EURÓPSKA KOMISIA

V Bruseli,30.9.2010
SEK(2010) 1127

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE POSÚDENIA VPLYVU

Sprievodný dokument

k návrhu

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o Európskej agentúre pre bezpečnosť sietí a informácií (ENISA)

{KOM(2010) 521 v konečnom znení}
{SEK(2010) 1126}

ZHRNUTIE POSÚDENIA VPLYVU

1. ROZSAH A SÚVISLOSTI

1.1. Rozsah

Toto posúdenie vplyvu je zamerané na to, ako by sa modernizovaná agentúra pre bezpečnosť sietí a informácií (NIS), ktorá je široko uznávaná ako vhodný a potrebný nástroj politiky, pomocou ktorého sa možno vysporiadať s problémami NIS, mala čo najlepšie utvárať tak, aby podporovala orgány členských štátov a Komisiu pri dosahovaní cieľov politiky v oblasti NIS, keď v marci 2012 vyprší mandát Európskej agentúry pre bezpečnosť sietí a informácií (ENISA).

1.2. Súvislosti

V dnešnom svete sa spoločnosť a hospodárstvo v rozhodujúcej miere opierajú o riadne fungovanie informačných a komunikačných technológií (IKT). Preto je nanajvýš dôležité zabezpečiť, aby tieto systémy boli stabilné a aby im používatelia dôverovali. Nárast počtu hrozieb, útokov a škodlivých aplikácií (malware) namierených proti systémom by mohol ohroziť riadne fungovanie základných sietí a informačných infraštruktúr. Vzhľadom na to, že tieto systémy a siete sú nadnárodné, je potrebná európska odpoveď na výzvu, ktorej musí čeliť bezpečnosť sietí a informácií (NIS).

Na vyriešenie týchto problémov bola v marci 2004 zriadená Európska agentúra pre bezpečnosť sietí a informácií (ENISA)[1] na obdobie piatich rokov, ktorej cieľom je *„zabezpečenie vysokej a účinnej úrovne bezpečnosti sietí a informácií v rámci Spoločenstva (...) 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“*.

Odvtedy sa výzvy, ktorým musí čeliť bezpečnosť sietí a informácií, neustále menia v súlade s rozvojom technológií a trhu. Preto už dávno pred vypršaním platnosti nariadenia ENISA v marci 2009 Komisia začala proces zisťovania u príslušných zainteresovaných strán, aké návrhy politík by najlepšie poslúžili cieľom EÚ v oblasti bezpečnosti sietí a informácií v období po roku 2009. Po priebežnom hodnotení agentúry ENISA v roku 2007[2] a verejnej konzultácii[3] 24. septembra 2008 Rada a Európsky parlament prijali nariadenie, ktorým sa predĺžil mandát agentúry ENISA v dovtedajšej podobe o tri roky do 13. marca 2012[4]. V odôvodneniach tohto nariadenia Rada a Európsky parlament vyzvali na ***„ďalšie úvahy o všeobecnom smerovaní európskeho úsilia zameraného na zvýšenie bezpečnosti sietí a informácií“***.

---

1 Nariadenie (ES) č. 460/2004 Európskeho parlamentu a Rady z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií.

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

3 Konzultácia prebiehala od 13. júna do 7. septembra 2007.

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

V novembri 2008 Komisia uľahčila diskusiu otvorením ďalšej verejnej konzultácie v rámci celej EÚ o možných cieľoch politiky posilnenej bezpečnosti sietí a informácií a o prostriedkoch na dosiahnutie týchto cieľov[5]. Okrem toho v decembri 2008 usporiadala workshop s odborníkmi z oblasti bezpečnosti sietí a informácií z príslušných orgánov členských štátov o nástrojoch a mechanizmoch posilnenej politiky EÚ v oblasti bezpečnosti sietí a informácií. V marci 2009 Komisia navyše prijala oznámenie o ochrane kritických informačných infraštruktúr (CIIP)[6], v ktorom sa pre agentúru ENISA určuje kľúčová úloha pre podporu pripravenosti, bezpečnosti a odolnosti v rámci EÚ. Tento prístup podporila ministerská konferencia o CIIP konaná v Tallinne 27. a 28. apríla 2009, jedným zo záverov ktorej bolo, že ***„nové a dlhodobé výzvy do budúcnosti si vyžadujú starostlivé prehodnotenie a preformulovanie mandátu agentúry ENISA s cieľom lepšie sa zamerať na priority a potreby Únie;*** *dosiahnuť schopnosť flexibilnejšej reakcie; rozvinúť európske skúsenosti a schopnosti; a podporiť prevádzkovú účinnosť a celkový vplyv agentúry. Agentúra ENISA by sa týmto spôsobom mohla stať trvalým prínosom pre každý členský štát a Európsku úniu ako celok*".

Dňa 18. decembra 2009 prijala Rada uznesenie o *„prístupe Európy k bezpečnosti sietí a informácií založenom na spolupráci"*[7], v ktorom sa okrem iného zdôrazňuje, že ***„agentúra ENISA by mala na základe revidovaného mandátu slúžiť ako odborné centrum EÚ v záležitostiach bezpečnosti sietí a informácií týkajúcich sa EÚ"***.

V dokumente Komisie Európa 2020 - Stratégia na zabezpečenie inteligentného, udržateľného a inkluzívneho rastu[8] sa ako jedna z prioritných iniciatív presadzujúcich Európu 2020 uvádza Európska digitálna agenda, v ktorej zohráva ústrednú rolu bezpečnosť sietí a informácií. **Cieľom tejto politickej iniciatívy na podporu dôvery a bezpečnosti v Európskej digitálnej agende je umožniť EÚ, 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**. Tým sa prispeje k zvýšeniu dôvery a bezpečnosti na európskom digitálnom jednotnom trhu a zlepší sa konkurencieschopnosť európskych podnikov.

2. VYMEDZENIE PROBLÉMU

2.1. V čom spočíva problém?

Ako faktory zraniteľnosti, vystavujúce zainteresované strany hrozbám a incidentom v oblasti bezpečnosti sietí a informácií, boli určené nasledujúce problémy. Všetky ilustrujú, že existuje potreba spoľahlivej štruktúry na úrovni EÚ, ktorá by sa zaoberala týmito problémami a bola schopná v rámci celej Európy držať krok s neustálymi zmenami technológií a trhových podmienok v oblasti bezpečnosti sietí a informácií.

- **Rozmanitosť a roztrieštenosť vnútroštátnych prístupov** Problémy bezpečnosti sietí a informácií sa nedajú obmedzovať štátnymi hranicami, a preto sa nemôžu účinne riešiť len

---

5 Od 7. novembra 2008 do 9. januára 2009, správa je k dispozícii na adrese http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm.

6 Oznámenie Komisie Európskemu parlamentu a Rade o ochrane kritických informačných infraštruktúr, KOM(2009)149, 30. 3. 2009.

7 Uznesenie Rady z 18. decembra 2009 o prístupe Európy k bezpečnosti sietí a informácií založenom na spolupráci (2009/C 321/01).

8 KOM(2010) 2020.

na vnútroštátnej úrovni. Problémom sa súčasne zaoberajú verejné orgány v rôznych členských štátov, a to mnohými rozličnými spôsobmi. Mnohé bezpečnostné požiadavky v rozličných členských štátoch zaťažujú podniky, ktoré pôsobia v rámci celej EÚ, bremenom nákladov, čo vedie k roztrieštenosti a nedostatku konkurencieschopnosti na európskom vnútornom trhu.

- **Obmedzené schopnosti európskeho včasného varovania a reakcie.** Súčasné vnútroštátne systémy včasného varovania a reakcie na incidenty sa v jednotlivých členských štátoch významne líšia a neexistuje nijaký systém na úrovni EÚ. EÚ potrebuje politické nástroje na identifikáciu rizík a nedostatkov v oblasti bezpečnosti sietí a informácií, na navrhnutie vhodných reakčných mechanizmov a na zabezpečenie toho, aby zainteresované strany tieto reakčné mechanizmy poznali a uplatňovali.

- **Nedostatok spoľahlivých údajov a obmedzenosť poznatkov o vznikajúcich problémoch.** Existuje len veľmi málo spoľahlivých kvantitatívnych informácií o vplyve, alebo čo len výskyte incidentov spojených s bezpečnosťou sietí a informácií, čo sťažuje tvorcom politík prijímanie adekvátnych politických opatrení a podnikom rozhodovanie o investíciách do bezpečnosti.

- **Nedostatok informovanosti o rizikách a problémoch v oblasti bezpečnosti sietí a informácií.** Zodpovednosť za zaistenie bezpečnosti sietí a informácií spočíva na jednotlivých zainteresovaných stranách; ich zodpovednosť však nie je vždy jasne definovaná a oznamovaná. Na druhej strane spotrebitelia často podceňujú riziká pre bezpečnosť sietí a informácií a ignorujú svoju osobnú zodpovednosť za zabezpečenie svojich systémov IKT. Na druhej strane podniky často vidia len náklady na bezpečnosť sietí a informácií, a nie potenciálne úspory, ktoré so sebou tieto náklady prinášajú.

- **Medzinárodný rozmer problémov bezpečnosti sietí a informácií** Hrozby pre bezpečnosť sietí a informácií a akékoľvek následné incidenty sú už svojou povahou medzinárodné, takže opatrenia EÚ môžu byť menej účinné, ak sa problémy bezpečnosti sietí a informácií dostatočne neriešia na medzinárodnej úrovni. Potrebujeme vytvoriť stratégiu EÚ a referenčný bod pre bezpečnosť sietí a informácií, ktorý by EÚ dostal z medzinárodného hľadiska do lepšej pozície.

- **Potreba modelov spolupráce na zaistenie adekvátneho vykonávania politík.** Adekvátne vykonávanie politík bezpečnosti sietí a informácií si vyžaduje model spolupráce na úrovni EÚ. Zainteresované strany potrebujú podporu pri odhaľovaní hrozieb pre bezpečnosť sietí a informácií a vytváraní osvedčených postupov v rámci vykonávania politík bezpečnosti sietí a informácií.

- **Potreba efektívnejších opatrení proti počítačovej kriminalite.** Snahy o bezpečnosť sietí a informácií sa predovšetkým organizovali v rámci bývalého prvého piliera, čiže záležitostí, o ktorých sa diskutovalo medzi inštitúciami. So začatím uplatňovania Lisabonskej zmluvy je však potrebné vziať do úvahy širší balík úloh pre agentúru pre bezpečnosť sietí a informácií, ktorý by pokrýval aj oblasti druhého a tretieho piliera, čiže záležitosti, o ktorých predtým rozhodovala len Rada.

2.2. Na koho najviac dolieha tento problém?

Incidenty v oblasti bezpečnosti sietí a informácií by mohli mať veľký vplyv na najrôznejšie zainteresované strany vrátane veľkých i malých podnikov, verejných orgánov a správ a

jednotlivých občanov. Inými slovami bezpečnosť sietí a informácií sa týka každého a sú za ňu zodpovední všetci.

K dispozícii máme len málo alebo dokonca žiadne kvantitatívne informácie o presnom počte incidentov spojených s bezpečnosťou sietí a informácií a/alebo o ich ekonomických dôsledkoch. Jedným náznakom je štúdia trhu z dielne IDC EMEA[9], v ktorej sa konštatuje, že za posledných 12 mesiacov 28 % domácností v rámci EÚ-27 malo problémy so spamom alebo vírusmi. Za posledný rok zažilo incident týkajúci sa bezpečnosti v priemere okolo 7 % používateľov vo sfére podnikov.

3. DÔVOD OPATRENÍ NA ÚROVNI EÚ, PRIDANÁ HODNOTA EÚ A SUBSIDIARITA

Vzájomná závislosť sietí a informačných systémov veľmi sťažuje, ak nie znemožňuje jednotlivým aktérom správne posúdenie globálneho vplyvu ich opatrení na ochranu proti incidentom spojeným s bezpečnosťou sietí a informácií na hospodárstvo a spoločnosť. Rozdielne vnútroštátne politiky a praktické opatrenia narúšajú vnútorný trh, a to tak v dôsledku negatívnych vonkajších vplyvov incidentov spojených s bezpečnosťou sietí a informácií (nedostatočné politiky ovplyvňujú trh v iných členských štátoch), ako aj pozitívnych vonkajších vplyvov osvedčených postupov v oblasti bezpečnosti sietí a informácií (osvedčené postupy v jednom členskom štáte zlepšujú bezpečnosť sietí a informácií ako celok, a tým vytvárajú jasný spoločenský prínos). Preto je zasahovanie prostredníctvom politík EÚ oprávnené, pretože by poskytlo skutočnú pridanú hodnotu k fungovaniu vnútorného trhu. Takáto pridaná hodnota sa uznáva aj v nariadení (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, ktorom sa ustanovuje, že pôsobenie agentúry ENISA je zamerané na prispievanie k plynulému fungovaniu vnútorného trhu

Navyše zasahovanie EÚ do politiky v oblasti bezpečnosti sietí a informácií je opodstatnené *zásadou subsidiarity*. Ako sa uvádza v oznámení o CIIP, stratégia EÚ spočívajúca v úplnom nezasahovaní do vnútroštátnych politík v oblasti bezpečnosti sietí a informácií by sa dosť podobala na situáciu, keď by sa od každého členského štátu žiadalo, aby chránil len svoj vlastný priestor, bez ohľadu na vzájomnú závislosť informačných systémov. Vhodný stupeň koordinácie medzi členskými štátmi zabezpečujúci, aby sa cezhraničné dôsledky rizík pre bezpečnosť sietí a informácií dali dobre zmanažovať, je preto v súlade so zásadou subsidiarity. Navyše opatrenie na úrovni EÚ by zlepšilo účinnosť akýchkoľvek existujúcich vnútroštátnych politík.

Občania EÚ v čoraz väčšej miere zverujú svoje údaje zložitým informačným systémom (napr. internetovému „oblaku počítačov“ – cloud computing). Vypracovanie spoločnej politiky a politiky založenej na spolupráci v oblasti bezpečnosti sietí a informácií môže preto mať výrazne prospešný vplyv na *účinnú ochranu základných práv* a konkrétne práva *na ochranu osobných údajov a súkromia*. Aj z tohto dôvodu sa zdá ďalšia politika EÚ dostatočne oprávnená.

[9] IDC EMEA, Európsky trh s bezpečnosťou sietí a informácií, scenáre, trendy a problémy, apríl 2009, s odkazmi na prehľad e-komunikácií Eurobarometra, apríl 2007.

4. POLITICKÉ CIELE

Toto posúdenie vplyvu skúma, do akej miery by sa dala modernizovaná agentúra pre bezpečnosť sietí a informácií, ktorá sa v širokej miere považuje za najvhodnejšiu organizačnú štruktúru, čo najlepšie rozsahovo prispôsobiť úlohe prispievať, spolu s inými nástrojmi Únie, k dosiahnutiu politických cieľov.

Všeobecným cieľom je umožniť EÚ, 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. Tým sa prispeje k zvýšeniu dôvery a bezpečnosti v európskom digitálnom jednotnom trhu a zlepší sa konkurencieschopnosť európskych podnikov.

Tento cieľ pozostáva zo siedmich **špecifických cieľov**:

(1) **Jednotnosť regulačných prístupov** — poskytovať usmernenia a poradenstvo Komisii a členským štátom pri aktualizácii a vytváraní holistického normatívneho rámca v oblasti bezpečnosti sietí a informácií;

(2) **Predchádzanie, odhalenie a reakcia** — zlepšovať pripravenosť prispievaním k európskej schopnosti včasného varovania a reakcie na incidenty prostredníctvom celoeurópskych plánov pre mimoriadne prípady a cvičení;

(3) **Podpora pri vytváraní politík** — poskytovať pomoc a poradenstvo Komisii a členským štátom;

(4) **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 MSP, ako aj rozvíjaním kultúry informovanosti o bezpečnosti sietí a informácií.

(5) **Posilnenie úlohy Európy v medzinárodnom kontexte** – dosiahnuť vysokú úroveň spolupráce s tretími krajinami a medzinárodnými organizáciami s cieľom presadzovať spoločný globálny prístup k bezpečnosti sietí a informácií a podporiť medzinárodné iniciatívy na vysokej úrovni v Európe.

(6) **Spoločná implementácia** — uľahčovať spoluprácu pri vykonávaní politík v oblasti bezpečnosti sietí a informácií.

(7) **Boj proti počítačovej kriminalite** — príprava účinnej reakcie na aspekty boja proti počítačovej kriminalite týkajúce sa bezpečnosti sietí a informácií prostredníctvom spolupráce s orgánmi (bývalého) druhého a tretieho piliera, napr. s Europolom.

5. MOŽNÉ ORGANIZAČNÉ FORMY A MOŽNOSTI POLITIKY

V posúdení vplyvu (kapitola 4 a príloha 4) sa skúma niekoľko možných organizačných foriem vrátane: i) agentúry, ii) viac či menej formalizovaného verejno-súkromného partnerstva (PPP), iii) siete neformálnych kontaktov, iv) stálej siete príslušných orgánov a v) priameho začlenenie do útvarov Komisie.

Pri porovnaní týchto rôznych organizačných foriem sa zdá najvhodnejším výberom pre nástroj politiky forma agentúry vďaka výhodám, pokiaľ ide o: (1) právnu istotu organizačnej štruktúry, ako aj o podstatu, (2) jej vhodnosť pre špecifické potreby takého citlivého sektora, akým je bezpečnosť sietí a informácií (organizovanie vonkajšej expertízy, koordinácia

vzťahov so zainteresovanými stranami, účasť/záväzky členských štátov a (3) povesť agentúry ENISA a jej prijatie komunitou bezpečnosti sietí a informácií.

Preto sa pripravili a pre organizačnú formu agentúry podrobne posúdili ďalej uvedené možnosti politiky.

Možnosť politiky č. 1: Žiadna politika

V rámci možnosti „žiadna politika“ sa predpokladá, že agentúra ENISA by po marci 2012 prestala existovať a jej súčasné aktivity by ani ako celok, ani čiastočne neprebrala nijaká iná inštitúcia EÚ.

Rozpustenie agentúry ENISA by znamenalo, že všetky doterajšie investície, napríklad investície do vytvárania organizácie schopnej pritiahnuť vysoko špecializovaných odborníkov, do získavania skúseností a do vytvárania siete prepojení so zainteresovanými stranami, medzi nimi a s medzinárodnými inštitúciami, by sa zrušili v okamihu, keď existujúca agentúra dosiahla potrebné pracovné tempo.

Komplexná povaha problémov v oblasti bezpečnosti sietí a informácií v rámci Európy si vyžaduje modernizovanú a posilnenú agentúru, a nie zavretie tej, ktorá už existuje. To potvrdzuje jasná úloha, ktorú dostala agentúra ENISA napríklad v reformovanom regulačnom rámci pre elektronické komunikácie[10], a všeobecná podpora, vyjadrená zainteresovanými stranami, významnejšej úlohy pre Európskej agentúry pre bezpečnosť sietí a informácií.

Možnosť politiky č. 2: Pokračovanie „à l'identique“ (rovnakým spôsobom)

Možnosť č. 2 predstavuje scenár „všetko po starom“, čiže pokračovanie rovnakého politického nástroja v rovnakej forme a s rovnakými zdrojmi. Medzi zainteresovanými stranami existuje všeobecná zhoda, že agentúra ENISA dozrela do dôveryhodného referenčného bodu pre otázky bezpečnosti sietí a informácií a vyvinula sa v svojej oblasti na centrum excelentnosti.

S prihliadnutím na súčasný stav zamestnancov a rozpočtové obmedzenia bude agentúra schopná ovplyvniť len veľmi obmedzený počet otázok bezpečnosti sietí a informácií. To však kontrastuje s celkovými očakávaniami zainteresovaných strán. Ak sa agentúre neumožní ďalej sa vyvíjať a nenaplnia sa tieto rastúce očakávania, mohlo by to v konečnom dôsledku viesť ku kríze dôveryhodnosti.

Možnosť politiky č. 3: Rozšírenie funkcií v súčasnosti definovaných pre agentúru ENISA a doplnenie orgánov v oblasti presadzovania práva a ochrany súkromia ako plne kvalifikovaných zainteresovaných strán

V rámci tejto možnosti by sa úloha agentúry pre bezpečnosť sietí a informácií rozšírila a zamerala na:

- vybudovanie a udržiavanie styčnej siete medzi zainteresovanými stranami a siete 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),

[10] Pozri http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:EN:HTML.

elektronický podpis (e-sign) a e-ID a normy obstarávania v oblasti bezpečnosti sietí a informácií);

- podporu politiky EÚ v oblasti CIIP a odolnosti (cvičenia, EP3R[11], Európsky systém zdieľania informácií a varovania atď.);
- vytvorenie rámca EÚ 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 a podávanie správ o nej;
- 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 súvisiacich s bezpečnosťou sietí a informácií.

Agentúra by mala k dispozícii všetky zdroje potrebné na to, aby svoje činnosti mohla vykonávať s dostatočnou dôkladnosťou, čiže aby mala možnosť získať skutočný vplyv. Ak by mala k dispozícii viac zdrojov, mohla by agentúra ENISA zohrávať oveľa aktívnejšiu úlohu a prichádzať s väčším množstvom iniciatív s cieľom stimulovať aktívnu účasť zainteresovaných strán. Navyše by táto nová situácia umožnila flexibilnejšiu a rýchlejšiu reakciu na zmeny v stále sa vyvíjajúcom prostredí bezpečnosti sietí a informácií.

Možnosť politiky č. 4: Pridanie operačných funkcií boja proti počítačovým útokom a reakcie na počítačové incidenty

Okrem činností uvedených v rámci možnosti č. 3 by agentúra mala operačné funkcie, ako sú prebranie aktívnejšej úlohy v CIIP EÚ, napríklad pri predchádzaní incidentom a reakcii na ne, najmä v úlohe tímu reakcie na núdzové počítačové situácie (CERT) v rámci bezpečnosti sietí a informácií EÚ a koordinátora vnútroštátnych tímov CERT ako stredisko EÚ proti útokom na bezpečnosť sietí a informácií vrátane každodenného riadenia a poskytovania núdzových služieb.

Táto možnosť by si vyžiadala podstatný nárast rozpočtu agentúry a ľudských zdrojov, čo vyvoláva obavy o jej schopnosti čerpania a účinného využívania rozpočtu vo vzťahu k očakávaným prínosom.

Možnosť politiky č. 5: Pridanie operačných funkcií na podporu orgánov presadzovania práva a súdnych orgánov pri boji proti počítačovej kriminalite

Okrem činností uvedených v možnosti č. 4 by táto možnosť zahŕňala funkcie agentúry týkajúce sa:

- poskytovania podpory procesného práva (pozri Dohovor o počítačovej kriminalite). Napríklad zber prevádzkových údajov, zachytávanie údajov o obsahu, monitorovanie tokov v prípade útokov spôsobujúcich nedostupnosť služieb;
- pôsobenia v úlohe strediska expertízy pre kriminálne vyšetrovanie vrátane aspektov bezpečnosti sietí a služieb.

[11] Európske verejno-súkromné partnerstvo pre odolnosť, pozri KOM(2009) 149.

Ako v prípade možnosti č. 4, aj táto by si vyžadovala podstatné zvýšenie zdrojov agentúry a vyvoláva podobné obavy v súvislosti s kapacitou čerpania a účinným využívaním rozpočtu.

6. POROVNANIE MOŽNOSTÍ POLITIKY A POSÚDENIE VPLYVU

Analýza možných hospodárskych, sociálnych a environmentálnych vplyvov ukazuje, že ***možnosť č. 1*** by mala negatívne účinky vo všetkých ohľadoch a situácia by sa zhoršila.

Možnosť č. 2 sa ukazuje ako neoptimálna, keďže agentúra by nemala potrebné zdroje na adekvátne vyrovnávanie sa s výzvami, aké predstavuje stále sa meniace prostredie bezpečnosti sietí a informácií, čo by mohlo viesť k riziku poškodenia dobrého mena a v konečnom dôsledku ku kríze dôveryhodnosti.

V rámci ***možnosti č. 3*** by modernizovaná agentúra pre bezpečnosť sietí a informácií prispela k:

Zmenšeniu roztrieštenosti vnútroštátnych prístupov (problémový moment č. 1), posilneniu politiky a rozhodovania založených na znalostiach a informáciách (problémový moment č. 3) a zvýšeniu celkovej informovanosti o rizikách a problémoch v oblasti bezpečnosti sietí a informácií a ich odstraňovania (problémový moment č. 4) tým, že by prispievala k:

- efektívnejšiemu zberu príslušných informácií o rizikách, hrozbách a nedostatkoch vo všetkých jednotlivých členských štátoch;
- zvýšenej dostupnosti informácií o súčasných a budúcich problémoch a rizikách v oblasti bezpečnosti sietí a informácií;
- zabezpečovaniu vyššej kvality politiky v oblasti bezpečnosti sietí a informácií v členských štátoch.

Zlepšeniu schopnosti európskeho včasného varovania a reakcie (problémový moment č. 2) tým, že:

- pomôže Komisii a členským štátom pripraviť celoeurópske cvičenia, a tým dosiahne úspory z rozsahu pri reagovaní na incidenty v rámci celej EÚ;
- uľahčí fungovanie EP3R, čo by nakoniec mohlo viesť k ďalším investíciám vyvolaným spoločnými politickými cieľmi a normami pre bezpečnosť a odolnosť na úrovni EÚ.

Podpore spoločného globálneho prístupu k bezpečnosti sietí a informácií (problémový moment č. 5) tým, že:

- zväčší rozsah výmeny informácií a poznatkov s nečlenskými krajinami EÚ.

Efektívnejšiemu a účinnejšiemu boju proti počítačovej kriminalite (problémový moment č. 7), a to:

- zapojením do neoperatívnych úloh týkajúcich sa aspektov spolupráce v rámci presadzovania práva a súdnictva súvisiacich s bezpečnosťou sietí a informácií,

ako je obojsmerná výmena informácií a školení (napr. v spolupráci s Európskou policajnou akadémiou CEPOL).

Možnosť č. 4 by okrem vplyvov, ktoré by sa mohli dosiahnuť v rámci možnosti č. 3, priniesla väčší vplyv na operatívnej úrovni. Tým, že by agentúra pôsobila ako CERT EÚ v oblasti bezpečnosti informácií a sietí, prispievala by k zvýšeniu úspor z rozsahu, ak by reagovala na incidenty v rámci celej EÚ, a k zníženiu prevádzkových rizík, napríklad vďaka vyšším úrovniam bezpečnosti a odolnosti.

Možnosť č. 5 by dosiahla vyššiu účinnosť v boji proti počítačovej kriminalite než možnosti č. 3 a 4, pričom by pri nej pribudli operačné funkcie na podporu orgánov presadzovania práva a súdnych orgánov.

Ale aj keď by možnosti č. 4 a 5 mali väčší pozitívny vplyv než možnosť č. 3, obe tieto možnosti by boli pre členské štáty politicky citlivé z hľadiska ich zodpovednosti za CIIP (t. j. istý počet členských štátov by nebol naklonený centralizovaniu operačných funkcií). Okrem toho rozšírenie mandátu posudzované na základe možností č. 4 a 5 môže znejasniť postavenie agentúry. Pridanie týchto nových a úplne odlišných operačných úloh k mandátu agentúry by sa navyše mohlo v krátkodobom horizonte ukázať ako veľmi náročné a existuje dosť veľké riziko, že by agentúra nebola schopná riadne vykonať takého úlohy v primeranej lehote. V neposlednom rade náklady na vykonávanie možností č. 4 a 5 sú neprijateľne vysoké — bol by potrebný štyrikrát až päťkrát väčší rozpočet, než je súčasný rozpočet agentúry ENISA.

Pri porovnaní vplyvu všetkých piatich možností politiky na organizačnú formu modernizovanej agentúry pre bezpečnosť sietí a informácií treba odmietnuť možnosti č. 1 a 2, pretože ani jedna z nich by neumožnila adekvátne riešiť komplexný problém bezpečnosti sietí a informácií na úrovni EÚ. Na druhej strane možnosti č. 3., 4 a 5 by EÚ umožnili, aby primerane riešila budúce možnosti politiky v oblasti bezpečnosti sietí a informácií. Možnosti č. 4 a 5 sa, aspoň zatiaľ, javia ako priveľmi ambiciózne tak z hľadiska politickej citlivosti väčšiny členských štátov, ako aj z hľadiska vplyvu na rozpočet. Preto ***sa možnosť č. 3 javí ako najlepšia možnosť čo najefektívnejšieho riešenia siedmich zistených problémov v oblasti bezpečnosti sietí a informácií.***

7. MONITOROVANIE A HODNOTENIE: AKO BY SA MALI MERAŤ SKUTOČNÉ NÁKLADY A PRÍNOSY A DOSAHOVANIE POŽADOVANÝCH ÚČINKOV?

Táto politická iniciatíva by zabezpečila pravidelné hodnotenie, ktoré by Komisia odovzdávala Európskemu parlamentu a Rade a zverejňovala. Toto hodnotenie by zohľadnilo názory všetkých príslušných zainteresovaných strán na základe referenčných podmienok dohodnutých so správnou radou agentúry a posúdilo by účinnosť agentúry pri dosahovaní jej cieľov, to, či je ešte vždy účinným nástrojom, a či by sa mali urobiť nejaké zmeny mandátu agentúry a/alebo iných aspektov nariadenia o jej zriadení. Po vyhodnotení by správna rada agentúry vydala odporúčanie Komisii týkajúce sa všetkých zmien, ktoré by bolo vhodné urobiť v tomto nariadení. Správna rada a výkonný riaditeľ by mali zohľadniť výsledky hodnotenia pri viacročnom plánovaní agentúry.

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