



V Bruseli 4. 10. 2017
COM(2017) 477 final

2017/0225 (COD)

NOTE

This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“)

(Text s významom pre EHP)

{SWD(2017) 500 final}

{SWD(2017) 501 final}

{SWD(2017) 502 final}

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Európska únia už prijala viacero opatrení s cieľom zvýšiť odolnosť a dosiahnuť lepšiu pripravenosť v oblasti kybernetickej bezpečnosti. V prvej stratégii kybernetickej bezpečnosti EÚ¹ prijatej v roku 2013 sa stanovujú strategické ciele a konkrétne opatrenia v záujme dosiahnutia odolnosti, znižovania počítačovej kriminality, rozvoja politiky a spôsobilostí v oblasti kybernetickej obrany, rozvoja priemyselných a technologických zdrojov a vytvorenia koherentnej medzinárodnej politiky v oblasti kybernetického priestoru pre EÚ. V tejto súvislosti sa odvtedy uskutočnili významné zmeny, najmä pokiaľ ide o druhý mandát Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA)² a prijatie **smernice o bezpečnosti sietí a informačných systémov**³ (smernica NIS), ktoré tvoria základ tohto návrhu.

V roku 2016 prijala Európska komisia oznámenie s názvom „Posilnenie odolnosti kybernetického systému a podpora konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe“⁴, v ktorom boli oznámené ďalšie opatrenia na prehĺbenie spolupráce a spoločného využívania informácií a poznatkov, ako aj na zvýšenie odolnosti a pripravenosti EÚ, a to aj vzhľadom na hrozbu rozsiahlych incidentov a možnej celoeurópskej krízy v oblasti kybernetickej bezpečnosti. V tejto súvislosti Komisia oznámila, že urýchli **hodnotenie** a **preskúmanie** nariadenia Európskeho parlamentu a Rady (EÚ) č. 526/2013 o agentúre ENISA a o zrušení nariadenia (ES) č. 460/2004 (ďalej len „nariadenie o agentúre ENISA“). Proces hodnotenia by mohol viesť k prípadnej reforme agentúry a posilneniu jej spôsobilostí a kapacity, aby mohla členským štátom poskytovať udržateľnú podporu. Agentúre by sa teda pridelená operatívnejšia a ústrednejšia úloha pri dosahovaní odolnosti v oblasti kybernetickej bezpečnosti a v novom mandáte agentúry by sa uznali jej nové zodpovednosti v rámci smernice NIS.

Smernica NIS je prvým zásadným krokom smerom k podpore kultúry riadenia rizika, a to zavedením bezpečnostných požiadaviek ako právnych záväzkov pre kľúčové hospodárske subjekty, najmä pre prevádzkovateľov základných služieb (prevádzkovatelia základných služieb – PZS) a dodávateľov niektorých kľúčových digitálnych služieb (poskytovatelia digitálnych služieb – PDS). Keďže bezpečnostné požiadavky sa považujú za nevyhnutné na ochranu výhod narastajúcej digitalizácie spoločnosti, a aj vzhľadom na rýchle šírenie prepojených zariadení (internet vecí – IoT), sa v oznámení z roku 2016 uviedol aj nápad vytvoriť rámec bezpečnostnej certifikácie produktov a služieb IKT s cieľom zvýšiť dôveru a bezpečnosť na digitálnom jednotnom trhu. Certifikácia kybernetickej bezpečnosti IKT je obzvlášť dôležitá vzhľadom na zvýšené využívanie technológií, ktoré si vyžadujú vysokú

¹ Spoločné oznámenie Európskej komisie a Európskej služby pre vonkajšiu činnosť: Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor – JOIN(2013).

² Nariadenie (EÚ) č. 526/2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a o zrušení nariadenia (ES) č. 460/2004.

³ Smernica (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

⁴ Oznámenie Komisie o posilnení odolnosti kybernetického systému a podpore konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe, COM(2016) 0410 final.

úroveň kybernetickej bezpečnosti, ako sú prepojené a automatizované vozidlá, elektronické zdravotnícke systémy alebo automatické priemyselné riadiace systémy (IACS).

Tieto politické opatrenia a oznámenia sa ďalej podporili **závermi Rady** z roku 2016, v ktorých sa uznáva, že „kybernetické hrozby a zraniteľné miesta sa neustále vyvíjajú a zintenzívňujú, čo si vyžaduje nepretržitú a užšiu spoluprácu, najmä pri riešení rozsiahlych cezhraničných kybernetických bezpečnostných incidentov“. Závermi sa potvrdilo, že „nariadenie o agentúre ENISA je jedným z hlavných prvkov rámca kybernetickej odolnosti v EÚ“⁵ a Komisia sa vyzvala na prijatie ďalších krokov s cieľom riešiť problematiku certifikácie na európskej úrovni.

Vytvorenie certifikačného systému by si vyžadovalo zriadenie vhodného systému riadenia na úrovni EÚ vrátane dôkladného odborného poradenstva poskytovaného nezávislou agentúrou EÚ. Súčasný návrh v tejto súvislosti identifikuje ENISA ako orgán na úrovni EÚ s prirodzenou zodpovednosťou v otázkach kybernetickej bezpečnosti, ktorý by mal túto úlohu prevziať s cieľom spojiť a skoordinať prácu príslušných vnútroštátnych orgánov v oblasti certifikácie.

Vo svojom oznámení o **preskúmaní stratégie digitálneho jednotného trhu v polovici trvania z mája 2017** Komisia ďalej uviedla, že do septembra 2017 preskúma mandát agentúry ENISA. Účelom je vymedziť úlohu agentúry v zmenenom ekosystéme kybernetickej bezpečnosti a vypracovať opatrenia v oblasti noriem kybernetickej bezpečnosti, certifikácie a označovania v záujme zvýšenia kybernetickej bezpečnosti systémov založených na IKT vrátane pripojených predmetov⁶. V **záveroch zo zasadnutia Európskej rady** v júni 2017⁷ sa uvítal zámer Komisie v septembri preskúmať stratégiu kybernetickej bezpečnosti a do konca roka 2017 navrhnuť ďalšie ciele opatrenia.

Navrhovaným nariadením sa stanovuje komplexný súbor opatrení, ktoré vychádzajú z predchádzajúcich krokov, pričom nariadenie napomáha rozvoju vzájomne sa podporujúcich konkrétnych cieľov:

- zvýšiť **spôsobilosti a pripravenosť** členských štátov a podnikov;
- zlepšiť **spoluprácu a koordináciu** v rámci členských štátov, inštitúcií, agentúr a orgánov EÚ;
- posilniť **spôsobilosti na úrovni EÚ na doplnenie činností členských štátov**, a to najmä v prípade cezhraničných kybernetických kríz;
- zvýšiť **informovanosť** občanov a podnikov o otázkach kybernetickej bezpečnosti;
- zvýšiť celkovú **transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti**⁸ produktov a služieb IKT, čím sa posilní dôvera v digitálny jednotný trh a v digitálnu inováciu a

⁵ Závery Rady o posilnení odolnosti kybernetického systému a podpore konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe z 15. novembra 2016.

⁶ Oznámenie Komisie o preskúmaní vykonávania stratégie digitálneho jednotného trhu v polovici trvania – COM(2017) 228.

⁷ Zasadnutie Európskej rady (22. a 23. júna 2017) – závery EUCO 8/17.

⁸ Transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti spočíva v poskytovaní dostatočných informácií používateľom o kyberneticko-bezpečnostných prvkoch, ktoré im umožnia objektívne určiť úroveň bezpečnosti daného produktu, služby alebo procesu IKT.

- zabrániť **roztrieštenosti systémov certifikácie** v EÚ a súvisiacich bezpečnostných požiadaviek a hodnotiacich kritérií v jednotlivých členských štátoch a odvetviach.

V nasledujúcej časti dôvodovej správy sa podrobnejšie vysvetľujú dôvody tejto iniciatívy, pokiaľ ide o navrhované opatrenia týkajúce sa agentúry ENISA a certifikácie kybernetickej bezpečnosti.

Agentúra ENISA

Agentúra ENISA pôsobí ako centrum odborných znalostí zameraných na zvýšenie sieťovej a informačnej bezpečnosti v Únii a na podporu budovania kapacít členských štátov.

Agentúra ENISA bola zriadená v roku 2004⁹ s cieľom prispieť k celkovému cieľu zabezpečenia vysokej úrovne sieťovej a informačnej bezpečnosti v EÚ. V roku 2013 sa nariadením (EÚ) č. 526/2013 stanovil nový mandát agentúry na obdobie siedmich rokov, teda do roku 2020. Agentúra má kancelárie v Grécku – administratívne sídlo v meste Heraklion (na Kréte) a svoje hlavné činnosti sústreď v Aténach.

ENISA je malá agentúra, ktorá má v porovnaní so všetkými agentúrami EÚ nízky rozpočet aj nízky počet zamestnancov. Jej mandát je časovo obmedzený.

Agentúra ENISA pomáha európskym inštitúciám, členským štátom a podnikateľskej komunite pri **riešení problémov spojených so sieťovou a informačnou bezpečnosťou, pri reakciách na ne, a najmä pri predchádzaní týmto problémom**. Uskutočňuje to prostredníctvom súboru činností v piatich oblastiach identifikovaných v jej stratégii¹⁰:

- Odborné znalosti: poskytovanie informácií a odborných znalostí o kľúčových otázkach týkajúcich sa sieťovej a informačnej bezpečnosti.
- Politika: podpora tvorby a vykonávania politík v Únii.
- Kapacity: podpora budovania kapacít v celej Únii (napr. prostredníctvom odbornej prípravy, odporúčaní, činností zameraných na zvyšovanie povedomia).
- Komunita: posilnenie komunity sieťovej a informačnej bezpečnosti [napr. podpora tímov reakcie na núdzové počítačové situácie (CERT), koordinácia celoeurópskych kybernetických cvičení].
- Podpora (napr. spolupráca so zainteresovanými stranami a medzinárodné vzťahy).

Počas rokovaní o smernici NIS sa spoluzákonnodarcovia EÚ rozhodli agentúre ENISA prideliť dôležité úlohy pri vykonávaní tejto smernice. Agentúra predovšetkým plní funkciu sekretariátu pre sieť jednotiek CSIRT (zriadenú na podporu rýchlej a účinnej operačnej spolupráce medzi členskými štátmi v prípade konkrétnych kybernetických incidentov a pri výmene informácií o rizikách) a takisto by mala pomáhať skupine pre spoluprácu pri plnení jej úloh. Smernicou sa okrem toho od agentúry ENISA vyžaduje, aby pomáhala členským štátom a Komisii, a to poskytovaním odborných znalostí a poradenstva a uľahčovaním výmeny osvedčených postupov.

V súlade s nariadením o agentúre ENISA vykonala Komisia hodnotenie agentúry, ktoré zahŕňa nezávislú štúdiu, ako aj verejnú konzultáciu. V rámci hodnotenia sa posudzovalo, akú má agentúra relevantnosť, dosah, efektívnosť, účinnosť, koherentnosť a pridanú hodnotu pre EÚ vzhľadom na jej výsledky, riadenie, vnútornú organizačnú štruktúru a pracovné postupy v období rokov 2013 – 2016.

⁹ 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).

¹⁰ <https://www.enisa.europa.eu/publications/corporate/enisa-strategy>

V rámci verejnej konzultácie celkové výsledky agentúry ENISA pozitívne hodnotila väčšina respondentov¹¹ (74 %). Väčšina respondentov sa ďalej domnievala, že agentúra ENISA dosahuje svoje konkrétne ciele (aspoň 63 % v prípade každého z cieľov). Služby a produkty agentúry ENISA pravidelne (mesačne alebo častejšie) používala takmer polovica respondentov (46 %) a tieto služby a produkty respondenti oceňujú kvôli tomu, že pochádzajú od orgánu na úrovni EÚ (83 %) a kvôli ich kvalite (62 %).

Veľká väčšina (88 %) respondentov sa však domnievala, že súčasné nástroje a mechanizmy, ktoré sú k dispozícii na úrovni EÚ, sú pri riešení súčasných výziev v oblasti kybernetickej bezpečnosti nedostatočné alebo postačujú len čiastočne. Veľká väčšina respondentov (98 %) uviedla, že na tieto potreby by mal reagovať orgán EÚ a spomedzi nich by 99 % respondentov na tento účel vybralo agentúru ENISA. Okrem toho 67,5 % respondentov vyjadrilo názor, že agentúra ENISA by mohla zohrávať úlohu pri stanovovaní harmonizovaného rámca bezpečnostnej certifikácie produktov a služieb IT.

Z celkového hodnotenia (založeného nielen na verejnej konzultácii, ale aj na niekoľkých individuálnych pohovoroch, ďalších cielených prieskumoch a seminároch) vyplynuli tieto závery:

- Ciele agentúry ENISA sú aktuálne aj dnes. Vzhľadom na rýchly technologický vývoj a vyvíjajúce sa hrozby, ako aj na stúpajúce globálne kyberneticko-bezpečnostné riziká existuje v EÚ jasná potreba podpory a ďalšieho posilnenia technických poznatkov na vysokej úrovni v otázkach kybernetickej bezpečnosti. V členských štátoch je zrejماً potreba budovania kapacít s cieľom pochopiť hrozby a reagovať na ne a je potrebné, aby zainteresované strany spolupracovali naprieč tematickými oblasťami a inštitúciami.
- Agentúra je napriek obmedzenej výške rozpočtových prostriedkov pri využívaní svojich zdrojov a pri vykonávaní svojich úloh prevádzkovo efektívna. Skutočnosť, že sa nachádza na dvoch miestach, v Aténach a Heraklione, však prináša ďalšie administratívne náklady.
- Pokiaľ ide o účinnosť, agentúra ENISA svoje ciele čiastočne splnila. Agentúra úspešne prispela k zlepšeniu sieťovej a informačnej bezpečnosti v Európe prostredníctvom ponuky budovania kapacít v 28 členských štátoch¹², zlepšenia spolupráce medzi členskými štátmi a zainteresovanými stranami v oblasti sieťovej a informačnej bezpečnosti, ako aj poskytovania odborných znalostí, budovania komunity a podpory rozvoja politík. Agentúra ENISA sa celkovo dôsledne zameriavala na vykonávanie svojho pracovného programu a konala ako dôveryhodný

¹¹ Na konzultáciu odpovedalo 90 zainteresovaných strán z 19 členských štátov (88 odpovedí a 2 pozičné dokumenty) vrátane vnútroštátnych orgánov z 15 členských štátov a 8 organizácií zastupujúcich značný počet európskych podnikov.

¹² Respondenti vo verejnej konzultácii boli požiadaní o vyjadrenie k tomu, čo vnímajú ako hlavné úspechy agentúry ENISA v období rokov 2013 – 2016. Respondenti zo všetkých skupín (spolu 55, z toho 13 z vnútroštátnych orgánov, 20 zo súkromného sektora a 22 z ostatných oblastí) vnímali ako hlavné úspechy agentúry ENISA tieto aspekty: 1. koordinácia cvičení CyberEurope; 2. poskytovanie podpory pre CERT/CSIRT v podobe odbornej prípravy a seminárov na podporu koordinácie a výmeny; 3. publikácie agentúry ENISA (usmernenia a odporúčania, správy o situácii v súvislosti s kybernetickými hrozbami, stratégie oznamovania incidentov a krízového riadenia atď.), ktoré sa považovali za užitočné na vytvorenie a aktualizovanie vnútroštátnych bezpečnostných rámcov, a aj ako východisko pre tvorcov politík a kybernetických odborníkov z praxe; 4. pomoc pri propagácii smernice NIS; 5. úsilie na zvýšenie informovanosti o kybernetickej bezpečnosti prostredníctvom mesiaca kybernetickej bezpečnosti.

partner svojich zainteresovaných strán v oblasti, ktorej sa len nedávno pripísal takýto silný cezhraničný význam.

- Agentúre ENISA sa síce podarilo v obrovskej oblasti sieťovej a informačnej bezpečnosti dosiahnuť určitý vplyv, nepodarilo sa jej však úplne etablovať ako silná značka, získať si dostatočnú viditeľnosť a presadiť sa ako „to pravé“ stredisko odbornosti v Európe. Dôvodom je široký mandát agentúry ENISA, ktorému sa nepridelili dostatočné zdroje. Agentúra ENISA je okrem toho stále jedinou agentúrou EÚ s časovo obmedzeným mandátom, čo obmedzuje jej schopnosť pripraviť dlhodobú víziu a udržateľne podporovať svoje zainteresované strany. Je to aj v rozpore s ustanoveniami smernice NIS, ktoré agentúre ENISA zverujú úlohy bez časového obmedzenia. Z posúdenia nakoniec vyplynulo, že túto obmedzenú účinnosť možno čiastočne vysvetliť vysokým podielom využívania externých odborných znalostí v porovnaní s vnútornými, ako aj ťažkosťami pri náboře a udržaní špecializovaných pracovníkov.
- V neposlednom rade sa v hodnotení dospelo k záveru, že prínos agentúry ENISA spočíva predovšetkým v jej schopnosti posilňovať spoluprácu, a to najmä medzi členskými štátmi, a aj so súvisiacimi komunitami sieťovej a informačnej bezpečnosti (najmä medzi jednotkami CSIRT). Na úrovni EÚ neexistuje žiadny iný aktér, ktorý by podporoval takýto široký rozsah zainteresovaných strán v oblasti sieťovej a informačnej bezpečnosti. Vzhľadom na potrebu prísne stanoviť priority týkajúce sa činností agentúry ENISA sa však pracovný program agentúry väčšinou riadi potrebami členských štátov. V dôsledku toho sa ním dostatočne neriešia potreby ďalších zainteresovaných strán, najmä príslušného odvetvia. Agentúra sa kvôli tomu takisto stala vnímavejšou k plneniu potrieb svojich hlavných zainteresovaných strán, čo jej bráni v tom, aby dosiahla väčší vplyv. Pridaná hodnota agentúry sa preto rôznila podľa rozdielnych potrieb jej zainteresovaných strán a podľa toho, do akej miery bola agentúra schopná na ne reagovať (napr. veľké členské štáty verzus malé členské štáty; členské štáty verzus odvetvie).

Stručne povedané, z výsledkov konzultácií so zainteresovanými stranami a hodnotenia vyplynulo, že zdroje a mandát agentúry ENISA je potrebné prispôbiť tak, aby mohla zohrávať primeranú úlohu pri riešení súčasných a budúcich problémov.

Vzhľadom na tieto zistenia sa v tomto návrhu prehodnocuje súčasný mandát agentúry ENISA a stanovuje nový súbor úloh a funkcií, aby sa efektívne a účinne poskytla podpora členským štátom, inštitúciám EÚ a ostatným zainteresovaným stranám v ich úsilí o zaistenie bezpečného kybernetického priestoru v Európskej únii. Tento nový navrhovaný mandát má agentúre priznať silnejšiu a ústrednejšiu úlohu, a to aj prostredníctvom podpory členských štátov pri vykonávaní smernice NIS a na účely aktívnejšieho boja proti konkrétnym hrozbám (operačná kapacita), ako aj tým, že sa stane strediskom odbornosti na podporu členských štátov a Komisie v otázkach kyberneticko-bezpečnostnej certifikácie. Na základe tohto návrhu:

- Agentúre ENISA by sa udelil trvalý mandát, ktorý by jej dal do budúcnosti stabilný základ. Jej mandát, ciele a úlohy by boli stále predmetom pravidelného preskúmania.
- Navrhovaným mandátom sa ďalej objasňuje úloha agentúry ENISA ako agentúry EÚ pre kybernetickú bezpečnosť a ako referenčného bodu v ekosystéme kybernetickej bezpečnosti EÚ, ktorý koná v úzkej spolupráci so všetkými ostatnými príslušnými orgánmi tohto ekosystému.

- Organizácia a riadenie agentúry, ktoré boli v hodnotení posúdené kladne, by sa preskúmali len v primeranej miere, a to najmä s cieľom zabezpečiť, aby sa v práci agentúry lepšie zohľadnili potreby širšieho spoločenstva zainteresovaných strán.
- V navrhovanom vymedzení rozsahu mandátu je mandát posilnený v tých oblastiach, kde agentúra preukázala jasnú pridanú hodnotu, a doplnený novými oblasťami, v ktorých je potrebná podpora vzhľadom na nové politické priority a nástroje, najmä pokiaľ ide o smernicu NIS, preskúmanie stratégie kybernetickej bezpečnosti EÚ, pripravovanú koncepciu kybernetickej bezpečnosti EÚ pre spoluprácu v prípade kybernetickej krízy a bezpečnostnú certifikáciu IKT.
 - **Príprava a vykonávanie politík EÚ:** Úlohou agentúry ENISA by bolo aktívne prispievať k rozvoju politiky v oblasti sieťovej a informačnej bezpečnosti, ako aj k iným politickým iniciatívam s prvkami kybernetickej bezpečnosti v rozličných odvetviach (napr. v oblasti energetiky, dopravy, financií). Na tento účel by mala silnú poradnú úlohu, ktorú by mohla plniť poskytovaním nezávislých posudkov a prípravných prác zameraných na rozvoj a aktualizáciu politiky a právnych predpisov. Agentúra ENISA by takisto podporovala politiku a právne predpisy EÚ v oblasti elektronickej komunikácie, elektronickej identifikácie a dôveryhodných služieb s cieľom posilňovať úroveň kybernetickej bezpečnosti. Vo fáze vykonávania, najmä v kontexte skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti vytvorenej smernicou NIS by agentúra ENISA pomáhala členským štátom pri dosahovaní jednotného prístupu k vykonávaniu smernice NIS naprieč hranicami aj odvetviami, ako aj v rámci iných príslušných politík a právnych predpisov. S cieľom podporiť pravidelné preskúmanie politiky a právnych predpisov v oblasti kybernetickej bezpečnosti by agentúra ENISA takisto poskytovala pravidelné správy o stave vykonávania právneho rámca EÚ.
 - **Budovanie kapacít:** Agentúra ENISA by prispievala k zlepšovaniu schopností a odborných znalostí vnútroštátnych verejných orgánov a verejných orgánov EÚ, a to aj v oblasti reakcie na incidenty a dohľadu nad regulačnými opatreniami súvisiacimi s kybernetickou bezpečnosťou. Úlohou agentúry by takisto bolo prispievať k vytváraniu stredísk pre výmenu a analýzu informácií (ISAC) v rôznych odvetviach poskytovaním osvedčených postupov a usmernení o dostupných nástrojoch a postupoch, ako aj vhodných riešení regulačných otázok spojených s výmenou informácií.
 - **Znalosti a informácie, zvyšovanie povedomia:** Agentúra ENISA by sa stala informačným centrom EÚ. Znamenalo by to podporu a výmenu osvedčených postupov a iniciatív v rámci EÚ prostredníctvom zhromažďovania informácií o kybernetickej bezpečnosti od inštitúcií, agentúr a orgánov EÚ a členských štátov. Agentúra by takisto sprístupňovala poradenstvo, usmernenia a osvedčené postupy, pokiaľ ide o bezpečnosť kritických infraštruktúr. V nadväznosti na rozsiahle cezhraničné kybernetické incidenty by agentúra ENISA okrem toho zostavovala správy s cieľom poskytnúť usmernenia podnikom a občanom v celej EÚ. Do tejto činnosti by patrilo aj pravidelné organizovanie aktivít na zvyšovanie povedomia v spolupráci s orgánmi členských štátov.
 - **Trhové úlohy (normalizácia, kyberneticko-bezpečnostná certifikácia):** Agentúra ENISA by plnila viaceré funkcie s osobitnou podporou vnútorného trhu a pokrývala by „monitor trhu“ kybernetickej bezpečnosti prostredníctvom

analýzy relevantných trendov na trhu kybernetickej bezpečnosti s cieľom lepšie zosúladiť dopyt a ponuku, ako aj prostredníctvom podpory rozvoja politiky EÚ v oblastiach normalizácie IKT a certifikácie kybernetickej bezpečnosti IKT. Pokiaľ ide konkrétne o normalizáciu, uľahčovala by vytváranie a zavádzanie kyberneticko-bezpečnostných noriem. Agentúra ENISA by takisto plnila úlohy stanovené v kontexte budúceho rámca pre certifikáciu (pozri oddiel ďalej).

- **Výskum a inovácia:** Agentúra ENISA by prispievala svojimi odbornými znalosťami v podobe poradenstva pre orgány EÚ a členských štátov, pokiaľ ide o stanovenie priorít v oblasti výskumu a vývoja, a to aj v kontexte zmluvného verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti (cPPP). Výskumné poradenstvo agentúry ENISA by sa premietlo do nového Európskeho strediska výskumu a kompetencií pre kybernetickú bezpečnosť v nasledujúcom viacročnom finančnom rámci. Agentúra ENISA by bola na požiadanie Komisie zapojená aj do vykonávania programov EÚ na financovanie výskumu a inovácie.
 - **Operačná spolupráca a krízové riadenie:** táto časť práce by mala byť založená na posilňovaní existujúcich preventívnych operačných spôsobilostí, najmä vylepšením celoeurópskych cvičení v oblasti kybernetickej bezpečnosti (CyberEurope), a to tým, že sa budú uskutočňovať každoročne, a mala by byť založená aj na podpornej úlohe v rámci operačnej spolupráce – ako sekretariát siete jednotiek CSIRT (podľa ustanovení smernice NIS) tým, že sa okrem iného zabezpečí dobré fungovanie IT infraštruktúry a komunikačných kanálov siete jednotiek CSIRT. V tejto súvislosti by sa vyžadovalo nadviazanie štruktúrovanej spolupráce s tímom CERT-EU, Európskym centrom boja proti počítačovej kriminalite (EC3) a inými relevantnými orgánmi EÚ. Štruktúrovaná spolupráca s tímom CERT-EU v tesnej fyzickej blízkosti by okrem toho mala viesť k funkcii poskytovať technickú pomoc v prípade závažných incidentov a podporovať analýzu incidentov. Členské štáty, ktoré by o to požiadali, by získali pomoc na zvládnutie incidentov, ako aj podporu pri analýze zraniteľných miest, artefaktov a incidentov, aby mohli posilniť svoju vlastnú schopnosť prevencie a reakcie.
 - Agentúra ENISA by takisto zohrávala úlohu pri **konceptii kybernetickej bezpečnosti EÚ** predloženej ako súčasť tohto balíka, ktorá predstavuje odporúčanie Komisie členským štátom, aby koordinovane reagovali na rozsiahle cezhraničné kybernetické incidenty a krízy na úrovni EÚ¹³. Agentúra ENISA by napomáhala spoluprácu medzi jednotlivými členskými štátmi pri reakciách na núdzové situácie prostredníctvom analýzy a zoskupovania situačných správ členských štátov na základe informácií, ktoré agentúre dobrovoľne sprístupnili členské štáty a iné subjekty.
- **Certifikácia kybernetickej bezpečnosti produktov a služieb IKT**

¹³

Táto koncepcia sa bude vzťahovať na kybernetické incidenty, ktoré majú za následok praveľké narušenie na to, aby ho ktorýkoľvek členský štát dokázal zvládnuť sám, alebo ktoré má na dva či viaceré členské štáty taký rôznorodý a výrazný dosah alebo má pre ne taký politický význam, že si incidenty vyžadujú správne načasovanú koordináciu politiky a reakciu na politickej úrovni Únie.

V záujme vytvorenia a zachovania dôvery a bezpečnosti je potrebné, aby sa do produktov a služieb IKT priamo začlenili kyberneticko-bezpečnostné prvky už v počiatočných fázach ich technického navrhovania a vývoja (bezpečnosť už v štádiu návrhu – security by design). Okrem toho je potrebné, aby zákazníci a používatelia boli schopní zistiť, akú úroveň bezpečnostnej dôveryhodnosti majú produkty a služby, ktoré si obstarávajú alebo kupujú.

Certifikácia, ktorá pozostáva z formálneho hodnotenia produktov, služieb a procesov nezávislým a akreditovaným subjektom na základe pevne stanovených noriem a kritérií a z vydania certifikátu o súlade, zohráva dôležitú úlohu pri zvyšovaní dôvery v produkty a služby a ich bezpečnosti. Hoci bezpečnostné hodnotenia sú dosť technickou oblasťou, certifikácia slúži na informovanie a uistenie kupujúcich a používateľov o bezpečnostných vlastnostiach produktov a služieb IKT, ktoré nakupujú alebo používajú. Ako sa už uviedlo, platí to predovšetkým pre nové systémy, ktoré v rozsiahlej miere využívajú digitálne technológie a ktoré si vyžadujú vysokú úroveň bezpečnosti, ako napríklad prepojené a automatizované autá, elektronické zdravotníctvo, riadiace systémy priemyselnej automatizácie (IACS)¹⁴ alebo inteligentné siete.

V súčasnosti je situácia v oblasti certifikácie kybernetickej bezpečnosti produktov a služieb IKT v EÚ pomerne nevyrovnaná. Existuje niekoľko medzinárodných iniciatív, ako napríklad tzv. spoločné kritériá hodnotenia bezpečnosti informačných technológií [Common Criteria (CC) for Information Technology Security Evaluation, ISO 15408], ktoré sú medzinárodnou normou na hodnotenie počítačovej bezpečnosti. Vychádzajú z hodnotenia treťou stranou a siedmich stupňov zaručiteľnosti bezpečnosti (EAL). Spoločné kritériá a sprievodná spoločná metodika na hodnotenie bezpečnosti informačných technológií sú technickým základom pre medzinárodnú dohodu, vzájomné uznávanie spoločných kritérií (Common Criteria Recognition Arrangement, CCRA), ktorá zabezpečuje, že certifikáty podľa spoločných kritérií uznávajú všetci signatári dohody CCRA. V súčasnej verzii dohody CCRA sa však vzájomne uznávajú len hodnotenia do 2. stupňa zaručiteľnosti bezpečnosti (EAL 2). Dohodu okrem toho podpísalo len 13 členských štátov.

Certifikačné orgány 12 členských štátov uzavreli dohodu o vzájomnom uznávaní, pokiaľ ide o certifikáty vydané v súlade s dohodou na základe spoločných kritérií¹⁵. V členských štátoch okrem toho v súčasnosti existujú alebo vznikajú viaceré iniciatívy certifikácie IKT. Hoci sú tieto iniciatívy dôležité, predstavujú riziko, že povedú k fragmentácii trhu a k problémom s interoperabilitou. V dôsledku toho možno bude potrebné, aby spoločnosti absolvovali niekoľko certifikačných postupov v rôznych členských štátoch, a až potom budú môcť ponúkať svoje produkty na viacerých trhoch. Napríklad výrobca inteligentných meradiel, ktorý by chcel svoje produkty predávať v troch členských štátoch, napr. v Nemecku, vo Francúzsku a v Spojenom kráľovstve, by mal v súčasnosti dodržiavať tri rôzne systémy certifikácie. Ide o Commercial Product Assurance (CPA) v Spojenom kráľovstve,

¹⁴ GR JRC uverejnilo správu, v ktorej sa navrhuje počiatočný súbor spoločných európskych požiadaviek a hlavné usmernenia týkajúce sa kyberneticko-bezpečnostnej certifikácie zložiek IACS. K dispozícii na adrese: <https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf><https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf>.

¹⁵ Skupina vysokých úradníkov pre bezpečnosť informačných systémov (SOG-IS), ktorá zahŕňa 12 členských štátov a Nórsko, vypracovala niekoľko profilov ochrany pri obmedzenom počte produktov, ako je napríklad digitálny podpis, digitálny tachograf a smart karty. Účastníci spoločne pracujú na koordinácii normalizácie profilov ochrany v rámci spoločných kritérií a koordinujú rozvoj profilov ochrany. Členské štáty často žiadajú certifikáciu SOG-IS pri vnútroštátnych postupoch verejného obstarávania.

Certification de Sécurité de Premier Niveau (CSPN) vo Francúzsku a osobitný profil ochrany založený na spoločných kritériách v Nemecku.

Táto situácia vedie k vyšším nákladom a predstavuje značnú administratívnu záťaž pre spoločnosti pôsobiace vo viacerých členských štátoch. Zatiaľ čo náklady na certifikáciu sa môžu výrazne líšiť v závislosti od príslušného produktu/služby, požadovaného stupňa zaručiteľnosti bezpečnosti a/alebo iných zložiek, vo všeobecnosti sú pre podniky dosť výrazné. Napríklad náklady na certifikát BSI „Smart Meter Gateway“ sú vyššie ako milión eur (najvyššia úroveň testov a dôveryhodnosti, a netýka sa len jedného produktu, ale aj celej súvisiacej infraštruktúry). Náklady na certifikáciu pre inteligentné meradlá v Spojenom kráľovstve predstavujú takmer 150 000 EUR. Vo Francúzsku sú náklady podobné ako v Spojenom kráľovstve, približne 150 000 EUR alebo viac.

Kľúčoví verejní a súkromní aktéri uznali, že v prípade neexistencie systému certifikácie kybernetickej bezpečnosti v celej EÚ musia byť spoločnosti za mnohých okolností certifikované jednotlivo v každom členskom štáte, čo vedie k fragmentácii trhu. Čo je najdôležitejšie, ak neexistujú harmonizačné právne predpisy EÚ pre produkty a služby IKT, rozdiely medzi normami a postupmi certifikácie kybernetickej bezpečnosti v členských štátoch by v praxi mohli viesť k vzniku 28 rôznych bezpečnostných trhov v EÚ, pričom každý z nich by mal svoje vlastné technické požiadavky, testovacie metódy a postupy certifikácie kybernetickej bezpečnosti. Ak sa na úrovni EÚ neprijmú primerané opatrenia, tieto rozdielne prístupy na národnej úrovni môžu byť významnou prekážkou pri dosahovaní jednotného digitálneho trhu a spomaliť prepojené pozitívne účinky z hľadiska rastu a pracovných miest alebo im zabrániť.

Na základe uvedených skutočností sa navrhovaným nariadením zavádza európsky rámec certifikácie kybernetickej bezpečnosti (ďalej len „**rámec**“) produktov a služieb IKT a špecifikujú základné funkcie a úlohy agentúry ENISA v oblasti certifikácie kybernetickej bezpečnosti. V tomto návrhu sa stanovuje celkový rámec pravidiel upravujúcich európske systémy certifikácie kybernetickej bezpečnosti. V návrhu sa priamo nezavádzajú operačné systémy certifikácie, ale skôr vytvára systém (rámec) na stanovenie špecifických systémov certifikácie pre osobitné produkty/služby IKT („európske systémy certifikácie kybernetickej bezpečnosti“). Vytvorenie európskych systémov certifikácie kybernetickej bezpečnosti v súlade s rámcom umožní, aby certifikáty vydané v rámci týchto systémov boli platné a uznávané vo všetkých členských štátoch, a aby sa tak riešila súčasná fragmentácia trhu.

Všeobecným účelom európskeho systému certifikácie kybernetickej bezpečnosti je potvrdiť, že produkty a služby IKT, ktoré boli certifikované v súlade s takýmto systémom, spĺňajú špecifikované kyberneticko-bezpečnostné požiadavky. Zahŕňalo by to napríklad ich schopnosť chrániť údaje (či už údaje uchovávané, prenášané alebo inak spracúvané) pred ich náhodným alebo nepovoleným uchovávaním, spracúvaním, zverejnením, zničením, ich náhodnou stratou či zmenou alebo pred náhodným či nepovoleným prístupom k takýmto údajom. Systémy certifikácie kybernetickej bezpečnosti EÚ by využívali existujúce normy týkajúce sa technických požiadaviek a postupov hodnotenia, ktoré by výrobky mali spĺňať, čiže systémy by technické normy nevyvíjali¹⁶. Certifikácia v celej EÚ pre produkty, ako napríklad smart karty, ktoré sú v súčasnosti testované podľa medzinárodných noriem spoločných kritérií (CC) v rámci multilaterálneho systému SOG-IS (ako sa už uviedlo), by znamenala, že tento systém by sa stal platným v celej EÚ.

¹⁶ V prípade európskych noriem to zabezpečujú európske normalizačné organizácie na základe schválenia Európskou komisiou uverejnením v úradnom vestníku (pozri nariadenie 1025/2012).

V návrhu sa stanovuje osobitný súbor bezpečnostných cieľov, ktoré treba zohľadniť pri tvorbe špecifického európskeho systému certifikácie kybernetickej bezpečnosti, a aj to, čo by takéto systémy prinajmenšom mali obsahovať. Takéto systémy budú musieť okrem iného definovať určitý počet osobitných prvkov vymedzujúcich rozsah a predmet certifikácie kybernetickej bezpečnosti. Patrí sem určenie kategórií dotknutých produktov a služieb, podrobná špecifikácia kyberneticko-bezpečnostných požiadaviek (napríklad s odvolaním na príslušné normy alebo technické špecifikácie), konkrétne hodnotiace kritériá a metódy, ako aj cieľový stupeň dôveryhodnosti, ktorá sa má zabezpečiť: (t. j. základná, pokročilá alebo vysoká).

Európske systémy certifikácie kybernetickej bezpečnosti pripraví agentúra ENISA v úzkej spolupráci s európskou skupinou pre certifikáciu kybernetickej bezpečnosti (pozri nižšie), ktorá bude agentúre poskytovať pomoc a odborné poradenstvo, a Komisia ich prijme prostredníctvom vykonávacích aktov. Ak sa zistí, že je potrebný systém certifikácie kybernetickej bezpečnosti, Komisia požiada agentúru ENISA o vypracovanie systému pre konkrétne produkty alebo služby IKT. Agentúra ENISA bude na danom systéme úzko spolupracovať s vnútroštátnymi orgánmi dohľadu nad certifikáciou zastúpenými v európskej skupine pre certifikáciu kybernetickej bezpečnosti. Členské štáty a uvedená skupina môžu Komisii navrhnúť, aby požiadala agentúru ENISA o vypracovanie určitého systému.

Certifikácia môže byť veľmi nákladný proces, ktorý môže viesť k vyšším cenám pre zákazníkov a spotrebiteľov. Potreba certifikácie sa môže výrazne líšiť aj v závislosti od špecifických podmienok používania produktov a služieb a rýchleho tempa technologických zmien. Využitie európskej kyberneticko-bezpečnostnej certifikácie by preto malo byť aj naďalej dobrovoľné, pokiaľ sa to nestanovuje inak v právnych predpisoch Únie, ktorými sa stanovujú bezpečnostné požiadavky týkajúce sa produktov a služieb IKT.

Aby sa zabezpečila harmonizácia a zabránilo fragmentácii, vnútroštátne systémy alebo postupy certifikácie kybernetickej bezpečnosti produktov a služieb IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, sa prestanú uplatňovať od dátumu stanoveného vo vykonávacom akte, ktorým sa systém prijíma. Členské štáty by okrem toho nemali zavádzať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti tých produktov a služieb IKT, na ktoré sa vzťahuje existujúci európsky systém certifikácie kybernetickej bezpečnosti.

Po prijatí európskeho systému certifikácie kybernetickej bezpečnosti budú môcť výrobcovia produktov IKT alebo poskytovatelia služieb IKT požiadať ktorýkoľvek orgán posudzovania zhody, ktorý si zvolia, o certifikáciu svojich produktov alebo služieb. Orgány posudzovania zhody by mal akreditovať akreditačný orgán, ak spĺňajú určité špecifikované požiadavky. Akreditácia sa vydá najviac na päť rokov, pričom ju možno obnoviť za rovnakých podmienok, pokiaľ orgán posudzovania zhody spĺňa požiadavky. Akreditačné orgány odoberú akreditáciu orgánu posudzovania zhody, ak nie sú alebo prestanú byť splnené akreditačné podmienky, alebo ak kroky daného orgánu posudzovania zhody porušujú toto nariadenie.

Na základe návrhu patria úlohy súvisiace s monitorovaním, dohľadom a presadzovaním do kompetencie členských štátov. Členské štáty budú musieť stanoviť jeden orgán dohľadu nad certifikáciou. Tento orgán bude mať za úlohu dohliadať na to, či sú orgány posudzovania zhody, ako aj certifikáty vydané orgánmi posudzovania zhody so sídlom na ich území, v súlade s požiadavkami tohto nariadenia a príslušnými európskymi systémami certifikácie kybernetickej bezpečnosti. Vnútroštátne orgány dohľadu nad certifikáciou budú mať právomoc vybavovať sťažnosti podané fyzickými alebo právnickými osobami v súvislosti s certifikátmi, ktoré vydali orgány posudzovania zhody so sídlom na ich území. Primerane prešetria predmet danej sťažnosti a sťažovateľa budú v primeranej lehote informovať o pokroku a výsledku tohto prešetrenia. Okrem toho budú spolupracovať s ostatnými orgánmi

dohľadu nad certifikáciou alebo ďalšími verejnými orgánmi, napríklad poskytovaním informácií o možnom nesúlade produktov a služieb IKT s požiadavkami tohto nariadenia alebo s konkrétnymi európskymi systémami certifikácie kybernetickej bezpečnosti.

Napokon sa v návrhu zriaďuje európska skupina pre certifikáciu kybernetickej bezpečnosti (ďalej len „skupina“) zložená z vnútroštátnych orgánov dohľadu nad certifikáciou všetkých členských štátov. Hlavnou úlohou skupiny je poskytovať Komisii poradenstvo v otázkach spojených s politikou certifikácie kybernetickej bezpečnosti a pracovať s agentúrou ENISA na vypracovaní návrhov európskych systémov certifikácie kybernetickej bezpečnosti. Agentúra ENISA bude Komisii pomáhať pri zabezpečovaní služieb sekretariátu skupiny a bude udržiavať aktualizovaný verejný zoznam systémov schválených v európskom rámci certifikácie kybernetickej bezpečnosti. Agentúra ENISA by takisto úzko spolupracovala s normalizačnými orgánmi s cieľom zabezpečiť, aby boli normy používané v schválených systémoch vhodné, ako aj identifikovať oblasti, v ktorých sú potrebné kyberneticko-bezpečnostné normy.

Európsky rámec certifikácie kybernetickej bezpečnosti (ďalej len „rámec“) bude poskytovať občanom a podnikom viaceré prínosy. Konkrétne:

- Vytvorenie špecifických systémov kyberneticko-bezpečnostnej certifikácie pre osobitné produkty alebo služby IKT v celej EÚ poskytne podnikom jednotnú referenciu pre certifikáciu kybernetickej bezpečnosti v Únii. Takéto spoločnosti budú môcť svoj produkt certifikovať iba raz a získať certifikát platný vo všetkých členských štátoch. Nebudú povinné opätovne certifikovať svoje produkty u rôznych vnútroštátnych certifikačných orgánov. Tým sa výrazne znížia náklady pre podniky, podporia cezhraničné operácie a v konečnom dôsledku zníži fragmentácia vnútorného trhu pre príslušné produkty, alebo sa jej zabráni.
- Rámcom sa stanovuje nadradenosť európskych systémov certifikácie kybernetickej bezpečnosti nad vnútroštátnymi systémami: podľa tohto pravidla prijatie európskeho systému certifikácie kybernetickej bezpečnosti nahradí všetky existujúce paralelné vnútroštátne systémy pre tie isté produkty alebo služby IKT na danom stupni dôveryhodnosti. To bude mať za následok lepší prehľad a povedie k zníženiu súčasného veľkého počtu prekrývajúcich sa a niekedy aj protichodných vnútroštátnych systémov certifikácie kybernetickej bezpečnosti.
- Tento návrh takisto podporuje a dopĺňa vykonávanie smernice NIS tým, že podnikom, na ktoré sa daná smernica vzťahuje, poskytuje veľmi užitočný nástroj na preukázanie splnenia požiadaviek v oblasti sieťovej a informačnej bezpečnosti v celej Únii. Komisia a agentúra ENISA budú pri vývoji nových systémov certifikácie kybernetickej bezpečnosti venovať osobitnú pozornosť potrebe zabezpečiť, aby sa v systémoch certifikácie kybernetickej bezpečnosti odzrkadľovali požiadavky smernice NIS.
- Návrhom sa podporí a uľahčí rozvoj európskej politiky v oblasti kybernetickej bezpečnosti zosúladením podmienok a základných požiadaviek týkajúcich sa certifikácie kybernetickej bezpečnosti produktov a služieb IKT v EÚ. Európske systémy certifikácie kybernetickej bezpečnosti budú odkazovať na spoločné normy alebo kritériá hodnotenia a testovacie metódy. To významne, aj keď nepriamo, prispeje k využívaniu spoločných bezpečnostných riešení v EÚ, a tým aj k odstráneniu prekážok na vnútornom trhu.
- Rámec je navrhnutý tak, aby sa ním zabezpečila potrebná pružnosť systémov certifikácie kybernetickej bezpečnosti. V závislosti od konkrétnych kyberneticko-

bezpečnostných potrieb sa môže produkt alebo služba certifikovať na vyššom alebo nižšom stupni zabezpečenia. Európske systémy certifikácie kybernetickej bezpečnosti sa vypracujú so zohľadnením tejto flexibility, a preto budú zabezpečovať rôzne stupne dôveryhodnosti (t. j. základnú, pokročilú alebo vysokú), aby sa mohli použiť na rôzne účely alebo v odlišných kontextoch.

- Všetky uvedené prvky zatriktívnia certifikáciu kybernetickej bezpečnosti pre podniky, keďže bude účinným prostriedkom poskytovania informácií o stupni dôveryhodnosti kybernetickej bezpečnosti produktov alebo služieb IKT. Ak sa kybernetická bezpečnosť stane lacnejšou, účinnejšou a komerčne atraktívnejšou, podniky budú mať väčšie stimuly na certifikovanie svojich produktov proti kyberneticko-bezpečnostným rizikám, čím sa prispeje k šíreniu lepších postupov v oblasti kybernetickej bezpečnosti pri navrhovaní produktov a služieb IKT (kybernetická bezpečnosť už v štádiu návrhu).

- **Súlady s existujúcimi politickými ustanoveniami v tejto oblasti politiky**

Podľa smernice NIS sú prevádzkovatelia pôsobiaci v odvetviach, ktoré sú kľúčové pre naše hospodárstvo a spoločnosť, ako je energetika, doprava, voda, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo a digitálna infraštruktúra, ako aj poskytovatelia digitálnych služieb (vyhľadávače, služby cloud computingu a online trhoviská), povinní prijať opatrenia na vhodné riadenie bezpečnostných rizík. Nové pravidlá tohto návrhu dopĺňajú ustanovenia smernice NIS a zabezpečujú súlad s nimi s cieľom ďalej zvyšovať kybernetickú odolnosť EÚ posilnením spôsobilostí, spolupráce, riadenia rizík a povedomia o kybernetickej bezpečnosti.

Pravidlá certifikácie kybernetickej bezpečnosti okrem toho predstavujú základný nástroj pre spoločnosti, na ktoré sa vzťahuje smernica NIS, keďže budú môcť certifikovať svoje produkty a služby IKT ako odolné proti kyberneticko-bezpečnostným rizikám na základe systémov certifikácie kybernetickej bezpečnosti, ktoré sú platné a uznávané v celej EÚ. Budú takisto doplnkom k bezpečnostným požiadavkám uvedeným v nariadení eIDAS¹⁷ a v smernici o rádiových zariadeniach¹⁸.

- **Súlady s ostatnými politikami Únie**

Nariadením (EÚ) 2016/679 (všeobecné nariadenie o ochrane údajov)¹⁹ sa stanovuje zriadenie certifikačných mechanizmov, pečatí a značiek ochrany údajov na preukázanie súladu spracovateľských operácií prevádzkovateľov a sprostredkovateľov s daným nariadením. Týmto nariadením nie je dotknutá certifikácia operácií spracovania údajov podľa všeobecného nariadenia o ochrane údajov, čo platí aj pre prípady, keď sú takéto operácie súčasťou produktov a služieb.

¹⁷ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

¹⁸ Smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES.

¹⁹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88).

Navrhovaným nariadením sa zabezpečí zlučiteľnosť s nariadením 765/2008 o požiadavkách akreditácie a dohľadu nad trhom²⁰ odvolaním na pravidlá uvedeného rámca, pokiaľ ide o vnútroštátne akreditačné orgány a orgány posudzovania zhody. Pokiaľ ide o orgány dohľadu, navrhovaným nariadením sa od členských štátov bude vyžadovať, aby určili vnútroštátne orgány dohľadu nad certifikáciou, ktorých úlohou by bol dohľad, monitorovanie a presadzovanie pravidiel. Tieto orgány budú aj naďalej oddelené od orgánov posudzovania zhody, ako sa stanovuje v nariadení č. 765/2008.

2. PRÁVNÝ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právny základ

Právnym základom pre opatrenie EÚ je článok 114 Zmluvy o fungovaní Európskej únie (ZFEÚ), ktorý sa týka aproximácie práva členských štátov v záujme dosiahnutia cieľov článku 26 ZFEÚ, t. j. riadneho fungovania vnútorného trhu.

Právny základ vnútorného trhu na zriadenie agentúry ENISA potvrdil Súdny dvor (vo veci C-217/04 Spojené kráľovstvo/Európsky parlament a Rada) a ďalej sa potvrdil v roku 2013 nariadením, ktorým sa stanovil súčasný mandát agentúry. Okrem toho činnosti, v rámci ktorých by sa zohľadňovali ciele posilnenia spolupráce a koordinácie medzi členskými štátmi a ktorými by sa pridávali spôsobilosti na úrovni EÚ na doplnenie opatrení členských štátov, by patrili do kategórie „operačnej spolupráce“. To sa výslovne uvádza v smernici NIS (ktorej právnym základom je článok 114 ZFEÚ) ako cieľ, ktorý sa má sledovať v rámci siete jednotiek CSIRT, pre ktorú „Agentúra ENISA zabezpečuje sekretariát a aktívne podporuje spoluprácu“ (článok 12 ods. 2). Konkrétne v článku 12 ods. 3 písm. f) sa ďalej ako úloha siete jednotiek CSIRT opisuje určenie ďalších foriem operačnej spolupráce, okrem iného aj v súvislosti: i) s kategóriami rizík a incidentov; ii) so včasnými varovaniami; iii) so vzájomnou pomocou; a iv) so zásadami a spôsobmi koordinácie, keď členské štáty reagujú na cezhraničné riziká a incidenty.

- Súčasná fragmentácia systémov certifikácie kybernetickej bezpečnosti produktov a služieb IKT je takisto výsledkom nedostatočného spoločného právne záväzného a účinného rámcového postupu uplatniteľného na členské štáty. To bráni tvorbe vnútorného trhu produktov a služieb IKT a brzdí konkurencieschopnosť európskeho priemyslu v tomto odvetví. Cieľom tohto návrhu je riešiť súčasnú fragmentáciu a súvisiace prekážky pre vnútorný trh, a to zabezpečením spoločného rámca na zriadenie systémov certifikácie kybernetickej bezpečnosti platných v celej EÚ.

Subsidiarita (v prípade inej ako výlučnej právomoci)

Zásada subsidiarity si vyžaduje posúdenie nevyhnutnosti a pridanej hodnoty opatrenia EÚ. Dodržiavanie zásady subsidiarity v tejto oblasti už bolo uznané pri prijímaní súčasného nariadenia o agentúre ENISA²¹.

Kybernetická bezpečnosť je otázkou spoločného záujmu Únie. Siete a informačné systémy sú vzájomne závislé do takej miery, že jednotliví aktéri (verejní a súkromní vrátane občanov) veľmi často nemôžu samostatne čeliť hrozbám kybernetických incidentov a riadiť riziká a

²⁰ Nariadenie (ES) č. 765/2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93.

²¹ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 526/2013 z 21. mája 2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a o zrušení nariadenia (ES) č. 460/2004.

možné vplyvy s nimi spojené. Na jednej strane je verejná intervencia na európskej úrovni nielen priaznivá, ale aj potrebná, a to z dôvodu vzájomnej závislosti členských štátov, aj pokiaľ ide o prevádzku kritických infraštruktúr (napríklad energetika, doprava, voda). Na druhej strane môže zásah EÚ priniesť pozitívny „vedľajší“ účinok šírenia osvedčených postupov medzi členskými štátmi, čo môže mať za následok zvýšenie kybernetickej bezpečnosti Únie.

V súčasnej situácii a pri pohľade na budúce možné scenáre sa zdá, že na **zvýšenie spoločnej kybernetickej odolnosti Únie** nebudú **jednotlivé činnosti členských štátov EÚ a nejednotný prístup ku kybernetickej bezpečnosti** postačovať.

Opatrenia EÚ sa považujú za nevyhnutné aj na riešenie problému fragmentácie súčasných systémov certifikácie kybernetickej bezpečnosti. To by výrobcovi umožnilo v plnej miere využívať výhody vnútorného trhu, pričom by výrazne ušetrili náklady z hľadiska testovania a prepracovania produktov. Hoci napríklad súčasná dohoda skupiny vysokých úradníkov pre bezpečnosť informačných systémov o vzájomnom uznávaní (SOG-IS) v tejto súvislosti dosiahla významné výsledky, ukázali sa aj dôležité obmedzenia, kvôli ktorým nie je úplne vhodná na poskytovanie dlhodobejšie udržateľných riešení pri dosahovaní plného potenciálu vnútorného trhu.

Pridaná hodnota prijatia krokov na úrovni EÚ, najmä s cieľom posilniť spoluprácu medzi členskými štátmi, ale aj medzi komunitami sieťovej a informačnej bezpečnosti, sa uznala v záveroch Rady z roku 2016²² a takisto jasne vyplynula z hodnotenia agentúry ENISA.

- **Proporcionalita**

Navrhnuté opatrenia neprekračujú rámec toho, čo je potrebné na dosiahnutie ich politických cieľov. Okrem toho rozsah intervencie EÚ nebráni prijatiu akýchkoľvek ďalších opatrení jednotlivých štátov v oblasti národnej bezpečnosti. Opatrenia na úrovni EÚ sú preto opodstatnené z hľadiska zásady subsidiarity a proporcionality.

- **Výber nástroja**

Týmto návrhom sa reviduje nariadenie (EÚ) č. 526/2013, ktorým sa stanovuje súčasný mandát a úlohy agentúry ENISA. Vzhľadom na dôležitú úlohu agentúry ENISA pri vytváraní a riadení rámca kyberneticko-bezpečnostnej certifikácie EÚ je okrem toho najlepším riešením stanoviť nový mandát agentúry ENISA a uvedený rámec jediným právnym nástrojom v podobe nariadenia.

3. VÝSLEDKY HODNOTENÍ *EX POST*, KONZULTÁCIÍ SO ZAJINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

Hodnotenia *ex post*/kontroly vhodnosti existujúcich právnych predpisov

Komisia v rámci plánu hodnotenia²³ posudzovala, akú má agentúra **relevantnosť, dosah, efektívnosť, účinnosť koherentnosť a pridanú hodnotu** vzhľadom na jej výsledky, riadenie, vnútornú organizačnú štruktúru a pracovné postupy v období rokov 2013 – 2016.

²² Závery Rady o posilnení odolnosti kybernetického systému a podpore konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe z 15. novembra 2016.

²³ http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

Najdôležitejšie zistenia možno zhrnúť takto (viac informácií sa uvádza v pracovnom dokumente útvarov Komisie o tejto veci, ktorý je pripojený k posúdeniu vplyvu).

- **Relevantnosť:** Vzhľadom na technologický vývoj a vyvíjajúce sa hrozby a vzhľadom na značnú potrebu zvýšenia kybernetickej bezpečnosti v EÚ sa ciele agentúry ENISA ukázali ako relevantné. Členské štáty a orgány EÚ sa opierajú o jej bohaté odborné znalosti otázok kybernetickej bezpečnosti. V členských štátoch treba okrem toho budovať kapacity s cieľom lepšie pochopiť hrozby a reagovať na ne a zainteresované strany by mali spolupracovať naprieč tematickými oblasťami a inštitúciami. Kybernetická bezpečnosť je aj naďalej kľúčovou politickou prioritou EÚ, na ktorú má agentúra ENISA reagovať; koncepcia agentúry ENISA ako agentúry EÚ s časovo obmedzeným mandátom však: i) neumožňuje dlhodobé plánovanie a udržateľnú podporu členských štátov a inštitúcií EÚ; ii) môže viesť k právnemu vákuu, keďže ustanovenia smernice NIS, ktorými sa agentúra ENISA poveruje úlohami, majú trvalý charakter²⁴; iii) nie je koherentná s víziou prepojenia agentúry ENISA s posilneným ekosystémom kybernetickej bezpečnosti EÚ.
- **Účinnosť:** Agentúra ENISA celkovo splnila svoje ciele a úlohy. Prispela k zvýšeniu bezpečnosti sietí a informácií v Európe prostredníctvom jej hlavných činností (budovanie kapacít, poskytovanie odborných znalostí, budovanie komunity a podpora politiky). Ukázalo sa však, že pri každej z činností ešte existuje priestor na zlepšenie. V hodnotení sa dospelo k záveru, že agentúra ENISA účinne vytvorila silné a spoľahlivé vzťahy s niektorými so svojich zainteresovaných strán, predovšetkým s členskými štátmi a spoločenstvom jednotiek CSIRT. Zásahy v oblasti budovania kapacít boli vnímané ako účinné, najmä z pohľadu členských štátov, ktoré disponujú menej zdrojmi. Jedným z najvýznamnejších prvkov bola podpora rozsiahlej spolupráce – zainteresované strany sa všeobecne zhodli v tom, že agentúra ENISA zohráva pozitívnu úlohu pri spájaní ľudí. Agentúra ENISA však čelila problémom pri snahách výrazne zapôsobiť v rozsiahlej oblasti bezpečnosti sietí a informácií. Bolo to aj preto, že pri veľmi rozsiahlom mandáte mala k dispozícii pomerne obmedzené ľudské a finančné zdroje. Hodnotením sa dospelo aj k záveru, že agentúra ENISA splnila svoj cieľ poskytovania odborných znalostí len čiastočne, čo súvisí s problémami pri nábore odborníkov (pozri tiež oddiel nižšie týkajúci sa efektívnosti).
- **Efektívnosť:** Agentúra dokázala napriek obmedzenému rozpočtu – jednému z najnižších v porovnaní s inými agentúrami EÚ, prispieť k cieľom, na ktoré bola zameraná, a celkovo preukázala efektívnosť pri využívaní svojich zdrojov. V hodnotení sa dospelo k záveru, že postupy boli vo všeobecnosti efektívne, a jasné vymedzenie zodpovedností v organizácii viedlo k dobre vykonanej práci. Jednou z hlavných výziev v súvislosti s efektívnosťou agentúry ENISA boli ťažkosti pri nábore a udržaní vysokokvalifikovaných odborníkov. Zo zistení vyplýva, že to možno vysvetliť kombináciou viacerých faktorov, medzi ktoré patria všeobecné ťažkosti verejného sektora konkurovať súkromnému sektoru pri snahe zamestnávať špecializovaných odborníkov, typ zmlúv (na dobu určitú), ktoré mohla agentúra vo väčšine prípadov ponúknuť, a do istej miery aj nízka atraktivita v súvislosti s umiestnením agentúry ENISA (napríklad ťažkosti partnerov zamestnancov nájsť si zamestnanie). Rozdelenie činností medzi Aténami a Heraklionom si vyžadovalo dodatočné úsilie o koordináciu a jeho dôsledkom boli dodatočné náklady, ale

²⁴

Odkaz na články 7, 9, 11, 12, 19 smernice o bezpečnosti sietí a informačných systémov (smernica NIS).

premiestnenie hlavných činností do Atén v roku 2013 zvýšilo prevádzkovú efektívnosť agentúry.

- **Koherentnosť:** Činnosti agentúry ENISA boli vo všeobecnosti v súlade s politikami a činnosťami jej zainteresovaných strán, a to na národnej úrovni aj na úrovni EÚ, ale je potrebný koordinovanejší prístup ku kybernetickej bezpečnosti na úrovni EÚ. Potenciál spolupráce medzi agentúrou ENISA a ďalšími orgánmi EÚ sa nevyužil v plnej miere. V dôsledku vývoja v oblasti právnych predpisov a politiky EÚ je dnes súčasný mandát menej koherentný.
- **Pridaná hodnota pre EÚ:** Pridaná hodnota agentúry ENISA spočíva predovšetkým v schopnosti agentúry posilňovať spoluprácu, a to najmä medzi členskými štátmi, ale aj spoluprácu súvisiacich spoločenstiev sieťovej a informačnej bezpečnosti. Na úrovni EÚ neexistuje žiadny iný aktér, ktorý by podporoval spoluprácu tak rôznorodej škály zainteresovaných strán v oblasti bezpečnosti sietí a informácií. Pridaná hodnota agentúry sa rôznila podľa rozdielnych potrieb a zdrojov jej zainteresovaných strán (napr. veľké členské štáty verzus malé členské štáty; členské štáty verzus odvetvie) a podľa potreby agentúry stanoviť priority pre svoje činnosti na základe pracovného programu. V hodnotení sa dospelo k záveru, že prípadné zrušenie agentúry ENISA by znamenalo premárnenú príležitosť pre všetky členské štáty. Zabezpečiť rovnaký stupeň budovania komunity a spolupráce medzi členskými štátmi v oblasti kybernetickej bezpečnosti nebude možné. Bez centralizovanejšej agentúry EÚ by bola celková situácia rozdrobenejšia a na prázdne miesto po agentúre ENISA by nastúpila bilaterálna alebo regionálna spolupráca.

S osobitným zreteľom na minulú prácu aj na budúcnosť agentúry ENISA z procesu konzultácií v roku 2017 vyplynuli tieto hlavné trendy²⁵:

- Celkové výsledky agentúry ENISA v období rokov 2013 – 2016 pozitívne hodnotila väčšina respondentov (74 %). Väčšina respondentov sa ďalej domnievala, že agentúra ENISA dosahuje svoje konkrétne ciele (aspoň 63 % v prípade každého z cieľov). Služby a produkty agentúry ENISA pravidelne (mesačne alebo častejšie) používala takmer polovica respondentov (46 %) a tieto služby a produkty respondenti oceňujú kvôli tomu, že pochádzajú od orgánu na úrovni EÚ (83 %) a kvôli ich kvalite (62 %).
- Respondenti uviedli viaceré nedostatky a výzvy pre budúcnosť kybernetickej bezpečnosti v EÚ, najmä týchto päť hlavných (spolu ich bolo šesťnásť): spolupráca medzi členskými štátmi; kapacita na predchádzanie, odhaľovanie a riešenie rozsiahlych kybernetických útokov; spolupráca medzi členskými štátmi v záležitostiach týkajúcich sa kybernetickej bezpečnosti; spolupráca a výmena informácií medzi rôznymi zainteresovanými stranami vrátane spolupráce medzi

²⁵

Na konzultáciu odpovedalo 90 zainteresovaných strán z 19 členských štátov (88 odpovedí a 2 pozičné dokumenty) vrátane národných orgánov z 15 členských štátov vrátane Francúzska, Talianska, Írska a Grécka a 8 organizácií zastupujúcich značný počet európskych organizácií, napríklad Európska banková federácia, Digital Europe (digitálna Európa, zastupujúca odvetvie digitálnych technológií v Európe), Združenie európskych prevádzkovateľov telekomunikačných sietí (ETNO). Verejná konzultácia o agentúre ENISA bola doplnená o niekoľko ďalších zdrojov vrátane: i) podrobných rozhovorov s približne 50 kľúčovými aktérmi z komunity kybernetickej bezpečnosti; ii) prieskumu v sieti jednotiek CSIRT; iii) prieskumu v správnej rade, výkonnej rade, stálej skupine zainteresovaných strán agentúry ENISA.

verejným a súkromným sektorom; ochrana kritickej infraštruktúry pred kybernetickými útokmi.

- Veľká väčšina (88 %) respondentov sa domnievala, že súčasné nástroje a mechanizmy, ktoré sú k dispozícii na úrovni EÚ, sú pri riešení uvedených nedostatkov a výziev nedostatočné alebo postačujú len čiastočne. Veľká väčšina respondentov (98 %) uviedla, že na tieto potreby by mal reagovať orgán EÚ a 99 % z nich by na tento účel vybralo agentúru ENISA.

Konzultácie so zainteresovanými stranami

- Komisia zorganizovala od 12. apríla do 5. júla 2016 verejnú konzultáciu na preskúmanie agentúry ENISA a dostala 421 odpovedí²⁶. Podľa výsledkov 67,5 % respondentov vyjadrilo názor, že agentúra ENISA by mohla zohrávať úlohu pri stanovovaní harmonizovaného rámca bezpečnostnej certifikácie produktov a služieb IT.

Z výsledkov konzultácie z roku 2016 o zmluvnom verejno-súkromnom partnerstve v oblasti kybernetickej bezpečnosti (cPPP)²⁷, pokiaľ ide o certifikáciu, vyplýva:

- 50,4 % (t. j. 121 z 240) respondentov nevie, či sú vnútroštátne systémy certifikácie vzájomne uznávané vo všetkých členských štátoch EÚ. 25,8 % (62 z 240) odpovedalo „nie“, zatiaľ čo 23,8 % (57 z 240) odpovedalo „áno“.
- 37,9 % respondentov (91 z 240) si myslí, že existujúce systémy certifikácie nepodporujú potreby európskeho priemyslu. Na druhej strane opačný názor vyjadrilo 17,5 % respondentov (42 z 240), predstavujúcich najmä globálne spoločnosti pôsobiace na európskom trhu.
- 49,6 % (119 z 240) respondentov tvrdí, že preukázať rovnocennosť noriem, systémov certifikácie a označení nie je ľahké. 37,9 % (91 z 240) odpovedalo „neviem“, zatiaľ čo iba 12,5 % (30 z 240) odpovedalo „áno“.

Získavanie a využívanie expertízy

Komisia vychádzala z tohto externého odborného poradenstva:

- Štúdia o hodnotení ENISA (Ramboll/Carsa 2017; SMART č. 2016/0077),
- Štúdia o bezpečnostnej certifikácii a označovaní IKT – zhromažďovanie dôkazov a hodnotenie vplyvu (PriceWaterhouseCoopers 2017; SMART č. 2016/0029).

Posúdenie vplyvu

- V správe o posúdení vplyvu tejto iniciatívy sa identifikovali tieto hlavné problémy, ktoré je potrebné riešiť:

²⁶ 162 príspevkov pochádzalo od občanov, 33 od organizácií občianskej spoločnosti a spotrebiteľských organizácií; 186 od odvetvia a 40 od orgánov verejnej moci vrátane príslušných orgánov presadzujúcich smernicu o súkromí a elektronických komunikáciách.

²⁷ Na oddiel o certifikácii reagovalo 240 zainteresovaných strán z radov vnútroštátnych verejných správ, veľkých podnikov, MSP, mikropodnikov a výskumných orgánov.

- fragmentácia politik a prístupov ku kybernetickej bezpečnosti v jednotlivých členských štátoch;
- rozptýlené vynakladanie zdrojov a fragmentácia prístupov ku kybernetickej bezpečnosti v rámci inštitúcií, agentúr a orgánov EÚ a
- nedostatočné povedomie a informovanosť občanov a spoločností spolu s narastajúcim množstvom systémov certifikácie jednotlivých členských štátov a odvetví.

V správe sa posudzovali tieto možnosti so zreteľom na mandát agentúry ENISA:

- zachovanie súčasného stavu, to znamená, že predĺžený mandát by bol stále časovo obmedzený (východisková možnosť);
- ukončenie súčasného mandátu agentúry ENISA bez predĺženia a ukončenie činnosti agentúry ENISA (bez zásahu);
- „reformovaná agentúra ENISA“ a
- agentúra EÚ pre kybernetickú bezpečnosť s plnými operačnými spôsobilosťami.

V správe sa posudzovali tieto možnosti so zreteľom na certifikáciu kybernetickej bezpečnosti:

- bez zásahu (východisková možnosť);
- nelegislatívne opatrenia (právne nezáväzné, „soft law“);
- legislatívny akt EÚ s cieľom vytvoriť povinný systém pre všetky členské štáty na základe systému SOG-IS a
- všeobecný rámec certifikácie kybernetickej bezpečnosti IKT v EÚ.

V analýze sa dospelo k záveru, že uprednostňovanou možnosťou je „reformovaná agentúra ENISA“ v kombinácii so všeobecným rámcom certifikácie kybernetickej bezpečnosti IKT v EÚ.

Usúdilo sa, že táto uprednostňovaná možnosť je pre EÚ najúčinnnejšia na dosiahnutie stanovených cieľov, ktorými sú: zvyšovanie spôsobilostí, pripravenosti, spolupráce, informovanosti, transparentnosti a zabráňovanie fragmentácii trhu v oblasti kybernetickej bezpečnosti. Taktiež sa vyhodnotila ako najkoherentnejšia s politickými prioritami stratégie kybernetickej bezpečnosti EÚ a súvisiacich politik (napr. smernice NIS) a so stratégiou digitálneho jednotného trhu. Z konzultačného procesu vyplynulo aj to, že táto uprednostňovaná možnosť sa teší podpore väčšiny zainteresovaných strán. Okrem toho sa pri analýze uskutočnenej v rámci posúdenia vplyvu ukázalo, že uprednostňovanou možnosťou by sa ciele dosiahli s rozumným vynaložením zdrojov.

Výbor Komisie pre kontrolu regulácie vydal najskôr 24. júla negatívne stanovisko, neskôr 25. augusta 2017 kladné stanovisko na základe opätovného predloženia. Pozmenená správa o posúdení vplyvu zahŕňala dodatočné podporné dôkazy, konečné závery hodnotenia agentúry ENISA a dodatočné vysvetlenia politických možností a ich vplyvu. Príloha 1 k záverečnej správe o posúdení vplyvu obsahuje zhrnutie toho, ako sa zohľadnili pripomienky výboru v druhom stanovisku. Správa sa aktualizovala s cieľom zahrnúť do nej podrobnejšie súvislosti kybernetickej bezpečnosti EÚ vrátane opatrení, ktoré sú uvedené v spoločnom oznámení s názvom „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ“ [JOIN(2017) 450]] a ktoré majú pre agentúru ENISA osobitný význam: koncepcia kybernetickej bezpečnosti EÚ a Európske stredisko výskumu a kompetencií pre kybernetickú

bezpečnosť, s ktorým by agentúra spojila svoje poradenstvo týkajúce sa potrieb výskumu v EÚ.

V správe sa uvádza, ako by táto reforma agentúry vrátane nových úloh, lepších podmienok zamestnávania a štrukturálnej spolupráce s orgánmi EÚ v tejto oblasti zlepšila jej príťažlivosť ako zamestnávateľa a pomohla riešiť problémy týkajúce sa náboru odborníkov. V prílohe 6 k správe je predstavený aj revidovaný odhad nákladov súvisiacich s rôznymi politickými možnosťami v prípade agentúry ENISA. Z hľadiska certifikácie sa správa zrevidovala s cieľom poskytnúť podrobnejšie vysvetlenie s grafickým znázornením uprednostňovanej možnosti, ako aj s cieľom poskytnúť odhady nákladov pre členské štáty a Komisiu v súvislosti s novým rámcom certifikácie. Výber agentúry ENISA ako kľúčového aktéra v danom rámci sa odôvodnil odbornosťou agentúry v danej oblasti a skutočnosťou, že na úrovni EÚ je jedinou agentúrou pre kybernetickú bezpečnosť. Oddiely týkajúce sa certifikácie sa preskúmali s cieľom objasniť aspekty súvisiace s rozdielom oproti súčasnemu systému SOGIS a výhody spojené s rôznymi politickými možnosťami a s cieľom vysvetliť, že druh produktov a služieb IKT, na ktoré sa vzťahuje európsky systém certifikácie, sa vymedzí v samotnom schválenom systéme.

Regulačná vhodnosť a zjednodušenie

Neuplatňuje sa.

Dosah na základné práva

Kybernetická bezpečnosť zohráva dôležitú úlohu pri ochrane súkromia a osobných údajov jednotlivcov v súlade s článkami 7 a 8 Charty základných práv EÚ. V prípade kybernetických incidentov jasne dochádza k vystaveniu súkromia a ochrany našich osobných údajov. Kybernetická bezpečnosť je preto nevyhnutnou podmienkou na rešpektovanie súkromia a dôvernosti našich osobných údajov. Z tohto pohľadu a so zameraním na posilnenie kybernetickej bezpečnosti v Európe je tento návrh dôležitým doplnkom existujúcich právnych predpisov chrániacich základné právo na súkromie a ochranu osobných údajov. Kybernetická bezpečnosť je dôležitá aj na ochranu dôvernosti našej elektronickej komunikácie, a preto aj pre uplatňovanie slobody prejavu a práva na informácie a ďalších súvisiacich práv, ako je sloboda myslenia, svedomia a náboženského vyznania.

4. VPLYV NA ROZPOČET

Pozri finančný výkaz.

5. ĎALŠIE PRVKY

• Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ

Komisia bude monitorovať uplatňovanie nariadenia a každých päť rokov predloží hodnotiacu správu Európskemu parlamentu, Rade a Európskemu hospodárskemu a sociálnemu výboru. Tieto správy budú verejné a budú sa týkať účinného uplatňovania a presadzovania tohto nariadenia.

- **Podrobné vysvetlenie konkrétnych ustanovení návrhu**

Hlava I tohto nariadenia obsahuje všeobecné ustanovenia: predmet úpravy (článok 1), vymedzenie pojmov (článok 2) vrátane odkazov na príslušné vymedzenia pojmov z ostatných nástrojov EÚ, ako je napríklad smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (smernica NIS), nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93, a nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 o európskej normalizácii.

Hlava II nariadenia obsahuje kľúčové ustanovenia týkajúce sa agentúry ENISA, Agentúry EÚ pre kybernetickú bezpečnosť.

V kapitole I tejto hlavy sa stanovuje mandát (článok 3), ciele (článok 4) a úlohy agentúry (články 5 až 11).

V kapitole II sa opisuje organizácia agentúry ENISA a kľúčové ustanovenia o jej štruktúre (článok 12). Zameriava sa na zloženie, pravidlá hlasovania a funkcie správnej rady (oddiel 1, články 13 až 17), výkonnej rady (oddiel 2, článok 18) a výkonného riaditeľa (oddiel 3, článok 19). Obsahuje aj ustanovenia o zložení a úlohe stálej skupiny zainteresovaných strán (oddiel 4, článok 20). V neposlednom rade sa v oddiele 5 tejto kapitoly podrobne uvádzajú pravidlá týkajúce sa činnosti agentúry, a to aj pokiaľ ide o plánovanie činností, konflikt záujmov, transparentnosť, dôvernosc a prístup k dokumentom (články 21 – 25).

Kapitola III sa týka zostavovania a štruktúry rozpočtu agentúry (články 26 a 27), ako aj pravidiel upravujúcich jeho plnenie (články 28 a 29). Obsahuje aj ustanovenia na uľahčenie boja proti podvodom, korupcii a iným nezákonným činnostiam (článok 30).

Kapitola IV sa týka personálu agentúry. Sú v nej uvedené všeobecné ustanovenia týkajúce sa služobného poriadku, podmienok zamestnávania a pravidiel upravujúcich výsady a imunity (článok 31 a 32). Podrobne sa v nej opisujú aj pravidlá výberu a vymenovania výkonného riaditeľa agentúry (článok 33). V neposlednom rade obsahuje ustanovenia, ktorými sa riadi využívanie vyslaných národných expertov alebo ďalších pracovníkov, ktorých agentúra nezamestnáva (článok 34).

Kapitola V obsahuje všeobecné ustanovenia týkajúce sa agentúry. Uvádza sa v nej právne postavenie (článok 35) a zahŕňa aj ustanovenia týkajúce sa otázok zodpovednosti, pravidiel používania jazykov, ochrany osobných údajov (články 36 – 38), ako aj bezpečnostné predpisy v oblasti ochrany utajovaných skutočností a citlivých neutajovaných skutočností (článok 40). Opisujú sa v nej pravidlá spolupráce agentúry s tretími krajinami a medzinárodnými organizáciami (článok 39). V neposlednom rade obsahuje aj ustanovenia týkajúce sa sídla agentúry a jej prevádzkových podmienok, ako aj administratívnej kontroly zo strany ombudsmana (články 41 a 42).

V hlave III nariadenia sa zriaďuje európsky rámec kyberneticko-bezpečnostnej certifikácie (ďalej len „**rámec**“) pre produkty a služby IKT ako *lex generalis* (článok 1). Vymedzuje sa v nej všeobecný účel európskych systémov certifikácie kybernetickej bezpečnosti, t. j. zabezpečiť, aby produkty a služby IKT spĺňali konkrétne kyberneticko-bezpečnostné požiadavky z hľadiska ich schopnosti na určitom stupni dôveryhodnosti odolať konaniu s cieľom ohroziť dostupnosť, pravosť, integritu a dôvernosc uložených, prenášaných alebo spracúvaných údajov alebo súvisiacich funkcií alebo služieb (článok 43). Okrem toho sa v nej uvádzajú ciele v oblasti bezpečnosti, na ktoré sa plánujú zamerať európske systémy certifikácie kybernetickej bezpečnosti (článok 45), ako je okrem iného schopnosť chrániť údaje pred náhodným alebo nepovoleným únikom, zničením či zmenou alebo pred náhodným

či nepovoleným prístupom k takýmto údajom, a obsah (t. j. prvky) európskych systémov certifikácie kybernetickej bezpečnosti, ako je podrobná špecifikácia rozsahu ich pôsobnosti, bezpečnostné ciele, hodnotiace kritériá atď. (článok 47).

V hlave III sa stanovujú aj hlavné právne účinky európskych systémov certifikácie kybernetickej bezpečnosti, a to i) povinnosť uplatniť systém na vnútroštátnej úrovni a dobrovoľný charakter certifikácie; ii) anulujúci účinok európskych systémov certifikácie kybernetickej bezpečnosti na vnútroštátne systémy v prípade rovnakých produktov alebo služieb (články 48 a 49).

V tejto hlave sa ďalej stanovuje postup na prijatie európskych systémov certifikácie kybernetickej bezpečnosti a príslušné úlohy Komisie, agentúry ENISA a európskej skupiny pre certifikáciu kybernetickej bezpečnosti (ďalej len „skupina“) (článok 44). Obsahuje aj ustanovenia o orgánoch posudzovania zhody vrátane ich povinností, právomocí a úloh, o vnútroštátnych orgánoch dohľadu nad certifikáciou, ako aj o sankciách.

Skupina sa v tejto v tejto hlave stanovuje ako významný orgán zložený zo zástupcov vnútroštátnych orgánov dohľadu nad certifikáciou, ktorého hlavnou funkciou je pracovať spoločne s agentúrou ENISA na príprave európskych systémov certifikácie kybernetickej bezpečnosti a poskytovať Komisii poradenstvo v súvislosti so všeobecnými alebo osobitnými problémami týkajúcimi sa politiky v oblasti kyberneticko-bezpečnostnej certifikácie.

Hlava IV nariadenia obsahuje záverečné ustanovenia, v ktorých sa opisuje vykonávanie delegovania právomoci, požiadavky na hodnotenie, zrušenie a nástupníctvo, ako aj nadobudnutie účinnosti.

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“)

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,
so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,
so zreteľom na návrh Európskej komisie,
po postúpení návrhu legislatívneho aktu národným parlamentom,
so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru²⁸,
so zreteľom na stanovisko Výboru regiónov²⁹,
konajúc v súlade s riadnym legislatívnym postupom,
keďže:

- (1) Siete, informačné systémy a telekomunikačné siete a služby sú pre našu spoločnosť kľúčové a stali sa oporným pilierom hospodárskeho rastu. Na informačných a komunikačných technológiách sú založené komplexné systémy, ktoré podporujú spoločenské činnosti, udržujú chod kľúčových odvetví hospodárstva ako zdravotníctvo, energetika, financie či doprava, a najmä podporujú fungovanie vnútorného trhu.
- (2) Občania, firmy i verejné orgány v Únii dnes využívajú siete a informačné systémy na každom kroku. Digitalizácia a prepojenie sa stávajú samozrejmosťou pre čoraz viac produktov a služieb, pričom sa očakáva, že s nástupom internetu vecí (IoT) prídu na trh EÚ v najbližšom desaťročí milióny, ak nie miliardy prepojených digitálnych zariadení. Na internet je pripojených čoraz viac zariadení, no ich bezpečnosť a odolnosť nie je vo fáze navrhovania dostatočne zohľadnená, čo vedie k nedostatočnej kybernetickej bezpečnosti. Keďže certifikácia sa v tomto kontexte využíva obmedzene, organizácie a jednotliví používatelia nie sú dostatočne informovaní o prvkoch kybernetickej bezpečnosti produktov a služieb IKT, čo znižuje dôveru v digitálne riešenia.
- (3) Rastúca miera digitalizácie a prepojenia zvyšuje kyberneticko-bezpečnostné riziká, takže spoločnosť ako taká je zraniteľnejšia voči kybernetickým hrozbám a prehľbuje sa nebezpečenstvo pre jednotlivcov vrátane zraniteľných skupín ako deti. V záujme zmiernenia rizík pre spoločnosť treba prijať všetky potrebné kroky na zvýšenie

²⁸ Ú. v. EÚ C , , s. .

²⁹ Ú. v. EÚ C , , s. .

kybernetickej bezpečnosti v EÚ, aby boli siete a informačné systémy, telekomunikačné siete, digitálne produkty, služby a zariadenia, ktoré využívajú občania, verejné správy i podniky – od MSP až po prevádzkovateľov kritickej infraštruktúry – lepšie chránené pred kybernetickými hrozbami.

- (4) Kybernetické útoky sú na vzostupe, takže potrebujeme lepšie brániť prepojené hospodárstvo a spoločnosť, ktoré sú voči kybernetickým hrozbám a útokom zraniteľnejšie. Zatiaľ čo kybernetické útoky sú často cezhraničné, politická reakcia orgánov zodpovedných za kybernetickú bezpečnosť a orgánov presadzovania práva prebieha prevažne na vnútroštátnej úrovni. Rozsiahle kybernetické incidenty by mohli narušiť poskytovanie základných služieb v celej EÚ. Táto situácia si vyžaduje účinnú reakciu a krízové riadenie na úrovni EÚ vychádzajúce z osobitných politík a všeobecnejších nástrojov pre európsku solidaritu a vzájomnú pomoc. Okrem toho je pre tvorcov politík, priemysel a používateľov dôležité pravidelné posudzovanie stavu kybernetickej bezpečnosti a odolnosti v Únii založené na spoľahlivých údajoch Únie, ako aj systematická predpoveď budúceho vývoja, výziev a hrozieb, a to tak na úrovni Únie, ako aj celosvetovo.
- (5) Keďže výzvy, ktorým Únia v oblasti kybernetickej bezpečnosti čelí, sa stupňujú, je potrebný komplexný súbor opatrení, ktoré nadviažu na predošlé kroky Únie a zaisťujú synergiu cieľov. Zahŕňa to potrebu ďalej posilniť spôsobilosti a pripravenosť členských štátov i podnikov, ako aj zlepšiť spoluprácu a koordináciu medzi členskými štátmi a inštitúciami, agentúrami a orgánmi EÚ. Okrem toho keďže kybernetické hrozby nepoznajú hranice, treba posilniť spôsobilosť na úrovni Únie, aby mohla doplniť opatrenia členských štátov, najmä pri rozsiahlych cezhraničných kybernetických incidentoch a krízach. Viac treba urobiť aj v otázke informovanosti občanov a podnikov o otázkach kybernetickej bezpečnosti. Transparentné informácie o úrovni bezpečnosti produktov a služieb IKT by navyše mohli posilniť celkovú dôveru v digitálny jednotný trh. Tento cieľ môže uľahčiť celouúijná certifikácia, ktorá poskytne spoločné kyberneticko-bezpečnostné požiadavky a kritériá hodnotenia naprieč vnútroštátnymi trhmi a odvetviami.
- (6) Európsky parlament a Rada prijali v roku 2004 nariadenie (ES) č. 460/2004³⁰ o zriadení agentúry ENISA, ktoré malo prispieť k cieľom v oblasti zabezpečenia vysokej úrovne sieťovej a informačnej bezpečnosti v rámci Únie a vybudovaniu kultúry sieťovej a informačnej bezpečnosti v prospech občanov, spotrebiteľov, podnikov a verejnej správy. V roku 2008 prijal Európsky parlament a Rada nariadenie (ES) č. 1007/2008³¹, ktorým sa predĺžil mandát agentúry do marca 2012. Nariadením (ES) č. 580/2011³² sa tento mandát agentúry ďalej predĺžil do 13. septembra 2013. V roku 2013 prijal Európsky parlament a Rada nariadenie (EÚ) č. 526/2013³³ o Agentúre

³⁰ 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).

³¹ 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, s. 1).

³² Nariadenie Európskeho parlamentu a Rady (EÚ) č. 580/2011 z 8. júna 2011, ktorým sa mení a dopĺňa nariadenie (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, pokiaľ ide o jej trvanie (Ú. v. EÚ L 165, 24.6.2011, s. 3).

³³ Nariadenie Európskeho parlamentu a Rady (EÚ) č. 526/2013 z 21. mája 2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a o zrušení nariadenia (ES) č. 460/2004 (Ú. v. EÚ L 165, 18.6.2013, s. 41).

ENISA a o zrušení nariadenia (ES) č. 460/2004, ktorým sa mandát agentúry predĺžil do júna 2020.

- (7) Únia už prijala dôležité kroky na zaistenie kybernetickej bezpečnosti a zvýšenie dôvery v digitálne technológie. V roku 2013 bola prijatá stratégia kybernetickej bezpečnosti EÚ, ktorá má viesť politickú reakciu Únie na kybernetické hrozby a riziká. V snahe lepšie chrániť Európanov v online svete prijala Únia v roku 2016 prvý legislatívny akt v oblasti kybernetickej bezpečnosti, a to smernicu (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (tzv. smernica NIS). V smernici NIS sa stanovujú požiadavky na vnútroštátne spôsobilosti v oblasti kybernetickej bezpečnosti, zriaďujú sa prvé mechanizmy na posilnenie strategickej a operačnej spolupráce členských štátov a zavádzajú sa povinnosti prijímať bezpečnostné opatrenia a oznamovať incidenty v odvetviach, ktoré sú pre hospodárstvo a spoločnosť kľúčové (ako energetika, doprava, voda, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, digitálna infraštruktúra), ako aj v prípade kľúčových poskytovateľov digitálnych služieb (vyhľadávače, služby cloud computingu a online trhoviská). Agentúre ENISA bola zverená kľúčová rola podpory vykonávania smernice NIS. Účinný boj proti počítačovej kriminalite je navyše dôležitou prioritou Európskeho programu v oblasti bezpečnosti a prispieva k celkovému cieľu vysokej úrovne kybernetickej bezpečnosti.
- (8) Je zrejmé, že od prijatia stratégie kybernetickej bezpečnosti EÚ v roku 2013 a od posledného prehodnotenia mandátu agentúry sa celkový politický kontext výrazne zmenil, a to aj z hľadiska neistejšieho a menej bezpečného globálneho prostredia. V tejto súvislosti a v rámci novej kyberneticko-bezpečnostnej politiky Únie treba mandát agentúry ENISA zrevidovať s cieľom vymedziť jej rolu v zmenenom ekosystéme kybernetickej bezpečnosti, aby účinne prispievala k reakcii Únie na výzvy v tejto sfére vyplývajúce z tejto radikálne zmenenej povahy hrozieb, keďže ako potvrdilo hodnotenie samotnej agentúry, jej súčasný mandát na to nestačí.
- (9) Agentúra zriadená týmto nariadením by mala byť nástupcom agentúry ENISA zriadenej nariadením (EÚ) č. 526/2013. Agentúra by mala vykonávať úlohy zverené týmto nariadením a právnymi aktmi Únie v oblasti kybernetickej bezpečnosti, okrem iného ako zdroj odborných poznatkov a poradenstva, ale i centrum informácií a znalostí v rámci Únie. Mala by podporovať výmenu osvedčených postupov medzi členskými štátmi a súkromnými aktérmi, ponúkať Európskej komisii a členským štátom politické návrhy, pôsobiť ako referenčný bod pre odvetvové politické iniciatívy Únie v otázkach kybernetickej bezpečnosti a podnecovať operačnú spoluprácu medzi členskými štátmi navzájom i vo vzťahu k inštitúciám, agentúram a orgánom EÚ.
- (10) V rozhodnutí 2004/97/ES, Euratom prijatom na zasadnutí Európskej rady 13. decembra 2003 zástupcovia členských štátov rozhodli, že agentúra ENISA má mať sídlo v gréckom meste, ktoré určí grécka vláda. Hostiteľský členský štát agentúry by mal zabezpečiť čo najlepšie podmienky pre bezproblémové a efektívne fungovanie agentúry. Pre riadne a efektívne plnenie jej úloh, prijímanie a udržanie zamestnancov a zvýšenie efektívnosti nadväzovania vzťahov je nevyhnutné, aby agentúra sídlila na vhodnom mieste, ktoré okrem iného poskytuje vhodné dopravné spojenia a zariadenia pre manželov (manželky) a deti sprevádzajúce zamestnancov agentúry. Potrebné opatrenia by sa mali stanoviť v dohode medzi agentúrou a hostiteľským členským štátom uzavretou po získaní súhlasu správnej rady agentúry.

- (11) Keďže Únia čelí narastajúcim kyberneticko-bezpečnostným výzvam, mal by sa zvýšiť objem finančných a ľudských zdrojov pridelených agentúre, aby sa odzrkadlilo jej posilnené poslanie a úlohy a jej rozhodujúce postavenie v ekosystéme organizácií brániacich európsky digitálny ekosystém.
- (12) Agentúra by mala zabezpečiť a udržiavať špičkové odborné poznatky a pôsobiť ako referenčný bod budujúci dôveru v jednotný trh svojou nezávislosťou, kvalitou poskytovaného poradenstva a šírených informácií, transparentnosťou svojich postupov a pracovných metód a dôslednosťou pri vykonávaní úloh. Agentúra by mala proaktívne prispievať k snahám členských štátov i Únie a mala by vykonávať svoje úlohy v plnej spolupráci s inštitúciami, orgánmi, úradmi a agentúrami Únie a s členskými štátmi. Okrem toho by agentúra mala nadväzovať na vstupy zo súkromného sektora a od ďalších relevantných zainteresovaných strán a na spoluprácu s nimi. Mal by sa stanoviť súbor úloh určujúcich, ako agentúra dosiahne svoje ciele, ktorý by mal umožniť flexibilitu jej činnosti.
- (13) Agentúra by mala pomáhať Komisii poskytovaním poradenstva, stanovísk a analýz týkajúcich sa všetkých záležitostí Únie súvisiacich s vývojom, ako aj s tvorbou, aktualizáciou a revíziou politík a právnych predpisov v oblasti kybernetickej bezpečnosti vrátane ochrany kritickej infraštruktúry a kybernetickej odolnosti. Agentúra by mala byť referenčným bodom poradenstva a odborných poznatkov pre odvetvové politické a legislatívne iniciatívy Únie zahŕňajúce rozmer kybernetickej bezpečnosti.
- (14) Základnou úlohou agentúry je presadzovať dôsledné vykonávanie príslušného právneho rámca, a najmä účinné vykonávanie smernice NIS, ktorá je kľúčom k posilneniu kybernetickej odolnosti. Keďže kybernetické hrozby sú neustále v pohybe, je jasné, že členské štáty potrebujú podporu komplexnejšieho prierezového prístupu k budovaniu kybernetickej odolnosti.
- (15) Agentúra by mala pomáhať členským štátom a inštitúciám, orgánom, úradom a agentúram Únie v ich úsilí vybudovať a zdokonaľovať spôsobilosti a pripravenosť predchádzať kyberneticko-bezpečnostným problémom a incidentom spojeným s bezpečnosťou sietí a informačných systémov, odhaľovať ich a reagovať na ne. Najmä by agentúra mala podporovať rozvoj a posilňovanie vnútroštátnych jednotiek CSIRT, aby v rámci Únie všetky dosiahli vysoký stupeň vývoja. Zároveň by agentúra mala pomáhať pri príprave a aktualizácii stratégií Únie a členských štátov v oblasti bezpečnosti sietí a informačných systémov (najmä kybernetickej), podporovať ich šírenie a sledovať pokrok v ich uplatňovaní. Mala by tiež verejným orgánom ponúkať školenia a vzdelávacie materiály a podľa potreby „školiť školiteľov“, aby členským štátom pomohla pri rozvoji ich vlastných školiacich kapacít.
- (16) Agentúra by mala pomáhať skupine pre spoluprácu zriadenej smernicou NIS pri výkone jej úloh, a to najmä poskytovaním odborných poznatkov, poradenstva a sprostredkovaním výmeny osvedčených postupov, predovšetkým z hľadiska identifikácie prevádzkovateľov základných služieb členskými štátmi z pohľadu rizík a incidentov, a to aj v súvislosti s cezhraničnou previazanosťou.
- (17) Na stimulovanie spolupráce verejného a súkromného sektora a v rámci súkromného sektora, a najmä na podporu ochrany kritických infraštruktúr by agentúra mala podporovať zriaďovanie odvetvových stredísk pre výmenu a analýzu informácií (ISAC), a to poskytovaním osvedčených postupov a usmernení k existujúcim nástrojom a postupom, ako aj usmerňovaním v otázke riešenia regulačných problémov spojených s výmenou informácií.

- (18) Agentúra by mala zhromažďovať a analyzovať správy vnútroštátnych jednotiek CSIRT a tímu CERT-EU a stanoviť spoločné pravidlá, jazyk a terminológiu na výmenu informácií. Okrem toho by agentúra mala angažovať súkromný sektor v zmysle smernice NIS, ktorá zriadením siete jednotiek CSIRT stanovila základ pre dobrovoľnú výmenu technických informácií na operačnej úrovni.
- (19) Agentúra by mala prispievať k reakcii na úrovni EÚ v prípade rozsiahlych cezhraničných kybernetických incidentov a kríz. Do tejto úlohy spadá aj zber relevantných informácií a uľahčovanie interakcie medzi sieťou jednotiek CSIRT a technickou obcou či aktérmi zodpovednými za krízové riadenie. Okrem toho by agentúra mohla podporovať riešenie incidentov z technickej stránky uľahčovaním výmeny relevantných technických riešení medzi členskými štátmi a zabezpečením vstupov pre komunikáciu s verejnosťou. Agentúra by tento proces mala podporovať skúšaním rôznych možností takejto spolupráce na každoročných kyberneticko-bezpečnostných cvičeniach.
- (20) Pri výkone svojich operačných úloh by agentúra mala využiť dostupné odborné poznatky tímu CERT-EU, a to štruktúrovanou spoluprácou vo vzájomnej fyzickej blízkosti. Táto štruktúrovaná spolupráca uľahčí potrebné synergie a budovanie odborných znalostí agentúry ENISA. Podľa potreby by sa mali medzi oboma organizáciami vytvoriť účelové dohody o fungovaní tejto spolupráce v praxi.
- (21) Agentúra by v súlade so svojimi operačnými úlohami mala byť schopná podporiť členské štáty, napríklad formou poradenstva alebo technickej pomoci, či zabezpečovaním analýzy hrozieb a incidentov. V odporúčaní Komisie o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu sa odporúča, aby členské štáty v dobrej viere spolupracovali a bez zbytočného odkladu sa vzájomne i s agentúrou ENISA delili o informácie o rozsiahlych kybernetických incidentoch a krízach. Tieto informácie by tiež mali agentúre ENISA pomôcť pri plnení jej operačných úloh.
- (22) V rámci bežnej technickej spolupráce na podporu situačného povedomia Únie by mala agentúra pravidelne vypracúvať technickú situačnú správu EÚ o incidentoch a hrozbách, ktorá vychádza z verejne dostupných informácií, jej vlastných analýz a správ, ktoré jej (dobrovoľne) poskytnú jednotky CSIRT členských štátov alebo jednotné kontaktné miesta podľa smernice NIS, Európske centrum boja proti počítačovej kriminalite (EC3) v rámci Europolu, CERT-EU a v náležitých prípadoch centrum EÚ pre spravodajské informácie (INTECEN) v rámci Európskej služby pre vonkajšiu činnosť (ESVČ). Táto správa by sa mala sprístupniť zodpovedným útvarom Rady, Komisie, vysokému predstaviteľovi Únie pre zahraničné veci a bezpečnostnú politiku a podpredsedovi Komisie a sieti jednotiek CSIRT.
- (23) Technické *ex post* skúmanie incidentov s výrazným dosahom vo viac než jednom členskom štáte, ktoré agentúra podporí alebo vykoná na požiadanie alebo so súhlasom dotknutých členských štátov, by sa malo zamerať na prevenciu incidentov v budúcnosti a nemali by ním byť dotknuté prípadné súdne alebo správne konania na určenie vinníka či zodpovednosti.
- (24) Dotknuté členské štáty by mali agentúre na účely tohto skúmania poskytnúť potrebné informácie a podporu bez toho, aby bol dotknutý článok 346 Zmluvy o fungovaní Európskej únie či iné verejno-politické motívy.

- (25) Členské štáty môžu prizvať podniky dotknuté daným incidentom k spolupráci v podobe poskytnutia potrebných informácií a podpory agentúre bez toho, aby bolo dotknuté ich právo na ochranu citlivých obchodných informácií.
- (26) Na lepšie pochopenie výziev v oblasti kybernetickej bezpečnosti a v záujme dlhodobého strategického poradenstva pre členské štáty a inštitúcie Únie musí agentúra analyzovať existujúce i nové riziká. Na to by agentúra mala v spolupráci s členskými štátmi a podľa potreby štatistickými orgánmi a ďalšími aktérmi zbierať relevantné informácie, analyzovať nové technológie a poskytovať tematické posúdenie očakávaných spoločenských, právnych, hospodárskych a regulačných vplyvov technologických inovácií na sieťovú a informačnú bezpečnosť, najmä kybernetickú. Agentúra by navyše mala členské štáty a inštitúcie, agentúry a orgány Únie podporovať pri identifikácii nastupujúcich trendov a pri predchádzaní kyberneticko-bezpečnostným problémom, a to analýzou hrozieb a incidentov.
- (27) V záujme posilnenia odolnosti Únie by agentúra mala rozvíjať špičkovú odbornosť vo sfére bezpečnosti internetovej infraštruktúry a kritických infraštruktúr, a to poradenstvom, usmerňovaním a šírením osvedčených postupov. S cieľom uľahčiť prístup k lepšie štruktúrovaným informáciám o kybernetických rizikách a ich možných riešeniach by agentúra mala zriadiť a prevádzkovať „informačné centrum“ Únie – portál s funkciou jednotného kontaktného miesta, ktorý bude verejnosti sprístupňovať informácie o kybernetickej bezpečnosti od inštitúcií, agentúr a orgánov EÚ i členských štátov.
- (28) Agentúra by mala prispievať k zvyšovaniu verejného povedomia o rizikách spojených s kybernetickou bezpečnosťou a odporúčať jednotlivým používateľom – občanom i organizáciám osvedčené postupy. Agentúra by mala prispievať k propagácii osvedčených postupov a riešení u jednotlivcov a organizácii aj zberom a analýzou verejne dostupných informácií o závažných incidentoch a vypracúvaním správ s cieľom poskytnúť podnikom a občanom usmernenia a zvýšiť celkovú pripravenosť a odolnosť. Agentúra by navyše mala v spolupráci s členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie organizovať pravidelné osvetové a vzdelávacie kampane pre verejnosť, ktoré sú určené koncovým používateľom a zameriavajú sa na propagáciu bezpečnejšieho správania jednotlivcov na internete a zvyšovanie povedomia o potenciálnych hrozbách v kybernetickom priestore vrátane počítačovej kriminality, ako sú phishingové útoky, botnety, finančné a bankové podvody; zároveň by mala poskytovať základné rady v oblasti autentifikácie a ochrany údajov. Agentúra by mala mať kľúčovú rolu pri urýchlennom zvyšovaní povedomia koncových používateľov o bezpečnosti zariadení.
- (29) Na podporu podnikov pôsobiacich v odvetví kybernetickej bezpečnosti, ale i používateľov kyberneticko-bezpečnostných riešení by agentúra mala vytvoriť a prevádzkovať „monitor trhu“, ktorý bude pravidelne analyzovať a šíriť hlavné trendy na trhu kybernetickej bezpečnosti – tak na strane dopytu, ako aj ponuky.
- (30) S cieľom zaistiť úplné splnenie svojich cieľov by agentúra mala udržiavať kontakty s relevantnými inštitúciami, agentúrami a orgánmi vrátane tímu CERT-EU, Európskeho centra boja proti počítačovej kriminalite (EC3) pri Europole, Európskej obrannej agentúry (EDA), Európskej agentúry na prevádzkové riadenie rozsiahlych informačných systémov (eu-LISA), Európskej agentúry pre bezpečnosť letectva (EASA) a prípadne ďalších agentúr EÚ angažovaných v otázkach kybernetickej bezpečnosti. Okrem toho by mala udržiavať kontakty aj s orgánmi zodpovednými za ochranu údajov s cieľom vymieňať si know-how a osvedčené postupy a poskytovať

poradenstvo o kyberneticko-bezpečnostných aspektoch, ktoré môžu ovplyvniť ich prácu. Zástupcovia vnútroštátnych orgánov a orgánov Únie v oblasti presadzovania práva a ochrany údajov by mali byť oprávnení na účasť v stálej skupine zainteresovaných strán agentúry. Pri styku s orgánmi presadzovania práva v otázkach sieťovej a informačnej bezpečnosti, ktoré by mohli mať vplyv na ich prácu, by agentúra mala rešpektovať existujúce informačné kanály a zavedené siete.

- (31) Agentúra ako člen siete jednotiek CSIRT, ktorý navyše zabezpečuje funkciu sekretariátu, by mala jednotky CSIRT členských štátov a tím CERT-EU podporovať v operačnej spolupráci pri všetkých relevantných úlohách siete jednotiek CSIRT v zmysle smernice NIS. Ďalej by agentúra mala presadzovať a podporovať spoluprácu medzi príslušnými jednotkami CSIRT v prípade incidentov, útokov alebo narušení sietí či infraštruktúr pod ich správou alebo ochranou, v prípadoch, ktoré zahŕňajú alebo môžu zahŕňať aspoň dve jednotky CSIRT, pričom sa riadne zohľadnia štandardné operačné postupy siete jednotiek CSIRT.
- (32) V záujme lepšej pripravenosti Únie reagovať na kybernetické incidenty by agentúra mala každoročne organizovať kyberneticko-bezpečnostné cvičenia na úrovni Únie a na požiadanie by mala podporiť členské štáty a inštitúcie, agentúry a orgány EÚ pri organizácii cvičení.
- (33) Agentúra by mala ďalej rozvíjať a udržiavať odborné poznatky o certifikácii kybernetickej bezpečnosti v záujme podpory politiky Únie v tomto smere. Agentúra by mala podporovať využívanie certifikácie kybernetickej bezpečnosti certifikácie v Únii, a to aj prispievaním k vytvoreniu a uchovávaniu kyberneticko-bezpečnostného certifikačného rámca na úrovni Únie, aby sa posilnila transparentnosť dôveryhodnosti kybernetickej bezpečnosti produktov a služieb IKT, čím sa posilní dôvera v digitálny vnútorný trh.
- (34) Účinné politiky kybernetickej bezpečnosti by mali vychádzať zo správne navrhnutých metód posudzovania rizika vo verejnom i v súkromnom sektore. Metódy posudzovania rizika sa používajú na rôznych úrovniach bez spoločného postupu ich účinného uplatňovania. Podpora a vývoj osvedčených postupov v oblasti posudzovania rizika a interoperabilných riešení riadenia rizika v organizáciách verejného a súkromného sektora zvýšia úroveň kybernetickej bezpečnosti v Únii. S týmto cieľom by agentúra mala podporovať spoluprácu zainteresovaných strán na úrovni Únie, pričom by mala uľahčovať ich úsilie o tvorbu a zavádzanie európskych a medzinárodných noriem pre riadenie rizík a merateľnú bezpečnosť elektronických produktov, systémov, sietí a služieb, ktoré spolu so softvérom tvoria sieťové a informačné systémy.
- (35) Agentúra by mala podnecovať členské štáty a poskytovateľov služieb k sprísňovaniu svojich všeobecných bezpečnostných noriem tak, aby všetci používatelia internetu mohli podniknúť potrebné kroky na zaistenie svojej osobnej kybernetickej bezpečnosti. Najmä poskytovatelia služieb a výrobcovia produktov by mali z trhu stiahnuť či prepracovať produkty a služby, ktoré kyberneticko-bezpečnostným normám nevyhovujú. V spolupráci s príslušnými orgánmi môže agentúra ENISA šíriť informácie o úrovni kybernetickej bezpečnosti produktov a služieb ponúkaných na vnútornom trhu, varovať pred určitými poskytovateľmi a výrobcami a žiadať ich o zvýšenie bezpečnosti (vrátane kybernetickej) svojich produktov a služieb.
- (36) Pri poskytovaní poradenstva inštitúciám, orgánom, úradom a agentúram Únie a na požiadanie prípadne aj členským štátom o potrebách výskumu v oblasti sieťovej a informačnej bezpečnosti, najmä kybernetickej, by agentúra mala plne zohľadňovať

prebiehajúci výskum, vývoj a technologické posudzovanie, najmä v rámci rôznych výskumných iniciatív Únie.

- (37) Kybernetická bezpečnosť je globálnym problémom. Je potrebná užšia medzinárodná spolupráca s cieľom zlepšiť bezpečnostné normy vrátane vymedzenia spoločných noriem správania, zlepšiť zdieľanie informácií a presadzovať rýchlejšiu medzinárodnú spoluprácu pri reakcii na problémy sieťovej a informačnej bezpečnosti, ako aj spoločný globálny prístup k nim. Agentúra by na tento účel mala podporovať výraznejšie zapojenie Únie a spoluprácu s tretími krajinami a medzinárodnými organizáciami tým, že vo vhodných prípadoch poskytne potrebné odborné znalosti a analýzu príslušným inštitúciám, orgánom, úradom a agentúram Únie.
- (38) Agentúra by mala byť schopná reagovať na *ad hoc* žiadosti členských štátov a inštitúcií, agentúr a orgánov EÚ o poradenstvo a pomoc spadajúcu do rozsahu cieľov agentúry.
- (39) Je potrebné uplatniť určité zásady týkajúce sa riadenia agentúry, aby sa dodržalo spoločné vyhlásenie a spoločný prístup dohodnutý medziinštitucionálnou pracovnou skupinou pre decentralizované agentúry EÚ v júli 2012, ktorých cieľom je zefektívniť činnosti agentúr a zlepšiť ich výkonnosť. Spoločné vyhlásenie a spoločný prístup by sa mali podľa potreby odraziť aj v pracovných programoch agentúry, jej hodnoteniach a praxi v oblasti podávania správ a administratívy.
- (40) Správna rada zložená zo zástupcov členských štátov a Komisie 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 zostavovanie rozpočtu, overovanie jeho plnenia, prijatie vhodných rozpočtových pravidiel, navrhnutie transparentných pracovných postupov rozhodovania agentúry, prijatie jednotného programového dokumentu, prijatie vlastného rokovacieho poriadku, menovanie výkonného riaditeľa a rozhodovanie o predlžovaní či ukončení jeho funkčného obdobia.
- (41) Aby agentúra mohla fungovať riadne a efektívne, Komisia a členské štáty by mali zabezpečiť, aby osoby, ktoré majú byť vymenované za členov správnej rady, mali zodpovedajúce odborné znalosti a skúsenosti v príslušných funkčných oblastiach. Komisia a členské štáty by mali vynaložiť úsilie aj na obmedzenie obmeny svojich zástupcov v správnej rade s cieľom zabezpečiť kontinuitu jej práce.
- (42) Bezproblémové fungovanie agentúry vyžaduje, aby bol jej výkonný riaditeľ vymenovaný na základe zásluh a zdokumentovaných administratívnych a riadiacich schopností, ako aj na základe kvalifikácie a skúseností vo sfére kybernetickej bezpečnosti, a aby vykonával svoje povinnosti úplne nezávisle. Výkonný riaditeľ by mal pripraviť návrh pracovného programu agentúry po predchádzajúcej konzultácii s Komisiou a prijať všetky potrebné opatrenia na zabezpečenie riadneho vykonania pracovného programu agentúry. Výkonný riaditeľ by mal vypracovať výročnú správu, ktorá sa predkladá správnej rade, návrh výkazu odhadov príjmov a výdavkov agentúry a mal by plniť rozpočet. Výkonný riaditeľ by okrem toho mal mať možnosť zriadiť *ad hoc* pracovné skupiny zamerané na osobitné záležitosti najmä vedeckého, technického, právneho či sociálno-ekonomického charakteru. Výkonný riaditeľ by mal zabezpečiť, aby sa členovia *ad hoc* pracovných skupín vyberali podľa najprísnejších požiadaviek na odbornosť, pričom by sa náležite zohľadnila reprezentatívna rovnováha medzi verejnými správami členských štátov, inštitúciami Únie, súkromným sektorom vrátane príslušného odvetvia, užívateľmi a akademickými expertmi v oblasti sieťovej a informačnej bezpečnosti, a to podľa konkrétnej tematiky.

- (43) Výkonná rada by mala prispievať k efektívnej činnosti správnej rady. V rámci prípravných prác spojených s rozhodnutiami správnej rady by mala podrobne skúmať relevantné informácie a dostupné možnosti, radiť a ponúkať riešenia na prípravu príslušných rozhodnutí správnej rady.
- (44) 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 správnu radou na návrh výkonného riaditeľa by sa mala zameriavať na otázky dôležité pre zainteresované strany a upriamiť na ne pozornosť agentúry. Zloženie stálej skupiny zainteresovaných strán a úlohy zverené tejto skupine, z ktorou treba konzultovať najmä návrh pracovného programu, by mali zabezpečiť dostatočné zastúpenie zainteresovaných strán na práci agentúry.
- (45) Agentúra by mala disponovať pravidlami na predchádzanie konfliktu záujmov a jeho riadenie. Agentúra by mala uplatňovať príslušné pravidlá Únie týkajúce sa prístupu verejnosti k dokumentom, ako sa stanovujú v nariadení Európskeho parlamentu a Rady (ES) č. 1049/2001³⁴. Na spracovanie osobných údajov agentúrou by sa malo vzťahovať 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 údajov³⁵. Agentúra by mala dodržiavať ustanovenia platné pre inštitúcie Únie, ako aj vnútroštátne právne predpisy o zaobchádzaní s informáciami, najmä s citlivými neutajovanými informáciami a utajovanými skutočnosťami EÚ.
- (46) S cieľom zaručiť úplnú autonómiu a nezávislosť agentúry a umožniť jej plniť ďalšie a nové úlohy vrátane nepredvídaných núdzových úloh by sa mal agentúre poskytnúť dostatočný a nezávislý rozpočet, ktorého príjmy pochádzajú predovšetkým z príspevku Únie a príspevkov tretích krajín, ktoré sa podieľajú na práci agentúry. Väčšina zamestnancov agentúry by mala byť priamo zapojená do operačného plnenia mandátu agentúry. Hostiteľský členský štát alebo akýkoľvek iný členský štát by mali mať možnosť dobrovoľne prispievať do príjmov agentúry. Rozpočtový postup Únie by sa mal naďalej uplatňovať, pokiaľ ide o všetky dotácie započítateľné do všeobecného rozpočtu Únie. Okrem toho by Dvor audítorov mal vykonať audit účtov agentúry v záujme transparentnosti a zodpovednosti.
- (47) Posudzovanie zhody je proces, ktorým sa preukazuje splnenie stanovených požiadaviek na určitý produkt, proces, službu, systém, osobu alebo orgán. Na účely tohto nariadenia by sa certifikácia mala považovať za istý typ posudzovania zhody kyberneticko-bezpečnostných prvkov produktu, procesu, služby, systému alebo ich kombinácie („produkty a služby IKT“) treťou stranou inou ako výrobca či poskytovateľ služby. Certifikácia sama osebe nemôže zaručiť, že certifikované produkty a služby IKT sú kyberneticky bezpečné. Ide skôr o postup a technickú metodiku na potvrdenie toho, že produkty a služby IKT boli preskúšané a spĺňajú určité kyberneticko-bezpečnostné požiadavky stanovené inde, napríklad v technických normách.
- (48) Certifikácia kybernetickej bezpečnosti zohráva významnú úlohu pri posilňovaní dôvery v produkty a služby IKT, ako aj ich bezpečnosti. Digitálny jednotný trh, a

³⁴ 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).

³⁵ Ú. v. ES L 8, 12.1.2001, s. 1.

najmä dátové hospodárstvo a internet vecí môžu prosperovať iba ak široká verejnosť verí, že takéto produkty a služby poskytujú určitú mieru dôveryhodnosti kybernetickej bezpečnosti. Prepojené a automatizované vozidlá, elektronické zdravotnícke pomôcky, automatické priemyselné riadiace systémy či inteligentné siete sú iba niektorými príkladmi odvetví, kde už sa certifikácia bežne využíva alebo sa začne využívať v blízkej budúcnosti. Smernica NIS pokrýva aj odvetvia, kde je certifikácia kybernetickej bezpečnosti kľúčová.

- (49) Vo svojom oznámení s názvom „Posilnenie odolnosti kybernetického systému a podpora konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe“ z roku 2016 Komisia zdôraznila potrebu kvalitných, cenovo dostupných a interoperabilných produktov a riešení v oblasti kybernetickej bezpečnosti. Ponuka produktov a služieb IKT na jednotnom trhu je geograficky stále veľmi fragmentovaná. Dôvodom je, že vývoj odvetvia kybernetickej bezpečnosti v Európe sa do značnej miery riadil dopytom verejných správ jednotlivých štátov. Medzi ďalšie nedostatky ovplyvňujúce kybernetickú bezpečnosť na jednotnom trhu patrí absencia interoperabilných riešení (technických noriem), postupov a celoúnijných mechanizmov certifikácie. Na jednej strane to európskym firmám sťažuje možnosť konkurovať na národnej, európskej i svetovej úrovni. Na druhej sa okliešťa ponuka reálne využiteľných kyberneticko-bezpečnostných technológií, ku ktorým majú jednotlivci a spoločnosti prístup. Podobne Komisia vo svojom preskúmaní vykonávania stratégie digitálneho jednotného trhu v polovici trvania zdôraznila potrebu bezpečných pripojených produktov a systémov a naznačila, že vytvorenie európskeho rámca bezpečnosti IKT, v ktorom sa stanovujú pravidlá organizovania certifikácie bezpečnosti IKT v Únii, by mohlo zachovať dôveru v internet a zároveň vyriešiť súčasnú fragmentáciu trhu kybernetickej bezpečnosti.
- (50) Certifikácia kybernetickej bezpečnosti produktov a služieb IKT sa dnes využíva iba obmedzene. Ak sa uplatňuje, je to zväčša na úrovni členských štátov alebo z iniciatívy odvetvia. V tomto kontexte certifikát vystavený niektorým orgánom kybernetickej bezpečnosti v zásade iné členské štáty neuznávajú. Môže sa teda stať, že spoločnosti musia svoje produkty a služby certifikovať v niekoľkých členských štátoch pôsobenia, napríklad ak sa chcú zapojiť do ich verejných obstarávaní. Okrem toho sa síce objavujú nové systémy, no nezdá sa, že by koherentne a holisticky pristupovali k horizontálnym otázkam kybernetickej bezpečnosti, ako je napríklad internet vecí. Existujúce systémy vykazujú výrazné nedostatky a rozdiely z hľadiska škály pokrytia produktov, úrovne dôveryhodnosti bezpečnosti, vecných kritérií a samotného využitia.
- (51) V minulosti sa objavili určité snahy smerujúce k vzájomnému uznávaniu certifikátov v Európe. Úspešné však boli iba sčasti. Najvýznamnejším príkladom v tomto smere je dohoda skupiny vysokých úradníkov pre bezpečnosť informačných systémov (SOG-IS) o vzájomnom uznávaní (DVU). Hoci ide o najvýznamnejší model spolupráce a vzájomného uznávania v oblasti bezpečnostnej certifikácie, SOG-IS DVU má určité výrazné nedostatky z hľadiska vysokých nákladov a obmedzenej pôsobnosti. Doposiaľ sa vypracovalo iba niekoľko profilov ochrany digitálnych produktov – napríklad pre digitálny podpis, digitálny tachograf či smart karty. Čo je však najpodstatnejšie, SOG-IS zahŕňa iba časť členských štátov Únie. Účinnosť dohody SOG-IS DVU na vnútornom trhu je teda obmedzená.
- (52) Z uvedených dôvodov treba zriadiť európsky rámec certifikácie kybernetickej bezpečnosti, v ktorom sa stanovujú základné horizontálne požiadavky európskych systémov certifikácie kybernetickej bezpečnosti, ktoré sa majú vypracovať, a umožní sa uznávanie a uplatňovanie certifikátov produktov a služieb IKT vo všetkých

členských štátoch. Tento európsky rámec by mal plniť dvojaký účel: na jednej strane by mal prispievať k posilneniu dôvery v produkty a služby IKT certifikované podľa takýchto systémov. Na druhej strane by mal predchádzať množeniu nekompatibilných či prekrývajúcich sa národných certifikácií kybernetickej bezpečnosti, čím sa znížia náklady podnikov pôsobiacich na digitálnom jednotnom trhu. Systémy by mali byť nediskriminačné a založené na medzinárodných a/alebo únijných normách, pokiaľ tieto nie sú neefektívne alebo nevhodné na plnenie legitímnych cieľov EÚ v tejto oblasti.

- (53) Komisia by mala byť splnomocnená na prijímanie európskych systémov certifikácie kybernetickej bezpečnosti pre konkrétne skupiny produktov a služieb IKT. Uplatňovanie týchto systémov a dohl'ad nad nimi by mali vykonávať vnútroštátne orgány dohl'adu nad certifikáciou, pričom certifikáty vydané podľa týchto systémov by mali byť platné a uznávané v celej Únii. Z pôsobnosti nariadenia by sa mali vyňať certifikačné systémy, ktoré uplatňuje príslušné odvetvie alebo iné súkromné organizácie. Orgány, ktoré takéto systémy prevádzkujú, však môžu Komisii navrhnúť zváženie ich použitia ako základ pre schválenie v podobe európskeho systému.
- (54) Ustanoveniami tohto nariadenia by nemala byť dotknutá legislatíva Únie stanovujúca konkrétne pravidlá certifikácie produktov a služieb IKT. Najmä všeobecné nariadenie o ochrane údajov obsahuje ustanovenia o zriadení certifikačných mechanizmov, pečatí a značiek ochrany údajov na preukázanie súladu spracovateľských operácií prevádzkovateľov a sprostredkovateľov s daným nariadením. Tieto certifikačné mechanizmy, pečate a značky ochrany údajov by mali dotknutým osobám umožniť rýchle vyhodnotenie, nakoľko príslušné produkty a služby chránia údaje. Týmto nariadením nie je dotknutá certifikácia operácií spracovania údajov podľa všeobecného nariadenia o ochrane údajov, čo platí aj pre prípady, keď sú takéto operácie súčasťou produktov a služieb.
- (55) Účelom európskych systémov certifikácie kybernetickej bezpečnosti by malo byť, aby produkty a služby IKT certifikované podľa príslušného systému spĺňali stanovené požiadavky. Medzi tieto požiadavky patrí schopnosť na určitom stupni dôveryhodnosti odolať konaniu, ktorého cieľom je ohroziť dostupnosť, pravosť, integritu a dôvernúť uložených, prenášaných alebo spracúvaných údajov alebo súvisiacich funkcií daných produktov, procesov, služieb a systémov v zmysle tohto nariadenia, či služieb, ktoré sa cez ne ponúkajú alebo sprístupňujú. V tomto nariadení nie je možné stanoviť podrobné kyberneticko-bezpečnostné požiadavky na všetky produkty a služby IKT. Produkty a služby IKT, ako aj súvisiace kyberneticko-bezpečnostné potreby sú také rozmanité, že je veľmi ťažké stanoviť všeobecné požiadavky na kybernetickú bezpečnosť, ktoré by sa dali uplatniť plošne. Treba preto prijať širokozáberový a všeobecný koncept kybernetickej bezpečnosti na účely certifikácie doplnený súborom špecifických kyberneticko-bezpečnostných cieľov, ktoré treba pri návrhu európskych systémov certifikácie kybernetickej bezpečnosti zohľadniť. Spôsoby, ktorými sa tieto ciele pri konkrétnych produktoch a službách IKT dosiahnu, by sa potom mali podrobnejšie vymedziť na úrovni príslušného systému certifikácie, ktorý prijme Komisia – napríklad s odvolaním sa na normy alebo technické špecifikácie.
- (56) Komisia by mala byť splnomocnená požiadať agentúru ENISA o prípravu kandidátskych systémov pre konkrétne produkty alebo služby IKT. Následne by Komisia mala byť splnomocnená na základe kandidátskeho systému navrhnutého agentúrou ENISA prijať európsky systém certifikácie kybernetickej bezpečnosti v podobe vykonávacích aktov. Zohľadňujúc všeobecný účel a bezpečnostné ciele identifikované v tomto nariadení, európske systémy certifikácie kybernetickej

bezpečnosti prijaté Komisiou by mali zahŕňať minimálny súbor prvkov, ktoré sa vzťahujú na danú problematiku, ako aj rozsah a fungovanie daného systému. Okrem iného by sem mal patriť rozsah a predmet certifikácie kybernetickej bezpečnosti vrátane kategórií pokrytých produktov a služieb IKT, podrobného vymedzenia kyberneticko-bezpečnostných požiadaviek (napríklad s odvolaním na normy alebo technické špecifikácie), konkrétne hodnotiace kritériá a metódy, ako aj cieľový stupeň dôveryhodnosti: základná, pokročilá a/alebo vysoká.

- (57) Využívanie európskej certifikácie kybernetickej bezpečnosti by malo zostať dobrovoľné, pokiaľ sa nestanovuje inak v únijských alebo vnútroštátnych právnych predpisoch. Aby sa však dosiahli ciele tohto nariadenia a aby sa predišlo fragmentácii vnútorného trhu, vnútroštátne systémy alebo postupy certifikácie kybernetickej bezpečnosti produktov a služieb IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, by mali stratiť účinky od dátumu, ktorý stanoví Komisia vo vykonávacom akte. Okrem toho by členské štáty nemali zavádzať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti v prípade produktov a služieb IKT, pre ktoré už existuje európsky systém certifikácie kybernetickej bezpečnosti.
- (58) Po prijatí určitého európskeho systému certifikácie kybernetickej bezpečnosti by mali výrobcovia produktov alebo poskytovatelia služieb IKT môcť požiadať o certifikáciu svojich produktov alebo služieb ktorýmkoľvek orgánom posudzovania zhody, ktorý si zvolia. Orgány posudzovania zhody by mali akreditovať akreditačný orgán, ak spĺňajú určité požiadavky stanovené v tomto nariadení. Akreditácia by sa mala vydávať najviac na päť rokov, pričom ju možno obnoviť za rovnakých podmienok, pokiaľ orgán posudzovania zhody spĺňa požiadavky. Akreditačné orgány by mali orgánu posudzovania zhody akreditáciu odňať, ak nie sú alebo prestanú byť splnené akreditačné podmienky, alebo ak kroky daného orgánu posudzovania zhody porušujú toto nariadenie.
- (59) Od všetkých členských štátov treba žiadať určenie jedného vnútroštátneho orgánu dohľadu nad certifikáciou kybernetickej bezpečnosti, ktorý bude dohliadať na súlad orgánov posudzovania zhody so sídlom na ich území a nimi vydaných certifikátov s požiadavkami tohto nariadenia a príslušných systémov certifikácie kybernetickej bezpečnosti. Vnútroštátne orgány dohľadu nad certifikáciou by mali vybavovať sťažnosti fyzických alebo právnických osôb v súvislosti s certifikátmi, ktoré vydali orgány posudzovania zhody so sídlom na ich území, primerane prešetriť predmet danej sťažnosti a sťažovateľa v primeranej lehote informovať o pokroku a výsledku tohto prešetrenia. Okrem toho by mali spolupracovať s ostatnými vnútroštátnymi orgánmi dohľadu nad certifikáciou alebo ďalšími verejnými orgánmi vrátane poskytovania informácií o možnom nesúlade produktov a služieb IKT s požiadavkami tohto nariadenia alebo konkrétnych kyberneticko-bezpečnostných systémov.
- (60) V záujme konzistentného uplatňovania európskeho rámca certifikácie kybernetickej bezpečnosti by sa mala zriadiť európska skupina pre certifikáciu kybernetickej bezpečnosti (ďalej len „skupina“) zložená z vnútroštátnych orgánov dohľadu nad certifikáciou. Medzi hlavné úlohy tejto skupiny by mali patriť poradenstvo a pomoc Komisii v jej úsilí o zaistenie konzistentného vykonávania a uplatňovania európskeho rámca certifikácie kybernetickej bezpečnosti; pomoc agentúre a úzka spolupráca s ňou pri príprave kandidátskych systémov certifikácie kybernetickej bezpečnosti; odporúčania, na základe ktorých Komisia žiada agentúru o vypracovanie kandidátskeho európskeho systému certifikácie kybernetickej bezpečnosti; a

prijímanie stanovísk pre Komisiu k udržiavaniu a prehodnocovaniu existujúcich európskych systémov certifikácie kybernetickej bezpečnosti.

- (61) Na zvýšenie povedomia a uľahčenie akceptácie budúcich únijných systémov certifikácie kybernetickej bezpečnosti môže Európska komisia vydať všeobecné či odvetvové usmernenia o kybernetickej bezpečnosti – napríklad o osvedčených postupoch a zodpovednom správaní sa v tejto oblasti, pričom sa zdôrazní pozitívny účinok využívania certifikovaných produktov a služieb IKT.
- (62) Podpora certifikácie kybernetickej bezpečnosti zo strany agentúry by mala zahŕňať aj kontakt s Bezpečnostným výborom Rady a príslušným vnútroštátnym orgánom, pokiaľ ide o kryptografické schvaľovanie produktov, ktoré sa majú používať v utajených sieťach.
- (63) Na bližšie určenie kritérií akreditácie orgánov posudzovania zhody by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 Zmluvy o fungovaní Európskej únie. Komisia by mala v rámci prípravných prác viesť náležité konzultácie, a to aj na úrovni expertov. Pri týchto konzultáciách by sa mali dodržiavať zásady stanovené v medziinštitucionálnej dohode o lepšej tvorbe práva z 13. apríla 2016. Predovšetkým v záujme rovnakého zastúpenia pri príprave delegovaných aktov by sa všetky dokumenty mali doručiť Európskemu parlamentu a Rade v rovnakom čase ako odborníkom z členských štátov, a odborníci Európskeho parlamentu a Rady by mali mať systematicky prístup na zasadnutia expertných skupín Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.
- (64) S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia by sa v prípadoch stanovených v tomto nariadení mali na Komisiu preniesť vykonávacie právomoci. Tieto právomoci by sa mali vykonávať v súlade s nariadením (EÚ) č. 182/2011.
- (65) Postup preskúmania by sa mal uplatniť pri prijímaní vykonávacích aktov o európskych systémoch certifikácie kybernetickej bezpečnosti produktov a služieb IKT, o modalitách skúmania zo strany agentúry, ako aj o okolnostiach, formátoch a postupoch, na základe ktorých majú vnútroštátne orgány dohľad nad certifikáciou Komisie oznamovať akreditované orgány posudzovania zhody.
- (66) Činnosť agentúry by sa mala vyhodnocovať nezávisle. V rámci toho by sa malo posúdiť napĺňanie cieľov agentúry, jej pracovné postupy a relevantnosť jej úloh. Zároveň by sa v hodnotení malo posúdiť dosah, efektívnosť a účinnosť európskeho rámca certifikácie kybernetickej bezpečnosti.
- (67) Nariadenie (EÚ) č. 526/2013 by sa malo zrušiť.
- (68) Keďže ciele tohto nariadenia nemožno uspokojivo dosiahnuť na úrovni jednotlivých členských štátov, ale možno ich lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa,

PRIJALI TOTO NARIADENIE:

HLAVA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

S cieľom zaistiť riadne fungovanie vnútorného trhu pri vysokej úrovni kybernetickej bezpečnosti, odolnosti a dôvery v rámci Únie sa v tomto nariadení:

- a) stanovujú ciele, úlohy a organizačné aspekty agentúry ENISA – Agentúry EÚ pre kybernetickú bezpečnosť (ďalej len „agentúra“) a
- b) stanovuje rámec vytvorenia európskych systémov certifikácie kybernetickej bezpečnosti na zaistenie primeranej úrovne kybernetickej bezpečnosti produktov a služieb IKT v Únii. Uplatňovaním tohto rámca nie sú dotknuté osobitné ustanovenia o dobrovoľnej či povinnej certifikácii podľa iných aktov Únie.

Článok 2 ***Vymedzenie pojmov***

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „kybernetická bezpečnosť“ zahŕňa všetky činnosti potrebné na ochranu sietí a informačných systémov, ich používateľov a dotknutých osôb pred kybernetickými hrozbami;
2. „sieť a informačný systém“ je systém v zmysle článku 4 bode 1 smernice (EÚ) 2016/1148;
3. „národná stratégia v oblasti bezpečnosti sietí a informačných systémov“ je rámec v zmysle článku 4 bode 3 smernice (EÚ) 2016/1148;
4. „prevádzkovateľ základných služieb“ je verejný alebo súkromný subjekt vymedzený v článku 4 bode 4 smernice (EÚ) 2016/1148;
5. „poskytovateľ digitálnych služieb“ je každá právnická osoba, ktorá poskytuje digitálnu službu, vymedzená v článku 4 bode 6 smernice (EÚ) 2016/1148;
6. „incident“ je každá udalosť vymedzená v článku 4 bode 7 smernice (EÚ) 2016/1148;
7. „riešenie incidentov“ je každý postup vymedzený v článku 4 bode 8 smernice (EÚ) 2016/1148;
8. „kybernetická hrozba“ je každá potenciálna okolnosť alebo udalosť, ktorá môže negatívne ovplyvniť siete a informačné systémy, ich používateľov a dotknuté osoby;
9. „európsky systém certifikácie kybernetickej bezpečnosti“ je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov vymedzený na úrovni Únie, ktorý sa uplatňuje na certifikáciu produktov a služieb informačných a komunikačných technológií (ďalej len „IKT“) spadajúcich do rozsahu pôsobnosti príslušného systému;
10. „európsky certifikát kybernetickej bezpečnosti“ je dokument vystavený orgánom posudzovania zhody, v ktorom sa potvrdzuje, že daný produkt alebo služba IKT spĺňa konkrétne požiadavky určitého európskeho systému certifikácie kybernetickej bezpečnosti;

11. „produkt a služba IKT“ je každý prvok alebo skupina prvkov sietí a informačných systémov;
12. „akreditácia“ je akreditácia vymedzená v článku 2 bode 10 nariadenia (ES) č. 765/2008;
13. „vnútroštátny akreditačný orgán“ je vnútroštátny akreditačný orgán vymedzený v článku 2 bode 11 nariadenia (ES) č. 765/2008;
14. „posudzovanie zhody“ je posudzovanie zhody vymedzené v článku 2 bode 12 nariadenia (ES) č. 765/2008;
15. „orgán posudzovania zhody“ je orgán posudzovania zhody vymedzený v článku 2 bode 13 nariadenia (ES) č. 765/2008;
16. „norma“ je norma vymedzená v článku 2 bode 1 nariadenia (EÚ) č. 1025/2012.

HLAVA II

ENISA – „Agentúra EÚ pre kybernetickú bezpečnosť“

KAPITOLA I

MANDÁT, CIELE A ÚLOHY

Článok 3

Mandát

1. Agentúra plní úlohy, ktoré jej ukladá toto nariadenie, s cieľom prispieť k vysokej úrovni kybernetickej bezpečnosti v Únii.
2. Agentúra plní úlohy zverené aktmi Únie, v ktorých sa stanovujú opatrenia na aproximáciu zákonov, iných právnych predpisov a správnych opatrení členských štátov v oblasti kybernetickej bezpečnosti.
3. Ciele a úlohy agentúry nemajú vplyv na právomoci členských štátov v oblasti kybernetickej bezpečnosti a v žiadnom prípade na činnosti spojené s verejnou bezpečnosťou, obranou, národnou bezpečnosťou a na činnosti štátu v oblasti trestného práva.

Článok 4

Ciele

1. Agentúra pôsobí ako stredisko odborných poznatkov o kybernetickej bezpečnosti, pretože sa vyznačuje nezávislosťou, vedeckou a technickou kvalitou poskytovaného poradenstva, pomoci a šírených informácií, transparentnosťou svojich prevádzkových postupov a pracovných metód a dôslednosťou pri vykonávaní svojich úloh.
2. Agentúra pomáha inštitúciám, agentúram a orgánom Únie, ako aj členským štátom pri príprave a vykonávaní politík spojených s kybernetickou bezpečnosťou.
3. Agentúra podporuje budovanie kapacít a pripravenosť v celej Únii tým, že Únii, členským štátom i verejným a súkromným aktérom pomáha pri zvyšovaní ochrany ich sietí a informačných systémov, rozvoji kyberneticko-bezpečnostných zručností a spôsobilostí a pri dosahovaní kybernetickej odolnosti.
4. Agentúra na úrovni Únie presadzuje spoluprácu a koordináciu členských štátov, inštitúcií, agentúr a orgánov Únie, ako aj relevantných zainteresovaných strán vrátane súkromného sektora v otázkach kybernetickej bezpečnosti.
5. Agentúra posilňuje kyberneticko-bezpečnostné spôsobilosti na úrovni Únie s cieľom doplniť činnosť členských štátov v prevencii kybernetických hrozieb a reakcii na ne, najmä pri cezhraničných incidentoch.
6. Agentúra podporuje využívanie certifikácie, a to aj prispievaním k vytvoreniu a uchovávaní rámca certifikácie kybernetickej bezpečnosti na úrovni Únie v súlade s hlavou III tohto nariadenia, aby sa posilnila transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti produktov a služieb IKT, čím sa posilní dôvera v digitálny vnútorný trh.

7. Agentúra presadzuje vysoké povedomie občanov a podnikov o otázkach kybernetickej bezpečnosti.

Článok 5

Úlohy spojené s tvorbou a vykonávaním politiky a legislatívy Únie

Agentúra prispieva k tvorbe a vykonávaniu politiky a legislatívy Únie tým, že:

1. pomáha a radí, najmä poskytuje nezávislé stanoviská a zabezpečuje prípravné práce k vypracovaniu a preskúmaniu politiky a legislatívy Únie v oblasti kybernetickej bezpečnosti, ale i odvetvových politík a legislatívnych iniciatív, ktoré rozmer kybernetickej bezpečnosti zahŕňajú;
2. pomáha členským štátom pri konzistentnom vykonávaní politiky a legislatívy Únie v oblasti kybernetickej bezpečnosti, najmä v súvislosti so smernicou (EÚ) 2016/1148, a to aj poskytovaním stanovísk, usmernení, poradenstva a osvedčených postupov v oblastiach ako riadenie rizík, oznamovanie incidentov a zdieľanie informácií, a zároveň v tomto smere uľahčuje výmenu informácií o osvedčených postupoch medzi príslušnými orgánmi;
3. prispieva k práci skupiny pre spoluprácu v zmysle článku 11 smernice (EÚ) 2016/1148 v podobe odborných poznatkov a poradenstva;
4. podporuje:
 1. tvorbu a vykonávanie politiky Únie v oblasti elektronickej identifikácie a dôveryhodných služieb, najmä formou poradenstva a technických usmernení, ako aj uľahčovaním výmeny osvedčených postupov medzi príslušnými orgánmi;
 2. presadzovanie zvýšenej úrovne bezpečnosti elektronických komunikácií, a to aj formou odborných poznatkov a poradenstva, ako aj uľahčovaním výmeny osvedčených postupov medzi príslušnými orgánmi;
5. podporuje pravidelné preskúmanie politickej činnosti Únie poskytovaním výročnej správy o stave vykonávania príslušného právneho rámca z hľadiska:
 - a) oznámení členských štátov o incidentoch, ktoré podľa článku 10 ods. 3 smernice (EÚ) 2016/1148 skupine pre spoluprácu poskytujú jednotné kontaktné miesta;
 - b) oznámení o narušení bezpečnosti a integrity u poskytovateľov dôveryhodných služieb, ktoré agentúre poskytujú orgány dohľadu podľa článku 19 ods. 3 nariadenia (EÚ) 910/2014;
 - c) oznámení o narušení bezpečnosti, ktoré podávajú podniky poskytujúce verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby a ktoré agentúre postupujú príslušné orgány podľa článku 40 [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie].

Článok 6
Úlohy spojené s budovaním kapacít

1. Agentúra pomáha:
 - a) členským štátom v ich úsilí zlepšovať prevenciu, odhaľovanie a analýzu kybernetických problémov a incidentov a schopnosť na ne reagovať vrátane poskytovania potrebných vedomostí a odborných poznatkov;
 - b) inštitúciám, orgánom, úradom a agentúram Únie v ich úsilí zlepšovať prevenciu, odhaľovanie a analýzu kybernetických problémov a incidentov a schopnosť na ne reagovať, a to primeranou podporou tímu reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (ďalej len „tím CERT-EU“);
 - c) členským štátom na požiadanie pri tvorbe vnútroštátnych jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „jednotky CSIRT“) podľa článku 9 ods. 5 smernice (EÚ) 2016/1148;
 - d) členským štátom na požiadanie pri vypracúvaní národných stratégií v oblasti bezpečnosti sietí a informačných systémov podľa článku 7 ods. 2 smernice (EÚ) 2016/1148; v záujme propagácie osvedčených postupov agentúra zároveň podporuje šírenie týchto stratégií v Únii a monitoruje pokrok v ich vykonávaní;
 - e) inštitúciám Únie pri príprave a revízii kyberneticko-bezpečnostných stratégií Únie, podpore ich šírenia a monitorovaní pokroku v ich vykonávaní;
 - f) jednotkám CSIRT členských štátov a Únie pri zdokonaľovaní ich spôsobilostí, a to i presadzovaním dialógu a výmeny informácií s cieľom zabezpečiť, aby sa s ohľadom na aktuálny stupeň vývoja každá jednotka CSIRT vyznačovala spoločným súborom minimálnych spôsobilostí a aby fungovala v súlade s osvedčenými postupmi;
 - g) členským štátom organizáciou každoročných rozsiahlych kyberneticko-bezpečnostných cvičení na úrovni Únie v zmysle článku 7 ods. 6 a formulovaním politických odporúčaní na základe hodnotenia týchto cvičení a takto získaných poznatkov;
 - h) relevantným verejným orgánom poskytovaním školení v oblasti kybernetickej bezpečnosti, podľa potreby v spolupráci so zainteresovanými stranami;
 - i) skupine pre spoluprácu výmenou osvedčených postupov v zmysle článku 11 ods. 3 písm. l) smernice (EÚ) 2016/1148, najmä z hľadiska identifikácie prevádzkovateľov základných služieb členskými štátmi, pokiaľ ide o riziká a incidenty, a to aj v súvislosti s cezhraničnou previazanosťou.
2. Agentúra podporuje zriaďovanie a zabezpečuje trvalú podporu odvetvových stredísk pre výmenu a analýzu informácií (ISAC), a to najmä v odvetviach uvedených v prílohe II k smernici (EÚ) 2016/1148, poskytovaním osvedčených postupov a usmernení o dostupných nástrojoch, postupoch i riešeniach regulačných otázok spojených s výmenou informácií.

Článok 7

Úlohy spojené s operačnou spoluprácou na úrovni Únie

1. Agentúra podporuje operačnú spoluprácu medzi príslušnými verejnými orgánmi i medzi zainteresovanými stranami.
2. Agentúra na operačnej úrovni spolupracuje a vytvára synergie s inštitúciami, orgánmi, úradmi a agentúrami Únie vrátane tímu CERT-EU, útvarov, ktoré sa zaoberajú počítačovou kriminalitou, a orgánov dohľadu zodpovedných za ochranu súkromia a osobných údajov, na účely riešenia otázok spoločného záujmu, a to aj:
 - a) výmenou know-how a osvedčených postupov;
 - b) poskytovaním poradenstva a usmernení k otázkam spojeným s kybernetickou bezpečnosťou;
 - c) zavedením praktických opatrení na výkon konkrétnych úloh po konzultácii s Komisiou.
3. Agentúra zabezpečuje sekretariát siete jednotiek CSIRT podľa článku 12 ods. 2 smernice (EÚ) 2016/1148 a aktívne podporuje výmenu informácií a spoluprácu jej členov.
4. Agentúra prispieva k operačnej spolupráci v rámci siete jednotiek CSIRT podporou členských štátov tak, že:
 - a) im radí, ako zdokonaľiť spôsobilosť predchádzať incidentom, odhaľovať ich a reagovať na ne;
 - b) im na požiadanie poskytuje technickú pomoc pri incidentoch s významným alebo závažným vplyvom;
 - c) analyzuje zraniteľné miesta, artefakty a incidenty.

Pri výkone týchto úloh agentúra a tím CERT-EU štruktúrované spolupracujú s cieľom využiť synergie, najmä z operačného pohľadu.

5. Na žiadosť dvoch alebo viacerých dotknutých členských štátov a výlučne s cieľom poradenstva na predchádzanie budúcim incidentom agentúra poskytne podporu alebo vykoná technické *ex post* skúmanie v nadväznosti na oznámenia podnikov zasiahnutých incidentmi s významným alebo závažným vplyvom v zmysle smernice (EÚ) 2016/1148. Agentúra takéto skúmanie vykoná aj na riadne odôvodnenú žiadosť Komisie so súhlasom dotknutých členských štátov, ak sa takéto incidenty týkajú viac než dvoch členských štátov.

Rozsah preskúmania i jeho postup dohodnú dotknuté členské štáty s agentúrou, pričom nesmie byť dotknuté žiadne prebiehajúce vyšetrowanie trestných činov v spojení s daným incidentom. Výsledkom preskúmania je záverečná technická správa, ktorú zostaví agentúra najmä na základe informácií a pripomienok od dotknutých členských štátov a podniku(-ov) a ktorú odsúhlasia dotknuté členské štáty. Zhrnutie tejto správy zamerané na odporúčania v záujme prevencie budúcich incidentov sa poskytne sieti jednotiek CSIRT.

6. Agentúra každoročne organizuje kyberneticko-bezpečnostné cvičenia na úrovni Únie a na požiadanie podporuje členské štáty a inštitúcie, agentúry a orgány EÚ pri organizácii ich cvičení. Každoročné cvičenia na úrovni Únie zahŕňajú technické, operačné a strategické prvky a pomáhajú s prípravou spoločnej reakcie na rozsiahle cezhraničné kybernetické incidenty na úrovni Únie. Agentúra zároveň prispieva a

podľa potreby pomáha organizovať odvetvové kyberneticko-bezpečnostné cvičenia spolu so strediskami ISAC a zároveň strediskám ISAC umožní účasť aj na kyberneticko-bezpečnostných cvičeniach na úrovni Únie.

7. Agentúra vypracúva pravidelnú technickú situačnú správu EÚ o kybernetických incidentoch a hrozbách, ktorá vychádza z verejne dostupných informácií, jej vlastných analýz a správ, ktoré okrem iných poskytnú: jednotky CSIRT členských štátov (dobrovoľne) alebo jednotné kontaktné miesta podľa smernice NIS (v súlade s článkom 14 ods. 5 smernice NIS); Európske centrum boja proti počítačovej kriminalite (EC3) pri Europole, tím CERT-EU.
8. Agentúra prispieva k vypracovaniu spoločnej reakcie (na úrovni Únie i na úrovni členských štátov) na rozsiahle cezhraničné incidenty alebo krízy v oblasti kybernetickej bezpečnosti, a to najmä:
 - a) zhromaždením správ z národných zdrojov s cieľom prispieť k vytvoreniu spoločného situačného povedomia;
 - b) zaistením efektívneho toku informácií a zabezpečením eskalačných mechanizmov medzi sieťou jednotiek CSIRT a subjektmi zodpovednými za technické a politické rozhodnutia na úrovni Únie;
 - c) podporou technického riešenia incidentu či krízy vrátane uľahčovania výmeny technických riešení medzi členskými štátmi;
 - d) podporou komunikácie s verejnosťou o danom incidente alebo kríze;
 - e) testovaním plánov spoločnej reakcie na takéto incidenty alebo krízy.

Článok 8

Úlohy spojené s trhom, certifikáciou kybernetickej bezpečnosti a normami

Agentúra:

- a) podporuje a presadzuje tvorbu a vykonávanie politiky Únie v oblasti certifikácie kybernetickej bezpečnosti produktov a služieb IKT v zmysle hlavy III tohto nariadenia, a to tak, že:
 1. vypracúva kandidátske európske systémy certifikácie kybernetickej bezpečnosti produktov a služieb IKT v súlade s článkom 44 tohto nariadenia;
 2. pomáha Komisii pri zabezpečovaní funkcie sekretariátu európskej skupiny pre certifikáciu kybernetickej bezpečnosti podľa článku 53 tohto nariadenia;
 3. zostavuje a uverejňuje usmernenia a vypracúva osvedčené postupy z hľadiska kyberneticko-bezpečnostných požiadaviek na produkty a služby IKT, a to v spolupráci s vnútroštátnymi orgánmi dohľadu nad certifikáciou a s príslušným odvetvím;
- b) podporuje zavádzanie a využívanie európskych i medzinárodných noriem v oblasti riadenia rizík a bezpečnosti produktov a služieb IKT, a zároveň v spolupráci s členskými štátmi pripravuje odporúčania a usmernenia v technických oblastiach spojených s bezpečnostnými požiadavkami kladenými na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, ako aj v oblasti už existujúcich noriem vrátane vnútroštátnych noriem členských štátov, podľa článku 19 ods. 2 smernice (EÚ) 2016/1148;

- c) vykonáva a šíri pravidelné analýzy hlavných trendov na trhu kybernetickej bezpečnosti, tak na strane dopytu, ako aj ponuky, s cieľom podporiť trh kybernetickej bezpečnosti v Únii.

Článok 9

Úlohy spojené so znalosťami, informáciami a zvyšovaním povedomia

Agentúra:

- a) analyzuje nastupujúce technológie a poskytuje tematicky zamerané posúdenia očakávaných spoločenských, právnych, hospodárskych a regulačných účinkov technologickej inovácie na kybernetickú bezpečnosť;
- b) vykonáva dlhodobé strategické analýzy kybernetických hrozieb a incidentov s cieľom identifikovať nové trendy a pomôcť predchádzať problémom spojeným s kybernetickou bezpečnosťou;
- c) v spolupráci s odborníkmi orgánov členských štátov poskytuje poradenstvo, usmernenia a osvedčené postupy v oblasti bezpečnosti sietí a informačných systémov, a najmä bezpečnosti internetovej infraštruktúry a infraštruktúr, o ktoré sa opierajú odvetvia uvedené v prílohe II k smernici (EÚ) 2016/1148;
- d) zhromažďuje, organizuje a na vyhradenom portáli uverejňuje informácie o kybernetickej bezpečnosti, ktoré poskytli inštitúcie, agentúry a orgány Únie;
- e) zvyšuje verejné povedomie o kyberneticko-bezpečnostných rizikách a odporúča jednotlivým používateľom – občanom i organizáciám osvedčené postupy;
- f) zhromažďuje a analyzuje verejne dostupné informácie o závažných incidentoch a pripravuje správy s cieľom poskytnúť usmernenia pre podniky i občanov v celej Únii;
- g) v spolupráci s členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie organizuje pravidelné osvetové kampane na zvýšenie kybernetickej bezpečnosti a jej viditeľnosti v Únii.

Článok 10

Úlohy spojené s výskumom a inováciou

V oblasti výskumu a inovácií agentúra:

- a) radí Únii a členským štátom o potrebách a prioritách výskumu v oblasti kybernetickej bezpečnosti s cieľom umožniť účinnú reakciu na existujúce i nové riziká a hrozby, a to i v súvislosti s novými a nastupujúcimi informačnými a komunikačnými technológiami, a účinne používať technológie na prevenciu rizika;
- b) ak na ňu Komisia deleguje príslušné právomoci, podieľa sa na implementačnej fáze programov financovania výskumu a inovácie, alebo sa na nich zúčastňuje ako príjemca.

Článok 11

Úlohy spojené s medzinárodnou spoluprácou

Agentúra prispieva k úsiliu Únie o spoluprácu s tretími krajinami a medzinárodnými organizáciami s cieľom podporiť medzinárodnú spoluprácu v kyberneticko-bezpečnostných otázkach, a to tým, že:

- a) sa v náležitých prípadoch angažuje ako pozorovateľ pri organizácii medzinárodných cvičení, analyzuje ich výsledky a podáva o nich správy správnej rade;
- b) na žiadosť Komisie sprostredkúva výmenu osvedčených postupov medzi relevantnými medzinárodnými organizáciami;
- c) na požiadanie poskytuje Komisii odborné poznatky.

KAPITOLA II ORGANIZÁCIA AGENTÚRY

Článok 12

Štruktúra

Administratívna a riadiaca štruktúra agentúry pozostáva z týchto prvkov:

- a) správna rada, ktorá plní funkcie stanovené v článku 14;
- b) výkonná rada, ktorá plní funkcie stanovené v článku 18;
- c) výkonný riaditeľ, ktorý plní funkcie stanovené v článku 19 a
- d) stála skupina zainteresovaných strán, ktorá plní funkcie stanovené v článku 20.

ODDIEL 1 SPRÁVNA RADA

Článok 13

Zloženie správnej rady

1. Správnu radu tvorí jeden zástupca každého členského štátu a dvaja zástupcovia vymenovaní Komisiou. Všetci zástupcovia majú hlasovacie právo.
2. Každý člen správnej rady má náhradníka, ktorý zastupuje člena v jeho neprítomnosti.
3. Členovia správnej rady a ich náhradníci sa vymenúvajú na základe ich znalostí v oblasti kybernetickej bezpečnosti s prihliadnutím na relevantné riadiace, administratívne a rozpočtové zručnosti. Komisia a členské štáty sa vynasnažia obmedziť fluktuáciu svojich zástupcov v správnej rade s cieľom zabezpečiť kontinuitu jej práce. Komisia a členské štáty sa usilujú o vyvážené zastúpenie mužov a žien v správnej rade.
4. Funkčné obdobie členov správnej rady a ich náhradníkov je štyri roky. Toto obdobie je obnoviteľné.

Článok 14
Funkcie správnej rady

1. Správna rada:

- a) vymedzuje všeobecné smerovanie činnosti agentúry a zabezpečuje, aby agentúra pracovala v súlade s pravidlami a zásadami stanovenými v tomto nariadení. Zabezpečuje aj súlad práce agentúry s činnosťami vykonávanými členskými štátmi i na úrovni Únie;
- b) prijíma návrh jednotného programového dokumentu uvedeného v článku 21 pred jeho predložením Komisii na posúdenie;
- c) zohľadňujúc posúdenie Komisie prijíma jednotný programový dokument agentúry dvojtretinovou väčšinou členských hlasov v súlade s článkom 17;
- d) dvojtretinovou väčšinou členských hlasov prijíma ročný rozpočet agentúry a vykonáva ostatné funkcie spojené s rozpočtom agentúry podľa kapitoly III;
- e) posudzuje a prijíma konsolidovanú výročnú správu o činnosti agentúry, pričom posúdenie i správu do 1. júla nasledujúceho roka zasiela Európskemu parlamentu, Rade, Komisii a Dvoru audítorov. Výročná správa zahŕňa účtovné výkazy a opisuje sa v nej, do akej miery agentúra splnila svoje ukazovatele výkonnosti. Výročná správa sa zverejní;
- f) prijíma rozpočtové pravidlá platné pre agentúru v súlade s článkom 29;
- g) prijíma stratégiu boja proti podvodom, ktorá musí byť primeraná riziku podvodov so zreteľom na analýzu efektívnosti nákladov na opatrenia, ktoré sa majú vykonávať;
- h) prijíma pravidlá predchádzania konfliktom záujmov svojich členov a ich riešenia;
- i) zabezpečí primerané následné opatrenia v nadväznosti na zistenia a odporúčania vyplývajúce z vyšetrovania Európskeho úradu pre boj proti podvodom (OLAF) a rôznych správ a hodnotení interného alebo externého auditu;
- j) prijíma svoj rokovací poriadok;
- k) v súlade s odsekom 2 vykonáva vo vzťahu k pracovníkom agentúry právomoci udelené služobným poriadkom zamestnancov menovaciemu orgánu a podmienkami zamestnávania ostatných zamestnancov Európskej únie orgánu oprávnenému uzatvárať pracovné zmluvy (ďalej len „právomoci menovacieho orgánu“);
- l) prijíma predpisy vykonávajúce služobný poriadok a podmienky zamestnávania ostatných zamestnancov v súlade s postupom uvedeným v článku 110 služobného poriadku;
- m) vymenúva výkonného riaditeľa a v náležitých prípadoch predlžuje jeho funkčné obdobie alebo ho z funkcie odvoláva v súlade s článkom 33 tohto nariadenia;
- n) vymenúva účtovníka, ktorým môže byť účtovník Komisie a ktorý je pri výkone svojich povinností úplne nezávislý;

- o) prijíma všetky rozhodnutia o zriadení vnútorných štruktúr agentúry a v prípade potreby o ich zmene, pričom prihliada na potreby činnosti agentúry a zásadu riadneho finančného hospodárenia;
 - p) schvaľuje dohadovanie modalít spolupráce v súlade s článkami 7 a 39.
- 2. Správna rada v súlade s článkom 110 služobného poriadku prijíma rozhodnutie na základe článku 2 ods. 1 služobného poriadku a článku 6 podmienok zamestnávania ostatných zamestnancov, ktorým deleguje príslušné právomoci menovacieho orgánu na výkonného riaditeľa a ktorým vymedzuje podmienky, za ktorých možno toto delegovanie právomoci pozastaviť. Výkonný riaditeľ je oprávnený tieto právomoci delegovať ďalej.
- 3. Ak si to vyžadujú mimoriadne okolnosti, správna rada môže na základe rozhodnutia dočasne pozastaviť delegovanie právomocí menovacieho orgánu na výkonného riaditeľa a na subjekty, ktorým ďalej delegoval právomoc, a tieto právomoci vykonávať sama alebo ich delegovať na jedného zo svojich členov alebo na zamestnanca, ktorý nie je výkonným riaditeľom.

Článok 15

Predseda správnej rady

Správna rada spomedzi svojich členov dvoj tretinovou väčšinou hlasov volí svojho predsedu a zástupcu predsedu na obdobie štyroch rokov, ktoré je obnoviteľné raz. Ak však ich členstvo v správnej rade kedykoľvek počas ich funkčného obdobia zanikne, ich funkčné obdobie sa automaticky končí k danému dátumu. Ak predseda nie je schopný plniť si svoje povinnosti, zástupca predsedu ho nahradí *ex officio*.

Článok 16

Zasadnutia správnej rady

- 1. Zasadnutia správnej rady zvoláva jej predseda.
- 2. Riadne zasadnutia správnej rady sa konajú aspoň dvakrát ročne. Na žiadosť predsedu, Komisie alebo najmenej tretiny svojich členov zasadá správna rada aj mimoriadne.
- 3. Výkonný riaditeľ sa zúčastňuje na zasadnutiach správnej rady, avšak bez hlasovacieho práva.
- 4. Na zasadnutiach správnej rady sa môžu na pozvanie predsedu zúčastniť členovia stálej skupiny zainteresovaných strán, avšak bez hlasovacieho práva.
- 5. Členom správnej rady a ich náhradníkom môžu v súlade s rokovacím poriadkom pomáhať poradcovia alebo experti.
- 6. Sekretariát pre správnu radu zabezpečuje agentúra.

Článok 17

Pravidlá hlasovania správnej rady

- 1. Správna rada prijíma rozhodnutia väčšinou hlasov svojich členov.
- 2. Dvoj tretinovú väčšinu hlasov všetkých členov správnej rady sa vyžaduje v prípade jednotného programového dokumentu, ročného rozpočtu, menovania a odvolania výkonného riaditeľa či predĺženia jeho funkčného obdobia.

3. Každý člen má jeden hlas. Ak je člen správnej rady neprítomný, toto hlasovacie právo môže uplatniť jeho náhradník.
4. Predseda sa na hlasovaní zúčastňuje.
5. Výkonný riaditeľ sa na hlasovaní nezúčastňuje.
6. V rokovacom poriadku správnej rady sa stanovujú podrobnejšie mechanizmy hlasovania, najmä podmienky, za ktorých môže člen konať v mene iného člena.

ODDIEL 2 VÝKONNÁ RADA

Článok 18 Výkonná rada

1. Správnej rade pomáha výkonná rada.
2. Výkonná rada:
 - a) pripravuje rozhodnutia, ktoré má prijať správna rada;
 - b) spolu so správnu radou zabezpečuje prijatie vhodných opatrení v nadväznosti na zistenia a odporúčania vyplývajúce z vyšetrovaní úradu OLAF a z rôznych interných alebo externých audítorských správ a hodnotení;
 - c) bez toho, aby boli dotknuté zodpovednosti výkonného riaditeľa stanovené v článku 19, pomáha a radí výkonnému riaditeľovi pri vykonávaní rozhodnutí správnej rady v administratívnej a rozpočtovej oblasti podľa článku 19.
3. Výkonná rada pozostáva z piatich členov vymenovaných spomedzi členov správnej rady, z ktorých jedným je predseda správnej rady, ktorý môže predsedáť aj výkonnej rade, a ďalším je jeden zo zástupcov Komisie. Výkonný riaditeľ sa zúčastňuje na zasadnutiach výkonnej rady, ale nemá hlasovacie právo.
4. Funkčné obdobie členov výkonnej rady je štyri roky. Toto obdobie je obnoviteľné.
5. Výkonná rada zasadá aspoň raz za tri mesiace. Predseda výkonnej rady zvoláva ďalšie zasadnutia na žiadosť jej členov.
6. Rokovací poriadok výkonnej rady stanovuje správna rada.
7. Ak je to potrebné z dôvodu naliehavosti, výkonná rada môže prijať určité dočasné rozhodnutia v mene správnej rady, a to najmä o otázkach administratívneho riadenia vrátane rozhodnutí o pozastavení delegovania právomocí menovacieho orgánu a o rozpočtových záležitostiach.

ODDIEL 3 VÝKONNÝ RIADITEĽ

Článok 19 Zodpovednosti výkonného riaditeľa

1. Agentúru riadi jej výkonný riaditeľ, ktorý je pri výkone svojich povinností nezávislý. Výkonný riaditeľ sa zodpovedá správnej rade.

2. Výkonný riaditeľ podáva na vyzvanie Európskemu parlamentu správu o plnení svojich povinností. Rada môže vyzvať výkonného riaditeľa, aby podal správu o plnení svojich povinností.
3. Výkonný riaditeľ je zodpovedný za:
 - a) každodennú správu agentúry;
 - b) vykonávanie rozhodnutí prijatých správnu radou;
 - c) prípravu návrhu jednotného programového dokumentu a jeho predloženie správnej rade na schválenie pred tým, než sa predloží Komisii;
 - d) vykonávanie jednotného programového dokumentu a zodpovedajúce informovanie správnej rady;
 - e) vypracovanie konsolidovanej výročnej správy o činnostiach agentúry a jej predloženie správnej rade na posúdenie a prijatie;
 - f) vypracovanie akčného plánu v nadväznosti na závery spätných hodnotení a predloženie správy o pokroku Komisii každé dva roky;
 - g) prípravu akčného plánu v nadväznosti na závery správ z interného alebo externého auditu, ako aj z vyšetrovania Európskeho úradu pre boj proti podvodom (OLAF) a za predkladanie správ o pokroku, a to dvakrát ročne Komisii a pravidelne správnej rade;
 - h) prípravu návrhu rozpočtových pravidiel platných pre agentúru;
 - i) prípravu návrhu výkazu odhadov príjmov a výdavkov agentúry a plnenie jej rozpočtu;
 - j) ochranu finančných záujmov Únie uplatňovaním preventívnych opatrení proti podvodom, korupcii a akýmkoľvek iným nezákonným činnostiam, účinnými kontrolami, ak sa zistia nezrovnalosti spätným získaním neoprávnene vyplatených súm, a prípadne účinnými, primeranými a odradzujúcimi administratívnymi a finančnými sankciami;
 - k) vypracovanie stratégie agentúry pre boj proti podvodom a jej predloženie správnej rade na schválenie;
 - l) nadviazanie a udržiavanie kontaktov s podnikateľskou komunitou a spotrebiteľskými organizáciami na zabezpečenie pravidelného dialógu s príslušnými zainteresovanými stranami;
 - m) ostatné úlohy, ktoré sú výkonnému riaditeľovi pridelené týmto nariadením.
4. V prípade potreby môže výkonný riaditeľ v rámci mandátu agentúry a v súlade s jej cieľmi a úlohami vytvoriť ad hoc pracovné skupiny zložené z expertov vrátane tých, ktorí pochádzajú z príslušných orgánov členských štátov. Správna rada o tom musí byť vopred informovaná. Postupy týkajúce sa najmä zloženia týchto pracovných skupín, menovania príslušných expertov výkonným riaditeľom a fungovania pracovných skupín sa spresnia vo vnútorných pravidlách činnosti agentúry.
5. Výkonný riaditeľ rozhodne, či treba v záujme účinného a efektívneho plnenia úloh agentúry umiestniť jej zamestnancov do niektorého alebo viacerých členských štátov. Pred tým, ako výkonný riaditeľ rozhodne o zriadení miestnej kancelárie, získa

vopred súhlas Komisie, správnej rady a príslušných členských štátov. V danom rozhodnutí sa vymedzí rozsah činností, ktoré sa majú v miestnej kancelárii vykonávať, a to tak, aby sa zabránilo vzniku zbytočných nákladov a duplicite administratívnych funkcií agentúry. Ak je to vhodné alebo požadované, uzavrie sa s príslušnými členskými štátmi dohoda.

ODDIEL 4

STÁLA SKUPINA ZAJINTERESOVANÝCH STRÁN

Článok 20

Stála skupina zainteresovaných strán

1. Správna rada konajúca na návrh výkonného riaditeľa zriadi stálu skupinu zainteresovaných strán zloženú z uznávaných expertov zastupujúcich príslušné zainteresované strany, ako sú odvetvie IKT, poskytovatelia verejne dostupných elektronických komunikačných sietí alebo služieb, spotrebiteľské skupiny, akademickí experti na kybernetickú bezpečnosť a zástupcovia príslušných orgánov notifikovaní podľa [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie], ako aj orgánov presadzovania práva a ochrany údajov.
2. Postupy stálej skupiny zainteresovaných strán, najmä z hľadiska počtu, zloženia a menovania jej členov správnou radou, návrhu výkonného riaditeľa a činnosti tejto skupiny sa vymedzia vo vnútorných pravidlách činnosti agentúry a zverejnia sa.
3. Stálej skupine zainteresovaných strán predsedá výkonný riaditeľ alebo ktorákoľvek osoba, ktorú výkonný riaditeľ v jednotlivých prípadoch vymenuje.
4. Funkčné obdobie členov stálej skupiny zainteresovaných strán je dva a pol roka. Členovia správnej rady nemôžu byť členmi stálej skupiny zainteresovaných strán. Experti z Komisie a členských štátov sú oprávnení zúčastňovať sa na zasadnutiach stálej skupiny zainteresovaných strán a podieľať sa na jej práci. Na zasadnutia stálej skupiny zainteresovaných strán a k účasti na jej práci možno prizvať aj zástupcov iných orgánov, ktoré výkonný riaditeľ považuje za relevantné a ktoré nie sú členmi stálej skupiny zainteresovaných strán.
5. Stála skupina zainteresovaných strán agentúre radí v súvislosti s vykonávaním jej činností. Predovšetkým radí výkonnému riaditeľovi pri vypracúvaní návrhu pracovného programu agentúry a pri zabezpečovaní komunikácie s príslušnými zainteresovanými stranami o všetkých otázkach týkajúcich sa pracovného programu.

ODDIEL 5

ČINNOSŤ

Článok 21

Jednotný programový dokument

1. Agentúra vykonáva svoje činnosti v súlade s jednotným programovým dokumentom, ktorý zahŕňa jej ročné a viacročné plánovanie vrátane všetkých jej plánovaných činností.

2. Výkonný riaditeľ každý rok vypracúva návrh jednotného programového dokumentu, ktorý obsahuje ročné a viacročné plánovanie vrátane plánovania zodpovedajúcich ľudských a finančných zdrojov v súlade s článkom 32 delegovaného nariadenia Komisie (EÚ) č. 1271/2013³⁶, pričom zohľadní usmernenia stanovené Komisiou.
3. Správna rada každoročne jednotný programový dokument uvedený v odseku 1 prijme do 30. novembra a zašle ho Európskemu parlamentu, Rade a Komisii najneskôr 31. januára nasledujúceho roka, pričom im zasiela aj všetky neskôr aktualizované verzie uvedeného dokumentu.
4. Jednotný programový dokument nadobudne konečné znenie po konečnom prijatí všeobecného rozpočtu Únie, pričom sa podľa potreby náležite upraví.
5. Ročný pracovný program zahŕňa podrobné ciele a očakávané výsledky vrátane ukazovateľov výkonnosti. Obsahuje aj opis opatrení, ktoré sa majú financovať, a odhad finančných a ľudských zdrojov vyčlenených na každé opatrenie v súlade so zásadami zostavovania rozpočtu a riadenia podľa činností. Ročný pracovný program musí byť v súlade s viacročným pracovným programom uvedeným v odseku 7. Jasne sa v ňom vymedzia úlohy, ktoré sa oproti predošlému rozpočtovému roku pridali, zmenili alebo zrušili.
6. Ak sa agentúre zverí nová úloha, správna rada prijatý ročný pracovný program zmení. Každá podstatná zmena ročného pracovného programu sa prijíma rovnakým postupom ako pôvodný ročný pracovný program. Právomoc vykonávať nepodstatné zmeny ročného pracovného programu môže správna rada delegovať na výkonného riaditeľa.
7. Vo viacročnom pracovnom programe sa stanovuje všeobecné strategické plánovanie vrátane cieľov, očakávaných výsledkov a ukazovateľov výkonnosti. Zároveň sa ňom uvádza plánovanie zdrojov vrátane viacročného rozpočtu a zamestnancov.
8. Plánovanie zdrojov sa každoročne aktualizuje. Strategické plánovanie sa aktualizuje podľa potreby, najmä so zámerom zohľadniť výsledky hodnotenia uvedeného v článku 56.

Článok 22

Vyhlásenie o záujmoch

1. Výkonný riaditeľ, ako aj každý člen správnej rady a každý úradník dočasne vyslaný členským štátom predloží vyhlásenie o záväzkoch a vyhlásenie o absencii alebo existencii akýchkoľvek priamych alebo nepriamych záujmov, ktoré by sa mohli považovať za záujmy ovplyvňujúce ich nezávislosť. Vyhlásenia musia byť presné a úplné, každoročne sa poskytujú písomne a podľa potreby sa aktualizujú.
2. Členovia správnej rady, výkonný riaditeľ a externí experti, ktorí sa zúčastňujú v *ad hoc* pracovných skupinách, presne a úplne oznámia najneskôr na začiatku každého zasadnutia akékoľvek záujmy, ktoré by sa mohli považovať za záujmy ovplyvňujúce

³⁶ Delegované nariadenie Komisie (EÚ) č. 1271/2013 z 30. septembra 2013 o rámcovom nariadení o rozpočtových pravidlách pre subjekty uvedené v článku 208 nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) č. 966/2012. (Ú. v. EÚ L 328, 7.12.2013, s. 42).

ich nezávislosť v súvislosti s bodmi programu, a zdržia sa účasti na diskusiách k týmto bodom a na hlasovaní o nich.

3. Agentúra vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia pre pravidlá o vyhláseniach o záujmoch uvedených v odsekoch 1 a 2.

Článok 23 **Transparentnosť**

1. Agentúra vykonáva svoje činnosti s vysokým stupňom transparentnosti a v súlade s článkom 25.
2. Agentúra zabezpečí, aby verejnosť a všetky zainteresované strany dostávali náležité, objektívne, spoľahlivé a ľahko dostupné informácie, najmä o výsledkoch jej práce. Agentúra takisto zverejňuje vyhlásenia o záujmoch predkladané podľa článku 22.
3. Správna rada konajúc na návrh výkonného riaditeľa môže subjektom, ktoré majú záujem, povoliť pozorovanie postupov niektorých činností agentúry.
4. Agentúra vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia na vykonávanie pravidiel transparentnosti uvedených v odsekoch 1 a 2.

Článok 24 **Dôvernosť informácií**

1. Bez toho, aby bol dotknutý článok 25, agentúra nesmie poskytovať tretím stranám informácie, ktoré spracúva alebo získava a v súvislosti s ktorými bola podaná odôvodnená žiadosť o úplné alebo čiastočné dôverné zaobchádzanie.
2. Členovia správnej rady, výkonný riaditeľ, členovia stálej skupiny zainteresovaných strán, externí experti zúčastňujúci sa ad hoc pracovných skupín a zamestnanci agentúry vrátane úradníkov dočasne vyslaných členskými štátmi musia spĺňať aj po skončení povinností požiadavky na dôvernosť informácií podľa článku 339 Zmluvy o fungovaní Európskej únie (ZFEÚ).
3. Agentúra vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia na vykonávanie pravidiel týkajúcich sa dôvernosti informácií uvedených v odsekoch 1 a 2.
4. Ak je to potrebné pre vykonávanie úloh agentúry, správna rada rozhodne, že agentúre povolí pracovať s utajovanými skutočnosťami. V takom prípade správna rada po dohode s útvarmi Komisie prijme vnútorné pravidlá činnosti, ktorými sa uplatňujú zásady bezpečnosti stanovené v rozhodnutiach Komisie (EÚ, Euratom) 2015/443³⁷ a 2015/444³⁸. Tieto pravidlá musia zahŕňať ustanovenia týkajúce sa výmeny, spracovania a uchovávaní utajovaných skutočností.

³⁷ [Rozhodnutie Komisie \(EÚ, Euratom\) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii](#) (Ú. v. EÚ L 72, 17.3.2015, s. 41).

³⁸ [Rozhodnutie Komisie \(EÚ, Euratom\) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ](#) (Ú. v. EÚ L 72, 17.3.2015, s. 53).

Článok 25

Prístup k dokumentom

1. Na dokumenty, ktoré má agentúra v držbe, 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 podanej ombudsmanovi podľa článku 228 ZFEÚ alebo konania pred Súdnym dvorom Európskej únie podľa článku 263 ZFEÚ.

KAPITOLA III ZOSTAVOVANIE A ŠTRUKTÚRA ROZPOČTU

Článok 26

Zostavovanie rozpočtu

1. Výkonný riaditeľ každoročne vypracúva návrh výkazu odhadov príjmov a výdavkov agentúry na nasledujúci rozpočtový rok a postupuje ho správnej rade spolu s návrhom plánu pracovných miest. Príjmy a výdavky musia byť v rovnováhe.
2. Správna rada každý rok na základe návrhu výkazu odhadov príjmov a výdavkov uvedeného v odseku 1 vytvorí výkaz odhadov príjmov a výdavkov agentúry na nasledujúci rozpočtový rok.
3. Výkaz odhadov uvedený v odseku 2, ktorý je súčasťou návrhu jednotného programového dokumentu, správna rada každoročne do 31. januára zasiela Komisii a tretím krajinám, s ktorými Únia uzatvorila dohody v súlade s článkom 39.
4. Komisia na základe tohto výkazu odhadov zaradí do návrhu rozpočtu Únie odhady, ktoré pokladá za potrebné pre plán pracovných miest, a výšku príspevku, ktorá sa má uhradiť zo všeobecného rozpočtu, ktoré predloží Európskemu parlamentu a Rade v súlade s článkom 313 a 314 ZFEÚ.
5. Európsky parlament a Rada schvaľujú rozpočtové prostriedky na príspevok agentúre.
6. Európsky parlament a Rada prijímajú plán pracovných miest agentúry.
7. Správna rada prijíma rozpočet agentúry spolu s jednotným programovým dokumentom. Rozpočet sa stáva konečným po prijatí všeobecného rozpočtu Únie s konečnou platnosťou. Správna rada v prípade potreby upraví rozpočet a jednotný programový dokument agentúry v súlade so všeobecným rozpočtom Únie.

Článok 27

Štruktúra rozpočtu

1. Bez toho, aby boli dotknuté iné zdroje, príjmy agentúry zahŕňajú:
 - a) príspevok z rozpočtu Únie;
 - b) príjmy určené na krytie konkrétnych výdavkových položiek v súlade s jej rozpočtovými pravidlami uvedenými v článku 29;

- c) finančné prostriedky Únie na základe dohôd o príspevku alebo *ad hoc* grantov v súlade s jej rozpočtovými pravidlami uvedenými v článku 29 a s ustanoveniami príslušných nástrojov na podporu politik Únie;
 - d) príspevky tretích krajín podieľajúcich sa na činnosti agentúry podľa článku 39;
 - e) prípadné peňažné či nepeňažné dobrovoľné príspevky členských štátov; členským štátom, ktoré poskytujú dobrovoľné príspevky, za ne nevzniká nárok na žiadne osobitné práva alebo služby.
2. Medzi výdavky agentúry patria výdavky na zamestnancov, administratívnu a technickú podporu, infraštruktúru a prevádzku a výdavky vyplývajúce zo zmlúv uzatvorených s tretími stranami.

Článok 28

Plnenie rozpočtu

1. Výkonný riaditeľ je zodpovedný za plnenie rozpočtu agentúry.
2. Vnútny audítor Komisie má rovnaké právomoci nad agentúrou ako nad oddeleniami Komisie.
3. Účtovník agentúry zasiela do 1. marca po každom rozpočtovom roku (1. marca roku N + 1) účtovníkovi Komisie a Dvoru audítorov predbežnú účtovnú závierku.
4. Po doručení pripomienok Dvora audítorov k predbežnej účtovnej závierke agentúry vypracuje účtovník agentúry na vlastnú zodpovednosť konečnú účtovnú závierku agentúry.
5. Výkonný riaditeľ predkladá konečnú účtovnú závierku na posúdenie správnej rade.
6. Výkonný riaditeľ zasiela do 31. marca roka N + 1 Európskemu parlamentu, Rade, Komisii a Dvoru audítorov správu o rozpočtovom a finančnom hospodárení.
7. Účtovník do 1. júla roka N + 1 zasiela konečnú účtovnú závierku Európskemu parlamentu, Rade, účtovníkovi Komisie a Dvoru audítorov spolu so stanoviskom správnej rady.
8. V deň zaslania konečnej účtovnej závierky účtovník zároveň zasiela Dvoru audítorov vyhlásenie k tejto konečnej účtovnej závierke a jeho kópiu zasiela účtovníkovi Komisie.
9. Výkonný riaditeľ uverejňuje konečnú účtovnú závierku do 15. novembra nasledujúceho roka.
10. Výkonný riaditeľ zasiela Dvoru audítorov do 30. septembra roka N + 1 odpoveď na jeho pripomienky, pričom kópiu tejto odpovede zasiela správnej rade a Komisii.
11. Výkonný riaditeľ predloží Európskemu parlamentu na jeho žiadosť všetky informácie potrebné na bezproblémové uplatnenie postupu udelenia absolútoría za daný rozpočtový rok, ako sa stanovuje v článku 165 ods. 3 nariadenia o rozpočtových pravidlách.
12. Európsky parlament konajúc na odporúčanie Rady do 15. mája roka N + 2 udelí výkonnému riaditeľovi absolútorium za plnenie rozpočtu za rok N.

Článok 29
Rozpočtové pravidlá

Rozpočtové pravidlá agentúry prijme správna rada po porade s Komisiou. Nesmú sa odchyľovať od nariadenia (EÚ) č. 1271/2013, pokiaľ takáto odchýlka nie je osobitne potrebná na prevádzku agentúry a Komisia s ňou vopred súhlasila.

Článok 30
Boj proti podvodom

1. V záujme uľahčenia boja proti podvodom, korupcii a ďalším nezákonným činnostiam podľa nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013³⁹ agentúra do šiestich mesiacov odo dňa začatia svojej činnosti pristúpi k medziinštitucionálnej dohode z 25. mája 1999, ktorá sa týka vnútorných vyšetrovaní Európskym úradom pre boj proti podvodom (OLAF), a prijme vhodné ustanovenia uplatniteľné na všetkých zamestnancov agentúry, pričom použije vzor uvedený v prílohe k uvedenej dohode.
2. Dvor audítorov je oprávnený vykonávať audit na základe dokumentov a na mieste u všetkých príjemcov grantov, dodávateľov a subdodávateľov, ktorým agentúra poskytla finančné prostriedky Únie.
3. OLAF môže vykonávať vyšetrovania vrátane kontrol a inšpekcií na mieste v súlade s ustanoveniami a postupmi stanovenými v nariadení Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013 a v nariadení Rady (Euratom, ES) č. 2185/96⁴⁰ z 11. novembra 1996 o kontrolách a inšpekciách na mieste vykonávaných Komisiou s cieľom ochrany finančných záujmov Únie pred spreneverou a inými podvodmi, aby zistil, či v súvislosti s grantom alebo zmluvou financovanými agentúrou nedošlo k podvodu, korupcii alebo akémukoľvek inému nezákonnému konaniu poškodzujúcemu finančné záujmy Únie.
4. Bez toho, aby boli dotknuté odseky 1, 2 a 3, dohody o spolupráci s tretími krajinami a s medzinárodnými organizáciami, zmluvy, dohody o grante a rozhodnutia agentúry o grante musia obsahovať ustanovenia, ktorými sa Dvoru audítorov a úradu OLAF výslovne udeľuje právomoc vykonávať takéto audity a vyšetrovania v súlade s ich príslušnými právomocami.

³⁹ [Nariadenie Európskeho parlamentu a Rady \(EÚ, Euratom\) No 883/2013 z 11. septembra 2013 o vyšetrovaniach vykonávaných Európskym úradom pre boj proti podvodom \(OLAF\), ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady \(ES\) č. 1073/1999 a nariadenie Rady \(Euratom\) č. 1074/1999](#) (Ú. v. EÚ L 248, 18.9.2013, s. 1).

⁴⁰ [Nariadenie Rady \(Euratom, ES\) č. 2185/96 z 11. novembra 1996 o kontrolách a inšpekciách na mieste vykonávaných Komisiou s cieľom ochrany finančných záujmov Európskych spoločenstiev pred spreneverou a inými podvodmi](#) (Ú. v. ES L 292, 15.11.1996, s. 2).

KAPITOLA IV PERSONÁL AGENTÚRY

Článok 31

Všeobecné ustanovenia

Na zamestnancov agentúry sa vzťahuje služobný poriadok a podmienky zamestnávania ostatných zamestnancov, ako aj pravidlá prijaté na základe dohody medzi inštitúciami Únie týkajúce sa vykonávania služobného poriadku.

Článok 32

Výsady a imunity

Na agentúru a jej zamestnancov sa vzťahuje Protokol č. 7 o výsadách a imunitách Európskej únie, ktorý je pripojený k Zmluve o Európskej únii a k ZFEÚ.

Článok 33

Výkonný riaditeľ

1. Výkonný riaditeľ pôsobí ako dočasný zástupca agentúry podľa článku 2 písm. a) podmienok zamestnávania ostatných zamestnancov.
2. Výkonného riaditeľa vymenúva správna rada zo zoznamu kandidátov navrhnutých Komisiou pri uplatnení otvoreného a transparentného výberového konania.
3. Na účely uzatvorenia zmluvy s výkonným riaditeľom zastupuje agentúru predseda správnej rady.
4. Kandidát, ktorého vybrala správna rada, sa pred vymenovaním vyjadrí pred príslušným výborom Európskeho parlamentu a odpovie na otázky jeho členov.
5. Funkčné obdobie výkonného riaditeľa je päť rokov. Na konci tohto obdobia Komisia vykoná posúdenie, v ktorom zohľadní hodnotenie výsledkov činnosti výkonného riaditeľa a budúce úlohy a výzvy agentúry.
6. Správna rada prijíma rozhodnutia o vymenovaní výkonného riaditeľa, predĺžení jeho funkčného obdobia alebo jeho odvolaní z funkcie na základe dvoj tretinovej väčšiny hlasov členov s hlasovacím právom.
7. Správna rada konajúc na návrh Komisie, v ktorom sa zohľadní posúdenie uvedené v odseku 5, môže predĺžiť funkčné obdobie výkonného riaditeľa raz, najviac o päť rokov.
8. Správna rada informuje Európsky parlament o svojom úmysle predĺžiť funkčné obdobie výkonného riaditeľa. Počas troch mesiacov pred takýmto predĺžením funkčného obdobia sa výkonný riaditeľ, ak k tomu bude vyzvaný, vyjadrí pred príslušným výborom Európskeho parlamentu a odpovie na otázky jeho členov.
9. Výkonný riaditeľ, ktorého funkčné obdobie sa predĺžilo, sa nemôže zúčastniť na ďalšom výberovom konaní na rovnakú funkciu.
10. Výkonný riaditeľ môže byť odvolaný z funkcie len na základe rozhodnutia správnej rady, ktorá koná na návrh Komisie.

Článok 34

Vyslaní národných expertov a ďalších pracovníkov

1. Agentúra môže využívať vyslaných národných expertov alebo ďalších pracovníkov, ktorých nezamestnáva. Služobný poriadok a podmienky zamestnávania ostatných zamestnancov sa na týchto pracovníkov nevzťahujú.
2. Správna rada prijme rozhodnutie, v ktorom stanoví pravidlá vysielania národných expertov do agentúry.

KAPITOLA V VŠEOBECNÉ USTANOVENIA

Článok 35

Právne postavenie agentúry

1. Agentúra je orgánom Únie a má právnu subjektivitu.
2. Agentúra má v každom členskom štáte najširšiu právnu spôsobilosť, akú jeho právo priznáva právnickým osobám. Môže najmä nadobúdať hnutel'ný a nehnuteľný majetok a nakladať s ním, ako aj byť účastníkom súdnych konaní.
3. Agentúru navonok zastupuje jej výkonný riaditeľ.

Článok 36

Zodpovednosť agentúry

1. Zmluvná zodpovednosť agentúry sa spravuje rozhodným právom pre danú zmluvu.
2. Súdny dvor Európskej únie má právomoc rozhodovať podľa akejkoľvek arbitrážnej doložky obsiahnutej v zmluve uzatvorenej agentúrou.
3. V prípade mimozmluvnej zodpovednosti agentúra nahradí v súlade so všeobecnými zásadami spoločnými pre práva členských štátov všetky škody, ktoré spôsobila agentúra alebo jej zamestnanci pri vykonávaní svojich povinností.
4. Vo všetkých sporoch súvisiacich s náhradou takejto škody má právomoc rozhodovať Súdny dvor Európskej únie.
5. Osobná zodpovednosť zamestnancov agentúry voči nej sa riadi príslušnými podmienkami uplatniteľnými na zamestnancov agentúry.

Článok 37

Pravidlá používania jazykov

1. Na agentúru sa vzťahuje nariadenie Rady č. 1⁴¹. Členské štáty a ostatné nimi menované orgány sa môžu obrátiť na agentúru a dostať odpoveď v úradnom jazyku inštitúcií Únie podľa ich výberu.

⁴¹ [Nariadenie č. 1, ktorým sa určujú jazyky používané Európskym spoločenstvom pre atómovú energiu](#) (Ú. v. ES L 17, 6.10.1958, s. 401).

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

Článok 38

Ochrana osobných údajov

1. Spracovávanie osobných údajov agentúrou podlieha nariadeniu Európskeho parlamentu a Rady (ES) č. 45/2001⁴².
2. Správna rada prijme vykonávacie opatrenia uvedené v článku 24 ods. 8 nariadenia (ES) č. 45/2001. Správna rada môže prijať dodatočné opatrenia potrebné na uplatňovanie uvedeného nariadenia agentúrou.

Článok 39

Spolupráca s tretími krajinami a medzinárodnými organizáciami

1. V rozsahu potrebnom na dosiahnutie cieľov stanovených v tomto nariadení môže agentúra spolupracovať s príslušnými orgánmi tretích krajín a/alebo s medzinárodnými organizáciami. Na tento účel môže agentúra s výhradou predchádzajúceho schválenia Komisiou dohodnúť modalitty spolupráce s uvedenými orgánmi tretích krajín a medzinárodnými organizáciami. Týmito modalitami nevznikajú Únii ani jej členským štátom žiadne právne záväzky.
2. Agentúra je otvorená účasti tretích krajín, ktoré na tento účel uzavreli dohody s Úniou. Podľa príslušných ustanovení týchto dohôd sa prijímajú opatrenia určujúce predovšetkým povahu, rozsah a spôsob, akým sa tieto krajiny budú podieľať na práci agentúry, vrátane ustanovení týkajúcich sa účasti na iniciatívach uskutočňovaných agentúrou, finančných príspevkov a personálnych otázok. Pokiaľ ide o personálne otázky, musia byť tieto opatrenia za každých okolností v súlade so služobným poriadkom.
3. Správna rada prijme stratégiu pre vzťahy s tretími krajinami alebo medzinárodnými organizáciami v otázkach spadajúcich do právomoci agentúry. Komisia sa uistí, že agentúra vykonáva svoje činnosti v súlade s mandátom a platným inštitucionálnym rámcom, a to uzavretím primeraných pracovných dojednaní s výkonným riaditeľom agentúry.

Článok 40

Bezpečnostné predpisy v oblasti ochrany utajovaných skutočností a citlivých neutajovaných skutočností

Agentúra v konzultácii s Komisiou prijme vlastné bezpečnostné predpisy, v ktorých uplatní bezpečnostné zásady obsiahnuté v bezpečnostných predpisoch Komisie na ochranu utajovaných skutočností Európskej únie (EUCI) a citlivých neutajovaných skutočností podľa rozhodnutí Komisie (EÚ, Euratom) 2015/443, resp. 2015/444. Okrem iného ide o ustanovenia týkajúce sa výmeny, spracovania a uchovávaní takýchto skutočností.

⁴²

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).

Článok 41

Dohoda o sídle a prevádzkové podmienky

1. Potrebné ustanovenia o poskytnutí sídla agentúre v hostiteľskom členskom štáte a o zariadeniach, ktoré má tento členský štát sprístupniť, ako aj osobitné pravidlá, ktoré sa v hostiteľskom členskom štáte vzťahujú na výkonného riaditeľa, členov správnej rady, zamestnancov agentúry a členov ich rodín, sa vymedzia v dohode o sídle uzatvorenej medzi agentúrou a členským štátom, v ktorom sa nachádza sídlo, po schválení správnu radou najneskôr [dva roky po nadobudnutí účinnosti tohto nariadenia].
2. Hostiteľský členský štát agentúry poskytne najlepšie možné podmienky s cieľom zabezpečiť jej riadne fungovanie vrátane dostupnosti miesta, zabezpečenia adekvátnych vzdelávacích zariadení pre deti zamestnancov, vhodného prístupu na trh práce, k sociálnemu zabezpečeniu a zdravotnej starostlivosti pre deti a manželov (manželky).

Článok 42

Administratívna kontrola

Nad činnosťou agentúry dohliada v súlade s článkom 228 ZFEÚ ombudsman.

HLAVA III

RÁMEC CERTIFIKÁCIE KYBERNETICKEJ BEZPEČNOSTI

Článok 43

Európske systémy certifikácie kybernetickej bezpečnosti

Európsky systém certifikácie kybernetickej bezpečnosti potvrdzuje, že príslušné produkty a služby IKT, ktoré boli certifikované v súlade s takýmto systémom, spĺňajú konkrétne požiadavky z hľadiska schopnosti odolať na určitom stupni dôveryhodnosti konaniu, ktorého cieľom je ohroziť dostupnosť, pravosť, integritu alebo dôvernosť uložených, prenášaných alebo spracúvaných údajov alebo funkcií či služieb, ktoré sa cez tieto produkty, procesy, služby a systémy ponúkajú alebo sprístupňujú.

Článok 44

Vypracovanie a prijatie európskeho systému certifikácie kybernetickej bezpečnosti

1. Agentúra ENISA na žiadosť Komisie vypracuje kandidátsky európsky systém certifikácie kybernetickej bezpečnosti, ktorý spĺňa požiadavky stanovené v článkoch 45, 46 a 47 tohto nariadenia. Členské štáty alebo európska skupina pre certifikáciu kybernetickej bezpečnosti (ďalej len „skupina“) zriadená podľa článku 53 môžu Komisii navrhnúť vypracovanie kandidátskeho európskeho systému certifikácie kybernetickej bezpečnosti.
2. Pri vypracúvaní kandidátskeho systému podľa odseku 1 tohto článku vedie agentúra ENISA konzultácie so všetkými relevantnými zainteresovanými stranami a úzko spolupracuje so skupinou. Skupina poskytuje agentúre ENISA pomoc a odborné poradenstvo, ktoré si agentúra vyžiada v súvislosti s vypracovaním kandidátskeho systému, podľa potreby vrátane stanovísk.
3. Agentúra ENISA postúpi kandidátsky európsky systém certifikácie kybernetickej bezpečnosti vypracovaný v súlade s odsekom 2 tohto článku Komisii.
4. Komisia môže na základe kandidátskeho systému navrhnutého agentúrou ENISA prijať vykonávacie akty v súlade s článkom 55 ods. 1, v ktorých sa stanovia európske systémy certifikácie kybernetickej bezpečnosti produktov a služieb IKT, ktoré spĺňajú požiadavky článkov 45, 46 a 47 tohto nariadenia.
5. Agentúra ENISA spravuje vyhradené webové stránky, na ktorých sa uvádzajú informácie o európskych systémoch certifikácie kybernetickej bezpečnosti a zabezpečuje ich publicitu.

Článok 45

Bezpečnostné ciele európskych systémov certifikácie kybernetickej bezpečnosti

Európsky systém certifikácie kybernetickej bezpečnosti musí byť navrhnutý tak, aby podľa potreby zohľadňoval tieto bezpečnostné ciele:

- a) chrániť uložené, prenášané alebo inak spracúvané údaje pred neúmyselným či neoprávneným ukladaním, spracovaním, prístupom alebo únikom;

- b) chrániť uložené, prenášané alebo inak spracúvané údaje pred neúmyselným či neoprávneným zničením, náhodnou stratou či pozmenením;
- c) zabezpečiť, aby mali oprávnené osoby, programy alebo zariadenia prístup výlučne k tým údajom, službám alebo funkciám, na ktoré sa vzťahujú ich prístupové práva;
- d) zaznamenávať, ktoré údaje, funkcie alebo služby sa poskytli, kedy a kto ich poskytol;
- e) zabezpečiť možnosť overiť, kto a kedy ku ktorým údajom, službám alebo funkciám pristupoval alebo ich použil;
- f) v prípade fyzického alebo technického incidentu promptne obnoviť dostupnosť údajov, služieb a funkcií a prístup k nim;
- g) zabezpečiť, že k produktom a službám IKT sa poskytuje aktualizovaný softvér bez známych zraniteľných miest, ako aj mechanizmy bezpečnej aktualizácie softvéru.

Článok 46

Stupne dôveryhodnosti európskych systémov certifikácie kybernetickej bezpečnosti

1. Európsky systém certifikácie kybernetickej bezpečnosti môže pre produkty a služby IKT certifikované v rámci daného systému uvádzať jeden alebo viacero z týchto stupňov dôveryhodnosti: základný, pokročilý a/vysoký.
2. Základný, pokročilý a vysoký stupeň dôveryhodnosti musia spĺňať tieto kritériá:
 - a) základný stupeň dôveryhodnosti označuje certifikát vydaný v kontexte európskeho systému certifikácie kybernetickej bezpečnosti, ktorý poskytuje obmedzený stupeň dôvery v uvádzané alebo údajné kyberneticko-bezpečnostné vlastnosti produktu alebo služby IKT, a charakterizuje sa s odvolaním na technické špecifikácie, normy a súvisiace postupy vrátane technických kontrol, ktorých účelom je znížiť riziko kybernetických incidentov;
 - b) pokročilý stupeň dôveryhodnosti označuje certifikát vydaný v kontexte európskeho systému certifikácie kybernetickej bezpečnosti, ktorý poskytuje výrazný stupeň dôvery v uvádzané alebo údajné kyberneticko-bezpečnostné vlastnosti produktu alebo služby IKT, a charakterizuje sa s odvolaním na technické špecifikácie, normy a súvisiace postupy vrátane technických kontrol, ktorých účelom je výrazne znížiť riziko kybernetických incidentov;
 - c) vysoký stupeň dôveryhodnosti označuje certifikát vydaný v kontexte európskeho systému certifikácie kybernetickej bezpečnosti, ktorý poskytuje vyšší stupeň dôvery v uvádzané alebo údajné kyberneticko-bezpečnostné vlastnosti produktu alebo služby IKT než certifikáty s pokročilým stupňom dôveryhodnosti, a charakterizuje sa s odvolaním na technické špecifikácie, normy a súvisiace postupy vrátane technických kontrol, ktorých účelom je predchádzať riziku kybernetických incidentov.

Článok 47

Prvky európskych systémov certifikácie kybernetickej bezpečnosti

1. Európsky systém certifikácie kybernetickej bezpečnosti musí zahŕňať tieto prvky:

- a) predmet úpravy a rozsah pôsobnosti danej certifikácie vrátane typu alebo kategórií pokrytých produktov a služieb IKT;
 - b) podrobnú špecifikáciu kyberneticko-bezpečnostných požiadaviek, z hľadiska ktorých sa konkrétne produkty a služby IKT hodnotia – napríklad s odkazom na európske alebo medzinárodné normy alebo technické špecifikácie;
 - c) podľa potreby jeden alebo viacero stupňov dôveryhodnosti;
 - d) konkrétne použité hodnotiace kritériá a metódy vrátane typov hodnotenia s cieľom preukázať, že sa dosiahli konkrétne ciele uvedené v článku 45;
 - e) informácie, ktoré má orgánom posudzovania zhody poskytnúť žiadateľ a ktoré sú potrebné na certifikáciu;
 - f) ak systém zahŕňa označenia alebo značky, podmienky, za ktorých možno takéto označenia alebo značky použiť;
 - g) ak systém zahŕňa dohľad, pravidlá monitorovania súladu s požiadavkami príslušného certifikátu vrátane mechanizmov na preukázanie trvalého súladu so stanovenými kyberneticko-bezpečnostnými požiadavkami;
 - h) podmienky udelenia, udržiavania, pokračovania, rozširovania a zužovania rozsahu certifikácie;
 - i) pravidlá týkajúce sa dôsledkov v prípade nesúladu certifikovaných produktov a služieb IKT s certifikačnými požiadavkami;
 - j) pravidlá nahlásovania a riešenia predtým nezistených zraniteľných miest produktov a služieb IKT z hľadiska kybernetickej bezpečnosti;
 - k) pravidlá uchovávanía záznamov orgánmi posudzovania zhody;
 - l) určenie vnútroštátnych systémov certifikácie kybernetickej bezpečnosti, ktoré sa vzťahujú na rovnaký typ alebo kategóriu produktov a služieb IKT;
 - m) obsah vydaného certifikátu.
2. Stanovené požiadavky daného systému nesmú byť v rozpore so žiadnymi platnými zákonnými požiadavkami, najmä s požiadavkami, ktoré vyplývajú z harmonizovanej legislatívy Únie.
 3. Ak sa to stanovuje v osobitnom akte Únie, certifikáciu v rámci európskeho systému certifikácie kybernetickej bezpečnosti možno použiť na preukázanie predpokladu zhody s požiadavkami daného aktu.
 4. Ak harmonizovaná legislatíva Únie absentuje, vo vnútroštátnom práve členských štátov sa zároveň môže stanoviť, že európsky systém certifikácie kybernetickej bezpečnosti možno použiť na určenie predpokladu zhody so zákonnými požiadavkami.

Článok 48

Certifikácia kybernetickej bezpečnosti

1. Produkty a služby IKT certifikované v rámci európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa článku 44 sa považujú za vyhovujúce požiadavkám daného systému.
2. Pokiaľ sa v právnych predpisoch Únie nestanovuje inak, certifikácia je dobrovoľná.

3. Európsky certifikát kybernetickej bezpečnosti podľa tohto článku vydávajú orgány posudzovania zhody uvedené v článku 51 na základe kritérií zahrnutých v európskom systéme certifikácie kybernetickej bezpečnosti prijatom podľa článku 44.
4. Odchyľne od odseku 3 sa v riadne odôvodnených prípadoch môže v konkrétnom európskom systéme certifikácie kybernetickej bezpečnosti určiť, že výsledný európsky certifikát kybernetickej bezpečnosti môže vydať len verejný orgán. Ide o jeden z týchto verejných orgánov:
 - a) vnútroštátny orgán dohľadu nad certifikáciou uvedený v článku 50 ods. 1;
 - b) orgán akreditovaný ako orgán posudzovania zhody podľa článku 51 ods. 1 alebo
 - c) orgán zriadený zákonmi, právnymi predpismi alebo inými úradnými administratívnymi postupmi dotknutého členského štátu, ktoré spĺňajú požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb podľa normy ISO/IEC 17065:2012.
5. Fyzická či právnická osoba, ktorá podrobuje svoje produkty alebo služby IKT mechanizmu certifikácie, musí orgánu posudzovania zhody uvedenému v článku 51 poskytnúť všetky informácie potrebné pre postup certifikácie.
6. Certifikáty sa vydávajú najviac na tri roky, pričom ich možno obnoviť za rovnakých podmienok, pokiaľ sú naďalej splnené relevantné požiadavky.
7. Európsky certifikát kybernetickej bezpečnosti vydaný podľa tohto článku sa uznáva vo všetkých členských štátoch.

Článok 49

Vnútroštátne systémy certifikácie a certifikáty kybernetickej bezpečnosti

1. Bez toho, aby bol dotknutý odsek 3, strácajú vnútroštátne systémy certifikácie kybernetickej bezpečnosti a súvisiace postupy pre produkty a služby IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, účinok k dátumu stanovenému vo vykonávacom akte prijatom podľa článku 44 ods. 4. Existujúce vnútroštátne systémy certifikácie kybernetickej bezpečnosti a súvisiace postupy pre produkty a služby IKT, na ktoré sa žiaden európsky systém certifikácie kybernetickej bezpečnosti nevzťahuje, existujú naďalej.
2. Členské štáty nesmú zavádzať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti tých produktov a služieb IKT, na ktoré sa vzťahuje platný európsky systém certifikácie kybernetickej bezpečnosti.
3. Existujúce certifikáty vydané na základe vnútroštátnych systémov certifikácie kybernetickej bezpečnosti platia naďalej až do uplynutia ich platnosti.

Článok 50

Vnútroštátne orgány dohľadu nad certifikáciou

1. Každý členský štát určí vnútroštátny orgán dohľadu nad certifikáciou.
2. Každý členský štát oznámi Komisii, ktorý orgán určil.

3. Každý vnútroštátny orgán dohľadu nad certifikáciou musí byť z hľadiska organizácie, rozhodnutí o financovaní, právnej štruktúry a rozhodovania nezávislý od orgánov, nad ktorými dohliada.
4. Členské štáty zabezpečia, aby vnútroštátne orgány dohľadu nad certifikáciou mali primerané zdroje na výkon svojich právomocí a aby zverené úlohy vykonávali účinne a efektívne.
5. V záujme účinného vykonávania tohto nariadenia je vhodné, aby sa tieto orgány aktívne, efektívne, účinne a bezpečne zapájali do práce európskej skupiny pre certifikáciu kybernetickej bezpečnosti zriadenej podľa článku 53.
6. Vnútroštátne orgány dohľadu nad certifikáciou:
 - a) monitorujú a presadzujú uplatňovanie ustanovení tejto hlavy na vnútroštátnej úrovni a dohliadajú nad súladom certifikátov, ktoré vydali orgány posudzovania zhody zriadené na území daného členského štátu, s požiadavkami tejto hlavy, ako aj s požiadavkami príslušného európskeho systému certifikácie kybernetickej bezpečnosti;
 - b) monitorujú a dohliadajú nad činnosťami orgánov posudzovania zhody na účely tohto nariadenia, a to aj v súvislosti s oznamovaním orgánov posudzovania zhody a súvisiacich úloh v zmysle článku 52 tohto nariadenia;
 - c) vybavujú sťažnosti fyzických alebo právnických osôb v súvislosti s certifikátmi, ktoré vydali orgány posudzovania zhody so sídlom na ich území, primerane prešetrujú predmet danej sťažnosti a sťažovateľa v primeranej lehote informujú o pokroku a výsledku tohto prešetrovania;
 - d) spolupracujú s ostatnými vnútroštátnymi orgánmi dohľadu nad certifikáciou alebo ďalšími verejnými orgánmi vrátane poskytovania informácií o možnom nesúlade produktov a služieb IKT s požiadavkami tohto nariadenia alebo konkrétnych európskych systémov certifikácie kybernetickej bezpečnosti;
 - e) monitorujú relevantné trendy vo sfére certifikácie kybernetickej bezpečnosti.
7. Každý vnútroštátny orgán dohľadu nad certifikáciou musí mať aspoň tieto právomoci:
 - a) žiadať od orgánov posudzovania zhody a držiteľov európskych certifikátov kybernetickej bezpečnosti akékoľvek informácie, ktoré potrebuje na plnenie svojich úloh;
 - b) viesť vyšetrovanie v podobe auditov orgánov posudzovania zhody a držiteľov európskych certifikátov kybernetickej bezpečnosti na overenie súladu s ustanoveniami hlavy III;
 - c) prijímať primerané opatrenia v súlade s vnútroštátnym právom na zaistenie súladu orgánov posudzovania zhody alebo držiteľov certifikátov s týmto nariadením alebo európskym systémom certifikácie kybernetickej bezpečnosti;
 - d) získať prístup do akýchkoľvek priestorov orgánov posudzovania zhody a držiteľov európskych certifikátov kybernetickej bezpečnosti na účely vyšetrovania v súlade s procesným právom Únie alebo daného členského štátu;
 - e) v súlade s vnútroštátnym právom odnímať certifikáty, ktoré nie sú v súlade s týmto nariadením alebo s európskym systémom certifikácie kybernetickej bezpečnosti;

- f) ukladať sankcie v zmysle článku 54 v súlade s vnútroštátnym právom a vyžadovať okamžité ukončenie porušovania povinností stanovených v tomto nariadení.
8. Vnútroštátne orgány dohľadu nad certifikáciou navzájom i s Komisiou spolupracujú, a najmä si vymieňajú informácie, skúsenosti a osvedčené postupy v oblasti certifikácie kybernetickej bezpečnosti a technických otázok súvisiacich s kybernetickou bezpečnosťou produktov a služieb IKT.

Článok 51

Orgány posudzovania zhody

1. Orgány posudzovania zhody akredituje vnútroštátny akreditačný orgán vymenovaný podľa nariadenia (ES) č. 765/2008, iba ak spĺňajú požiadavky stanovené v prílohe k tomuto nariadeniu.
2. Akreditácia sa udeľuje najviac na päť rokov a možno ju obnoviť za rovnakých podmienok, pokiaľ orgán posudzovania zhody spĺňa požiadavky stanovené v tomto článku. Akreditačné orgány odoberú orgánu posudzovania zhody akreditáciu v zmysle odseku 1 tohto článku, ak nie sú alebo prestanú byť splnené akreditačné podmienky, alebo ak daný orgán svojím konaním porušuje toto nariadenie.

Článok 52

Oznamovanie

1. Pri každom európskom systéme certifikácie kybernetickej bezpečnosti prijatom podľa článku 44 vnútroštátne orgány dohľadu nad certifikáciou oznámia Komisii orgány posudzovania zhody, ktoré sú akreditované na vydávanie certifikátov pri určených stupňoch dôveryhodnosti v zmysle článku 46, a bezodkladne aj akékoľvek následné zmeny v tomto smere.
2. Rok po nadobudnutí účinnosti každého európskeho systému certifikácie kybernetickej bezpečnosti Komisia v úradnom vestníku uverejní zoznam oznámených orgánov posudzovania zhody.
3. Ak Komisia dostane oznámenie po lehote stanovenej v odseku 2, v *Úradnom vestníku Európskej únie* uverejní zmeny zoznamu uvedeného v odseku 2 do dvoch mesiacov od prijatia daného oznámenia.
4. Vnútroštátny orgán dohľadu nad certifikáciou môže Komisii predložiť žiadosť o vyňatie niektorého orgánu posudzovania zhody, ktorý daný vnútroštátny orgán dohľadu nad certifikáciou oznámil, zo zoznamu uvedeného v odseku 2 tohto článku. Komisia v *Úradnom vestníku Európskej únie* uverejní príslušné zmeny zoznamu do jedného mesiaca od prijatia predmetnej žiadosti vnútroštátneho orgánu dohľadu nad certifikáciou.
5. Komisia môže vo vykonávacích aktoch vymedziť okolnosti, formáty a postupy oznamovania uvedeného v odseku 1 tohto článku. Dané vykonávacie akty sa prijímú v súlade s postupom preskúmania uvedeným v článku 55 ods. 2.

Článok 53

Európska skupina pre certifikáciu kybernetickej bezpečnosti

1. Zriadi sa európska skupina pre certifikáciu kybernetickej bezpečnosti (ďalej len „skupina“).
2. Skupina pozostáva z vnútroštátnych orgánov dohľadu nad certifikáciou. Tieto orgány zastupujú riaditelia alebo iní čelní predstavitelia vnútroštátnych orgánov dohľadu nad certifikáciou.
3. Skupina má tieto úlohy:
 - a) radiť a pomáhať Komisii v jej úsilí o zabezpečenie konzistentného vykonávania a uplatňovania tejto hlavy, najmä z hľadiska politických otázok spojených s certifikáciou kybernetickej bezpečnosti, koordinácie politických prístupov a vypracovania európskych systémov certifikácie kybernetickej bezpečnosti;
 - b) radiť a pomáhať agentúre ENISA a spolupracovať s ňou pri vypracúvaní kandidátskych systémov v súlade s článkom 44 tohto nariadenia;
 - c) navrhovať Komisii, aby agentúru požiadala o vypracovanie kandidátskeho európskeho systému certifikácie kybernetickej bezpečnosti v súlade s článkom 44 tohto nariadenia;
 - d) prijímať stanoviská pre Komisiu k udržiavaniu a prehodnocovaniu existujúcich európskych systémov certifikácie kybernetickej bezpečnosti;
 - e) skúmať relevantné trendy vo sfére certifikácie kybernetickej bezpečnosti a vymieňať si osvedčené postupy v oblasti systémov certifikácie kybernetickej bezpečnosti;
 - f) uľahčovať spoluprácu medzi vnútroštátnymi orgánmi dohľadu nad certifikáciou podľa tejto hlavy výmenou informácií, najmä vytvorením metód efektívnej výmeny informácií o všetkých otázkach spojených s certifikáciou kybernetickej bezpečnosti.
4. Skupine predsedá a jej sekretariát zabezpečuje Komisia za pomoci agentúry ENISA v zmysle článku 8 písm. a).

Článok 54

Sankcie

Členské štáty stanovujú pravidlá sankcionovania porušení ustanovení tejto hlavy a európskych systémov certifikácie kybernetickej bezpečnosti a prijímajú všetky potrebné opatrenia na zaistenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty [do .../bezodkladne] oznámia uvedené pravidlá a opatrenia Komisii a informujú ju o všetkých následných zmenách, ktoré na ne majú vplyv.

HLAVA IV

ZÁVEREČNÉ USTANOVENIA

Článok 55

Postup výboru

1. Komisii pomáha výbor. Tento výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.
2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 4 nariadenia (EÚ) č. 182/2011.

Článok 56

Hodnotenie a preskúmanie

1. Najneskôr do piatich rokov od dátumu uvedeného v článku 58 a následne každých päť rokov Komisia posúdi dosah, účinnosť a efektívnosť agentúry a jej pracovných postupov, ako aj prípadnú potrebu upraviť mandát agentúry a finančné dôsledky takýchto prípadných úprav. Pri tomto hodnotení sa zohľadní každá prípadná spätná väzba, ktorú agentúra dostala v nadväznosti na svoje činnosti. Ak sa Komisia domnieva, že existencia agentúry už nie je vzhľadom na jej stanovené ciele, mandát a úlohy odôvodnená, môže navrhnúť zmenu tohto nariadenia z hľadiska ustanovení, ktoré sa týkajú agentúry.
2. V hodnotení sa zároveň posúdi vplyv, účinnosť a efektívnosť ustanovení hlavy III z hľadiska cieľov zaistiť primeranú kybernetickú bezpečnosť produktov a služieb IKT v Únii a zlepšiť fungovanie vnútorného trhu.
3. Komisia predloží hodnotiacu správu spolu s jej závermi Európskemu parlamentu, Rade a správnej rade. Zistenia z hodnotiacej správy sa zverejnia.

Článok 57

Zrušenie a nástupníctvo

1. Nariadenie (ES) č. 526/2013 sa zrušuje s účinnosťou od [...].
2. Odkazy na nariadenie (ES) č. 526/2013 a na agentúru ENISA sa považujú za odkazy na toto nariadenie a na agentúru.
3. Agentúra je nástupcom agentúry, ktorá bola zriadená nariadením (ES) č. 526/2013, pokiaľ ide o vlastníctvo, dohody, právne záväzky, pracovné zmluvy, finančné záväzky a zodpovednosť. Všetky existujúce rozhodnutia správnej rady a výkonnej rady zostávajú v platnosti, pokiaľ nie sú v rozpore s ustanoveniami tohto nariadenia.
4. Agentúra sa zriaďuje na neurčité obdobie od [...].
5. Výkonný riaditeľ menovaný podľa článku 24 ods. 4 nariadenia (ES) č. 526/2013 zostáva výkonným riaditeľom agentúry až do konca svojho funkčného obdobia.

6. Členovia správnej rady a ich náhradníci menovaní podľa článku 6 nariadenia (ES) č. 526/2013 zostávajú členmi správnej rady agentúry a náhradníkmi až do konca svojho funkčného obdobia.

Článok 58

1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.
2. Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

*Za Európsky parlament
predseda*

*Za Radu
predseda*

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Návrh nariadenia Európskeho parlamentu a Rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii bezpečnosti informačných a komunikačných technológií („akt/nariadenie o kybernetickej bezpečnosti“)

1.2. Príslušné oblasti politiky

Oblasť politiky: 09 – Komunikačné siete, obsah a technológie
Činnosť: 09.02 Digitálny jednotný trh

1.3. Druh návrhu/iniciatívy

☒ Návrh/iniciatíva sa týka **novej akcie (Hlava III – Certifikácia)**

☐ Návrh/iniciatíva sa týka **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu**⁴³

☒ Návrh/iniciatíva sa týka **predĺženia trvania existujúcej akcie (Hlava II – Mandát agentúry ENISA)**

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

1.4. Ciele

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

1. Zvýšiť odolnosť členských štátov, podnikov a EÚ ako celku
2. Zabezpečiť riadne fungovanie vnútorného trhu EÚ s produktmi a službami IKT
3. Zvýšiť svetovú konkurencieschopnosť spoločností EÚ pôsobiacich v oblasti IKT
4. Aproximovať zákony, iné právne predpisy a správne opatrenia členských štátov, ktoré si vyžadujú kybernetickú bezpečnosť.

1.4.2. Osobitné ciele

S prihliadnutím na všeobecné ciele v širšom kontexte revidovanej stratégie kybernetickej bezpečnosti má tento nástroj vymedzením rozsahu pôsobnosti a mandátu agentúry ENISA a vytvorením európskeho certifikačného rámca pre produkty a služby IKT dosiahnuť tieto konkrétne ciele:

1. Posilniť **spôsobilosti a pripravenosť** členských štátov a podnikov
2. Zlepšiť **spoluprácu a koordináciu** naprieč členskými štátmi a inštitúciami, agentúrami a orgánmi EÚ
3. Posilniť **spôsobilosti na úrovni EÚ na doplnenie činností členských štátov**, a to najmä v prípade cezhraničných kybernetických kríz
4. Zvýšiť **informovanosť** občanov a podnikov o otázkach kybernetickej bezpečnosti
5. Posilniť dôveru v digitálny jednotný trh a digitálne inovácie zvýšením celkovej **transparentnosti uistenia o dôveryhodnosti kybernetickej bezpečnosti**⁴⁴ produktov a služieb IKT

⁴³

Podľa článku 54 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

ENISA sa bude podieľať na dosiahnutí uvedených cieľov takto:

Posilnená podpora pri tvorbe politiky – poskytovať usmernenia a odporúčania Komisii a členským štátom pri aktualizácii a vypracúvaní holistického normatívneho rámca v oblasti kybernetickej bezpečnosti, ako aj odvetvových politických a právnych iniciatív, ktorých súčasťou sú otázky kybernetickej bezpečnosti; prispievať k práci skupiny pre spoluprácu v zmysle článku 11 smernice (EÚ) 2016/1148, a to poskytovaním odborných poznatkov a pomoci; podporovať tvorbu a vykonávanie politiky v oblasti elektronickej identifikácie a dôveryhodných služieb; podporovať výmenu osvedčených postupov medzi príslušnými orgánmi;

Posilnená podpora pri budovaní kapacít – poskytovať podporu členským štátom, inštitúciám, orgánom, úradom a agentúram Únie pri rozvoji a zlepšovaní prevencie, odhaľovania, analýzy kyberneticko-bezpečnostných problémov a incidentov, ako aj schopnosti reagovať na ne; pomáhať členským štátom na ich žiadosť pri rozvoji vnútroštátnych jednotiek CSIRT a vypracovaní vnútroštátnych stratégií kybernetickej bezpečnosti; pomáhať inštitúciám Únie pri tvorbe a revízii stratégie kybernetickej bezpečnosti Únie; poskytovať odbornú prípravu v oblasti kybernetickej bezpečnosti; pomáhať členským štátom pri výmene osvedčených postupov prostredníctvom skupiny pre spoluprácu; uľahčovať zriaďovanie odvetvových stredísk pre výmenu a analýzu informácií (ISAC).

Operačná spolupráca a podpora krízového riadenia – podporovať spoluprácu medzi príslušnými verejnými orgánmi a medzi zainteresovanými stranami vytvorením systematickej spolupráce s inštitúciami, orgánmi, úradmi a agentúrami Únie, ktoré sa zaoberajú kybernetickou bezpečnosťou, počítačovou kriminalitou a ochranou súkromia a osobných údajov; zabezpečovať sekretariát siete jednotiek CSIRT [článok 12 ods. 2 smernice (EÚ) 2016/1148], ako aj prispievať k operačnej spolupráci v rámci siete poskytnutím podpory členským štátom, ktoré o ňu požiadajú, v spolupráci s tímom CERT-EU; organizovať pravidelné cvičenia v oblasti kybernetickej bezpečnosti; prispievať k rozvoju spolupráce v rámci reakcie na cezhraničné kybernetické incidenty a krízy veľkého rozsahu; v spolupráci so sieťou tímov CSIRT viesť *ex post* technické skúmanie závažných incidentov a vydávať odporúčania na nadväzné činnosti;

Úlohy súvisiace s trhom (normalizácia, certifikácia) – vykonávať viaceré osobitné funkcie na podporu vnútorného trhu: „monitor trhu“ kybernetickej bezpečnosti prostredníctvom analýzy relevantných trendov na trhu kybernetickej bezpečnosti na účely lepšieho zosúladenia ponuky a dopytu; podporovať a presadzovať rozvoj a vykonávanie politiky Únie v oblasti certifikácie kybernetickej bezpečnosti produktov a služieb IKT vypracovaním kandidátskych európskych systémov certifikácie kybernetickej bezpečnosti produktov a služieb IKT, zabezpečením služieb sekretariátu skupiny pre certifikáciu kybernetickej bezpečnosti Únie, poskytovaním usmernení a osvedčených postupov týkajúcich sa bezpečnostných požiadaviek na produkty a služby IKT v spolupráci s vnútroštátnymi orgánmi dohľadu nad certifikáciou a odvetvím; **Zlepšené znalosti, informovanie a podpora zvyšovania povedomia** – poskytovať pomoc a odporúčania Komisii a členským štátom, aby dosiahli vysokú úroveň znalostí v rámci celej Únie o otázkach súvisiacich so sieťovou a informačnou bezpečnosťou a s jej uplatňovaním na zainteresované strany z odvetvia. Predpokladom toho je aj združovanie, organizovanie a uverejňovanie informácií o bezpečnosti sieťových a informačných systémov [alebo kybernetickej bezpečnosti], a to na osobitnom portáli. Ďalším dôležitým prvkom sú

činnosti zamerané na zvyšovanie povedomia a informačné kampane pre širokú verejnosť zamerané na riziká súvisiace s kybernetickou bezpečnosťou.

Intenzívnejšia podpora výskumu a inovácií – poskytovať poradenstvo týkajúce sa potrieb výskumu a stanovenia priorít v oblasti kybernetickej bezpečnosti;

Podpora medzinárodnej spolupráce – podporovať úsilie Únie o spoluprácu s tretími krajinami a medzinárodnými organizáciami s cieľom presadzovať medzinárodnú spoluprácu v oblasti kybernetickej bezpečnosti.

CERTIFIKÁCIA

Certifikačný rámec prispeje k dosiahnutiu týchto cieľov zvýšením celkovej transparentnosti uistenia o dôveryhodnosti kybernetickej bezpečnosti⁴⁵ produktov a služieb IKT, čím sa posilní dôvera v digitálny jednotný trh a v digitálnu inováciu. To by malo tiež pomôcť zabrániť roztrieštenosti systémov certifikácie v EÚ a súvisiacich bezpečnostných požiadaviek a hodnotiacich kritérií v jednotlivých členských štátoch a odvetviach;

1.4.3. *Očakávané výsledky a vplyv*

Uved'te, aký vplyv by mal mať návrh/iniciatíva na príjemcov/cieľové skupiny.

Očakáva sa, že posilnená agentúra ENISA (podporujúca spôsobilosti, prevenciu, spoluprácu a povedomie na úrovni EÚ, a teda určená na zvýšenie celkovej kybernetickej odolnosti v EÚ), ako aj podpora úijného rámca certifikácie produktov a služieb IKT bude mať tento vplyv (neúplný zoznam):

Celkový vplyv:

– celkový pozitívny vplyv na vnútorný trh vďaka menšej roztrieštenosti trhu a budovaniu dôvery v digitálne technológie prostredníctvom lepšej spolupráce, harmonizovanejších prístupov k politike kybernetickej bezpečnosti EÚ a posilneným spôsobilostiam na úrovni EÚ. Výsledkom toho by mal byť pozitívny hospodársky vplyv, keďže pomôže znížiť náklady na kybernetickú bezpečnosť/incidenty, ktorých odhadovaný hospodársky vplyv v Únii dosahuje 0,41 % HDP EÚ (približne 55 miliárd EUR).

Konkrétne výsledky:

Lepšie kyberneticko-bezpečnostné spôsobilosti a pripravenosť členských štátov a podnikov

– lepšie kyberneticko-bezpečnostné spôsobilosti a pripravenosť členských štátov (vďaka dlhodobej strategickej analýze kybernetických hrozieb a incidentov, usmerneniam a správam, sprostredkovaniu poznatkov a osvedčených postupov, dostupnosti odbornej prípravy a vzdelávacích materiálov, posilnených cvičení CyberEurope)

– lepšie spôsobilosti súkromných subjektov vďaka podpore zriadeniu stredísk pre výmenu a analýzu informácií (ISAC) v rôznych odvetviach.

– lepšia kyberneticko-bezpečnostná pripravenosť EÚ a členských štátov vďaka dostupnosti riadne odskúšaných a odsúhlasených plánov v prípade cezhraničného kybernetického incidentu veľkého rozsahu testovaných v rámci cvičení CyberEurope;

⁴⁵

Transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti spočíva v poskytovaní dostatočných informácií používateľom o kyberneticko-bezpečnostných prvkoch, ktoré im umožnia objektívne určiť úroveň bezpečnosti daného produktu, služby alebo procesu IKT.

Lepšia spolupráca a koordinácia naprieč členskými štátmi a inštitúciami, agentúrami a orgánmi EÚ

- lepšia spolupráca v rámci verejného a súkromného sektora, ako aj medzi nimi;
- konzistentnejší prístup k cezhraničnému a medziodvetvovému vykonávaniu smernice NIS

– lepšia spolupráca v oblasti certifikácie vďaka inštitucionálnemu rámcu, ktorý umožňuje rozvoj európskych systémov certifikácie kybernetickej bezpečnosti a spoločnej politiky v tejto oblasti.

Posilnená spôsobilosť EÚ na doplnenie činnosti členských štátov

– lepšia „operačná kapacita EÚ“ na doplnenie a podporu činnosti členských štátov na požiadanie a vo vzťahu k obmedzeným a vopred určeným službám. Očakáva sa jej pozitívny vplyv na úspešnosť prevencie a odhaľovania incidentov, ako aj reakcie na ne, a to na úrovni členských štátov aj Únie;

Vyššie povedomie občanov a podnikov o otázkach kybernetickej bezpečnosti

- vyššie všeobecné povedomie občanov a podnikov o otázkach kybernetickej bezpečnosti
- lepšia schopnosť prijímať informované rozhodnutia pri kúpe produktov a služieb IKT vďaka certifikácii kybernetickej bezpečnosti

Pevnejšia dôvera v digitálny jednotný trh a digitálne inovácie vďaka vyššej celkovej transparentnosti uistenia o dôveryhodnosti kybernetickej bezpečnosti produktov a služieb IKT

– väčšia transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti⁴⁶ produktov a služieb IKT vďaka zjednodušeniu postupov certifikácie bezpečnosti prostredníctvom celoúniijného rámca

– vyšší stupeň uistenia o dôveryhodnosti bezpečnostných vlastností produktov a služieb IKT

– väčšie využívanie certifikácie bezpečnosti motivované zjednodušenými postupmi, zníženými nákladmi a perspektívou podnikateľských príležitostí v celej EÚ neobmedzovaných roztrieštenosťou trhu

– vyššia konkurencieschopnosť na trhu kybernetickej bezpečnosti v rámci EÚ vďaka zníženiu nákladov a administratívnej záťaže pre MSP a odstráneniu prípadných prekážok vstupu na trh spôsobených viacerými vnútroštátnymi systémami certifikácie

Iné

- Pri žiadnom z týchto cieľov sa neočakáva významný vplyv na životné prostredie.
- Pokiaľ ide o rozpočet EÚ, možno očakávať zvýšenie efektívnosti vďaka posilnenej spolupráci a koordinácii činností medzi inštitúciami, agentúrami a orgánmi EÚ.

1.4.4. Ukazovatele výsledkov a vplyvu

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

⁴⁶

Transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti spočíva v poskytovaní dostatočných informácií používateľom o kyberneticko-bezpečnostných prvkoch, ktoré im umožnia objektívne určiť úroveň bezpečnosti daného produktu, služby alebo procesu IKT.

Cieľ: Posilniť spôsobilosti a pripravenosť členských štátov a podnikov:

- počet školení zorganizovaných agentúrou ENISA
- geografické rozloženie (počet krajín a oblastí) priamej pomoci poskytovanej agentúrou ENISA
- úroveň pripravenosti, ktorú dosiahli členské štáty z hľadiska funkčnosti jednotiek CSIRT a dohľadu nad regulačnými opatreniami súvisiacimi s kybernetickou bezpečnosťou
- počet celoúnijných osvedčených postupov, ktoré pre kritické infraštruktúry poskytuje agentúra ENISA
- počet celoúnijných osvedčených postupov pre MSP, ktoré poskytuje agentúra ENISA
- uverejňovanie ročných strategických analýz kybernetických hrozieb a incidentov agentúrou ENISA na účely identifikácie nových trendov
- pravidelné prispievanie agentúry ENISA k činnosti pracovných skupín Európskych normalizačných organizácií (ESO) pre kybernetickú bezpečnosť.

Cieľ: Zlepšiť spoluprácu a koordináciu naprieč členskými štátmi a inštitúciami, agentúrami a orgánmi EÚ:

- počet členských štátov, ktoré využili odporúčania a stanoviská agentúry ENISA pri svojom procese tvorby politiky
- počet inštitúcií, agentúr a orgánov EÚ, ktoré využili odporúčania a stanoviská agentúry ENISA pri svojom procese tvorby politiky
- pravidelné vykonávanie pracovného programu siete jednotiek CSIRT a riadne fungujúca infraštruktúra IT a komunikačné kanály siete jednotiek CSIRT
- počet technických správ, ktoré má k dispozícii a používa skupina pre spoluprácu
- konzistentný prístup k cezhraničnému a medziodvetvovému vykonávaniu smernice NIS
- počet hodnotení dodržiavania predpisov vykonaných agentúrou ENISA
- počet stredísk pre výmenu a analýzu informácií (ISAC) v jednotlivých odvetviach, a to najmä v prípade kritických infraštruktúr
- zriadenie a trvalé fungovanie informačnej platformy na šírenie informácií o kybernetickej bezpečnosti od inštitúcií, agentúr a orgánov EÚ
- pravidelné prispievanie k príprave pracovných programov EÚ v oblasti výskumu a inovácií
- existujúca dohoda o spolupráci medzi agentúrou ENISA, EC3 a tímom CERT-EU
- počet systémov certifikácie zahrnutých a vyvinutých na základe rámca

Cieľ: Posilniť spôsobilosti na úrovni EÚ na doplnenie činností členských štátov, a to najmä v prípade cezhraničných kybernetických kríz:

- uverejňovanie ročných strategických analýz kybernetických hrozieb a incidentov agentúrou ENISA na účely identifikácie nových trendov

- uverejňovanie zhromaždených informácií o incidentoch, ktoré nahlásila agentúra ENISA na základe smernice NIS
- počet celoeurópskych cvičení koordinovaných agentúrou a počet zapojených členských štátov a organizácií
- počet žiadostí o podporu reakcie na núdzové situácie podaných členskými štátmi a realizovaných agentúrou ENISA
- počet analýz zraniteľností, artefaktov a incidentov vykonaných agentúrou ENISA v spolupráci s tímom CERT-EU
- dostupnosť celoúnijných situačných správ na základe informácií sprístupnených agentúre ENISA zo strany členských štátov a ostatných subjektov v prípade cezhraničného kybernetického incidentu veľkého rozsahu

Cieľ: Zvýšiť informovanosť občanov a podnikov o otázkach kybernetickej bezpečnosti:

- Pravidelné konanie celoúnijných a vnútroštátnych kampaní na zvyšovanie informovanosti a pravidelná aktualizácia tém na základe vznikajúcich vzdelávacích potrieb.
- Zvýšenie povedomia občanov EÚ o problematike kybernetickej bezpečnosti
- Pravidelné konanie kvízu o kybernetickej bezpečnosti a postupné zvyšovanie podielu správnych odpovedí.
- Pravidelné uverejňovanie osvedčených postupov kybernetickej bezpečnosti a počítačovej hygieny zameraných na zamestnancov a organizácie.

Cieľ: Posilniť dôveru v digitálny jednotný trh a digitálne inovácie zvýšením celkovej transparentnosti uistenia o dôveryhodnosti kybernetickej bezpečnosti⁴⁷ produktov a služieb IKT:

- počet systémov, ktoré dodržiavajú tento rámec EÚ
- nižšie náklady na získanie certifikátu bezpečnosti IKT
- počet orgánov posudzovania zhody so špecializáciou na certifikáciu IKT vo všetkých členských štátoch
- zriadenie európskej skupiny pre certifikáciu kybernetickej bezpečnosti a pravidelné organizovanie jej zasadnutí
- usmernenia pre certifikáciu na základe platného rámca EÚ
- pravidelné uverejňovanie analýz hlavných trendov na trhu kybernetickej bezpečnosti v EÚ
- počet certifikovaných produktov a služieb IKT v súlade s pravidlami európskeho rámca bezpečnostnej certifikácie IKT
- väčší počet koncových používateľov, ktorí sú si vedomí bezpečnostných znakov produktov a služieb IKT

b)

⁴⁷

Transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti spočíva v poskytovaní dostatočných informácií používateľom o kyberneticko-bezpečnostných prvkoch, ktoré im umožnia objektívne určiť úroveň bezpečnosti daného produktu, služby alebo procesu IKT.

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

Vzhľadom na regulačné požiadavky a rýchlo sa vyvíjajúce prostredie kybernetických hrozieb treba preskúmať mandát agentúry ENISA s cieľom stanoviť nový súbor úloh a funkcií, aby sa efektívne a účinne podporili členské štáty, inštitúcie EÚ a ostatné zainteresované strany v ich úsilí o zaistenie bezpečného kybernetického priestoru v Európskej únii. V navrhovanom vymedzení rozsahu mandátu sa posilňujú tie oblasti, kde agentúra preukázala jasnú pridanú hodnotu, a dopĺňajú sa oblasti, v ktorých je potrebná podpora vzhľadom na nové politické priority a nástroje, najmä pokiaľ ide o smernicu NIS, preskúmanie stratégie kybernetickej bezpečnosti EÚ, koncepciu kybernetickej bezpečnosti EÚ pre spoluprácu v prípade kybernetickej krízy a bezpečnostnú certifikáciu IKT. Tento nový navrhovaný mandát má agentúre priznať silnejšiu a ústrednejšiu úlohu, aby okrem iného aktívnejšie podporovala členské štáty v boji proti konkrétnym hrozbám (operačná kapacita) a aby sa stala strediskom odbornosti na podporu členských štátov a Komisie v otázkach kyberneticko-bezpečnostnej certifikácie.

Zároveň sa týmto návrhom zavádza európsky rámec certifikácie kybernetickej bezpečnosti produktov a služieb IKT a špecifikujú sa základné funkcie a úlohy agentúry ENISA v oblasti certifikácie kybernetickej bezpečnosti. V tomto rámci sa stanovujú spoločné ustanovenia a postupy, ktoré umožňujú vytvorenie celoeurópskych systémov certifikácie kybernetickej bezpečnosti vo vzťahu k jednotlivým produktom/službám IKT alebo kyberneticko-bezpečnostným rizikám. Vytvorenie európskych systémov certifikácie kybernetickej bezpečnosti v súlade s týmto rámcom umožní, aby certifikáty vydané na ich základe boli platné a uznávané vo všetkých členských štátoch a aby sa tak riešila súčasná fragmentácia trhu.

1.4.6. *Prínos zapojenia Únie*

Kybernetická bezpečnosť je skutočne globálny problém, ktorý je svojou podstatou cezhraničný a čoraz viac medziodvetvový vzhľadom na vzájomné prepojenia medzi sieťami a informačnými systémami. Počet, zložitosť a rozsah kybernetických incidentov a ich vplyv na hospodárstvo a spoločnosť postupne narastá a očakáva sa, že sa bude ďalej zvyšovať súbežne s technologickým vývojom, napríklad rozširovaním internetu vecí. Z toho vyplýva, že nemožno očakávať, že sa v budúcnosti zníži potreba väčšieho spoločného úsilia členských štátov, inštitúcií EÚ a súkromných zainteresovaných strán reagovať na kyberneticko-bezpečnostné hrozby.

Od svojho založenia v roku 2004 sa agentúra ENISA zameriava na podporu spolupráce medzi členskými štátmi a zainteresovanými stranami v oblasti sieťovej a informačnej bezpečnosti vrátane podpory spolupráce verejného a súkromného sektora. Táto podpora spolupráce spočívala v odbornej činnosti na poskytnutie celoeurópskeho prehľadu hrozieb, zriadení expertných skupín a organizovaní celoeurópskych cvičení pre verejný a súkromný sektor zameraných na kybernetické incidenty a krízové riadenie (najmä cvičenie „CyberEurope“). V smernici NIS sa agentúra ENISA poverila ďalšími úlohami, a to aj pokiaľ ide o zabezpečovanie sekretariátu siete jednotiek CSIRT pre operačnú spoluprácu medzi členskými štátmi.

Pridaná hodnota konania na úrovni EÚ, najmä na účely posilnenia spolupráce medzi členskými štátmi, ale aj medzi kyberneticko-bezpečnostnými komunitami, je uznaná v záveroch Rady z roku 2016⁴⁸ a takisto zreteľne vychádza z hodnotenia agentúry ENISA z

⁴⁸ Závery Rady o posilnení európskeho systému kybernetickej odolnosti a podpore konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti z 15. novembra 2016.

roku 2017, z ktorého vyplýva, že prínos agentúry spočíva predovšetkým v jej schopnosti posilniť spoluprácu medzi týmito zainteresovanými stranami. Na úrovni EÚ neexistuje žiadny iný subjekt, ktorý by podporoval spoluprácu takto rôznorodej škály zainteresovaných strán v oblasti sieťovej a informačnej bezpečnosti.

Pridaná hodnota agentúry ENISA v zbližovaní kyberneticko-bezpečnostných komunít a zainteresovaných strán je viditeľná aj v oblasti certifikácie. V dôsledku nárastu počítačovej kriminality a bezpečnostných hrozieb vznikajú vnútroštátne iniciatívy, v rámci ktorých sa na vysokej úrovni stanovujú kyberneticko-bezpečnostné a certifikačné požiadavky na komponenty IKT používané v tradičnej infraštruktúre. Napriek svojmu významu tieto iniciatívy nesú riziko roztrieštenia jednotného trhu a vytvorenia prekážok pre interoperabilitu. Dochádza k prípadom, keď predajca IKT musí absolvovať niekoľko postupov certifikácie, aby mohol predávať vo viacerých členských štátoch. Bez zásahu na úrovni EÚ sa pravdepodobne neodstráni neúčinnosť/neefektívnosť súčasných systémov certifikácie. Bez prijatia opatrenia sa v dôsledku vzniku nových systémov certifikácie v krátkodobom horizonte (najbližších 5 až 10 rokov) veľmi pravdepodobne zvýši fragmentácia trhu. Nedostatočná koordinácia a interoperabilita medzi takýmito systémami je prvok, ktorý znižuje potenciál digitálneho jednotného trhu. To je dôkazom pridanej hodnoty zavedenia európskeho rámca certifikácie kybernetickej bezpečnosti produktov a služieb IKT, ktorým sa stanovujú správne podmienky na účinné riešenie problémov súvisiacich so súbežnou existenciou viacerých postupov certifikácie v rôznych členských štátoch, čím sa znížia náklady na certifikáciu, ktorá sa tak v EÚ celkovo zatriktívni z obchodného a konkurenčného hľadiska.

1.4.7. *Poznatky získané z podobných skúseností v minulosti*

V súlade s právnym základom pre agentúru ENISA Komisia vykonala hodnotenie agentúry, ktoré zahŕňalo nezávislú štúdiu, ako aj verejnú konzultáciu. V hodnotení sa dospelo k záveru, že ciele agentúry ENISA sú aktuálne aj dnes. Vzhľadom na technologický vývoj, meniace sa hrozby a výraznú potrebu zvýšenia sieťovej a informačnej bezpečnosti (NIS) v EÚ sú potrebné odborné znalosti o vývoji v oblasti sieťovej a informačnej bezpečnosti. V členských štátoch treba budovať kapacity s cieľom pochopiť a reagovať na hrozby a zainteresované strany musia spolupracovať nad rámec tematických oblastí a inštitúcií.

Agentúra úspešne prispieva k zvýšeniu sieťovej a informačnej bezpečnosti v Európe ponukou na budovanie kapacít v 28 členských štátoch, posilňovaním spolupráce medzi členskými štátmi a zainteresovanými stranami v oblasti sieťovej a informačnej bezpečnosti; poskytovaním odborných znalostí, budovaním komunít a podporou politiky.

Agentúre ENISA sa síce podarilo v obrovskej oblasti sieťovej a informačnej bezpečnosti dosiahnuť určitý vplyv, nepodarilo sa jej však úplne etablovať ako silná značka, získať dostatočnú viditeľnosť a presadiť sa ako to pravé stredisko odbornosti v Európe. Dôvodom je široký mandát agentúry ENISA, ktorému nezodpovedajú dostatočne veľké zdroje. Okrem toho je agentúra ENISA jedinou agentúrou EÚ s časovo obmedzeným mandátom, ktorý obmedzuje jej schopnosť pripraviť dlhodobú víziu a udržateľne podporovať zainteresované strany. Je to aj v rozpore s ustanoveniami smernice NIS, ktoré agentúre ENISA zverujú úlohy bez časového obmedzenia.

Pokiaľ ide o certifikáciu kybernetickej bezpečnosti produktov a služieb IKT, v súčasnosti neexistuje žiadny európsky rámec. V dôsledku nárastu počítačovej kriminality a bezpečnostných hrozieb však vznikajú vnútroštátne iniciatívy, ktoré vytvárajú riziko roztrieštenia jednotného trhu.

1.4.8. *Zlučiteľnosť a možná synergia s inými vhodnými nástrojmi*

Táto iniciatíva je vysoko koherentná s existujúcimi politikami, najmä v oblasti vnútorného trhu. Je skutočne koncipovaná v súlade s celkovým prístupom ku kybernetickej bezpečnosti vymedzeným v preskúmaní stratégie digitálneho jednotného trhu, aby doplnila komplexný súbor opatrení, napríklad preskúmanie stratégie kybernetickej bezpečnosti EÚ, koncepciu spolupráce v prípade kybernetickej krízy a iniciatív boja proti počítačovej kriminalite. Zabezpečila by zosúladenie s ustanoveniami existujúcich právnych predpisov v oblasti kybernetickej bezpečnosti a vychádzala by z nich, najmä zo smernice NIS, s cieľom ďalej zvyšovať kybernetickú odolnosť EÚ posilnením spôsobilostí, spolupráce, riadenia rizík a povedomia o kybernetickej bezpečnosti.

Navrhované certifikačné opatrenia by mali riešiť potenciálnu roztrieštenosť spôsobenú existujúcimi a novovznikajúcimi vnútroštátnymi systémami certifikácie, a tak prispieť k rozvoju digitálneho jednotného trhu. Táto iniciatíva takisto podporuje a dopĺňa vykonávanie smernice NIS tým, že podnikom, na ktoré sa táto smernica vzťahuje, poskytuje nástroj na preukázanie splnenia požiadaviek sieťovej a informačnej bezpečnosti v celej Únii.

Navrhovaný európsky rámec certifikácie kybernetickej bezpečnosti IKT nemá vplyv na všeobecné nariadenie o ochrane údajov (GDPR)⁴⁹, a najmä na príslušné ustanovenia o certifikácii⁵⁰, ktoré sa uplatňujú na bezpečnosť spracovávaní osobných údajov. V neposlednom rade by sa systémy navrhované v budúcom európskom rámci mali v čo najväčšej miere opierať o medzinárodné normy ako spôsob zabránenia vzniku obchodných prekážok a zabezpečenia súladu s medzinárodnými iniciatívami.

⁴⁹ Nariadenie (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

⁵⁰ Napríklad články 42 (certifikácia) a 43 (certifikačné orgány), ako aj články 57, 58 a 70 týkajúce sa príslušných úloh a právomocí nezávislých orgánov dohľadu a úloh Európskeho výboru pre ochranu údajov.

1.5. Trvanie a finančný vplyv

☐ Návrh/iniciatíva s **obmedzeným trvaním**

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

– ☐ Finančný vplyv trvá od RRRR do RRRR.

☒ Návrh/iniciatíva s **neobmedzeným trvaním**

– Počiatočná fáza vykonávania bude trvať od roku 2019 do roku 2020

– a potom bude vykonávanie pokračovať v plnom rozsahu.

1.6. Plánovaný spôsob hospodárenia⁵¹

☒ **Priame hospodárenie** na úrovni Komisie (Hlava III – Certifikácia) prostredníctvom

– ☐ výkonných agentúr

☐ **Zdieľané hospodárenie** s členskými štátmi

☒ **Nepriame hospodárenie** so zverením úloh súvisiacich s plnením rozpočtu:

☐ medzinárodným organizáciám a ich agentúram (uved'te),

☐ Európskej investičnej banke (EIB) a Európskemu investičnému fondu,

☒ subjektom podľa článkov 208 a 209 (Hlava II – ENISA),

☐ verejnoprávnym subjektom,

☐ súkromnoprávnym subjektom povereným vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,

☐ súkromnoprávnym subjektom spravovaným právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú dostatočné finančné záruky,

☐ osobám povereným vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určeným v príslušnom základnom akte.

Poznámky

Nariadenie zahŕňa:

– Hlavu II navrhovaného nariadenia, v ktorej sa preskúma mandát Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), pričom sa agentúre priznáva dôležitá úloha pri certifikácii, a

– Hlavu III, v ktorej sa ustanovuje rámec na vytvorenie európskych systémov certifikácie kybernetickej bezpečnosti produktov a služieb IKT, v ktorom agentúra ENISA zohráva kľúčovú úlohu.

⁵¹

Vysvetlenie spôsobov hospodárenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovej stránke BudgWeb: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

Uved'te časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Monitorovanie sa začne hneď po prijatí právneho nástroja a bude sa zameriavať na jeho uplatňovanie. Komisia zorganizuje stretnutia s agentúrou ENISA, zástupcami členských štátov (napr. expertná skupina) a príslušnými zainteresovanými stranami, najmä s cieľom uľahčiť vykonávanie pravidiel certifikácie, ako je napríklad zriadenie rady.

Prvé hodnotenie by sa malo uskutočniť 5 rokov po nadobudnutí účinnosti právneho nástroja za predpokladu, že je k dispozícii dostatok údajov. Právny nástroj obsahuje konkrétne ustanovenie o hodnotení a preskúmaní [článok XXX], na základe ktorého Komisia vykoná nezávislé hodnotenie. Komisia následne predloží správu Európskemu parlamentu a Rade o svojom hodnotení a v prípade potreby predloží návrh na jeho preskúmanie s cieľom zmerať vplyv nariadenia a jeho pridanú hodnotu. Ďalšie hodnotenia by sa mali vykonávať každých päť rokov. Na hodnotenie sa bude uplatňovať metodika lepšej právnej regulácie Komisie. Tieto hodnotenia sa budú realizovať za pomoci cielených diskusií odborníkov, štúdií a rozsiahlej konzultácie so zainteresovanými stranami.

Výkonný riaditeľ agentúry ENISA by mal každé dva roky predložiť správnej rade *ex post* hodnotenie činnosti agentúry ENISA. Agentúra by mala tiež vypracovať nadväzný akčný plán týkajúci sa záverov retrospektívnych hodnotení a každé dva roky predkladať správy o pokroku Komisii. Správna rada by mala dohliadať na primerané kroky nadväzujúce na takéto závery.

Údajné prípady nesprávneho úradného postupu agentúry môžu podliehať vyšetrovaniu európskeho ombudsmana v súlade s ustanoveniami článku 228 zmluvy.

Údaje pre plánované monitorovanie by poskytovali hlavne ENISA, európska skupina pre certifikáciu kybernetickej bezpečnosti, skupina pre spoluprácu, sieť jednotiek CSIRT a orgány členských štátov. Okrem údajov pochádzajúcich zo správ (vrátane výročných správ o činnosti) agentúry ENISA, európskej skupiny pre certifikáciu kybernetickej bezpečnosti, skupiny pre spoluprácu a siete jednotiek CSIRT sa v prípade potreby použijú osobitné nástroje zberu údajov (napríklad prieskumy vnútroštátnych orgánov, Eurobarometer a správy z kampane Mesiac kybernetickej bezpečnosti a z celoeurópskych cvičení).

2.2. Systémy riadenia a kontroly

2.2.1. Zistené riziká.

Zistené riziká sú obmedzené: agentúra Európskej únie už existuje a jej mandát sa vymedzí a posilní v tých oblastiach, kde agentúra preukázala jasnú pridanú hodnotu, a doplní sa o nové oblasti, v ktorých je potrebná podpora vzhľadom na nové politické priority a nástroje, najmä smernicu NIS, preskúmanie stratégie kybernetickej bezpečnosti EÚ, pripravovanú koncepciu kybernetickej bezpečnosti EÚ pre spoluprácu v prípade kybernetickej krízy a bezpečnostnú certifikáciu IKT.

V návrhu sa preto určujú funkcie agentúry vedúce k zvýšeniu efektívnosti. Rozšírenie operačných kompetencií a úloh nepredstavuje skutočné riziko, keďže budú dopĺňať činnosti

členských štátov a podporovať ich na požiadanie a vo vzťahu k obmedzeným a vopred určeným službám.

Okrem toho navrhovaný model agentúry v súlade so spoločným prístupom zabezpečí zavedenie dostatočnej kontroly, aby agentúra ENISA dosahovala svoje ciele. Prevádzkové a finančné riziká navrhovaných zmien sa zdajú obmedzené.

Zároveň je potrebné zabezpečiť primerané finančné zdroje pre agentúru ENISA, aby plnila úlohy, ktoré jej boli zverené v novom mandáte, a to aj v oblasti certifikácie.

2.2.2. *Plánovaný spôsob kontroly*

Účtovné závierky agentúry sa budú predkladať na schválenie Dvoru audítorov, budú podliehať postupu udeľovania absolutória a plánujú sa audity.

Činnosť agentúry tiež podlieha dohľadu ombudsmana v súlade s ustanoveniami článku 228 zmluvy.

Pozri aj bod 2.1 a 2.2.1.

2.3. **Opatrenia na predchádzanie podvodom a nezrovnalostiam**

Uveďte existujúce a plánované preventívne a ochranné opatrenia.

Budú sa uplatňovať preventívne a ochranné opatrenia agentúry ENISA, a to:

– 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. Ustanovenia proti podvodom (dohľad, požiadavky na podávanie správ atď.) sa zahrnú do všetkých dohôd a zmlúv uzavretých medzi agentúrou a príjemcami akýchkoľvek platieb.

– Na boj proti podvodom, korupcii a iným protiprávnym aktivitám sa bez obmedzenia uplatňujú ustanovenia nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013 z 25. mája 1999 o vyšetрованиach vykonávaných Európskym úradom pre boj proti podvodom (OLAF).

– Agentúra do šiestich mesiacov od nadobudnutia účinnosti tohto nariadenia pristúpi k medziinštitucionálnej dohode z 25. mája 1999 medzi Európskym parlamentom, Radou Európskej únie a Komisiou Európskych spoločenstiev o vnútornom vyšetřovaní vykonávanom Európskym úradom pre boj proti podvodom (OLAF) a bezodkladne vydá príslušné ustanovenia uplatniteľné na všetkých zamestnancov agentúry.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

- Existujúce rozpočtové riadky

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

Okruh viacročného finančného rámca:	Rozpočtový riadok	Druh výdavkov	Príspevky			
		DRP/N RP. ⁵²	krajín EZVO ⁵³	kandidátskych krajín ⁵⁴	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách
1a Konkurencieschopnosť pre rast a zamestnanosť	09.0203 ENISA a bezpečnostná certifikácia informačných a komunikačných technológií	DRP	ÁNO	NIE	NIE	NIE
5 Administratívne výdavky]	09.0101 Výdavky vzťahujúce sa na zamestnancov v aktívnom pracovnom pomere v oblasti komunikačných sietí, obsahu a technológií 09.0102 Výdavky vzťahujúce sa na externých zamestnancov v aktívnom pracovnom	NRP	NIE	NIE	NIE	NIE

⁵² DRP = diferencované rozpočtové prostriedky / NRP = nediferencované rozpočtové prostriedky.

⁵³ EZVO: Európske združenie voľného obchodu.

⁵⁴ Kandidátske krajiny a prípadne potenciálne kandidátske krajiny západného Balkánu.

	pomere v oblasti komunikačných sietí, obsahu a technológií 09.010211 Ostatné výdavky na riadenie					
--	--	--	--	--	--	--

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca		1a	Konkurencieschopnosť pre rast a zamestnanosť					
ENISA			Východiskový stav 2017 (31/12/2016)	2019 (od 1. 7. 2019)	2020	2021	2022	SPOLU
Hlava 1: Výdavky na zamestnancov (vrátane výdavkov na prijímanie zamestnancov, odbornú prípravu, sociálnu a zdravotnícku infraštruktúru a externé služby)	Závazky	(1)	6,387	9,899	12,082	13,349	13,894	49,224
	Platby	(2)	6,387	9,899	12,082	13,349	13,894	49,224
Hlava 2: Výdavky na infraštruktúru a operačné výdavky	Závazky	(1a)	1,770	1,957	2,232	2,461	2,565	9,215
	Platby	(2a)	1,770	1,957	2,232	2,461	2,565	9,215
Hlava 3: Operačné výdavky	Závazky	(3a)	3,086	4,694	6,332	6,438	6,564	24,028
	Platby	(3b)	3,086	4,694	6,332	6,438	6,564	24,028
Rozpočtové prostriedky	Závazky	= 1 + 1a + 3a	11,244	16,550	20,646	22,248	23,023	82,467

pre agentúru ENISA SPOLU	Platby	= 2 + 2a + 3b	11,244	16,550	20,646	22,248	23,023	82,467
---------------------------------	--------	---------------------	---------------	---------------	---------------	---------------	---------------	---------------

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

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2019 <i>(od 1. 7. 2019)</i>	2020	2021	2022	SPOLU
GR: CNECT						
• Ľudské zdroje		0,216	0,846	0,846	0,846	2,754
• Ostatné administratívne výdavky		0,102	0,235	0,238	0,242	0,817
SPOLU GR CNECT	Rozpočtové prostriedky	0,318	1,081	1,084	1,088	3,571

Náklady na zamestnancov sa vypočítali podľa predpokladaného dátumu prijatia do zamestnania (začiatok pracovného pomeru sa predpokladá od 1. 7. 2019).

Výhladové zdroje na obdobie po roku 2020 majú len orientačnú povahu a nie sú nimi dotknuté návrhy Komisie na viacročný finančný rámec po roku 2020

Rozpočtové prostriedky OKRUHU 5 viacročného finančného rámca SPOLU	(Závázky spolu = Platby spolu)	0,318	1,081	1,084	1,088	3,571
---	-----------------------------------	-------	-------	-------	-------	--------------

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2019	2020	2021	2022	SPOLU
Rozpočtové prostriedky OKRUHOV 1 až 5 viacročného finančného rámca SPOLU	Závazky	16,868	21,727	23,332	24,11	86,038
	Platby	16,868	21,727	23,332	24,11	86,038

3.2.2. Odhadovaný vplyv na rozpočtové prostriedky agentúry

- ☐ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov.
- ☒ Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

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

Uved'te ciele a výstupy ⁵⁵ ↓	2019	2020	2021	2022	SPOLU
Posilniť spôsobilosti a pripravenosť členských štátov a podnikov	1,408	1,900	1,931	1,969	7,208
Zlepšiť spoluprácu a koordináciu medzi členskými štátmi, inštitúciami, agentúrami a orgánmi EÚ	0,939	1,266	1,288	1,313	4,806
Posilniť spôsobilosť EÚ na doplnenie činnosti členských štátov, a to najmä v prípade cezhraničných kybernetických kríz	0,704	0,950	0,965	0,985	3,604
Zvýšiť informovanosť občanov a podnikov o otázkach kybernetickej bezpečnosti	0,704	0,950	0,965	0,985	3,604
Posilniť dôveru v digitálny jednotný trh a digitálne inovácie zvýšením celkovej transparentnosti uistenia o dôveryhodnosti kybernetickej bezpečnosti produktov a služieb IKT	0,939	1,266	1,288	1,313	4,806
NÁKLADY SPOLU	4 694	6,332	6,437	6,565	24,028

⁵⁵

Táto tabuľka obsahuje len operačné výdavky podľa hlavy 3.

3.2.3. Odhadovaný vplyv na ľudské zdroje agentúry

3.2.3.1. Zhrnutie

- ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov.
- ☒ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

	Q3/4 2019	2020	2021	2022
Dočasní úradníci (funkčná skupina AD)	4,242	5,695	6,381	6,709
Dočasní úradníci (funkčná skupina AST)	1,601	1,998	2,217	2,217
Zmluvní zamestnanci	2,041	2,041	2,041	2,041
Vyslaní národní experti	0,306	0,447	0,656	0,796
SPOLU	8,190	10,181	11,295	11,763

Náklady na zamestnancov sa vypočítali podľa predpokladaného dátumu prijatia do zamestnania (začiatok pracovného pomeru terajších zamestnancov agentúry ENISA sa predpokladá od 1. 1. 2019). Pri nových zamestnancoch sa predpokladal postupný nástup do zamestnania so začiatkom od 1. 7. 2019 a dosiahnutie plnej zamestnanosti v roku 2022. Výhľadové zdroje na obdobie po roku 2020 majú len orientačnú povahu a nie sú nimi dotknuté návrhy Komisie na viacročný finančný rámec po roku 2020

Odhadovaný vplyv na zamestnancov (dodatočný ekvivalent plného pracovného času) – plán pracovných miest

Funkčná skupina a trieda	2017 Súčasní zamestnanci agentúry ENISA	Q3/Q4 2019	2020	2021	2022
AD 16					
AD 15	1				
AD 14					
AD 13					
AD 12	3	3			
AD 11					
AD 10	5				
AD 9	10	2			
AD 8	15	4	2		1
AD 7			3	3	2
AD 6			3	3	

AD 5					
AD spolu	34	9	8	6	3
AST 11					
AST 10					
AST 9					
AST 8					
AST 7	2	1	1	1	
AST 6	5	2	1		
AST 5	5				
AST 4	2				
AST 3					
AST 2					
AST 1					
AST spolu	14	3	2	1	
AST/SC 6					
AST/SC 5					
AST/SC 4					
AST/SC 3					
AST/SC 2					
AST/SC 1					
AST/SC spolu					
CELKOVÝ SÚČET	48	12	10	7	3

Úlohy pre ďalších zamestnancov AD/AST na dosiahnutie cieľov tohto nástroja, ako sa uvádza v oddiele 1.4.2:

Úlohy	AD	AST	VNE	Spolu
Politika a budovanie kapacít	8	1		9
Operačná spolupráca	8	1	7	16
Certifikácia (trhové úlohy)	9	3	2	14
Znalosti, informovanosť a povedomie	1	1		2
SPOLU	26	6	9	41

Opis úloh, ktoré sa majú vykonať:

Úlohy	Potreba dodatočných zdrojov
Tvorba a vykonávanie politiky EÚ a budovanie kapacít	K úlohám bude patriť pomoc skupine pre spoluprácu, podpora jednotného cezhraničného vykonávania smernice NIS, pravidelné podávanie správ o stave vykonávania právneho rámca EÚ; poskytovanie poradenstva a koordinácia odvetvových iniciatív v oblasti kybernetickej bezpečnosti vrátane odvetví energetiky a dopravy (napr. letecká, cestná, námorná)

	doprava/prepojené vozidlá), zdravotníctva, finančníctva a poskytovanie podpory na zriadenie stredísk pre výmenu a analýzu informácií (ISAC) v rôznych odvetviach.
Operačná spolupráca a krízové riadenie	K úlohám bude patriť: Zabezpečovať sekretariát pre sieť jednotiek CSIRT, okrem iného aj zabezpečením riadne fungujúcej IT infraštruktúry a komunikačných kanálov siete jednotiek CSIRT. Zabezpečovať štruktúrovanú spoluprácu s CERT-EU, EC3 a ostatnými príslušnými orgánmi EÚ. Organizovať cvičenia CyberEurope⁵⁶ – úlohy súvisiace so skrátením intervalu konania cvičení z dvojročného na ročný a zabezpečením sledovania incidentov od ich vzniku až do konca. Technická pomoc – k úlohám bude patriť štruktúrovaná spolupráca s CERT-EU pri poskytovaní technickej pomoci v prípade závažných incidentov a podpore analýzy incidentov. V tom by bola zahrnutá pomoc pre členské štáty pri riešení incidentov a analýze zraniteľností, ako aj artefaktov a incidentov. Ďalej napomáhať spoluprácu medzi jednotlivými členskými štátmi pri reakciách na núdzové situácie prostredníctvom analýzy a zoskupovania situačných správ členských štátov na základe informácií, ktoré agentúre sprístupnili členské štáty a iné subjekty. Koncepcia koordinovanej reakcie na cezhraničné kybernetické incidenty veľkého rozsahu – agentúra sa bude podieľať na vývoji spoločnej reakcie na úrovni Únie a členských štátov v prípade rozsiahlych cezhraničných incidentov alebo kríz kybernetickej bezpečnosti, a to plnením celej škály úloh od podieľania sa na budovaní situačného povedomia na úrovni Únie až po testovanie plánov spolupráce v prípade incidentov. Technické ex post skúmanie incidentov – viesť technické ex post skúmanie incidentov alebo k

⁵⁶

CyberEurope je zatiaľ najväčšie a najkomplexnejšie cvičenie kybernetickej bezpečnosti EÚ, na ktorom sa zúčastnilo viac ako 700 odborníkov na kybernetickú bezpečnosť z 28 členských štátov. Koná sa každý druhý rok. Z hodnotenia agentúry ENISA a stratégie kybernetickej bezpečnosti EÚ z roku 2013 vyplýva, že mnohé zainteresované strany presadzujú, aby sa toto cvičenie konalo každý rok vzhľadom na rýchlo sa meniacu povahu kybernetických hrozieb. Z dôvodu obmedzených zdrojov agentúry to však zatiaľ nie je možné.

	nim prispievať v spolupráci so sieťou jednotiek CSIRT s cieľom vydávať odporúčania a posilniť spôsobilosti vo forme verejných správ na účely lepšieho zabránenia budúcim incidentom.
Trhové úlohy (normalizácia, certifikácia)	K úlohám bude patriť aktívna podpora práce vykonávanej v certifikačnom rámci vrátane poskytovania technických poznatkov na prípravu kandidátskych európskych systémov certifikácie kybernetickej bezpečnosti. Úlohy budú zahŕňať aj podporu pri vypracovaní a vykonávaní politiky Únie v oblasti normalizácie, certifikácie a monitorovania trhu – to si bude vyžadovať napomáhanie preberania noriem riadenia rizika v súvislosti s elektronickými produktmi, sieťami a službami a poskytovanie odporúčaní pre prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb o technických bezpečnostných požiadavkách. Úlohy budú zahŕňať aj poskytovanie analýz hlavných trendov na trhu kybernetickej bezpečnosti.
Znalosti a informácie, zvyšovanie povedomia:	S cieľom zabezpečiť ľahší prístup k lepšie štruktúrovaným informáciám o rizikách súvisiacich s kybernetickou bezpečnosťou a možných nápravných opatreniach sa v tomto návrhu zveruje agentúre nová úloha zriadiť a prevádzkovať „informačné centrum“ Únie. K úlohám bude patriť zhromažďovanie informácií od inštitúcií, agentúr a orgánov EÚ o bezpečnosti (najmä kybernetickej) sieťových a informačných systémov, ich usporiadanie a sprístupňovanie verejnosti na vyhradenom portáli. Úlohy budú zahŕňať aj podporu činností agentúry ENISA v oblasti zvyšovania informovanosti s cieľom umožniť jej zintenzívniť úsilie.

3.2.3.2. Odhadované potreby ľudských zdrojov pre príslušné GR

- ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.
- ☒ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

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

		Dodatoční zamestnanci			
	Východiskový stav v roku 2017	Q3/4 2019	2020	2021	2020
• Plán pracovných miest (úradníci a dočasní zamestnanci)					
09 01 01 01 (ústredie a zastúpenia Komisie)	1	2	3		
• Externí zamestnanci (ekvivalent plného pracovného času)⁵⁷					
09 01 02 01 (ZZ, VNE, DAZ z celkového balíka prostriedkov)	1	2			
SPOLU		4	3		

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	Zastupujú Komisiu v správnej rade agentúry. Vypracúvajú stanoviská Komisie k jednotnému programovému dokumentu agentúry ENISA a monitorujú jeho vykonávanie. Dohliadajú na prípravu rozpočtu agentúry a monitorujú jeho plnenie. Pomáhajú agentúre pri rozvoji jej činností v súlade s politikami Únie, a to aj účasťou na príslušných stretnutiach. Dohliadajú na vykonávanie rámca pre európske systémy certifikácie kybernetickej bezpečnosti produktov a služieb IKT. Udržiavajú kontakty s členskými štátmi a ďalšími zainteresovanými stranami v súvislosti s činnosťami certifikácie. Spolupracujú s agentúrou ENISA v otázke kandidátskych systémov. Pripravujú kandidátske európske systémy certifikácie kybernetickej bezpečnosti.
--------------------------------	--

⁵⁷

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

Externí zamestnanci	Ako vyššie
---------------------	------------

3.2.4. Súlad s platným viacročným finančným rámcom

- ☐ Návrh/iniciatíva je v súlade s platným viacročným finančným rámcom.
- ☒ Návrh/iniciatíva si vyžaduje zmenu v plánovaní príslušného okruhu vo viacročnom finančnom rámci.

Návrh si vyžaduje preprogramovanie článku 09 02 03 z dôvodu revízie mandátu agentúry ENISA, v rámci ktorej sa agentúre zverujú nové úlohy, ktoré sa okrem iného týkajú vykonávania smernice NIS a európskeho rámca certifikácie kybernetickej bezpečnosti. Zodpovedajúce sumy:

Rok	Plán	Požiadavka
2019	10,739	16,550
2020	10,954	20,646
2021	Neuvádza sa	22,248*
2022	Neuvádza sa	23,023*

* Odhad financovanie zo zdrojov EÚ po roku 2020 sa preskúma v kontexte debaty o všetkých návrhoch v rámci celej Komisie na obdobie po roku 2020. To znamená, že keď Komisia predloží návrh budúceho viacročného finančného rámca, predloží zároveň aj zmenený legislatívny finančný výkaz zohľadňujúci závery posúdenia vplyvu⁵⁸.

- ☐ Návrh/iniciatíva si vyžaduje, aby sa použil nástroj flexibility alebo aby sa uskutočnila revízia viacročného finančného rámca⁵⁹.

3.2.5. Príspevky od tretích strán

- ☐ Návrh/iniciatíva nezahŕňa spolufinancovanie tretími stranami.
- ☒ Návrh/iniciatíva zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

⁵⁸

Odkaz na stránku s posúdením vplyvu.

⁵⁹

Pozri články 11 a 17 nariadenia Rady (EÚ, Euratom) č. 1311/2013, ktorým sa ustanovuje viacročný finančný rámec na roky 2014 – 2020.

	Rok 2019	Rok 2020	Rok 2021	Rok 2022
EZVO	p.m. ⁶⁰ .	p.m.	p.m.	p.m.

3.3. Odhadovaný vplyv na príjmy

- ☒ Návrh/iniciatíva nemá finančný vplyv na príjmy.
- ☐ Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:
 - ☐ vplyv na vlastné zdroje
 - ☐ vplyv na rôzne príjmy

⁶⁰

Presná suma na nasledujúce roky bude známa, keď sa stanoví faktor proporcionality EZVO na príslušný rok.