoc a výdavky určené na financovanie realizácie programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

Európska agentúra pre bezpečnosť sietí a informácií (ENISA) by na základe svojho mandátu mohla pomôcť členským štátom a Komisii pri vykonávaní smernice a tým, že sa prerozdelia zdroje, ktoré boli podľa VFR 2014 – 2020 plánované pre túto agentúru, t. j. bez ďalších rozpočtových prostriedkov alebo ľudských zdrojov.

3.2.3.2. Odhadované potreby ľudských zdrojov

– ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.

– ☑ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov Komisie, ako je uvedené v nasledujúcej tabuľke:

V zásade by nebola potrebná žiadna ďalšia pracovná sila. Požadované ľudské zdroje budú veľmi obmedzené a budú pokryté pracovníkmi z GR, ktorí sú už poverení riadením tejto činnosti.

Odhady sa zaokrúhľujú na celé čísla (alebo najviac na jedno desatinné miesto)

	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Nasledujúce roky (2019 – 2021) a ďalšie		
• Plán pracovných miest (úradníci a dočasní zamestnanci)							
09 01 01 01 (ústredie a zastúpenia Komisie)	4	4	4	4	4	4	4
XX 01 01 02 (delegácie)							
XX 01 05 01 (nepriamy výskum)							
10 01 05 01 (priamy výskum)							
• Externí zamestnanci (ekvivalent plného pracovného času)[51]							
09 01 02 01 (ZZ, DAZ, VNE z celkového finančného krytia)	1	1	1	1	1	1	1
XX 01 02 02 (ZZ, DAZ, PED, MZ a VNE v delegáciách)							
XX 01 04 ***yy*** [52] – ústredie[53]							
XX 01 04 ***yy*** [52] – delegácie							
XX 01 05 02 (ZZ, DAZ, VNE – nepriamy výskum)							
10 01 05 02 (ZZ, DAZ, VNE – priamy výskum)							
Iné rozpočtové riadky (uveďte)							
SPOLU	**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX predstavuje príslušnú oblasť politiky alebo rozpočtovú hlavu.

Potreby ľudských zdrojov budú pokryté úradníkmi GR CNECT, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Európska agentúra pre bezpečnosť sietí a informácií (ENISA) by na základe svojho súčasného mandátu mohla pomôcť členským štátom a Komisii pri vykonávaní smernice a tým, že sa prerozdelia zdroje, ktoré boli podľa VFR 2014 – 2020 plánované pre túto agentúru, t. j. bez ďalších rozpočtových prostriedkov alebo ľudských zdrojov.

[51] ZZ = zmluvný zamestnanec; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii; MZ = miestny zamestnanec; VNE = vyslaný národný expert.

[52] Pod stropom pre externých zamestnancov z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

[53] Najmä pre štrukturálne fondy, Európsky poľnohospodársky fond pre rozvoj vidieka (EPFRV) a Európsky fond pre rybné hospodárstvo (EFRH).

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	– Pripravovať delegované akty podľa článku 14 ods. 3, – pripravovať vykonávacie akty podľa článku 8, článku 9 ods. 2, článku 12, článku 14 ods. 5, článku 16, – prispievať k spolupráci v rámci siete na politickej aj operačnej úrovni, – zapájať sa do medzinárodných rokovaní a prípadných uzatváraní medzinárodných zmlúv.
Externí zamestnanci	Pomáhať podľa potreby pri všetkých uvedených úlohách.

3.2.4. Súlad s platným viacročným finančným rámcom

– ☑ Návrh/iniciatíva je v súlade s platným viacročným finančným rámcom.

– ☐ Návrh/iniciatíva si vyžaduje zmenu v plánovaní príslušného okruhu vo viacročnom finančnom rámci.

Odhadovaný finančný vplyv na operačné výdavky návrhu nastane, ak sa členské štáty rozhodnú prispôsobiť existujúcu infraštruktúru a poveria Komisiu, aby vykonala toto prispôsobenie v rámci VFR 2014 – 2020. Jednorazové náklady, ktoré sú s tým spojené, by boli pokryté v rámci nástroja CEF pod podmienkou, že bude k dispozícii dostatok finančných prostriedkov. Členské štáty si môžu prípadne buď rozdeliť náklady na prispôsobenie infraštruktúry alebo náklady na vytvorenie novej infraštruktúry.

– ☐ Návrh/iniciatíva si vyžaduje, aby sa použil nástroj flexibility alebo aby sa uskutočnila revízia viacročného finančného rámca[54].

Neuplatňuje sa.

3.2.5. Účasť tretích strán na financovaní

– Návrh/iniciatíva nezahŕňa spolufinancovanie tretími stranami.

3.3. Odhadovaný vplyv na príjmy

– ☑ Návrh/iniciatíva nemá finančný vplyv na príjmy.

[54] Pozri body 19 a 24 medziinštitucionálnej dohody.