Rada
Evropské unie

Brusel 1. března 2018
(OR. en)

Interinstitucionální spis:
2017/0225 (COD)

12183/2/17
REV 2

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139
CSC 276
CSCI 68

NÁVRH

Č. dok. Komise:	COM(2017) 477 final/3
Předmět:	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o agentuře ENISA, Agentuře EU pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“)

Delegace naleznou v příloze dokument COM(2017) 477 final/3.

Příloha: COM(2017) 477 final/3

EVROPSKÁ
KOMISE

V Bruselu dne 22.2.2018
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o agentuře ENISA, Agentuře EU pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“)

(Text s významem pro EHP)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Evropská unie přijala celou řadu opatření na zvýšení odolnosti a zlepšení své připravenosti v oblasti kybernetické bezpečnosti. První strategie kybernetické bezpečnosti Evropské unie[1] přijatá v roce 2013 stanovila strategické cíle a konkrétní opatření s cílem dosáhnout odolnosti, snížit kyberkriminalitu, vypracovat politiku kybernetické obrany a související kapacity, vytvořit průmyslové a technologické zdroje a zavést soudržnou mezinárodní politiku Evropské unie v oblasti kyberprostoru. V této souvislosti od té doby došlo k důležitému vývoji, k němuž patří zejména druhý mandát pro Agenturu Evropské unie pro bezpečnost sítí a informací (agentura ENISA)[2] a přijetí **směrnice o bezpečnosti sítí a informačních systémů**[3] (dále jen „směrnice o bezpečnosti sítí a informací“), které tvoří základ tohoto návrhu.

Dále **Evropská komise v roce 2016 přijala sdělení o posílení evropského systému kybernetické odolnosti a o podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti**[4], v němž byla oznámena další opatření k posílení spolupráce, sdílení informací a znalostí a ke zvýšení odolnosti a připravenosti EU, a to i s ohledem na možnost rozsáhlých incidentů a možnou celoevropskou krizi v oblasti kybernetické bezpečnosti. Komise v této souvislosti oznámila, že uspíší **hodnocení** a **přezkum** nařízení Evropského parlamentu a Rady (EU) č. 526/2013 o agentuře ENISA a o zrušení nařízení (ES) č. 460/2004 (dále jen „nařízení o agentuře ENISA“). Proces hodnocení by mohl vést k případné reformě agentury a k posílení jejích schopností a kapacit udržitelným způsobem podporovat členské státy. Tato reforma by tedy agentuře přisoudila operativnější a více ústřední úlohu při dosahování odolnosti z hlediska kybernetické bezpečnosti a v novém mandátu agentury by uznala nové úkoly agentury na základě směrnice o bezpečnosti sítí a informací.

Směrnice o bezpečnosti sítí a informací je prvním zásadním krokem směrem k podpoře kultury řízení rizik, jelikož zavádí bezpečnostní požadavky jakožto právní povinnost pro klíčové hospodářské subjekty, zejména pro provozovatele poskytující základní služby (provozovatelé základních služeb) a pro dodavatele některých klíčových digitálních služeb (poskytovatelé digitálních služeb). Vzhledem k tomu, že bezpečnostní požadavky jsou vnímány jako stěžejní pro zajištění výhod rozvíjející se digitalizace společnosti, a vzhledem k rychlému a strmému nárůstu počtu zařízení připojených k internetu (internet věcí) sdělení z roku 2016 rovněž nastínilo myšlenku zřízení rámce pro certifikaci bezpečnosti produktů a služeb IKT za účelem zvýšení důvěry a bezpečnosti na jednotném digitálním trhu. Certifikace kybernetické bezpečnosti IKT se stává obzvláště důležitou s ohledem na rostoucí využívání technologií, které vyžadují vysokou úroveň kybernetické bezpečnosti, jako jsou například

---

1 Společné sdělení Evropské komise a Evropské služby pro vnější činnost: Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor – JOIN(2013).

2 Nařízení (EU) č. 526/2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004.

3 Směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

4 Sdělení Komise o posílení evropského systému kybernetické odolnosti a o podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti, COM/2016/0410 final.

propojené a automatizované automobily, elektronické zdravotnictví nebo průmyslové automatizační řídicí systémy (IACS).

Tato politická opatření a oznámení byla dále posílena **závěry Rady** z roku 2016, v nichž bylo uznáno, že „kybernetické hrozby a zranitelnost se nadále vyvíjí a stupňují, což bude vyžadovat pokračující a užší spolupráci, zejména při řešení rozsáhlých přeshraničních kybernetických bezpečnostních incidentů“. Závěry znovu potvrdily, že „nařízení o agentuře ENISA je jedním ze zásadních prvků rámce kybernetické odolnosti EU“[5], a vyzvaly Komisi, aby učinila další kroky k řešení otázky certifikace na evropské úrovni.

Zavedení systému certifikace by vyžadovalo vytvoření vhodného systému řízení na úrovni EU, jenž by zahrnoval podrobné odborné poradenství poskytované nezávislou agenturou EU. Tento návrh v této souvislosti identifikuje agenturu ENISA jako přirozenou instituci na úrovni EU, která je příslušná pro otázky kybernetické bezpečnosti a která by měla tuto úlohu přijmout a propojit a koordinovat práci příslušných vnitrostátních orgánů v oblasti certifikace.

Komise ve svém sdělení **z května 2017 o přezkumu strategie pro jednotný digitální trh v polovině období** dále upřesnila, že do září 2017 přezkoumá mandát agentury ENISA. Účelem tohoto přezkumu je nové vymezení role agentury v měnícím se kybernetickobezpečnostním ekosystému a vypracování opatření v oblasti norem kybernetické bezpečnosti, certifikace a označování v zájmu lepšího kybernetického zabezpečení systémů IKT včetně propojených objektů[6]. **Evropská rada ve svých závěrech** z června 2017[7] uvítala záměr Komise přezkoumat v září strategii kybernetické bezpečnosti a ještě do konce roku 2017 navrhnout další cílená opatření.

Navrhované nařízení stanoví komplexní soubor opatření, která vycházejí z předchozích opatření a podporují vzájemně se doplňující specifické cíle:

- **zvýšení schopností a připravenosti** členských států a podniků,
- zlepšení **spolupráce a koordinace** napříč členskými státy a orgány, agenturami a dalšími subjekty EU,
- zvýšení **úrovně schopností EU doplňovat opatření členských států**, zejména v případě přeshraničních kybernetických krizí,
- zvýšení **informovanosti** občanů a podniků o otázkách týkajících se kybernetické bezpečnosti,
- zvýšení celkové **transparentnosti záruky kybernetické bezpečnosti**[8] produktů a služeb IKT, aby se posílila důvěra v jednotný digitální trh a digitální inovace, a
- zabránění **roztříštěnosti systémů certifikace** v EU a souvisejících bezpečnostních požadavků a hodnoticích kritérií napříč členskými státy a odvětvími.

---

5 Závěry Rady o posílení evropského systému kybernetické odolnosti a o podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti – 15. listopadu 2016.

6 Sdělení Komise o přezkumu v polovině období provádění strategie pro jednotný digitální trh – COM(2017) 228.

7 Zasedání Evropské rady (22. a 23. června 2017) – závěry EUCO 8/17.

8 Transparentnost záruky kybernetické bezpečnosti spočívá v tom, že jsou uživatelům poskytovány dostatečné informace o vlastnostech kybernetické bezpečnosti, které těmto uživatelům umožňují objektivně stanovit úroveň bezpečnosti daného produktu, služby nebo procesu IKT.

Následující část důvodové zprávy podrobněji vysvětluje odůvodnění tohoto podnětu s ohledem na navrhovaná opatření týkající se agentury ENISA a certifikace kybernetické bezpečnosti.

Agentura ENISA

Agentura ENISA působí jako odborné středisko zaměřené na zvýšení bezpečnosti sítí a informací v Unii a na podporu budování kapacit členských států.

Agentura ENISA byla zřízena v roce 2004[9], aby přispěla k celkovému cíli zajištění vysoké úrovně bezpečnosti sítí a informací v EU. Nařízení (EU) č. 526/2013 v roce 2013 stanovilo pro agenturu nový mandát na dobu sedmi let, do roku 2020. Agentura má své kanceláře v Řecku, konkrétně správní sídlo v Heraklionu (Kréta) a hlavní útvary v Aténách.

Agentura ENISA je ve srovnání s ostatními agenturami EU malou agenturou s nízkým rozpočtem a počtem zaměstnanců. Má mandát na dobu určitou.

Agentura ENISA podporuje evropské orgány, členské státy a podnikatelský sektor při **řešení problémů v oblasti bezpečnosti sítí a informací, reagování na tyto problémy a především při předcházení těmto problémům.** Činí tak prostřednictvím souboru činností napříč pěti oblastmi stanovenými v její strategii[10]:

- Odborné znalosti: poskytování informací a odborných znalostí týkajících se klíčových otázek bezpečnosti sítí a informací.
- Politika: podpora tvorby politik a jejich provádění v Unii.
- Kapacita: podpora budování kapacit v Unii (např. prostřednictvím školení, doporučení, osvětových činností).
- Společenství: podpora komunity v oblasti bezpečnosti sítí a informací (např. podpora skupin pro reakce na počítačové hrozby (CERT), koordinace celoevropských kybernetických cvičení).
- Umožňování (např. spolupráce se zúčastněnými stranami a zapojení v rámci mezinárodních vztahů).

V průběhu jednání o směrnici o bezpečnosti sítí a informací se spolunormotvůrci EU rozhodli svěřit agentuře ENISA důležité úkoly při provádění této směrnice. Agentura zejména zajišťuje služby sekretariátu pro síť CSIRT (zřízenou za účelem podpory rychlé a účinné operativní spolupráce mezi členskými státy při konkrétních kybernetických bezpečnostních incidentech a při sdílení informací o rizicích) a jejím úkolem je rovněž být nápomocna skupině pro spolupráci při plnění jejích úkolů. Kromě toho směrnice požaduje, aby agentura ENISA pomáhala členským státům a Komisi poskytováním odborných rad a doporučení a usnadňováním výměny osvědčených postupů.

Komise v souladu s nařízením o agentuře ENISA vypracovala hodnocení agentury, které zahrnuje nezávislou studii, jakož i veřejnou konzultaci. V rámci hodnocení se posuzovaly význam, dopad, účinnost, efektivita, soudržnost a evropská přidaná hodnota agentury s ohledem na její výkon, řízení, vnitřní organizační strukturu a pracovní postupy v období 2013–2016.

---

9 Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, Úř. věst. L 77, 13.3.2004, s. 1.

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

Většina respondentů[11] (74 %) v rámci veřejné konzultace hodnotila celkový výkon agentury ENISA kladně. Většina respondentů se dále domnívala, že agentura ENISA dosahuje svých různých cílů (u každého z cílů alespoň 63 %). Služby a produkty agentury ENISA pravidelně (každý měsíc nebo častěji) používá téměř polovina respondentů (46 %) a oceňována je skutečnost, že jsou zajišťovány subjektem na úrovni EU (83 %) a jejich kvalita (62 %).

Velká většina respondentů (88 %) se však domnívala, že stávající nástroje a mechanismy dostupné na úrovni EU jsou pro řešení stávajících kybernetických bezpečnostních výzev nedostatečné nebo pouze částečně přiměřené. Převážná většina respondentů (98 %) uvedla, že by tyto potřeby měla řešit instituce EU, a 99 % z těchto respondentů se domnívalo, že by to měla být právě agentura ENISA. Kromě toho 67,5 % respondentů vyjádřilo názor, že ENISA by se mohla zapojit do vytváření harmonizovaného rámce pro certifikaci bezpečnosti produktů a služeb IT.

V rámci celkového hodnocení (vycházejícího nejen ze zmíněné veřejné konzultace, ale také z řady individuálních rozhovorů, dalších cílených průzkumů a seminářů) se dospělo k následujícím závěrům:

- Cíle agentury ENISA jsou stále aktuální. V kontextu rychlého technologického vývoje a nových hrozeb a s ohledem na rostoucí celosvětová kybernetická bezpečnostní rizika existuje v EU jasná potřeba podporovat a dále posilovat technické odborné znalosti na vysoké úrovni, co se týče otázek kybernetické bezpečnosti. V členských státech je třeba budovat kapacity pro rozpoznávání hrozeb a reagování na ně a zúčastněné strany musí spolupracovat napříč tematickými oblastmi a napříč institucemi.
- I přes svůj malý rozpočet je agentura při využívání svých zdrojů a provádění svých úkolů z provozního hlediska efektivní. Nicméně rozdělení umístění mezi Atény a Heraklion také způsobilo další administrativní náklady.
- Z hlediska účinnosti agentura ENISA částečně splnila své cíle. Agentura úspěšně přispěla ke zlepšení bezpečnosti sítí a informací v Evropě, a to tím, že zajistila budování kapacit ve 28 členských státech[12], posílila spolupráci mezi členskými státy a zúčastněnými stranami z oblasti bezpečností sítí a informací a zajistila odborné znalosti, budování komunit a podporu pro rozvoj politik. Celkově lze říci, že se agentura ENISA pečlivě soustředila na provádění svého pracovního programu, a ve vztahu ke svým zúčastněným stranám jednala jako důvěryhodný partner, a to v oblasti, jejíž tak silný přeshraniční význam byl uznán teprve nedávno.

---

11 V rámci konzultace odpovědělo 90 zúčastněných stran z 19 členských států (88 odpovědí a dvě stanoviska), včetně vnitrostátních orgánů z 15 členských států a 8 zastřešujících organizací zastupujících významný počet evropských podniků.

12 Respondenti ve veřejné konzultaci byli požádáni, aby se vyjádřili k tomu, co považují za hlavní úspěchy agentury ENISA v období 2013–2016. Respondenti ze všech skupin (celkem 55 respondentů, 13 ze skupiny vnitrostátních orgánů, 20 ze soukromého sektoru a 22 ze skupiny „ostatní“) považovali za hlavní úspěchy agentury ENISA následující: 1) koordinaci cvičení Cyber Europe; 2) poskytování podpory skupinám CERT/CSIRT prostřednictvím školení a seminářů podporujících spolupráci a výměnu zkušeností; 3) publikace agentury ENISA (pokyny a doporučení, zprávy o hrozbách, strategie pro hlášení incidentů a řešení krizí atd.), které byly považovány za užitečné pro vytváření a aktualizaci vnitrostátních bezpečnostních rámců a které tvůrci politik a odborníci v příslušné oblasti používali rovněž pro referenční účely; 4) pomoc při prosazování směrnice o bezpečnosti sítí a informací; 5) úsilí o zvýšení informovanosti ohledně kybernetické bezpečnosti prostřednictvím Měsíce kybernetické bezpečnosti.

- Agentuře ENISA se, alespoň do určité míry, podařilo ovlivnit rozsáhlou oblast bezpečnosti sítí a informací, nepodařilo se jí však plně uspět při budování silné značky a při získávání dostatečné viditelnosti, aby začala být uznávána jako „ono“ odborné středisko v Evropě. Vysvětlení této skutečnosti spočívá v širokém mandátu agentury ENISA, která nebyla vybavena úměrně dostatečnými prostředky. Kromě toho agentura ENISA zůstává jedinou agenturou EU s mandátem na dobu určitou, což omezuje její schopnost rozvíjet dlouhodobou vizi a udržitelným způsobem podporovat své zúčastněné strany. Je to rovněž v rozporu s ustanoveními směrnice o bezpečnosti sítí a informací, která agentuře ENISA svěřují úkoly, u nichž není stanoveno konečné datum. A konečně, na základě posouzení bylo zjištěno, že tuto omezenou účinnost lze částečně vysvětlit vysokou mírou spoléhání se na vnější odborné znalosti namísto interních odborných znalostí a obtížemi s najímáním specializovaných zaměstnanců a s jejich udržením.
- V neposlední řadě hodnocení dospělo k závěru, že přidaná hodnota agentury ENISA spočívá především ve schopnosti agentury posilovat spolupráci hlavně mezi členskými státy, a zvláště se spřízněnými komunitami v oblasti bezpečnosti sítí a informací (zejména mezi skupinami CSIRT). Na úrovni EU není žádný jiný subjekt, který podporuje tak široké spektrum zúčastněných stran z oblasti bezpečnosti sítí a informací. Vzhledem k tomu, že agentura ENISA musí přísně dbát na priority své činnosti, se její pracovní program řídí převážně potřebami členských států. V důsledku toho agentura dostatečně neřeší potřeby jiných zúčastněných stran, zejména průmyslu. Agentura také kvůli tomu reaguje v zájmu uspokojování potřeb svých klíčových zúčastněných stran, což jí brání v dosažení většího dopadu. Přidaná hodnota, již agentura poskytovala, se proto lišila v závislosti na rozdílných potřebách jejích zúčastněných stran a podle míry, do jaké byla agentura schopna na tyto potřeby reagovat (např. velké versus malé členské státy, členské státy versus průmysl).

Souhrnně lze říci, že výsledky konzultace se zúčastněnými stranami a hodnocení naznačují, že mandát a prostředky agentury ENISA je třeba upravit, aby mohla agentura hrát odpovídající úlohu při reagování na současné i budoucí problémy.

Tento návrh s ohledem na tato zjištění přezkoumává stávající mandát agentury ENISA a stanoví obnovený soubor úkolů a funkcí s cílem účinně a efektivně podporovat členské státy, orgány EU a další zúčastněné strany v jejich úsilí zajistit bezpečný kyberprostor v Evropské unii. Nový navrhovaný mandát se snaží udělit agentuře silnější a více ústřední úlohu, zejména tím, že rovněž podporuje členské státy při provádění směrnice o bezpečnosti sítí a informací a při aktivnějším čelení konkrétním hrozbám (operativní kapacita), a také tím, že se agentura stane odborným střediskem podporujícím členské státy a Komisi v otázkách certifikace kybernetické bezpečnosti. Podle tohoto návrhu:

- Agentuře ENISA by byl udělen trvalý mandát a agentura by tak do budoucna měla pevný základ. Mandát, cíle a úkoly by stále měly podléhat pravidelnému přezkumu.
- Navrhovaný mandát dále upřesňuje úlohu agentury ENISA jakožto agentury EU pro kybernetickou bezpečnost a jakožto referenčního místa v kybernetickobezpečnostním ekosystému EU, které úzce spolupracuje se všemi dalšími příslušnými subjekty v tomto ekosystému.
- Organizace a řízení agentury, které byly v průběhu hodnocení posouzeny kladně, by byly přezkoumány pouze mírně, zejména aby se zajistilo, že v práci agentury se lépe odrážejí potřeby širšího společenství zúčastněných stran.

- Navrhovaný rozsah mandátu je vymezen tak, aby posílil oblasti, kde se ukázala jasná přidaná hodnota agentury, a aby byly přidány nové oblasti, v nichž je nezbytná pomoc s ohledem na nové politické priority a nástroje, zejména na směrnici o bezpečnosti sítí a informací, na přezkum strategie kybernetické bezpečnosti Evropské unie a na nadcházející plán kybernetické bezpečnosti EU pro koordinaci v případě kybernetických krizí a pro certifikaci bezpečnosti IKT.

    - **Rozvoj a provádění politiky EU:** Agentura ENISA by byla pověřena, aby aktivně přispívala k rozvoji politiky v oblasti bezpečnosti sítí a informací, jakož i k dalším politickým iniciativám s prvky kybernetické bezpečnosti v různých odvětvích (např. energetika, doprava, finančnictví). Za tímto účelem by měla silnou poradní úlohu, kterou by mohla naplňovat poskytováním nezávislých stanovisek a přípravnými činnostmi pro rozvoj a aktualizaci politiky a právních předpisů. Agentura ENISA by rovněž podporovala politiku a právní předpisy EU v oblastech elektronických komunikací, elektronické identity a služeb vytvářejících důvěru, a to s cílem podporovat vyšší úroveň kybernetické bezpečnosti. Ve fázi provádění, zejména v kontextu skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, by agentura ENISA pomáhala členským státům dosahovat jednotného přístupu k provádění směrnice o bezpečnosti sítí a informací napříč hranicemi a odvětvími, jakož i v dalších oblastech příslušných politik a právních předpisů. S cílem podpořit pravidelný přezkum politik a právních předpisů v oblasti kybernetické bezpečnosti by agentura ENISA rovněž podávala pravidelné zprávy o stavu provádění právního rámce EU.

    - **Budování kapacit:** Agentura ENISA by přispívala ke zlepšení schopností a odborných znalostí orgánů EU a vnitrostátních veřejných orgánů členských států, včetně schopností a znalostí týkajících se reakcí na incidenty a dozoru nad regulačními opatřeními souvisejícími s kybernetickou bezpečností. Agentura by rovněž byla povinna přispět ke zřízení středisek pro analýzu a sdílení informací v různých odvětvích, a to tím, že by poskytovala osvědčené postupy a pokyny k dostupným nástrojům a postupům, jakož i tím, že by odpovídajícím způsobem řešila regulační otázky týkající se sdílení informací.

    - **Znalosti a informace, zvyšování informovanosti:** Agentura ENISA by se stala informačním centrem EU. To by znamenalo podporu a sdílení osvědčených postupů a iniciativ v celé EU prostřednictvím shromažďování informací o kybernetické bezpečnosti získaných od unijních a vnitrostátních orgánů, institucí a jiných subjektů. Agentura by rovněž zpřístupňovala poradenství, pokyny a osvědčené postupy týkající se bezpečnosti kritických infrastruktur. Po významných přeshraničních kybernetických bezpečnostních incidentech by agentura ENISA dále vypracovávala zprávy s cílem poskytnout pokyny podnikům a občanům v celé EU. Tato řada úkolů by rovněž zahrnovala pravidelné organizování činností na zvyšování informovanosti ve spolupráci s orgány členských států.

    - **Úkoly související s trhem (normalizace, certifikace kybernetické bezpečnosti):** agentura ENISA by vykonávala řadu funkcí, které by konkrétně podporovaly vnitřní trh a pokrývaly „sledování trhu“ kybernetické bezpečnosti, a to tak, že by analyzovala příslušné trendy na trhu kybernetické bezpečnosti, aby bylo možné lépe sladit nabídku a poptávku, a podporovala by rozvoj politiky EU v oblastech normalizace IKT a certifikace kybernetické

bezpečnosti IKT. Zejména, pokud jde o normalizaci, by agentura usnadňovala vytváření a zavádění norem kybernetické bezpečnosti. Agentura by rovněž prováděla úkoly předpokládané v souvislosti s budoucím rámcem pro certifikaci (viz oddíl níže).

- **Výzkum a inovace:** agentura ENISA by přispěla svými odbornými znalostmi tím, že by orgánům EU a vnitrostátním orgánům poskytovala poradenství ke stanovení priorit ve výzkumu a vývoji, a to i v kontextu smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost. Doporučení agentury ENISA v oblasti výzkumu by se v rámci příštího víceletého finančního rámce shromažďovala v novém evropském výzkumném a odborném středisku pro kybernetickou bezpečnost. Pokud by o to byla požádána Komisí, agentura ENISA by se rovněž účastnila provádění programů EU v oblasti financování výzkumu a inovací.
- **Operativní spolupráce a řešení krizí:** tato řada úkolů by měla vycházet z posílení stávajících preventivních operativních schopností, zejména z aktualizace celoevropských cvičení v oblasti kybernetické bezpečnosti (Cyber Europe) tak, že se budou konat každoročně, a z podpůrné role při operativní spolupráci jakožto sekretariát sítě CSIRT (podle ustanovení směrnice o bezpečnosti sítí a informací) tím, že agentura bude mimo jiné zajišťovat řádné fungování infrastruktury IT sítě CSIRT a jejích komunikačních kanálů. V této souvislosti by byla vyžadována strukturovaná spolupráce s CERT-EU, Evropským centrem pro boj proti kyberkriminalitě (EC3) a dalšími příslušnými subjekty EU. Kromě toho by strukturovaná spolupráce s CERT-EU, v těsné fyzické blízkosti, měla vést k funkci spočívající v poskytování technické pomoci v případě významných incidentů a v podpoře analýzy incidentu. Členským státům, které o to požádají, se dostane pomoci při řešení incidentů a podpory při analýze zranitelnosti, artefaktů a incidentů s cílem posílit jejich vlastní schopnosti, co se týče prevence a reakce.
- Agentura ENISA by rovněž hrála úlohu v **plánu kybernetické bezpečnosti EU** představeném jako součást tohoto balíčku a ve stanovování doporučení Komise určeného členským státům ohledně koordinované reakce na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty a krize na úrovni EU[13]. Agentura ENISA by usnadnila spolupráci mezi jednotlivými členskými státy při řešení reakcí na mimořádné události, a to tím, že by na základě informací, které agentuře na bázi dobrovolnosti poskytnou členské státy a jiné subjekty, analyzovala a agregovala vnitrostátní situační zprávy.

- **Certifikace kybernetické bezpečnosti produktů a služeb IKT**

Za účelem vytvoření a zachování důvěry a bezpečnosti musí být bezpečnostní prvky do produktů a služeb IKT začleněny přímo v raných fázích jejich technického designu a vývoje (bezpečnost coby aspekt návrhu). Zákazníci a uživatelé navíc musí být schopni zjistit úroveň záruk bezpečnosti produktů a služeb, které si pořídí nebo koupí.

[13] „Plán“ se bude vztahovat na kybernetické bezpečnostní incidenty, které způsobí narušení, jež je rozsáhlejší, než může jakýkoliv členský stát zvládnout sám, nebo které mají pro dva či více členských států tak rozsáhlý a významný dopad nebo politický význam, že vyžadují včasnou koordinaci politik a odpověď na politické úrovni Unie.

Certifikace, která spočívá ve formálním hodnocení produktů, služeb a procesů podle definovaného souboru kritérií a norem provedeném nezávislým a akreditovaným subjektem a ve vydání certifikátu o souladu, hraje důležitou úlohu při zvyšování důvěry v produkty a služby a jejich bezpečnosti. I když hodnocení bezpečnosti představuje relativně technickou oblast, certifikace slouží k tomu, aby kupující a uživatele informovala a ujistila je o bezpečnostních vlastnostech produktů a služeb IKT, které používají nebo si kupují. Jak je uvedeno výše, to platí zejména pro nové systémy, které velkou měrou využívají digitálních technologií a vyžadují vysokou úroveň bezpečnosti, jako jsou například propojené a automatizované automobily, elektronické zdravotnictví, průmyslové automatizační řídicí systémy (IACS)[14] nebo inteligentní sítě.

Prostředí certifikace kybernetické bezpečnosti produktů a služeb IKT v EU je v současné době poměrně nejednotné. Existuje řada mezinárodních iniciativ, jako například tzv. společná kritéria (CC) pro hodnocení bezpečnosti informačních technologií (norma ISO 15408), což je mezinárodní norma pro hodnocení počítačové bezpečnosti. Je založena na hodnocení třetí stranou a předpokládá sedm úrovní záruky hodnocení (Evaluation Assurancec Levels, EAL). Společná kritéria (CC) a doprovodná společná metodika pro hodnocení bezpečnosti informačních technologií (CEM) tvoří technický základ pro mezinárodní dohodu, dohodu o uznávání společných kritérií (Common Criteria Recognition Arrangement, CCRA), která zajišťuje, že certifikáty CC jsou uznávány všemi signatáři dohody CCRA. V rámci stávající verze dohody CCRA jsou však vzájemně uznávána pouze hodnocení do úrovně EAL 2. Dohodu navíc podepsalo pouze 13 členských států.

Certifikační orgány z 12 členských států uzavřely dohodu o vzájemném uznávání týkajícím se certifikátů vydaných v souladu s dohodou na základě společných kritérií[15]. Kromě toho v členských státech v současné době existuje nebo je zaváděna řada iniciativ týkajících se certifikace IKT. I když jsou tyto iniciativy důležité, obnáší riziko, že povedou k roztříštění trhu a k problémům s interoperabilitou. V důsledku toho se může stát, že aby společnost mohla nabízet svůj produkt na více trzích, musí podstoupit několik postupů certifikace v různých členských státech. Například výrobce inteligentních měřicích přístrojů, který chce své produkty prodávat ve třech členských státech, např. v Německu, ve Francii a ve Spojeném království, musí v současné době vyhovět třem různým systémům certifikace. Ve Spojeném království je to Commercial Product Assurance (CPA), ve Francii Certification de Sécurité de Premier Niveau (CSPN) a v Německu specifický profil ochrany založený na společných kritériích.

Tato situace vede k vyšším nákladům a pro společnosti působící v několika členských státech představuje značnou administrativní zátěž. Ačkoliv náklady na certifikaci se mohou významně lišit v závislosti na dotčeném produktu/službě, na úrovni záruky hodnocení, o kterou podnik usiluje, a/nebo v závislosti na komponentech, pro podniky jsou tyto náklady obecně značně vysoké. Například náklady na BSI certifikát pro ústřednu inteligentních měřicích přístrojů „Smart Meter Gateway“ jsou vyšší než 1 milion EUR (nejvyšší úroveň testování a záruky, která se netýká pouze jednoho výrobku, ale také celé související

---

14 GŘ SVS zveřejnilo zprávu, která navrhuje počáteční soubor společných evropských požadavků a hlavních směrů týkajících se certifikace kybernetické bezpečnosti složek IACS. Dostupné na internetových stránkách: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf.

15 Skupina vyšších úředníků pro bezpečnost informačních systémů (SOG-IS) zahrnuje 12 členských států plus Norsko a vypracovala několik profilů ochrany pro omezený počet produktů, jako jsou například digitální podpis, digitální tachograf a čipové karty. Účastníci spolupracují na koordinaci normalizace profilů ochrany CC a koordinují vypracování profilů ochrany. Členské státy při zadávání vnitrostátních veřejných zakázek často vyžadují certifikaci skupiny SOG-IS.

infrastruktury). Náklady na certifikaci inteligentních měřicích přístrojů ve Spojeném království představují téměř 150 000 EUR. Ve Francii jsou náklady podobné jako ve Spojeném království, tedy asi 150 000 EUR nebo více.

Klíčové zúčastněné strany z veřejného a soukromého sektoru uznaly, že neexistuje-li celoevropský systém certifikace kybernetické bezpečnosti, musí být společnosti v mnoha případech certifikovány jednotlivě v každém členském státě, což vede k roztříštěnosti trhu. Nejdůležitější je, že při neexistenci harmonizačních právních předpisů EU pro produkty a služby IKT mohou normy a postupy certifikace kybernetické bezpečnosti v členských státech v praxi v EU vytvářet 28 oddělených bezpečnostních trhů, každý se svými vlastními technickými požadavky, zkušebními metodami a postupy certifikace kybernetické bezpečnosti. Tyto rozdílné přístupy na vnitrostátní úrovni mohou způsobit – nebude-li na úrovni EU přijato žádné odpovídající opatření – zásadní nezdar při dosahování jednotného digitálního trhu, což zpomalí související pozitivní účinky, pokud jde o růst a pracovní místa, nebo zabrání jejich vzniku.

Navrhované nařízení na základě výše uvedeného vývoje zřizuje evropský rámec pro certifikaci kybernetické bezpečnosti (dále jen „**rámec**“) pro produkty a služby IKT a upřesňuje základní funkce a úkoly agentury ENISA v oblasti certifikace kybernetické bezpečnosti. Tento návrh stanoví celkový rámec pravidel upravujících systémy evropské certifikace kybernetické bezpečnosti. Návrh přímo nezavádí operativní systémy certifikace, ale vytváří systém (rámec) pro zavedení konkrétních systémů certifikace pro konkrétní produkty/služby IKT („evropské systémy certifikace kybernetické bezpečnosti“). Vytvoření evropských systémů certifikace kybernetické bezpečnosti v souladu s rámcem umožní, aby byly certifikáty vydané podle těchto systémů platné a uznávané ve všech členských státech, a umožní také řešení stávající roztříštěnosti trhu.

Obecným účelem evropských systémů certifikace kybernetické bezpečnosti je osvědčit, že produkty a služby IKT, které byly certifikovány v souladu s takovým systémem, splňují specifikované kybernetickobezpečnostní požadavky. To by zahrnovalo například schopnost ochránit údaje (ať už ukládané, předávané nebo jinak zpracovávané) proti náhodnému nebo neoprávněnému ukládání, zpracování, přístupu, sdělování, zničení, náhodné ztrátě nebo úpravám. Pokud jde o technické požadavky a hodnoticí postupy, které musí produkty splňovat, evropské systémy certifikace kybernetické bezpečnosti by využívaly stávající normy a technické normy by samy nevyvíjely[16]. Například celoevropská certifikace pro produkty jako čipové karty, které jsou v současné době testovány podle mezinárodních CC norem v rámci mnohostranného systému SOG-IS (jak již bylo popsáno), by znamenalo, že tento systém by byl platný v celé EU.

Návrh kromě toho, že uvádí specifický soubor bezpečnostních cílů, které je třeba zohlednit při navrhování konkrétního evropského systému certifikace kybernetické bezpečnosti, také stanoví, jaký by měl být minimální obsah takových systémů. Tyto systémy budou muset mimo jiné definovat řadu konkrétních prvků stanovujících rozsah a předmět certifikace kybernetické bezpečnosti. To zahrnuje identifikaci kategorie produktů a služeb spadajících do systému, podrobnou specifikaci kybernetickobezpečnostních požadavků (například prostřednictvím odkazu na příslušnou normu nebo technickou specifikaci), konkrétní kritéria a metody hodnocení a úroveň záruky, kterou chtějí zajistit (tj. základní, významnou nebo vysokou).

[16] V případě evropských norem k tomu dochází prostřednictvím evropských normalizačních organizací a schválením Evropskou komisí zveřejněním v *Úředním věstníku* (viz nařízení 1025/2012).

Evropské systémy certifikace kybernetické bezpečnosti vypracuje ENISA v úzké spolupráci s Evropskou skupinou pro certifikaci kybernetické bezpečnosti (viz níže), která jí bude poskytovat pomoc a odborná doporučení, a přijímat je bude Komise prostřednictvím prováděcích aktů. Bude-li zjištěna potřeba systému certifikace kybernetické bezpečnosti, Komise agenturu ENISA požádá, aby vypracovala systém pro konkrétní produkty nebo služby IKT. Agentura ENISA bude na systému pracovat v úzké spolupráci s vnitrostátními orgány dozoru nad certifikací zastoupenými ve skupině. Členské státy a skupina mohou Komisi navrhnout, aby agenturu ENISA požádala o vypracování konkrétního systému.

Certifikace může představovat velmi nákladný proces, což by pak mohlo vést k vyšším cenám pro zákazníky a spotřebitele. Potřeba certifikace se rovněž může významně lišit podle konkrétního kontextu využití produktů a služeb a rychlého tempa technologické změny. Využití evropské certifikace kybernetické bezpečnosti by proto mělo zůstat dobrovolné, nestanoví-li jinak právní předpisy Unie, které stanoví bezpečnostní požadavky produktů a služeb IKT.

Aby byla zajištěna harmonizace a zabránilo se roztříštěnosti, přestanou vnitrostátní systémy nebo postupy certifikace kybernetické bezpečnosti produktů a služeb IKT, na které se vztahuje evropský systém certifikace kybernetické bezpečnosti, platit ode dne stanoveného v prováděcím aktu, jímž se daný systém přijímá. Členské státy by dále neměly zavádět nové vnitrostátní systémy certifikace kybernetické bezpečnosti pro produkty a služby IKT zahrnuté do určitého systému evropské certifikace kybernetické bezpečnosti.

Jakmile bude určitý evropský systém certifikace kybernetické bezpečnosti přijat, výrobci produktů IKT nebo poskytovatelé služeb IKT budou moci subjektu posuzování shody podle své volby předložit žádost o certifikaci svých produktů nebo služeb. Subjekty posuzování shody by měly být akreditovány akreditačním orgánem, splňují-li určité konkrétní požadavky. Akreditace se bude vydávat na období nejvýše pěti let a lze ji obnovit za stejných podmínek, pokud daný subjekt posuzování shody splňuje příslušné požadavky. Akreditační orgány zruší akreditaci subjektu posuzování shody, pokud podmínky pro akreditaci nejsou nebo přestanou být splňovány, nebo pokud opatření přijatá subjektem posuzování shody porušují toto nařízení.

Podle uvedeného návrhu úkoly související se sledováním, dozorem a vymáháním přísluší členským státům. Členské státy budou muset stanovit jeden orgán dozoru nad certifikací. Tento orgán bude pověřen dozorem nad tím, zda subjekty posuzování shody, jakož i certifikáty vydané subjekty posuzování shody usazenými na území příslušného členského státu, dodržují požadavky tohoto nařízení a příslušných evropských systémů certifikace kybernetické bezpečnosti. Vnitrostátní orgány dozoru nad certifikací budou příslušné k řešení stížností podaných fyzickými nebo právnickými osobami v souvislosti s certifikáty vydanými subjekty posuzování shody usazenými na jejich území. V přiměřeném rozsahu budou šetřit předmět stížnosti a v přiměřené lhůtě budou informovat stěžovatele o pokroku a výsledku šetření. Kromě toho budou spolupracovat s dalšími orgány dozoru nad certifikací nebo jinými veřejnými orgány, například prostřednictvím sdílení informací o možných případech, kdy produkty a služby IKT nevyhovují požadavkům tohoto nařízení, nebo kdy nejsou v souladu s konkrétními evropskými systémy certifikace kybernetické bezpečnosti.

A konečně návrh zřizuje Evropskou skupinu pro certifikaci kybernetické bezpečnosti (dále jen „skupina“), sestávající z vnitrostátních orgánů dozoru nad certifikací všech členských států. Hlavním úkolem skupiny je poskytovat Komisi poradenství v otázkách týkajících se politiky v oblasti certifikace kybernetické bezpečnosti a pracovat s agenturou ENISA na vypracování návrhu evropských systémů certifikace kybernetické bezpečnosti. Agentura ENISA bude napomáhat Komisi při zajišťování služeb sekretariátu skupiny a vést aktualizovaný veřejný

seznam systémů schválených podle evropského rámce pro certifikaci kybernetické bezpečnosti. Agentura ENISA by rovněž spolupracovala s normalizačními orgány, a to za účelem zajištění vhodnosti norem použitých ve schválených systémech a za účelem určení oblastí, kde jsou zapotřebí normy kybernetické bezpečnosti.

Evropský rámec pro certifikaci kybernetické bezpečnosti („rámec“) poskytne občanům a podnikům několik výhod. Zejména:

- Vytvoření celoevropských systémů certifikace kybernetické bezpečnosti pro konkrétní produkty nebo služby společnostem poskytne jednotné místo („one-stop-shop“) pro certifikaci kybernetické bezpečnosti v EU. Tyto společnosti budou moci certifikovat své produkty pouze jednou a získat certifikát platný ve všech členských státech. Nebudou mít povinnosti své produkty znovu certifikovat u různých vnitrostátních certifikačních subjektů. Tím se společnostem významně sníží náklady, usnadní se tím přeshraniční operace a v konečném důsledku se tím sníží roztříštěnost vnitřního trhu pro dotčené výrobky a bude se jí předcházet.
- Rámec stanoví, že evropské systémy certifikace kybernetické bezpečnosti jsou nadřazeny vnitrostátním systémům: podle tohoto pravidla přijetí evropského systému certifikace kybernetické bezpečnosti nahradí všechny stávající paralelní vnitrostátní systémy pro stejné produkty nebo služby IKT na dané úrovni záruky. To celou situaci dále vyjasní a omezí se stávající šíření překrývajících se a případně protichůdných vnitrostátních systémů certifikace kybernetické bezpečnosti.
- Návrh podporuje a doplňuje provádění směrnice o bezpečnosti sítí a informací, a to tím, že podnikům, na něž se směrnice vztahuje, poskytuje velmi užitečný nástroj pro prokázání souladu s požadavky týkajícími se bezpečnosti sítí a informací v celé Unii. Komise a agentura ENISA budou při vývoji nových systémů certifikace kybernetické bezpečnosti věnovat zvláštní pozornost nutnosti zajistit, aby požadavky týkající se bezpečnosti sítí a informací byly v systémech certifikace kybernetické bezpečnosti zohledněny.
- Návrh podpoří a usnadní rozvoj evropské politiky v oblasti kybernetické bezpečnosti, a to tím, že harmonizuje podmínky a hlavní požadavky pro certifikaci kybernetické bezpečnosti produktů a služeb IKT v EU. Evropské systémy certifikace kybernetické bezpečnosti budou odkazovat na společné normy nebo kritéria hodnocení a zkušební metody. To významně, i když nepřímo, přispěje k zavádění společných bezpečnostních řešení v EU, čímž rovněž dojde k odstranění překážek vnitřního trhu.
- Rámec je navržen takovým způsobem, aby zajistil nezbytnou flexibilitu systémů certifikace kybernetické bezpečnosti. V závislosti na konkrétních kybernetickobezpečnostních potřebách může být produkt nebo služba certifikována na vyšší nebo nižší úroveň bezpečnosti. Evropské systémy certifikace kybernetické bezpečnosti budou navrženy s ohledem na tuto flexibilitu, a budou proto poskytovat různé úrovně záruk (tj. základní, významnou nebo vysokou), aby mohly být použity pro různé účely nebo v různých kontextech.
- Díky všem výše uvedeným prvkům bude certifikace kybernetické bezpečnosti pro podniky atraktivnější jako účinný prostředek pro sdělování úrovně záruky kybernetické bezpečnosti produktů a služeb IKT. Pokud bude certifikace kybernetické bezpečnosti méně nákladná, účinnější a komerčně přitažlivější, budou mít podniky větší motivaci své produkty certifikovat z hlediska rizik kybernetické bezpečnosti, čímž přispějí k šíření lepších kybernetickobezpečnostních postupů při navrhování produktů a služeb IKT (kybernetická bezpečnost coby aspekt návrhu).

- **Soulad s platnými předpisy v této oblasti politiky**

Podle směrnice o bezpečnosti sítí a informací jsou provozovatelé působící v odvětvích zásadních pro naše hospodářství a společnost, jako například energetika, doprava, vodohospodářství, bankovnictví, infrastruktura finančního trhu, zdravotní péče a digitální infrastruktura, jakož i poskytovatelé digitálních služeb (tj. internetové vyhledávače, služby cloud computingu a on-line tržiště) povinni přijmout opatření k odpovídajícímu zvládnutí bezpečnostních rizik. Nová pravidla tohoto návrhu doplňují ustanovení směrnice o bezpečnosti sítí a informací a zajišťují s nimi soulad, aby se prostřednictvím zlepšení schopností, spolupráce, řízení rizik a informování o počítačových útocích ještě více posílila kybernetická odolnost EU.

Pravidla týkající se certifikace kybernetické bezpečnosti navíc poskytují základní nástroj pro společnosti, na něž se vztahuje směrnice o bezpečnosti sítí a informací, jelikož tyto společnosti budou schopny své produkty a služby IKT certifikovat z hlediska rizik kybernetické bezpečnosti, a to na základě systémů certifikace kybernetické bezpečnosti platných a uznávaných v celé Evropské unii. Budou rovněž doplňovat bezpečnostní požadavky uvedené v nařízení eIDAS[17] a ve směrnici o rádiových zařízeních[18].

- **Soulad s ostatními politikami Unie**

Nařízení (EU) 2016/679 („obecné nařízení o ochraně osobních údajů“)[19] obsahuje ustanovení týkající se zavedení mechanismů pro vydávání osvědčení a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s tímto nařízením v případě operací zpracování prováděných správci a zpracovateli. Tímto nařízením není dotčena certifikace operací zpracování údajů podle obecného nařízení o ochraně osobních údajů, včetně situací, kdy jsou tyto operace zabudované v produktech a službách.

Navrhované nařízení zajistí soulad s nařízením 765/2008 o akreditaci a požadavcích na dozor nad trhem[20], a to odkazem na pravidla tohoto rámce týkající se vnitrostátních akreditačních orgánů a subjektů posuzování shody. Co se týče orgánů dozoru, navrhované nařízení bude vyžadovat, aby členské státy určily vnitrostátní orgány dozoru nad certifikací odpovědné za dozor nad dodržováním pravidel a za sledování a vymáhání dodržování pravidel. Tyto orgány zůstanou oddělené od subjektů posuzování shody předepsaných nařízením 765/2008.

---

17 Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

18 Směrnice Evropského parlamentu a Rady 2014/53/EU ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/ES.

19 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1–88).

20 Nařízení (ES) č. 765/2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- **Právní základ**

Právním základem pro opatření EU je článek 114 Smlouvy o fungování Evropské unie (SFEU), který se zabývá sbližováním právních předpisů členských států za účelem dosažení cílů stanovených v článku 26 SFEU, konkrétně řádného fungování vnitřního trhu.

Právní základ pro zřízení agentury ENISA týkající se vnitřního trhu byl potvrzen Soudním dvorem Evropské unie (ve věci C-217/04 *Spojené království v. Evropský parlament a Rada*) a dále potvrzen nařízením z roku 2013, které stanoví stávající mandát agentury. Kromě toho činnosti, které by odrážely cíle v podobě zvýšení spolupráce a koordinace mezi členskými státy, a cíle, které by přispěly k úrovni schopností EU doplňovat opatření členských států, by spadaly do kategorie „operativní spolupráce“. Toto je ve směrnici o bezpečnosti sítí a informací (jejímž právním základem je článek 114 SFEU) konkrétně uvedeno jako cíl, který by měl být sledován v souvislosti se sítí CSIRT, přičemž „agentura ENISA zajistí služby sekretariátu a aktivně podporuje spolupráci“ (čl. 12 odst. 2). Především čl. 12 odst. 3 písm. f) jako úkol pro síť CSIRT dále uvádí vymezení dalších forem operativní spolupráce, a to mimo jiné ve vztahu: i) ke kategoriím rizik a incidentů, ii) k včasným varováním, iii) k vzájemné pomoci, a iv) k zásadám a způsobům koordinace členských států při reakci na přeshraniční rizika a incidenty.

- Stávající roztříštěnost systémů certifikace pro produkty a služby IKT je rovněž výsledkem nedostatečného společného právně závazného a účinného rámcového procesu použitelného na členské státy. To brání vytvoření vnitřního trhu s produkty a službami IKT a brzdí konkurenceschopnost evropského průmyslu v tomto odvětví. Cílem tohoto návrhu je řešit stávající roztříštěnost a související překážky na vnitřním trhu, a to poskytnutím společného rámce pro zavedení systémů certifikace kybernetické bezpečnosti platných v celé EU.

Subsidiarita (v případě nevýlučné pravomoci)

Zásada subsidiarity vyžaduje posouzení nezbytnosti a přidané hodnoty opatření na úrovni EU. Dodržování zásady subsidiarity v této oblasti bylo uznáno již při přijímání stávajícího nařízení o agentuře ENISA[21].

Kybernetická bezpečnost je otázkou společného zájmu Unie. Vzájemné závislosti mezi sítěmi a informačními systémy jsou takové, že jednotlivé subjekty (veřejné a soukromé, včetně občanů) často nemohou samostatně čelit hrozbám a řídit rizika a možné dopady kybernetických incidentů. Na jedné straně vzhledem k vzájemné závislosti napříč členskými státy, včetně vzájemné závislosti týkající se provozu kritických infrastruktur (energetika, doprava, vodohospodářství, abychom vyjmenovali alespoň některé), je veřejná intervence na evropské úrovni nejen přínosná, ale také potřebná. Na druhé straně intervence EU může díky sdílení osvědčených postupů napříč členskými státy přinést pozitivní „přelévající se“ účinek, který může vést ke zvýšení kybernetické bezpečnosti Unie.

Souhrnně lze říci, že v současném kontextu a s ohledem na budoucí scénáře se zdá, že pro **zvýšení společné kybernetické odolnosti** Unie nebudou **individuální opatření členských států EU a roztříštěný přístup ke kybernetické bezpečnosti** dostatečná.

[21] Nařízení Evropského parlamentu a Rady (EU) č. 526/2013 ze dne 21. května 2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004.

Opatření na úrovni EU je rovněž považováno za nezbytné pro řešení roztříštěnosti stávajících systémů certifikace kybernetické bezpečnosti. Výrobcům by to umožnilo plně využívat výhod vnitřního trhu, přičemž by došlo ke značným úsporám nákladů na testování a konstrukční změny. I když například stávající dohoda o vzájemném uznávání skupiny vyšších úředníků – bezpečnost informačních systémů (SOG-IS) dosáhla v tomto ohledu důležitých výsledků, rovněž ukázala významná omezení, která brání tomu, aby byla vhodná pro poskytování dlouhodobějších udržitelných řešení při využívání plného potenciálu vnitřního trhu.

Přidaná hodnota opatření na úrovni EU, zejména opatření ke zvýšení spolupráce mezi členskými státy, ale také mezi společenstvími zabývajícími se bezpečností sítí a informací, byla uznána v závěrech Rady z roku 2016[22], a rovněž jasně vyplývá z hodnocení agentury ENISA.

- **Proporcionalita**

Navrhovaná opatření nepřekračují rámec toho, co je nezbytné k dosažení jejich cílů politiky. Kromě toho rozsah intervence EU nebrání přijímání dalších vnitrostátních opatření v oblasti národní bezpečnosti. Na základě subsidiarity a proporcionality je proto opatření na úrovni EU odůvodněné.

- **Volba nástroje**

Tento návrh přezkoumává nařízení (EU) č. 526/2013, které stanoví stávající mandát a úkoly agentury ENISA. Kromě toho vzhledem k důležité úloze agentury ENISA při zřizování a řízení rámce EU pro certifikaci kybernetické bezpečnosti bude nejlepší, aby byly nový mandát agentury ENISA a uvedený rámec zavedeny podle jednoho právního nástroje za použití nástroje v podobě nařízení.

3. VÝSLEDKY HODNOCENÍ EX POST, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

Hodnocení *ex post* / kontroly účelnosti platných právních předpisů

Komise v souladu s plánem hodnocení[23] posuzovala **význam, dopad, účinnost, efektivitu, soudržnost a přidanou hodnotu** agentury s ohledem na její výkon, řízení, vnitřní organizační strukturu a pracovní postupy v období 2013–2016. Hlavní zjištění lze shrnout takto (více informací viz pracovní dokument útvarů Komise na toto téma, který je připojen k posouzení dopadů).

- **Význam:** V kontextu technologického rozvoje a vyvíjejících se hrozeb a s ohledem na značnou potřebu zvýšit kybernetickou bezpečnost v EU se ukázalo, že cíle agentury ENISA mají význam. Členské státy a subjekty EU spoléhají na její značné odborné znalosti týkající se otázek kybernetické bezpečnosti. Kromě toho je v členských státech třeba vybudovat kapacity pro lepší pochopení hrozeb a reagování na ně a zúčastněné strany musí spolupracovat napříč tematickými oblastmi a napříč institucemi. Kybernetická bezpečnost je nadále klíčovou politickou prioritou EU a očekává se, že agentura ENISA na ni odpoví; podoba agentury ENISA jakožto

[22] Závěry Rady o posílení evropského systému kybernetické odolnosti a o podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti – 15. listopadu 2016.

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

agentury EU s mandátem na určitou dobu však: i) neumožňuje dlouhodobé plánování a udržitelnou podporu členských států a orgánů EU; ii) může vést k právnímu vakuu, jelikož ustanovení směrnice o bezpečnosti sítí a informací pověřující agenturu ENISA úkoly jsou trvalé povahy[24]; iii) není soudržná s vizí, která agenturu ENISA spojuje s posíleným kybernetickobezpečnostním ekosystémem EU.

- **Účinnost:** Agentura ENISA celkově splnila své cíle a provedla své úkoly. Prostřednictvím svých hlavních činností (budování kapacit, poskytování odborných znalostí, budování společenství a podpora politiky) přispěla k posílení bezpečnosti sítí a informací v Evropě. Ve vztahu ke každé z těchto činností však ukázala potenciál ke zlepšení. Hodnocení dospělo k závěru, že agentura ENISA účinně vytvořila silné a důvěrné vztahy s některými ze svých zúčastněných stran, zejména s členskými státy a společenstvím CSIRT. Intervence v oblasti budování kapacit byly vnímány jako účinné zejména v případě členských států s menšími prostředky. Jedním z nejvíce zdůrazňovaných bodů byla stimulace široké spolupráce, přičemž zúčastněné strany se široce shodly na pozitivní úloze, kterou agentura ENISA hraje při spojování lidí. Agentura ENISA však čelila potížím, když se pokoušela mít velký dopad na rozsáhlou oblast bezpečnosti sítí a informací. To bylo rovněž způsobeno skutečností, že pro splnění velmi širokého mandátu měla dosti omezené lidské a finanční zdroje. Hodnocení rovněž dospělo k závěru, že agentura ENISA částečně splnila cíl poskytování odborných poznatků, což souviselo s problémy s najímáním odborníků (viz také níže v oddíle týkajícím se efektivity).
- **Efektivita:** I přes svůj malý rozpočet – ve srovnání s jinými agenturami EU patří k nejnižším – byla agentura ENISA schopna přispět ke sledovaným cílům, což ukazuje celkovou efektivitu při využívání jejích zdrojů. Hodnocení dospělo k závěru, že procesy byly obecně efektivní, a jasné vymezení odpovědností v rámci organizace vedlo k dobrému vykonávání práce. Jeden z hlavních problémů týkajících se efektivity agentury souvisí s obtížemi agentury ENISA s najímáním a udržením vysoce kvalifikovaných odborníků. Zjištění ukazují, že tuto skutečnost lze vysvětlit kombinací faktorů, včetně obecných obtíží veřejného sektoru konkurovat soukromému sektoru ve snaze najmout vysoce specializované odborníky, druhu smluv (na dobu určitou), které mohla agentura většinou nabízet, a poněkud nižší úrovně atraktivity související s umístěním agentury ENISA, které souvisela například s obtížemi manželů či manželek při hledání práce. Rozdělení umístění mezi Atény a Heraklion vyžadovalo další úsilí při koordinaci a vedlo k dalším nákladům, ale přesun oddělení hlavních činností do Atén v roce 2013 provozní účinnost agentury zvýšil.
- **Soudržnost:** Činnosti agentury ENISA byly obecně v souladu s politikami a činnostmi jejích zúčastněných stran, a to na vnitrostátní úrovni i na úrovni EU, je však třeba koordinovanějšího přístupu ke kybernetické bezpečnosti na úrovni EU. Potenciál pro spolupráci mezi agenturou ENISA a subjekty EU nebyl plně využit. Vzhledem k vývoji právního a politického prostředí v EU je dnes stávající mandát méně soudržný.
- **Přidaná hodnota na úrovni EU**: Přidaná hodnota agentury ENISA spočívá především ve schopnosti agentury zvyšovat spolupráci, a to zejména mezi členskými státy, ale také se souvisejícími společenstvími zabývajícími se bezpečností sítí a

[24] Odkaz na články 7, 9, 11, 12 a 19 směrnice o bezpečnosti sítí a informačních systémů (směrnice o bezpečnosti sítí a informací).

informací. Na úrovni EU není žádný jiný subjekt, který podporuje spolupráci stejné škály zúčastněných stran zabývajících se bezpečností sítí a informací. Přidaná hodnota poskytovaná agenturou se lišila podle rozdílných potřeb a zdrojů zúčastněných stran (např. velké versus malé členské státy, členské státy versus odvětví) a podle nutnosti, aby agentura stanovovala priority svých činností podle pracovního programu. Hodnocení dospělo k závěru, že potenciální přerušení činnosti agentury ENISA by pro všechny členské státy bylo promarněnou příležitostí. V oblasti kybernetické bezpečnosti nebude možné zajistit stejnou úroveň budování společenství a spolupráce napříč členskými státy. Bez centralizovanější agentury EU by byl obrázek roztříštěnější a prázdné místo zanechané agenturou ENISA by bylo vyplněno dvoustrannou nebo regionální spoluprací.

Se zvláštním ohledem na dřívější výsledky a budoucnost agentury ENISA jsou hlavní trendy vyplývající z konzultace v roce 2017 tyto[25]:

- Většina respondentů (74 %) hodnotila celkový výkon agentury ENISA v období 2013 až 2016 kladně. Většina respondentů se dále domnívala, že agentura ENISA dosahuje svých různých cílů (u každého z cílů alespoň 63 %). Služby a produkty agentury ENISA jsou pravidelně (každý měsíc nebo častěji) používány téměř polovinou respondentů (46 %) a jsou oceňovány za skutečnost, že pocházejí ze subjektu na úrovni EU (83 %) a za svou kvalitu (62 %).
- Respondenti z hlediska budoucnosti kybernetické bezpečnosti v EU identifikovali řadu nedostatků a problémů, přičemž k pěti nejčastějším (ze seznamu 16) patřilo zejména: spolupráce napříč členskými státy, kapacita předcházet rozsáhlým kybernetickým útokům, odhalovat je a řešit je, spolupráce napříč členskými státy v záležitostech týkajících se kybernetické bezpečnosti, spolupráce a sdílení informací mezi různými zúčastněnými stranami včetně spolupráce veřejného a soukromého sektoru, ochrana kritické infrastruktury před kybernetickými útoky.
- Velká většina respondentů (88 %) se domnívala, že stávající nástroje a mechanismy dostupné na úrovni EU jsou pro řešení těchto nedostatků a problémů nedostatečné nebo pouze částečně přiměřené. Převážná většina respondentů (98 %) uvedla, že by na tyto potřeby měla reagovat instituce EU, a podle 99 % z těchto respondentů by to měla být právě ENISA.

Konzultace se zúčastněnými stranami

- Komise zorganizovala veřejnou konzultaci o přezkumu agentury ENISA, která probíhala od 12. dubna do 5. července 2016, a obdržela 421 odpovědí[26]. Podle

[25] V rámci konzultace odpovědělo 90 zúčastněných stran z 19 členských států (88 odpovědí a 2 dvě stanoviska), a to včetně vnitrostátních orgánů z 15 členských států včetně Francie, Itálie, Irska a Řecka a 8 zastřešujících organizací zastupujících významný počet evropských podniků, například Evropská bankovní federace, organizace Digital Europe (zastupující odvětví digitální technologie v Evropě) a Sdružení evropských provozovatelů telekomunikačních sítí (ETNO). Veřejná konzultace týkající se agentury ENISA byla doplněna několika dalšími zdroji, včetně: i) podrobných rozhovorů s přibližně 50 klíčovými aktéry z oblasti kybernetické bezpečnosti; ii) průzkumu zaměřeného na síť CSIRT; iii) průzkumu zaměřeného na správní radu, výkonnou radu a stálou skupinu zúčastněných stran agentury ENISA.

[26] 162 příspěvků od občanů, 33 od organizací občanské společnosti a spotřebitelských organizací, 186 od průmyslu a 40 od veřejných orgánů, včetně orgánů příslušných pro vymáhání směrnice o soukromí a elektronických komunikacích.

výsledků konzultace 67,5 % respondentů vyjádřilo názor, že agentura ENISA by mohla hrát úlohu při zavádění harmonizovaného rámce pro certifikaci bezpečnosti produktů a služeb IT.

Výsledky konzultace z roku 2016 o partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost[27], pokud jde o oddíl týkající se certifikace, ukazují, že:

- 50,4 % (tj. 121 z 240) respondentů neví, zda jsou vnitrostátní systémy certifikace v členských státech EU vzájemně uznávány. 25,8 % (62 z 240) odpovědělo „Ne“, zatímco 23,8 % (57 z 240) odpovědělo „Ano“.
- 37,9 % respondentů (91 z 240) si myslí, že stávající systémy certifikace nezajišťují potřeby evropského průmyslu. Na druhou stranu 17,5 % (42 z 240) – zejména globální společnosti působící na evropském trhu – bylo opačného názoru.
- 49,6 % (119 z 240) respondentů uvádí, že není snadné prokázat rovnocennost norem, systémů certifikace a označení. 37,9 % (91 z 240) odpovědělo „Nevím“, zatímco pouze 12,5 % (30 z 240) odpovědělo „Ano“.

Sběr a využití výsledků odborných konzultací

Komise zohlednila následující doporučení externích odborníků:

- studie týkající se hodnocení agentury ENISA (Study on the Evaluation of ENISA (Ramboll/Carsa 2017; zpráva SMART č. 2016/0077)),
- Studie týkající se certifikace a označování bezpečnosti IKT – Shromáždění údajů a posouzení dopadů (PriceWaterhouseCoopers 2017; zpráva SMART č. 2016/0029)).

Posouzení dopadů

- Zpráva o posouzení dopadů týkající se této iniciativy zjistila tyto hlavní problémy, které je třeba řešit:
- roztříštěnost politik a přístupů ke kybernetické bezpečnosti napříč členskými státy,
- rozptýlené zdroje a roztříštěnost přístupů ke kybernetické bezpečnosti napříč orgány, institucemi a jinými subjekty EU, a
- nedostatečné povědomí a informovanost občanů a společností ve spojení se skutečností, že vzniká stále více různých vnitrostátních a odvětvových systémů certifikace.

Pokud jde o mandát agentury ENISA, zpráva posuzovala tyto možnosti:

- zachovat *status quo*, což by znamenalo rozšířený mandát, který by byl stále časově omezený (základní možnost),
- vypršení stávajícího mandátu agentury ENISA, aniž by došlo k obnovení nebo ukončení činnosti agentury ENISA (žádný politický zásah),
- „reforma agentury ENISA“, a

[27] Na oddíl o certifikaci odpovědělo 240 zúčastněných stran z vnitrostátních veřejných správ, velkých podniků, malých a středních podniků, mikropodniků a výzkumných organizací.

- agentura EU pro kybernetickou bezpečnost s plnými operativními schopnostmi.

Pokud jde o certifikaci kybernetické bezpečnosti, zpráva posuzovala tyto možnosti:

- žádný politický zásah (základní možnost),
- nelegislativní opatření („měkké právo“),
- legislativní akt EU, kterým by došlo k vytvoření povinného systému pro všechny členské státy založeného na systému SOG-IS, a
- obecný rámec EU pro certifikaci kybernetické bezpečnosti IKT.

Analýza vedla k závěru, že upřednostňovanou možností je „reforma agentury ENISA“ ve spojení s obecným rámcem EU pro certifikaci kybernetické bezpečnosti IKT.

Upřednostňovaná možnost byla vyhodnocena jako nejefektivnější způsob, jímž má EU dosáhnout stanovených cílů, a sice: zlepšení schopností, připravenosti, spolupráce, informovanosti a transparentnosti v oblasti kybernetické bezpečnosti a zamezení roztříštěnosti trhu. Rovněž byla vyhodnocena jako nejlépe odpovídající politickým prioritám strategie EU v oblasti kybernetické bezpečnosti a souvisejících politik (např. směrnice o bezpečnosti sítí a informací) a strategie pro jednotný digitální trh. Z provedených konzultací nadto vyplynulo, že upřednostňovaná možnost má podporu většiny zúčastněných stran. Kromě toho analýza provedená v rámci posouzení dopadů ukázala, že upřednostňovaná možnost by vedla k dosažení cílů s přiměřeným využitím zdrojů.

Výbor Komise pro kontrolu regulace nejprve vydal dne 24. července záporné stanovisko, a po novém předložení vydal dne 25. srpna 2017 stanovisko kladné. Upravená zpráva o posouzení dopadů obsahovala dodatečné podpůrné údaje, konečné závěry hodnocení agentury ENISA a další vysvětlení možností politiky a jejich dopadů. Příloha 1 závěrečné zprávy o posouzení dopadů shrnuje, jak byly připomínky výboru ve druhém stanovisku zohledněny. Zpráva byla zejména aktualizována tak, že podrobněji popisuje situaci v oblasti kybernetické bezpečnosti v EU, včetně opatření, která jsou uvedena ve společném sdělení „Odolnost, odrazující opatření a obrana – Budování robustní kybernetické bezpečnosti v EU“, (JOIN(2017) 450) a která jsou zvláště relevantní pro agenturu ENISA: plán EU v oblasti kybernetické bezpečnosti a evropské výzkumné a odborné středisko pro kybernetickou bezpečnost, jemuž by agentura směřovala svá doporučení ohledně výzkumných potřeb EU.

Ve zprávě se vysvětluje, jak by reforma agentury, včetně nových úkolů, lepších podmínek pro zaměstnance a strukturální spolupráce s institucemi EU v dané oblasti, zlepšila její atraktivitu jako zaměstnavatele a pomohla řešit problémy spojené s náborem odborníků. Příloha 6 zprávy rovněž obsahuje přepracovaný odhad nákladů spojených s možnostmi politiky, co se týče agentury ENISA. Pokud jde o téma certifikace, zpráva byla přepracována tak, aby poskytovala podrobnější vysvětlení upřednostňované možnosti, včetně grafického znázornění, a rovněž odhady nákladů, jež v souvislosti s novým rámcem certifikace vzniknou členským státům a Komisi. Důvody volby agentury ENISA jako klíčového aktéra v tomto rámci byly dále vysvětleny na základě její odbornosti v dané oblasti a skutečnosti, že se jedná o jedinou agenturu působící v oblasti kybernetické bezpečnosti na úrovni EU. Oddíly týkající se certifikace byly rovněž přepracovány tak, aby objasňovaly aspekty spojené s odlišnostmi stávajícího systému skupiny SOG-IS a výhody spojené s uvedenými možnostmi politiky a aby upřesnily, že typy produktů a služeb IKT, na něž se bude vztahovat určitý evropský systém certifikace, budou vymezeny přímo v daném schváleném systému.

Účelnost a zjednodušování právních předpisů

Nevztahuje se na tento návrh.

Dopad na základní práva

Kybernetická bezpečnost hraje zásadní úlohu při ochraně soukromí a osobních údajů jednotlivců v souladu s články 7 a 8 Listiny základních práv Evropské unie. V případě počítačových bezpečnostních událostí jsou soukromí a ochrana našich osobních údajů jasně ohroženy. Kybernetická bezpečnost je tedy nezbytnou podmínkou pro ochranu soukromí a důvěrnosti našich osobních údajů. Z tohoto hlediska návrh tím, že usiluje o posílení kybernetické bezpečnosti v Evropě, poskytuje důležitý doplněk stávajících právních předpisů chránících základní právo na soukromí a osobní údaje. Kybernetická bezpečnost je rovněž důležitá pro ochranu důvěrného charakteru našich elektronických komunikací, a tím i pro uplatňování práva na svobodu projevu a informací a dalších souvisejících práv, jako například svobody myšlení, svědomí a náboženského vyznání.

4. ROZPOČTOVÉ DŮSLEDKY

Viz finanční výkaz.

5. OSTATNÍ PRVKY

- **Plány provádění a monitorování, hodnocení a podávání zpráv**

Komise bude monitorovat uplatňování nařízení a každých pět let Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru předloží zprávu o svém hodnocení. Tyto zprávy budou veřejné a budou uvádět podrobné informace týkající se účinného uplatňování a vymáhání tohoto nařízení.

- **Podrobné vysvětlení konkrétních ustanovení návrhu**

Hlava I nařízení obsahuje obecná ustanovení: předmět (článek 1), definice (článek 2), a to včetně odkazů na příslušné definice z jiných nástrojů EU, jako například ze směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice o bezpečnosti sítí a informací), z nařízení Evropského parlamentu a Rady (ES) č. 765/2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 a z nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 o normalizaci.

Hlava II nařízení obsahuje klíčová ustanovení týkající se agentury ENISA, Agentury EU pro kybernetickou bezpečnost.

Kapitola I této hlavy uvádí mandát (článek 3), cíle (článek 4) a úkoly agentury (články 5 až 11).

Kapitola II uvádí organizaci agentury ENISA a obsahuje klíčová ustanovení týkající se její struktury (článek 12). Zabývá se složením, pravidly hlasování a funkcemi správní rady (oddíl I, články 13 až 17), výkonné rady (oddíl 2, článek 18) a výkonného ředitele (oddíl 3, článek 19). Obsahuje rovněž ustanovení týkající se složení a úlohy stálé skupiny zúčastněných stran (oddíl 4, článek 20). V neposlední řadě oddíl 5 této kapitoly podrobně popisuje provozní

pravidla agentury, včetně pravidel týkajících se programování jejích činností, střetu zájmů, transparentnosti, důvěrnosti a přístupu k dokumentům (články 21 až 25).

Kapitola III se týká sestavování a skladby rozpočtu agentury (články 26 a 27), jakož i pravidel, jimiž se řídí plnění rozpočtu (články 28 a 29). Obsahuje rovněž ustanovení usnadňující boj proti podvodům, korupci a jiným protiprávním činnostem (článek 30).

Kapitola IV se vztahuje k personálnímu obsazení agentury. Obsahuje obecná ustanovení týkající se služebního řádu a pracovního řádu a pravidel, jimiž se řídí výsady a imunita (články 31 a 32). Rovněž podrobně popisuje pravidla týkající se přijímání a jmenování výkonného ředitele agentury (článek 33). V neposlední řadě obsahuje ustanovení, jimiž se řídí využívání vyslaných národních odborníků nebo dalších pracovníků, kteří nejsou zaměstnáni agenturou (článek 34).

Konečně kapitola V obsahuje obecná ustanovení týkající se agentury. Uvádí právní status (článek 35) a obsahuje ustanovení upravující otázky odpovědnosti, jazykového režimu, ochrany osobních údajů (články 36 až 38), jakož i bezpečnostní předpisy týkající se ochrany utajených informací a citlivých informací nepodléhajících utajení (článek 40). Popisuje pravidla, jimiž se řídí spolupráce agentury se třetími zeměmi a mezinárodními organizacemi (článek 39). V neposlední řadě obsahuje rovněž ustanovení týkající se sídla a provozních podmínek agentury, jakož i správní kontroly veřejného ochránce práv (články 41 a 42).

Hlava III nařízení zřizuje evropský rámec pro certifikaci kybernetické bezpečnosti (dále jen **„rámec“**) pro produkty a služby IKT jako *lex generalis* (článek 1). Definuje obecný účel evropských systémů certifikace kybernetické bezpečnosti, tj. zajistit, aby produkty a služby IKT byly v souladu se specifikovanými požadavky kybernetické bezpečnosti, pokud jde o jejich schopnost na dané úrovni záruky odolávat činnostem, které ohrožují přístupnost, autentičnost, neporušenost a důvěrnost ukládaných, předávaných nebo zpracovávaných údajů nebo souvisejících funkcí či služeb (článek 43). Kromě toho obsahuje seznam bezpečnostních cílů, o jejichž splnění by měly evropské systémy certifikace kybernetické bezpečnosti usilovat (článek 45), k nimž patří mimo jiné schopnost ochránit údaje proti náhodnému nebo neoprávněnému přístupu nebo sdělování, zničení nebo úpravám, a obsah (tj. prvky) evropských systémů certifikace kybernetické bezpečnosti, jako jsou například podrobná specifikace jejich rozsahu, bezpečnostní cíle, hodnoticí kritéria atd. (článek 47).

Hlava III rovněž stanoví hlavní právní účinky evropských systémů certifikace kybernetické bezpečnosti, konkrétně i) povinnost zavést systém na vnitrostátní úrovni a dobrovolnou povahu certifikace; ii) zneplatňující účinek evropských systémů certifikace kybernetické bezpečnosti na vnitrostátní systémy pro stejný produkt nebo službu (články 48 a 49).

Tato hlava dále stanoví postup pro přijímání evropských systémů certifikace kybernetické bezpečnosti a příslušnou úlohu Komise, agentury ENISA a Evropské skupiny pro certifikaci kybernetické bezpečnosti – „skupiny“ (článek 44). Konečně tato hlava stanoví ustanovení, jimiž se řídí subjekty posuzování shody, a to včetně jejich požadavků, pravomocí a úkolů, a vnitrostátní orgány dozoru nad certifikací, a stanoví rovněž sankce.

Tato hlava rovněž obsahuje ustanovení o zřízení skupiny jakožto hlavního subjektu sestávajícího ze zástupců vnitrostátních orgánů dozoru nad certifikací, jehož hlavní úlohou je spolupracovat s agenturou ENISA na přípravě evropských systémů certifikace kybernetické bezpečnosti a radit Komisi v obecných či specifických otázkách týkajících se politiky v oblasti certifikace kybernetické bezpečnosti.

Hlava IV nařízení obsahuje závěrečná ustanovení popisující výkon přenesení pravomoci, požadavky na hodnocení, zrušení a nástupnictví, jakož i vstup v platnost.

2017/0225 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o agentuře ENISA, Agentuře EU pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“)

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[28],

s ohledem na stanovisko Výboru regionů[29],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Sítě, informační systémy a telekomunikační sítě a služby mají zásadní význam pro společnost a staly se páteří hospodářského růstu. Informační a komunikační technologie podporuje komplexní systémy, které podporují společenské činnosti, udržují v chodu naše ekonomiky v klíčových odvětvích jako například zdravotnictví, energetika, finančnictví a doprava, a zejména podporují fungování vnitřního trhu.

(2) Využívání sítí a informačních systémů občany, podniky a vládami v celé Unii je v současné době všudypřítomné. Digitalizace a konektivita se stávají hlavními prvky stále rostoucího počtu produktů a služeb a očekává se, že s nástupem internetu věcí budou v celé EU během příštího desetiletí připojeny miliony, ne-li miliardy, nových digitálních zařízení. I když je k internetu připojen rostoucí počet zařízení, tato zařízení nejsou konstruována s dostatečnými bezpečnostními prvky a odolností, což vede k nedostatečné kybernetické bezpečnosti. Omezené využívání certifikace v této souvislosti vede k tomu, že organizace a soukromí uživatelé nemají dostatečné informace o prvcích kybernetické bezpečnosti produktů a služeb IKT, což narušuje důvěru v digitální řešení.

(3) Nárůst digitalizace a propojenosti vede k nárůstu kybernetických bezpečnostních rizik, což způsobuje, že společnost jako celek je zranitelnější vůči kybernetickým hrozbám a zhoršujícím se nebezpečím, s nimiž se setkávají jednotliví uživatelé včetně zranitelných osob, jako jsou děti. Za účelem zmírnění těchto rizik pro společnost je třeba přijmout veškerá opatření potřebná ke zlepšení kybernetické bezpečnosti v EU,

[28] Úř. věst. C, , s. .
[29] Úř. věst. C, , s. .

aby byly sítě a informační systémy, telekomunikační sítě, digitální produkty, služby a zařízení používané občany, vládami a podniky – od malých a středních podniků až po provozovatele kritických infrastruktur – lépe chráněny před kybernetickými hrozbami.

(4) Počet kybernetických útoků roste a propojená ekonomika a společnost, která je zranitelnější vůči kybernetickým hrozbám a útokům, vyžaduje silnější ochranu. I když kybernetické útoky jsou často přeshraniční povahy, reakce orgánů zabývajících se kybernetickou bezpečností na úrovni opatření politiky a kompetence k vymáhání právních předpisů jsou převážně vnitrostátní. Rozsáhlé kybernetické incidenty by mohly narušit poskytování základních služeb v celé EU. To vyžaduje účinnou reakci a řešení krizí na úrovni EU, které budou vycházet ze speciálních politik a širších nástrojů pro evropskou solidaritu a vzájemnou pomoc. Kromě toho je proto pro tvůrce politik, odvětví a uživatele důležité provádět pravidelné posuzování stavu kybernetické bezpečnosti a odolnosti v Unii, na základě spolehlivých unijních údajů, a také systematické předpovědi budoucího vývoje, výzev a hrozeb, a to jak na úrovni Unie, tak na celosvětové úrovni.

(5) S ohledem na nárůst kybernetických bezpečnostních hrozeb, kterým Unie čelí, existuje potřeba komplexního souboru opatření, která by vycházela z předchozích opatření Unie a podporovala vzájemně se posilující cíle. Mezi tato opatření patří nutnost dále zvýšit schopnosti a připravenost členských států a podniků a rovněž zlepšit spolupráci a koordinaci mezi členskými státy a orgány, agenturami a institucemi EU. Kromě toho vzhledem k bezhraniční povaze kybernetických hrozeb existuje potřeba zvýšit schopnosti na úrovni Unie, které by mohly doplňovat opatření členských států, zejména v případě rozsáhlých přeshraničních kybernetických incidentů a krizí. Je rovněž třeba další úsilí ke zvýšení informovanosti občanů a podniků o otázkách týkajících se kybernetické bezpečnosti. Kromě toho důvěra v jednotný digitální trh by měla být dále posílena tím, že budou poskytovány transparentní informace o úrovni bezpečnosti produktů a služeb IKT. Toto lze usnadnit celoevropskou certifikací, která bude poskytovat společné kybernetickobezpečnostní požadavky a hodnoticí kritéria napříč vnitrostátními trhy a odvětvími.

(6) Evropský parlament a Rada přijaly v roce 2004 nařízení (ES) č. 460/2004[30] o zřízení agentury ENISA za účelem přispět k cílům zajištění vysoké úrovně bezpečnosti sítí a informací v Unii a vytvoření kultury bezpečnosti sítí a informací v zájmu občanů, spotřebitelů, podniků a veřejné správy. V roce 2008 přijaly Evropský parlament a Rada nařízení (ES) č. 1007/2008[31], kterým byl mandát agentury prodloužen do března 2012. Nařízení (ES) č. 580/2011[32] prodlužuje mandát agentury do 13. září 2013. V roce 2013 přijaly Evropský parlament a Rada nařízení (EU) č. 526/2013[33] o agentuře

---

30 Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací (Úř. věst. L 77, 13.3.2004, s. 1).

31 Nařízení Evropského parlamentu a Rady (ES) č. 1007/2008 ze dne 24. září 2008, kterým se mění nařízení (ES) č. 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, pokud jde o období její činnosti (Úř. věst. L 293, 31.10.2008, s. 1).

32 Nařízení Evropského parlamentu a Rady (EU) č. 580/2011 ze dne 8. června 2011, kterým se mění nařízení (ES) č. 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, pokud jde o období její činnosti (Úř. věst. L 165, 24.6.2011, s. 3).

33 Nařízení Evropského parlamentu a Rady (EU) č. 526/2013 ze dne 21. května 2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004 (Úř. věst. L 165, 18.6.2013, s. 41).

ENISA a o zrušení nařízení (ES) č. 460/2004, kterým byl mandát agentury prodloužen do června 2020.

(7) Unie již podnikla důležité kroky k zajištění kybernetické bezpečnosti a zvýšení důvěry v digitální technologie. V roce 2013 byla přijata strategie kybernetické bezpečnosti EU jako základ pro politickou reakci Unie na kybernetické bezpečnostní hrozby a rizika. Ve snaze lépe chránit Evropany v on-line prostředí Unie v roce 2016 přijala první legislativní akt v oblasti kybernetické bezpečnosti, směrnici (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii („směrnice o bezpečnosti sítí a informací“). Směrnice o bezpečnosti sítí a informací zavedla požadavky týkající se vnitrostátních kapacit v oblasti kybernetické bezpečnosti, zřídila první mechanismy pro posílení strategické a operativní spolupráce mezi členskými státy a zavedla povinnosti týkající se bezpečnostních opatření a hlášení o incidentech napříč odvětvími, která jsou zásadní pro hospodářství a pro společnost, jako například energetika, doprava, vodohospodářství, bankovnictví, infrastruktura finančního trhu, zdravotní péče a digitální infrastruktura, jakož i poskytovatelé klíčových digitálních služeb (tj. internetové vyhledávače, služby cloud computingu a on-line tržiště). Klíčová role při podpoře provádění této směrnice byla přisouzena agentuře ENISA. Kromě toho účinný boj proti kyberkriminalitě je důležitou prioritou Evropského programu pro bezpečnost, a přispívá tak k celkovému cíli dosažení vysoké úrovně kybernetické bezpečnosti.

(8) Je třeba poznamenat, že od přijetí strategie kybernetické bezpečnosti EU v roce 2013 a od poslední revize mandátu agentury se celkový politický kontext významně změnil, mimo jiné s ohledem na více nejisté a méně bezpečné globální prostředí. V této souvislosti a v rámci nové politiky Unie v oblasti kybernetické bezpečnosti je nezbytné přezkoumat mandát agentury ENISA, aby bylo možné vymezit její roli v měnícím se ekosystému kybernetické bezpečnosti a zajistit, že účinně přispívá k reakci Unie na kybernetické bezpečnostní výzvy plynoucí z radikálně transformovaných hrozeb, k čemuž, jak bylo uznáno při hodnocení agentury, není stávající mandát dostatečný.

(9) Agentura zřízená tímto nařízením by měla být nástupcem agentury ENISA zřízené nařízením (EU) č. 526/2013. Agentura by měla plnit úkoly, které jí jsou svěřeny tímto nařízením a právními akty Unie v oblasti kybernetické bezpečnosti, mimo jiné tím, že bude poskytovat odborné poradenství a doporučení a působit jako centrum informací a znalostí Unie. Měla by podporovat výměnu osvědčených postupů mezi členskými státy a zúčastněnými stranami ze soukromého sektoru, předkládat politická doporučení Evropské komisi a členským státům, působit jako referenční místo pro odvětvové politické iniciativy Unie v souvislosti s otázkami kybernetické bezpečnosti a podporovat operativní spolupráci mezi členskými státy a mezi členskými státy a orgány, agenturami a institucemi EU.

(10) Zástupci členských států v rámci rozhodnutí 2004/97/ES, Euratom, přijatém na zasedání Evropské rady dne 13. prosince 2003, rozhodli, že agentura ENISA bude mít sídlo v Řecku ve městě, které určí řecká vláda. Hostitelský členský stát agentury by měl zajistit co nejlepší podmínky pro bezproblémové a účinné fungování agentury. V zájmu zajištění řádného a účinného plnění úkolů agentury, přijímání a udržení zaměstnanců a v zájmu zvýšení účinnosti v oblasti vytváření sítí je naprosto nezbytné, aby bylo sídlo agentury vhodně umístěno, přičemž by mimo jiné mělo být zajištěno odpovídající dopravní spojení a zařízení pro manžely/manželky a děti zaměstnanců agentury. Nezbytná opatření by měla být stanovena v dohodě mezi agenturou a daným

hostitelským členským státem, která bude uzavřena poté, co ji schválí správní rada agentury.

(11) Vzhledem k nárůstu kybernetických bezpečnostních hrozeb, kterým Unie čelí, by měly být navýšeny finanční a lidské zdroje přidělené agentuře, aby odrážely posílení úlohy a úkolů agentury a její zásadní postavení v ekosystému organizací bránících evropský digitální ekosystém.

(12) Agentura by měla rozvíjet a udržovat vysokou úroveň odborných znalostí a působit jako referenční bod, který díky své nezávislosti, kvalitě poskytovaného poradenství a informací, transparentnosti svých postupů a metod práce a pečlivosti, s níž plní svěřené úkoly, vytváří důvěru v jednotný trh. Agentura by měla aktivně přispívat k vnitrostátnímu úsilí a úsilí Unie a plnit své úkoly v plné spolupráci s orgány, institucemi a jinými subjekty Unie a s členskými státy. Kromě toho by agentura měla reagovat na podněty od soukromého sektoru a jiných příslušných zúčastněných stran a spolupracovat s nimi. Měl by být určen soubor úkolů, jenž by stanovil, jak má agentura plnit své cíle, a současně umožňoval flexibilitu jejích činností.

(13) Agentura by měla být nápomocna Komisi prostřednictvím poradenství, stanovisek a analýz ke všem záležitostem Unie souvisejícím s rozvojem politiky a právních předpisů a prostřednictvím aktualizací a přezkumů v oblasti kybernetické bezpečnosti, včetně ochrany kritické infrastruktury a kybernetické odolnosti. Pro politiky Unie v konkrétních odvětvích a pro iniciativy Unie v oblasti právních předpisů by agentura měla působit jako referenční bod poskytující doporučení a odborné poradenství v případech, kdy se tyto politiky a iniciativy týkají otázek souvisejících s kybernetickou bezpečností.

(14) Hlavním úkolem agentury je prosazovat jednotné provádění příslušného právního rámce, zejména účinné provádění směrnice o bezpečnosti sítí a informací, která je zásadní pro zvýšení kybernetické odolnosti. S ohledem na rychle se vyvíjející oblast kybernetických bezpečnostních hrozeb je zřejmé, že se členské státy musí opírat o komplexnější přístup k budování kybernetické odolnosti přesahující jednotlivé politiky.

(15) Agentura by měla být nápomocna členským státům a orgánům, institucím a jiným subjektům Unie při jejich úsilí o vytváření a rozvoj schopností a připravenosti předcházet problémům a incidentům týkajícím se kybernetické bezpečnosti, odhalovat je a reagovat na ně, a také v souvislosti s bezpečností sítí a informačních systémů. Agentura by zejména měla podporovat rozvoj a posilování vnitrostátních týmů CSIRT s cílem dosáhnout v Unii vysoké společné úrovně jejich vyspělosti. Agentura by rovněž měla pomáhat s rozvíjením a aktualizováním strategií Unie a členských států pro bezpečnost sítí a informačních systémů, zejména strategií pro kybernetickou bezpečnost, podporovat jejich šíření a sledovat pokrok při jejich provádění. Agentura by měla také poskytovat školení a vzdělávací materiály veřejným subjektům, a případně „školit školitele“, a tím pomáhat členským státům při rozvoji vlastních školicích kapacit.

(16) Agentura by měla být nápomocna skupině pro spolupráci zřízené směrnicí o bezpečnosti sítí a informací při provádění jejích úkolů, zejména prostřednictvím poskytování odborných poznatků a poradenství a prostřednictvím usnadňování výměny osvědčených postupů týkajících se rizik a incidentů, zejména pak pokud jde o identifikaci provozovatelů základních služeb členskými státy, a to i ve vztahu k přeshraničním vazbám.

(17) S cílem podněcovat spolupráci mezi veřejným a soukromým sektorem a v rámci soukromého sektoru, zejména za účelem podpory ochrany kritické infrastruktury, by agentura měla usnadnit vytváření odvětvových center sdílení a analýzy informací, a to prostřednictvím poskytování osvědčených postupů a doporučení týkajících se dostupných nástrojů a postupů a poskytováním pokynů k řešení regulačních otázek spojených se sdílením informací.

(18) Agentura by měla agregovat a analyzovat vnitrostátní zprávy od týmů CSIRT a skupiny CERT-EU a stanovovat společná pravidla, jazyk a terminologii pro výměnu informací. Agentura by rovněž měla zapojit soukromý sektor, a to v rámci směrnice o bezpečnosti sítí a informací, která vytvořením sítě CSIRT stanovila základ pro dobrovolnou výměnu technických informací na operativní úrovni.

(19) V případě rozsáhlých přeshraničních kybernetických bezpečnostních incidentů a krizí by agentura měla přispět k reakci na úrovni EU. Tato funkce by měla zahrnovat shromažďování příslušných informací a působení jako zprostředkovatel mezi sítí CSIRT a technickou komunitou a mezi subjekty s rozhodovací pravomocí příslušnými pro řešení krizí. Agentura by dále mohla podporovat řešení incidentů po technické stránce, a to tím, že by usnadňovala příslušnou technickou výměnu řešení mezi členskými státy a poskytovala vstupy do veřejných komunikací. Agentura by měla tento proces podporovat testováním způsobů takové spolupráce prostřednictvím každoročních cvičení v oblasti kybernetické bezpečnosti.

(20) Za účelem plnění svých operačních úkolů by agentura měla využít dostupné odborné poznatky skupiny CERT-EU, a to prostřednictvím strukturované spolupráce v těsné fyzické blízkosti. Strukturovaná spolupráce usnadní nezbytné synergie a akumulaci odborných poznatků agentury ENISA. V případě potřeby by měla být učiněna speciální ujednání mezi oběma organizacemi o praktické podobě takové spolupráce.

(21) V souladu se svými operačními úkoly by agentura měla být schopna poskytovat podporu členským státům, například ve formě poradenství nebo technické pomoci či zajišťování analýz hrozeb a incidentů. Doporučení Komise ohledně koordinované reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize doporučují, aby členské státy spolupracovaly v dobré víře a aby mezi sebou a s agenturou ENISA bez zbytečného odkladu sdílely informace o rozsáhlých kybernetických bezpečnostních incidentech a krizích. Tyto informace by agentuře ENISA měly dále pomoci při plnění jejích operačních úkolů.

(22) Jakou součást pravidelné spolupráce na technické úrovni na podporu informovanosti Unie o aktuální situaci by agentura měla pravidelně připravovat technickou zprávu EU o situaci v oblasti kybernetické bezpečnosti týkající se incidentů a hrozeb, a to na základě veřejně dostupných informací, svých vlastních analýz a zpráv, které s ní (dobrovolně) sdílejí týmy CSIRT členských států nebo jednotná kontaktní místa zřízená podle směrnice o bezpečnosti sítí a informací, Evropské centrum pro boj proti kyberkriminalitě (EC3) při Europolu, skupina CERT-EU a případně Středisko Evropské unie pro analýzu zpravodajských informací (INTCEN) při Evropské službě pro vnější činnost (ESVČ). Zpráva by měla být k dispozici příslušným místům Rady, Komisi, vysoké představitelce Unie pro zahraniční věci a bezpečnostní politiku a síti týmů CSIRT.

(23) Technická šetření ex post týkající se incidentů s významným dopadem ve více než jednom členském státě, která jsou agenturou podporována nebo prováděna na základě žádosti nebo se souhlasem dotčených členských států, by se měla zaměřovat na

předcházení budoucím incidentům a měla by být prováděna, aniž jsou dotčena správní nebo soudní řízení k určení míry zavinění nebo odpovědnosti.

(24) Dotčené členské státy by měly agentuře pro účely šetření poskytnout nezbytné informace a veškerou pomoc, aniž by byl dotčen článek 346 Smlouvy o fungování Evropské unie nebo jiné důvody související s ochranou veřejného pořádku.

(25) Členské státy mohou podniky dotčené incidentem vyzvat, aby spolupracovaly tak, že agentuře poskytnou nezbytné informace a veškerou pomoc, aniž je dotčeno jejich právo na ochranu obchodně citlivých informací.

(26) K lepšímu pochopení výzev v oblasti kybernetické bezpečnosti a s cílem poskytovat členským státům a orgánům Unie dlouhodobé strategické poradenství je třeba, aby agentura analyzovala současná a nově se objevující rizika. Za tímto účelem by agentura měla, ve spolupráci s členskými státy a případně statistickými orgány a dalšími subjekty, shromažďovat příslušné informace, provádět analýzy nově vznikajících technologií a poskytovat konkrétně zaměřená posouzení společenských, právních, hospodářských a regulačních dopadů technologických inovací na bezpečnost sítí a informací, zejména na kybernetickou bezpečnost. Agentura by měla také podporovat členské státy a orgány, instituce a jiné subjekty Unie při určování nových trendů a při předcházení problémům souvisejícím s kybernetickou bezpečností tak, že bude provádět analýzy hrozeb a incidentů.

(27) Za účelem zvýšení odolnosti Unie by agentura měla rozvíjet excelenci v oblasti bezpečnosti internetové infrastruktury a kritických infrastruktur, a to poskytováním poradenství, pokynů a osvědčených postupů. S cílem zajistit snazší přístup k lépe strukturovaným informacím o kybernetických bezpečnostních rizicích a o potenciálních prostředcích nápravy by agentura měla vytvořit a spravovat „informační centrum“ Unie, jednotný portál („one-stop-shop“) poskytující veřejnosti informace o kybernetické bezpečnosti získané od EU a vnitrostátních orgánů, institucí a subjektů.

(28) Agentura by měla přispívat ke zvyšování informovanosti veřejnosti ohledně rizik souvisejících s kybernetickou bezpečností a poskytovat pokyny a osvědčené postupy pro jednotlivé uživatele zaměřené na občany a organizace. Agentura by rovněž měla přispívat k podpoře osvědčených postupů a řešení na úrovni jednotlivců a organizací, a to shromažďováním a analyzováním veřejně dostupných informací týkajících se závažných incidentů a sestavováním zpráv s cílem poskytnout podnikům a občanům pokyny a zlepšit celkovou úroveň připravenosti a odolnosti. Agentura by dále měla ve spolupráci s členskými státy a orgány, institucemi a jinými subjekty Unie organizovat pravidelné veřejné vzdělávací kampaně pro koncové uživatele s cílem podporovat bezpečnější chování jednotlivců na internetu a zvyšovat informovanost o potenciálních hrozbách v kyberprostoru, včetně počítačové kriminality jako phishingové útoky, botnety a finanční a bankovní podvody, a podporovat základní nástroje ověřování a ochrany údajů. Agentura by rovněž měla hrát ústřední úlohu při urychlování informovanosti koncových uživatelů o bezpečnosti zařízení.

(29) Za účelem podpory podniků působících v odvětví kybernetické bezpečnosti a rovněž uživatelů řešení v oblasti kybernetické bezpečnosti by agentura měla vytvořit a provozovat „středisko pro sledování trhu“ prostřednictvím provádění pravidelných analýz a šíření hlavních trendů na trhu kybernetické bezpečnosti, a to jak na straně poptávky, tak na straně nabídky.

(30) Aby bylo zajištěno, že agentura plně dosahuje svých cílů, měla by spolupracovat s příslušnými orgány, institucemi a jinými subjekty, včetně skupiny CERT-EU,

Evropského centra pro boj proti kyberkriminalitě (EC3) při Europolu, Evropské agentury pro provozní řízení rozsáhlých informačních systémů (eu-LISA), Evropské agentury pro bezpečnost letectví (EASA) a dalších agentur EU zapojených do kybernetické bezpečnosti. Měla by rovněž spolupracovat s orgány zabývajícími se ochranou údajů, a to za účelem výměny know-how a osvědčených postupů a poskytování poradenství ohledně aspektů kybernetické bezpečnosti, které mohou mít dopad na práci těchto orgánů. Zástupcům vnitrostátních a unijních donucovacích orgánů a orgánů na ochranu údajů by měla být umožněna účast ve stálé skupině zúčastněných stran agentury. Při spolupráci s donucovacími orgány týkající se aspektů bezpečnosti sítí a informací, které by mohly mít dopad na jejich práci, by agentura měla respektovat stávající informační kanály a zavedené sítě.

(31) Agentura, jakožto člen, který rovněž zajišťuje služby sekretariátu sítě týmů CSIRT, by měla podporovat týmy CSIRT členských států a skupinu CERT-EU při operativní spolupráci na základě všech příslušných úkolů sítě týmu CSIRT, jak jsou vymezeny ve směrnici o bezpečnosti sítí a informací. Agentura by dále měla prosazovat a podporovat spolupráci mezi příslušnými týmy CSIRT v případě incidentů, útoků či poruch sítí nebo infrastruktury, které jsou spravovány nebo chráněny týmy CSIRT a které postihují nebo potenciálně postihují alespoň dvě skupiny CERT, přičemž by měla náležitě zohlednit standardní operační postupy sítě týmu CSIRT.

(32) Za účelem zvýšení připravenosti Unie v oblasti reakce na kybernetické bezpečnostní incidenty by agentura měla pořádat každoroční cvičení v oblasti kybernetické bezpečnosti na úrovni Unie a poskytovat podporu institucím, orgánům, agenturám a jiným subjektům členských států a EU na jejich žádost při pořádání cvičení.

(33) Agentura by měla dále rozvíjet a udržovat svoji odbornost v oblasti certifikace kybernetické bezpečnosti s cílem podporovat politiku Unie v této oblasti. Agentura by měla s cílem zvýšení transparentnosti záruk kybernetické bezpečnosti produktů a služeb IKT a s tím souvisejícího posílení důvěry v digitální vnitřní trh prosazovat zavádění certifikace kybernetické bezpečnosti v Unii, a to včetně toho, že bude přispívat k zavedení a správě rámce pro certifikaci kybernetické bezpečnosti na úrovni Unie.

(34) Účinná politika v oblasti kybernetické bezpečnosti by měla být založena na pečlivě vyvinutých metodách posuzování rizika ve veřejném i v soukromém sektoru. Metody posuzování rizika se používají na různých úrovních, aniž by existoval jednotný systém, který by zaručoval jejich účinné uplatňování. Podpora a rozvoj osvědčených postupů posuzování rizika a interoperabilních řešení řízení rizik u organizací veřejného a soukromého sektoru zvýší úroveň kybernetické bezpečnosti v Unii. Agentura by měla za tímto účelem podporovat spolupráci mezi zúčastněnými stranami na úrovni Unie a usnadňovat jejich úsilí zaměřené na vytvoření a používání evropských a mezinárodních standardů řízení rizik a měřitelné bezpečnosti elektronických produktů, systémů, sítí a služeb, které společně se softwarem tvoří sítě a informační systémy.

(35) Agentura by měla vybízet členské státy a poskytovatele služeb, aby zvýšili své obecné standardy v oblasti bezpečnosti, a umožnili tak všem uživatelům internetu podniknout potřebné kroky k zajištění své vlastní kybernetické bezpečnosti Poskytovatelé služeb a výrobci produktů by zejména měli stáhnout nebo recyklovat produkty a služby, které nesplňují normy kybernetické bezpečnosti. Agentura ENISA může ve spolupráci s příslušnými orgány šířit informace týkající se úrovně kybernetické bezpečnosti produktů a služeb nabízených na vnitřním trhu a vydávat varování, která jsou určená

poskytovatelům a výrobcům a která od nich požadují, aby zvýšili bezpečnost svých produktů a služeb, včetně kybernetické bezpečnosti.

(36) Agentura by měla plně zohlednit činnosti probíhající v oblasti výzkumu, vývoje a technologického hodnocení, zejména činnosti prováděné v rámci různých výzkumných iniciativ Unie, aby mohla orgánům, institucím a jiným subjektům Unie a případně členským státům, které o to požádají, poskytovat poradenství ohledně potřeb výzkumu v oblasti bezpečnosti sítí a informací, zejména pak kybernetické bezpečnosti.

(37) Problémy týkající se kybernetické bezpečnosti jsou globální záležitostí. Je nutná užší mezinárodní spolupráce pro zvýšení bezpečnostních standardů, včetně stanovení společných norem chování, a zlepšení sdílení informací, jež podpoří pružnější mezinárodní spolupráci v reakci na problémy týkající se bezpečnosti sítí a informací, ale i společný globální přístup k nim. Agentura by za tímto účelem měla podporovat větší zapojení Unie a spolupráci se třetími zeměmi a mezinárodními organizacemi tím, že případně poskytne nezbytné odborné znalosti a analýzy příslušným orgánům, institucím a jiným subjektům Unie.

(38) Agentura by měla být schopna reagovat na žádosti ad hoc o poradenství a pomoc od členských států a orgánů, institucí a jiných subjektů EU, které jsou v souladu s cíli agentury.

(39) Aby bylo dosaženo souladu se společným prohlášením a společným přístupem, na nichž se v červenci 2012 dohodla interinstitucionální pracovní skupina pro decentralizované agentury EU, je nezbytné stanovit určité zásady týkající se řízení agentury, přičemž účelem zmíněného prohlášení a přístupu je zjednodušit činnost agentur a zlepšit jejich výkonnost. Společné prohlášení a společný přístup by se případně měly odrazit také v pracovních programech agentury, hodnoceních agentury a postupech, které agentura používá pro podávání zpráv a v administrativě.

(40) Správní rada složená z členských států a Komise by měla vymezit obecné směry činnosti agentury a zaručit, že bude své úkoly plnit v souladu s tímto nařízením. Správní radě by měly být svěřeny pravomoci potřebné pro sestavování rozpočtu, ověřování jeho plnění, schvalování příslušných finančních předpisů, stanovení transparentních pracovních postupů pro přijímání rozhodnutí agentury, schvalování jednotného programového dokumentu agentury, přijímání jejího jednacího řádu, jmenování výkonného ředitele a rozhodování o prodloužení funkčního období výkonného ředitele a o jeho odvolání.

(41) V zájmu řádného a účinného fungování agentury by Komise a členské státy měly zajistit, aby osoby, které mají být jmenovány členy správní rady, měly patřičnou odbornou kvalifikaci a zkušenosti v oblastech činnosti. Komise a členské státy by měly usilovat o omezení obměny svých zástupců ve správní radě, aby byla zajištěna kontinuita její činnosti.

(42) Řádné fungování agentury vyžaduje, aby byl její výkonný ředitel jmenován na základě projevených kvalit a doložených administrativních a řídicích schopností a rovněž odbornosti a zkušeností v oblasti kybernetické bezpečnosti a aby vykonával své povinnosti zcela nezávisle. Výkonný ředitel by měl za tímto účelem po předchozích konzultacích s Komisí zpracovat návrh pracovního programu agentury a učinit veškeré kroky nezbytné k zajištění jeho řádného plnění. Výkonný ředitel by měl vypracovávat výroční zprávy, které se předloží správní radě, a návrh odhadu příjmů a výdajů agentury a měl by plnit rozpočet. Výkonný ředitel by měl mít dále možnost sestavovat ad hoc pracovní skupiny, které by se věnovaly konkrétním otázkám, zejména vědecké,

technické nebo právní či socioekonomické povahy. Výkonný ředitel by měl zajistit, aby byli členové ad hoc pracovní skupiny vybráni na základě vysokých standardů odborných znalostí a se zřetelem k rovnovážnému zastoupení podle obsahu činnosti mezi zástupci veřejné správy členských států, zástupci orgánů Unie a zástupci soukromého sektoru, včetně průmyslu, a zástupci uživatelů a vědeckých odborníků v oblasti bezpečnosti sítí a informací.

(43) Výkonná rada by měla přispívat k účinnému fungování správní rady. Jako součást své přípravné činnosti související s rozhodnutími správní rady by měla podrobně prověřit příslušné informace, prozkoumat dostupné možnosti a nabídnout poradenství a řešení pro přípravu příslušných rozhodnutí správní rady.

(44) Pro pravidelný dialog se soukromým sektorem, organizacemi spotřebitelů a ostatními dotčenými zúčastněnými stranami by agentura měla mít stálou skupinu zúčastněných stran. Stálá skupina zúčastněných stran ustavená správní radou na návrh výkonného ředitele by se měla věnovat otázkám, které mají význam pro zúčastněné strany, a měla by je předkládat agentuře. Složení stálé skupiny zúčastněných stran a úkoly, jimiž je pověřena, které je třeba konzultovat zejména v rámci návrhu pracovního programu, by měly zajistit dostatečnou účast zúčastněných stran na činnosti agentury.

(45) Agentura by měla mít zavedena pravidla týkající se prevence a řešení střetu zájmů. Agentura by rovněž měla uplatňovat odpovídající ustanovení práva Unie týkající se přístupu veřejnosti k dokumentům podle nařízení Evropského parlamentu a Rady (ES) č. 1049/2001[34]. Osobní údaje by měly být agenturou zpracovávány v souladu s nařízením Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů[35]. Agentura by měla zejména dodržovat předpisy vztahující se na orgány Unie a rovněž vnitrostátní předpisy o nakládání s informacemi, zejména s citlivými informacemi nepodléhajícími utajení a utajovanými informacemi EU.

(46) Aby byla zaručena plná autonomie a nezávislost agentury a bylo jí umožněno vykonávat další nové úkoly, včetně nečekaných naléhavých úkolů, měla by mít k dispozici dostatečný a samostatný rozpočet, který je rozhodující měrou financován z příspěvků Unie a z příspěvků třetích zemí podílejících se na práci agentury. Většina zaměstnanců agentury by se měla přímo podílet na operativním plnění mandátu agentury. Hostitelský nebo jakýkoli jiný členský stát by měl mít možnost poskytnout dobrovolné příspěvky k příjmům agentury. Všechny subvence ze souhrnného rozpočtu Unie by měly podléhat rozpočtovému procesu Unie. Účetní dvůr by měl navíc provádět audit účetnictví agentury s cílem zajistit transparentnost a odpovědnost.

(47) Posuzování shody je postup k prokázání, zda byly splněny konkrétní požadavky týkající se produktu, postupu, služby, systému, osoby nebo subjektu. Pro účely tohoto nařízení by certifikace měla být považována za typ posuzování shody, který se týká kybernetickobezpečnostních prvků produktů, procesů, služeb a systémů nebo jejich kombinací („produkty a služby IKT“) a který je prováděn nezávislou třetí stranou jinou než výrobcem produktu nebo poskytovatelem služby. Certifikace nemůže sama o sobě zaručit, že certifikované produkty a služby IKT jsou kyberneticky bezpečné. Spíše se jedná o proces a technickou metodiku sloužící k potvrzení, že produkty a

---

[34] Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (Úř. věst. L 145, 31.5.2001, s. 43).

[35] Úř. věst. L 8, 12.1.2001, s. 1.

služby IKT byly testovány a že splňují určité stanovené kybernetickobezpečnostní požadavky, např. požadavky stanovené v technických normách.

(48) Certifikace kybernetické bezpečnosti hraje důležitou úlohu při zvyšování důvěry v produkty a služby a jejich bezpečnosti. Jednotný digitální trh a zejména ekonomika dat a internet věcí se mohou rozvíjet, pouze bude-li existovat obecná důvěra veřejnosti, že dané produkty a služby poskytují určitou úroveň záruky kybernetické bezpečnosti. Propojené a automatizované automobily, elektronická zdravotnická zařízení, průmyslové automatizační řídicí systémy nebo inteligentní sítě, to je pouze několik příkladů odvětví, v nichž je certifikace již široce využívána, nebo je pravděpodobné, že v blízké budoucnosti využívána bude. Odvětví regulovaná směrnicí o bezpečnosti sítí a informací jsou zároveň odvětvími, v nichž má certifikace kybernetické bezpečnosti zásadní význam.

(49) Komise ve svém sdělení „Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti“ z roku 2016 nastínila potřebu vysoce kvalitních, cenově dostupných a interoperabilních kybernetickobezpečnostních produktů a řešení. Dodávky produktů a služeb IKT v rámci jednotného trhu jsou geograficky velmi roztříštěné. Důvodem je skutečnost, že odvětví kybernetické bezpečnosti v Evropě se vyvíjelo převážně na základě poptávky vnitrostátních vlád. Mezi další nedostatky, které ovlivňují jednotný trh kybernetické bezpečnosti, patří dále absence interoperabilních řešení (technických norem), postupů a celoevropských mechanismů pro certifikaci. To na straně jedné snižuje konkurenceschopnost evropských společností na vnitrostátní, evropské i celosvětové úrovni. Na straně druhé to omezuje výběr funkčních a užitečných kybernetickobezpečnostních technologií, ke kterým mají občané a podniky přístup. Podobně Komise ve svém přezkumu v polovině období provádění strategie pro jednotný digitální trh zdůraznila potřebu bezpečných propojených produktů a systémů a uvedla, že vytvoření evropského bezpečnostního rámce IKT stanovujícího pravidla pro systémy certifikace bezpečnosti IKT v Unii by mohla zachovat důvěru v internet a řešit stávající roztříštěnost trhu kybernetické bezpečnosti.

(50) Certifikace kybernetické bezpečnosti produktů a služeb IKT je v současné době využívána pouze v omezené míře. Pokud existuje, pak převážně na úrovni členských států nebo v rámci systémů podporovaných potřebami průmyslu. Certifikát vydaný jedním vnitrostátním orgánem pro kybernetickou bezpečnost v této souvislosti v zásadě není uznáván jinými členskými státy. Společnosti proto musí své produkty a služby certifikovat v několika členských státech, v nichž působí, například s cílem účastnit se vnitrostátních zadávacích řízení. Kromě toho, i když se objevují nové systémy, zdá se, že pokud jde o horizontální otázky kybernetické bezpečnosti, např. v oblasti internetu věcí, neexistuje žádný jednotný a ucelený přístup. Stávající systémy vykazují významné nedostatky a rozdíly z hlediska pokrytí produktů, úrovní záruk, podstatných kritérií a skutečného využití.

(51) V minulosti bylo vynaloženo určité úsilí za účelem vzájemného uznávání certifikátů v Evropě. Toto úsilí však bylo úspěšné pouze částečně. Nejdůležitějším příkladem je v tomto ohledu dohoda o vzájemném uznávání skupiny vyšších úředníků – bezpečnost informačních systémů (SOG-IS). Ačkoliv dohoda o vzájemném uznávání skupiny SOG-IS představuje nejdůležitější model spolupráce a vzájemného uznávání v oblasti certifikace bezpečnosti, obsahuje některé významné nedostatky související s jejími vysokými náklady a omezenou působností. Dosud bylo vyvinuto pouze několik profilů ochrany pro digitální výrobky, jako např. digitální podpis, digitální tachograf a čipové karty. Nejdůležitější je, že skupina SOG-IS zahrnuje pouze část členských států Unie.

To z pohledu vnitřního trhu účinnost dohody o vzájemném uznávání skupiny SOG-IS omezuje.

(52) S ohledem na výše uvedené je nezbytné zřídit evropský rámec pro certifikaci kybernetické bezpečnosti, který stanoví hlavní horizontální požadavky pro evropské systémy certifikace kybernetické bezpečnosti, které mají být vypracovány, a umožní, aby byly certifikáty pro produkty a služby IKT uznávané a používané ve všech členských státech. Evropský rámec by měl mít dvojí účel: na straně jedné by měl pomoci zvýšit důvěru v produkty a služby IKT, které byly certifikovány podle takových systémů. Na straně druhé by měl zabránit násobení protichůdných nebo odporujících si vnitrostátních certifikací kybernetické bezpečnosti, a tím snížit náklady podniků působících na jednotném digitálním trhu. Systémy by měly být nediskriminační a měly by být založeny na mezinárodních normách a/nebo na normách Unie, pokud tyto normy nejsou neúčinné nebo nevhodné k dosažení cílů, které jsou v tomto ohledu oprávněné.

(53) Komisi by měla být svěřena pravomoc přijímat evropské systémy certifikace kybernetické bezpečnosti týkající se konkrétních skupin produktů a služeb IKT. Tyto systémy by měly provádět a dozor nad nimi by měly vykonávat vnitrostátní orgány dozoru nad certifikací a certifikáty vydané v rámci těchto systémů by měly být platné a uznávané v celé Unii. Systémy certifikace provozované odvětvím nebo jinými soukromými organizacemi by měly spadat mimo oblast působnosti tohoto nařízení. Subjekty provozující tyto systémy však mohou Komisi navrhnout, aby tyto systémy zvážila jako základ pro jejich schválení jakožto evropského systému.

(54) Ustanoveními tohoto nařízení by neměly být dotčeny právní předpisy Unie stanovující zvláštní pravidla týkající se certifikace produktů a služeb IKT. Zejména obecné nařízení o ochraně osobních údajů obsahuje ustanovení týkající se zavedení mechanismů pro vydávání osvědčení a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s tímto nařízením v případě operací zpracování prováděných správci a zpracovateli. Tyto mechanismy pro vydávání osvědčení a pečetě a známky dokládající ochranu údajů by měly subjektům údajů u příslušných produktů a služeb umožnit rychlé posouzení úrovně ochrany údajů. Tímto nařízením není dotčena certifikace operací zpracování údajů podle obecného nařízení o ochraně osobních údajů, včetně situací, kdy jsou tyto operace zabudované v produktech a službách.

(55) Účelem evropských systémů certifikace kybernetické bezpečnosti by mělo být zajistit, aby produkty a služby IKT certifikované podle takového systému splňovaly konkrétní požadavky. Tyto požadavky se týkají schopnosti na dané úrovni záruky odolávat činnostem, které ohrožují přístupnost, autentičnost, neporušenost a důvěrnost ukládaných, předávaných nebo zpracovávaných údajů nebo souvisejících funkcí či služeb nabízených nebo dostupných prostřednictvím těchto produktů, procesů, služeb a systémů ve smyslu tohoto nařízení. V tomto nařízení není možné podrobně stanovit kybernetickobezpečnostní požadavky týkající se veškerých produktů a služeb IKT. Produkty a služby IKT a související potřeby v oblasti kybernetické bezpečnosti jsou natolik rozmanité, že je velmi obtížné přijít s obecnými kybernetckobezpečnostními požadavky, které by byly všeobecně platné. Proto je pro účely certifikace nutné přijmout obecný a široký obsah pojmu kybernetická bezpečnost, doplněný souborem konkrétních cílů v oblasti kybernetické bezpečnosti, které je třeba zohlednit při navrhování evropských systémů certifikace kybernetické bezpečnosti. Způsoby, jimiž bude těchto cílů u konkrétních produktů a služeb IKT dosaženo, by poté měly být dále

podrobně specifikovány na úrovni jednotlivých systémů certifikace přijatých Komisí, například prostřednictvím odkazu na normy nebo technické specifikace.

(56) Komisi by měla být svěřena pravomoc požádat agenturu ENISA, aby vypracovala návrhy systémů pro konkrétní produkty nebo služby IKT. Komisi by poté měla být svěřena pravomoc, aby na základě návrhu systému předloženého agenturou ENISA přijala evropský systém certifikace kybernetické bezpečnosti prostřednictvím prováděcích aktů. S ohledem na obecný účel a bezpečnostní cíle stanovené v tomto nařízení by evropské systémy certifikace kybernetické bezpečnosti přijaté Komisí měly určovat minimální soubor prvků týkajících se předmětu, rozsahu a fungování konkrétního systému. Ty by měly mimo jiné zahrnovat rozsah a předmět certifikace kybernetické bezpečnosti včetně kategorií produktů a služeb IKT, na které se certifikace vztahuje, podrobnou specifikaci kybernetickobezpečnostních požadavků, například prostřednictvím odkazu na příslušnou normu nebo technickou specifikaci, konkrétní kritéria a metody hodnocení a úroveň záruky, kterou mají zajistit: základní, významnou a/nebo vysokou.

(57) Využití evropské certifikace kybernetické bezpečnosti by mělo zůstat dobrovolné, pokud unijní nebo vnitrostátní právní předpisy nestanoví jinak. Avšak s cílem dosažení cílů tohoto nařízení a zabránění roztříštěnosti vnitřního trhu by vnitrostátní systémy nebo postupy certifikace kybernetické bezpečnosti pro produkty a služby IKT zahrnuté do evropského systému certifikace kybernetické bezpečnosti měly ode dne stanoveného Komisí prostřednictvím prováděcího aktu pozbýt účinnosti. Členské státy by navíc neměly zavádět nové vnitrostátní systémy stanovující systémy certifikace kybernetické bezpečnosti pro produkty a služby IKT, které jsou již zahrnuty do určitého evropského systému certifikace kybernetické bezpečnosti.

(58) Jakmile je přijat určitý evropský systém certifikace kybernetické bezpečnosti, výrobci produktů IKT nebo poskytovatelé služeb IKT by měli být schopni subjektu posuzování shody podlé své volby předložit žádost o certifikaci svých produktů nebo služeb. Subjekty posuzování shody by měly být akreditovány akreditačním orgánem, splňují-li určité konkrétní požadavky stanovené v tomto nařízení. Akreditace by měla být vydávána na období nejvýše pěti let a lze ji obnovit za stejných podmínek, pokud daný subjekt posuzování shody splňuje příslušné požadavky. Akreditační orgány by měly zrušit akreditaci subjektu posuzování shody, pokud podmínky pro akreditaci nejsou nebo přestanou být splňovány, nebo pokud opatření přijatá subjektem posuzování shody porušují toto nařízení.

(59) Je nezbytné od všech členských států požadovat, aby určily jeden orgán dozoru nad certifikací kybernetické bezpečnosti, který bude dohlížet na to, aby subjekty posuzování shody a certifikáty vydané subjekty posuzování shody usazenými na jejich území splňovaly požadavky tohoto nařízení a příslušných systémů certifikace kybernetické bezpečnosti. Vnitrostátní orgány dozoru nad certifikací by měly řešit stížnosti podané fyzickými nebo právnickými osobami v souvislosti s certifikáty vydanými subjekty posuzování shody usazenými na jejich území, v přiměřeném rozsahu šetřit předmět stížnosti a v přiměřené lhůtě informovat stěžovatele o pokroku a výsledku šetření. Kromě toho by měly spolupracovat s dalšími vnitrostátními orgány dozoru nad certifikací nebo jinými veřejnými orgány, a to i prostřednictvím sdílení informací o možných případech, kdy produkty a služby IKT nesplňují požadavky tohoto nařízení nebo konkrétních systémů kybernetické bezpečnosti.

(60) S cílem zajistit jednotné uplatňování evropského rámce pro certifikaci kybernetické bezpečnosti by měla být zřízena Evropská skupina pro certifikaci kybernetické

bezpečnosti (dále jen „skupina“) sestávající z vnitrostátních orgánů dozoru nad certifikací. Hlavními úkoly skupiny by mělo být poskytování poradenství a pomoci Komisi při její práci směřující k zajištění jednotného provádění a uplatňování evropského rámce pro certifikaci kybernetické bezpečnosti; pomáhat agentuře a úzce s ní spolupracovat při přípravě návrhů systémů certifikace kybernetické bezpečnosti; doporučovat, aby Komise požádala agenturu, aby vypracovala návrh evropského systému certifikace kybernetické bezpečnosti; a přijímat stanoviska určená Komisi týkající se zachování a přezkumu stávajících evropských systémů certifikace kybernetické bezpečnosti.

(61) Evropská komise může za účelem zvyšování informovanosti a usnadnění uznávání budoucích systémů evropské kybernetické bezpečnosti vydávat obecné kybernetické bezpečnostní pokyny nebo kybernetické bezpečnostní pokyny pro konkrétní odvětví, např. osvědčené postupy v oblasti kybernetické bezpečnosti nebo pokyny týkající se odpovědného chování v oblasti kybernetické bezpečnosti zdůrazňující pozitivní účinek používání certifikovaných produktů a služeb IKT.

(62) Podpora certifikace kybernetické bezpečnosti ze strany agentury by rovněž měla zahrnovat spolupráci s Bezpečnostním výborem Rady a s příslušnými vnitrostátními orgány ohledně schválení kryptografických prostředků u produktů pro použití v sítích podléhajících utajení.

(63) Za účelem dalšího upřesnění kritérií pro akreditaci subjektů posuzování shody by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie. Komise by během přípravné činnosti měla provádět příslušné konzultace, včetně konzultací na úrovni odborníků. Tyto konzultace by měly být prováděny v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci by měly Evropský parlament a Rada obdržet veškeré dokumenty současně s odborníky z členských států a jejich odborníci by měly mít automaticky přístup na setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

(64) V zájmu zajištění jednotných podmínek pro provádění tohoto nařízení je třeba svěřit Komisi prováděcí pravomoci v případech stanovených tímto nařízením. Tyto pravomoci by měly být vykonávány v souladu s nařízením (EU) č. 182/2011.

(65) Přezkumný postup by měl být použit pro přijímání prováděcích aktů týkajících se evropských systémů certifikace kybernetické bezpečnosti pro produkty a služby IKT; způsobů, jakými agentura provádí šetření; jakož i okolností, formátů a postupů oznamování akreditovaných subjektů posuzování shody podávaných vnitrostátními orgány dozoru nad certifikací Komisi.

(66) Činnosti agentury by měly být hodnoceny nezávisle. Hodnocení by se mělo týkat toho, jak agentura dosahuje svých cílů, jejích pracovních postupů a relevantnosti jejích úkolů. Hodnocení by rovněž mělo posuzovat dopad, účinnost a účelnost evropského rámce pro certifikaci kybernetické bezpečnosti.

(67) Nařízení (EU) č. 526/2013 by mělo být zrušeno.

(68) Jelikož cílů tohoto nařízení nemůže být uspokojivě dosaženo na úrovni členských států, nýbrž může jich být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku toto nařízení nepřekračuje rámec toho, co je nezbytné pro dosažení uvedeného cíle,

PŘIJALY TOTO NAŘÍZENÍ:

HLAVA I
OBECNÁ USTANOVENÍ

Článek 1
Předmět a oblast působnosti

Za účelem zajištění řádného fungování vnitřního trhu a vysoké úrovně kybernetické bezpečnosti, kybernetické odolnosti a důvěry v Unii toto nařízení:

a) stanoví cíle, úkoly a organizační aspekty agentury ENISA, „Agentury EU pro kybernetickou bezpečnost“, dále jen „agentura“, a

b) stanoví rámec pro zavedení evropského systému certifikace kybernetické bezpečnosti za účelem zajištění odpovídající úrovně kybernetické bezpečnosti produktů a služeb IKT v Unii. Tento rámec se použije, aniž jsou dotčena zvláštní ustanovení týkající se dobrovolné nebo povinné certifikace stanovená v jiných právních předpisech Unie.

Článek 2
Definice

Pro účely tohoto nařízení se rozumí:

1) „kybernetickou bezpečností“ veškeré činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a osob dotčených kybernetickými hrozbami;

2) „sítí a informačním systémem“ systém ve smyslu čl. 4 bodu 1 směrnice (EU) 2016/1148;

3) „národní strategií pro bezpečnost sítí a informačních systémů“ rámec ve smyslu čl. 4 bodu 3 směrnice (EU) 2016/1148;

4) „provozovatelem základních služeb“ veřejný nebo soukromý subjekt definovaný v čl. 4 bodu 4 směrnice (EU) 2016/1148;

5) „poskytovatelem digitálních služeb“ jakákoli právnická osoba poskytující digitální službu definovaná v čl. 4 bodu 6 směrnice (EU) 2016/1148;

6) „incidentem“ jakákoliv událost definovaná v čl. 4 bodu 7 směrnice (EU) 2016/1148;

7) „řešením incidentu“ veškeré postupy definované v čl. 4 bodu 8 směrnice (EU) 2016/1148;

8) „kybernetickou hrozbou“ jakákoliv potenciální okolnost nebo událost, která může nepříznivě ovlivnit sítě a informační systémy, jejich uživatele a dotčené osoby;

9) „evropským systémem certifikace kybernetické bezpečnosti“ komplexní soubor pravidel, technických požadavků, norem a postupů definovaných na úrovni Unie, které se uplatňují na certifikaci produktů a služeb informačních a komunikačních technologií (IKT) spadajících do oblasti působnosti konkrétního systému;

10) „evropským certifikátem kybernetické bezpečnosti“ dokument vydaný subjektem posuzování shody, který osvědčuje, že daný produkt nebo služba IKT splňuje konkrétní požadavky stanovené v evropském systému certifikace kybernetické bezpečnosti;

11) „produktem a službou IKT“ jakýkoliv prvek nebo skupina prvků sítí a informačních systémů;

12) „akreditací“ akreditace definovaná v čl. 2 bodě 10 nařízení (ES) č. 765/2008;

13) „vnitrostátním akreditačním orgánem“ vnitrostátní akreditační orgán definovaný v čl. 2 bodě 11 nařízení (ES) č. 765/2008;

14) „posouzením shody“ posouzení shody definované v čl. 2 bodě 12 nařízení (ES) č. 765/2008;

15) „subjektem posuzování shody“ subjekt posuzování shody definovaný v čl. 2 bodě 13 nařízení (ES) č. 765/2008;

16) „normou“ norma ve smyslu čl. 2 bodu 1 nařízení (EU) č. 1025/2012.

HLAVA II
ENISA – „Agentura EU pro kybernetickou bezpečnost“

KAPITOLA I
MANDÁT, CÍLE A ÚKOLY

Článek 3
Mandát

1. Agentura plní úkoly, které jsou jí uloženy tímto nařízením za účelem zajištění vysoké úrovně kybernetické bezpečnosti v Unii.
2. Agentura plní úkoly, které jsou jí svěřeny akty Unie stanovícími opatření pro sbližování právních a správních předpisů členských států týkajících se kybernetické bezpečnosti.
3. Úkoly a cíli agentury nejsou dotčeny pravomoci členských států týkající se kybernetické bezpečnosti a v žádném případě jimi nejsou dotčeny činnosti týkající se veřejné bezpečnosti, obrany, národní bezpečnosti ani činnosti státu v oblastech trestního práva.

Článek 4
Cíle

1. Agentura je odborným střediskem pro kybernetickou bezpečnost vzhledem ke své nezávislosti, vědecké a technické kvalitě poradenství a pomoci, které poskytuje, a informací, které šíří, transparentnosti svých operativních postupů a metod práce a náležité péči při plnění svých úkolů.
2. Agentura je nápomocna orgánům, institucím a jiným subjektům Unie, jakož i členským státům při vypracovávání a provádění politik týkajících se kybernetické bezpečnosti.
3. Agentura podporuje budování a připravenost kapacit v celé Unii tím, že pomáhá Unii, členským státům a zúčastněným stranám z veřejného a soukromého sektoru zvyšovat ochranu jejich sítí a informačních systémů, rozvíjet schopnosti a odbornost v oblasti kybernetické bezpečnosti a dosahovat kybernetické odolnosti.
4. Agentura podporuje spolupráci a koordinaci na úrovni Unie mezi členskými státy, orgány, institucemi a jinými subjekty Unie a příslušnými zúčastněnými stranami včetně soukromého sektoru v záležitostech týkajících se kybernetické bezpečnosti.
5. Agentura zvyšuje schopnosti v oblasti kybernetické bezpečnosti na úrovni Unie s cílem doplňovat opatření členských států v oblasti předcházení kybernetickým hrozbám a reakce a ně, zejména v případě přeshraničních incidentů.
6. Aby agentura zvýšila transparentnost záruk kybernetické bezpečnosti produktů a služeb IKT, a posílila tím důvěru v digitální vnitřní trh, prosazuje využívání certifikace, mimo jiné tím, že přispívá k zavedení a správě rámce pro certifikaci kybernetické bezpečnosti na úrovni Unie v souladu s hlavou III tohoto nařízení.

7. Agentura podporuje vysokou úroveň informovanosti občanů a podniků o otázkách týkajících se kybernetické bezpečnosti.

Článek 5
Úkoly týkající se tvorby a provádění politiky a práva Unie

Agentura přispívá k tvorbě a provádění politiky a práva Unie tím, že:

1. je nápomocna a poskytuje poradenství ohledně tvorby a přezkumu politiky a práva Unie v oblasti kybernetické bezpečnosti, jakož i ohledně odvětvových politik a iniciativ v oblasti práva, pokud se tyto politiky a iniciativy týkají záležitostí souvisejících s kybernetickou bezpečností, a to zejména poskytováním svých nezávislých stanovisek a zajišťováním přípravných činností;
2. je nápomocna členským státům při jednotném uplatňování politiky a práva Unie v oblasti kybernetické bezpečnosti, zejména pokud jde o směrnici (EU) 2016/1148, mimo jiné formou stanovisek, pokynů, poradenství a osvědčených postupů týkajících se témat jako řízení rizik, hlášení incidentů a sdílení informací, jakož i usnadňováním výměny souvisejících osvědčených postupů mezi příslušnými orgány;
3. přispívá k činnosti skupiny pro spolupráci podle článku 11 směrnice (EU) 2016/1148 poskytováním svých odborných poznatků a pomoci;
4. podporuje:
    1) tvorbu a provádění politiky Unie v oblasti elektronické identity a služeb vytvářejících důvěru, zejména poskytováním poradenství a technických pokynů, jakož i usnadňováním výměny osvědčených postupů mezi příslušnými orgány;
    2) prosazování vyšší úrovně bezpečnosti elektronických komunikací, mimo jiné poskytováním odborných poznatků a poradenství a usnadňováním výměny osvědčených postupů mezi příslušnými orgány;
5. podporuje pravidelný přezkum činností v oblasti politiky Unie tím, že poskytuje výroční zprávu o stavu provádění příslušného právního rámce týkajícího se:
    a) hlášení incidentů členských států podaných jednotným kontaktním místem skupině pro spolupráci podle čl. 10 odst. 3 směrnice (EU) 2016/1148;
    b) oznámení o narušení bezpečnosti a ztrátě integrity týkajících se poskytovatelů služeb vytvářejících důvěru, které agentuře poskytly orgány dohledu podle čl. 19 odst. 3 nařízení (EU) 910/2014;
    c) oznámení o narušení bezpečnosti předaných podniky poskytujícími veřejné komunikační sítě nebo veřejně dostupné služby elektronických komunikací, které agentuře poskytly příslušné orgány podle článku 40 [směrnice, kterou se stanoví evropský kodex pro elektronické komunikace].

Článek 6

Úkoly týkající se budování kapacit

1. Agentura je nápomocna:

a) členským státům v jejich úsilí zdokonalovat prevenci, odhalování a analýzu kybernetických bezpečnostních problémů a incidentů a schopnost na ně reagovat, a to tím, že jim poskytuje nezbytné znalosti a odborné poznatky;

b) orgánům, institucím a jiným subjektům Unie v jejich úsilí zdokonalovat prevenci, odhalování a analýzu kybernetických bezpečnostních problémů a incidentů a schopnost na ně reagovat, a to tím, že poskytuje odpovídající podporu týmu CERT pro orgány, instituce a jiné subjekty Unie (CERT-EU);

c) členským státům na jejich žádost při budování vnitrostátních týmů pro reakci na počítačové bezpečnostní incidenty (CSIRT) podle čl. 9 odst. 5 směrnice (EU) 2016/1148;

d) členským státům na jejich žádost při vypracovávání národních strategií pro bezpečnost sítí a informačních systémů podle čl. 7 odst. 2 směrnice (EU) 2016/1148; agentura za účelem prosazování osvědčených postupů rovněž podporuje šíření těchto strategií v Unii a sleduje pokrok při jejich provádění;

e) orgánům Unie při vypracovávání a přezkumu strategií Unie týkajících se kybernetické bezpečnosti tím, že podporuje jejich šíření a sleduje pokrok při jejich provádění;

f) vnitrostátním a unijním týmům CSIRT při zvyšování úrovně jejich schopností, mimo jiné podporou dialogu a výměnou informací za účelem zajištění toho, aby s ohledem na aktuální stav každý tým CSIRT vykazoval společný soubor minimálních schopností a pracoval v souladu s osvědčenými postupy;

g) členským státům tím, že každý rok zorganizuje rozsáhlé cvičení v oblasti kybernetické bezpečnosti na úrovni EU podle čl. 7 odst. 6 a na základě vyhodnocení těchto cvičení a poznatků z těchto cvičení předloží politická doporučení;

h) příslušným veřejným orgánům tím, že jim nabídne školení v oblasti kybernetické bezpečnosti, případně ve spolupráci se zúčastněnými stranami;

i) skupině pro spolupráci tím, že podle čl. 11 odst. 3 písm. l) směrnice (EU) 2016/1148 zajišťuje výměnu osvědčených postupů, zejména pro určování provozovatelů základních služeb členskými státy, a to rovněž ve vztahu k přeshraničním vazbám, souvisejících s riziky a incidenty.

2. Agentura usnadňuje zřizování odvětvových středisek pro sdílení a analýzu informací (ISAC), zejména v odvětvích uvedených v příloze II směrnice (EU) 2016/1148, a průběžně je podporuje poskytováním osvědčených postupů a vydáváním pokynů k dostupným nástrojům a postupům, jakož i k řešení regulačních otázek týkajících se sdílení informací.

Článek 7

Úkoly týkající se operativní spolupráce na úrovni Unie

1. Agentura podporuje operativní spolupráci mezi příslušnými veřejnými orgány a mezi zúčastněnými stranami.

2. Agentura na operativní úrovni spolupracuje a vytváří synergie s orgány, institucemi a jinými subjekty Unie, včetně týmu CERT-EU, útvarů zabývajících se kyberkriminalitou a orgánů dozoru zabývajících se ochranou soukromí a osobních údajů, s cílem řešit otázky společného zájmu, včetně:

   a) výměny *know-how* a osvědčených postupů;

   b) poskytování poradenství a pokynů týkajících se příslušných otázek souvisejících s kyberkriminalitou;

   c) po konzultaci s Komisí zavádění praktických opatření pro výkon konkrétních úkolů.

3. Agentura zajistí služby sekretariátu sítě CSIRT podle čl. 12 odst. 2 směrnice (EU) 2016/1148 a aktivně usnadňuje sdílení informací a spolupráci mezi jejími členy.

4. Agentura přispívá k operativní spolupráci v rámci sítě CSIRT a poskytuje podporu členským státům tím, že:

   a) poskytuje poradenství, jak zlepšit jejich schopnosti předcházet, odhalovat a reagovat na incidenty;

   b) poskytuje na jejich žádost technickou pomoc v případě incidentů se závažným nebo významným dopadem;

   c) analyzuje zranitelnosti, artefakty a incidenty.

Při provádění těchto úkolů se agentura a tým CERT-EU zapojí do strukturované spolupráce, aby využily synergií, zejména pokud jde o operativní aspekty.

5. Na žádost jednoho nebo více dotčených členských států a výhradně pro účely poskytování poradenství ohledně předcházení budoucím incidentům agentura může provádět technická šetření ex post, nebo k nim poskytovat podporu, a to v návaznosti na oznámení dotčených podniků o incidentech se závažným nebo významným dopadem podle směrnice (EU) 2016/1148. V případě, že tyto incidenty mají dopad na více než dva členské státy, agentura toto šetření provede rovněž na řádně odůvodněnou žádost Komise po dohodě s dotčenými členskými státy.

   Rozsah šetření a postupy, jež se při provádění tohoto šetření použijí, schválí dotčené členské státy a agentura, přičemž tímto šetřením není dotčeno žádné probíhající trestní vyšetřování týkající se téhož incidentu. Šetření se uzavře závěrečnou technickou zprávou, kterou vypracuje agentura zejména na základě informací a připomínek, jež dotčené členské státy a podnik či podniky poskytly a s nimiž dotčené členské státy souhlasily. Shrnutí zprávy zaměřené na doporučení k předcházení budoucím incidentům je sdíleno se sítí CSIRT.

6. Agentura organizuje každoroční cvičení v oblasti kybernetické bezpečnosti na úrovni Unie a při organizování těchto cvičení podporuje členské státy a orgány, instituce a jiné subjekty EU, pokud o to požádají. Každoroční cvičení na úrovni Unie zahrnují technické, operativní a strategické prvky a pomáhají s přípravou koordinované reakce na úrovni Unie na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty.

Agentura případně rovněž přispívá k odvětvovým cvičením v oblasti kybernetické bezpečnosti a pomáhá je organizovat spolu s příslušnými středisky ISAC a dává střediskům ISAC povolení účastnit se rovněž cvičení v oblasti kybernetické bezpečnosti na úrovni Unie.

7. Agentura vypracovává pravidelnou technickou zprávu EU o situaci v oblasti kybernetické bezpečnosti týkající se incidentů a hrozeb na základě informací z otevřených zdrojů, vlastní analýzy a zpráv, které jí poskytly mimo jiné: týmy CSIRT členských států (na dobrovolném základě) nebo jednotná kontaktní místa podle směrnice o bezpečnosti sítí a informací (v souladu s čl. 14 odst. 5 směrnice o bezpečnosti sítí a informací); Evropským centrem pro boj proti kyberkriminalitě (EC3) při Europolu a týmem CERT-EU.

8. Agentura přispívá k vytváření koordinované reakce na úrovni Unie a členských států na rozsáhlé přeshraniční incidenty nebo krize související s kybernetickou bezpečností, a to především tím, že:

   a) agreguje zprávy z vnitrostátních zdrojů, aby přispěla k vytvoření společného povědomí o situaci;

   b) zajišťuje efektivní tok informací a poskytování eskalačních mechanismů mezi sítí CSIRT a osobami přijímajícími technická a politická rozhodnutí na úrovni Unie;

   c) podporuje technické řešení incidentů a krizí, včetně toho, že usnadňuje sdílení technických řešení mezi členskými státy;

   d) podporuje veřejnou komunikaci ohledně incidentu nebo krize;

   e) zkouší plány spolupráce pro reakci na tyto incidenty nebo krize.

Článek 8

Úkoly týkající se trhu, certifikace kybernetické bezpečnosti a normalizace

Agentura:

a) podporuje a prosazuje tvorbu a provádění politiky Unie v oblasti certifikace kybernetické bezpečnosti produktů a služeb IKT, jak je stanoveno v hlavě III tohoto nařízení, tím, že:

   1) vypracovává návrhy evropských systémů certifikace kybernetické bezpečnosti pro produkty a služby IKT v souladu s článkem 44 tohoto nařízení;

   2) je nápomocna Komisi při zajišťování služeb sekretariátu pro Evropskou skupinu pro certifikaci kybernetické bezpečnosti podle článku 53 tohoto nařízení;

   3) ve spolupráci s vnitrostátními orgány dozoru nad certifikací a odvětvím sestavuje a zveřejňuje pokyny a vypracovává osvědčené postupy týkající se požadavků na kybernetickou bezpečnost produktů a služeb IKT;

b) usnadňuje stanovení a zavádění evropských a mezinárodních norem pro řízení rizik a pro bezpečnost produktů a služeb IKT a ve spolupráci s členskými státy vydává podle čl. 19 odst. 2 směrnice (EU) 2016/1148 doporučení a pokyny týkající se technických oblastí souvisejících s bezpečnostními požadavky pro provozovatele základních služeb a poskytovatele digitálních služeb, jakož i s ohledem na již existující normy, včetně vnitrostátních norem členských států;

c) s cílem podpořit trh kybernetické bezpečnosti v Unii provádí pravidelné analýzy hlavních trendů na trhu kybernetické bezpečnosti, a to jak na straně poptávky, tak na straně nabídky, a šíří výsledky těchto analýz.

Článek 9

Úkoly týkající se znalostí, informací a zvyšování informovanosti

Agentura:

a) provádí analýzy nově vznikajících technologií a poskytuje tematicky zaměřená posouzení očekávaných společenských, právních, hospodářských a regulačních dopadů technologických inovací na kybernetickou bezpečnost;

b) provádí dlouhodobé strategické analýzy kybernetických bezpečnostních hrozeb a incidentů, aby zjišťovala nové trendy a pomáhala předcházet problémům souvisejícím s kybernetickou bezpečností;

c) ve spolupráci s odborníky z orgánů členských států poskytuje poradenství, pokyny a osvědčené postupy týkající se bezpečnosti sítí a informačních systémů, zejména bezpečnosti internetové infrastruktury a infrastruktur podporujících odvětví uvedená v příloze II směrnice (EU) 2016/1148;

d) shromažďuje, uspořádává a prostřednictvím specializovaného portálu zpřístupňuje veřejnosti informace o kybernetické bezpečnosti poskytnuté orgány, institucemi a jinými subjekty Unie;

e) zvyšuje informovanost veřejnosti ohledně kybernetických bezpečnostních rizik a poskytuje pokyny týkající se osvědčených postupů pro jednotlivé uživatele zaměřené na občany a organizace;

f) shromažďuje a analyzuje veřejně dostupné informace o závažných incidentech a sestavuje zprávy s cílem poskytnout pokyny podnikům a občanům v celé Unii;

g) ve spolupráci s členskými státy a orgány, institucemi a jinými subjekty Unie organizuje pravidelné informační kampaně za účelem zvýšení kybernetické bezpečnosti a jejího zviditelnění v Unii.

Článek 10

Úkoly týkající se výzkumu a inovací

Ve vztahu k výzkumu a inovacím agentura:

a) poskytuje Unii a členským státům poradenství ohledně potřeb a priorit výzkumu v oblasti kybernetické bezpečnosti s cílem umožnit účinnou reakci na současná a nově vznikající rizika a hrozby, a to i pokud jde o nové a nově vznikající informační a komunikační technologie, a efektivně využívat technologie pro prevenci rizik;

b) pokud na ni Komise přenesla příslušné pravomoci, účastní se prováděcí fáze programů financování výzkumu a inovací, nebo je jejich příjemcem.

Článek 11
Úkoly týkající se mezinárodní spolupráce

Agentura přispívá k úsilí Unie zaměřenému na spolupráci se třetími zeměmi a mezinárodními organizacemi v zájmu prosazení mezinárodní spolupráce v otázkách týkajících se kybernetické bezpečnosti tím, že:

a) se případně angažuje jako pozorovatel při organizování mezinárodních cvičení, provádí analýzu jejich výsledků a předkládá o nich zprávu správní radě;

b) na žádost Komise usnadňuje výměnu osvědčených postupů mezi příslušnými mezinárodními organizacemi;

c) na žádost Komisi poskytuje odborné poznatky.

KAPITOLA II
ORGANIZACE AGENTURY

Článek 12
Struktura

Správní a řídicí struktura agentury se skládá:

a) ze správní rady, která plní funkce stanovené v článku 14;

b) z výkonné rady, která plní funkce stanovené v článku 18;

c) z výkonného ředitele, který plní povinnosti stanovené v článku 19, a

d) ze stálé skupiny zúčastněných stran, která plní funkce stanovené v článku 20.

ODDÍL 1
SPRÁVNÍ RADA

Článek 13
Složení správní rady

1. Správní radu tvoří jeden zástupce každého členského státu a dva zástupci jmenovaní Komisí. Všichni zástupci mají hlasovací právo.

2. Každý člen správní rady má náhradníka, který jej zastupuje v případě jeho nepřítomnosti.

3. Členové správní rady a jejich náhradníci jsou jmenováni na základě svých znalostí problematiky kybernetické bezpečnosti a s ohledem na své dovednosti v oblasti řízení, správy a rozpočtu. Komise a členské státy usilují o to, aby se omezila fluktuace jejich zástupců ve správní radě, a zajistila se tak kontinuita práce rady. Komise a členské státy usilují o dosažení vyváženého zastoupení mužů a žen ve správní radě.

4. Funkční období členů správní rady a jejich náhradníků je čtyři roky. Toto období lze prodloužit.

Článek 14
Funkce správní rady

1. Správní rada:

a) stanoví obecné směry činnosti agentury a rovněž zajišťuje, aby agentura pracovala v souladu s předpisy a zásadami stanovenými v tomto nařízení. Rovněž zajišťuje, aby práce agentury byla v souladu s činnostmi členských států a na úrovni Unie;

b) přijímá návrh jednotného programového dokumentu agentury podle článku 21 před jeho předložením Komisi k vyjádření stanoviska;

c) s ohledem na stanovisko Komise přijímá dvoutřetinovou většinou hlasů svých členů a v souladu s článkem 17 jednotný programový dokument agentury;

d) přijímá dvoutřetinovou většinou hlasů svých členů roční rozpočet agentury a vykonává další funkce ve vztahu k rozpočtu agentury podle kapitoly III;

e) posuzuje a přijímá souhrnnou výroční zprávu o činnosti agentury a do 1. července následujícího roku zprávu a její posouzení zašle Evropskému parlamentu, Radě, Komisi a Účetnímu dvoru. Výroční zpráva obsahuje účetní výkaz a popisuje, nakolik agentura naplnila ukazatele výkonnosti. Výroční zpráva se zveřejňuje;

f) přijímá finanční pravidla použitelná na agenturu v souladu s článkem 29;

g) přijímá strategii proti podvodům, která je úměrná rizikům podvodu s ohledem na analýzy nákladů a přínosů opatření, jež mají být provedena;

h) přijímá pravidla pro předcházení střetům zájmů a řešení těchto střetů u svých členů;

i) zajišťuje náležitá opatření v návaznosti na zjištění a doporučení vyplývající z šetření Evropského úřadu pro boj proti podvodům (OLAF) a z různých interních či externích auditních zpráv a hodnocení;

j) přijímá svůj jednací řád;

k) v souladu s odstavcem 2 vykonává ve vztahu k zaměstnancům agentury pravomoci, které služební řád úředníků svěřuje orgánu oprávněnému ke jmenování a které pracovní řád ostatních zaměstnanců Evropské unie svěřuje orgánu oprávněnému uzavírat pracovní smlouvy (dále jen „pravomoci orgánu oprávněného ke jmenování“);

l) přijímá prováděcí pravidla ke služebnímu řádu a pracovnímu řádu ostatních zaměstnanců v souladu s postupem podle článku 110 služebního řádu;

m) jmenuje výkonného ředitele a případně prodlužuje jeho funkční období nebo jej odvolává z funkce v souladu s článkem 33 tohoto nařízení;

n) jmenuje účetního, který může být účetním Komise a který je při plnění svých povinností naprosto nezávislý;

o) přijímá veškerá rozhodnutí o zřízení vnitřních struktur agentury a o jejich případných změnách s ohledem na potřeby činností agentury a na řádné rozpočtové řízení;

p) povoluje uzavírání pracovních ujednání v souladu s články 7 a 39.

2. Správní rada přijme v souladu s článkem 110 služebního řádu rozhodnutí na základě čl. 2 odst. 1 služebního řádu a článku 6 pracovního řádu ostatních zaměstnanců, kterým přenese příslušné pravomoci orgánu oprávněného ke jmenování na výkonného ředitele a kterým stanoví podmínky, za nichž může být toto přenesení pravomocí pozastaveno. Výkonný ředitel je oprávněn přenést tyto pravomoci na další osoby.

3. Vyžadují-li to zvláštní okolnosti, může správní rada rozhodnout o dočasném pozastavení přenesení pravomocí orgánu oprávněného ke jmenování na výkonného ředitele a pravomocí jím přenesených na další osoby a vykonávat je sama, případně je přenést na jednoho ze svých členů nebo na zaměstnance, který zároveň není výkonným ředitelem.

Článek 15
Předseda správní rady

Správní rada si dvoutřetinovou většinou hlasů svých členů zvolí z řad svých členů předsedu a místopředsedu na období čtyř let, které lze jednou prodloužit. Pokud však v průběhu jejich funkčního období jejich členství ve správní radě skončí, zanikne týmž dnem automaticky i jejich funkce předsedy či místopředsedy. Nemůže-li předseda vykonávat své povinnosti, zaujme jeho místo z moci úřední místopředseda.

Článek 16
Zasedání správní rady

1. Zasedání správní rady svolává její předseda.

2. Řádná zasedání správní rady se konají alespoň dvakrát za rok. Z podnětu předsedy, z podnětu Komise nebo na žádost nejméně jedné třetiny členů správní rady se konají

3. Zasedání správní rady se bez hlasovacího práva účastní výkonný ředitel.

4. Zasedání správní rady se na pozvání předsedy mohou bez hlasovacího práva účastnit členové stálé skupiny zúčastněných stran.

5. Členům správní rady a jejich náhradníkům mohou být v souladu s jednacím řádem na zasedáních nápomocni poradci nebo odborníci.

6. Služby sekretariátu pro správní radu zajišťuje agentura.

Článek 17
Pravidla hlasování ve správní radě

1. Správní rada přijímá rozhodnutí absolutní většinou hlasů svých členů.

2. Pro přijetí jednotného programového dokumentu a ročního rozpočtu a pro jmenování, prodloužení funkčního období nebo odvolání výkonného ředitele je nutná dvoutřetinová většina hlasů všech členů správní rady.

3. Každý člen má jeden hlas. V nepřítomnosti člena je k výkonu hlasovacího práva oprávněn jeho náhradník.

4. Předseda se hlasování účastní.

5. Výkonný ředitel se hlasování neúčastní.

6. Jednací řád správní rady stanoví podrobnější pravidla hlasování, zejména podmínky, za nichž může člen zastupovat jiného člena.

ODDÍL 2
VÝKONNÁ RADA

Článek 18
Výkonná rada

1. Správní radě je nápomocna výkonná rada.
2. Výkonná rada:
   a) připravuje rozhodnutí přijímaná správní radou;
   b) společně se správní radou zajistí náležitá opatření v návaznosti na zjištění a doporučení vyplývající z šetření úřadu OLAF a z různých interních či externích auditních zpráv a hodnocení;
   c) aniž jsou dotčeny povinnosti výkonného ředitele stanovené v článku 19, je nápomocna výkonnému řediteli a radí mu, pokud jde o provádění rozhodnutí správní rady v administrativních a rozpočtových záležitostech podle článku 19.
3. Výkonná rada se skládá z pěti členů jmenovaných z řad členů správní rady, z nichž jedním je předseda správní rady, který smí předsedat i výkonné radě, a dalším jeden ze zástupců Komise. Výkonný ředitel se účastní zasedání výkonné rady, avšak nemá hlasovací právo.
4. Funkční období členů výkonné rady je čtyři roky. Toto období lze prodloužit.
5. Zasedání výkonné rady se koná alespoň jednou za tři měsíce. Předseda výkonné rady svolává další zasedání na žádost členů této rady.
6. Správní rada stanoví jednací řád výkonné rady.
7. Je-li to z naléhavých důvodů nezbytné, může výkonná rada přijmout určitá prozatímní rozhodnutí jménem správní rady, zejména ve věcech správního řízení, včetně pozastavení přenesení pravomocí orgánu oprávněného ke jmenování, a v rozpočtových záležitostech.

ODDÍL 3
VÝKONNÝ ŘEDITEL

Článek 19
Povinnosti výkonného ředitele

1. Agenturu řídí výkonný ředitel, který je při výkonu svých povinností nezávislý. Výkonný ředitel se zodpovídá správní radě.
2. Výkonný ředitel předkládá Evropskému parlamentu na jeho žádost zprávu o plnění svých povinností. Rada může výkonného ředitele vyzvat, aby o plnění svých povinností předložil zprávu.
3. Výkonný ředitel je odpovědný za:

a) běžnou správu agentury;

b) provádění rozhodnutí přijatých správní radou;

c) vypracování návrhu jednotného programového dokumentu a jeho předložení správní radě ke schválení před jeho předložením Komisi;

d) provádění jednotného programového dokumentu a podávání zpráv o jeho provádění správní radě;

e) vypracování souhrnné výroční zprávy o činnosti agentury a předložení této zprávy správní radě k posouzení a přijetí;

f) vypracování akčního plánu v návaznosti na závěry zpětných hodnocení a zprávy o pokroku, kterou předkládá každé dva roky Komisi;

g) vypracování akčního plánu v návaznosti na závěry zpráv o interním nebo externím auditu, jakož i na šetření Evropského úřadu pro boj proti podvodům (OLAF), a dvakrát za rok předložení zprávy o pokroku Komisi a pravidelně správní radě;

h) vypracování návrhu finančních pravidel použitelných na agenturu;

i) vypracování návrhu odhadu příjmů a výdajů agentury a za plnění jejího rozpočtu;

j) ochranu finančních zájmů Unie uplatňováním preventivních opatření proti podvodům, korupci a jakýmkoli jiným protiprávním jednáním, účinnými kontrolami a zpětným získáním nesprávně vyplacených částek v případech, kdy jsou zjištěny nesrovnalosti, a případně účinnými, přiměřenými a odrazujícími správními a finančními sankcemi;

k) vypracování strategie agentury pro boj proti podvodům a její předložení správní radě ke schválení;

l) rozvíjení a udržování styků s podnikatelským sektorem a organizacemi spotřebitelů pro zajištění pravidelného dialogu s příslušnými zúčastněnými stranami;

m) jiné úkoly, které jsou výkonnému řediteli uloženy tímto nařízením.

4. Výkonný ředitel může v případě potřeby, v rámci mandátu agentury a v souladu s cíli a úkoly agentury zřizovat pracovní skupiny ad hoc složené z odborníků, mimo jiné z odborníků příslušných orgánů členských států. V předstihu o tom informuje správní radu. Postupy týkající se zejména složení pracovních skupin, jmenování odborníků pracovních skupin výkonným ředitelem a činnosti pracovních skupin jsou stanoveny ve vnitřních organizačních předpisech agentury.

5. Výkonný ředitel rozhodne, zda je nezbytné umístit jednoho či více zaměstnanců v jednom nebo více členských státech za účelem účinného a efektivního provádění úkolů agentury. Před rozhodnutím o zřízení místního úřadu výkonný ředitel získá předchozí souhlas Komise, správní rady a dotčeného členského státu nebo států. Uvedeným rozhodnutím se určí rozsah činností, jež mají být v daném místním úřadu prováděny, způsobem, který zabrání zbytečným nákladům a zdvojování správních

funkcí agentury. V příslušném případě nebo v případě nutnosti se s dotčeným členským státem nebo státy uzavře dohoda.

ODDÍL 4
STÁLÁ SKUPINA ZÚČASTNĚNÝCH STRAN

Článek 20
Stálá skupina zúčastněných stran

1. Správní rada na návrh výkonného ředitele ustaví stálou skupinu zúčastněných stran složenou z uznávaných odborníků zastupujících příslušné zúčastněné strany, jako jsou odvětví informačních a komunikačních technologií, poskytovatelé veřejně dostupných sítí nebo služeb elektronických komunikací, organizace spotřebitelů, akademičtí odborníci v oblasti kybernetické bezpečnosti a zástupci příslušných orgánů oznámených podle [směrnice, kterou se stanoví evropský kodex pro elektronické komunikace] i donucovacích orgánů a orgánů dozoru pro ochranu údajů.
2. Postupy týkající se stálé skupiny zúčastněných stran, zejména počtu, složení a jmenování jejích členů správní radou, návrhu výkonného ředitele a činnosti skupiny jsou stanoveny ve vnitřních organizačních předpisech agentury a jsou zveřejňovány.
3. Stálé skupině zúčastněných stran předsedá výkonný ředitel nebo osoba, kterou výkonný ředitel pro danou záležitost určí.
4. Funkční období členů stálé skupiny zúčastněných stran je dva a půl roku. Členy stálé skupiny zúčastněných stran nesmějí být členové správní rady. Odborníci z řad Komise a členských států jsou oprávněni účastnit se zasedání a podílet se na činnosti stálé skupiny zúčastněných stran. K účasti na zasedáních a na činnosti stálé skupiny zúčastněných stran mohou být přizváni zástupci dalších subjektů, kteří nejsou členy stálé skupiny zúčastněných stran a jejichž účast považuje výkonný ředitel za důležitou.
5. Stálá skupina zúčastněných stran poskytuje agentuře poradenství při výkonu jejích činností. Radí zejména výkonnému řediteli při vypracovávání návrhu pracovního programu agentury a při zajišťování komunikace s příslušnými zúčastněnými stranami ve všech otázkách souvisejících s pracovním programem.

ODDÍL 5
ČINNOST

Článek 21
Jednotný programový dokument

1. Agentura vykonává svou činnost v souladu s jednotným programovým dokumentem obsahujícím její víceletý a roční program, který obsahuje všechny plánované aktivity.
2. Výkonný ředitel každý rok vypracuje návrh jednotného programového dokumentu, který obsahuje roční a víceletý program spolu s odpovídajícím plánem lidských

a finančních zdrojů v souladu s článkem 32 nařízení Komise v přenesené pravomoci (EU) č. 1271/2013[36], přičemž zohlední pokyny stanovené Komisí.

3. Jednotný programový dokument uvedený v odstavci 1 přijme správní rada do 30. listopadu každého roku a předá jej Evropskému parlamentu, Radě a Komisi do 31. ledna následujícího roku; to se týká i všech pozdějších aktualizovaných verzí tohoto dokumentu.

4. Jednotný programový dokument nabývá definitivní podoby po konečném přijetí souhrnného rozpočtu Unie a v případě potřeby se odpovídajícím způsobem upraví.

5. Roční pracovní program obsahuje podrobné cíle a očekávané výsledky včetně ukazatelů výkonnosti. Obsahuje rovněž popis opatření, která mají být financována, a stanovení finančních a lidských zdrojů, které jsou na jednotlivá opatření přiděleny, v souladu se zásadami sestavování rozpočtu a řízení podle činností. Roční pracovní program musí být v souladu s víceletým pracovním programem uvedeným v odstavci 7. Je v něm jasně uvedeno, jaké úkoly byly ve srovnání s předchozím rozpočtovým rokem přidány, změněny nebo zrušeny.

6. Je-li agentuře svěřen nový úkol, správní rada přijatý roční pracovní program změní. Každá podstatná změna ročního pracovního programu se přijme stejným postupem jako původní roční pracovní program. Správní rada může přenést pravomoc k provádění nepodstatných změn ročního pracovního programu na výkonného ředitele.

7. Víceletý pracovní program stanoví celkový strategický plán včetně cílů, očekávaných výsledků a ukazatelů výkonnosti. Stanoví rovněž plán zdrojů včetně víceletého rozpočtu a zaměstnanců.

8. Plán zdrojů je jednou ročně aktualizován. Strategický plán je aktualizován podle potřeby, a zejména je-li nutno zohlednit výsledek hodnocení uvedeného v článku 56.

Článek 22
Prohlášení o zájmech

1. Členové správní rady, výkonný ředitel a úředníci dočasně přidělení členskými státy učiní prohlášení o závazcích a prohlášení, z něhož vyplývá, že neexistují, nebo naopak existují přímé či nepřímé zájmy, které by bylo možné považovat za zájmy ovlivňující jejich nezávislost. Tato prohlášení musí být správná a úplná, musí být podávána každoročně písemnou formou a v případě potřeby aktualizována.

2. Členové správní rady, výkonný ředitel a externí odborníci, kteří spolupracují na činnosti pracovních skupin ad hoc, učiní nejpozději na začátku každého zasedání pravdivé a úplné prohlášení o zájmech, které by bylo možné považovat za zájmy ovlivňující jejich nezávislost vzhledem k bodům na pořadu jednání, a neúčastní se jednání a hlasování o těchto bodech.

---

[36] Nařízení Komise v přenesené pravomoci (EU) č. 1271/2013 ze dne 30. září 2013 o rámcovém finančním nařízení pro subjekty uvedené v článku 208 nařízení Evropského parlamentu a Rady (EU, Euratom) č. 966/2012 (Úř. věst. L 328, 7.12.2013, s. 42).

3. Agentura ve svých vnitřních organizačních předpisech stanoví praktická opatření upravující pravidla týkající se prohlášení o zájmech podle odstavců 1 a 2.

Článek 23
Transparentnost

1. Agentura vykonává své činnosti s vysokou mírou transparentnosti a v souladu s článkem 25.
2. Agentura zajistí, aby veřejnost a všechny zainteresované strany měly k dispozici náležité, objektivní, spolehlivé a snadno dostupné informace, zejména s ohledem na výsledky její činnosti. Zveřejní rovněž prohlášení o zájmech učiněná v souladu s článkem 22.
3. Správní rada může na návrh výkonného ředitele zainteresovaným stranám umožnit, aby se účastnily projednání některých činností agentury jako pozorovatelé.
4. Agentura ve svých vnitřních organizačních předpisech stanoví praktická opatření pro provádění pravidel transparentnosti podle odstavců 1 a 2.

Článek 24
Důvěrnost

1. Aniž je dotčen článek 25, agentura nesděluje třetím osobám informace, které zpracovává nebo které obdržela a pro které bylo odůvodněně vyžádáno zcela či částečně důvěrné zacházení.
2. Členové správní rady, výkonný ředitel, členové stálé skupiny zúčastněných stran, externí odborníci účastnící se pracovních skupin ad hoc a zaměstnanci agentury, včetně úředníků dočasně přidělených členskými státy, jsou povinni i po skončení svých funkcí dodržovat požadavky na důvěrnost podle článku 339 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“).
3. Agentura ve svých vnitřních organizačních předpisech stanoví praktická opatření pro provádění pravidel důvěrnosti podle odstavců 1 a 2.
4. Pokud je to třeba pro vykonávání úkolů agentury, správní rada rozhodne, že agentuře umožní zpracovávat utajované informace. Správní rada v tomto případě po dohodě s útvary Komise přijme vnitřní organizační předpisy, v nichž se uplatňují bezpečnostní zásady stanovené v rozhodnutích Komise (EU, Euratom) 2015/443[37] a 2015/444[38]. Tyto předpisy musí zahrnovat ustanovení o výměně, zpracování a ukládání utajovaných informací.

Článek 25
Přístup k dokumentům

1. Na dokumenty, které má agentura v držení, se vztahuje nařízení (ES) č. 1049/2001.

---

37 Rozhodnutí Komise (EU, Euratom) 2015/443 ze dne 13. března 2015 o bezpečnosti v Komisi (Úř. věst. L 72, 17.3.2015, s. 41).

38 Rozhodnutí Komise (EU, Euratom) 2015/444 ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU (Úř. věst. L 72, 17.3.2015, s. 53).

2. Správní rada přijme do šesti měsíců od zřízení agentury prováděcí pravidla k nařízení (ES) č. 1049/2001.

3. Proti rozhodnutím přijatým agenturou podle článku 8 nařízení (ES) č. 1049/2001 lze podat stížnost veřejnému ochránci práv za podmínek stanovených v článku 228 Smlouvy o fungování EU nebo žalobu k Soudnímu dvoru Evropské unie za podmínek stanovených v článku 263 Smlouvy o fungování EU.

KAPITOLA III
SESTAVOVÁNÍ A SKLADBA ROZPOČTU

Článek 26
Sestavování rozpočtu

1. Výkonný ředitel každý rok vypracuje návrh odhadu příjmů a výdajů agentury pro následující rozpočtový rok a spolu s návrhem plánu pracovních míst jej předá správní radě. Příjmy a výdaje musí být vyrovnané.

2. Správní rada každý rok sestaví na základě návrhu odhadu příjmů a výdajů uvedeného v odstavci 1 odhad příjmů a výdajů agentury pro následující rozpočtový rok.

3. Správní rada zašle každý rok do 31. ledna návrh odhadu uvedený v odstavci 2, který je součástí návrhu jednotného programového dokumentu, Komisi a třetím zemím, s nimiž Unie uzavřela dohody v souladu s článkem 39.

4. Komise na základě tohoto odhadu zanese do návrhu rozpočtu Unie odhady, které považuje za nezbytné pro plán pracovních míst, a výši příspěvku ze souhrnného rozpočtu a předloží je Evropskému parlamentu a Radě v souladu s články 313 a 314 Smlouvy o fungování EU.

5. Evropský parlament a Rada schvalují prostředky příspěvku pro agenturu.

6. Evropský parlament a Rada přijmou plán pracovních míst agentury.

7. Správní rada přijme rozpočet agentury spolu s jednotným programovým dokumentem. Rozpočet agentury se stává konečným po přijetí souhrnného rozpočtu Unie. Správní rada rozpočet a jednotný programový dokument agentury případně upraví v souladu se souhrnným rozpočtem Unie.

Článek 27
Skladba rozpočtu

1. Aniž jsou dotčeny jiné zdroje, příjmy agentury zahrnují:

   a) příspěvek z rozpočtu Unie;

   b) příjmy účelově vázané na konkrétní položky výdajů v souladu s finančními pravidly uvedenými v článku 29;

   c) finanční prostředky Unie ve formě dohod o přiznání příspěvku nebo grantů *ad hoc* v souladu s jejími finančními předpisy uvedenými v článku 29 a ustanoveními příslušných nástrojů na podporu politik Unie;

d) příspěvky třetích zemí, které se podílejí na činnosti agentury na základě článku 39;

e) dobrovolné finanční či věcné příspěvky členských států; členské státy, které poskytují dobrovolné příspěvky, nesmí na základě tohoto příspěvku požadovat žádné zvláštní právo nebo službu.

2. Výdaje agentury zahrnují výdaje na zaměstnance, správu, technickou podporu, infrastrukturu a provoz a výdaje vyplývající ze smluv uzavřených s třetími stranami.

Článek 28
Plnění rozpočtu

1. Za plnění rozpočtu agentury je odpovědný výkonný ředitel.

2. Interní auditor Komise vykonává ve vztahu k agentuře stejné pravomoci jako ve vztahu k útvarům Komise.

3. Účetní agentury zašle do 1. března následujícího rozpočtového roku (1. března roku N+1) předběžnou účetní závěrku účetnímu Komise a Účetnímu dvoru.

4. Po obdržení připomínek Účetního dvora k předběžné účetní závěrce agentury vypracuje účetní agentury na vlastní odpovědnost konečnou účetní závěrku agentury.

5. Výkonný ředitel předloží konečnou účetní závěrku k vyjádření správní radě.

6. Výkonný ředitel zašle do 31. března roku N+1 zprávu o rozpočtovém a finančním řízení Evropskému parlamentu, Radě, Komisi a Účetnímu dvoru.

7. Účetní předá konečnou účetní závěrku spolu se stanoviskem správní rady do 1. července roku N+1 Evropskému parlamentu, Radě, účetnímu Komise a Účetnímu dvoru.

8. Účetní ke stejnému datu, k němuž předal konečnou účetní závěrku, rovněž zašle Účetnímu dvoru prohlášení vedení k této konečné účetní závěrce a jedno vyhotovení zašle účetnímu Komise.

9. Výkonný ředitel konečnou účetní závěrku zveřejní do 15. listopadu následujícího roku.

10. Výkonný ředitel odpoví Účetnímu dvoru na jeho připomínky do 30. září roku N + 1 a jedno vyhotovení této odpovědi rovněž zašle správní radě a Komisi.

11. Výkonný ředitel předloží Evropskému parlamentu na jeho žádost veškeré informace nezbytné pro řádný průběh udělení absolutoria za daný rozpočtový rok v souladu s čl. 165 odst. 3 finančního nařízení.

12. Absolutorium za plnění rozpočtu na rok N udělí Evropský parlament výkonnému řediteli na základě doporučení Rady do 15. května roku N + 2.

Článek 29
Finanční pravidla

Správní rada přijme po konzultaci s Komisí finanční pravidla použitelná na agenturu. Tato pravidla se mohou odchýlit od nařízení (EU) č. 1271/2013, pouze pokud je to nezbytné pro zvláštní potřeby činnosti agentury, a s předchozím souhlasem Komise.

Článek 30
Boj proti podvodům

1. V zájmu usnadnění boje proti podvodům, úplatkářství a jinému protiprávnímu jednání podle nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013[39] agentura během šesti měsíců od zahájení činnosti přistoupí k interinstitucionální dohodě ze dne 25. května 1999 o vnitřním vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) a přijme příslušná ustanovení vztahující se na veškeré zaměstnance agentury, přičemž použije šablonu stanovenou v příloze uvedené dohody.

2. Účetní dvůr má pravomoc provádět na základě kontroly dokumentů a inspekce na místě audit u všech příjemců grantů, zhotovitelů, dodavatelů nebo poskytovatelů a subdodavatelů, kteří od agentury obdrželi finanční prostředky Unie.

3. Úřad OLAF smí provádět šetření, včetně kontrol a inspekcí na místě, v souladu s ustanoveními a postupy uvedenými v nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 a v nařízení Rady (Euratom, ES) č. 2185/96[40] ze dne 11. listopadu 1996 o kontrolách a inspekcích na místě prováděných Komisí za účelem ochrany finančních zájmů Evropských společenství proti podvodům a jiným nesrovnalostem, aby se zjistilo, zda v souvislosti s grantem nebo zakázkou financovanou ze strany agentury nedošlo k podvodu, úplatkářství nebo jinému protiprávnímu jednání ohrožujícímu finanční zájmy Unie.

4. Aniž jsou dotčeny odstavce 1, 2 a 3, musí dohody o spolupráci se třetími zeměmi a mezinárodními organizacemi, smlouvy, grantové dohody a rozhodnutí o udělení grantu přijatá agenturou obsahovat ustanovení, která výslovně zmocňují Účetní dvůr a úřad OLAF k provádění těchto auditů a šetření v souladu s jejich příslušnými pravomocemi.

KAPITOLA IV
ZAMĚSTNANCI AGENTURY

Článek 31
Obecná ustanovení

Na zaměstnance agentury se vztahuje služební řád a pracovní řád ostatních zaměstnanců a pravidla přijatá na základě dohody mezi orgány Unie k provedení tohoto služebního řádu.

Článek 32
Výsady a imunita

Na agenturu a její zaměstnance se vztahuje Protokol č. 7 o výsadách a imunitách Evropské unie, připojený ke Smlouvě o Evropské unii a ke Smlouvě o fungování EU.

---

39 Nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 ze dne 11. září 2013 o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1073/1999 a nařízení Rady (Euratom) č. 1074/1999 (Úř. věst. L 248, 18.9.2013, s. 1).

40 Nařízení Rady (Euratom, ES) č. 2185/96 ze dne 11. listopadu 1996 o kontrolách a inspekcích na místě prováděných Komisí za účelem ochrany finančních zájmů Evropských společenství proti podvodům a jiným nesrovnalostem (Úř. věst. L 292, 15.11.1996, s. 2).

Článek 33

Výkonný ředitel

1. Výkonný ředitel je zaměstnán jako dočasný zaměstnanec agentury podle čl. 2 písm. a) pracovního řádu ostatních zaměstnanců.

2. Výkonného ředitele jmenuje po otevřeném a transparentním výběrovém řízení správní rada ze seznamu kandidátů navržených Komisí.

3. Pro účely uzavření smlouvy s výkonným ředitelem je agentura zastoupena předsedou správní rady.

4. Před jmenováním je kandidát zvolený správní radou vyzván, aby před příslušným výborem Evropského parlamentu učinil prohlášení a zodpověděl otázky jeho členů.

5. Funkční období výkonného ředitele je pět let. Do konce tohoto období Komise provede posouzení, které zohlední hodnocení výsledků výkonného ředitele a budoucí úkoly a výzvy agentury.

6. Správní rada přijímá rozhodnutí o jmenování, prodloužení funkčního období nebo odvolání výkonného ředitele dvoutřetinovou většinou hlasů svých členů s hlasovacím právem.

7. Správní rada může na návrh Komise, v němž je zohledněno posouzení podle odstavce 5, funkční období výkonného ředitele jednou prodloužit o další období nejvýše pěti let.

8. Správní rada informuje o svém záměru prodloužit funkční období výkonného ředitele Evropský parlament. Je-li výkonný ředitel vyzván, učiní do tří měsíců před tímto prodloužením prohlášení před příslušným výborem Evropského parlamentu a zodpoví otázky jeho členů.

9. Výkonný ředitel, jehož funkční období bylo prodlouženo, se nesmí účastnit dalšího výběrového řízení na tutéž pozici.

10. Výkonný ředitel může být odvolán z funkce pouze na základě rozhodnutí správní rady jednající na návrh Komise.

Článek 34

Vyslaní národní odborníci a další pracovníci

1. Agentura může využívat vyslané národní odborníky nebo jiné pracovníky, kteří nejsou v agentuře zaměstnáni. Na tyto pracovníky se nevztahuje služební řád ani pracovní řád ostatních zaměstnanců.

2. Správní rada přijme rozhodnutí, kterým stanoví pravidla pro vysílání národních odborníků do agentury.

KAPITOLA V
OBECNÁ USTANOVENÍ

Článek 35
Právní status agentury

1. Agentura je institucí Unie a má právní subjektivitu.
2. Agentura má v každém členském státě nejširší způsobilost k právním úkonům, kterou vnitrostátní právo daného členského státu přiznává právnickým osobám. Zejména může nabývat a zcizovat movitý a nemovitý majetek a vystupovat před soudem, nebo obojí.
3. Agenturu zastupuje její výkonný ředitel.

Článek 36
Odpovědnost agentury

1. Smluvní odpovědnost agentury se řídí právem rozhodným pro danou smlouvu.
2. Soudní dvůr Evropské unie má pravomoc rozhodovat na základě jakékoli rozhodčí doložky obsažené ve smlouvě uzavřené agenturou.
3. V případě mimosmluvní odpovědnosti nahradí agentura v souladu s obecnými zásadami, které jsou společné právním řádům členských států, škodu, kterou způsobí ona nebo její zaměstnanci při výkonu svých povinností.
4. Soudní dvůr Evropské unie má pravomoc rozhodovat veškeré spory o náhradu této škody.
5. Osobní odpovědnost zaměstnanců vůči agentuře se řídí odpovídajícími předpisy vztahujícími se na zaměstnance agentury.

Článek 37
Jazykový režim

1. Na agenturu se vztahuje nařízení Rady č. 1[41]. Členské státy a ostatní jimi jmenované subjekty se mohou na agenturu obracet a přijímat odpovědi v libovolném úředním jazyce orgánů Unie.
2. Překladatelské služby potřebné pro činnost agentury poskytuje Překladatelské středisko pro instituce Evropské unie.

Článek 38
Ochrana osobních údajů

1. Zpracování osobních údajů agenturou se řídí nařízením Evropského parlamentu a Rady (ES) č. 45/2001[42].

---

41 Nařízení č. 1 o užívání jazyků v Evropském společenství pro atomovou energii (Úř. věst. 17, 6.10.1958, s. 401).

2. Správní rada přijme prováděcí opatření uvedená v čl. 24 odst. 8 nařízení (ES) č. 45/2001. Správní rada může přijmout další opatření nezbytná pro uplatňování nařízení (ES) č. 45/2001 ze strany agentury.

Článek 39

Spolupráce s třetími zeměmi a mezinárodními organizacemi

1. Je-li to nezbytné pro dosažení cílů uvedených v tomto nařízení, může agentura spolupracovat s příslušnými orgány třetích zemí, s mezinárodními organizacemi nebo s oběma. Za tímto účelem může agentura po předchozím schválení Komisí uzavřít s orgány třetích zemí a s mezinárodními organizacemi pracovní ujednání. Z těchto ujednání nevyplývají pro Unii ani její členské státy žádné právní závazky.

2. Agentura je otevřena účasti třetích zemí, které za tímto účelem uzavřely dohody s Unií. Na základě příslušných ustanovení těchto dohod budou vytvořena ujednání, která určí zejména povahu, rozsah a způsob účasti těchto zemí na činnosti agentury, včetně ustanovení týkajících se účasti na iniciativách agentury, finančních příspěvků a zaměstnanců. Pokud jde o záležitosti týkající se zaměstnanců, musí být tato ujednání v každém případě v souladu se služebním řádem.

3. Správní rada přijme strategii pro vztahy se třetími zeměmi nebo mezinárodními organizacemi v otázkách, které spadají do oblasti působnosti agentury. Komise zajistí, aby agentura působila v mezích svého mandátu a stávajícího institucionálního rámce tím, že s výkonným ředitelem agentury uzavře příslušné pracovní ujednání.

Článek 40

Bezpečnostní předpisy týkající se ochrany utajovaných informací a citlivých informací nepodléhajících utajení

Po konzultaci s Komisí agentura přijme své bezpečnostní předpisy uplatňující bezpečnostní zásady obsažené v bezpečnostních pravidlech Komise pro ochranu utajovaných informací Evropské unie (EUCI) a citlivých informací nepodléhajících utajení, která jsou stanovena v rozhodnutích Komise (EU, Euratom) 2015/443 a 2015/444. To se kromě jiného vztahuje na ustanovení o výměně, zpracování a ukládání těchto informací.

Článek 41

Dohoda o sídle a provozní podmínky

1. Nezbytná ujednání související s umístěním agentury v hostitelském členském státě a s prostory, které tento členský stát dává k dispozici, a zvláštní pravidla, která se v hostitelském členském státě vztahují na výkonného ředitele, členy správní rady, zaměstnance agentury a jejich rodinné příslušníky, se stanoví v dohodě o sídle uzavřené mezi agenturou a členským státem, kde se sídlo nachází, poté, co k tomu správní rada dá souhlas, nejpozději však [dva roky po vstupu tohoto nařízení v platnost].

2. Hostitelský členský stát agentury poskytne nejlepší možné podmínky pro zajištění řádného fungování agentury, včetně přístupnosti lokality, existence vhodných vzdělávacích zařízení pro děti zaměstnanců, patřičného přístupu na pracovní trh,

---

[42] Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

sociálního zabezpečení a zdravotní péče pro děti i pro manžely a manželky zaměstnanců.

Článek 42
Správní kontrola

Na činnost agentury dohlíží veřejný ochránce práv v souladu s článkem 228 Smlouvy o fungování EU.

HLAVA III
RÁMEC PRO CERTIFIKACI KYBERNETICKÉ BEZPEČNOSTI

Článek 43

Evropské systémy certifikace kybernetické bezpečnosti

Evropský systém certifikace kybernetické bezpečnosti osvědčuje, že produkty a služby IKT, které byly v souladu s tímto systémem certifikovány, splňují specifikované požadavky na jejich schopnost odolávat s příslušnou úrovní záruky činnostem, které ohrožují přístupnost, pravost, neporušenost nebo důvěrnost ukládaných, předávaných nebo zpracovávaných údajů nebo funkcí či služeb, jež jsou prostřednictvím těchto produktů, procesů, služeb a systémů nabízené nebo přístupné.

Článek 44

Vypracování a přijetí evropského systému certifikace kybernetické bezpečnosti

1. Agentura ENISA na základě žádosti Komise vypracuje návrh evropského systému certifikace kybernetické bezpečnosti, který splňuje požadavky stanovené v článcích 45, 46 a 47 tohoto nařízení. Vypracování návrhu evropského systému certifikace kybernetické bezpečnosti mohou Komisi navrhnout členské státy nebo Evropská skupina pro certifikaci kybernetické bezpečnosti (dále jen „skupina“), zřízená podle článku 53.
2. Při vypracovávání návrhu systému uvedeného v odstavci 1 tohoto článku agentura ENISA konzultuje všechny příslušné zúčastněné strany a úzce spolupracuje se skupinou. Skupina poskytne agentuře ENISA pomoc a odborné poradenství, které si agentura ENISA v souvislosti s vypracováním návrhu systému vyžádá, mimo jiné případným poskytováním stanovisek.
3. Agentura ENISA návrh evropského systému certifikace kybernetické bezpečnosti, vypracovaný v souladu s odstavcem 2 tohoto článku, předá Komisi.
4. V souladu s čl. 55 odst. 2 může Komise na základě návrhu systému vypracovaného agenturou ENISA přijímat prováděcí akty, kterými stanoví evropské systémy certifikace kybernetické bezpečnosti produktů a služeb IKT splňující požadavky článků 45, 46 a 47 tohoto nařízení.
5. Agentura ENISA spravuje zvláštní internetové stránky poskytující informace o evropských systémech certifikace kybernetické bezpečnosti a zajišťující jejich propagaci.

Článek 45

Bezpečnostní cíle evropských systémů certifikace kybernetické bezpečnosti

Evropský systém certifikace kybernetické bezpečnosti je navržen tak, aby zohledňoval tyto bezpečnostní cíle:

a) chránit ukládané, předávané nebo jinak zpracovávané údaje proti náhodnému nebo neoprávněnému ukládání, zpracování, přístupu nebo sdělování;

b) chránit ukládané, předávané nebo jinak zpracovávané údaje proti náhodnému nebo neoprávněnému zničení, náhodné ztrátě nebo úpravám;

c) zajistit, aby oprávněné osoby, programy nebo stroje měly přístup výhradně k údajům, službám nebo funkcím, jichž se týkají jejich přístupová práva;

d) zaznamenat, které údaje, funkce nebo služby byly kdy a kým sděleny;

e) zajistit, aby bylo možné kontrolovat, ke kterým údajům, službám nebo funkcím kdy a kdo získal přístup nebo je použil;

f) včas obnovit dostupnost údajů, služeb a funkcí a přístup k nim v případě fyzických nebo technických incidentů;

g) zajistit, aby produkty a služby IKT byly poskytovány s aktualizovaným softwarem, který neobsahuje známá slabá místa, a aby byly zavedeny mechanismy pro bezpečné aktualizace softwaru.

Článek 46

Úrovně záruky evropských systémů certifikace kybernetické bezpečnosti

1. Evropský systém certifikace kybernetické bezpečnosti může u produktů a služeb IKT, jež jsou v rámci daného systému vydány, určit jednu nebo více těchto úrovní záruky: základní, významnou a/nebo vysokou.

2. Úrovně záruky „základní“, „významná“ a „vysoká“ splňují tato kritéria:

a) základní úroveň záruky odkazuje na certifikát vydaný v rámci evropského systému certifikace kybernetické bezpečnosti, který poskytuje omezený stupeň důvěry v deklarované nebo uváděné kybernetickobezpečnostní kvality produktu nebo služby IKT a je charakterizován odkazem na související technické specifikace, normy a postupy, včetně technických kontrol, jejichž účelem je snížit riziko kybernetických bezpečnostních incidentů;

b) významná úroveň záruky odkazuje na certifikát vydaný v rámci evropského systému certifikace kybernetické bezpečnosti, který poskytuje významný stupeň důvěry v deklarované nebo uváděné kybernetickobezpečnostní kvality produktu nebo služby IKT a je charakterizován odkazem na související technické specifikace, normy a postupy, včetně technických kontrol, jejichž účelem je významně snížit riziko kybernetických bezpečnostních incidentů;

c) vysoká úroveň záruky odkazuje na certifikát vydaný v rámci evropského systému certifikace kybernetické bezpečnosti, který poskytuje vyšší stupeň důvěry v deklarované nebo uváděné kybernetickobezpečnostní kvality produktu nebo služby IKT než certifikáty s významnou úrovní záruky a je charakterizován odkazem na související technické specifikace, normy a postupy, včetně technických kontrol, jejichž účelem je předcházet kybernetickým bezpečnostním incidentům.

Článek 47

Prvky evropských systémů certifikace kybernetické bezpečnosti

1. Evropský systém certifikace kybernetické bezpečnosti zahrnuje tyto prvky:

a) předmět a rozsah certifikace včetně druhu nebo kategorií zahrnutých produktů a služeb IKT;

b) podrobnou specifikaci kybernetickobezpečnostních požadavků, na jejichž základě jsou konkrétní produkty a služby IKT hodnoceny, například prostřednictvím odkazu na unijní nebo mezinárodní normy nebo technické specifikace;

c) případně jednu nebo více úrovní záruky;

d) konkrétní kritéria a metody hodnocení použité k prokázání toho, že bylo dosaženo konkrétních cílů uvedených v článku 45, včetně typů těchto hodnocení;

e) informace nezbytné pro certifikaci, které žadatel předkládá subjektům posuzování shody;

f) stanoví-li systém známky nebo označení, podmínky používání těchto známek nebo označení;

g) je-li součástí systému dozor, pravidla pro sledování souladu s požadavky uvedenými v certifikátech, včetně mechanismů pro prokázání trvalého souladu s uvedenými kybernetickobezpečnostními požadavky;

h) podmínky pro udělení, zachování, prodloužení, rozšíření a omezení rozsahu certifikace;

i) pravidla upravující důsledky nesouladu certifikovaných produktů a služeb IKT s požadavky certifikace;

j) pravidla upravující způsob oznamování a řešení dříve nezjištěných slabých míst v kybernetické bezpečnosti produktů a služeb IKT;

k) pravidla upravující uchovávání záznamů subjekty posuzování shody;

l) označení vnitrostátních systémů certifikace kybernetické bezpečnosti pokrývajících stejný druh nebo kategorie produktů a služeb IKT;

m) obsah vydaného certifikátu.

2. Specifikované požadavky systému nesmí být v rozporu s příslušnými právními požadavky, zejména s požadavky plynoucími z harmonizovaných právních předpisů Unie.

3. Pokud tak konkrétní akt Unie stanoví, lze certifikaci podle evropského systému certifikace kybernetické bezpečnosti použít k prokázání předpokladu shody s požadavky daného aktu.

4. Pokud harmonizované právní předpisy Unie neexistují, může skutečnost, že evropský systém certifikace kybernetické bezpečnosti lze použít k vyslovení předpokladu shody s právními požadavky, stanovit právo členského státu.

Článek 48

Certifikace kybernetické bezpečnosti

1. U produktů a služeb IKT, které byly certifikovány podle evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 44, se předpokládá, že splňují požadavky daného systému.

2. Certifikace je dobrovolná, nestanoví-li právo Unie jinak.

3. Evropský certifikát kybernetické bezpečnosti podle tohoto článku vydávají subjekty posuzování shody uvedené v článku 51 na základě kritérií obsažených v evropském systému certifikace kybernetické bezpečnosti přijatém podle článku 44.

4. Odchylně od odstavce 3 může konkrétní evropský systém certifikace kybernetické bezpečnosti v řádně odůvodněných případech stanovit, že evropský certifikát kybernetické bezpečnosti vyplývající z daného systému může být vydán pouze veřejným subjektem. Tímto veřejným subjektem je:

   a) vnitrostátní orgán dozoru nad certifikací uvedený v čl. 50 odst. 1;

   b) subjekt, který je akreditován jako subjekt posuzování shody podle čl. 51 odst. 1, nebo

   c) subjekt zřízený podle zákonů, právních předpisů nebo jiných oficiálních správních postupů dotčeného členského státu, který splňuje požadavky na orgány certifikující produkty, procesy a služby podle normy ISO/IEC 17065:2012.

5. Fyzická nebo právnická osoba, která předkládá své produkty nebo služby IKT certifikačnímu mechanismu, poskytne subjektu posuzování shody uvedenému v článku 51 veškeré informace nezbytné k provedení certifikačního postupu.

6. Certifikáty se vydávají na období nejvýše tří let a lze je obnovit za stejných podmínek, pokud jsou nadále splněny příslušné požadavky.

7. Evropský certifikát kybernetické bezpečnosti vydaný podle tohoto článku je uznáván ve všech členských státech.

Článek 49

Vnitrostátní systémy certifikace kybernetické bezpečnosti a certifikáty

1. Aniž je dotčen odstavec 3, vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty a služby IKT zahrnuté do evropského systému certifikace kybernetické bezpečnosti ztrácejí svou účinnost od data uvedeného v prováděcím aktu přijatém podle čl. 44 odst. 4. Stávající vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty a služby IKT, na něž se evropský systém certifikace kybernetické bezpečnosti nevztahuje, zůstávají v platnosti.

2. Členské státy nesmějí zavádět nové vnitrostátní systémy certifikace kybernetické bezpečnosti pro produkty a služby IKT zahrnuté do platného evropského systému certifikace kybernetické bezpečnosti.

3. Stávající certifikáty vydané v rámci vnitrostátních systémů certifikace kybernetické bezpečnosti zůstávají platné až do data skončení své platnosti.

Článek 50

Vnitrostátní orgány dozoru nad certifikací

1. Každý členský stát jmenuje vnitrostátní orgán dozoru nad certifikací.

2. Každý členský stát Komisi sdělí totožnost jmenovaného orgánu.

3. Každý vnitrostátní orgán dozoru nad certifikací je z hlediska své organizace, finančních rozhodnutí, právní struktury a rozhodování nezávislý na subjektech, nad nimiž vykonává dozor.

4. Členské státy zajistí, aby vnitrostátní orgány dozoru nad certifikací měly odpovídající zdroje pro výkon svých pravomocí a pro efektivní a účinné provádění úkolů, které jim byly svěřeny.

5. Za účelem efektivního provádění tohoto nařízení je vhodné, aby se tyto orgány aktivním, efektivním, účinným a bezpečným způsobem podílely na činnosti Evropské skupiny pro certifikaci kybernetické bezpečnosti zřízené podle článku 53.

6. Vnitrostátní orgány dozoru nad certifikací:

   a) sledují a vymáhají uplatňování ustanovení podle této hlavy na vnitrostátní úrovni a dohlížejí na to, aby certifikáty vydané subjekty posuzování shody usazenými na jejich území splňovaly požadavky stanovené v této hlavě a v odpovídajícím evropském systému certifikace kybernetické bezpečnosti;

   b) sledují a dohlížejí na činnosti subjektů posuzování shody pro účely tohoto nařízení, mimo jiné ve vztahu k oznámením subjektů posuzování shody a k souvisejícím úkolům stanoveným v článku 52 tohoto nařízení;

   c) řeší stížnosti podané fyzickými nebo právnickými osobami v souvislosti s certifikáty vydanými subjekty posuzování shody usazenými na jejich území, v přiměřeném rozsahu šetří předmět stížnosti a v přiměřené lhůtě informují stěžovatele o průběhu a výsledku šetření;

   d) spolupracují s dalšími vnitrostátními orgány dozoru nad certifikací nebo jinými veřejnými orgány, mimo jiné prostřednictvím sdílení informací o možných případech nesouladu produktů a služeb IKT s požadavky tohoto nařízení nebo konkrétních evropských systémů certifikace kybernetické bezpečnosti;

   e) sledují příslušný vývoj v oblasti certifikace kybernetické bezpečnosti.

7. Každý vnitrostátní orgán dozoru nad certifikací má alespoň tyto pravomoci:

   a) žádat subjekty posuzování shody a držitele evropského certifikátu kybernetické bezpečnosti o poskytnutí veškerých informací nezbytných pro plnění jeho úkolů;

   b) za účelem ověření souladu s ustanoveními podle hlavy III provádět šetření v podobě auditů u subjektů posuzování shody a držitelů evropských certifikátů kybernetické bezpečnosti;

   c) v souladu s vnitrostátním právem přijímat vhodná opatření za účelem zajištění toho, aby subjekty posuzování shody nebo držitelé certifikátů dodržovali toto nařízení nebo evropský systém certifikace kybernetické bezpečnosti;

   d) získat přístup do všech prostor subjektů posuzování shody a držitelů evropských certifikátů kybernetické bezpečnosti za účelem provádění šetření v souladu s procesním právem Unie nebo členských států;

   e) v souladu s vnitrostátním právem odnímat certifikáty, které nejsou v souladu s tímto nařízením nebo evropským systémem certifikace kybernetické bezpečnosti;

f) v souladu s vnitrostátním právem ukládat sankce stanovené v článku 54 a požadovat okamžité zastavení porušování povinností stanovených v tomto nařízení.

8. Vnitrostátní orgány dozoru nad certifikací spolupracují mezi sebou a s Komisí, a zejména si vyměňují informace, zkušenosti a osvědčené postupy týkající se certifikace kybernetické bezpečnosti a technických otázek týkajících se kybernetické bezpečnosti produktů a služeb IKT.

Článek 51
Subjekty posuzování shody

1. Subjekty posuzování shody jsou akreditovány vnitrostátním akreditačním orgánem jmenovaným podle nařízení (ES) č. 765/2008, pouze pokud splňují požadavky stanovené v příloze tohoto nařízení.

2. Akreditace se vydává na období nejvýše pěti let a lze ji za stejných podmínek obnovit, pokud daný subjekt posuzování shody splňuje požadavky stanovené v tomto článku. Akreditační orgány akreditaci subjektu posuzování shody podle odstavce 1 tohoto článku zruší, pokud podmínky pro udělení akreditace nejsou splněny nebo přestanou být plněny nebo pokud opatření přijatá subjektem posuzování shody porušují toto nařízení.

Článek 52
Oznámení

1. Ke každému evropskému systému certifikace kybernetické bezpečnosti přijatému podle článku 44 vnitrostátní orgány dozoru nad certifikací oznámí Komisi akreditované subjekty posuzování shody oprávněné k vydávání certifikátů s určenými úrovněmi záruky podle článku 46 a bez zbytečného odkladu i jakékoliv jejich následné změny.

2. Komise zveřejní seznam oznámených subjektů posuzování shody jeden rok po vstupu evropského systému certifikace kybernetické bezpečnosti v platnost v Úředním věstníku.

3. Obdrží-li Komise oznámení po uplynutí lhůty uvedené v odstavci 2, zveřejní změny v seznamu podle odstavce 2 do dvou měsíců ode dne přijetí tohoto oznámení v Úředním věstníku Evropské unie.

4. Vnitrostátní orgán dozoru nad certifikací může Komisi předložit žádost o odstranění subjektu posuzování shody oznámeného daným vnitrostátním orgánem dozoru nad certifikací ze seznamu uvedeného v odstavci 2 tohoto článku. Komise odpovídající změny seznamu zveřejní do jednoho měsíce ode dne přijetí žádosti vnitrostátního orgánu dozoru nad certifikací v Úředním věstníku Evropské unie.

5. Komise může stanovit prostřednictvím prováděcích aktů okolnosti, formáty a postupy oznámení uvedených v odstavci 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 55 odst. 2.

Článek 53
Evropská skupina pro certifikaci kybernetické bezpečnosti

1. Zřizuje se Evropská skupina pro certifikaci kybernetické bezpečnosti (dále jen „skupina“).

2. Skupina je složena z vnitrostátních orgánů dozoru nad certifikací. Orgány jsou zastoupeny řediteli nebo jinými vysokými představiteli vnitrostátních orgánů dozoru nad certifikací.

3. Skupina má tyto úkoly:

   a) poskytovat poradenství a pomoc Komisi v její činnosti spojené se zajištěním soudržného provádění a uplatňování této hlavy, zejména pokud jde o záležitosti politiky v oblasti certifikace kybernetické bezpečnosti, koordinaci politických přístupů a vypracování evropských systémů certifikace kybernetické bezpečnosti;

   b) poskytovat poradenství a pomoc agentuře ENISA a spolupracovat s ní v souvislosti s vypracováním návrhu systému v souladu s článkem 44 tohoto nařízení;

   c) navrhovat Komisi, aby agenturu požádala o vypracování návrhu evropského systému certifikace kybernetické bezpečnosti v souladu s článkem 44 tohoto nařízení;

   d) přijímat stanoviska určená Komisi v souvislosti se zachováním a přezkumem stávajících evropských systémů certifikace kybernetické bezpečnosti;

   e) zkoumat relevantní vývoj v oblasti certifikace kybernetické bezpečnosti a vyměňovat osvědčené postupy týkající se systémů certifikace kybernetické bezpečnosti;

   f) usnadňovat prostřednictvím výměny informací spolupráci mezi vnitrostátními orgány dozoru nad certifikací podle této hlavy, zejména stanovením metod pro účinnou výměnu informací o veškerých otázkách týkajících se certifikace kybernetické bezpečnosti.

4. Skupině předsedá Komise a s pomocí agentury ENISA jí podle čl. 8 písm. a) zajišťuje služby sekretariátu.

Článek 54
Sankce

Členské státy stanoví pravidla upravující sankce za porušení této hlavy a evropských systémů certifikace kybernetické bezpečnosti a přijmou veškerá nezbytná opatření pro zajištění jejich provádění. Stanovené sankce musí být účinné, přiměřené a odrazující. Členské státy [do …/neprodleně] uvědomí o těchto pravidlech a o těchto opatřeních Komisi a informují ji o veškerých jejich pozdějších změnách.

HLAVA IV
ZÁVĚREČNÁ USTANOVENÍ

Článek 55
Postup projednávání ve výboru

1. Komisi je nápomocen výbor. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.
2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

Článek 56
Hodnocení a přezkum

1. Nejpozději pět let po dni uvedeném v článku 58 a poté každých pět let Komise posoudí dopad, efektivitu a účinnost agentury a jejích pracovních postupů, jakož i případnou potřebu změnit mandát agentury a finanční důsledky této změny. Hodnocení zohledňuje veškerou zpětnou vazbu, kterou agentura v reakci na svou činnost zaznamenala. Pokud se Komise domnívá, že zachování agentury již není s ohledem na cíle, mandát a úkoly, které jí byly svěřeny, odůvodněné, může navrhnout, aby byla ustanovení tohoto nařízení týkající se agentury změněna.
2. Hodnocení rovněž posoudí dopad, efektivnost a účinnost ustanovení hlavy III s ohledem na cíle zajištění odpovídající úrovně kybernetické bezpečnosti produktů a služeb IKT v Unii a zlepšení fungování vnitřního trhu.
3. Komise předá hodnotící zprávu společně se svými závěry Evropskému parlamentu, Radě a správní radě. Zjištění hodnotící zprávy se zveřejní.

Článek 57
Zrušení a nástupnictví

1. Nařízení (EU) č. 526/2013 se zrušuje s účinkem od […].
2. Odkazy na nařízení (EU) č. 526/2013 a na agenturu ENISA se považují za odkazy na toto nařízení a na agenturu.
3. Agentura je nástupkyní agentury zřízené nařízením (EU) č. 526/2013, pokud jde o veškeré vlastnictví, dohody, právní závazky, pracovní smlouvy, finanční závazky a odpovědnost. Všechna stávající rozhodnutí správní a výkonné rady zůstávají v platnosti, nejsou-li v rozporu s ustanoveními tohoto nařízení.
4. Agentura se zřizuje na neomezené období počínaje […].
5. Výkonný ředitel jmenovaný podle čl. 24 odst. 4 nařízení (EU) č. 526/2013 je výkonným ředitelem agentury po zbývající část svého funkčního období.
6. Členové správní rady a jejich náhradníci jmenovaní podle článku 6 nařízení (EU) č. 526/213 jsou členy a náhradníky správní rady agentury po zbývající část svého funkčního období.

Článek 58

Vstup v platnost

1. Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v Úředním věstníku Evropské unie.

2. Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament *předseda*	*Za Radu* *předseda/předsedkyně*

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Návrh nařízení Evropského parlamentu a Rady o agentuře ENISA, Agentuře EU pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“)

1.2. Příslušné oblasti politik

Oblast politiky: 09 – Komunikační sítě, obsah a technologie

Činnost: 09.02 Jednotný digitální trh

1.3. Povaha návrhu/podnětu

☒ Návrh/podnět se týká **nové akce (Hlava III – Certifikace)**

☐ Návrh/podnět se týká **nové akce následující po pilotním projektu / přípravné akci**[43]

☒Návrh/podnět se týká **prodloužení stávající akce (Hlava II – Mandát agentury ENISA)**

☐ Návrh/podnět se týká **akce přesměrované na jinou akci**

1.4. Cíle

1.4.1. Víceleté strategické cíle Komise sledované návrhem/podnětem

1. Zvýšení odolnosti členských států, podniků a EU jako celku

2. Zajištění řádného fungování vnitřního trhu EU s produkty a službami IKT

3. Zvýšení globální konkurenceschopnosti společností EU působících v oblasti IKT

4. Sbližování právních a správních předpisů členských států vyžadujících kybernetickou bezpečnost

1.4.2. Specifické cíle

S ohledem na obecné cíle a v širších souvislostech revidované strategie kybernetické bezpečnosti nástroj vymezením oblasti působnosti a mandátu agentury ENISA a zřízením evropského rámce pro certifikaci produktů a služeb IKT hodlá dosáhnout těchto cílů:

1. Zvýšit **schopnosti a připravenost** členských států a podniků.
2. Zlepšit **spolupráci a koordinaci** napříč členskými státy a orgány, agenturami a institucemi EU.
3. Zvýšit **schopnost na úrovni EU doplňovat opatření členských států**, zejména v případě přeshraničních kybernetických krizí.
4. Zvýšit **informovanost** občanů a podniků o otázkách týkajících se kybernetické bezpečnosti.
5. Posílit důvěru v jednotný digitální trh a digitální inovace zvýšením celkové **transparentnosti záruky kybernetické bezpečnosti**[44] produktů a služeb IKT.

[43] Uvedené v čl. 54 odst. 2 písm. a) nebo b) finančního nařízení.

Agentura ENISA přispěje k dosažení výše uvedených cílů:

Větší podporou tvorby politik – poskytování pokynů a poradenství Komisi a členským státům za účelem aktualizace a rozvoje uceleného právního rámce v oblasti kybernetické bezpečnosti, jakož i odvětvových politik a iniciativ v oblasti právních předpisů zahrnujících otázky kybernetické bezpečnosti; přispívání k činnosti skupiny pro spolupráci (článek 11 směrnice (EU) 2016/1148) poskytováním odborných poznatků a pomoci; podpora rozvoje a provádění politik v oblasti elektronické totožnosti a služeb vytvářejících důvěru; prosazování výměny osvědčených postupů mezi příslušnými orgány.

Větší podporou budování kapacit – poskytování podpory členským státům a orgánům, institucím a jiným subjektům Unie za účelem rozvoje a zdokonalování prevence, odhalování a analýzy kybernetických bezpečnostních problémů a incidentů a schopnosti reagovat na ně; pomoc členským státům na jejich žádost při tvorbě vnitrostátních týmů CSIRT a národních strategií kybernetické bezpečnosti; pomoc orgánům Unie při vypracovávání a přezkumu strategií Unie týkajících se kybernetické bezpečnosti; zajišťování školení týkajících se kybernetické bezpečnosti; pomoc členským státům při výměně osvědčených postupů prostřednictvím skupiny pro spolupráci; usnadňování vytváření odvětvových středisek pro sdílení a analýzu informací (ISAC).

Podporou operativní spolupráce a řešení krizí – podpora spolupráce mezi příslušnými veřejnými orgány a mezi zúčastněnými stranami zaváděním systematické spolupráce s orgány, institucemi a jinými subjekty Unie zabývajícími se kybernetickou bezpečností, kyberkriminalitou a ochranou soukromí a osobních údajů; zajišťování služeb sekretariátu pro síť CSIRT (čl. 12 odst. 2 směrnice (EU) 2016/1148), jakož i přispívání k operativní spolupráci v rámci sítě poskytováním podpory ve spolupráci s týmem CERT-EU členským státům na jejich žádost; organizování pravidelných cvičení v oblasti kybernetické bezpečnosti; přispívání k vytváření společné reakce na rozsáhlé přeshraniční kybernetické bezpečnostní incidenty a krize; provádění technických šetření *ex post* ve spolupráci se sítí CSIRT, která se týkají významných incidentů, a vydávání navazujících doporučení.

Úkoly souvisejícími s trhem (normalizace, certifikace) – vykonávání řady funkcí konkrétně podporujících vnitřní trh: „středisko pro sledování trhu“ kybernetické bezpečnosti, analyzování příslušných trendů na trhu kybernetické bezpečnosti za účelem lepšího sladění poptávky a nabídky; podpora a prosazování rozvoje a provádění politiky Unie v oblasti certifikace kybernetické bezpečnosti produktů a služeb IKT vypracováváním návrhů evropských systémů certifikace kybernetické bezpečnosti produktů a služeb IKT, zajišťování služeb sekretariátu unijní skupině pro certifikaci kybernetické bezpečnosti, poskytování pokynů a osvědčených postupů týkajících se bezpečnostních požadavků na produkty a služby IKT ve spolupráci s vnitrostátními orgány dozoru nad certifikací a odvětvím.

Větší podporou znalostí, informací a zvyšování informovanosti – poskytování pomoci a poradenství Komisi a členským státům za účelem dosažení vysoké úrovně znalostí v celé Unii o otázkách týkajících se bezpečnosti sítí a informací a jejich uplatňování na zúčastněné strany z odvětví. To předpokládá rovněž shromažďování a uspořádávání informací o bezpečnosti sítí a informačních systémů [nebo o kybernetické bezpečnosti] a jejich zpřístupňování veřejnosti prostřednictvím specializovaného portálu. Dalším důležitým prvkem jsou činnosti na zvyšování informovanosti a informační kampaně o rizicích kybernetické bezpečnosti zaměřené na širokou veřejnost.

---

[44] Transparentnost záruky kybernetické bezpečnosti spočívá v tom, že jsou uživatelům poskytovány dostatečné informace o kybernetickobezpečnostních vlastnostech, které těmto uživatelům umožňují objektivně stanovit úroveň bezpečnosti daného produktu, služby nebo procesu IKT.

Větší podporou výzkumu a inovací – poskytování poradenství ohledně potřeb výzkumu a stanovování priorit v oblasti kybernetické bezpečnosti.

Podporou mezinárodní spolupráce – podpora úsilí Unie zaměřeného na spolupráci s třetími zeměmi a s mezinárodními organizacemi v zájmu prosazení mezinárodní spolupráce v oblasti kybernetické bezpečnosti.

CERTIFIKACE

Rámec pro certifikaci přispěje k dosažení cílů tím, že zvýší celkovou transparentnost záruky kybernetické bezpečnosti[45] produktů a služeb IKT, čímž dojde k posílení důvěry v jednotný digitální trh a digitální inovace. Rovněž by měl pomoci zabránit roztříštěnosti systémů certifikace v EU a souvisejících bezpečnostních požadavků a hodnoticích kritérií v různých členských státech a odvětvích.

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Očekává se, že posílená agentura ENISA (podporující schopnosti, prevenci, spolupráci a informovanost na úrovni EU, a tedy navržená za účelem zvýšení celkové kybernetické odolnosti EU), jakož i podpora rámce EU pro certifikaci produktů a služeb IKT budou mít tyto dopady (neúplný seznam):

Celkový dopad:

– Celkový pozitivní dopad na vnitřní trh díky snížené roztříštěnosti trhu a budování důvěry v digitální technologie prostřednictvím lepší spolupráce, harmonizovanějších přístupů k politikám EU v oblasti kybernetické bezpečnosti a zvýšeným schopnostem na úrovni EU. To by mělo vést k pozitivnímu hospodářskému dopadu, jelikož to pomůže snížit náklady na kybernetické bezpečnostní incidenty / incidenty kyberkriminality, jejichž odhadovaný hospodářský dopad v Unii činí 0,41 % HDP EU (tj. přibližně 55 miliard EUR).

Konkrétní výsledky:

Zvýšené schopnosti a připravenost členských států a podniků v oblasti kybernetické bezpečnosti

– Zvýšené schopnosti a připravenost členských států v oblasti kybernetické bezpečnosti (díky dlouhodobé strategické analýze kybernetických hrozeb a incidentů, pokynům a zprávám, zprostředkování odborných poznatků a osvědčených postupů, dostupnosti školení a školicích materiálů a posíleným cvičením CyberEurope).

– Zlepšené schopnosti soukromých subjektů díky podpoře zřizování středisek pro sdílení a analýzu informací (ISAC) v různých odvětvích.

– Větší připravenost EU a členských států v oblasti kybernetické bezpečnosti díky dostupnosti nacvičených a dohodnutých plánů pro případ rozsáhlého přeshraničního kybernetického bezpečnostního incidentu, které byly otestovány v rámci cvičení CyberEurope.

Zlepšená spolupráce a koordinace napříč členskými státy a orgány, institucemi a jinými subjekty EU:

[45] Transparentnost záruky kybernetické bezpečnosti spočívá v tom, že jsou uživatelům poskytovány dostatečné informace o kybernetickobezpečnostních vlastnostech, které těmto uživatelům umožňují objektivně stanovit úroveň bezpečnosti daného produktu, služby nebo procesu IKT.

– Zlepšená spolupráce v rámci veřejného a soukromého sektoru i mezi veřejným a soukromým sektorem.

– Větší jednotnost přístupu k provádění směrnice o bezpečnosti sítí a informací v přeshraničním rozměru a v různých odvětvích.

– Zlepšená spolupráce v oblasti certifikace díky institucionálnímu rámci umožňujícímu vypracování evropských systémů certifikace kybernetické bezpečnosti a tvorbu společné politiky v této oblasti.

Zvýšená schopnost na úrovni EU doplňovat opatření členských států

– Větší „operativní kapacita EU“ doplňovat opatření členských států a na jejich žádost je podporovat ve vztahu k omezeným a předem identifikovaným službám. Očekává se, že to bude mít pozitivní dopad na úspěšnou prevenci a odhalování incidentů a reakce na ně jak na úrovni členských států, tak na úrovni Unie.

Zvýšená informovanost občanů a podniků o otázkách týkajících se kybernetické bezpečnosti

– Zvýšená obecná informovanost občanů a podniků o otázkách týkajících se kybernetické bezpečnosti.

– Větší schopnost přijímat informovaná rozhodnutí ohledně nákupu produktů a služeb IKT díky certifikaci kybernetické bezpečnosti.

Posílená důvěra v jednotný digitální trh a digitální inovace prostřednictvím větší transparentnosti záruky kybernetické bezpečnosti produktů a služeb IKT

– Větší transparentnost záruky kybernetické bezpečnosti[46] produktů a služeb IKT díky zjednodušení postupů pro bezpečnostní certifikaci prostřednictvím celounijního rámce.

– Vyšší úroveň záruky bezpečnostních vlastností produktů a služeb IKT.

– Větší zavádění bezpečnostní certifikace díky zjednodušeným postupům, nižším nákladům a předpokladu, že celounijní podnikatelské příležitosti nebudou omezovány roztříštěností trhu.

– Větší konkurenceschopnost na unijním trhu kybernetické bezpečnosti v důsledku snížení nákladů a administrativní zátěže pro malé a střední podniky a odstranění potenciálních překážek vstupu na trh způsobených velkým počtem vnitrostátních systémů certifikace.

Ostatní

– U žádného z cílů se neočekává významný dopad na životní prostředí.

– Pokud jde o rozpočet EU, lze očekávat úspory z důvodu větší efektivity v důsledku zvýšené spolupráce a koordinace činností mezi orgány, institucemi a jinými subjekty EU.

1.4.4. Ukazatele výsledků a dopadů

Upřesněte ukazatele, podle kterých je možno uskutečňování návrhu/podnětu sledovat.

a)

[46] Transparentnost záruky kybernetické bezpečnosti spočívá v tom, že jsou uživatelům poskytovány dostatečné informace o kybernetickobezpečnostních vlastnostech, které těmto uživatelům umožňují objektivně stanovit úroveň bezpečnosti daného produktu, služby nebo procesu IKT.

Cíl: Zvýšení schopností a připravenosti členských států a podniků:

- Počet školení organizovaných agenturou ENISA
- Zeměpisné pokrytí (počet zemí a oblastí) přímé pomoci poskytované agenturou ENISA
- Úroveň připravenosti dosažená členskými státy z hlediska vyzrálosti týmů CSIRT a dohledu nad regulačními opatřeními souvisejícími s kybernetickou bezpečností
- Počet celounijních osvědčených postupů pro kritické infrastruktury poskytnutých agenturou ENISA
- Počet celounijních osvědčených postupů pro malé a střední podniky poskytnutých agenturou ENISA
- Zveřejňování každoročních strategických analýz kybernetických hrozeb a incidentů za účelem zjišťování nových trendů agenturou ENISA
- Pravidelné příspěvky agentury ENISA k činnosti pracovních skupin pro kybernetickou bezpečnost v rámci evropských normalizačních organizací.

Cíl: Zlepšení spolupráce a koordinace napříč členskými státy a orgány, institucemi a jinými subjekty EU:

- Počet členských států, které v procesu tvorby svých politik využily doporučení a stanoviska agentury ENISA
- Počet orgánů, institucí a jiných subjektů EU, které v procesu tvorby svých politik využily doporučení a stanoviska agentury ENISA
- Pravidelné provádění pracovního programu sítě CSIRT a správné fungování IT infrastruktury a komunikačních kanálů sítě CSIRT
- Počet technických zpráv, které byly poskytnuty skupině pro spolupráci a které tato skupina využila
- Jednotný přístup k provádění směrnice o bezpečnosti sítí a informací v přeshraničním rozměru a v různých odvětvích
- Počet posouzení týkajících se dodržování právních předpisů, které provedla agentura ENISA
- Počet středisek ISAC zřízených v různých odvětvích, zejména u kritických infrastruktur
- Zřízení a pravidelné provozování informační platformy pro šíření informací o kybernetické bezpečnosti získaných od orgánů, institucí a jiných subjektů EU
- Pravidelné příspěvky k přípravě pracovních programů EU týkajících se výzkumu a inovací
- Uzavření dohody o spolupráci mezi agenturou ENISA, centrem EC3 a týmem CERT-EU
- Počet systémů certifikace zahrnutých do rámce a vypracovaných podle rámce

Cíl: Zvýšení schopnosti na úrovni EU doplňovat opatření členských států, zejména v případě přeshraničních kybernetických krizí:

- Zveřejňování každoročních strategických analýz kybernetických hrozeb a incidentů za účelem zjišťování nových trendů agenturou ENISA

- Zveřejňování agregovaných informací o incidentech ohlášených podle směrnice o bezpečnosti sítí a informací agenturou ENISA
- Počet celoevropských cvičení koordinovaných agenturou a počet zapojených členských států a organizací
- Počet žádostí o podporu při reakci na mimořádné události, které členské státy zaslaly agentuře ENISA a kterým agentura vyhověla
- Počet analýz zranitelností, artefaktů a incidentů provedených agenturou ENISA ve spolupráci s týmem CERT-EU
- Dostupnost celounijních situačních zpráv založených na informacích, které agentuře ENISA poskytly členské státy a jiné subjekty v případech rozsáhlých přeshraničních kybernetických incidentů

Cíl: Zvýšení informovanosti občanů a podniků o otázkách týkajících se kybernetické bezpečnosti:

- Pravidelné provozování celounijních a vnitrostátních kampaní na zvyšování informovanosti a pravidelné aktualizování témat podle aktuálních vzdělávacích potřeb
- Zvýšení informovanosti občanů EU o kybernetické bezpečnosti
- Pravidelné provozování osvětového kvízu o kybernetické bezpečnosti a zvýšení procenta správných odpovědí v průběhu času
- Pravidelné zveřejňování osvědčených postupů týkajících se kybernetické bezpečnosti a kybernetické hygieny zaměřené na zaměstnance a organizace

Cíl: Posílení důvěry v jednotný digitální trh a digitální inovace zvýšením celkové transparentnosti záruky kybernetické bezpečnosti[47] produktů a služeb IKT:

- Počet systémů dodržujících rámec EU
- Snížené náklady na získání certifikátu bezpečnosti IKT
- Počet subjektů posuzování shody specializujících se na certifikaci IKT ve všech členských státech
- Zřízení Evropské skupiny pro certifikaci kybernetické bezpečnosti a pravidelné pořádání jejích zasedání
- Zavedení pokynů pro certifikaci podle rámce EU
- Pravidelné zveřejňování analýz hlavních trendů na unijním trhu kybernetické bezpečnosti
- Počet produktů a služeb IKT certifikovaných podle pravidel evropského rámce pro certifikaci bezpečnosti IKT
- Větší počet koncových uživatelů, kteří si jsou vědomi bezpečnostních prvků produktů a služeb IKT

b)

[47] Transparentnost záruky kybernetické bezpečnosti spočívá v tom, že jsou uživatelům poskytovány dostatečné informace o kybernetickobezpečnostních vlastnostech, které těmto uživatelům umožňují objektivně stanovit úroveň bezpečnosti daného produktu, služby nebo procesu IKT.

1.4.5. 1.4.5. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu

S ohledem na regulační požadavky a rychle se vyvíjející oblast kybernetických bezpečnostních hrozeb je třeba přezkoumat mandát agentury ENISA tak, aby stanovil obnovený soubor úkolů a funkcí s cílem účinně a efektivně podporovat členské státy, orgány EU a další zúčastněné strany v jejich úsilí zajistit bezpečný kyberprostor v Evropské unii. Navrhovaná působnost mandátu je vymezena posílením oblastí, kde se jasně ukázala přidaná hodnota agentury, a doplněním nových oblastí, v nichž je nezbytná pomoc s ohledem na nové politické priority a nástroje, zejména na směrnici o bezpečnosti sítí a informací, na přezkum strategie kybernetické bezpečnosti EU a na plán kybernetické bezpečnosti EU pro spolupráci v případě kybernetických krizí a pro certifikaci bezpečnosti IKT. Nový navrhovaný mandát se snaží udělit agentuře silnější a centrálnější úlohu, zejména tím, že rovněž podporuje členské státy v aktivnějším boji proti konkrétním hrozbám (operativní kapacita), a dále tím, že se agentura stane odborným střediskem podporujícím členské státy a Komisi v otázkách certifikace kybernetické bezpečnosti.

Návrh zároveň zřizuje evropský rámec pro certifikaci kybernetické bezpečnosti produktů a služeb IKT a upřesňuje základní funkce a úkoly agentury ENISA v oblasti certifikace kybernetické bezpečnosti. Tento rámec stanoví společná ustanovení a postupy umožňující vytvoření celounijních systémů certifikace kybernetické bezpečnosti pro konkrétní produkty/služby IKT nebo kybernetická bezpečnostní rizika. Vytvoření evropských systémů certifikace kybernetické bezpečnosti v souladu s uvedeným rámcem umožní, aby byly certifikáty vydané podle těchto systémů platné a uznávané ve všech členských státech, a zároveň umožní vyřešit stávající roztříštěnost trhu.

1.4.6. Přidaná hodnota ze zapojení EU

Kybernetická bezpečnost je vskutku globální záležitostí, která je přeshraniční povahy a která se vzhledem k vzájemné provázanosti sítí a informačních systémů stává stále více meziodvětvovou. Počet, složitost a rozsah kybernetických bezpečnostních incidentů a jejich dopad na ekonomiku a společnost se postupem času zvyšují a očekává se, že souběžně s technologickým rozvojem, například šířením internetu věcí, se budou zvyšovat i nadále. Z toho vyplývá, že potřeba většího společného úsilí členských států, orgánů EU a zúčastněných stran ze soukromého sektoru čelit kybernetickým bezpečnostním hrozbám se v budoucnu pravděpodobně nezmenší.

Cílem agentury ENISA byla od jejího zřízení v roce 2004 podpora spolupráce mezi členskými státy a zúčastněnými stranami směrnice o bezpečnosti sítí a informací, včetně podpory spolupráce veřejného a soukromého sektoru. Tato podpora spolupráce zahrnovala technické činnosti, jež měly poskytnout celounijní obrázek o stavu kybernetických bezpečnostních hrozeb, zřizování skupin odborníků a organizování celoevropských cvičení pro soukromý a veřejný sektor zaměřených na řešení kybernetických incidentů a krizí (zejména „Cyber Europe“). Směrnice o bezpečnosti sítí a informací pověřila agenturu ENISA dodatečnými úkoly, včetně zajištění služeb sekretariátu pro síť CSIRT zřízené za účelem operativní spolupráce mezi členskými státy.

Přidaná hodnota opatření na úrovni EU, zejména opatření ke zvýšení spolupráce mezi členskými státy, ale také mezi komunitami v oblasti bezpečnosti sítí a informací, byla uznána v závěrech Rady z roku 2016[48] a rovněž jasně vyplývá z hodnocení agentury ENISA z roku 2017, které ukazuje, že přidaná hodnota agentury spočívá především v její

[48] Závěry Rady o posílení evropského systému kybernetické odolnosti a o podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti – 15. listopadu 2016.

schopnosti posilovat spolupráci mezi těmito zúčastněnými stranami. Na úrovni EU není žádný jiný subjekt, který v oblasti bezpečnosti sítí a informací podporuje spolupráci stejné škály zúčastněných stran.

Přidaná hodnota agentury ENISA spočívající ve sbližování komunit a zúčastněných stran v oblasti kybernetické bezpečnosti se projevuje také v oblasti certifikace. Nárůst kyberkriminality a bezpečnostních hrozeb měl za následek vznik vnitrostátních iniciativ stanovících přísné požadavky na kybernetickou bezpečnost a certifikaci komponentů IKT používaných v tradiční infrastruktuře. Ačkoliv jsou tyto iniciativy důležité, je s nimi spojeno riziko, že povedou k roztříštěnosti jednotného trhu a vytvoří překážky bránící interoperabilitě. Aby prodejci IKT mohli prodávat v několika členských státech, musí často podstoupit několik certifikačních procesů. Je nepravděpodobné, že by se neúčinnost/neefektivnost stávajících systémů certifikace podařilo vyřešit bez zásahu EU. A je velmi pravděpodobné, že bez opatření se roztříštěnost trhu spolu se vznikem nových systémů certifikace ve střednědobém horizontu (příštích 5 až 10 let) ještě zvýší. Nedostatečná koordinace a interoperabilita mezi systémy je prvek, který snižuje potenciál jednotného digitálního trhu. To dokazuje přidanou hodnotu zavedení evropského rámce pro certifikaci kybernetické bezpečnosti produktů a služeb IKT, který zavádí vhodné podmínky pro účinné řešení problému souvisejícího s koexistencí různých certifikačních postupů v různých členských státech a snižuje náklady na certifikaci, čímž certifikaci v EU z komerčního a konkurenčního hlediska celkově zatraktivňuje.

1.4.7. Závěry vyvozené z podobných zkušeností v minulosti

Komise v souladu s právním základem agentury ENISA provedla hodnocení agentury, které zahrnovalo nezávislou studii, jakož i veřejnou konzultaci. Hodnocení dospělo k závěru, že cíle agentury ENISA jsou stále aktuální. V souvislosti s technologickým rozvojem a vyvíjejícími se hrozbami a s ohledem na naléhavou nutnost zvýšit bezpečnost informací a sítí v EU je zapotřebí technických odborných poznatků o vývoji problémů, jež jsou s bezpečnosti sítí a informací spojeny. V členských státech je třeba vybudovat kapacity, které umožní porozumět hrozbám a reagovat na ně, a zúčastněné strany musí spolupracovat napříč tematickými oblastmi a napříč institucemi.

Agentura úspěšně přispívá k větší bezpečnosti sítí a informací v Evropě tím, že nabízí budování kapacit ve 28 členských státech a posiluje spolupráci mezi členskými státy a zúčastněnými stranami v oblasti bezpečnosti sítí a informací, a dále poskytováním odborných poznatků, budováním komunit a podporou politiky.

Agentuře ENISA se alespoň do určité míry podařilo ovlivnit rozsáhlou oblast bezpečnosti sítí a informací, úplně se jí však nepodařilo vytvořit si silnou značku a zajistit si dostatečnou viditelnost, aby začala být uznávána jako hlavní odborné středisko v Evropě. Lze to vysvětlit širokým mandátem agentury ENISA, na který nebyly vyčleněny dostatečné prostředky. Kromě toho agentura ENISA zůstává jedinou agenturou EU s mandátem na dobu určitou, což omezuje její schopnost rozvíjet dlouhodobou vizi a udržitelným způsobem podporovat své zúčastněné strany. Je to rovněž v rozporu s ustanoveními směrnice o bezpečnosti sítí a informací, která agentuře ENISA svěřují úkoly, u nichž není stanoveno konečné datum.

Pokud jde o certifikaci kybernetické bezpečnosti produktů a služeb IKT, v současné době neexistuje žádný evropský rámec. Nárůst kyberkriminality a bezpečnostních hrozeb měl však za následek vznik vnitrostátních iniciativ, které vytvářejí riziko roztříštěnosti jednotného trhu.

1.4.8. Soulad a možná synergie s dalšími vhodnými nástroji

Tento podnět je v naprostém souladu se stávajícími politikami, zejména v oblasti vnitřního trhu. Je navržen v souladu s celkovým přístupem ke kybernetické bezpečnosti, definovaným v přezkumu strategie pro jednotný digitální trh, aby doplňoval komplexní soubor opatření, např. přezkum strategie kybernetické bezpečnosti EU, plán spolupráce v případě kybernetických krizí a iniciativy na boj proti kyberkriminalitě. Zajistil by sblížení s ustanoveními stávajících právních předpisů o kybernetické bezpečnosti a vycházel by z nich, zejména směrnice o bezpečnosti sítí a informací, a to za účelem dalšího prosazování kybernetické odolnosti EU zlepšováním schopností, spolupráce a řízení rizik a zvyšováním informovanosti o otázkách kybernetické bezpečnosti.

Navrhovaná certifikační opatření by měla řešit potenciální roztříštěnost způsobenou stávajícími a vznikajícími vnitrostátními systémy certifikace, čímž by přispěla k rozvoji jednotného digitálního trhu. Podnět rovněž podporuje a doplňuje provádění směrnice o bezpečnosti sítí a informací tím, že podnikům, na něž se směrnice vztahuje, poskytuje nástroj k prokázání souladu s požadavky na bezpečnost sítí a informací v celé Unii.

Navrhovaným evropským rámcem pro certifikaci kybernetické bezpečnosti IKT není dotčeno obecné nařízení o ochraně osobních údajů[49], a zejména příslušná ustanovení týkající se certifikace[50] uplatňovaná na bezpečnost zpracování osobních údajů. V neposlední řadě by systémy navržené v budoucím evropském rámci měly vycházet z mezinárodních norem, aby se předešlo vytváření překážek obchodu a zajistila soudržnost s mezinárodními iniciativami.

[49] Nařízení (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[50] Například články 42 (Vydávání osvědčení) a 43 (Subjekty pro vydávání osvědčení), jakož i články 57, 58 a 70 týkající se příslušných úkolů a pravomocí nezávislých dozorových úřadů a úkolů Evropského sboru pro ochranu osobních údajů.

1.5. Doba trvání akce a finanční dopad

☐ **Časově omezený** návrh/podnět

– ☐ Návrh/podnět s platností od [DD/MM]RRRR do [DD/MM]RRRR

– ☐ Finanční dopad od RRRR do RRRR

☒ **Časově neomezený** návrh/podnět

– Provádění s obdobím rozběhu od roku 2019 do roku 2020,

– poté plné fungování.

1.6. Předpokládaný způsob řízení[51]

☒ **Přímé řízení** Komisí (Hlava III – Certifikace)

– ☐ prostřednictvím výkonných agentur

☐ **Sdílené řízení** s členskými státy

☒ **Nepřímé řízení**, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

☐ mezinárodní organizace a jejich agentury (upřesněte);

☐ EIB a Evropský investiční fond;

☒ subjekty uvedené v článcích 208 a 209 finančního nařízení (Hlava II – agentura ENISA)

☐ veřejnoprávní subjekty;

☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém poskytují dostatečné finanční záruky;

☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství soukromého a veřejného sektoru a poskytující dostatečné finanční záruky;

☐ osoby pověřené prováděním zvláštních činností v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.

Poznámky

Nařízení se vztahuje na: – hlava II navrhovaného nařízení přezkoumává mandát Agentury Evropské unie pro bezpečnost sítí a informací (ENISA) a přiznává jí důležitou úlohu při certifikaci, zatímco – hlava III zřizuje rámec pro vytvoření evropských systémů certifikace kybernetické bezpečnosti produktů a služeb IKT, v němž agentura ENISA plní zásadní úlohu.

[51] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Sledování bude zahájeno ihned po přijetí právního nástroje a bude se zaměřovat na jeho uplatňování. Komise bude organizovat setkání s agenturou ENISA, zástupci členských států (např. skupinou odborníků) a příslušnými zúčastněnými stranami, zejména za účelem usnadnění provádění předpisů týkajících se certifikace, jak např. zřízení rady.

První hodnocení by se mělo konat pět let po vstupu právního nástroje v platnost, budou-li k dispozici dostatečné údaje. Do právního nástroje je začleněno explicitní ustanovení o hodnocení a přezkumu [článek XXX], na jehož základě Komise provede nezávislé hodnocení. Komise následně o svém hodnocení podá zprávu Evropskému parlamentu a Radě, případně spolu s návrhem na přezkum, za účelem změření dopadu nařízení a jeho přidané hodnoty. Další hodnocení by se měla konat každých pět let. Na hodnocení se použije metodika Komise pro zdokonalení tvorby právních předpisů. Tato hodnocení budou provedena s pomocí cílených odborných diskusí, studií a širokých konzultací se zúčastněnými stranami.

Výkonný ředitel agentury ENISA by měl správní radě každé dva roky předložit hodnocení *ex post* týkající se činnosti agentury ENISA. Agentura by rovněž měla vypracovat akční plán v návaznosti na závěry zpětných hodnocení a jednou za dva roky podat Komisi zprávu o pokroku. Za dohled nad přijetím odpovídajících opatření v návaznosti na tyto závěry by měla nést odpovědnost správní rada.

Údajné případy nesprávného úředního postupu při činnostech agentury mohou podléhat šetřením evropského veřejného ochránce práv podle ustanovení článku 228 Smlouvy.

Zdrojem údajů pro plánované sledování by byly převážně agentura ENISA, Evropská skupina pro certifikaci kybernetické bezpečnosti, skupina pro spolupráci, síť CSIRT a orgány členských států. Kromě údajů získaných ze zpráv (včetně výročních zpráv o činnosti) agentury ENISA, Evropské skupiny pro certifikaci kybernetické bezpečnosti, skupiny pro spolupráci a sítě CSIRT se v případě potřeby použijí konkrétní nástroje pro shromažďování údajů (například průzkumy prováděné u vnitrostátních orgánů, Eurobarometr a zprávy z kampaně Měsíc kybernetické bezpečnosti a z celoevropských cvičení).

2.2. Systém řízení a kontroly

2.2.1. Zjištěná rizika

Zjištěná rizika jsou omezená: agentura Unie již existuje a její mandát bude vymezen posílením oblastí, kde se jasně ukázala přidaná hodnota agentury, doplněním nových oblastí, v nichž je nezbytná pomoc s ohledem na nové politické priority a nástroje, zejména na směrnici o bezpečnosti sítí a informací, na přezkum strategie kybernetické bezpečnosti EU a na nadcházející plán kybernetické bezpečnosti EU pro spolupráci v případě kybernetických krizí a pro certifikaci bezpečnosti IKT.

Návrh proto podrobně popisuje funkce agentury a vede k úsporám z důvodu vyšší efektivity. Zvýšení operačních pravomocí a úkolů nepředstavuje skutečné riziko, jelikož tyto úkoly

a pravomoci mají doplňovat opatření členských států a na jejich žádost je podporovat ve vztahu k omezeným a předem identifikovaným službám.

V rámci společného přístupu navrhovaný model agentury navíc zajistí, že bude zavedena dostatečná kontrola zaručující, že agentura ENISA plní své cíle. Provozní a finanční rizika navrhovaných změn se zdají být omezená.

Zároveň je nutné zajistit přiměřené finanční zdroje, aby agentura ENISA mohla plnit úkoly, které jí byly svěřeny novým mandátem, a to i v oblasti certifikace.

2.2.2. Předpokládané metody kontroly

Účetní závěrky agentury budou předkládány ke schválení Účetnímu dvoru a budou podléhat postupu udělení absolutoria; zároveň se počítá s audity.

Činnost agentury je rovněž pod dohledem veřejného ochránce práv v souladu s článkem 228 Smlouvy.

Viz také body 2.1 a 2.2.1 výše.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření.

Použijí se preventivní a ochranná opatření agentury ENISA, konkrétně:

– Platby za veškeré požadované služby nebo studie jsou před provedením kontrolovány zaměstnanci agentury při zohlednění veškerých smluvních závazků, hospodářských zásad a osvědčených finančních nebo řídicích postupů. Ustanovení proti podvodům jsou součástí veškerých dohod a smluv uzavřených mezi agenturou a příjemci jakýchkoli plateb (dohled, požadavky na hlášení atd.).

– V zájmu boje proti podvodům, korupci a jiným protiprávním činnostem se na agenturu bez omezení vztahuje nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 a nařízení Rady ze dne 11. září 2013 o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF).

– Agentura do šesti měsíců ode dne vstupu tohoto nařízení v platnost přistoupí k interinstitucionální dohodě ze dne 25. května 1999 mezi Evropským parlamentem, Radou Evropské unie a Komisí Evropských společenství o interním vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) a neprodleně přijme příslušná ustanovení vztahující se na všechny zaměstnance agentury.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

- Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
		RP/NRP[52].	zemí ESVO[53]	kandidátských zemí[54]	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
1a Konkurenceschopnost pro růst a zaměstnanost	09.0203 Agentura ENISA a certifikace bezpečnosti informační a komunikační technologie	RP	ANO	NE	NE	NE
5 Správní výdaje]	09.0101 Výdaje související se zaměstnanci v činné službě v oblasti politiky „Komunikační sítě, obsah a technologie“ 09.0102 Výdaje související s externími pracovníky v činné službě v oblasti politiky „Komunikační sítě, obsah a technologie“	NRP	NE	NE	NE	NE

[52] RP = rozlišené prostředky / NRP = nerozlišené prostředky.
[53] ESVO: Evropské sdružení volného obchodu.
[54] Kandidátské země a případně potenciální kandidátské země západního Balkánu.

	09.010211 Ostatní výdaje na řízení					

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	1a	Konkurenceschopnost pro růst a zaměstnanost

Agentura ENISA			**Výchozí rok** **2017 (31. 12. 2016)**		**2019** ***(od 1. 7. 2019)***	**2020**	**2021**	**2022**	**CELKEM**
Hlava 1: Výdaje na zaměstnance *(zahrnují rovněž výdaje související s přijímáním zaměstnanců, školením, socio-lékařskou infrastrukturou a externími službami)*	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: Výdaje na infrastrukturu a provozní výdaje	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: Provozní výdaje	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**
CELKEM prostředky pro agenturu ENISA	Závazky	=1+1 a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Platby	=2+2 a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Okruh víceletého finančního rámce	**5**	„Správní výdaje“

v milionech EUR (zaokrouhleno na tři desetinná místa)

		2019 *(od 1. 7. 2019)*	**2020**	**2021**	**2022**	**CELKEM**
GŘ: CNECT						
• Lidské zdroje		0,216	0,846	0,846	0,846	**2,754**
• Ostatní správní výdaje		0,102	0,235	0,238	0,242	**0,817**
CELKEM GŘ CNECT	Prostředky	0,318	1,081	1,084	1,088	**3,571**

Náklady na zaměstnance byly vypočítány podle plánovaného data náboru (předpokládá se, že zaměstnání bude zahájeno od 1. 7. 2019).

Výhled zdrojů po roce 2020 je orientační a nejsou jím dotčeny návrhy Komise týkající se víceletého finančního rámce na období po roce 2020.

CELKEM prostředky na OKRUH 5 víceletého finančního rámce	(Závazky celkem = platby celkem)	0,318	1,081	1,084	1,088	**3,571**

v milionech EUR (zaokrouhleno na tři desetinná místa)

		2019	**2020**	**2021**	**2022**	**CELKEM**
CELKEM prostředky	Závazky	16,868	21,727	23,332	24,11	**86,038**

z OKRUHU 1 až 5 víceletého finančního rámce	Platby	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Odhadovaný dopad na prostředky agentury

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků

– ☒ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy[55] ⇩	**2019**	**2020**	**2021**	**2022**	**CELKEM**
Zvýšení schopností a připravenosti členských států a podniků	1,408	1,900	1,931	1,969	7,208
Zlepšení spolupráce a koordinace napříč členskými státy a orgány, institucemi a jinými subjekty EU	0,939	1,266	1,288	1,313	4,806
Zvýšení schopnost na úrovni EU doplňovat opatření členských států, zejména v případě přeshraničních kybernetických krizí	0,704	0,950	0,965	0,985	3,604
Zvyšování informovanosti občanů a podniků o otázkách týkajících se kybernetické bezpečnosti	0,704	0,950	0,965	0,985	3,604
Posílení důvěry v jednotný digitální trh a digitální inovace zvýšením celkové transparentnosti záruky kybernetické bezpečnosti produktů a služeb IKT	0,939	1,266	1,288	1,313	4,806
NÁKLADY CELKEM	4,694	6,332	6,437	6,565	24,028

[55] Tato tabulka uvádí pouze provozní výdaje podle hlavy 3.

3.2.3. Odhadovaný dopad na lidské zdroje agentury

3.2.3.1. Shrnutí

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

– ☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	3./4. čtvrtletí 2019	**2020**	**2021**	**2022**
Dočasní úředníci (třídy AD)	4,242	5,695	6,381	6,709
Dočasní úředníci (třídy AST)	1,601	1,998	2,217	2,217
Smluvní zaměstnanci	2,041	2,041	2,041	2,041
Vyslaní národní odborníci	0,306	0,447	0,656	0,796
CELKEM	**8,190**	**10,181**	**11,295**	**11,763**

Náklady na zaměstnance byly vypočítány podle plánovaného data náboru (u současných zaměstnanců agentury ENISA byla plná zaměstnanost předpokládána od 1. 1. 2019). V případě nových zaměstnanců se předpokládalo postupné zaměstnávání od 1. 7. 2019 a dosažení plné zaměstnanosti v roce 2022. Výhled zdrojů po roce 2020 je orientační a nejsou jím dotčeny návrhy Komise týkající se víceletého finančního rámce na období po roce 2020.

Odhadovaný dopad na zaměstnance (dodatečné plné pracovní úvazky) – plán pracovních míst

Funkční skupina a třída	2017 **Stávající agentura ENISA**	3./4. čtvrtletí 2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
Celkem AD	34	9	8	6	3

AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Celkem AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Celkem AST/SC					
CELKOVÝ SOUČET	48	12	10	7	3

Úkoly dodatečných zaměstnanců třídy AD/AST za účelem dosažení cílů nástroje popsaných v oddíle 1.4.2:

Úkoly	AD	AST	VNO	Celkem
Tvorba politiky a budování kapacit	8	1		9
Operativní spolupráce	8	1	7	16
Certifikace (úkoly související s trhem)	9	3	2	14
Znalosti, informace a zvyšování informovanosti	1	1		2
CELKEM	26	6	9	41

Popis úkolů:

Úkoly	**Požadované dodatečné zdroje**
Tvorba a provádění politiky EU a budování kapacit	Úkoly by zahrnovaly pomoc skupině pro spolupráci, podporu jednotného uplatňování bezpečnosti sítí a informací v přeshraničním rozměru, pravidelné podávání zpráv o stavu provádění právního rámce EU; poskytovaní poradenství a zajišťování koordinace pro potřeby odvětvových iniciativ v oblasti kybernetické bezpečnosti, včetně odvětví energetiky, dopravy (např. letecká/silniční/námořní doprava, propojená vozidla), zdravotnictví, finančnictví,

	poskytování podpory při zřizování středisek pro sdílení a analýzu informací (ISAC) v různých odvětvích.
Operativní spolupráce a řešení krizí	**Úkoly by zahrnovaly:** Zajišťování služeb sekretariátu pro síť CSIRT, mimo jiné zajišťováním řádného fungování infrastruktury IT a komunikačních kanálů sítě CSIRT. Zajišťování strukturované spolupráce s týmem CERT-EU, centrem EC3 a dalšími příslušnými subjekty EU. Organizování **cvičení Cyber Europe**[56] – úkoly související se zvýšením četnosti cvičení z události konající se jednou za dva roky na každoroční událost a zajištěním toho, aby cvičení pokrývala incident od jeho začátku až do konce. **Technická pomoc** – úkoly by zahrnovaly strukturovanou spolupráci s týmem CERT-EU za účelem poskytnutí technické pomoci v případě významných incidentů a podporu analýzy incidentů. Součástí by bylo poskytnout členským státům pomoc při řešení incidentů a analýze zranitelností, artefaktů a incidentů. Usnadnění spolupráce mezi jednotlivými členskými státy při řešení reakcí na mimořádné události analýzou a agregováním vnitrostátních situačních zpráv na základě informací, které agentuře poskytnou členské státy a jiné subjekty. **Plán koordinované reakce na rozsáhlé přeshraniční kybernetické incidenty** – agentura bude na úrovni Unie a členských států přispívat k rozvoji koordinované reakce na rozsáhlé přeshraniční incidenty nebo krize související s kybernetickou bezpečností řadou úkolů od podpory vytváření povědomí o situaci na úrovni Unie až po zkoušení plánů spolupráce v případě incidentů. **Technická šetření incidentů** *ex post* – ve spolupráci se sítí CSIRT provádět technická šetření incidentů *ex post* nebo k nim přispívat s cílem posilovat schopnosti a vydávat doporučení ve formě veřejných zpráv, aby bylo

[56] Cyber Europe je dodnes největším a nejúplnějším cvičením EU v oblasti kybernetické bezpečnosti, do kterého je zapojeno více než 700 odborníků na kybernetickou bezpečnost ze všech 28 členských států. Koná se jednou za dva roky. Hodnocení agentury ENISA a strategie kybernetické bezpečnosti EU z roku 2013 poukazují na skutečnost, že řada zúčastněných stran vzhledem k rychle se rozvíjející povaze kybernetických hrozeb podporuje zvýšení četnosti cvičení Cyber Europe tak, aby se konalo jednou ročně. To však vzhledem k omezeným zdrojům agentury není v současné době proveditelné.

	možné lépe předcházet budoucím incidentům.
Úkoly související s trhem (normalizace, certifikace)	Úkoly by zahrnovaly aktivní podporu činností prováděných v rámci rámce pro certifikaci, včetně poskytování technických odborných znalostí pro vypracování návrhů evropských systémů certifikace kybernetické bezpečnosti. Úkoly by rovněž zahrnovaly podporu tvorby a provádění politiky Unie v oblasti normalizace, certifikace a sledování trhu – to si vyžádá snazší zavádění norem pro řízení rizik u elektronických produktů, sítí a služeb a poskytování poradenství provozovatelům základních služeb a poskytovatelům digitálních služeb ohledně technických bezpečnostních požadavků. Úkoly by rovněž zahrnovaly poskytování analýzy hlavních trendů na trhu kybernetické bezpečnosti.
Znalosti, informace a zvyšování informovanosti	S cílem zajistit snazší přístup k lépe strukturovaným informacím o rizicích kybernetické bezpečnosti a o potenciálních prostředcích nápravy návrh svěřuje agentuře nový úkol, a to vytvořit a spravovat „informační centrum“ Unie. Úkol by zahrnoval shromažďování a uspořádávání informací o bezpečnosti sítí a informačních systémů, zejména pak kybernetické bezpečnosti, poskytnutých orgány a dalšími subjekty EU, a jejich zpřístupňování veřejnosti prostřednictvím specializovaného portálu. Úkoly by rovněž zahrnovaly podporu činností agentury ENISA v oblasti zvyšování informovanosti, čímž by agentura měla více zviditelnit své úsilí.

3.2.3.2. Odhadované potřeby v oblasti lidských zdrojů mateřského GŘ

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.

– ☒ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v celých číslech (nebo zaokrouhlete nejvýše na jedno desetinné místo)

		Dodateční zaměstnanci			
	Výchozí rok 2017	3./4. čtvrtletí 2019	2020	2021	2020
• **Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)**					
09 01 01 01 (v ústředí a v zastoupeních Komise)	1	2	3		
• **Externí zaměstnanci (v přepočtu na plné pracovní úvazky: ekvivalent plného pracovního úvazku)**[57]					
09 01 02 01 (SZ, VNO, ZAP z celkového rámce)	1	2			
CELKEM		**4**	**3**		

Popis úkolů:

Úředníci a dočasní zaměstnanci	Zastupují Komisi ve správní radě agentury. Vypracovávají stanoviska Komise k jednotnému programovému dokumentu agentury ENISA a sledují jeho provádění. Dohlížejí na přípravu rozpočtu agentury a sledují jeho plnění. Napomáhají agentuře při rozvoji jejích činností v souladu s politikami Unie, mimo jiné účastí na příslušných zasedáních. Dohlížejí na zavádění rámce pro evropské systémy certifikace kybernetické bezpečnosti produktů a služeb IKT. Udržují kontakty s členskými státy a dalšími příslušnými zúčastněnými stranami v souvislosti s certifikačním úsilím. Spolupracují s agenturou ENISA, pokud jde o návrhy systémů. Vypracovávají návrhy evropských systémů certifikace kybernetické bezpečnosti.

[57] SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

Externí zaměstnanci	viz výše

3.2.4. Soulad se stávajícím víceletým finančním rámcem

– ☐ Návrh/podnět je v souladu se stávajícím víceletým finančním rámcem.

– ☒ Návrh/podnět si vyžádá úpravu příslušného okruhu víceletého finančního rámce.

Návrh si vzhledem k revizi mandátu agentury ENISA, který agentuře svěřuje nové úkoly týkající se mimo jiné provádění směrnice o bezpečnosti sítí a informací a evropského rámce pro certifikaci kybernetické bezpečnosti, vyžádá úpravu článku 09 02 03. Odpovídající částky:

Rok	Předpokládané	Požadované
2019	10,739	16,550
2020	10,954	20,646
2021	Nepoužije se	22,248
2022	Nepoužije se	23,023*

***** Jedná se o odhad. Finanční prostředky EU po roce 2020 budou zkoumány v rámci debaty celé Komise týkající se veškerých návrhů na období po roce 2020. To znamená, že jakmile Komise předloží svůj návrh příštího víceletého finančního rámce, předloží Komise pozměněný legislativní finanční výkaz zohledňující závěry posouzení dopadů[58].

– ☐ Návrh/podnět vyžaduje použití nástroje pružnosti nebo změnu víceletého finančního rámce[59].

3.2.5. Příspěvky třetích stran

– ☐ Návrh/podnět nepočítá se spolufinancováním od třetích stran.

– ☒ Návrh/podnět počítá se spolufinancováním podle následujícího odhadu:

	Rok **2019**	Rok **2020**	Rok **2021**	Rok **2022**
ESVO	p.m[60].	p.m.	p.m.	p.m.

58 Odkaz na stránku s posouzením dopadů.

59 Viz články 11 a 17 nařízení Rady (EU, Euratom) č. 1311/2013, kterým se stanoví víceletý finanční rámec na období 2014–2020.

60 Přesná částka pro následující roky bude známa poté, co bude pro dotyčný rok stanoven činitel úměrnosti pro ESVO.

3.3. Odhadovaný dopad na příjmy

– ☒ Návrh/podnět nemá žádný finanční dopad na příjmy.

– ☐ Návrh/podnět má tento finanční dopad:

  – ☐ dopad na vlastní zdroje

  – ☐ dopad na různé příjmy