Rada
Evropské unie

Brusel 29. května 2018
(OR. en)

9350/18

Interinstitucionální spis:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

POZNÁMKA

Odesílatel:	Předsednictví
Příjemce:	Rada
Č. předchozího dokumentu:	8834/18
Č. dok. Komise:	12183/17
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“) – obecný přístup

I. ÚVOD

1. Dne 13. září 2017 Komise v rámci jednotného digitálního trhu přijala a předložila Radě a Evropskému parlamentu výše uvedený návrh[1], přičemž jako právní základ použila článek 114 SFEU. Jakožto součást tzv. balíčku předpisů v oblasti kybernetické bezpečnosti je cílem tohoto návrhu vysoká úroveň kybernetické bezpečnosti, kybernetické odolnosti a důvěry v rámci Unie s cílem zajistit řádné fungování vnitřního trhu.

2. Navrhované nařízení stanoví cíle, úlohy a organizační aspekty agentury ENISA, jež je agenturou EU pro kybernetickou bezpečnost, a tvoří rámec pro zavedení evropských systémů certifikace kybernetické bezpečnosti pro účely zajištění odpovídající úrovně kybernetické bezpečnosti produktů a služeb IKT v Unii. Návrh Komise je doplněn o posouzení dopadu, které zkoumá specifický soubor osmi politických možností vztahujících se na přezkum agentury ENISA a certifikaci kybernetické bezpečnosti IKT.

3. Navrhované nařízení zahrnuje dvě hlavní oblasti:

   - trvalý mandát pro agenturu s vymezenou oblastí působnosti s ohledem na potřeby v rámci nových priorit a nástrojů politiky a obnoveným souborem úkolů a funkcí pro agenturu s cílem umožnit účinnou a efektivní podporu úsilí členských států, orgánů EU a dalších zúčastněných stran v zájmu zajištění bezpečného kybernetického prostoru;

   - evropský rámec pro certifikaci kybernetické bezpečnosti pro produkty a služby IKT a pravidla, jimiž se řídí evropské systémy certifikace kybernetické bezpečnosti umožňující, aby osvědčení vydaná v rámci těchto systémů byla platná a uznávaná ve všech členských státech a aby se tak řešila stávající roztříštěnost trhu.

[1] Dokument 12183/17; dokument 12183/1/17 REV 1; Dokument 12183/2/17 REV 2.

4. V říjnu 2017 Evropská rada[2] vyzvala k tomu, aby návrhy Komise týkající se kybernetické bezpečnosti byly vypracovávány holisticky, aby byly předkládány včas a neprodleně projednávány, a to na základě akčního plánu, jejž stanoví Rada.

5. Dne 12. prosince 2017 Rada pro obecné záležitosti přijala akční plán[3] pro účely provádění závěrů Rady[4] o společném sdělení[5] Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU. Tento akční plán zohlednil ambici Rady dosáhnout obecného přístupu k návrhu do června 2018.

6. V Evropském parlamentu byla zpravodajkou jmenována Angelika NIEBLEROVÁ (ITRE, EPP). Hlasování výboru ITRE o její zprávě je naplánováno na 19. června 2018.

7. Evropský hospodářský a sociální výbor přijal stanovisko dne 14. února 2018.

II. ČINNOST V RÁMCI RADY

8. Komise tento návrh a své posouzení dopadu předložila na zasedání Horizontální pracovní skupiny pro otázky týkající se kybernetiky (dále jen „pracovní skupina“) dne 26. září 2017 a následně předložila přezkum posouzení dopadu na zasedání této pracovní skupiny konaném dne 20. října 2017. Následné diskuse se soustředily na operativní kapacitu agentury a rozsah její spolupráce s vnitrostátními příslušnými orgány, jakož i na dopad rámce certifikace na trh a konkurenceschopnost podniků. Obecně byla odezva delegací na posouzení dopadů i na návrh příznivá.

Dokument EUCO 14/17, s. 11.

[3] Dokument 15748/17.

[4] Dokument 14435/17.

[5] Dokument 12211/17.

9. Projednávání návrhu samotného pracovní skupinou bylo zahájeno v listopadu 2017 za estonského předsednictví a pokračovalo za bulharského předsednictví. K tomuto návrhu se konalo 12 zasedání, z nichž vzešlo osm následných revidovaných verzí návrhu s cílem dosáhnout dohody o obecném přístupu na nadcházejícím zasedání Rady pro dopravu, telekomunikace a energetiku (telekomunikace), jež se bude konat dne 8. června 2018.

10. Výsledek jednání na zasedání pracovní skupiny konaném ve dnech 14. a 15. května 2018, jakož i revidované kompromisní znění předsednictví jsou uvedeny v příloze této poznámky. Body odůvodnění byly upraveny tak, aby odrážely změny hmotněprávních ustanovení. Změny oproti návrhu Komise jsou vyznačeny **tučně** nebo symbolem [...]. Změny oproti poslednímu dokumentu pracovní skupiny 8834/18 jsou uvedeny **tučně podtrženě** a vypuštěný text je označen symbolem **[...]**.

III. ZÁVĚR

11. Kompromisní znění předsednictví, jak je uvedeno v příloze, zohledňuje úsilí předsednictví a členských států dosáhnout řádné vyváženosti znění.

12. Dne 25. května 2018 dosáhl Výbor stálých zástupců dohody o kompromisním znění předsednictví s výhradou změn v čl. 19 odst. 5 a čl. 48 odst. 5 ve znění uvedeném v příloze.

13. Rada se proto vyzývá, aby na svém zasedání konaném dne 8. června 2018 přijala obecný přístup a pověřila předsednictví k zahájení jednání o tomto návrhu se zástupci Evropského parlamentu a Evropské komise.

PŘÍLOHA

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o agentuře ENISA, *[...] Agentuře Evropské unie 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[6],

s ohledem na stanovisko Výboru regionů[7],

v souladu s řádným legislativním postupem,

[6] Úř. věst. C, , s. .
[7] Úř. věst. C, , s. .

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, nejsou navrženy s dostatečnými zabudovanými 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 se stává zranitelnější vůči kybernetickým hrozbám a zhoršuje se nebezpečí pro jednotlivé uživatele, 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, 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[8] o zřízení agentury ENISA za účelem přispět k cílům zajištění vysoké úrovně bezpečnosti sítí a informací v Unii a vytvořit kulturu 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[9], kterým byl mandát agentury prodloužen do března 2012. Nařízení (ES) č. 580/2011[10] prodlužuje mandát agentury do 13. září 2013. V roce 2013 přijaly Evropský parlament a Rada nařízení (EU) č. 526/2013[11] o agentuře ENISA a o zrušení nařízení (ES) č. 460/2004, kterým byl mandát agentury prodloužen do června 2020.

---

8 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).

9 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).

10 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).

11 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).

(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 stanovila 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, včetně poskytovatelů 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 transformovaného prostředí 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 **podporovat**[...] vnitrostátní úsilí a **aktivně přispívat k** 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 **a k aspektům specifickým pro dané odvětví s cílem zvýšit význam politik EU a právních předpisů s rozměrem kybernetické bezpečnosti a umožnit soudržnost při jejich provádění na vnitrostátní úrovni** [...]. 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 v jejich úsilí o vytváření a rozvoj schopností a připravenosti předcházet kybernetickým [...] **hrozbám** a incidentům, 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. **Činnosti provedené agenturou ENISA týkající se operativních kapacit členských států by měly být výhradně doplňkové k vlastním opatřením přijatým členskými státy s cílem splnit jejich povinnosti vyplývající ze směrnice o bezpečnosti sítí a informací, a proto by je neměly nahrazovat** [...].

(15a) 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 [...] **by agentura měla** podporovat **sdílení informací v rámci odvětví i mezi nimi, zejména v odvětvích uvedených v příloze II směrnice (EU) 2016/1148, a to poskytováním osvědčených postupů a pokynů ohledně dostupných nástrojů a postupů, jakož i pokynů ohledně toho, jak řešit otázky regulace týkající se sdílení informací, například usnadněním** [...] vytváření odvětvových středisek pro sdílení a analýzu informací (ISAC) [...].

(18) Agentura by měla agregovat a analyzovat **dobrovolně sdílené** vnitrostátní zprávy od týmů CSIRT a skupiny CERT-EU **pro účely pomoci členským státům** při stanovování společných [...] **postupů**, jazyka a terminologie pro výměnu informací. Agentura by rovněž měla zapojit soukromý sektor, a to v rámci směrnice o bezpečnosti sítí a informací, která stanovila základ pro dobrovolnou výměnu technických informací na operativní úrovni [...] **v rámci** sítě CSIRT.

(19) V případě rozsáhlých přeshraničních kybernetických bezpečnostních incidentů a krizí by agentura měla přispět k reakci na úrovni EU. Tato funkce by měla **být plněna v souladu s jejím mandátem v souladu s tímto nařízením a členské státy by měly dohodnout přístup v rámci doporučení Komise o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize. Mohla by** 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 [...] **pravidelných** cvičení v oblasti kybernetické bezpečnosti.

(20) [...]**Při podpoře** operační **spolupráce**[...] by agentura měla využít dostupné **technické a operační** poznatky skupiny CERT-EU, a to prostřednictvím strukturované spolupráce [...]. [...]. V případě potřeby by měla být učiněna speciální ujednání mezi oběma organizacemi o praktické podobě takové spolupráce **a mělo by se zabránit zdvojování činností**.

(21) V souladu s jejími [...] úkoly **k podpoře operační koordinace v rámci sítě týmů CSIRT** by agentura měla být schopna poskytnout členským státům **na jejich žádost** podporu, například ve formě poradenství **ohledně způsobu zlepšení jejich schopností předcházet incidentům, odhalovat je a reagovat na ně [...] usnadněním** [...] technického **řešení incidentů, které mají závažný nebo významný dopad**[...], nebo **prostřednictvím** zajišťování analýz hrozeb a incidentů. **Usnadnění technického řešení incidentů, které mají závažný nebo významný dopad, by mělo zejména zahrnovat, aby agentura ENISA podporovala dobrovolné sdílení technických řešení mezi členskými státy nebo aby vytvářela kombinované technické informace, jako jsou technická řešení dobrovolně sdílená členskými státy.** 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 [...] **podpoře operační spolupráce**.

(22) Jako součást pravidelné spolupráce na technické úrovni na podporu informovanosti Unie o aktuální situaci by agentura měla pravidelně **a v úzké spolupráci s členskými státy** 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 [...] sdílejí týmy CSIRT členských států nebo jednotná kontaktní místa zřízená podle směrnice o bezpečnosti sítí a informací **(obě dobrovolně)**, 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) **Podpora agentury** [...] technickým **šetřením** ex post [...] incidentů s významným dopadem [...] na základě žádosti [...] **dotčených** členských států by se měla zaměřovat na předcházení budoucím incidentům [...]. **Dotčené členské státy by měly poskytnout nezbytné informace s cílem umožnit agentuře technické šetření účinně podpořit.**

(24) [...]

(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 **veřejně dostupné nebo dobrovolně sdílené** 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 **incidentům** [...] 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 **kybernetické** bezpečnosti **infrastruktur podporujících zejména odvětví uvedená v příloze II směrnice o bezpečnosti sítí a informací a odvětví využitých poskytovateli digitálních služeb uvedených v příloze III této směrnice** [...], 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 obranné agentury (EDA), Evropské agentury pro provozní řízení rozsáhlých informačních systémů (eu-LISA), Evropské agentury pro bezpečnost letectví (EASA), **Agentury pro evropský globální navigační družicový systém (agentury pro GNSS)** 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 **ve funkci** [...] 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 [...] **pravidelná** 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 [...] kybernetické bezpečnosti. **S cílem stanovit potřeby v oblasti výzkumu by agentura měla rovněž konzultovat příslušné skupiny uživatelů.**

(37) [...] Kybernetické **hrozby** jsou globální záležitostí. Je nutná užší mezinárodní spolupráce pro zvýšení [...] standardů **v oblasti kybernetické bezpečnosti**, 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 **zahrnující provádění ročního pracovního programu agentury**, 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[12]. 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[13]. 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.

---

[12] 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).

[13] L 8, 12.1.2001, s. 1.

(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) [...]

(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 **procesů,** 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, 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 **a EU prohlášení o shodě** 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 nebo na [...] **evropských** normách, 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 **procesů,** produktů a služeb IKT. Tyto systémy by měly provádět a dozor nad nimi by měly vykonávat vnitrostátní orgány certifikace **kybernetické bezpečnosti** [...] 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 **procesy,** produkty a služby IKT certifikované podle takového systému splňovaly konkrétní požadavky [...] **s** cílem [...] **chránit** dostupnost, autentičnost, integritu nebo důvěrnost uchovávaných nebo předávaných nebo zpracovávaných dat nebo funkcí nebo služeb nabízených nebo dostupných prostřednictvím těchto produktů, procesů, služeb a systémů **v rámci jejich životního cyklu** ve smyslu tohoto nařízení. V tomto nařízení není možné podrobně stanovit kybernetickobezpečnostní požadavky týkající se veškerých **procesů,** produktů a služeb IKT. **Procesy,** produkty a služby IKT a související potřeby v oblasti kybernetické bezpečnosti jsou natolik rozmanité, že je velmi obtížné přijít s obecnými kybernetickobezpečnostními 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 **procesů,** 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**, nejsou-li dostupné odpovídající normy**.

(55a) Technické specifikace, které by měly být využity v evropském systému certifikace kybernetické bezpečnosti, by měly být stanoveny při respektování zásad stanovených v příloze II nařízení (EU) 1025/2012. Některé odchylky od těchto zásad by však mohly být v řádně odůvodněných případech považovány za nezbytné, pokud tyto technické specifikace musí být využity v evropském systému certifikace kybernetické bezpečnosti s odkazem na úroveň záruky „vysoká“. Důvody pro takové odchylky je třeba veřejně zpřístupnit.

(55b) Certifikované posuzování shody je procesem posouzení, zda byly splněny stanovené požadavky týkající procesu, produktu nebo služby IKT. Tento proces provádí nezávislá třetí strana, jiná něž výrobce produktu nebo poskytovatel služby. Proces vydání certifikátu následuje po procesu úspěšného posouzení procesu, produktu nebo služby IKT. Je třeba jej považovat za potvrzení toho, že příslušné posouzení bylo řádně provedeno. V závislosti na úrovni záruky by evropský systém pro kybernetickou bezpečnost měl stanovit, zda certifikát vydal soukromý nebo veřejný orgán. Posouzení shody a certifikace nemohou samy 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 služby IKT byly testovány a že splňují určité stanovené kybernetickobezpečnostní požadavky, např. požadavky stanovené v technických normách.

(55c) Uživatelé certifikátu by měli vybírat odpovídající úroveň certifikace a s ní spojené bezpečnostní požadavky na základě analýzy rizik použití procesů, produktů nebo služeb IKT. Úroveň záruky by tak měla odpovídat úrovni rizika spojeného se zamýšleným použitím procesu, produktu nebo služby IKT.

(55d) Evropský systém certifikace kybernetické bezpečnosti by mohl stanovit posouzení shody, která má být provedena v rámci výhradní odpovědnosti výrobce nebo poskytovatele produktů a služeb IKT (sebehodnocení shody). V takových případech je postačující, že výrobce nebo poskytovatel provede sám všechny kontroly s cílem zajistit soulad procesu, produktu nebo služeb IKT se systémem certifikace. Tento druh posouzení shody by měl být považován za vhodný pro produkty a služby IKT s nízkou složitostí (např. jednoduchý projekční a výrobní mechanismus), který představuje nízké riziko pro veřejný zájem. Navíc by se mohly předmětem sebehodnocení shody stát pouze produkty a služby IKT odpovídající úrovni záruky „základní“.

(55e) Evropský systém certifikace kybernetické bezpečnosti by mohl umožnit certifikaci i sebehodnocení shody produktů a služeb IKT. V takovém případě by systém měl stanovit jasné a srozumitelné prostředky pro spotřebitele nebo jiné uživatele pro rozlišení mezi produkty a službami, které jsou posuzovány v rámci odpovědnosti výrobce nebo poskytovatele, a produkty a službami, které jsou certifikovány třetí stranou.

(55f) Výrobce nebo poskytovatel produktů a služeb IKT, který provádí sebehodnocení shody, by měl vypracovat a podepsat EU prohlášení o shodě jako součást postupu posuzování shody. EU prohlášení o shodě je dokumentem, který uvádí, že určitý produkt nebo služba IKT splňuje požadavky systému. Vypracováním a podepsáním EU prohlášení o shodě výrobce nebo poskytovatel přebírá odpovědnost za to, že produkt nebo služba IKT splňuje právní požadavky tohoto systému. Kopie EU prohlášení o shodě by měla být předložena vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a agentuře ENISA.

(55g) Výrobce nebo poskytovatel produktů a služeb IKT by měl zachovat EU prohlášení o shodě a technickou dokumentaci se všemi důležitými informacemi týkajícími se shody produktů nebo služeb IKT se systémem, který je k dispozici příslušnému vnitrostátnímu orgánu certifikace kybernetické bezpečnosti po dobu vymezenou v daném evropském systému certifikace kybernetické bezpečnosti. Technická dokumentace by měla upřesňovat platné požadavky a v míře nutné pro posouzení se vztahovat na navrhování, výrobu a provoz produktu nebo služby IKT. Složení technické dokumentace by mělo být takové, aby umožnilo posouzení shody produktu nebo služby IKT s příslušnými požadavky.

(55h) Členské státy a zainteresované zúčastněné organizace by měly být oprávněny navrhovat Evropské skupině pro certifikaci kybernetické bezpečnosti přípravu navrhovaného systému. Zainteresované zúčastněné organizace jsou organizace zastupující průmysl nebo spotřebitele, včetně zástupců malých a středních podniků, které mají legitimní zájem na rozvoji určitého evropského systému certifikace kybernetické bezpečnosti. Takové návrhy by měly být posouzeny s ohledem na kritéria vypracovaná Evropskou skupinou pro certifikaci kybernetické bezpečnosti na základě pokynů založených na zásadách transparentnosti, otevřenosti, nestrannosti, konsenzu, účinnosti, relevantnosti a soudržnosti.

56) Komisi **a skupině** by měla být svěřena pravomoc požádat agenturu ENISA, aby **bezodkladně** vypracovala návrhy systémů pro konkrétní **procesy,** 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 **procesů,** produktů a služeb IKT, na které se certifikace vztahuje, podrobnou specifikaci kyberneticko-bezpečnostních požadavků, například prostřednictvím odkazu na příslušnou normu nebo technickou specifikaci, konkrétní kritéria a metody hodnocení a úroveň záruky: základní, podstatná nebo vysoká, kterou mají zajistit**, a případně úroveň hodnocení**.

56a) Záruka evropského systému certifikace je podkladem pro důvěru, že proces, produkt či služba IKT splňuje bezpečnostní požadavky konkrétního evropského systému certifikace kybernetické bezpečnosti. V zájmu zajištění soudržnosti rámce pro certifikované procesy, produkty a služby IKT by evropský systém certifikace kybernetické bezpečnosti mohl stanovit úrovně záruky pro evropské certifikáty kybernetické bezpečnosti a v rámci tohoto systému vydávat prohlášení EU o shodě. Každý certifikát by mohl uvádět jednu úroveň záruky: základní, podstatnou či vysokou, zatímco prohlášení EU o shodě by se mohlo vztahovat pouze na základní úroveň záruky. Úroveň záruky odráží odpovídající stupeň úsilí vynaloženého na hodnocení [...] a je popsána odkazem na technické specifikace, normy a postupy v ní uvedené, včetně technických kontrol, přičemž jejím účelem je zmírnit dopady kybernetických bezpečnostních incidentů nebo jim zabránit. Každá úroveň záruky by měla být konzistentní v rámci jednotlivých odvětví, v nichž se certifikace používá.

56b) Evropský systém certifikace kybernetické bezpečnosti může specifikovat několik hodnotících úrovní v závislosti na náročnosti a zevrubnosti použité hodnotící metodiky, která by měla odpovídat jedné z úrovní záruk a být navázána na příslušnou kombinaci složek záruky. Pro každou úroveň záruky by produkt či služba IKT měla obsahovat řadu bezpečných funkcí stanovených v systému, jež mohou zahrnovat: bezpečnou přednastavenou konfiguraci, digitální podpis, bezpečnou aktualizaci a ochranu před zneužitím slabých míst v zabezpečení a přetečením na paměťovém zásobníku. Tyto funkce již měly být vyvinuty a měly by být provozovány za použití bezpečnostně orientovaných vývojových přístupů a souvisejících nástrojů, aby byla zajištěna spolehlivá integrace účinných (softwarových i hardwarových) mechanismů. Pro základní úroveň záruky by mělo hodnocení vycházet alespoň z následujících prvků: hodnocení by mělo přinejmenším zahrnovat přezkum technické dokumentace produktu či služby IKT ze strany orgánu pro posuzování shody. Zahrnuje-li certifikace procesy IKT, měl by do předmětu přezkumu spadat též proces použitý k navržení, vývoji a provozu produktu či služby IKT. V případech, kdy evropský systém certifikace kybernetické bezpečnosti stanoví vlastní posouzení souladu, by mělo postačovat, že výrobce či poskytovatel provedl vlastní posouzení souladu procesu, produktů či služeb IKT se systémem certifikace. Pro podstatnou úroveň záruky by hodnocení mělo navíc k základní úrovni záruky vycházet přinejmenším z ověření souladu bezpečnostních funkcí produktu či služby IKT s příslušnou technickou dokumentací. Pro vysokou úroveň záruky by hodnocení mělo navíc k podstatné úrovni záruky vycházet přinejmenším z ověření účinnosti posuzujícího odolnost bezpečnostních funkcí produktu či služby IKT vůči propracovaným kybernetickým útokům spáchaným subjekty se značnými dovednostmi a zdroji.

56c) Při vypracovávání návrhu systému by agentura ENISA měla konzultovat všechny relevantní zúčastněné strany, jako jsou evropské normalizační organizace, příslušné vnitrostátní orgány, organizace založené na dohodách o vzájemném uznávání, jako je skupina SOG-IS, MSP, spotřebitelské organizace, jakož i zúčastněné subjekty v oblasti životního prostředí a v sociální oblasti.

56d) Agentura ENISA by měla provozovat internetovou stránku, která poskytuje informace o evropských systémech certifikace kybernetické bezpečnosti a tyto systémy propaguje a která by mimo jiné měla zahrnovat žádosti o návrh evropského systému certifikace kybernetické bezpečnosti, jakož i zpětnou vazbu získanou v přípravné fázi agenturou ENISA v rámci konzultačního procesu. Tato internetová stránka by měla rovněž poskytovat informace o osvědčeních a prohlášeních EU o shodě podle tohoto nařízení.

57) Využití evropské certifikace kybernetické bezpečnosti **a prohlášení EU o shodě** by mělo zůstat dobrovolné, pokud unijní nebo vnitrostátní právní předpisy **přijaté v souladu s právem Unie** nestanoví jinak. **V případě neexistence harmonizovaných právních předpisů mohou členské státy přijmout vnitrostátní technická nařízení v souladu se směrnicí (EU) 2018/1535, která stanoví povinnou certifikaci v rámci evropského systému certifikace kybernetické bezpečnosti. Členské státy by mohly rovněž využít evropské certifikace kybernetické bezpečnosti v souvislosti se zadáváním veřejných zakázek a se směrnicí 2014/214/EU**. [...]

57a) V zájmu 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. Členským státům by však nemělo být bráněno v přijímání či v zachování vnitrostátních systémů certifikace pro účely národní 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 **omezit, pozastavit či** 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) [...] Členské státy [...] **by měly** určit jeden **nebo více orgánů** certifikace kybernetické bezpečnosti [...] s cílem dohlížet na soulad **s povinnostmi vyplývajícími z tohoto nařízení. Považuje-li to členský stát za vhodné, mohou být příslušné úkoly přiděleny již existujícím orgánům. Na základě vzájemné dohody s jiným členským státem by členské státy rovněž měly mít možnost rozhodnout, že určí jeden nebo více orgánů dohledu na území tohoto jiného členského státu. Orgán by měl zejména monitorovat a vymáhat povinnosti výrobce nebo poskytovatele produktů a služeb IKT usazených na jejich příslušném území, pokud jde o prohlášení EU o shodě, pomáhat vnitrostátním akreditačním orgánům při sledování a dohledu nad činnostmi subjektů posuzování shody tím, že jim poskytuje odborné znalosti a relevantní informace, a pověřovat subjekty posuzování shody prováděním svých úkolů, pokud plní dodatečné požadavky stanovené v systému a sledují příslušný vývoj v oblasti certifikace kybernetické bezpečnosti** [...]. Vnitrostátní orgány [...] certifikace **kybernetické bezpečnosti** by měly řešit stížnosti podané fyzickými nebo právnickými osobami v souvislosti s certifikáty vydanými **jimi nebo subjekty posuzování shody, uvádějí-li vysokou úroveň záruky** [...], 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 certifikace **kybernetické bezpečnosti** [...] 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 **ze zástupců** vnitrostátních orgánů [...] certifikace **kybernetické bezpečnosti nebo jiných příslušných vnitrostátních orgánů**. 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 agentuře ohledně návrhů systémů a** Komisi ohledně zachování a přezkumu stávajících evropských systémů certifikace kybernetické bezpečnosti.

60a) Skupina by měla usnadnit sdílení osvědčených postupů a odborných znalostí mezi vnitrostátními orgány certifikace kybernetické bezpečnosti odpovědnými za pověřování subjektů posuzování shody a vydávání certifikátů. Skupina by měla podpořit vypracování mechanismu vzájemného hodnocení v souvislosti s přípravou návrhu systému a jeho prováděním pro orgány vydávající evropské certifikáty kybernetické bezpečnosti pro vysokou úroveň záruky. Tato vzájemná hodnocení by měla zejména posuzovat, zda dotčené orgány disponují příslušnými odbornými znalostmi a své úkoly plní harmonizovaným způsobem. Výsledky vzájemných hodnocení by měly být zpřístupněny veřejnosti. Tyto orgány mohou přijmout vhodná opatření s cílem přizpůsobit své postupy a odborné znalosti.

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.

61a) V zájmu dalšího usnadnění obchodu a s vědomím, že dodavatelské řetězce IKT jsou globální, může Unie v souladu s článkem 218 SFEU uzavírat dohody o vzájemném uznávání týkající se certifikátů vydaných systémy zřízenými podle evropského rámce pro certifikaci kybernetické bezpečnosti. Komise při zohlednění poradenství ze strany agentury ENISA a Evropské skupiny pro certifikaci kybernetické bezpečnosti může doporučit zahájení příslušných jednání. Každý systém by měl poskytovat konkrétní podmínky pro vzájemné uznávání se třetími zeměmi.

62) [...]

63) [...]

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 [...] certifikace **kybernetické bezpečnosti** 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

1. 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 **Evropské unie** pro kybernetickou bezpečnost“ (dále jen „agentura“); a

b) stanoví rámec pro zavedení evropského systému certifikace kybernetické bezpečnosti za účelem zajištění odpovídající úrovně kybernetické bezpečnosti **procesů,** 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.

2. **Tímto nařízením 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 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 **poškodit, narušit nebo jinak** 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 **nebo na posouzení shody procesů,** produktů a služeb IKT spadajících do oblasti působnosti konkrétního systému;

9a) „vnitrostátním systémem certifikace kybernetické bezpečnosti“ komplexní soubor pravidel, technických požadavků, norem a postupů, které vyvinuly a přijaly vnitrostátní veřejné orgány a které se uplatňují na certifikaci nebo na posouzení shody procesů, produktů a služeb IKT spadajících do oblasti působnosti konkrétního systému;

10) „certifikátem kybernetické bezpečnosti“ dokument [...] osvědčující, že **byl hodnocen soulad** daného **procesu**, produktu či služby IKT [...], pokud jde o konkrétní **bezpečnostní** požadavky stanovené v evropském systému certifikace kybernetické bezpečnosti;

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

11a) „službou IKT“ jakákoli služba spočívající plně nebo převážně v přenosu, ukládání, získávání či zpracovávání informací prostřednictvím sítí a informačních systémů;

11b) „procesem IKT“ jakýkoli soubor činností prováděných za účelem navrhování, vývoje, poskytování a údržby produktů nebo služeb IKT;

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;

16a) „technickou specifikací“ dokument, který předepisuje technické požadavky, které má proces, postup nebo služba IKT splňovat;

16b) „úrovní záruky“ podklad pro důvěru, že proces, produkt či služba IKT splňuje bezpečnostní požadavky konkrétního evropského systému certifikace kybernetické bezpečnosti, přičemž je uvedeno, pro kterou úroveň bylo hodnocení provedeno; úroveň záruky neměří bezpečnost samotného procesu, produktu či služby IKT.

HLAVA II

ENISA – „ *[...] Agentura Evropské unie pro kybernetickou bezpečnost*“

KAPITOLA I

MANDÁT A CÍLE *[...]*

Článek 3

Mandát

1. Agentura plní úkoly, které jsou jí uloženy tímto nařízením za účelem zajištění vysoké úrovně kybernetické bezpečnosti [...] v **celé** Unii**, zejména podporování členských států, jakož i orgánů, institucí a jiných subjektů Unie, pokud jde o zlepšování kybernetické bezpečnosti**. **Agentura funguje jako referenční bod pro poradenství a odborné znalosti v oblasti kybernetické bezpečnosti pro orgány, instituce a jiné subjekty Unie.**

2. Agentura plní úkoly, které jsou jí svěřeny akty Unie stanovícími opatření pro sbližování právních a správních předpisů členských států týkajících se kybernetické bezpečnosti.

2a. Při plnění svých úkolů agentura koná nezávisle a v nejvyšší možné míře zohledňuje vnitrostátní odborné znalosti příslušných orgánů členských států, přičemž se vyvaruje zdvojování činností.

3. [...]

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 **Unie** týkajících se kybernetické bezpečnosti**, včetně odvětvových politik týkajících se kybernetické bezpečnosti.**

3. Agentura podporuje budování a připravenost kapacit v celé Unii tím, že pomáhá **orgánům, institucím a jiným subjektům Unie, jakož i** členským státům a zúčastněným stranám z veřejného a soukromého sektoru zvyšovat ochranu jejich sítí a informačních systémů, rozvíjet **a zlepšovat schopnosti kybernetické odolnosti a reakce a rozvíjet** schopnosti a odbornost v oblasti kybernetické bezpečnosti [...].

4. Agentura podporuje spolupráci a koordinaci na úrovni Unie mezi členskými státy, orgány, institucemi a jinými subjekty Unie a příslušnými zúčastněnými stranami [...] **ze soukromého i veřejného sektoru** v záležitostech týkajících se kybernetické bezpečnosti.

5. Agentura **přispívá ke zvýšení** schopností v oblasti kybernetické bezpečnosti na úrovni Unie s cílem **pomáhat** členským státům v oblasti předcházení kybernetickým hrozbám a reakce a ně, zejména v případě přeshraničních incidentů.

6. Agentura prosazuje využívání certifikace**, aby se zabránilo tříštění systémů certifikace v EU.** Aby **agentura** zvýšila transparentnost záruk kybernetické bezpečnosti produktů a služeb IKT, a posílila tím důvěru v digitální vnitřní trh, **přispívá zejména** 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.

KAPITOLA IA
ÚKOLY

Článek 5

*[...]**Tvorba 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 [...] bezpečnostních **incidentech** 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

[...] ***Budování kapacit***

1. Agentura je nápomocna:

a) členským státům v jejich úsilí zdokonalovat prevenci, odhalování a analýzu kybernetických bezpečnostních [...] **hrozeb** 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 [...] **hrozeb** a incidentů a schopnost na ně reagovat, **zejména** 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** 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 **pravidelně** organizuje [...] cvičení v oblasti kybernetické bezpečnosti na úrovni EU podle čl. 7 odst. 6 a na základě hodnocení 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 [...] **podporuje sdílení informací v rámci jednotlivých odvětví a napříč odvětvími**, zejména pak v odvětvích uvedených v příloze II směrnice (EU) 2016/1148, [...] poskytováním osvědčených postupů a vydáváním pokynů k dostupným nástrojům a postupům, jakož i k řešení regulačních otázek týkajících se sdílení informací.

Článek 7

[...] ***Operativní spolupráce na úrovni Unie***

1. Agentura podporuje operativní spolupráci mezi **členskými státy, orgány, institucemi a ostatními subjekty Unie**, jakož i 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 **v této funkci** usnadňuje sdílení informací a spolupráci mezi jejími členy.

4. Agentura [...] **podporuje** operativní spolupráci v rámci sítě CSIRT a členským státům **na jejich žádost** poskytuje podporu tím, že:

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

   b) [...]**usnadňuje** technické **řešení** [...] incidentů se závažným nebo významným dopadem**, mimo jiné zejména podporou dobrovolného sdílení technických řešení mezi členskými státy**;

   c) analyzuje zranitelnosti [...] a incidenty**;**

   ca) poskytuje podporu následným technickým šetřením incidentů, které mají závažný či významný dopad podle směrnice (EU) 2016/1148.

Při provádění těchto úkolů se agentura a tým CERT-EU zapojí do strukturované spolupráce, aby využily synergií [...] **a zamezily zdvojování činností**.

5. [...]

[...]

6. Agentura organizuje **pravidelná** [...] 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. **Tato cvičení na úrovni Unie mohou zahrnovat technické, operativní či strategické prvky** [...]. **Jednou za dva roky se pořádá velké cvičení, které zahrnuje všechny tyto prvky.** Agentura případně rovněž přispívá k odvětvovým cvičením v oblasti kybernetické bezpečnosti a pomáhá je organizovat spolu s příslušnými [...] **organizacemi, které se mohou** účastnit cvičení v oblasti kybernetické bezpečnosti i na úrovni Unie.

7. Agentura **v úzké spolupráci s členskými státy** 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 [...] nebo jednotná kontaktní místa podle směrnice o bezpečnosti sítí a informací (**obojí dobrovolně** [...]); Evropské centrum pro boj proti kyberkriminalitě (EC3) při Europolu a tým 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) shromažďuje zprávy sdílené **na dobrovolném základě** 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) [...] **na žádost členských států usnadňuje** technické řešení incidentu nebo krize, mimo jiné **zejména** [...] **podporou dobrovolného** sdílení technických řešení mezi členskými státy;

d) podporuje **orgány, instituce a jiné subjekty EU a na žádost členské státy v** komunikaci s veřejností ohledně incidentu nebo krize;

e) **podporuje členské státy na jejich žádost při** testování [...] plánů spolupráce pro reakci na tyto incidenty nebo krize.

Článek 8

[...] ***Trh, certifikace kybernetické bezpečnosti a normalizace***

Agentura:

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

1) vypracovává návrhy evropských systémů certifikace **kybernetické** bezpečnosti pro **procesy,** produkty a služby IKT **ve spolupráci s průmyslovými podniky a 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 [...] certifikace **kybernetické bezpečnosti** a odvětvím sestavuje a zveřejňuje pokyny a vypracovává osvědčené postupy týkající se požadavků na kybernetickou bezpečnost produktů a služeb IKT;

3a) doporučuje vhodné technické specifikace k použití při vypracovávání systémů certifikace kybernetické bezpečnosti podle čl. 47 odst. 1 písm. b) v případech, kdy normy nejsou k dispozici;

3b) přispívá k dostatečnému budování kapacit, pokud jde o hodnotící a certifikační procesy, shromažďováním a zveřejňováním pokynů a rovněž poskytováním podpory členským státům na jejich žádost;

b) usnadňuje stanovení a zavádění evropských a mezinárodních norem pro řízení rizik a pro bezpečnost **procesů,** produktů a služeb [...]**;**

ba) vydává ve spolupráci s členskými státy 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

[...] ***Znalosti* a *informace*** [...]

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 za účelem odhalení nových trendů a aby pomohla předcházet [...] kybernetickým bezpečnostním **incidentům**;

c) ve spolupráci s odborníky z orgánů členských států poskytuje poradenství, pokyny a osvědčené postupy týkající se bezpečnosti sítí a informačních systémů, zejména [...] infrastruktur podporujících odvětví uvedená v příloze II směrnice (EU) 2016/1148, **a takových, které používají poskytovatelé digitálních služeb uvedených v příloze III této směrnice**;

d) shromažďuje, uspořádává a prostřednictvím specializovaného portálu zpřístupňuje veřejnosti informace o kybernetické bezpečnosti poskytnuté orgány, institucemi a jinými subjekty Unie **a dobrovolně zpřístupněné členskými státy a veřejnými a soukromými zúčastněnými stranami**;

e) [...]

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

g) [...].

Článek 9a

Zvyšování povědomí a vzdělávání

Agentura:

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

b) 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;

c) pomáhá členským státům v jejich úsilí zvyšovat povědomí o kybernetické bezpečnosti a prosazovat vzdělávání v oblasti kybernetické bezpečnosti;

d) podporuje užší spolupráci a sdílení osvědčených postupů mezi členskými státy, pokud jde o vzdělávání v oblasti kybernetické bezpečnosti a povědomí o této problematice, usnadněním vytváření a udržování sítě vnitrostátních kontaktních míst v oblasti vzdělávání.

Článek 10

*[...] **Výzkum a inovace***

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

[...] ***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) usnadňuje sdílení osvědčených postupů [...] **v příslušných rámcích mezinárodní spolupráce**;

c) na žádost poskytuje odborné poznatky Komisi;

ca) ve spolupráci s Evropskou skupinou pro certifikaci kybernetické bezpečnosti zřízenou podle článku 53 poskytuje poradenství a podporu Komisi ohledně záležitostí týkajících se vzájemného uznávání certifikátů kybernetické bezpečnosti se třetími zeměmi.

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) výkonného ředitele, který plní povinnosti stanovené v článku 19; [...]

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

da) ze sítě národních styčných úředníků, která plní funkce stanovené v článku 20a.

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;

ca) dohlíží na provádění víceletých a ročních programů obsažených v jednotném programovém dokumentu;

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 rovněž její mimořádná zasedání.

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. […]

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 **včetně provádění ročního pracovního programu** 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;

la) pravidelnou výměnu informací s orgány a subjekty Unie o jejich činnosti v oblasti kybernetické bezpečnosti, aby byla zajištěna soudržnost při vývoji a uskutečňování politiky EU;

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. **Je-li to nezbytné, může** výkonný ředitel **za účelem účinného a efektivního provádění úkolů agentury a na základě náležité analýzy nákladů a přínosů** rozhodnout [...] **o zřízení jednoho nebo více místních úřadů v jednom nebo více členských státech.**. Před rozhodnutím o zřízení místního úřadu si výkonný ředitel **vyžádá stanovisko dotčeného členského státu nebo dotčených členských států, včetně členského státu, v němž se nachází sídlo agentury, a** získá předchozí souhlas Komise **a** správní rady [...]. **Nedojde-li během konzultačního procesu mezi výkonným ředitelem a dotčenými členskými státy ke shodě, předá se věc k projednání Radě.** Uvedeným rozhodnutím se určí rozsah činností, jež mají být v daném místním úřadu prováděny, způsobem, který zabrání zbytečným nákladům a zdvojování správních funkcí agentury. [...] **Počet zaměstnanců ve všech místních úřadech musí být omezen na minimum a celkově nepřekročí 40 % [...] zaměstnanců umístěných v členském státě, v němž se nachází sídlo agentury. Počet zaměstnanců v každém místním úřadu nepřekročí 10 % [...] počtu [...] zaměstnanců umístěných v členském státě, v němž se nachází sídlo agentury.**

ODDÍL 4
STÁLÁ SKUPINA ZÚČASTNĚNÝCH STRAN

Článek 20

Stálá skupina zastoupených zájmů

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, **provozovatelé základních služeb**, 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.

5a. Stálá skupina zúčastněných stran o své činnosti pravidelně informuje správní radu.

ODDÍL 4A
SÍŤ NÁRODNÍCH STYČNÝCH ÚŘEDNÍKŮ

Článek 20a

Síť národních styčných úředníků

1. Správní rada zřídí na návrh výkonného ředitele síť národních styčných úředníků složenou ze zástupců členských států.

2. Síť národních styčných úředníků se skládá ze zástupců všech členských států. Každý členský stát jmenuje jednoho zástupce. Zasedání sítě se mohou konat v různých odborných formátech.

3. Síť národních styčných úředníků zejména usnadňuje výměnu informací mezi agenturou ENISA a členskými státy. Zejména podporuje agenturu ENISA v šíření činností, zjištění a doporučení v celé EU, příslušným zúčastněným stranám.

4. Národní styční úředníci působí jako kontaktní místa na vnitrostátní úrovni s cílem usnadnit spolupráci mezi agenturou ENISA a národními odborníky v rámci provádění pracovního programu agentury.

5. Národní styční úředníci by sice měli úzce spolupracovat se zástupcem své země ve správní radě, avšak samotná síť nesmí vykonávat tutéž práci jako správní rada nebo jiné fórum EU.

6. Funkce a postupy sítě národních styčných úředníků se stanoví ve vnitřních organizačních předpisech agentury a zveřejní se.

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[14], 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.

[14] 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).

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.

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[15] a 2015/444[16]. Tyto předpisy musí zahrnovat ustanovení o výměně, zpracování a ukládání utajovaných informací.

---

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

[16] 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).

Článek 25

Přístup k dokumentům

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

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[17] 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.

[17] 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).

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[18] 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.

[18] 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 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.

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 **čtyři roky** [...]. 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 **čtyř** [...] 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 rozhodnutím správní rady [...].

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 [...].

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[19]. 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[20].

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.

---

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

[20] 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).

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 poskytuje [...] podmínky, aby bylo zajištěno řádné fungování agentury, včetně přístupnosti lokality, existence vhodných vzdělávacích zařízení pro děti zaměstnanců, patřičného přístupu na pracovní trh, 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

Rámec *pro certifikaci kybernetické bezpečnosti* [...]

1. **Rámec pro certifikaci kybernetické bezpečnosti se zřizuje s cílem zlepšit podmínky fungování vnitřního trhu zvýšením úrovně kybernetické bezpečnosti v Unii. Tento rámec stanoví rámec řízení umožňující harmonizovaný přístup k evropským systémům certifikace kybernetické bezpečnosti na úrovni EU s cílem vytvořit jednotný digitální trh pro procesy, produkty a služby IKT.**

2. **Rámec pro certifikaci kybernetické bezpečnosti definuje mechanismus pro zřizování** [...] evropských systémů certifikace kybernetické bezpečnosti **a** přezkoušení, zda **procesy**, produkty a služby IKT [...] **hodnocené** v souladu s takovými systémy jsou v souladu se stanovenými **bezpečnostními** požadavky s cílem chránit dostupnost, autentičnost, integritu nebo důvěrnost uchovávaných nebo předávaných nebo zpracovávaných dat nebo funkcí nebo služeb nabízených nebo dostupných v rámci těchto produktů, procesů **a** služeb [...] **v rámci jejich životního cyklu**.

Článek 44

Vypracování a přijetí evropského systému certifikace kybernetické bezpečnosti

1. Agentura ENISA na základě žádosti Komise **nebo evropské skupiny pro certifikaci kybernetické bezpečnosti („skupiny“) zřízené podle článku 53** vypracuje návrh evropského systému certifikace kybernetické bezpečnosti, který splňuje požadavky stanovené v článcích 45, 46 a 47 tohoto nařízení.[...]

1a. Přípravu navrhovaného evropského systému certifikace kybernetické bezpečnosti mohou skupině navrhovat členské státy nebo organizace sdružující zúčastněné zainteresované strany. Skupina posoudí takové návrhy podle kritérií definovaných skupinou prostřednictvím pokynů v souladu s čl. 53 odst. 3 písm. ca) a může požádat agenturu ENISA, aby připravila návrh evropského systému certifikace kybernetické bezpečnosti.

2. Při vypracovávání návrhu systému uvedeného v odstavci 1 tohoto článku agentura ENISA konzultuje všechny příslušné zúčastněné strany **prostřednictvím transparentních konzultačních postupů** a úzce spolupracuje se skupinou. Skupina poskytuje agentuře ENISA pomoc a odborné poradenství [...] v souvislosti s přípravou navrhovaného systému **a vydá stanovisko k navrhovanému systému před jeho předložením Komisi** [...]. **Agentura ENISA zajistí, aby navrhované systémy byly v souladu s použitelnou harmonizovanou normou použitou pro akreditace subjektu posuzování shody.**

3. Agentura ENISA **maximálně zohlední stanovisko skupiny před předložením** [...] navrhovaného [...]systému vypracovaného v souladu s odstavcem 2 tohoto článku 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 **procesů,** produktů a služeb IKT splňující požadavky článků 45, 46 a 47 tohoto nařízení.

5. […]

Článek 44a

Údržba evropského systému certifikace kybernetické bezpečnosti

1. Agentura udržuje příslušnou webovou stránku pro poskytování informací a publicity o evropských systémech certifikaci kybernetické bezpečnosti a certifikátech, jakož i o unijních prohlášeních o shodě vydaných podle článku 47a.

2. Agentura přezkoumá minimálně jednou za 5 let v úzké spolupráci se skupinou přijaté evropské systémy certifikace kybernetické bezpečnosti a zohlední přitom zkušenosti získané zúčastněnými stranami. Pokud to bude považováno za nutné, Komise nebo skupina mohou požádat agenturu, aby zahájila postup vypracování revidovaného navrhovaného systému podle čl. 44 odst. 2 a 3.

Článek 45

Bezpečnostní cíle evropských systémů certifikace kybernetické bezpečnosti

Evropský systém certifikace kybernetické bezpečnosti je navržen tak, aby [...] případně **dosáhl alespoň** tyto bezpečnostní cíle:

a) chránit ukládané, předávané nebo jinak zpracovávané údaje proti náhodnému nebo neoprávněnému ukládání, zpracování, přístupu nebo sdělování **během celého procesu, nebo životního cyklu produktu nebo služby**;

b) chránit údaje ukládané, předávané nebo jinak zpracovávané proti náhodnému nebo neoprávněnému zničení, [...] ztrátě nebo změně **nebo nedostupnosti během celého procesu, nebo životního cyklu produktu nebo služby**;

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 [...] **předmětem přístupu, použity nebo jinak zpracovány**;

e) [...] zajistit, aby bylo možné kontrolovat, ke kterým údajům, službám nebo funkcím kdy a kdo získal přístup [...], použil je **nebo jinak zpracoval**;

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

g) [...] **procesy,** produkty a služby IKT se poskytují s aktualizovaným softwarem **a hardwarem**, které [...] neobsahují **veřejně** známá slabá místa a obsahují mechanismy pro bezpečné aktualizace [...]**;**

ga) Procesy, produkty a služby se vypracovávají, vyrábějí a dodávají podle bezpečnostních požadavků uvedených v příslušném systému.

Článek 46

Úrovně záruky evropských systémů certifikace kybernetické bezpečnosti

1. Evropský systém certifikace kybernetické bezpečnosti může u **procesů,** produktů a služeb IKT [...], jež jsou v rámci daného systému vydány, určit jednu nebo více těchto úrovní záruky: základní, významnou nebo vysokou. **Úroveň záruky odpovídá úrovni rizik spojené se zamýšleným použitím procesu, produktu nebo služby IKT.**

2. Základní, významná a vysoká úroveň záruky [...] **odkazuje na certifikát nebo unijní prohlášení o shodě vydané v kontextu evropského systému certifikace kybernetické bezpečnosti, který stanovuje pro každou úroveň záruky příslušné bezpečnostní požadavky včetně bezpečnostní funkce a odpovídajícího stupně úsilí o vyhodnocení určitého procesu, produktu nebo služby IKT. Certifikát nebo unijní prohlášení o shodě jsou charakterizovány odkazem na technické specifikace, normy a procesy s nimi související, včetně technických kontrol, jejichž účelem je snížit riziko incidentů kybernetické bezpečnosti nebo jim předcházet takto:**

a) **Evropský certifikát kybernetické bezpečnosti nebo unijní prohlášení o shodě, které odkazují na** úroveň záruky „základní“, **poskytují záruku, že procesy, produkty a služby IKT splňují příslušné bezpečnostní požadavky včetně bezpečnostní funkce a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat známá základní rizika kybernetických incidentů a kybernetických útoků. Hodnotící činnosti musí obsahovat alespoň přezkum technické dokumentace, nebo, pokud není k dispozici, musí obsahovat náhradní aktivity s rovnocenným účinkem**[...];

b) **Evropský certifikát kybernetické bezpečnosti, který odkazuje na** úroveň záruky „významnou“, **poskytuje záruku, že procesy, produkty a služby IKT splňují příslušné bezpečnostní požadavky, včetně bezpečnostní funkce, a že byly vyhodnoceny na úrovni, které účelem je minimalizovat známá kybernetická rizika, kybernetické incidenty a kybernetické útoky, prováděné aktéry s omezenými dovednostmi a zdroji; Hodnotící aktivity zahrnou alespoň: přezkum nepoužitelnosti veřejně známých slabých míst a přezkoušení, zda procesy, produkty nebo služby IKT náležitě zavádějí nezbytnou bezpečnostní funkci; nebo, pokud nejsou k dispozici, zahrnou náhradní aktivity s rovnocenným účinkem** [...];

c) **Evropský certifikát kybernetické bezpečnosti, který odkazuje na** úroveň záruky „vysokou“, **poskytuje záruku, že procesy, produkty a služby IKT splňují příslušné bezpečnostní požadavky, včetně bezpečnostní funkce, a že byly vyhodnoceny na úrovni, které účelem je minimalizovat rizika sofistikovaných kybernetických útoků, prováděných aktéry s významnými dovednostmi a zdroji. Hodnotící činnosti musí obsahovat alespoň tyto prvky: přezkum nepoužitelnosti veřejně známých slabých míst, přezkoušení, zda procesy, produkty nebo služby IKT náležitě zavádějí bezpečnostní funkci na aktuální úrovni, a posouzení jejich odolnosti vůči zručným útočníkům prostřednictvím zkoušky penetrace; nebo, pokud nejsou k dispozici, zahrnou náhradní aktivity s rovnocenným účinkem** [...];

2a. Evropský systém certifikace kybernetické bezpečnosti může specifikovat několik hodnotících úrovní v závislosti na náročnosti a podrobnosti hodnotící metodiky. Každá z hodnotících úrovní odpovídá jedné z úrovní záruky a je definována odpovídající kombinací záručních prvků.

Článek 47

Prvky evropských systémů certifikace kybernetické bezpečnosti

1. Evropský systém certifikace kybernetické bezpečnosti zahrnuje **alespoň** tyto prvky:

a) předmět a rozsah **systému** certifikace včetně druhu nebo kategorií zahrnutých **procesů,** produktů, procesů a služeb IKT **a odůvodnění toho, jak systém certifikace splňuje potřeby předpokládaných cílových skupin;**

b) [...] odkaz na [...]mezinárodní**, evropské nebo vnitrostátní** normy, **jimiž se hodnocení řídilo. Nejsou-li normy k dispozici, uvede se odkaz na** [...] technické specifikace, **které splňují požadavky přílohy II nařízení 1025/2012, nebo, nejsou-li k dispozici, na technické specifikace nebo požadavky kybernetické bezpečnosti definované v příslušném systému;**

c) případně jednu nebo více úrovní záruky;

ca) případně specifické nebo dodatečné požadavky použitelné pro subjekty posuzování shody s cílem zajistit jejich technickou způsobilost k hodnocení požadavků na kybernetickou bezpečnost;

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

e) **případně** informace nezbytné pro certifikaci, které žadatel předkládá **nebo jinak zpřístupňuje** subjektům posuzování shody;

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

g) [...] pravidla pro monitorování plnění požadavků certifikátů **nebo unijního prohlášení o shodě**, včetně mechanismů prokázání pokračujícího plnění specifikovaných požadavků kybernetické bezpečnosti;

h) **případně** podmínky pro udělení **a obnovení certifikátu, jakož i** údržba, pokračování, rozšíření nebo omezení rozsahu certifikace;

i) pravidla upravující důsledky nesouladu certifikovaných **nebo sebehodnocených** produktů a služeb IKT s [...] požadavky **příslušného systému**;

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

k) **případně** pravidla upravující uchovávání záznamů subjekty posuzování shody;

l) identifikaci vnitrostátních **nebo mezinárodních** systémů certifikace kybernetické bezpečnosti zahrnující stejné druhy nebo kategorie **procesů,** produktů a služeb IKT, **bezpečnostní požadavky a hodnotící kritéria a metody**;

m) obsah vydaného certifikátu nebo unijního prohlášení o shodě;

ma) dobu uchování unijního prohlášení o shodě a technickou dokumentaci týkající se všech relevantních informací výrobce nebo poskytovatele produktů a služeb IKT;

mb[...]) maximální dobu platnosti certifikátů;

mc[...]) politiku zveřejňování udělených, pozměněných nebo pozastavených certifikátů;

md[...]) podmínky pro vzájemné uznávání systémů certifikace s třetími zeměmi;

me[...]) případně pravidla týkající se mechanismu vzájemného hodnocení pro subjekty vydávající evropské certifikáty kybernetické bezpečnosti pro vysokou úroveň záruky podle čl. 48 odst. 4a.

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 **nebo unijní prohlášení o shodě** 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 47a

Sebehodnocení shody

1. Evropský systém certifikace kybernetické bezpečnosti může umožnit provádění hodnocení shody v souladu s výhradní odpovědností výrobce nebo poskytovatele produktů a služeb IKT. Takové posouzení shody se použije pouze u produktů a služeb IKT s nízkým rizikem odpovídajícím základní úrovni záruky.

2. Výrobce nebo poskytovatel produktů nebo služeb IKT může vydat unijní prohlášení o shodě uvádějící, že bylo prokázáno plnění požadavků stanovených v příslušném systému. Vydáním tohoto prohlášení výrobce nebo poskytovatel produktů a služeb IKT přebírá odpovědnost za shodu produktu nebo služby IKT s požadavky stanovenými v systému.

3. Výrobce nebo poskytovatel produktů nebo služeb IKT uchovává unijní prohlášení o shodě a technickou dokumentaci týkající se všech relevantních informací souvisejících se shodou produktů nebo služeb IKT se systémem, který je k dispozici u vnitrostátního orgánu certifikace kybernetické bezpečnosti podle čl. 50 odst. 1, po dobu definovanou v odpovídajícím evropském systému certifikace kybernetické bezpečnosti. Jedno vyhotovení unijního prohlášení o shodě se předkládá vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a jedno vyhotovení agentuře ENISA.

4. Vydání unijního prohlášení o shodě je nepovinné, nestanoví-li unijní nebo vnitrostátní právo jinak.

5. Unijní prohlášení o shodě vydané podle tohoto článku je uznáváno ve všech členských státech.

Článek 48

Certifikace kybernetické bezpečnosti

1. U **procesů,** 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 unijní **nebo vnitrostátní** právo jinak.

3. Evropský certifikát kybernetické bezpečnosti podle tohoto článku **odkazující na základní nebo významnou úroveň záruky** 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 konkrétní evropský certifikát kybernetické bezpečnosti vyplývající z daného systému může být vydán pouze veřejným subjektem. Tímto veřejným subjektem je:

a) vnitrostátní orgán certifikace [...] **kybernetické bezpečnosti** uvedený v čl. 50 odst. 1;

b) **veřejný** subjekt, který je akreditován jako subjekt posuzování shody podle čl. 51 odst. 1[...];

c) [...].

4a. Pokud evropský systém certifikace kybernetické bezpečnosti podle článku 44 požaduje vysokou úroveň záruky, certifikát může vydat pouze vnitrostátní orgán certifikace kybernetické bezpečnosti uvedený v čl. 50 odst. 1 nebo za níže uvedených podmínek subjekt posuzování shody podle článku 51:

a) po předchozím schválení vnitrostátním orgánem certifikace kybernetické bezpečnosti pro každý jednotlivý certifikát vydaný orgánem posuzování shody; nebo

b) po předcházejícím obecném delegování tohoto úkolu subjektu posuzování shody ze strany vnitrostátního orgánu certifikace kybernetické bezpečnosti.

5. Fyzická nebo právnická osoba, která předloží své procesy, produkty nebo služby IKT do certifikačního mechanismu, [...] **umožní** subjektu posuzování shody podle článku 51 **nebo vnitrostátnímu orgánu certifikace kybernetické bezpečnosti podle článku 50, pokud tento orgán je subjektem vydávajícím příslušný certifikát,** [...] veškeré informace nezbytné pro provádění certifikačního procesu.

5a. Držitel certifikátu informuje subjekt vydávající certifikát o veškerých později zjištěných slabých místech nebo nepravidelnostech týkajících se bezpečnosti certifikace procesů, produktů nebo služeb IKT, které by mohly mít dopad na požadavky související s příslušnou certifikaci. Příslušný subjekt neprodleně tyto informace předloží příslušnému vnitrostátnímu orgánu certifikace kybernetické bezpečnosti.

6. Certifikáty se vydávají na [...] **období definované konkrétním systémem certifikace** a mohou být obnoveny, [...] budou-li nadále plněny příslušné relevantní 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 **procesy,** 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. Vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro **procesy,** 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 **procesy,** produkty a služby IKT zahrnuté do platného evropského systému certifikace kybernetické bezpečnosti.

3. Stávající certifikáty vydané v rámci vnitrostátních systémů certifikace kybernetické bezpečnosti, **na něž se vztahuje evropský systém certifikace kybernetické bezpečnosti,** zůstávají platné až do data skončení své platnosti.

Článek 50

Vnitrostátní orgány certifikace **kybernetické bezpečnosti** *[...]*

1. Každý členský stát [...] **určí jeden nebo více** vnitrostátních orgánů certifikace kybernetické bezpečnosti [...] **na svém území nebo po vzájemné dohodě s jiným členským státem určí jeden nebo více orgánů usazených v tomto jiném členském státě, který bude odpovídat za úkoly dohledu v určeném členském státě.**

2. Každý členský stát informuje Komisi o identitě **orgánů [...], které byly určeny, a o úkolech, které jim byly stanoveny**.

3. **Aniž jsou dotčena ustanovení čl. 48 odst. 4 písm. a) a čl. 48 odst. 4a,** [...] musí být každý vnitrostátní orgán certifikace **kybernetické bezpečnosti** [...] ve své organizaci, finančních rozhodnutích, právní struktuře a rozhodovacím procesu nezávislý na subjektech, nad nimiž vykonává dozor.

3a. Členské státy zajistí, aby aktivity příslušného vnitrostátního orgánu certifikace kybernetické bezpečnosti související s vydáváním certifikátů podle čl. 48 odst. 4 písm. a) a odst. 4a byly striktně odděleny, pokud jde o jejich úlohy a odpovědnosti, od dohledových aktivit podle tohoto článku a aby obě aktivity fungovaly na sobě nezávisle.

4. Členské státy zajistí, aby vnitrostátní orgány certifikace **kybernetické bezpečnosti** [...] 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 certifikace **kybernetické bezpečnosti** [...]:

a) […]

aa) monitorují a vymáhají povinnosti výrobce nebo poskytovatele produktů nebo služeb IKT, kteří jsou usazeni na jejich příslušných územích a uvedeni v čl. 47a odst. 2 a 3 a v odpovídajícím evropském systému certifikace kybernetické bezpečnosti;

b) [...] **aniž je dotčen čl. 51 odst. 1b, napomáhají vnitrostátním subjektům akreditace při monitorování a dohledu** aktivit subjektů posuzování shody pro účely tohoto nařízení[...];

ba) monitorují a dohlížejí nad aktivitami subjektů uvedených v čl. 48 odst. 4;

bb) autorizují subjekty posuzování shody podle čl. 51 odst. 1b a omezují, pozastavují nebo odebírají stávající autorizaci v případech neplnění požadavků tohoto nařízení;

c) řeší stížnosti podané fyzickými nebo právnickými osobami v souvislosti s certifikáty vydanými [...] **vnitrostátními orgány certifikace kybernetické bezpečnosti nebo v souladu s čl. 48 odst. 4a subjekty posuzování shody**, v přiměřeném rozsahu šetří předmět stížnosti a v přiměřené lhůtě informují stěžovatele o průběhu a výsledku šetření;

d) spolupracují s dalšími vnitrostátními orgány [...] certifikace **kybernetické bezpečnosti** nebo jinými veřejnými orgány, mimo jiné prostřednictvím sdílení informací o možných případech nesouladu **procesů,** 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 certifikace kybernetické bezpečnosti [...] má alespoň tyto pravomoci:

a) požadovat po subjektech posuzování shody**,** [...] držitelích evropského certifikátu kybernetické bezpečnosti **a vydavatelích unijního prohlášení o shodě,** aby poskytovaly veškeré informace, které požaduje pro vykonávání svého úkolu;

b) za účelem ověření souladu s ustanoveními podle hlavy III provádět šetření v podobě auditů u subjektů posuzování shody, [...] držitelů evropských certifikátů kybernetické bezpečnosti **a vydavatelů unijního prohlášení o shodě;**

c) v souladu s vnitrostátním právem přijímat vhodná opatření za účelem zajištění toho, aby subjekty posuzování shody, [...] držitelé certifikátů a **vydavatelů unijního prohlášení o shodě** 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) zrušit v souladu s vnitrostátním právem certifikáty **vydané příslušným vnitrostátním orgánem certifikace kybernetické bezpečnosti nebo v souladu s čl. 48 odst. 4a subjekty posuzování shody,** které nejsou v souladu s tímto nařízením nebo s evropským systém 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 [...] certifikace **kybernetické bezpečnosti** [...] 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 **procesů,** 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.

1a. Je-li evropský certifikát kybernetické bezpečnosti vydán vnitrostátním orgánem certifikace kybernetické bezpečnosti podle čl. 48 odst. 4 písm. a) a odst. 4a, certifikační subjekt příslušného vnitrostátního orgánu certifikace kybernetické bezpečnosti je akreditován jako subjekt posuzování shody podle odst. 1 tohoto článku.

1b. V případě potřeby jsou subjekty posuzování shody pověřeny příslušným vnitrostátním orgánem certifikace kybernetické bezpečnosti, aby prováděl své úkoly, splňují-li konkrétní nebo dodatečné požadavky stanovené v příslušném evropském systému certifikace podle čl. 47 odst. 1 písm. ca).

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 **přijmou veškerá odpovídající opatření v přiměřené lhůtě s cílem omezit, pozastavit nebo** zrušit akreditaci subjektu posuzování shody podle odstavce 1 tohoto článku, 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 [...] certifikace **kybernetické bezpečnosti** oznámí Komisi akreditované subjekty, **případně pověřené podle čl. 51 odst. 1b** 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 certifikace **kybernetické bezpečnosti** [...] 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 certifikace **kybernetické bezpečnosti** [...] 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 se skládá ze **zástupců** vnitrostátních orgánů [...] certifikace kybernetické bezpečnosti **nebo zástupců jiných relevantních vnitrostátních orgánů**. [...] **Jakýkoli člen skupiny nemůže zastupovat více než jeden další členský stát**.

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;

ba) vydat stanovisko k navrhovanému systému podle článku 44 tohoto nařízení;

c) [...] **požadovat** po agentuře, aby vypracovala návrh evropského systému certifikace kybernetické bezpečnosti v souladu s článkem 44 tohoto nařízení;

ca) vypracovat a přijmout pokyny ke kritériím pro posuzování návrhů na vypracování navrhovaného systému předkládaného [...] skupině podle čl. 11 odst. 1a;

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 [...] certifikace **kybernetické bezpečnosti** podle této hlavy **budováním kapacit**, stanovením metod pro účinnou výměnu informací o veškerých otázkách týkajících se certifikace kybernetické bezpečnosti;

fa) poskytovat podporu provádění mechanismu vzájemného hodnocení v souladu s pravidly stanovenými v evropském systému certifikace kybernetické bezpečnosti podle čl. 47 odst. 1 písm. md) tohoto nařízení.

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

Článek 53a

Právo podávat stížnosti u vnitrostátního orgánu certifikace **kybernetické bezpečnosti** ***[...]***

1. Fyzické nebo právnické osoby mají právo podávat stížnosti u vnitrostátního orgánu certifikace kybernetické bezpečnosti v souvislosti s certifikátem vydaným stejným orgánem nebo subjekty posuzování shody v souladu s čl. 48 odst. 4a.

2. Vnitrostátní orgán certifikace kybernetické bezpečnosti, kterému byla stížnost podána, informuje stěžovatele o pokroku v řešení stížnosti a o jeho výsledku, jakož i o možnosti opravných prostředků podle článku 53b.

Článek 53b

Právo na účinné opravné prostředky

1. Fyzické nebo právnické osoby mají právo na účinné opravné prostředky vůči právně závaznému rozhodnutí vnitrostátního orgánu certifikace kybernetické bezpečnosti, které se jich týká.

2. Fyzické nebo právnické osoby mají právo na účinné opravné prostředky v případech, kdy vnitrostátní orgán certifikace kybernetické bezpečnosti nevyřídí stížnost.

3. Jednání vůči vnitrostátnímu orgánu certifikace kybernetické bezpečnosti se vede u příslušných soudů členského státu, ve kterém, je příslušný orgán usazen.

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 čl. 5 **odst. 4 písm. b)** 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.

1a. Toto nařízení se použije od […] s výjimkou článků 50, 51, 52, 53a, 53b a 54, které se použijí od [24 měsíce ode dne zveřejnění nařízení 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	*Za Radu*
předseda	*předseda/předsedkyně*

PŘÍLOHA

POŽADAVKY, KTERÉ MUSÍ SPLŇOVAT SUBJEKTY POSUZOVÁNÍ SHODY

Subjekty posuzování shody, které chtějí získat akreditaci, musí splňovat tyto požadavky:

1. Subjekt posuzování shody je zřízen podle vnitrostátních právních předpisů a má právní subjektivitu.

2. Subjekt posuzování shody musí být třetí stranou nezávislou na organizaci nebo produktu či službě IKT, které posuzuje.

3. Za subjekt posuzování shody lze považovat subjekt patřící k hospodářskému sdružení nebo profesnímu svazu zastupujícímu podniky, jež se podílejí na navrhování, výrobě, dodávání, montáži, používání nebo údržbě produktů či služeb IKT, které tento subjekt posuzuje, pokud je prokázána jeho nezávislost a neexistence jakéhokoli střetu zájmů.

4. Subjekt posuzování shody, jeho nejvyšší vedení a pracovníci odpovědní za plnění úkolů posuzování shody nesmějí být osobami, které navrhují, vyrábějí, dodávají, instalují, nakupují, vlastní, používají nebo udržují produkt či službu IKT, jež je předmětem posouzení, ani zplnomocněnými zástupci jakékoli z těchto stran. To nevylučuje používání posuzovaných produktů, které jsou nezbytné pro činnost subjektu posuzování shody, ani používání takových produktů k osobním účelům.

5. Subjekt posuzování shody, jeho nejvyšší vedení a pracovníci odpovědní za plnění úkolů posuzování shody se nesmí přímo podílet na navrhování, výrobě nebo konstrukci, uvádění na trh, instalaci, používání ani údržbě těchto produktů nebo služeb IKT, ani nesmí zastupovat strany, které se těmito činnostmi zabývají. Nesmí vykonávat žádnou činnost, která by mohla ohrozit jejich nezávislý úsudek nebo důvěryhodnost ve vztahu k činnostem posuzování shody, k jejichž vykonávání jsou oznámeni. To platí zejména pro poradenské služby.

6. Subjekty posuzování shody musí zajistit, aby činnosti jejich dceřiných společností nebo subdodavatelů neohrožovaly důvěrnost, objektivitu nebo nestrannost jejich činností posuzování shody.

7. Subjekty posuzování shody a jejich pracovníci vykonávají činnosti posuzování shody na nejvyšší úrovni profesionální důvěryhodnosti a požadované odborné způsobilosti v konkrétní oblasti a nesmějí být vystaveni žádným tlakům a podnětům, například finančním, které by mohly ovlivnit jejich úsudek nebo výsledky jejich činností posuzování shody, zejména ze strany osob nebo skupin osob, které mají na výsledcích těchto činností zájem.

8. Subjekt posuzování shody musí být schopen provádět všechny úkoly v rámci posuzování shody, které tomuto subjektu ukládá toto nařízení, ať již tyto úkoly provádí subjekt posuzování shody sám, nebo jsou prováděny jeho jménem a na jeho odpovědnost.

9. Subjekt posuzování shody musí mít k dispozici vždy, pro každý postup posuzování shody a pro každý druh, kategorii nebo podkategorii produktů či služeb IKT, pro něž je oznámen, potřebné:

a) pracovníky s odbornými znalostmi a dostatečnými zkušenostmi potřebnými k plnění úkolů posuzování shody;

b) popisy postupů, podle nichž je posuzování shody prováděno, aby byla zajištěna transparentnost těchto postupů a možnost jejich zopakování. Musí mít zavedenu náležitou politiku a postupy pro rozlišení mezi úkoly, jež vykonává jako oznámený subjekt, a dalšími činnostmi;

c) postupy pro výkon činností, jež řádně zohledňují velikost a strukturu podniku, odvětví, v němž působí, míru složitosti dané technologie produktu či služby IKT a hromadnou či sériovou povahu výrobního procesu.

10. Subjekt posuzování shody musí mít prostředky nezbytné k řádnému plnění technických a administrativních úkolů spojených s činnostmi posuzování shody a musí mít přístup k veškerému potřebnému vybavení a zařízení.

11. Pracovníci odpovědní za provádění činností spojených s posuzováním shody musí:

a) mít přiměřené technické a odborné vzdělání v oblasti všech činností spojených s posuzováním shody;

b) mít uspokojivou znalost požadavků souvisejících s posuzováním, které provádějí, a odpovídající pravomoc toto posuzování provádět;

c) mít odpovídající znalosti a pochopení příslušných požadavků a zkušebních norem;

d) být schopni vypracovávat certifikáty, záznamy, protokoly a zprávy prokazující, že posouzení byla provedena.

12. Musí být zaručena nestrannost subjektů posuzování shody, jejich nejvyššího vedení a pracovníků, kteří provádějí posuzování.

13. Odměňování nejvyššího vedení a pracovníků subjektu posuzování shody, kteří provádějí posuzování, nesmí záviset na počtu provedených posouzení ani na výsledcích těchto posouzení.

14. Subjekty posuzování shody uzavřou pojištění odpovědnosti za škodu, pokud tuto odpovědnost nepřevzal stát v souladu s vnitrostátními právními předpisy nebo pokud není za posuzování shody přímo odpovědný sám členský stát.

15. Pracovníci subjektu posuzování shody jsou povinni zachovávat služební tajemství, s výjimkou styku s příslušnými orgány členských států, v nichž vykonávají svou činnost, pokud jde o veškeré informace, které obdrželi při plnění svých úkolů podle tohoto nařízení nebo podle jakéhokoli ustanovení vnitrostátních právních předpisů, kterým se uvedená směrnice provádí.

16. Subjekty posuzování shody plní požadavky **příslušné relevantní** normy, **která je harmonizována podle nařízení (ES) 765/2008 pro akreditaci subjektů posuzování shody provádějící certifikaci procesů, produktů nebo služeb** [...].

17. Subjekty posuzování shody zajistí, aby zkušební laboratoře používané pro účely posuzování shody plnily požadavky **příslušné** normy, **která je harmonizována podle nařízení (ES) 765/2008 pro akreditaci laboratoří provádějících zkoušení** [...].