EURÓPSKA KOMISIA

Brusel, 30.9.2010
KOM(2010) 521 v konečnom znení

2010/0275 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o Európskej agentúre pre bezpečnosť sietí a informácií (ENISA)

{SEK(2010) 1126}
{SEK(2010) 1127}

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

1.1. Politický kontext

Európska agentúra pre bezpečnosť sietí a informácií (ENISA) bola zriadená v marci 2004 na počiatočné obdobie piatich rokov na základe nariadenia (ES) č. 460/2004[1] s hlavným cieľom *„zabezpečenie vysokej a účinnej úrovne bezpečnosti sietí a informácií v rámci [Únie] […] s cieľom vybudovať kultúru bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora Európskej únie, a tým prispejúc k plynulému fungovaniu vnútorného trhu.“* Nariadením č. 1007/2008[2] sa predĺžil mandát agentúry ENISA do marca 2012.

Predĺženie mandátu agentúry ENISA v roku 2008 takisto vyvolalo diskusiu o všeobecnom smerovaní európskeho úsilia zameraného na zvýšenie bezpečnosti sietí a informácií, ku ktorej Komisia prispela otvorením verejnej konzultácie o možných cieľoch posilnenej politiky v oblasti bezpečnosti sietí a informácií na úrovni Únie. Táto verejná konzultácia prebiehala v období od novembra 2008 do januára 2009 a v rámci nej sa zhromaždilo takmer 600 príspevkov[3].

Komisia prijala 30. marca 2009 oznámenie o ochrane kritických informačných infraštruktúr[4] (CIIP), ktoré sa zameriava na ochranu Európy pred kybernetickými útokmi a narušeniami zvyšovaním pripravenosti, bezpečnosti a odolnosti spolu s akčným plánom, v ktorom sa agentúra ENISA vyzýva, aby zohrávala úlohu najmä pri podpore členských štátov. Akčný plán bol vo všeobecnosti schválený pri rozhovoroch na ministerskej konferencii o ochrane kritických informačných infraštruktúr (CIIP), ktorá sa konala v Tallinne v Estónsku v dňoch 27. a 28. apríla 2009[5]. V záveroch z konferencie predsedníctva Európskej únie sa zdôrazňuje význam *„zvýšenia operačnej podpory“* agentúry ENISA; uvádza sa v nich, že agentúra ENISA *„predstavuje cenný nástroj podpory úsilia v tejto oblasti, založeného na spolupráci v rámci celej Únie“* a poukazuje sa na potrebu prehodnotiť a preformulovať mandát agentúry *„s cieľom lepšie sa zamerať na priority a potreby EÚ; dosiahnuť schopnosť flexibilnejšej reakcie; rozvinúť zručnosti a kompetencie a zvýšiť prevádzkovú účinnosť a celkový vplyv agentúry“*, aby sa agentúra stala *„stálym prínosom pre každý členský štát a Európsku úniu ako celok“*.

Po rozhovoroch na zasadnutí rady pre telekomunikácie z 11. júna 2009, v rámci ktorých členské štáty vyjadrili podporu predĺženiu mandátu agentúry ENISA a zvýšeniu jej zdrojov

---

[1] 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 77 13.3.2004, s. 1).

[2] Nariadenie Európskeho parlamentu a Rady (ES) č. 1007/2008 z 24. septembra 2008, ktorým sa mení a dopĺňa nariadenie (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, pokiaľ ide o dobu jej trvania (Ú. v. EÚ L 293, 31.10.2008, s. 1).

[3] Súhrnná správa o výsledkoch verejnej konzultácie „Smerom k posilnenej politike v oblasti bezpečnosti sietí a informácií v Európe“ je priložená ako príloha 11 k posúdeniu vplyvu, ktoré je priložené k tomuto návrhu.

[4] KOM(2009) 149, 30.3.2009.

[5] Diskusný dokument: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf
Závery predsedníctva:
http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf.

vzhľadom na dôležitosť bezpečnosti sietí a informácií a vznikajúce problémy v oblasti, diskusia dospela k záveru v rámci švédskeho predsedníctva Únie. V uznesení Rady z 18. decembra 2009 o prístupe Európy k bezpečnosti sietí a informácií založenom na spolupráci[6] sa uznáva úloha a potenciál agentúry ENISA a potreba „*ďalej rozvinúť agentúru ENISA na účinný orgán*“. Zdôrazňuje sa v ňom aj potreba zmodernizovať a posilniť agentúru s cieľom podporiť Komisiu a členské štáty pri prekonávaní medzery medzi technológiou a politikou a slúžiť ako odborné centrum Únie v záležitostiach bezpečnosti sietí a informácií.

1.2. Všeobecný kontext

Informačné a komunikačné technológie (IKT) sa stali základom európskeho hospodárstva a spoločnosti ako celku. IKT sú citlivé na hrozby, ktoré už nerešpektujú národné hranice a ktoré sa zmenili v súvislosti s vývojom technológií a trhov. Keďže IKT sú globálne, vzájomne prepojené a navzájom závislé od iných infraštruktúr, ich bezpečnosť a odolnosť nie je možné zabezpečiť len vnútroštátnymi a nekoordinovanými prístupmi. Zároveň, problémy spojené s bezpečnosťou sietí a informácií sa rýchlo vyvíjajú. Siete a informačné systémy sa musia účinne chrániť proti všetkým druhom narušení a porúch vrátane útokov spôsobených ľudským faktorom.

Politiky týkajúce sa bezpečnosti sietí a informácií zohrávajú ústrednú úlohu v rámci Digitálnej agendy pre Európu[7] (DAE), hlavnej iniciatívy v rámci stratégie EÚ 2020, s cieľom využiť a zlepšiť potenciál IKT a previesť tento potenciál do udržateľného rastu a inovácií. Podpora využívania IKT a podpora istoty a dôvery v informačnú spoločnosť sú základnými prioritami DAE.

Agentúra ENISA bola pôvodne zriadená s cieľom zabezpečiť vysokú a účinnú úroveň bezpečnosti sietí a informácií v rámci Únie. Skúsenosti získané s agentúrou a problémy a hrozby zdôraznili potrebu modernizovať jej mandát, aby lepšie zodpovedal potrebám Európskej únie vyplývajúcim z:

- roztrieštenosť vnútroštátnych prístupov k riešeniu vznikajúcich problémov,
- nedostatku modelov na vykonávanie politík v oblasti bezpečnosti sietí a informácií založených na spolupráci,
- nedostatočnej úrovne pripravenosti aj v dôsledku obmedzenej schopnosti európskeho včasného varovania a reakcie,
- nedostatku spoľahlivých európskych údajov a obmedzenosti poznatkov o vznikajúcich problémoch,
- nízkej úrovne informovanosti o rizikách a problémoch v oblasti bezpečnosti sietí a informácií,
- potreby účinnejšie začleniť aspekty súvisiace s bezpečnosťou sietí a informácií do politík zameraných na boj proti počítačovej kriminalite.

---

[6] Uznesenie Rady z 18. decembra 2009 o prístupe Európy k bezpečnosti sietí a informácií založenom na spolupráci (Ú. v. EÚ C 321, 29.12.2009, s. 1). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

[7] KOM(2010) 245, 19.5.2010.

1.3. Ciele politiky

Všeobecným cieľom navrhovaného nariadenia je umožniť Únii, členským štátom a zainteresovaným stranám rozvinúť vysoký stupeň schopnosti a pripravenosti predchádzať problémom v oblasti bezpečnosti sietí a informácií, odhaľovať ich a lepšie na ne reagovať. To pomôže vybudovať dôveru, ktorá je predpokladom rozvoja informačnej spoločnosti, s cieľom zlepšiť konkurencieschopnosť európskych podnikov a zabezpečiť účinné fungovanie vnútorného trhu.

1.4. Existujúce ustanovenia v oblasti návrhu

Tento návrh dopĺňa regulačné a neregulačné politické iniciatívy týkajúce sa bezpečnosti sietí a informácií, ktoré sa prijali na úrovni Únie s cieľom zlepšiť bezpečnosť a odolnosť IKT:

- Akčný plán spustený na základe oznámenia o CIIP sa zameral na zriadenie:

    (1) Európskeho fóra pre členské štáty (EFMS) zameraného na podporu rozhovorov a výmenu týkajúcu sa dobrej politickej praxe s cieľom stanoviť si spoločné politické ciele a priority týkajúce sa bezpečnosti a odolnosti infraštruktúr IKT, ktorým tiež priamo prináša prospech fungovanie agentúry a ňou poskytovaná podpora.

    (2) Európskeho verejno-súkromného partnerstva pre odolnosť (EP3R), ktoré predstavuje flexibilný celoeurópsky riadiaci rámec pre odolnosť infraštruktúry IKT, pôsobiaci prostredníctvom podpory spolupráce medzi verejným a súkromným sektorom, týkajúcej sa cieľov v oblasti bezpečnosti a odolnosti, základných požiadaviek, dobrej politickej praxe a opatrení.

- Štokholmský program, ktorý Európska rada prijala 11. decembra 2009, podporuje politiky zabezpečujúce bezpečnosť sietí a umožňujúce rýchlejšiu reakciu v prípade počítačových útokov v Únii.

- Tieto iniciatívy prispievajú k účinnosti Digitálnej agendy pre Európu. Politiky v oblasti bezpečnosti sietí a informácií zohrávajú ústrednú úlohu v tej časti stratégie, ktorá sa zameriava na zvýšenie dôvery a bezpečnosti v informačnej spoločnosti. Podporujú aj podporné opatrenia a politiky Komisie týkajúce sa ochrany súkromia (najmä tzv. „privacy by design“ – ochrana súkromia už v štádiu návrhu) a osobných údajov (revízia rámca), sieť CPC, riadenie identity a program pre bezpečnejší internet.

1.5. Vývoj súčasnej politiky v oblasti bezpečnosti sietí a informácií týkajúci sa návrhu

Viaceré prebiehajúce politiky v oblasti bezpečnosti sietí a informácií, najmä tie, ktoré sa oznámili v Digitálnej agende pre Európu, využívajú podporu a expertízy agentúry ENISA. Medzi tieto politiky patria:

- - Posilnenie spolupráce v oblasti politiky zameranej na bezpečnosť sietí a informácií zintenzívnením činností v **Európskom fóre členských štátov (EFMS)**, ktoré s priamou podporou agentúry ENISA pomôže:

    – vymedziť spôsoby vytvorenia účinnej európskej siete prostredníctvom cezhraničnej spolupráce medzi národnými/vládnymi tímami reakcie na núdzové počítačové situácie (Computer Emergency Response Teams, CERT),

– vymedziť dlhodobé ciele a priority pre celoeurópske cvičenia zamerané na incidenty spojené s bezpečnosťou sietí a informácií vo veľkom rozsahu,

– posilniť minimálne požiadavky týkajúce sa verejného obstarávania s cieľom zvýšiť bezpečnosť a odolnosť verejných systémov a sietí,

– určiť hospodárske a regulačné podnety pre bezpečnosť a odolnosť,

– posúdiť stav zdravia bezpečnosti sietí a informácií v Európe.

- Posilnenie spolupráce a partnerstva medzi verejným a súkromným sektorom podporou **Európskeho verejno-súkromného partnerstva pre odolnosť (EP3R)**. Agentúra ENISA zohráva rastúcu úlohu pri uľahčovaní zasadnutí a činností EP3R. Medzi ďalšie opatrenia EP3R budú patriť:

  – Prediskutovanie inovatívnych opatrení a nástrojov na zlepšenie bezpečnosti a odolnosti, ako sú:

  (1) základné požiadavky na bezpečnosť a odolnosť, najmä pri verejnom obstarávaní výrobkov alebo služieb IKT, s cieľom poskytovať rovnaké podmienky pri zabezpečení primeranej úrovne pripravenosti a prevencie;

  (2) preskúmanie záležitostí spojených so zodpovednosťou hospodárskych subjektov, napríklad pri zavádzaní minimálnych bezpečnostných požiadaviek;

  (3) hospodárske stimuly pre rozvoj a prevzatie postupov riadenia rizika, bezpečnostných postupov a výrobkov;

  (4) schémy hodnotenia a riadenia rizika s cieľom posúdiť a riadiť významné incidenty na spoločnom základe porozumenia,

  (5) spolupráca medzi súkromným a verejným sektorom v prípade incidentov veľkého rozsahu;

  (6) Zorganizovanie **obchodného samitu** o hospodárskych prekážkach a hlavných faktoroch ovplyvňujúcich bezpečnosť a odolnosť.

- Zavedenie bezpečnostných požiadaviek uvedených v regulačnom balíku o elektronickej komunikácii do praxe, čo si vyžaduje expertízy a podporu agentúry ENISA:

  – podporiť členské štáty a Komisiu, pričom sa podľa potreby zohľadnia stanoviská súkromného sektora, navrhne sa rámec pravidiel a postupov s cieľom vykonať ustanovenia týkajúce sa ohlasovania porušení bezpečnosti (ustanovené v článku 13 písm. a) revidovanej rámcovej smernice),

  – vytvoriť ročné Fórum pre vnútroštátne príslušné orgány/národné regulačné orgány a zainteresované strany zo súkromného sektora pôsobiace v oblasti bezpečnosti sietí a informácií, aby prediskutovali získané skúsenosti a vymenili si osvedčené postupy pri uplatňovaní regulačných opatrení zameraných na bezpečnosť sietí a informácií.

- Uľahčenie **celoeurópskych cvičení zameraných na pripravenosť v oblasti počítačovej bezpečnosti** s podporou Komisie a príspevkom agentúry ENISA s výhľadom na rozšírenie takýchto cvičení v ďalšej fáze na medzinárodnú úroveň.

- **Vytvorenie CERT (tím reakcie na núdzové počítačové situácie) pre inštitúcie EÚ**. Kľúčové opatrenie 6 Digitálnej agendy pre Európu je, že Komisia predostrie „návrhy opatrení zamerané na posilnenie politiky v oblasti bezpečnosti sietí a informácií vysokej úrovne […] ako aj opatrenia umožňujúce rýchlejšie reagovať v prípade počítačových útokov vrátane CERT pre inštitúcie EÚ“[8]. To si bude vyžadovať, aby Komisia a ostatné inštitúcie Únie analyzovali a zriadili tímy reakcie na núdzové počítačové situácie, ktorým agentúra ENISA môže poskytovať technickú podporu a expertízy.

- Mobilizácia a podpora členských štátov pri kompletizácii a v prípade potreby zriaďovaní **vnútroštátnych/vládnych CERT s cieľom vytvoriť riadne fungujúcu sieť CERT pokrývajúcu celú Európu**. Táto činnosť bude rozhodujúca aj pre ďalší rozvoj Európskeho systému zdieľania informácií a varovania (EISAS) pre občanov a MSP, ktorý sa má vybudovať pomocou vnútroštátnych zdrojov a kapacít do konca roku 2012.

- **Zvyšovanie informovanosti** o problémoch v oblasti bezpečnosti sietí a informácií, ktoré zahŕňa:

  – spoluprácu Komisie s agentúrou ENISA pri navrhovaní usmernení o presadzovaní noriem v oblasti bezpečnosti sietí a informácií, správnej praxe a kultúry riadenia rizika. Vypracuje sa prvá vzorka usmernení,

  – agentúra ENISA zorganizuje v spolupráci s členskými štátmi „**Európsky mesiac bezpečnosti sietí a informácií pre všetkých“**, uvádzajúci národné/európske súťaže v oblasti počítačovej bezpečnosti.

1.6. Súlad s ostatnými politikami a cieľmi Únie

Návrh je v súlade so súčasnými politikami a cieľmi Európskej únie a je úplne v súlade s cieľom prispievať k hladkému fungovaniu vnútorného trhu prostredníctvom zlepšovania pripravenosti a schopnosti reagovať na problémy týkajúce sa bezpečnosti sietí a informácií.

2. VÝSLEDKY KONZULTÁCIÍ A POSÚDENIE VPLYVU

2.1. Konzultácie so zainteresovanými stranami

Táto politická iniciatíva je výsledkom širokej diskusie vykonanej na základe rozsiahleho prístupu a pri dodržaní zásad účasti, otvorenosti, zodpovednosti, účinnosti a jednotnosti. Široký proces, ktorý sa vykonal, zahŕňal hodnotenie agentúry v období rokov 2006 – 2007 na základe odporúčaní správnej rady agentúry ENISA, dve verejné konzultácie (v rokoch 2007 a 2008 – 2009) a množstvo seminárov o záležitostiach týkajúcich sa bezpečnosti sietí a informácií.

---

[8] V uznesení Rady z 18. decembra 2009 o prístupe Európy k bezpečnosti sietí a informácií založenom na spolupráci sa takisto ustanovuje, že: „Rada […] uznáva […] význam preskúmania strategických účinkov, rizík a perspektív vytvárania jednotiek CERT pre inštitúcie EÚ a zváženie prípadnej úlohy agentúry ENISA v tejto záležitosti v budúcnosti.“

Prvá verejná konzultácia sa začala v súvislosti s oznámením Komisie o priebežnom hodnotení agentúry ENISA. Konzultácia sa zameriavala na budúcnosť agentúry, prebiehala od 13. júna do 7. septembra 2007 a v rámci nej sa získalo celkovo 44 elektronických príspevkov a dva príspevky predložené v písomnej forme. Odpovede prišli od mnohých zainteresovaných strán vrátane ministerstiev, regulačných orgánov, odvetvia a združení spotrebiteľov, akademických inštitúcií, spoločností a jednotlivých občanov členských štátov.

Odpovede poukázali na množstvo zaujímavých otázok týkajúcich sa vývoja scenára v prípade hrozby; potreby objasniť nariadenie a vniesť doň vyššiu flexibilitu, aby sa agentúra ENISA mohla prispôsobovať problémom; dôležitosti zabezpečenia účinného vzájomného pôsobenia so zainteresovanými stranami a príležitosti na obmedzené zvýšenie jej zdrojov.

Druhá verejná konzultácia, ktorá sa konala v čase od 7. novembra 2008 do 9. januára 2009, sa zamerala na stanovenie prioritných cieľov pre silnejšiu politiku v oblasti bezpečnosti sietí a informácií na európskej úrovni a prostriedkov na dosiahnutie týchto cieľov. Takmer 600 príspevkov poskytli orgány členských štátov, akademické/výskumné inštitúcie, priemyselné združenia, súkromné spoločnosti a iné zainteresované strany, ako sú organizácie a konzultačné spoločnosti v oblasti ochrany údajov a jednotlivci.

Veľká väčšina respondentov[9] podporila predĺžený mandát agentúry a zasadzovala sa o rozšírenie jej úlohy pri koordinácii činností v oblasti bezpečnosti sietí a informácií na európskej úrovni a o zvýšenie jej zdrojov. Základnými prioritami boli potreba koordinovanejšieho prístupu k počítačovým hrozbám v celej Európe, nadnárodná spolupráca s cieľom reagovať na rozsiahle počítačové útoky, vybudovanie dôvery a lepšia výmena informácií medzi zainteresovanými stranami.

Posúdenie vplyvu návrhu sa vykonávalo od septembra 2009 na základe prípravnej štúdie, ktorú vypracoval externý kontraktor. Zapojilo sa doňho široké spektrum zainteresovaných strán a expertov. Medzi prispievateľov patrili orgány v oblasti bezpečnosti sietí a informácií členských štátov, národné regulačné orgány, telekomunikační operátori a poskytovatelia internetových služieb a združenia z pridružených odvetví, združenia spotrebiteľov, výrobcovia IKT, tímy reakcie na núdzové počítačové situácie (CERT), akademici a firemní užívatelia. Na podporu procesu posúdenia vplyvu bola zriadená medziodvetvová riadiaca skupina zložená z príslušných generálnych riaditeľstiev Komisie.

2.2. Posúdenie vplyvu

Zachovanie agentúry bolo určené ako vhodné riešenie na dosiahnutie európskych politických cieľov[10]. Na základe postupu predbežného hodnotenia sa na ďalšiu analýzu vybralo päť politických možností:

- Možnosť 1 – Žiadna politika,
- Možnosť 2 – Konať ako predtým, t. j. s podobným mandátom a pri rovnakej úrovni zdrojov,
- Možnosť 3 – Rozšírenie úloh agentúry ENISA, začlenenie orgánov v oblasti presadzovania práva a ochrany súkromia ako plne kvalifikovaných zainteresovaných strán,

[9] Pozri prílohu XI k posúdeniu vplyvu.
[10] Pozri prílohu IV k posúdeniu vplyvu.

- Možnosť 4 – Pridanie boja proti počítačovým útokom a reakcie na počítačové incidenty medzi jej úlohy,

- Možnosť 5 – Pridanie podpory orgánov presadzovania práva a súdnych orgánov pri boji proti počítačovej kriminalite k jej úlohám.

Na základe komparatívnej analýzy nákladov a prínosov sa možnosť 3 vyhodnotila ako najlepší nákladovo účinný a najefektívnejší spôsob dosiahnutia politických cieľov.

Na základe možnosti 3 sa predpokladá rozšírenie úlohy agentúry ENISA s cieľom zamerať sa na:

- vybudovanie a udržiavanie styčnej siete medzi zainteresovanými stranami a siete informácií s cieľom zabezpečiť, aby bola agentúra ENISA súhrnne informovaná o európskom prostredí bezpečnosti sietí a informácií;
- pôsobenie v úlohe podporného strediska v oblasti bezpečnosti sietí a informácií pre politický rozvoj a vykonávanie politiky (najmä vzhľadom na e-súkromie (e-privacy), elektronický podpis (e-sign) a e-ID a normy obstarávania v oblasti bezpečnosti sietí a informácií);
- podporu únijnej politiky CIIP a odolnosti (cvičenia, EP3R, Európsky systém zdieľania informácií a varovania atď.);
- vytvorenie rámca Únie pre zber údajov o bezpečnosti sietí a informácií vrátane navrhnutia metód a postupov pre podávanie a zdieľanie správ na základe právnych predpisov;
- štúdium ekonomiky bezpečnosti sietí a informácií;
- stimulovanie spolupráce s tretími krajinami a medzinárodnými organizáciami s cieľom podporiť spoločný globálny prístup k bezpečnosti sietí a informácií a získavania vplyvu na medzinárodné iniciatívy na vysokej úrovni v Európe;
- vykonávanie neoperatívnych úloh týkajúcich sa aspektov spolupráce v rámci presadzovania práva a súdnictva v oblasti počítačovej kriminality súvisiacich s bezpečnosťou sietí a informácií.

3. PRÁVNE PRVKY NÁVRHU

3.1. Zhrnutie navrhovaných opatrení

Navrhované nariadenie sa zameriava na posilnenie a modernizáciu Európskej agentúry pre bezpečnosť sietí a informácií (ENISA) a zriadenie nového mandátu na obdobie piatich rokov.

Návrh obsahuje niektoré základné zmeny oproti pôvodnému nariadeniu:

(1) **Vyššia flexibilita, adaptabilita a schopnosť zamerať sa**. Úlohy sú celkovo aktualizované a preformulované s cieľom poskytnúť väčší priestor činnostiam agentúry; sú dostatočne presné na zobrazenie spôsobov, ktorými sa ciele majú dosiahnuť. Presnejšie sa tak vymedzuje zameranie agentúry, zlepšuje sa jej schopnosť dosiahnuť ciele a posilňujú sa jej úlohy zamerané na podporu vykonávania politiky Únie.

(2) **Lepšie zosúladenie agentúry s politickým a regulačným procesom Únie**. Európske inštitúcie a orgány sa môžu obrátiť na agentúru o pomoc a poradenstvo. To je v súlade s politickým a regulačným vývojom: Rada sa začala obracať na agentúru priamo v uzneseniach a Európsky parlament a Rada udelili agentúre úlohy súvisiace s bezpečnosťou sietí a informácií v regulačnom rámci o elektronických komunikáciách.

(3) **Prepojenie s bojom proti počítačovej kriminalite**. Agentúra pri dosahovaní svojich cieľov zohľadňuje boj proti počítačovej kriminalite. Orgány v oblasti presadzovania práva a ochrany súkromia sa stanú plne kvalifikovanými zainteresovanými stranami agentúry, a to v stálej skupine zainteresovaných strán.

(4) **Posilnená riadiaca štruktúra**. Návrhom sa zvyšuje úloha správnej rady agentúry, v ktorej majú zastúpenie členské štáty a Komisia, v oblasti dohľadu. Napríklad správna rada môže vydať všeobecné usmernenia týkajúce sa zamestnancov, čo bola predtým výlučná právomoc výkonného riaditeľa. Môže zriadiť aj pracovné orgány, ktoré jej budú pomáhať pri vykonávaní úloh vrátane monitorovania vykonávania jej rozhodnutí.

(5) **Zjednodušenie postupov**. Postupy, ktoré sa ukázali ako zbytočne náročné, sa zjednodušujú. Príklady: a) zjednodušený postup pre vnútorné pravidlá správnej rady, b) stanovisko k pracovnému programu agentúry ENISA vydávajú útvary Komisie namiesto toho, aby sa poskytovalo prostredníctvom rozhodnutia Komisie. Správna rada takisto disponuje primeranými zdrojmi, ak potrebuje prijať vykonávacie rozhodnutia a realizovať ich (napr. ak zamestnanec podá sťažnosť na výkonného riaditeľa alebo na samu radu).

(6) **Postupné zvyšovanie zdrojov**. Očakáva sa, že finančné a ľudské zdroje agentúry sa budú v rokoch 2012 až 2016 postupne zvyšovať s cieľom splniť posilnené európske priority a rozšírené výzvy, bez toho, aby tým bol dotknutý návrh ďalšieho viacročného finančného rámca predložený Komisiou. Na základe návrhu nariadenia predloženého Komisiou, ktorým sa stanovuje viacročný finančný rámec na obdobie po roku 2013, a s prihliadnutím na závery posúdenia vplyvu, Komisia predloží zmenený a doplnený legislatívny finančný výkaz.

(7) **Možnosť predĺžiť funkčné obdobie výkonného riaditeľa**. Správna rada môže predĺžiť funkčné obdobie výkonného riaditeľa o tri roky.

3.2. Právny základ

Tento návrh sa zakladá na článku 114 Zmluvy o fungovaní Európskej únie[11] (ZFEÚ).

V súlade s rozsudkom Európskeho súdneho dvora[12] pred nadobudnutím platnosti Lisabonskej zmluvy sa podľa **článku 95 Zmluvy o ES** musel posúdiť vhodný právny základ na zriadenie orgánu na účely zabezpečenia vysokej a účinnej úrovne bezpečnosti sietí a informácií v rámci Únie. Použitím výrazu „opatrenia na aproximáciu“ v článku 95 autori zmluvy zamýšľali zveriť zákonodarnému orgánu Únie možnosť vybrať vhodné opatrenia na dosiahnutie

[11] Ú. v. EÚ C 115, 9.5.2008, s. 94.

[12] ESD, 2.5.2006, C-217/04, Spojené kráľovstvo Veľkej Británie a Severného Írska/Európsky parlament a Rada Európskej únie.

želaného výsledku. Zvýšenie bezpečnosti a odolnosti infraštruktúr IKT je teda dôležitým prvkom, ktorý prispieva k hladkému fungovaniu vnútorného trhu.

Na základe Lisabonskej zmluvy sa **v článku 114 ZFEÚ**[13] opisuje – takmer zhodne – zodpovednosť za vnútorný trh. Z uvedených dôvodov bude tento článok naďalej uplatniteľným právnym základom pre prijímanie opatrení na zlepšenie bezpečnosti sietí a informácií. Zodpovednosť za vnútorný trh je teraz spoločnou právomocou Únie a členských štátov (článok 4 ods. 2 písm. a) ZFEÚ). To znamená, že Únia a členské štáty môžu prijať (záväzné) opatrenia a že členské štáty budú konať, keď Únia nevyužije svoju právomoc alebo sa rozhodne už nekonať (článok 2 ods. 2 ZFEÚ).

Opatrenia v rámci zodpovednosti za vnútorný trh si vyžadujú riadny legislatívny postup (články 289 a 294 ZFEÚ), ktorý sa podobá[14] predchádzajúcemu spolurozhodovaciemu postupu (článok 251 Zmluvy o ES).

Na základe Lisabonskej zmluvy sa predchádzajúce rozlišovanie pilierov zrušilo. Predchádzanie trestnej činnosti a boj proti nej sa stali spoločnou právomocou Únie. To vytvorilo príležitosť pre agentúru ENISA, aby zohrávala úlohu platformy pre aspekty boja proti počítačovej kriminalite týkajúce sa bezpečnosti sietí a informácií a vymieňanie stanovísk a najlepších postupov s orgánmi pôsobiacimi v oblasti počítačovej obrany, presadzovania práva a ochrany súkromia.

3.3. Zásada subsidiarity

Návrh je v súlade so zásadou subsidiarity: politika v oblasti bezpečnosti sietí a informácií si vyžaduje prístup založený na spolupráci a ciele návrhu nemôžu dosiahnuť členské štáty samostatne.

Úplná neintervenčná stratégia Únie v národných politikách v oblasti bezpečnosti sietí a informácií by ponechala úlohy na členských štátoch bez ohľadu na zjavnú vzájomnú závislosť existujúcich informačných systémov. Opatrenie zabezpečujúce primeranú úroveň koordinácie medzi členskými štátmi s cieľom zabezpečiť, aby sa riziká súvisiace s bezpečnosťou sietí a informácií riadne riadili v cezhraničnom kontexte, v ktorom vznikajú, preto dodržiava zásadu subsidiarity. Európske opatrenie by okrem toho zlepšilo účinnosť existujúcich národných politík, a tým pridalo hodnotu.

Navrhnutie spoločnej politiky a politiky založenej na spolupráci v oblasti bezpečnosti sietí a informácií bude mať okrem toho prospešný vplyv na ochranu základných práv a konkrétne práva na ochranu osobných údajov a súkromia. Potreba ochrany údajov je v súčasnosti rozhodujúca vzhľadom na skutočnosť, že európski občania čoraz častejšie zverujú svoje údaje zložitým informačným systémom, či už s možnosťou, alebo bez možnosti výberu, a bez toho, aby boli schopní správne posúdiť riziká súvisiace s ochranou údajov. Pri vzniku incidentov preto nemusia byť v každom prípade schopní prijať vhodné opatrenia, a nie je ani isté, či by členské štáty boli schopné účinne riešiť medzinárodné incidenty bez európskej koordinácie bezpečnosti sietí a informácií.

---

[13] Pozri vyššie.

[14] Riadny legislatívny postup sa líši najmä z hľadiska požiadaviek na väčšinu v Rade a Európskom parlamente.

3.4. Zásada proporcionality

Tento návrh je v súlade so zásadou proporcionality, pretože nezachádza nad rámec toho, čo je potrebné na dosiahnutie jeho cieľov.

3.5. Výber nástrojov

Navrhovaný nástroj: nariadenie, ktoré je priamo uplatniteľné vo všetkých členských štátoch.

4. VPLYV NA ROZPOČET

Návrh bude mať vplyv na rozpočet Únie.

Keďže sa ustanovujú úlohy, ktoré sa začlenia do nového mandátu agentúry ENISA, očakáva sa, že agentúre sa poskytnú zdroje potrebné na uspokojivé vykonávanie jej činností. Hodnotenie agentúry, rozsiahly konzultačný proces so zainteresovanými stranami na všetkých úrovniach a posúdenie vplyvu poukazujú na všeobecnú zhodu, že veľkosť agentúry je pod jej kritickou masou a že je potrebné zvýšenie zdrojov. Dôsledky a vplyv zvýšenia počtu zamestnancov a rozpočtu agentúry sa analyzujú v posúdení vplyvu, ktoré je pripojené k návrhu.

Financovanie zo zdrojov EÚ po roku 2013 sa preskúma v kontexte debaty o všetkých návrhoch v rámci celej Komisie na obdobie po roku 2013.

5. DODATOČNÉ POZNÁMKY

5.1. Trvanie

Nariadenie sa vzťahuje na obdobie piatich rokov.

5.2. Doložka o revízii

V nariadení sa ustanovuje hodnotenie agentúry, ktoré sa vzťahuje na obdobie od predchádzajúceho hodnotenia v roku 2007. Posúdi sa účinnosť agentúry pri dosahovaní jej cieľov uvedených v nariadení, to, či je agentúra stále účinným nástrojom a či by sa trvanie agentúry malo ďalej predĺžiť. Správna rada na základe zistení poskytne Komisii odporúčania týkajúce sa zmien tohto nariadenia, agentúry a jej pracovných postupov. S cieľom umožniť Komisii vypracovať akýkoľvek návrh na predĺženie mandátu v riadnom čase sa hodnotenie musí vykonať do konca druhého roku mandátu poskytnutého na základe nariadenia.

5.3. Prechodné opatrenia

Komisia si uvedomuje, že legislatívny proces Európskeho parlamentu a Rady si môže vyžadovať dlhší čas na debatu k návrhu a existuje riziko právneho vákua, ak sa nový mandát agentúry neprijme včas pred uplynutím existujúceho mandátu. Komisia preto navrhuje spolu s týmto návrhom nariadenie, ktorým sa predĺži existujúci mandát agentúry o 18 mesiacov, aby sa vytvoril dostatočný čas na rozhovory a riadny proces.

2010/0275 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o Európskej agentúre pre bezpečnosť sietí a informácií (ENISA)

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,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[15],

so zreteľom na stanovisko Výboru regiónov[16],

po postúpení návrhu národným parlamentom,

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) Elektronické komunikácie, infraštruktúry a služby sú hlavným faktorom v hospodárskom a spoločenskom vývoji. Zohrávajú rozhodujúcu úlohu pre spoločnosť a stali sa všadeprítomnými verejnými službami rovnako ako dodávky elektrickej energie alebo vody. Ich prerušenie má potenciál spôsobiť značné hospodárske škody, čo zdôrazňuje význam opatrení na zvýšenie ochrany a odolnosti zameraných na zabezpečenie kontinuity kritických služieb. Bezpečnosť elektronických komunikácií, infraštruktúr a služieb, najmä ich integrita a dostupnosť, stále čelia rastúcim problémom. Toto vyvoláva v spoločnosti čoraz väčšie obavy nielen pre možnosť problémov vyplývajúcich zo zložitosti systému, z nehôd, chýb a útokov, ktoré môžu mať následky pre fyzické infraštruktúry, ktoré dodávajú služby rozhodujúce pre blahobyt európskych občanov.

(2) Prostredie hrozieb sa stále mení a bezpečnostné incidenty môžu ohroziť dôveru užívateľov. Keďže závažné prerušenie elektronickej komunikácie, infraštruktúry a služieb môže mať významný hospodársky a sociálny vplyv, každodenné porušenia bezpečnosti, problémy a poškodenia hrozia narušením dôvery verejnosti v technológie, siete a služby.

(3) Pravidelné posúdenie stavu bezpečnosti sietí a informácií v Európe založené na spoľahlivých európskych údajoch je preto dôležité pre politikov, priemysel a užívateľov.

---

15 Ú. v. EÚ C [...], [...], s. [...].
16 Ú. v. EÚ C [...], [...], s. [...].

(4) Zástupcovia členských štátov, ktorí sa stretli na Európskej rade 13. decembra 2003, rozhodli, že Európska agentúra pre bezpečnosť sietí a informácií (ENISA), ktorá sa mala zriadiť na základe návrhu predloženého Komisiou, bude mať sídlo v niektorom z gréckych miest, ktoré určí grécka vláda.

(5) Európsky parlament a Rada prijali v roku 2004 nariadenie (ES) č. 460/2004[17] o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, ktoré malo prispieť k zabezpečeniu vysokej a účinnej úrovne bezpečnosti sietí a informácií v rámci Únie a vybudovaniu kultúru bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora. Európsky parlament a Rada prijali v roku 2008 nariadenie (ES) č. 1007/2008[18], ktorým sa predĺžil mandát agentúry do marca 2012.

(6) Od zriadenia agentúry sa problémy spojené s bezpečnosťou sietí a informácií zmenili spolu s vývojom technológií, trhov a sociálno-ekonomickým vývojom a boli predmetom ďalších úvah a rozhovorov. V reakcii na meniace sa problémy Únia aktualizovala svoje priority politiky bezpečnosti sietí a informácií v mnohých dokumentoch, vrátane oznámenia Komisie z roku 2006 *Stratégia pre bezpečnú informačnú spoločnosť – Dialóg, partnerstvo a aktívne pôsobenie*[19], uznesenia Rady z roku 2007 o stratégii pre bezpečnú informačnú spoločnosť v Európe[20], oznámenia z roku 2009 *Ochrana kritických informačných infraštruktúr – „Ochrana Európy pred rozsiahlymi kybernetickými útokmi a narušeniami: zvyšovanie pripravenosti, bezpečnosti a odolnosti“*[21], záverov predsedníctva ministerskej konferencie o ochrane kritických informačných infraštruktúr (CIIP), uznesenia Rady z roku 2009 o prístupe Európy k bezpečnosti sietí a informácií založenom na spolupráci[22]. Bola uznaná potreba modernizovať a posilniť agentúru, aby úspešne prispievala k úsiliu európskych inštitúcií a členských štátov rozvinúť európsku schopnosť riešiť problémy spojené s bezpečnosťou sietí a informácií. Komisia nedávno prijala Digitálnu agendu pre Európu[23] ako hlavnú iniciatívu v rámci stratégie Európa 2020. Táto rozsiahla agenda má za cieľ využiť a rozvinúť potenciál IKT, aby ho bolo možné premeniť na udržateľný rast a inovácie. Podpora dôvery v informačnú spoločnosť je jedným z kľúčových cieľov tejto rozsiahlej agendy ohlasujúcej celý rad opatrení, ktoré má Komisia v tejto oblasti prijať a medzi ktoré patrí aj tento návrh.

(7) Opatrenia vnútorného trhu v oblasti bezpečnosti elektronických komunikácií a všeobecnejšie bezpečnosti sietí a informácií požadujú od členských štátov a Komisie rôzne formy technických a organizačných aplikácií. Heterogénne uplatňovanie týchto požiadaviek môže viesť k nedostatkom a môže vytvoriť prekážky pre vnútorný trh. Je preto potrebné odborné centrum na európskej úrovni, ktoré poskytuje usmernenia, poradenstvo a na požiadanie aj pomoc v otázkach spojených s bezpečnosťou sietí a informácií a na ktoré sa môžu členské štáty a európske inštitúcie spoľahnúť. Agentúra môže uspokojiť tieto potreby vytvorením a udržiavaním vysokej úrovne

---

17 Ú. v. ES L 77, 13.3.2004, s. 1.
18 Ú. v. EÚ L 293, 31.10.2008, s. 1.
19 KOM(2006) 251, 31.5.2006.
20 Uznesenie Rady z 22. marca 2007 o stratégii pre bezpečnú informačnú spoločnosť v Európe (Ú. v. EÚ C 68, 24.3.2007, s. 1).
21 KOM(2009) 149, 30.3.2009.
22 Uznesenie Rady z 18. decembra 2009 o prístupe Európy k bezpečnosti sietí a informácií založenom na spolupráci (Ú. v. EÚ C 321, 29.12.2009, s. 1).
23 KOM(2010) 245, 19.5.2010.

odbornosti a tým, že členským štátom, Komisii, a v dôsledku toho aj podnikateľskej obci, pomôže dodržiavať právne a regulačné požiadavky na bezpečnosť sietí a informácií, čím prispeje k hladkému fungovaniu vnútorného trhu.

(8) Agentúra by mala vykonávať úlohy, ktoré jej boli zverené na základe súčasných právnych predpisov Únie v oblasti elektronickej komunikácie, a vo všeobecnosti prispievať k vyššej úrovni bezpečnosti elektronickej komunikácie, okrem iného prostredníctvom poskytovania expertíz a poradenstva a podporou výmeny správnej praxe.

(9) V smernici Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica)[24] sa ďalej požaduje, aby poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb prijali vhodné opatrenia na zachovanie ich integrity a bezpečnosti a zaviedli požiadavky na oznamovanie narušení bezpečnosti a strát integrity. Ak je to vhodné, agentúre posielajú hlásenia aj národné regulačné orgány, ktoré musia Komisii a agentúre predkladať aj ročnú súhrnnú správu o hláseniach, ktoré dostali, a o prijatých opatreniach. V smernici 2002/21/ES sa agentúra ďalej vyzýva, aby poskytovaním stanovísk prispievala k harmonizácii vhodných technických a organizačných bezpečnostných opatrení.

(10) 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)[25], sa vyžaduje, aby poskytovateľ verejne dostupných elektronických komunikačných služieb prijal primerané technické a organizačné opatrenia na zachovanie bezpečnosti jeho služieb, a takisto sa požaduje dôvernosť komunikácií a súvisiaceho pohybu údajov. V smernici 2002/58/ES sa zavádzajú požiadavky na informácie o porušeniach osobných údajov a ich nahlasovanie pre poskytovateľov elektronických komunikačných služieb. Takisto sa v nej požaduje, aby Komisia konzultovala agentúru pri všetkých technických vykonávacích opatreniach, ktoré sa majú prijať a ktoré sa týkajú okolností alebo formátu a postupov uplatniteľných na požiadavky týkajúce sa informácií a nahlasovania. V smernici Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov[26] sa vyžaduje, aby členské štáty ustanovili, že kontrolór musí zaviesť vhodné technické a organizačné opatrenia na ochranu osobných údajov proti náhodnému alebo nezákonnému zničeniu alebo náhodnej strate, zmene, neoprávnenému zverejneniu alebo prístupu, najmä ak spracovanie zahŕňa prenos údajov v sieti, a proti všetkým ostatným nezákonným formám spracovania.

(11) Agentúra by mala prispievať k vysokej úrovni bezpečnosti sietí a informácií v rámci Únie a k vytvoreniu kultúry bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora v Európskej únii, a tak prispievať k hladkému fungovaniu vnútorného trhu.

---

[24] Ú. v. ES L 108, 24.4.2002, s. 33.
[25] Ú. v. ES L 201, 31.7.2002, s. 37.
[26] Ú. v. ES L 281, 23.11.1995, s. 31.

(12) Súbor úloh by mal naznačiť, ako agentúra dosiahne svoje ciele, pričom by mal umožniť flexibilitu jej činností. Medzi úlohy, ktoré agentúra vykonáva, by mali patriť zber vhodných informácií a údajov potrebných na vykonanie analýz rizík spojených s bezpečnosťou a odolnosťou elektronickej komunikácie, infraštruktúr a služieb a na posúdenie stavu bezpečnosti sietí a informácií v Európe v spolupráci s členskými štátmi. Agentúra by mala zabezpečovať koordináciu s členskými štátmi a zlepšovať spoluprácu medzi zainteresovanými stranami v Európe, predovšetkým zapojením príslušných vnútroštátnych orgánov a expertov zo súkromného sektora do jej činností v oblasti bezpečnosti sietí a informácií. Agentúra by mala poskytovať pomoc Komisii a členským štátom pri ich dialógu s odvetvím s cieľom vyriešiť problémy spojené s bezpečnosťou v hardvérových a softvérových výrobkoch, čím by prispievala k prístupu k bezpečnosti sietí a informácií založenom na spolupráci.

(13) Agentúra by mala pôsobiť ako referenčný bod a vybudovať si dôveryhodnosť svojou nezávislosťou, kvalitou poskytovaného poradenstva a šírených informácií, transparentnosťou svojich postupov a pracovných metód a dôslednosťou pri vykonávaní pridelených úloh. Agentúra by mala stavať na vnútroštátnom úsilí a úsilí Únie, a preto vykonávať svoje úlohy v úplnej spolupráci s členskými štátmi, a mala by byť otvorená kontaktom s priemyslom a inými príslušnými zainteresovanými stranami. Agentúra by okrem toho mala budovať na vstupoch zo súkromného sektora a spolupráci s týmto sektorom, ktorý zohráva významnú úlohu pri zabezpečovaní elektronickej komunikácie, infraštruktúr a služieb.

(14) Komisia iniciovala európske verejno-súkromné partnerstvo pre odolnosť ako flexibilný celoeurópsky riadiaci rámec pre odolnosť infraštruktúry IKT, v ktorom by agentúra mala zohrávať uľahčujúcu úlohu, spájať zainteresované strany z verejného a súkromného sektora s cieľom prediskutovať priority verejnej politiky, ekonomické a trhové rozmery výzev a opatrenia zamerané na odolnosť infraštruktúry IKT a vymedziť zodpovednosť zainteresovaných strán.

(15) Agentúra by mala poskytovať poradenstvo Komisii prostredníctvom stanovísk a technických a sociálno-ekonomických analýz na žiadosť Komisie alebo z vlastného podnetu, mala by pomáhať pri navrhovaní politiky v oblasti bezpečnosti sietí a informácií. Agentúra by mala na požiadanie pomáhať aj členským štátom a európskym inštitúciám a orgánom v ich úsilí rozvinúť politiku a kapacity v oblasti bezpečnosti sietí a informácií.

(16) Agentúra by mala pomáhať členským štátom a európskym inštitúciám pri ich úsilí vybudovať a zlepšiť cezhraničné kapacity a pripravenosti predchádzať problémom a incidentom spojeným s bezpečnosťou sietí a informácií, odhaľovať ich, zmierňovať ich a reagovať na ne; v tomto smere by agentúra mala uľahčovať spoluprácu medzi členskými štátmi a členskými štátmi a Komisiou. Agentúra by mala na tento účel zohrávať aktívnu úlohu pri podpore členských štátov v ich trvalom úsilí zlepšovať svoje reakčné schopnosti a organizovať a vykonávať vnútroštátne a európske cvičenia týkajúce sa bezpečnostných incidentov.

(17) Spracovanie osobných údajov vykonávané podľa tohto nariadenia sa riadi smernicou 95/46/ES.

(18) S cieľom lepšie pochopiť výzvy v oblasti bezpečnosti sietí a informácií musí agentúra analyzovať existujúce a vznikajúce riziká. Agentúra by na tento účel mala v spolupráci

s členskými štátmi a v prípade vhodnosti so štatistickými orgánmi zhromažďovať príslušné informácie. Agentúra by mala okrem toho pomáhať členským štátom a európskym inštitúciám a orgánom pri ich úsilí zhromažďovať, analyzovať a rozširovať údaje o bezpečnosti sietí a informácií.

(19) Agentúra by pri vykonávaní monitorovacích činností v Únii mala uľahčovať spoluprácu medzi Úniou a členskými štátmi pri posudzovaní stavu bezpečnosti sietí a informácií v Európe a podieľať sa na hodnotiacich činnostiach v spolupráci s členskými štátmi.

(20) Agentúra by mala uľahčovať spoluprácu príslušných verejných orgánov členských štátov, predovšetkým podporou rozvoja a výmeny osvedčených postupov a noriem pre vzdelávacie programy a schémy na zvyšovanie informovanosti. Intenzívnejšia výmena informácií medzi členskými štátmi uľahčí takúto činnosť. Agentúra by mala takisto podporovať spoluprácu medzi verejnými a súkromnými zainteresovanými stranami na úrovni Únie, čiastočne prostredníctvom podpory spoločného využívania informácií, kampaní na zvýšenie informovanosti a vzdelávacích a školiacich programov.

(21) Účinné bezpečnostné politiky by mali vychádzať zo správne navrhnutých metód posudzovania rizika vo verejnom i v súkromnom sektore. Metódy a postupy posudzovania rizika sa používajú na rôznych úrovniach bez spoločného postupu pre ich účinné uplatňovanie. Podpora a vývoj najlepších postupov na posudzovanie rizika a interoperačné riešenia riadenia rizika v organizáciách verejného a súkromného sektora zvýšia stupeň bezpečnosti sietí a informačných systémov v Európe. S týmto cieľom by agentúra mala podporovať spoluprácu verejných a súkromných zainteresovaných strán na úrovni Únie, pričom by mala uľahčovať ich úsilie týkajúce sa navrhovania a preberania noriem riadenia rizika a merateľnej bezpečnosti elektronických výrobkov, systémov, sietí a služieb.

(22) Pri práci agentúry by sa mal využívať prebiehajúci výskum, rozvoj a činnosti technologického zisťovania, najmä tie, ktoré vykonávajú rôzne výskumné iniciatívy Európskej únie.

(23) Ak je to vhodné a užitočné pre napĺňanie jej rozsahu pôsobnosti, cieľov a úloh, agentúra by sa mala deliť o skúsenosti a všeobecné informácie s orgánmi a agentúrami vytvorenými podľa práva Európskej únie, ktoré sa zaoberajú bezpečnosťou sietí a informácií.

(24) Spoluprácou s orgánmi presadzovania práva v oblasti bezpečnostných aspektov počítačovej kriminality agentúra rešpektuje existujúce informačné kanály a vytvorené siete, ako sú kontaktné miesta uvedené v navrhovanej smernici Európskeho parlamentu a Rady o útokoch na informačné systémy, ktorou sa zrušuje rámcové rozhodnutie 2005/222/SVV, alebo v rámci Europolu vedenia jednotiek boja proti trestnej činnosti páchanej prostredníctvom moderných technológií.

(25) Agentúra by pri zabezpečovaní naplnenia svojich cieľov mala spolupracovať s orgánmi presadzovania práva a s orgánmi na ochranu súkromia na zvýrazňovaní a náležitom zohľadňovaní aspektov boja proti počítačovej kriminalite súvisiacich s bezpečnosťou sietí a informácií. Zástupcovia týchto orgánov by sa mali stať plne kvalifikovanými zainteresovanými stranami agentúry a mali by mať zastúpenie v stálej skupine zainteresovaných strán agentúry.

(26) Problémy súvisiace s bezpečnosťou sietí a informácií sú globálne problémy. Je potrebné užšia medzinárodná spolupráca s cieľom zlepšiť bezpečnostné normy, zlepšiť výmenu informácií a presadzovať spoločný globálny prístup k záležitostiam týkajúcim sa bezpečnosti sietí a informácií. Agentúra by na tento účel mala podporovať spoluprácu s tretími krajinami a medzinárodnými organizáciami, vo vhodných prípadoch v spolupráci s EEAS.

(27) Vykonávanie úloh agentúry by nemalo zasahovať do kompetencií ani by nemalo brániť či prekážať činnosti alebo sa prekrývať s príslušnými právomocami a úlohami: národných regulačných orgánov uvedených v smerniciach týkajúcich sa elektronických komunikačných sietí a služieb, ako aj Orgán európskych regulátorov pre elektronické komunikácie (BEREC) zriadeného nariadením Európskeho parlamentu a Rady 1211/2009[27] a výboru pre komunikáciu uvedeného v smernici 2002/21/ES, európskych orgánov pre normalizáciu, národných orgánov pre normalizáciu a stáleho výboru, ako sa uvádzajú 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 vzťahujúcich sa na služby informačnej spoločnosti[28] a dozorných orgánov členských štátov spojených s ochranou jednotlivcov vzhľadom na spracovanie osobných údajov a voľný pohyb takých údajov.

(28) S cieľom zabezpečiť, aby agentúra bola efektívna, členské štáty a Komisia by mali mať zastúpenie v správnej rade, ktorá by mala vymedziť všeobecné smerovanie činnosti agentúry a zabezpečiť, aby agentúra vykonávala svoje úlohy v súlade s týmto nariadením. Správna rada by mala mať potrebné právomoci na navrhnutie rozpočtu, overovanie jeho plnenia, prijatie vhodných rozpočtových pravidiel, navrhnutie transparentných pracovných postupov na rozhodovanie agentúry, prijatie pracovného programu agentúry, prijatie vlastného rokovacieho poriadku a vnútorných pravidiel činnosti agentúry a menovanie a rozhodovanie o predĺžení alebo ukončení mandátu výkonného riaditeľa. Správna rada by mala byť schopná zriadiť pracovné orgány, ktoré jej pomôžu pri vykonávaní jej úloh; takéto orgány by napríklad mohli navrhovať jej rozhodnutia alebo monitorovať ich vykonávanie.

(29) Hladké fungovanie agentúry vyžaduje, aby výkonný riaditeľ bol vymenovaný na základe zásluh a zdokumentovaných administratívnych a riadiacich schopností, ako aj na základe kvalifikácie a skúseností v súvislosti s bezpečnosťou sietí a informácií a aby vykonával svoje povinnosti úplne nezávisle, pokiaľ ide o organizáciu vnútorného chodu agentúry. Výkonný riaditeľ by mal na tento účel pripraviť návrh pracovného programu agentúry po predchádzajúcej konzultácii útvarov Komisie a prijať všetky potrebné opatrenia na zabezpečenie riadneho vykonania pracovného programu agentúry. Každý rok by mal vypracovať návrh všeobecnej správy, ktorý by sa mal predložiť správnej rade, návrh výkazu odhadov príjmov a výdavkov agentúry a mal by plniť rozpočet.

(30) Výkonný riaditeľ by mal mať možnosť zriadiť ad hoc pracovné skupiny s cieľom zamerať sa na osobitné záležitosti, najmä vedeckého, technického, právneho alebo sociálno-ekonomického charakteru. Výkonný riaditeľ by mal pri zriaďovaní ad hoc pracovných skupín požadovať vstupy z príslušných externých expertíz a využívať tieto expertízy potrebné na to, aby agentúra mala prístup k aktuálnym dostupným

---

[27] Ú. v. EÚ L 337, 18.12.2009, s. 1.
[28] Ú. v. ES L 204, 21.7.1998, s. 37.

informáciám o výzvach v oblasti bezpečnosti vyvolaných rozvíjajúcou sa informačnou spoločnosťou. Agentúra by mala zabezpečiť, aby sa členovia ad hoc pracovných skupín vyberali podľa najvyšších noriem na odbornosť, pričom by sa, v súlade s konkrétnymi podmienkami, náležite zohľadnila reprezentatívna rovnováha medzi verejnými správami členských štátov, súkromným sektorom vrátane odvetvia, užívateľmi a akademickými expertmi v oblasti bezpečnosti sietí a informácií. Agentúra môže v prípade potreby prizvať jednotlivých expertov uznaných za kompetentných v príslušnej oblasti, aby sa v jednotlivých prípadoch zúčastnili na konaniach pracovnej skupiny. Ich výdavky by mala hradiť agentúra v súlade so svojimi vnútornými pravidlami a v zhode s platnými nariadeniami o rozpočtových pravidlách.

(31) Agentúra by mala mať stálu skupinu zainteresovaných strán ako poradný orgán s cieľom zabezpečiť pravidelný dialóg so súkromným sektorom, organizáciami spotrebiteľov a inými príslušnými zainteresovanými stranami. Stála skupina zainteresovaných strán zriadená správnou radou na návrh výkonného riaditeľa by sa mala zameriavať na otázky dôležité pre všetky zainteresované strany a upriamiť na ne pozornosť agentúry. Výkonný riaditeľ môže, tam kde to bude vhodné a podľa programu zasadnutí, pozvať zástupcov Európskeho parlamentu a iných príslušných orgánov, aby sa zúčastnili na zasadnutiach skupiny.

(32) Agentúra vykonáva svoju činnosť podľa i) zásady subsidiarity, pričom zabezpečuje primeranú úroveň koordinácie medzi členskými štátmi v záležitostiach súvisiacich s bezpečnosťou sietí a informácií a zlepšuje účinnosť vnútroštátnych politík, čím im pridáva na hodnote a ii) zásadou proporcionality, pričom nezachádza nad rámec toho, čo je potrebné na dosiahnutie cieľov vymedzených v tomto nariadení.

(33) Agentúra by mala uplatňovať právne predpisy Únie týkajúce sa prístupu verejnosti k dokumentom, ako sa ustanovuje v nariadení Európskeho parlamentu a Rady (ES) č. 1049/2001[29], a ochrany jednotlivcov so zreteľom na spracovanie osobných údajov, ako sa vymedzuje v nariadení 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[30].

(34) Agentúra by mala v rámci rozsahu pôsobnosti, cieľov a pri vykonávaní úloh dodržiavať najmä ustanovenia uplatniteľné na európske inštitúcie a vnútroštátne právne predpisy týkajúce sa zaobchádzania s citlivými dokumentmi. Správna rada by mala mať právomoc prijať rozhodnutie, ktoré umožní agentúre spracovávať utajované informácie.

(35) S cieľom zaručiť úplnú autonómiu a nezávislosť agentúry sa považuje za nevyhnutné poskytnúť jej nezávislý rozpočet, ktorého príjmy pochádzajú predovšetkým z príspevku Únie a príspevkov tretích krajín, ktoré sa podieľajú na práci agentúry. Hostiteľský členský štát alebo akýkoľvek iný členský štát by mali mať možnosť dobrovoľne prispievať na príjmy agentúry. Rozpočtový postup Únie sa naďalej

---

[29] Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (Ú. v. ES L 145, 31.5.2001, s. 43).

[30] Nariadenie 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 (Ú. v. ES L 8, 12.1.2001, s. 1).

uplatňuje, pokiaľ ide o všetky dotácie účtované k všeobecnému rozpočtu Európskej únie. Okrem toho Dvor audítorov by mal vykonať audit účtov.

(36) Agentúra by mala byť nástupcom agentúry ENISA zriadenej nariadením č. 460/2004. V rámci rozhodnutia zástupcov členských štátov na zasadnutí Európskej rady z 13. decembra 2003 by hostiteľský členský štát mal udržiavať a rozvíjať súčasné praktické dojednania, aby zabezpečil hladkú a efektívnu prevádzku agentúry, najmä z hľadiska spolupráce agentúry s Komisiou a jej pomocou Komisii, členským štátom a ich príslušným orgánom, iným inštitúciám a orgánom Únie a zainteresovaným stranám z verejného i súkromného sektora v celej Európe.

(37) Agentúra by sa mala zriadiť na obmedzené obdobie. Jej činnosť by sa mala posúdiť vzhľadom na účinnosť dosahovania cieľov a účinnosť jej pracovných postupov s cieľom zistiť, či sú ciele agentúry stále aktuálne, a na základe toho určiť, či by sa malo trvanie jej činnosti ďalej predĺžiť,

PRIJALI TOTO NARIADENIE:

ODDIEL 1 ROZSAH PÔSOBNOSTI, CIELE A ÚLOHY

Článok 1
Predmet a rozsah pôsobnosti

1. Týmto nariadením sa zriaďuje Európska agentúra pre bezpečnosť sietí a informácií (ďalej len „agentúra“) so zámerom prispieť k vysokej úrovni bezpečnosti sietí a informácií v rámci Únie a s cieľom zvýšiť informovanosť a rozvinúť v spoločnosti kultúru bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora v Únii, a tak prispieť k hladkému fungovaniu vnútorného trhu.

2. Ciele a úlohy agentúry nemajú vplyv na právomoci členských štátov týkajúce sa bezpečnosti sietí a informácií a v žiadnom prípade na činnosti spojené s verejnou bezpečnosťou, obranou, bezpečnosťou štátu (vrátane hospodárskeho blahobytu štátu, ak problémy súvisia so záležitosťami bezpečnosti štátu) a na činnosti štátu v oblasti trestného práva.

3. Na účely toho nariadenia „bezpečnosť sietí a informácií“ znamená schopnosť siete alebo informačného systému odolať pri určitej úrovni dôvernosti náhodným udalostiam alebo nezákonnému alebo zlomyseľnému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov.

Článok 2
Ciele

1. Agentúra pomáha Komisii a členským štátom plniť právne a regulačné požiadavky na bezpečnosť sietí a informácií uvedené v súčasných a budúcich právnych predpisoch Únie, a tak prispieva k hladkému fungovaniu vnútorného trhu.

2. Agentúra zvyšuje schopnosť a pripravenosť Únie a členských štátov predchádzať problémom a nehodám v oblasti bezpečnosti sietí a informácií, odhaľovať ich a reagovať na ne.

3. Agentúra vytvára a udržiava vysokú úroveň odbornosti a túto odbornosť používa na podnietenie širokej spolupráce medzi subjektmi z verejného a súkromného sektora.

Článok 3
Úlohy

1. Na účel vymedzený v článku 1 agentúra vykonáva tieto úlohy:

a) pomáha Komisii na jej žiadosť alebo z vlastného podnetu pri navrhovaní politiky v oblasti bezpečnosti sietí a informácií, pričom jej poskytuje poradenstvo a stanoviská a technické a sociálno-ekonomické analýzy a vykonáva prípravné práce v prípade navrhovania a aktualizácie právnych predpisov Únie v oblasti bezpečnosti sietí a informácií;

b) uľahčuje spoluprácu medzi členskými štátmi a medzi členskými štátmi a Komisiou v rámci ich úsilia s cezhraničným rozmerom zabrániť incidentom týkajúcim sa bezpečnosti sietí a informácií, odhaliť ich a reagovať na ne;

c) pomáha členským štátom a európskym inštitúciám a orgánom v ich úsilí zhromažďovať, analyzovať a rozširovať údaje o bezpečnosti sietí a informácií;

d) v spolupráci s členskými štátmi a európskymi inštitúciami pravidelne posudzuje stav bezpečnosti sietí a informácií v Európe;

e) podporuje spoluprácu príslušných verejných orgánov v Európe, najmä podporou ich úsilia navrhnúť a vymieňať si osvedčené postupy a normy;

f) pomáha Únii a členským štátom pri presadzovaní používania riadenia rizika a správnej praxe a noriem v oblasti bezpečnosti pri elektronických výrobkoch, systémoch a službách;

g) podporuje spoluprácu verejných a súkromných zainteresovaných strán na úrovni Únie, okrem iného presadzovaním spoločného využívania informácií a zvyšovaním informovanosti a uľahčovaním ich úsilia o rozvoj a preberanie noriem riadenia rizika a bezpečnosti elektronických výrobkov, sietí a služieb;

h) uľahčuje výmenu správnej praxe a dialóg o bezpečnosti sietí a informácií, vrátane aspektov spojených s bojom proti počítačovej kriminalite, medzi verejnými a súkromnými zainteresovanými stranami; pomáha Komisii pri navrhovaní politiky, ktorá zohľadňuje aspekty bezpečnosti sietí a informácií v rámci boja proti počítačovej kriminalite;

i) na požiadanie pomáha členským štátom a európskym inštitúciám a orgánom v ich úsilí o rozvíjanie schopnosti odhaľovať problémy v oblasti bezpečnosti sietí a informácií, analyzovať ich a reagovať na ne;

j) podporuje dialóg a spoluprácu Únie s tretími krajinami a medzinárodnými organizáciami, vo vhodných prípadoch v spolupráci s EEAS, s cieľom podporiť medzinárodnú spoluprácu a globálny spoločný prístup k otázkam spojeným s bezpečnosťou sietí a informácií;

k) vykonáva úlohy zverené agentúre na základe legislatívnych aktov Únie.

ODDIEL 2 ORGANIZÁCIA

Článok 4
Orgány agentúry

Agentúru tvorí:

a) správna rada;

b) výkonný riaditeľ a zamestnanci a

c) stála skupina zainteresovaných strán.

Článok 5
Správna rada

1. Správna rada vymedzuje všeobecné smerovanie činnosti agentúry a zabezpečuje, aby agentúra pracovala v súlade s pravidlami a zásadami ustanovenými v tomto nariadení. Zabezpečuje aj súlad práce agentúry s činnosťami vykonávanými členskými štátmi i na úrovni Únie.

2. Správna rada prijíma svoj rokovací poriadok po dohode s príslušnými útvarmi Komisie.

3. Správna rada prijíma vnútorné pravidlá činnosti po dohode s príslušnými útvarmi Komisie. Tieto pravidlá sa uverejňujú.

4. Správna rada vymenúva výkonného riaditeľa v súlade s článkom 10 ods. 2 a môže výkonného riaditeľa odvolať. Správna rada vykonáva disciplinárnu právomoc nad výkonným riaditeľom.

5. Správna rada prijíma pracovný program agentúry v súlade s článkom 13 ods. 3 a všeobecnú správu o činnosti agentúry za predchádzajúci rok v súlade s článkom 14 ods. 2.

6. Správna rada prijíma rozpočtové pravidlá platné pre agentúru. Tieto pravidlá sa môžu odchyľovať od nariadenia Komisie (ES, Euratom) č. 2343/2002 z 19. novembra 2002 o rámcovom rozpočtovom nariadení pre subjekty uvedené v článku 185 nariadenia Rady (ES, Euratom) č. 1605/2002 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Európskych spoločenstiev[31], pokiaľ sa to osobitne nevyžaduje na prevádzku agentúry a s predchádzajúcim súhlasom Komisie.

7. Správna rada po dohode s Komisiou prijíma vhodné vykonávacie predpisy v súlade s článkom 110 služobného poriadku.

8. Správna rada môže zriadiť pracovné orgány zložené z jej členov, aby jej pomáhali pri vykonávaní úloh vrátane navrhovania rozhodnutí a monitorovania ich vykonávania.

---

[31] Ú. v. ES L 357, 31.12.2002, s. 72.

9. Správna rada môže prijať viacročný plán v oblasti zamestnaneckej politiky po konzultácii s útvarmi Komisie a po náležitom informovaní rozpočtového orgánu.

Článok 6
Zloženie správnej rady

1. Správnu radu tvorí jeden zástupca každého členského štátu, traja zástupcovia vymenovaní Komisiou a traja zástupcovia vymenovaní Komisiou bez hlasovacieho práva, z ktorých každý zastupuje jednu z týchto skupín:

a) priemysel informačných a komunikačných technológií;

b) skupiny spotrebiteľov;

c) akademickí experti na bezpečnosť sietí a informácií.

2. Členovia rady a ich zástupcovia sa menujú na základe úrovne príslušných skúseností a odbornosti v oblasti bezpečnosti sietí a informácií.

3. Funkčné obdobie zástupcov skupín uvedených v odseku 1 písm. a), b) a c) trvá štyri roky. Toto funkčné obdobie sa môže raz predĺžiť. Ak zástupca ukončí svoje členstvo v príslušnej záujmovej skupine, Komisia vymenuje náhradníka.

Článok 7
Predseda správnej rady

Správna rada volí spomedzi svojich členov svojho predsedu a zástupcu predsedu na obdobie troch rokov, ktoré je obnoviteľné. Zástupca predsedu nahradí ex officio predsedu, ak predseda nebude schopný plniť si svoje povinnosti.

Článok 8
Zasadnutia

1. Zasadnutia správnej rady zvoláva jej predseda.

2. Riadne zasadnutia správnej rady sa konajú dvakrát za rok. Na žiadosť predsedu alebo najmenej tretiny jej členov s hlasovacím právom sa môžu uskutočniť mimoriadne zasadnutia správnej rady.

3. Výkonný riaditeľ sa zúčastňuje na zasadnutiach správnej rady bez hlasovacích práv.

Článok 9
Hlasovanie

1. Správna rada prijíma svoje rozhodnutia väčšinou členov s hlasovacím právom.

2. Na prijatie rokovacieho poriadku správnej rady, vnútorných pravidiel činnosti agentúry, rozpočtu, ročného pracovného programu, ako aj na vymenovanie, predĺženie funkčného

obdobia alebo odvolanie výkonného riaditeľa je potrebná dvojtretinová väčšina všetkých členov správnej rady s hlasovacím právom.

Článok 10
Výkonný riaditeľ

1. Agentúru riadi jej výkonný riaditeľ, ktorý je nezávislý pri výkone svojich povinností.

2. Výkonného riaditeľa menuje a odvoláva správna rada. Osoba vybraná zo zoznamu kandidátov navrhnutých Komisiou sa menuje na obdobie piatich rokov na základe zásluh a zdokumentovaných administratívnych a riadiacich schopností, ako aj na základe konkrétnej kvalifikácie a skúseností. Pred vymenovaním možno kandidáta, ktorého vybrala správna rada, vyzvať, aby urobil vyhlásenie pred príslušným výborom Európskeho parlamentu a odpovedal na otázky jeho členov.

3. V priebehu deviatich mesiacov pred koncom tohto obdobia Komisia vykoná hodnotenie. V hodnotení Komisia posudzuje predovšetkým:

– výsledky činnosti výkonného riaditeľa,

– úlohy a požiadavky agentúry v nadchádzajúcich rokoch.

4. Správna rada môže na návrh Komisie so zreteľom na hodnotiacu správu a iba v prípadoch, keď to možno odôvodniť úlohami a požiadavkami na agentúru, jedenkrát predĺžiť funkčné obdobie riaditeľa najviac o tri roky.

5. Správna rada informuje Európsky parlament o svojom úmysle predĺžiť funkčné obdobie výkonného riaditeľa. Mesiac pred predĺžením funkčného obdobia môže byť výkonný riaditeľ vyzvaný, aby urobil vyhlásenie pred príslušným výborom Európskeho parlamentu a odpovedal na otázky jeho členov.

6. Ak sa funkčné obdobie nepredĺži, výkonný riaditeľ ostáva vo funkcii až do vymenovania svojho nástupcu.

7. Výkonný riaditeľ je zodpovedný za:

a) každodennú správu agentúry;

b) vykonávanie pracovného programu a rozhodnutí prijatých správnou radou;

c) zabezpečenie toho, aby agentúra vykonávala svoje úlohy v súlade s požiadavkami tých, ktorí využívajú jej služby, najmä vzhľadom na primeranosť poskytovaných služieb;

d) všetky osobitné záležitosti týkajúce sa zamestnancov, pričom zabezpečuje dodržiavanie všeobecných pokynov správnej rady a rozhodnutí správnej rady všeobecného charakteru;

e) nadviazanie a udržiavanie kontaktov s európskymi inštitúciami a orgánmi;

f) nadviazanie a udržiavanie kontaktov s podnikateľskou komunitou a spotrebiteľskými organizáciami na zabezpečenie pravidelného dialógu s príslušnými zainteresovanými stranami;

g) ostatné úlohy, ktoré sú mu pridelené na základe tohto nariadenia.

8. V prípade potreby a v rámci cieľov a úloh agentúry môže výkonný riaditeľ vytvoriť ad hoc pracovné skupiny zložené z expertov. Vopred o tom informuje správnu radu. Postupy týkajúce sa najmä zloženia, vymenovania expertov výkonným riaditeľom a činnosti ad hoc pracovných skupín sa upresňujú vo vnútorných pravidlách činnosti agentúry.

9. Výkonný riaditeľ správnej rade v prípade potreby zabezpečuje administratívnu podporu poskytovanú zamestnancami a iné zdroje.

Článok 11
Stála skupina zainteresovaných strán

1. Správna rada na návrh výkonného riaditeľa zriadi stálu skupinu zainteresovaných strán zloženú z expertov zastupujúcich príslušné zainteresované strany, ako sú odvetvie informačných a komunikačných technológií, skupiny spotrebiteľov, akademickí experti na bezpečnosť sietí a informácií a orgány pôsobiace v oblasti presadzovania práva a ochrany súkromia.

2. Postupy týkajúce sa najmä počtu, zloženia, vymenovania členov správnou radou, návrhu výkonného riaditeľa a činnosti skupiny sa vymedzia vo vnútorných pravidlách činnosti agentúry a uverejnia sa.

3. Skupine predsedá výkonný riaditeľ.

4. Funkčné obdobie členov skupiny je dva a pol roka. Členovia správnej rady nemôžu byť členmi skupiny. Zamestnanci Komisie sú oprávnení zúčastňovať sa na zasadnutiach skupiny a podieľať sa na jej práci.

5. Skupina poskytuje poradenstvo agentúre pri vykonávaní jej činností. Skupina predovšetkým poskytuje poradenstvo výkonnému riaditeľovi pri vypracovaní návrhu pracovného programu agentúry a pri zabezpečovaní komunikácie s príslušnými zainteresovanými stranami o všetkých otázkach týkajúcich sa pracovného programu.

ODDIEL 3 ČINNOSŤ

Článok 12
Pracovný program

1. Agentúra vykonáva svoje činnosti v súlade so svojím pracovným programom, ktorý obsahuje všetky jej plánované činnosti. Pracovný program nebráni agentúre ujať sa vykonávania nepredvídaných činností, ktoré možno zahrnúť do jej cieľov a úloh a do rámca rozpočtových obmedzení. Výkonný riaditeľ informuje správnu radu o činnostiach agentúry, ktoré nie sú uvedené v pracovnom programe.

2. Výkonný riaditeľ zodpovedá za vypracovanie návrhu pracovného programu agentúry po predchádzajúcej konzultácii s útvarmi Komisie. Výkonný riaditeľ do 15. marca každého roka predkladá správnej rade návrh pracovného programu na nasledujúci rok.

3. Správna rada prijíma každý rok do 30. novembra pracovný program agentúry na ďalší rok po konzultácii s útvarmi Komisie. Pracovný program obsahuje viacročný výhľad. Správna rada zabezpečuje, aby bol pracovný program v súlade s cieľmi agentúry a s legislatívnymi a politickými prioritami Únie v oblasti bezpečnosti sietí a informácií.

4. Pracovný program je štruktúrovaný v súlade so zásadou riadenia založeného na činnostiach (Activity-Based Management – ABM). Pracovný program je v súlade s výkazom odhadov príjmov a výdavkov agentúry a rozpočtom agentúry na ten istý rozpočtový rok.

5. Výkonný riaditeľ posiela pracovný program po jeho prijatí správnou radou Európskemu parlamentu, Rade, Komisii a členským štátom a zabezpečuje jeho uverejnenie.

Článok 13
Všeobecná správa

1. Výkonný riaditeľ predkladá každý rok správnej rade návrh všeobecnej správy, ktorá sa vzťahuje na všetky činnosti agentúry v predchádzajúcom roku.

2. Správna rada prijíma každý rok do 31. mája všeobecnú správu o činnostiach agentúry za predchádzajúci rok.

3. Výkonný riaditeľ zasiela všeobecnú správu agentúry po jej prijatí správnou radou Európskemu parlamentu, Rade, Komisii, Dvoru audítorov, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov a zabezpečuje jej uverejnenie.

Článok 14
Žiadosti adresované agentúre

1. Žiadosti o radu a pomoc v rozsahu pôsobnosti, cieľov a úloh agentúry sa adresujú výkonnému riaditeľovi a dopĺňajú sa všeobecnými informáciami vysvetľujúcimi záležitosť, ktorá sa má riešiť. Výkonný riaditeľ informuje správnu radu o prijatých žiadostiach a následne o spracovaní žiadostí. Ak agentúra odmietne žiadosť, musí poskytnúť odôvodnenie.

2. Žiadosti uvedené v odseku 1 môže predložiť:

a) Európsky parlament;

b) Rada;

c) Komisia;

d) akýkoľvek príslušný orgán menovaný členským štátom, ako je napríklad národný regulačný orgán, ako sa definuje v článku 2 smernice 2002/21/ES.

3. Praktické opatrenia pre uplatňovanie odsekov 1 a 2 týkajúce sa najmä predkladania žiadostí, určovania ich priority, spracovania a informovania správnej rady o žiadostiach predložených agentúre ustanovuje správna rada vo vnútorných pravidlách činnosti agentúry.

Článok 15
Vyhlásenie o záujmoch

1. Výkonný riaditeľ a úradníci dočasne vyslaní členskými štátmi podávajú písomné vyhlásenie o záväzkoch a písomné vyhlásenie, v ktorom sa uvádza, že nemajú žiadne priame alebo nepriame záujmy, ktoré by sa mohli považovať za záujmy poškodzujúce ich nezávislosť.

2. Externí experti zúčastňujúci sa v ad hoc pracovných skupinách oznamujú na každom zasadnutí akékoľvek záujmy, ktoré by sa mohli považovať za záujmy poškodzujúce ich nezávislosť v súvislosti s bodmi programu, a zdržiavajú sa účasti na diskusiách k týmto bodom.

Článok 16
Transparentnosť

1. Agentúra zabezpečí, aby vykonávala svoje činnosti s vysokým stupňom transparentnosti a v súlade s článkami 13 a 14.

2. Agentúra zabezpečí, aby verejnosť a všetky zainteresované strany dostávali v náležitých prípadoch objektívne, spoľahlivé a ľahko dostupné informácie, najmä o výsledkoch jej práce. Agentúra takisto zverejňuje vyhlásenia o záujmoch podávané výkonným riaditeľom a dočasne vyslanými úradníkmi z členských štátov spolu s vyhláseniami o záujmoch expertov v súvislosti s bodmi programu zasadnutí ad hoc pracovných skupín.

3. Správna rada, konajúc na návrh výkonného riaditeľa, môže zainteresovaným stranám povoliť sledovanie postupu niektorých činností agentúry.

4. Agentúra stanovuje vo svojich vnútorných pravidlách činnosti praktické opatrenia na vykonávanie pravidiel transparentnosti uvedených v odsekoch 1 a 2.

Článok 17
Dôvernosť

1. Bez toho, aby bol dotknutý článok 14, agentúra nemôže tretím stranám poskytovať informácie, ktoré spracúva alebo získava a pri ktorých sa vyžaduje dôverné zaobchádzanie.

2. Členovia správnej rady, výkonný riaditeľ, členovia stálej skupiny zainteresovaných strán, externí experti, účastníci ad hoc pracovných skupín, a zamestnanci agentúry vrátane úradníkov dočasne vyslaných členskými štátmi podliehajú aj po skončení ich povinností požiadavkám na dôvernosť podľa článku 339 zmluvy.

3. Agentúra ustanovuje vo svojich vnútorných pravidlách činnosti praktické opatrenia na vykonávanie pravidiel dôvernosti uvedených v odsekoch 1 a 2.

4. Správna rada sa môže rozhodnúť, že agentúre povolí pracovať s utajovanými informáciami. V takom prípade správna rada po dohode s príslušnými útvarmi Komisie prijíma vnútorné pravidlá činnosti, ktorými sa uplatňujú zásady bezpečnosti obsiahnuté v rozhodnutí Komisie 2001/844/ES, ESUO, Euratom z 29. novembra 2001, ktorým sa mení a dopĺňa jej rokovací

poriadok[32]. Okrem iného ide o ustanovenia týkajúce sa výmeny, spracovania a uchovávania utajovaných informácií.

Článok 18
Prístup k dokumentom

1. Na dokumenty agentúry sa vzťahuje nariadenie (ES) č. 1049/2001.

2. Správna rada prijme opatrenia na vykonanie nariadenia (ES) č. 1049/2001 do šiestich mesiacov od zriadenia agentúry.

3. Rozhodnutia prijaté agentúrou podľa článku 8 nariadenia (ES) č. 1049/2001 môžu byť predmetom sťažnosti ombudsmanovi alebo konania pred Súdnym dvorom Európskej únie podľa článkov 228 a 263 zmluvy.

ODDIEL 4 FINANČNÉ USTANOVENIA

Článok 19
Prijatie rozpočtu

1. Príjmy agentúry pozostávajú z príspevku Európskej únie, príspevkov z tretích krajín zúčastňujúcich sa na práci agentúry, ako sa ustanovuje v článku 29, a príspevkov členských štátov.

2. Medzi výdavky agentúry patria výdavky na zamestnancov, administratívnu a technickú podporu, infraštruktúru a prevádzku a výdavky vyplývajúce zo zmlúv uzatvorených s tretími stranami.

3. Výkonný riaditeľ najneskôr do 1. marca každý rok vypracuje návrh výkazu odhadov príjmov a výdavkov agentúry pre nasledujúci rozpočtový rok a pošle ho správnej rade spolu s návrhom organizačného členenia.

4. Príjmy a výdavky musia byť v rovnováhe.

5. Správna rada každý rok na základe návrhu výkazu odhadov príjmov a výdavkov vyhotoveného výkonným riaditeľom vytvára návrh výkazu odhadov príjmov a výdavkov agentúry na nasledujúci rozpočtový rok.

6. Tento výkaz odhadov, ktorý obsahuje návrh organizačného členenia spolu s návrhom pracovného programu, musí správna rada najneskôr do 31. marca poslať Komisii a štátom, s ktorými Európska únia uzatvorila dohody v súlade s článkom 24.

7. Komisia postupuje výkaz odhadov Európskemu parlamentu a Rade (obidva ďalej len „rozpočtový orgán“) spolu s návrhom všeobecného rozpočtu Európskej únie.

8. Komisia na základe tohto výkazu odhadov zaraďuje do predbežného všeobecného rozpočtu Európskej únie odhady, ktoré pokladá za potrebné na organizačné členenie, a výšku dotácie,

[32] Ú. v. ES L 317, 3.12.2001, s. 1.

ktorá bude uhradená zo všeobecného rozpočtu, ktorý odovzdáva rozpočtovému orgánu v súlade s článkom 314 zmluvy.

9. Rozpočtový orgán schvaľuje rozpočtové prostriedky na dotácie agentúre.

10. Rozpočtový orgán prijíma organizačné členenie agentúry.

11. Správna rada prijíma rozpočet agentúry spolu s pracovným programom. Rozpočet sa stáva konečným po konečnom prijatí všeobecného rozpočtu Európskej únie. Správna rada, kde je to vhodné, upravuje rozpočet a pracovný program agentúry v súlade so všeobecným rozpočtom Európskej únie. Správna rada ho bezodkladne zasiela Komisii a rozpočtovému orgánu.

Článok 20
Boj proti podvodom

1. V záujme boja proti podvodom, korupcii a ďalším protizákonným činnostiam sa ustanovenia nariadenia Európskeho parlamentu a Rady (ES) č. 1073/1999 z 25. mája 1999 týkajúce sa vyšetrovaní vykonávaných Európskym úradom pre boj proti podvodom (OLAF)[33] uplatňujú bez obmedzenia.

2. Agentúra pristúpi k Medziinštitucionálnej dohode z 25. mája 1999 medzi Európskym parlamentom a Radou Európskej únie a Komisiou Európskych spoločenstiev, ktorá sa týka vnútorných vyšetrovaní Európskym úradom proti podvodom (OLAF)[34], a bezodkladne vydá náležité ustanovenia uplatniteľné na všetkých zamestnancov agentúry.

Článok 21
Plnenie rozpočtu

1. Výkonný riaditeľ plní rozpočet agentúry.

2. Vnútorný audítor Komisie má rovnaké právomoci nad agentúrou ako nad oddeleniami Komisie.

3. Najneskôr do 1. marca po každom rozpočtovom roku zasiela účtovník agentúry účtovníkovi Komisie priebežné účtovné závierky spolu so správou o rozpočtovom a finančnom hospodárení za tento rozpočtový rok. Účtovník Komisie konsoliduje predbežné účtovné závierky inštitúcií a decentralizovaných orgánov v súlade s článkom 128 nariadenia Rady (ES, Euratom) č. 1605/2002 z 25. júna 2002 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Európskych spoločenstiev[35] (ďalej len „nariadenie o rozpočtových pravidlách“).

4. Najneskôr do 31. marca po ukončení každého rozpočtového roku zasiela účtovník Komisie predbežné účtovné závierky agentúry Dvoru audítorov spolu so správou o rozpočtovom a finančnom riadení za tento rozpočtový rok. Správu o rozpočtovom a finančnom riadení pre daný rozpočtový rok posiela aj rozpočtovému orgánu.

---

33 Ú. v. ES L 136, 31.5.1999, s. 1.
34 Ú. v. ES L 136, 31.5.1999, s. 15.
35 Ú. v. ES L 248, 16.9.2002, s. 1.

5. Výkonný riaditeľ po prijatí pripomienok Dvora audítorov k predbežným účtom agentúry podľa článku 129 všeobecného rozpočtového nariadenia vypracúva na vlastnú zodpovednosť konečné účty a posiela ich správnej rade, ktorá k nim zaujíma stanovisko.

6. Správna rada prijíma stanovisko ku konečným účtovným výkazom agentúry.

7. Výkonný riaditeľ najneskôr do 1. júla nasledujúceho po každom rozpočtovom roku doručí záverečné vyúčtovanie spolu so stanoviskom správnej rady Európskemu parlamentu, Rade, Komisii a Dvoru audítorov.

8. Výkonný riaditeľ uverejňuje záverečné účtovné výkazy.

9. Výkonný riaditeľ posiela Dvoru audítorov najneskôr do 30. septembra odpoveď na jeho pripomienky. Túto odpoveď posiela aj správnej rade.

10. Výkonný riaditeľ predkladá Európskemu parlamentu na požiadanie všetky informácie potrebné pre bezproblémové uplatnenie postupu vyrovnania pre daný finančný rok, ako sa ustanovuje v článku 146 ods. 3 všeobecného nariadenia o rozpočtových pravidlách.

11. Európsky parlament na odporúčanie Rady do 30. apríla roku N + 2 poskytuje výkonnému riaditeľovi vyrovnanie v súvislosti s plnením rozpočtu za rok N.

ODDIEL 5 VŠEOBECNÉ USTANOVENIA

Článok 22
Právny štatút

1. Agentúra je orgánom Únie. Má právnu subjektivitu.

2. V každom z členských štátov využíva agentúra najrozsiahlejšiu spôsobilosť na právne úkony, udeľovanú právnickým osobám podľa jeho zákonov. Môže najmä nadobúdať hnuteľný a nehnuteľný majetok alebo s ním nakladať, ako aj byť účastníkom súdnych konaní.

3. V mene agentúry koná jej výkonný riaditeľ.

Článok 23
Zamestnanci

1. Zamestnanci agentúry vrátane jej výkonného riaditeľa podliehajú pravidlám a nariadeniam uplatniteľným na úradníkov a ostatných zamestnancov Európskej únie.

2. Správna rada vo vzťahu k výkonnému riaditeľovi vykonáva právomoci zverené služobným poriadkom ustanovujúcemu orgánu a podmienkami zamestnávania orgánu poverenému uzatváraním zmlúv.

3. Výkonný riaditeľ vo vzťahu k zamestnancom agentúry vykonáva právomoci zverené služobným poriadkom ustanovujúcemu orgánu a podmienkami zamestnávania orgánu poverenému uzatváraním zmlúv.

4. Agentúra môže zamestnať dočasne preložených národných expertov z členských štátov. Agentúra ustanovuje vo svojich vnútorných pravidlách činnosti praktické opatrenia na umožnenie zamestnania takýchto expertov.

Článok 24
Výsady a imunity

Na agentúru a jej zamestnancov sa uplatňuje Protokol o výsadách a imunitách Európskych spoločenstiev.

Článok 25
Zodpovednosť

1. Zmluvná zodpovednosť agentúry sa riadi právom, ktorým sa spravuje príslušná zmluva.

Súdny dvor Európskej únie má súdnu právomoc vydávať rozsudky podľa akejkoľvek arbitrážnej doložky uvedenej v zmluve, ktorú uzavrela agentúra.

2. V prípade nezmluvnej zodpovednosti agentúra napravuje v súlade so všeobecnými princípmi spoločnými pre práva členských štátov všetky škody, ktoré spôsobila agentúra alebo jej zamestnanci pri vykonávaní svojich povinností.

Vo všetkých sporoch súvisiacich s náhradou takejto škody má právomoc rozhodovať Súdny dvor.

3. Právna subjektivita jej zamestnancov voči agentúre sa riadi príslušnými podmienkami uplatniteľnými na zamestnancov agentúry.

Článok 26
Jazyky

1. Na agentúru sa vzťahujú ustanovenia uvedené v nariadení č. 1 z 15. apríla 1958 o používaní jazykov v Európskom hospodárskom spoločenstve[36]. Členské štáty a ostatné nimi menované orgány sa môžu obrátiť na agentúru a dostať odpoveď v jazyku Európskej únie podľa ich výberu.

2. Prekladateľské služby potrebné na chod agentúry zabezpečuje Prekladateľské stredisko pre orgány Európskej únie.

Článok 27
Ochrana osobných údajov

Pri spracovaní údajov týkajúcich sa jednotlivcov podlieha agentúra ustanoveniam nariadenia (ES) č. 45/2001.

---

[36] Ú. v. ES 17, 6.10.1958, s. 385/58. Nariadenie naposledy zmenené a doplnené Aktom o pristúpení z roku 1994.

Článok 28
Účasť tretích krajín

1. Agentúra je otvorená účasti tretích krajín, ktoré uzatvorili dohody s Európskou úniou, na základe ktorých prijali a uplatňujú právne predpisy Únie v oblasti, na ktorú sa vzťahuje toto nariadenie.

2. Podľa príslušných ustanovení týchto dohôd sa prijímajú opatrenia, na základe ktorých sa vymedzuje predovšetkým povaha, rozsah a spôsob, akým sa tieto krajiny majú podieľať na práci agentúry, vrátane ustanovení týkajúcich sa účasti na iniciatívach uskutočňovaných agentúrou, finančných príspevkov a zamestnancov.

ODDIEL 6 ZÁVEREČNÉ USTANOVENIA

Článok 29
Doložka o revízii

1. Komisia do troch rokov od dátumu zriadenia uvedeného v článku 34 vykoná hodnotenie na základe referenčného rámca dohodnutého so správnou radou, pričom zohľadní názory všetkých príslušných zainteresovaných strán. Pri hodnotení sa posúdi vplyv a účinnosť agentúry pri dosahovaní cieľov uvedených v článku 2 a účinnosť pracovných postupov agentúry. Komisia vykoná hodnotenie najmä s cieľom určiť, či je agentúra stále účinným nástrojom a či by sa doba trvania agentúry nemala ďalej predĺžiť za obdobie uvedené v článku 34.

2. Zistenia z hodnotenia predloží Komisia Európskemu parlamentu a Rada a uverejnia sa.

3. Správna rada dostane hodnotenie a vydá Komisii odporúčania týkajúce sa zmien tohto nariadenia, agentúry a jej pracovných postupov. Správna rada a výkonný riaditeľ zohľadnia výsledky hodnotenia pri viacročnom plánovaní agentúry.

Článok 30
Spolupráca s hostiteľským členským štátom

Členský štát, ktorý je hostiteľským štátom agentúry, zabezpečuje čo najlepšie podmienky pre bezproblémové a účinné fungovanie agentúry.

Článok 31
Správna kontrola

Činnosti agentúry podliehajú dohľadu verejného ochrancu práv v súlade s ustanoveniami článku 228 zmluvy.

Článok 32
Zrušenie a nástupníctvo

1. Nariadenie (ES) č. 460/2004 sa zrušuje.

Odkazy na nariadenie (ES) č. 460/2004 a na agentúru ENISA sa považujú za odkazy na toto nariadenie a agentúru.

2. Agentúra je nástupcom agentúry, ktorá bola zriadená na základe nariadenia (ES) č. 460/2004, pokiaľ ide o vlastníctvo, dohody, právne záväzky, pracovné zmluvy, finančné záväzky a povinnosti.

Článok 33
Trvanie

Agentúra sa zriaďuje od […] na obdobie piatich rokov.

Článok 34
Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* a uplatňuje sa od 14. marca 2012 alebo odo dňa nasledujúceho po jeho uverejnení podľa toho, čo nastane skôr.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V […]

Za Európsky parlament	*Za Radu*
predseda	*predseda*

LEGISLATÍVNY FINANČNÝ VÝKAZ PRE NÁVRHY

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Návrh nariadenia Európskeho parlamentu a Rady o Európskej agentúre pre bezpečnosť sietí a informácií (ENISA)

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

Informačná spoločnosť a médiá.

Regulačný rámec pre Digitálnu agendu

1.3. Charakter návrhu/iniciatívy

☐ Návrh/iniciatíva sa týka **nového opatrenia**

☐ Návrh/iniciatíva sa týka **nového opatrenia na základe pilotného projektu/prípravného opatrenia**[38]

☑ Návrh/iniciatíva sa týka **predĺženia existujúceho opatrenia**

☐ Návrh/iniciatíva sa týka **opatrenia presmerovaného na nové opatrenie**

1.4. Ciele

1.4.1. Viacročné strategické ciele Komisie, na ktoré sa zameriava návrh/iniciatíva

Jednotnosť regulačných prístupov – poskytovať usmernenia a poradenstvo Komisii a členským štátom pri aktualizácii a vytváraní holistického normatívneho rámca v oblasti bezpečnosti sietí a informácií.

Predchádzanie, odhalenie a reakcia – zlepšovať pripravenosť prispením k schopnosti európskeho včasného varovania a reakcie na incidenty prostredníctvom celoeurópskych plánov pre mimoriadne prípady a cvičení.

Zlepšenie poznatkov politikov – zabezpečovať pomoc a poskytovať poradenstvo Komisii a členským štátom s cieľom dosiahnuť vysokú úroveň vedomostí v celej Únii o otázkach spojených s bezpečnosťou sietí a informácií a ich uplatňovania na zainteresované strany z odvetvia. To zahŕňa aj tvorbu, analýzu a sprístupňovanie údajov týkajúcich sa ekonomiky a vplyvu porušení bezpečnosti sietí a informácií, motivujúce faktory pre zainteresované strany, aby investovali do opatrení v oblasti bezpečnosti sietí a informácií, identifikáciu rizík, ukazovatele stavu bezpečnosti sietí a informácií v Únii atď.

---

[37] ABM: riadenie založené na činnosti – ABB: rozpočtovanie založené na činnosti.

[38] Ako sa uvádza v článku 49 ods. 6 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

Oprávnenie zainteresovaných strán – rozvíjať kultúru bezpečnosti a riadenia rizika podporou spoločného využívania informácií a širšej spolupráce subjektov z verejného a súkromného sektora aj v priamy prospech občanov a rozvíjaním kultúry informovanosti o bezpečnosti sietí a informácií.

Ochrana Európy pred medzinárodnými hrozbami – dosiahnuť vysokú úroveň spolupráce s tretími krajinami a s medzinárodnými organizáciami s cieľom presadzovať spoločný globálny prístup k bezpečnosti sietí a informácií a podporiť medzinárodné iniciatívy na vysokej úrovni v Európe.

Smerovanie k spoločnej implementácii – uľahčovať spoluprácu pri vykonávaní politík v oblasti bezpečnosti sietí a informácií.

Boj proti počítačovej kriminalite – začleniť aspekty boja proti počítačovej kriminalite, týkajúce sa bezpečnosti sietí a informácií, do rozhovorov a výmeny správnej praxe medzi verejnými a súkromnými zainteresovanými stranami, najmä prostredníctvom spolupráce s orgánmi (bývalého) 2. a 3. piliera, napr. s Europolom.

1.4.2. Príslušné špecifické ciele a činnosti ABM/ABB

Špecifický cieľ č.

Zvýšiť bezpečnosť sietí a informácií (BSI), rozvinúť kultúru bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektora a vymedziť politické výzvy, ktoré vyvolávajú budúce siete a internet.

Príslušné činnosti ABM/ABB

Politika elektronických komunikácií a bezpečnosť sietí

1.4.3. Očakávané výsledky a vplyv

Očakáva sa, že iniciatíva prinesie tento hospodársky vplyv:

– vyššia dostupnosť informácií o súčasných a budúcich výzvach a rizikách v prípade bezpečnosti a odolnosti,

– neduplikovanie úsilia pri zbere príslušných informácií o rizikách, hrozbách a nedostatkoch každým jednotlivým členským štátom,

– vyššia úroveň informovanosti politikov pri rozhodovaní,

– vyššia kvalita politických ustanovení týkajúcich sa bezpečnosti sietí a informácií v členských štátoch v dôsledku rozširovania najlepších postupov,

– úspory z rozsahu v reakcii na incidenty na úrovni EÚ,

– viac investícií vyvolaných spoločnými politickými cieľmi a normami pre bezpečnosť a odolnosť na úrovni EÚ,

– nižšie operačné riziká pre podniky v dôsledku vyššej úrovne bezpečnosti a odolnosti,

– jednotnejšie opatrenia na boj proti počítačovej kriminalite.

Očakáva sa, že iniciatíva prinesie tento sociálny vplyv:

– vyššia dôvera užívateľov služieb a systémov informačnej spoločnosti,

– vyššia dôvera vo fungovanie vnútorného trhu EÚ dosiahnutím vyššej úrovne ochrany spotrebiteľov,

– výmena informácií a poznatkov s nečlenskými krajinami EÚ vo väčšom rozsahu,

– lepšia ochrana základných ľudských práv EÚ zabezpečením rovnakej úrovne ochrany osobných údajov a súkromia občanov EÚ.

Očakávaný environmentálny vplyv je minimálny:

– nižší vplyv emisií CO2 v dôsledku napr. obmedzenejšieho cestovania spojeného s vyššou dôverou k používaniu systémov a služieb IKT a nižšej spotreby energie spojenej s úsporami z rozsahu pri vykonávaní bezpečnostných povinností.

1.4.4. Ukazovatele výsledkov a vplyvu

Ukazovatele monitorovania podľa cieľov sú:

Jednotnosť regulačných prístupov:

– počet členských štátov, ktoré používajú odporúčania agentúry pri svojom procese tvorby politiky,

– počet štúdií zameraných na identifikáciu medzier a nezrovnalostí v oblasti normalizácie v súvislosti s bezpečnosťou sietí a informácií,

– menšie odlišnosti v prístupoch členských štátov k bezpečnosti sietí a informácií.

Predchádzanie, odhalenie a reakcia:

– počet zorganizovaných školení týkajúcich sa bezpečnosti sietí,

– dostupnosť fungujúceho systému včasného varovania v prípade vznikajúcich rizík a útokov,

– počet cvičení v oblasti bezpečnosti sietí a informácií na úrovni EÚ koordinovaných agentúrou.

Zlepšenie poznatkov tvorcov politiky:

– počet štúdií s cieľom zhromaždiť informácie o existujúcich a očakávaných rizikách v oblasti bezpečnosti sietí a informácií a o technológiách na zabráneniu vzniku rizík,

– počet konzultácií s verejnými orgánmi pracujúcimi s bezpečnosťou sietí a informácií,

– dostupnosť európskeho rámca pre organizáciu zberu údajov o bezpečnosti sietí a informácií.

Oprávnenie zainteresovaných strán:

– počet identifikovaných správnych praxí pre odvetvie,

– výška investícií do bezpečnostných opatrení súkromných zainteresovaných strán.

Ochrana Európy pred medzinárodnými hrozbami:

– počet konferencií/stretnutí členských štátov EÚ s cieľom vymedziť spoločne odsúhlasené ciele pre bezpečnosť sietí a informácií,

– počet stretnutí európskych a medzinárodných expertov v oblasti bezpečnosti sietí a informácií.

Smerom k spoločnej implementácii:

– počet hodnotení dodržiavania predpisov,

– počet postupov v oblasti bezpečnosti sietí a informácií pre celú EÚ.

Boj proti počítačovej kriminalite:

– pravidelnosť vzájomných opatrení s agentúrami bývalého 2. a 3. piliera,

– počet prípadov, keď bola poskytnutá expertíza pri trestných vyšetrovaniach.

1.5. Dôvody návrhu/iniciatívy

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

Agentúra ENISA bola pôvodne zriadená v roku 2004 s cieľom zaoberať sa hrozbami a možnými následnými narušeniami bezpečnosti sietí a informácií. Odvtedy sa problémy súvisiace s bezpečnosťou sietí a informácií rozvinuli spolu s rozvojom technológií a trhov a boli predmetom ďalších úvah a rozhovorov, ktoré v súčasnosti umožnili aktualizáciu a podrobnejší opis zistených presných problémov a toho, ako sú ovplyvnené meniacim sa prostredím v oblasti bezpečnosti sietí a informácií.

1.5.2. Pridaná hodnota v prípade zapojenia EÚ

Problémy bezpečnosti sietí a informácií nerešpektujú národné hranice, a preto sa nemôžu účinne riešiť len na národnej úrovni. Zároveň existuje veľká rôznorodosť pri riešení problémov verejnými orgánmi v rôznych členských štátoch. Tieto rozdiely môžu predstavovať veľkú prekážku pri zavádzaní vhodných mechanizmov v celej Únii s cieľom podporiť bezpečnosť sietí a informácií v Európe. Vzhľadom na vzájomne prepojený charakter infraštruktúr IKT je účinnosť opatrení prijatých na vnútroštátnej úrovni v jednom členskom štáte ešte vždy výrazne ovplyvnená nižšou úrovňou opatrení v iných členských štátoch

a nedostatočnou systematickou cezhraničnou spoluprácou. Nedostatočné opatrenia v oblasti bezpečnosti sietí a informácií vedúce k incidentu v jednom členskom štáte môže spôsobiť poruchy služieb v ostatných členských štátoch.

Množenie bezpečnostných požiadaviek okrem toho znamená nákladovú záťaž pre podniky, ktoré pôsobia na úrovni Európskej únie, a vedie k roztrieštenosti a nedostatku konkurencieschopnosti na európskom vnútornom trhu.

Zatiaľ čo sa závislosť sietí a informačných systémov zvyšuje, pripravenosť riešiť incidenty sa javí ako nedostatočná.

Súčasné systémy vnútroštátneho včasného varovania a reakcie na incidenty majú významné nedostatky. Procesy a postupy monitorovania a predkladania správ o incidentoch týkajúcich sa bezpečnosti sietí sa v členských štátoch výrazne líšia. V niektorých krajinách nie sú procesy formalizované, zatiaľ čo v iných krajinách neexistuje príslušný orgán pre prijímanie a spracovanie správ o incidentoch. Európske systémy neexistujú. V dôsledku toho by sa zabezpečenie základných potrieb mohlo podstatne narušiť incidentmi v oblasti bezpečnosti sietí a informácií a mali by sa pripraviť primerané reakcie. V oznámení Komisie o CIIP sa takisto zdôraznila potreba schopnosti včasného varovania a reakcie na incidenty, podľa možnosti podporenej prostredníctvom cvičení európskeho rozsahu.

Zjavne sú potrebné politické nástroje zamerané na proaktívnu identifikáciu rizík a nedostatkov v oblasti bezpečnosti sietí a informácií, na navrhnutie vhodných reakčných mechanizmov (napr. prostredníctvom vymedzenia a rozšírenia osvedčených postupov) a na zabezpečenie, aby zainteresované strany tieto reakčné mechanizmy poznali a uplatňovali.

1.5.3. Ponaučenia získané z podobných skúseností v minulosti

Pozri body 1.5.1 a 1.5.2.

1.5.4. Súlad a možná synergia s ostatnými príslušnými nástrojmi

Táto iniciatíva je úplne v súlade so všeobecnými rozhovormi o bezpečnosti sietí a informácií a s inými politickými iniciatívami, ktoré sa zameriavajú na budúcnosť bezpečnosti sietí a informácií. Je jednou zo základných zložiek Digitálnej agendy pre Európu, ktorá je hlavnou iniciatívou stratégie Európa 2020.

1.6. Trvanie a finančný vplyv

☑ Návrh/iniciatíva s **obmedzeným trvaním**

– ☑ Začiatok 5-ročného predĺženia bude 14. 3. 2012 alebo v deň nadobudnutia účinnosti nového nariadenia podľa toho, čo bude neskôr

– ☑ Finančný vplyv do roku 2012 do roku 2017

☐ Návrh/iniciatíva s **neobmedzeným trvaním**

– - Realizácia s začiatočným obdobím od RRRR do RRRR,

– po ktorom nasleduje činnosť v plnom rozsahu.

1.7. Plánované metódy riadenia[39]

☐ **Centrálne priame riadenie** na úrovni Komisie

☑ **Centrálne nepriame riadenie** s delegovaním vykonania úloh na:

– ☐ výkonné agentúry

– ☑ subjekty zriadené Spoločenstvami[40]

– ☐ národné verejné subjekty/subjekty poverené poskytovaním služieb vo verejnom záujme

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

☐ **Zdieľané riadenie** s členskými štátmi

☐ **Decentralizované riadenie** s tretími krajinami

☐ **Spoločné riadenie** s medzinárodnými organizáciami ***(spresnite)***

---

[39] Podrobné informácie o spôsoboch riadenia a odkazy na nariadenie o rozpočtových pravidlách sú dostupné na stránke BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Ako sa uvádza v článku 185 nariadenia o rozpočtových pravidlách.

2. RIADIACE OPATRENIA

2.1. Pravidlá monitorovania a predkladania správ

Výkonný riaditeľ je zodpovedný za účinné monitorovanie a hodnotenie činnosti agentúry z pohľadu jej cieľov a ročne podáva správu správnej rade.

Výkonný riaditeľ zostavuje celkovú správu zahŕňajúcu všetky činnosti agentúry v predchádzajúcom roku, ktorá najmä porovnáva dosiahnuté výsledky s cieľmi ročného programu činností. Táto správa sa po prijatí správnou radou posiela Európskemu parlamentu, Rade, Komisii, Dvoru audítorov, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov a uverejňuje sa.

2.2. Systém riadenia a kontroly

2.2.1. Zistené riziká

Od založenia v roku 2004 bola agentúra ENISA predmetom externých a interných hodnotení.

V súlade s článkom 25 nariadenia o agentúre ENISA bolo prvým krokom v tomto procese nezávislé hodnotenie agentúry ENISA skupinou externých expertov v rokoch 2006 – 2007. Na základe správy skupiny externých expertov[41] sa potvrdilo, že pôvodné politické dôvody na zriadenie agentúry ENISA a jej pôvodné ciele sú stále platné, a agentúra bola takisto užitočná na otvorenie niektorých otázok, ktorými sa treba zaoberať.

Komisia predložila v marci 2007 správu o hodnotení správnej rade, ktorá potom vypracovala vlastné odporúčania o budúcnosti agentúry a o zmenách nariadenia o agentúre ENISA[42].

V júni 2007 predložila Komisia vlastné hodnotenie výsledkov externého hodnotenia a odporúčaní správnej rady v oznámení Európskemu parlamentu a Rade[43]. V oznámení sa uvádza, že je potrebné sa rozhodnúť, či sa má mandát agentúry predĺžiť alebo sa agentúra nahradí iným mechanizmom, ako napríklad stálym fórom zainteresovaných strán alebo sieťou bezpečnostných organizácií. Oznámením sa začali aj verejné konzultácie k tejto záležitosti, pričom sa požiadalo o príspevok zainteresovaných strán v Európe so zoznamom otázok, ktoré usmernia ďalšie diskusie[44].

2.2.2. Plánované spôsoby kontroly

Pozri bod 2.1 a bod 2.2.1.

---

41 http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

42 Ako je ustanovené v článku 25 nariadenia o agentúre ENISA. Úplný text dokumentu schváleného správnou radou agentúry ENISA, ktorý tiež obsahuje poznámky správnej rady, je dostupný na tejto webovej stránke: http://enisa.europa.eu/pages/03_02.htm.

43 Oznámenie Komisie Európskemu parlamentu a Rade o hodnotení Európskej agentúry pre bezpečnosť sietí a informácií (ENISA), KOM(2007) 285 v konečnom znení z 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT.

44 http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Platby za všetky požadované služby alebo štúdie kontrolujú zamestnanci agentúry pred zaplatením, berúc do úvahy všetky zmluvné náležitosti, hospodárske zásady a osvedčené finančné alebo riadiace postupy. Opatrenia proti podvodom (kontrola, požiadavky na hlásenie a pod.) sa zahrnú do všetkých dohôd a zmlúv uzavretých medzi agentúrou a príjemcami všetkých platieb.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVHRU/INICIATÍVY

3.1. Príslušné kapitoly viacročného finančného rámca a dotknuté výdavkové položky rozpočtu

- Existujúce výdavkové rozpočtové položky

Kapitola viacročného finančného rámca	Rozpočtová položka	Druh výdavkov	Príspevok			
	Číslo/opis	Dif./Nedif. (45)	krajín EZVO[46]	kandidátskych krajín[47]	tretích krajín	v zmysle článku 18 ods. 1 písm. aa) nariadenia o rozpočtových pravidlách
1.a Konkurencieschopnosť pre rast a zamestnanosť	09 02 03 01 Európska agentúra pre bezpečnosť sietí a informácií – dotácie v rámci kapitol 1 a 2	Dif.	ÁNO	NIE	NIE	NIE
	09 02 03 02 Európska agentúra pre bezpečnosť sietí a informácií – dotácie v rámci kapitoly 3	Dif.	ÁNO	NIE	NIE	NIE
5 Administratívne výdavky	09 01 01 Výdavky vzťahujúce sa na zamestnancov v aktívnom služobnom pomere v oblasti politiky	Nedif.	NIE	NIE	NIE	NIE
	09 01 02 11 Ostatné výdavky na riadenie	Nedif.	NIE	NIE	NIE	NIE

* Odhadovaný finančný vplyv návrhu na obdobie presahujúce súčasné programovacie obdobie rokov 2007 – 2013 tento legislatívny finančný výkaz nepokrýva. Na základe návrhu nariadenia predloženého Komisiou, ktorým sa stanovuje viacročný finančný rámec na obdobie po roku 2013, a s prihliadnutím na závery posúdenia vplyvu, Komisia predloží zmenený a doplnený legislatívny finančný výkaz.

45 Dif. = Diferencované rozpočtové prostriedky/Nedif. = Nediferencované rozpočtové prostriedky.

46 EZVO: Európske združenie voľného obchodu.

47 Kandidátske krajiny a prípadne potenciálne kandidátske krajiny zo západného Balkánu.

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Položka viacročného finančného rámca:	1.a	Konkurencieschopnosť pre rast a zamestnanosť

ENISA			1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017	**14. mar. 2012 – 13. mar. 2017 SPOLU**
Prevádzkové rozpočtové prostriedky										
09 02 03 02 Európska agentúra pre bezpečnosť sietí a informácií – dotácie v rámci kapitoly 3	Záväzky	(1)	0,454	1,976	2,470	--	--	--	--	--
	Platby	(2)	0,454	1,976	2,470	--	--	--	--	--
Administratívne rozpočtové prostriedky										
09 02 03 01 Európska agentúra pre bezpečnosť sietí a informácií – dotácie v rámci kapitol 1 a 2		(3)	1,293	4,697	6,120	--	--	--	--	--
Rozpočtové prostriedky v rámci KAPITOLY 1a SPOLU	Záväzky	=1 +3	1,747	6,673	8,590	--	--	--	--	--
	Platby	=2+3	1,747	6,673	8,590	--	--	--	--	--

Prevádzkové rozpočtové prostriedky SPOLU	Záväzky	(4)	0,454	1,976	2,470	--	--	--	--	--
	Platby	(5)	0,454	1,976	2,470	--	--	--	--	--
Rozpočtové prostriedky administratívneho charakteru financované z obálky špecifických programov SPOLU		(6)	1,293	4,697	6,120	--	--	--	--	--
Rozpočtové prostriedky v rámci KAPITOLY 1.a viacročného rámcového programu **SPOLU**	Záväzky	=4+6	1,747	6,673	8,590	--	--	--	--	--
	Platby	=5+6	1,747	6,673	8,590	--	--	--	--	--

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Položka viacročného finančného rámca:	5	Administratívne výdavky

		1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017	Spolu
Ľudské zdroje		0,085	0,342	0,427	--	--	--	--	--
Ostatné administratívne výdavky		0,002	0,013	0,015	--	--	--	--	--
GR INFSO SPOLU	Rozpočtové prostriedky	0,087	0,355	0,442	--	--	--	--	--

Rozpočtové prostriedky v rámci KAPITOLY 5 viacročného rámcového programu **SPOLU**	(Celkové záväzky = celkové platby)	0,087	0,355	0,442	--	--	--	--	--

		1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017	Spolu
Rozpočtové prostriedky v rámci KAPITOL 1 až 5 viacročného rámcového programu **SPOLU**	Záväzky	1,834	7,028	9,032	--	--	--	--	--
	Platby	1,834	7,028	9,032	--	--	--	--	--

3.2.2. Odhadovaný vplyv na prevádzkové rozpočtové prostriedky

– ☐ Návrh/iniciatíva si nevyžaduje využitie prevádzkových rozpočtových prostriedkov

– ☑ Návrh/iniciatíva si vyžaduje využitie prevádzkových rozpočtových prostriedkov, ako sa objasňuje ďalej:

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

Uveďte ciele a výstupy ⇩	1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017	**14. mar. 2012 – 13. mar. 2017 SPOLU**
Jednotnosť regulačných prístupov	0,114	0,494	0,620	--	--	--	--	--
Predchádzanie, odhalenie a reakcia	0,114	0,494	0,620	--	--	--	--	--
Zlepšenie poznatkov politikov	0,068	0,297	0,370	--	--	--	--	--
Oprávnenie zainteresovaných strán	0,050	0,218	0,270	--	--	--	--	--
Ochrana Európy pred medzinárodnými hrozbami	0,023	0,099	0,120	--	--	--	--	--
Smerom k spoločnej implementácii	0,064	0,276	0,340	--	--	--	--	--
Boj proti počítačovej kriminalite	0,023	0,098	0,120	--	--	--	--	--
NÁKLADY SPOLU	0,454	1,976	2,460	--	--	--	--	--

3.2.3. Odhadovaný vplyv na rozpočtové prostriedky administratívneho charakteru[48]

3.2.3.1. Zhrnutie

– ☐ Návrh/iniciatíva si nevyžaduje využitie administratívnych rozpočtových prostriedkov

– ☑ Návrh/iniciatíva si vyžaduje využitie administratívnych rozpočtových prostriedkov, ako sa objasňuje ďalej:

a) Administratívne výdavky v rámci kapitoly 5 viacročného finančného rámca

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

KAPITOLA 5 viacročného finančného rámca	1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017	**14. mar. 2012 – 13. mar. 2017 spolu**
Ľudské zdroje	0,085	0,342	0,427	--	--	--	--	--
Ostatné administratívne výdavky	0,002	0,013	0,015	--	--	--	--	--
SPOLU	0,087	0,355	0,442	--	--	--	--	--

b) Administratívne výdavky súvisiace s ENISA – pokryté z rozpočtovej položky „09.020301 Bezpečnosť európskych sietí a informácií: Kapitola 1 – Zamestnanci a Kapitola 2 – Fungovanie agentúry.“

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017	**14. mar. 2012 – 13. mar. 2017 spolu**
Ľudské zdroje – kapitola 1 – Zamestnanci	1,153	4,329	5,607	--	--	--	--	--
Ostatné výdavky administratívneho charakteru – kapitola 2 – Fungovanie agentúry	0,140	0,368	0,513	--	--	--	--	--

[48] Príloha k legislatívnemu finančnému výkazu nie je vyplnená, pretože sa neuplatňuje na tento návrh.

SPOLU	**1,293**	**4,697**	**6,120**	--	--	--	--	--

3.2.3.2. Odhadované požiadavky na ľudské zdroje

Organizačné členenie agentúry sa každý rok vysvetlí a odôvodní v dokumente nazvanom Plán v oblasti zamestnaneckej politiky, ktorý sa predloží rozpočtovému orgánu.

– ☐ Návrh/iniciatíva si nevyžaduje využitie ľudských zdrojov.

– ☑ Návrh/iniciatíva si vyžaduje využitie ľudských zdrojov, ako sa objasňuje ďalej:

a) Ľudské zdroje v rámci Komisie

	1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017
Pracovné miesta podľa organizačného členenia (úradníci a dočasní zamestnanci)							
XX 01 01 01 (Ústredie a reprezentačné kancelárie Komisie)	3,5	3,5	3,5	--	--	--	--
SPOLU	**3,5**	**3,5**	**3,5**	--	--	--	--

b) Ľudské zdroje ENISA

		1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017
Organizačné členenie ENISA (ekvivalent plného pracovného času – FTE)								
Úradníci alebo dočasní zamestnanci	AD	29	31	31	--	--	--	--
	AST	15	16	16	--	--	--	--
Úradníci alebo dočasní zamestnanci SPOLU		44	47	47	--	--	--	--
Iní zamestnanci (v FTE)								
Zmluvní zamestnanci		13	14	14	--	--	--	--
Vyslaní národní experti (SNE)		5	5	5	--	--	--	--
Iní zamestnanci SPOLU		18	19	19	--	--	--	--
SPOLU		**62**	**66**	**66**	--	--	--	--

Opis úloh, ktoré majú vykonávať zamestnanci agentúry:

Úradníci a dočasní zamestnanci	Agentúra bude naďalej: – - vykonávať poradnú a koordinačnú funkciu, v rámci ktorej **zbiera a analyzuje údaje** o bezpečnosti informácií. V súčasnosti verejné i súkromné organizácie s rôznymi cieľmi zbierajú údaje o IT incidentoch a iné údaje s významom pre bezpečnosť informácií. Na európskej úrovni však neexistuje centrálna organizácia, ktorá by komplexne zbierala a analyzovala údaje a poskytovala stanoviská a rady na podporu politiky Únie v oblasti bezpečnosti sietí a informácií, – - **slúžiť** ako **odborné centrum**, na ktoré sa členské štáty a inštitúcie Spoločenstva môžu obrátiť, ak chcú získať **stanoviská a rady k technickým záležitostiam** týkajúcim sa bezpečnosti, – - prispievať k **širokej spolupráci medzi rôznymi činiteľmi** na poli bezpečnosti informácií, napr. pomocou pri následných činnostiach pri podpore bezpečného elektronického podnikania (secure e-business). Takáto spolupráca bude základným predpokladom pre bezpečné fungovanie sietí a informačných systémov v Európe. Je potrebná účasť a angažovanosť všetkých zainteresovaných strán, – - prispievať ku koordinovanému prístupu k bezpečnosti informácií poskytovaním podpory **členským štátom**, napr. **podporou hodnotenia rizika** a aktivitami zvyšujúcimi informovanosť, – - zabezpečovať **interoperabilitu sietí a informačných systémov**, keď členské štáty **uplatňujú** technické požiadavky, ktoré sa týkajú bezpečnosti, – - určovať **príslušné štandardizačné** požiadavky a hodnotiť existujúce bezpečnostné normy a certifikačné schémy a presadzovať ich čo najširšie využívanie pri podpore európskej legislatívy, – - podporovať **medzinárodnú spoluprácu** na tomto poli, ktorá je stále potrebnejšia, keďže otázky bezpečnosti sietí a informácií sú globálne.
Externí zamestnanci	Pozri vyššie

3.2.4. Zlučiteľnosť so súčasným viacročným finančným rámcom

– ☑ Návrh/iniciatíva je zlučiteľný so súčasným viacročným finančným rámcom.

– ☐ Návrh/iniciatíva si vyžaduje zmenu v plánovaní príslušnej výdavkovej kapitoly vo viacročnom finančnom rámci.

– ☐ Návrh/iniciatíva si vyžaduje uplatnenie nástroja flexibility alebo revíziu viacročného finančného rámca[49].

Financovanie zo zdrojov EÚ po roku 2013 sa preskúma v kontexte debaty o všetkých návrhoch v rámci celej Komisie na obdobie po roku 2013. To znamená, že keď Komisia predloží návrh budúceho viacročného finančného rámca, predloží zároveň aj zmenený a doplnený legislatívny finančný výkaz zohľadňujúci závery posúdenia vplyvu.

3.2.5. Príspevky tretích strán

– ☐ Návrh/iniciatíva si nevyžaduje spolufinancovanie tretími stranami

– ☑ Návrh/iniciatíva si vyžaduje spolufinancovanie, ktoré sa odhaduje takto:

Indikatívne rozpočtové prostriedky v miliónoch EUR (zaokrúhlené na 3 desatinné miesta)

	1. jan. – 13 mar. 2012	14. mar. – 31. dec. 2012	2013	2014	2015	2016	1. jan. – 13 mar. 2017	**14. mar. 2012 – 13. mar. 2017 spolu**
EZVO	0,042	0,160	0,206	--	--	--	--	--

3.3. Odhadovaný vplyv na príjmy

– ☑ Návrh/iniciatíva nemá finančný vplyv na príjmy.

– ☐ Návrh/iniciatíva má finančný vplyv s týmto účinkom:

– ☐ na vlastné zdroje

– ☐ na zmiešané príjmy

[49] Pozri body 19 a 24 medziinštitucionálnej dohody.