NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2019/881

ze dne 17. dubna 2019

o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („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 ([1]),

s ohledem na stanovisko Výboru regionů ([2]),

v souladu s řádným legislativním postupem ([3]),

vzhledem k těmto důvodům:

(1) Sítě a informační systémy a sítě a služby elektronických komunikací mají zásadní význam pro společnost a staly se páteří hospodářského růstu. Informační a komunikační technologie (IKT) jsou základem komplexních systémů, které podporují běžné společenské činnosti, udržují v chodu naši ekonomiku v klíčových odvětvích, jako je například zdravotnictví, energetika, finančnictví a doprava, a zejména podporují fungování vnitřního trhu.

(2) Využívání sítí a informačních systémů občany, organizacemi a podniky 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 Unii během příštího desetiletí připojeny extrémně vysoké počty 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 fyzické osoby, organizace ani podniky nemají dostatečné informace o prvcích kybernetické bezpečnosti produktů, služeb a procesů IKT, které používají, což narušuje důvěru v digitální řešení. Sítě a informační systémy mohou napomáhat ve všech aspektech našich životů a jsou hnacím motorem hospodářského růstu Unie. Jsou úhelným kamenem pro dosažení jednotného digitálního trhu.

(3) Nárůst digitalizace a propojenosti zvyšuje kybernetická bezpečnostní rizika, 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 je třeba přijmout veškerá opatření potřebná ke zlepšení kybernetické bezpečnosti v Unii, aby byly sítě a informační systémy, komunikační sítě, digitální produkty, služby a zařízení používané občany, organizacemi a podniky – od malých a středních podniků ve smyslu doporučení Komise 2003/361/ES ([4]) až po provozovatele kritických infrastruktur – lépe chráněny před kybernetickými hrozbami.

([1]) Úř. věst. C 227, 28.6.2018, s. 86.
([2]) Úř. věst. C 176, 23.5.2018, s. 29.
([3]) Postoj Evropského parlamentu ze dne 12. března 2019 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 9. dubna 2019.
([4]) Doporučení Komise ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

(4) Agentura Evropské unie pro bezpečnost sítí a informací (ENISA), zřízená nařízením Evropského parlamentu a Rady (EU) č. 526/2013 ([5]), přispívá zpřístupňováním příslušných informací veřejnosti k rozvoji odvětví kybernetické bezpečnosti v Unii, zejména malých a středních podniků a začínajících podniků. Agentura ENISA by měla usilovat o těsnější spolupráci s univerzitami a výzkumnými subjekty s cílem přispět ke snížení závislosti na produktech v oblasti kybernetické bezpečnosti a služeb z oblasti mimo Unie a posílit dodavatelské řetězce v rámci Unie.

(5) 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, kompetence a opatření politik orgánů zabývajících se kybernetickou bezpečností a donucovacích orgánů jsou převážně vnitrostátní. Rozsáhlé incidenty by mohly narušit poskytování základních služeb v celé Unii. To vyžaduje účinnou a koordinovanou reakci a řešení krizí na úrovni Unie, které budou vycházet ze speciálních politik a širších nástrojů pro evropskou solidaritu a vzájemnou pomoc. Proto je pro tvůrce politik, průmyslové odvětví a uživatele rovněž 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 úrovni celosvětové.

(6) 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. Tyto cíle obnášejí nutnost dále zvýšit schopnosti a připravenost členských států a podniků a rovněž zlepšit spolupráci, sdílení informací a koordinaci mezi členskými státy a orgány, institucemi a subjekty Unie. 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; zároveň je však nutné vzít v úvahu to, že je důležité zachovat schopnost členských států reagovat na kybernetické hrozby nejrůznějšího rozsahu a tyto schopnosti rozšiřovat.

(7) Je rovněž třeba další úsilí ke zvýšení informovanosti občanů, organizací a podniků o otázkách týkajících se kybernetické bezpečnosti. Vzhledem k tomu, že incidenty narušují důvěru v poskytovatele digitálních služeb a samotný jednotný digitální trh, zejména mezi spotřebiteli, je nutné navíc tuto důvěru dále posílit tím, že budou transparentním způsobem poskytovány informace o úrovni bezpečnosti produktů, služeb a procesů IKT, přičemž je třeba zdůraznit, že ani vysoká úroveň certifikace kybernetické bezpečnosti nemůže zaručit, že produkt, služba nebo proces IKT jsou zcela bezpečné. Posílení důvěry lze usnadnit certifikací v rámci Unie, která bude poskytovat společné požadavky na kybernetickou bezpečnost a kritéria jejího hodnocení napříč vnitrostátními trhy a odvětvími.

(8) Kybernetická bezpečnost není jen otázkou technologie, důležité je rovněž i lidské chování. Proto by měla být výrazně prosazována „kybernetická hygiena“ ve smyslu jednoduchých rutinních opatření, která – jsou-li zavedena a pravidelně prováděna občany, organizacemi a podniky – minimalizují jejich vystavení rizikům kybernetických hrozeb.

(9) Pro účely posilování struktur kybernetické bezpečnosti v Unii je důležité zachovávat a rozvíjet schopnosti členských států v zájmu komplexní reakce na kybernetické hrozby včetně přeshraničních incidentů.

(10) Podniky i jednotliví spotřebitelé by měli mít přesné informace ohledně toho, na jakou úroveň záruky bezpečnosti jsou jejich produkty, služby a procesy a IKT certifikovány. Zároveň však žádný produkt ani služba IKT nejsou zcela kyberneticky bezpečné a je třeba podporovat a upřednostňovat základní zásady kybernetické hygieny. Vzhledem k rostoucí dostupnosti zařízení internetu věcí je k dispozici řada dobrovolných opatření, která může soukromý sektor přijmout, aby posílil důvěru v bezpečnost produktů, služeb a procesů IKT.

(11) Moderní produkty a systémy IKT často zahrnují jednu nebo více technologií a prvků třetí strany, jako jsou softwarové moduly, knihovny nebo rozhraní pro programování aplikací (API), a spoléhají na ně. Toto spoléhání, k němuž se často odkazuje jako k „závislosti“, by mohlo představovat další kybernetická bezpečnostní rizika, poněvadž zranitelnosti zjištěné v prvcích třetí strany by mohly mít též vliv na bezpečnost produktů, služeb a procesů IKT. V mnoha případech umožňuje nalezení a zdokumentování takových závislostí koncovým uživatelům produktů, služeb a procesů IKT zlepšit jejich činnosti řízení kybernetických bezpečnostních rizik zlepšením například řízení kybernetické bezpečnostní zranitelnosti uživatele a postupů nápravy.

([5]) 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).

(12) Organizace, výrobci nebo poskytovatelé zapojení do navrhování a vývoje produktů, služeb či procesů IKT by měli být podporováni v provádění opatření, a to již v nejranějších fázích návrhu a vývoje, aby chránili bezpečnost těchto produktů, služeb a procesů v nejvyšší možné míře, a to tak, aby byl předpokládán výskyt kybernetických útoků a aby byl předpokládán a minimalizován jejich dopad („bezpečnost již od fáze návrhu“). Bezpečnost by měla být zajištěna v průběhu celého životního cyklu produktu, služby či procesu IKT prostřednictvím neustálého rozvíjení postupů navrhování a vývoje, s cílem omezit riziko zneužití.

(13) Podniky, organizace a veřejný sektor by měly konfigurovat produkty, služby nebo procesy IKT jimi navržené způsobem, který zajistí vyšší úroveň bezpečnosti, což by mělo prvnímu uživateli umožnit obdržet standardní konfiguraci s co nejbezpečnějším nastavením (dále jen „standardní bezpečnost“), čímž se sníží zátěž pro uživatele spojená s nutností odpovídající konfigurace produktu, služby či procesu IKT. Standardní bezpečnost by neměla vyžadovat provedení rozsáhlé konfigurace ani specifické technické znalosti či jiné než intuitivní chování uživatele, a je-li použita, měla by fungovat snadno a spolehlivě. Pokud v individuálním případě vedou analýzy rizika a využitelnosti k závěru, že takové nastavení není proveditelné, měli by být uživatelé nabádáni ke zvolení nejbezpečnějšího nastavení.

(14) Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ([6]) zřídilo agenturu ENISA za účelem přispět k cílům zajištění vysoké a účinné úrovně bezpečnosti sítí a informací v Unii a vytvořit kulturu bezpečnosti sítí a informací v zájmu občanů, spotřebitelů, podniků a veřejné správy. Nařízení Evropského parlamentu a Rady (ES) č. 1007/2008 ([7]) prodloužilo mandát agentury ENISA do března 2012. Nařízení Evropského parlamentu a Rady (EU) č. 580/2011 ([8]) dále prodloužilo mandát agentury ENISA do 13. září 2013. Nařízení (EU) č. 526/2013 prodloužilo mandát agentury ENISA do 19. června 2020.

(15) Unie již podnikla důležité kroky k zajištění kybernetické bezpečnosti a zvýšení důvěry v digitální technologie. V roce 2013 byla přijata strategie kybernetické bezpečnosti Evropské unie jako základ pro politickou reakci Unie na kybernetické hrozby a rizika. Ve snaze lépe chránit občany v on-line prostředí Unie v roce 2016 přijala první legislativní akt v oblasti kybernetické bezpečnosti, směrnici Evropského parlamentu a Rady (EU) 2016/1148 ([9]). Směrnice (EU) 2016/1148 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, dodávky a rozvody pitné vody, bankovnictví, infrastruktura finančních trhů, zdravotnictví a digitální infrastruktura včetně poskytovatelů klíčových digitálních služeb (internetových vyhledávačů, služeb cloud computingu a on-line tržišť).

Klíčová role při podpoře provádění uvedené směrnice byla přisouzena agentuře ENISA. Kromě toho je účinný boj proti kyberkriminalitě důležitou prioritou Evropského programu pro bezpečnost, a přispívá tak k celkovému cíli dosažení vysoké úrovně kybernetické bezpečnosti. Jiné právní akty, jako je nařízení Evropského parlamentu a Rady (EU) 2016/679 ([10]) a směrnice Evropského parlamentu a Rady 2002/58/ES ([11]) a směrnice (EU) 2018/1972 ([12]),rovněž přispívají k vysoké míře kybernetické bezpečnosti na jednotném digitálním trhu.

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

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

([11]) Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) (Úř. věst. L 201, 31.7.2002, s. 37).

([12]) Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (Úř. věst. L 321, 17.12.2018, s. 36).

(16) Od přijetí strategie kybernetické bezpečnosti Evropské unie v roce 2013 a od poslední revize mandátu agentury ENISA se celkový politický kontext významně změnil s ohledem na více nejisté a méně bezpečné globální prostředí. Za těchto okolností a v souvislosti s pozitivním vývojem role agentury ENISA jakožto referenčního bodu pro poradenství a odborné znalosti a zprostředkovatele spolupráce a budování kapacit a v rámci nové politiky Unie v oblasti kybernetické bezpečnosti je nezbytné přezkoumat mandát agentury ENISA, vymezit její roli v měnícím se ekosystému kybernetické bezpečnosti a zajistit, aby účinně přispívala k reakci Unie na kybernetické bezpečnostní výzvy plynoucí z radikálně transformovaných kybernetických hrozeb, k čemuž, jak bylo uznáno při hodnocení agentury ENISA, není stávající mandát dostatečný.

(17) Agentura ENISA zřízená tímto nařízením by měla být nástupcem agentury ENISA zřízené nařízením (EU) č. 526/2013. Agentura ENISA by měla plnit úkoly, které jí jsou svěřeny tímto nařízením a jinými právními akty Unie v oblasti kybernetické bezpečnosti, mimo jiné tím, že bude poskytovat poradenství a odborné znalosti 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 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, institucemi a jinými subjekty Unie.

(18) V rámci rozhodnutí (2004/97/ES, Euratom), přijatém vzájemnou dohodou zástupců členských států, zasedajících na úrovni hlav států a předsedů vlád ([13]), zástupci členských států 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 ENISA. V zájmu zajištění řádného a účinného plnění úkolů agentury ENISA, přijímání a udržení si zaměstnanců a v zájmu zvýšení účinnosti v oblasti vytváření sítí je naprosto nezbytné, aby bylo sídlo agentury ENISA 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 ENISA a daným hostitelským členským státem uzavřené poté, co bude schválena správní rada agentury ENISA.

(19) Vzhledem k nárůstu kybernetických bezpečnostních rizik a výzev, kterým Unie čelí, by měly být navýšeny finanční a lidské zdroje přidělené agentuře ENISA, aby odrážely širší úlohu a množství úkolů agentury a její zásadní postavení v ekosystému organizací bránících digitální ekosystém Unie a umožnily jí, aby účinně plnila úkoly, které jí byly svěřeny tímto nařízením.

(20) Agentura ENISA by měla rozvíjet a udržovat vysokou úroveň odborných znalostí a působit jako referenční bod a díky své nezávislosti, kvalitě poskytovaného poradenství a informací, transparentnosti svých postupů a metod práce a pečlivosti, s níž plní svěřené úkoly, vytvářet důvěru v jednotný trh. Agentura ENISA by měla aktivně 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, přičemž by měla předcházet zdvojování práce a podporovat součinnost. Kromě toho by agentura ENISA 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 ENISA plnit své cíle, a současně umožňoval flexibilitu jejích činností.

(21) Aby mohla agentura ENISA přiměřeně podporovat operativní spolupráci mezi členskými státy, měla by dále rozšířit své technické a lidské schopnosti a odborné dovednosti. Agentura ENISA by měla zvýšit své know-how a kapacity. Agentura ENISA a členské státy by mohly dobrovolně rozvíjet programy pro vysílání národních odborníků do agentury ENISA, vytvářet skupiny expertů a provádět výměnu pracovníků.

(22) Agentura ENISA 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 jejích aspektů specifických pro jednotlivá odvětví s cílem zvýšit význam politik Unie a právních předpisů s rozměrem kybernetické bezpečnosti a umožnit soudržnost při provádění těchto politik a předpisů na vnitrostátní úrovni. Pro politiky Unie v konkrétních odvětvích a pro iniciativy Unie v oblasti právních předpisů by agentura ENISA měla působit jako referenční bod poskytující poradenství a odborné znalosti v případech, kdy se tyto politiky a iniciativy týkají otázek souvisejících s kybernetickou bezpečností. Agentura ENISA by měla Evropský parlament pravidelně informovat o své činnosti.

([13]) Rozhodnutí 2004/97/ES, Euratom přijaté vzájemnou dohodou zástupců členských států, zasedajících na úrovni hlav států a předsedů vlád, ze dne 13. prosince 2003 o umístění sídel některých subjektů Evropské unie (Úř. věst. L 29, 3.2.2004, s. 15).

(23) Veřejné jádro otevřeného internetu, tedy hlavní protokoly a infrastruktura, jež jsou globálním veřejným statkem, zajišťuje základní funkci internetu jako celku a je základem pro jeho běžný provoz. Agentura ENISA by měla podpořit bezpečnost veřejného jádra otevřeného internetu a stabilitu jeho fungování, včetně klíčových protokolů (zejména DNS, BGP, a IPv6), provozu systému doménových jmen (včetně provozu všech domén na vrcholné úrovni) a provozu root zone.

(24) Základním úkolem agentury ENISA je prosazovat jednotné provádění příslušného právního rámce, zejména účinné provádění směrnice (EU) 2016/1148 a dalších příslušných právních nástrojů zahrnujících aspekty kybernetické bezpečnosti, což je zásadní pro zvýšení kybernetické odolnosti. S ohledem na rychle se vyvíjející oblast kybernetických hrozeb je zřejmé, že se členské státy musí opírat o komplexnější přístup k budování kybernetické odolnosti, který přesahuje jednotlivé politiky.

(25) Agentura ENISA 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 ENISA by zejména měla podporovat rozvoj a posilování vnitrostátních a unijních bezpečnostních týmů CSIRT podle směrnice (EU) 2016/1148 s cílem dosáhnout v Unii vysoké společné úrovně jejich vyspělosti. Činnosti prováděné agenturou ENISA ve vztahu k operativním kapacitám členských států by měly aktivně podporovat opatření přijatá členskými státy za účelem plnění jejich povinností vyplývajících ze směrnice (EU) 2016/1148, a tedy by je neměly nahrazovat.

(26) Agentura ENISA by rovněž měla pomáhat s rozvíjením a aktualizováním strategií pro bezpečnost sítí a informačních systémů na úrovni Unie a členských států, pokud o to požádají, a to zejména strategií pro kybernetickou bezpečnost, a měla by podporovat šíření těchto strategií a sledovat pokrok při jejich provádění. Agentura ENISA by měla také přispívat k pokrytí potřeb ohledně školení a vzdělávacích materiálů, zejména potřeb veřejných subjektů, a případně ve velké míře „školit školitele“ na základě rámce digitálních kompetencí pro občany, a tím pomáhat členským státům a orgánům, institucím a jiným subjektům Unie při rozvoji jejich vlastních školicích kapacit.

(27) Agentura ENISA by měla podporovat členské státy, pokud jde o zvyšování informovanosti a vzdělávání v oblasti kybernetické bezpečnosti usnadňováním těsnější koordinace a výměny osvědčených postupů mezi členskými státy. Tato podpora by mohla spočívat v rozvíjení sítě vnitrostátních kontaktních míst v oblasti vzdělávání a platformy odborné přípravy pro kybernetickou bezpečnost. Síť vnitrostátních kontaktních míst v oblasti vzdělávání by mohla být činná v rámci sítě národních styčných úředníků a být výchozím bodem pro budoucí koordinaci v rámci členských států.

(28) Agentura ENISA by měla být nápomocna skupině pro spolupráci zřízené směrnicí (EU) 2016/1148 při provádění jejích úkolů, zejména prostřednictvím poskytování odborných znalostí a poradenství a prostřednictvím usnadňování výměny osvědčených postupů týkajících se rizik a incidentů, zejména pak pokud jde o určování provozovatelů základních služeb členskými státy, a to i ve vztahu k přeshraničním vazbám.

(29) S cílem podněcovat spolupráci mezi veřejným a soukromým sektorem a v rámci soukromého sektoru, zejména za účelem podpory ochrany kritických infrastruktur, by agentura ENISA 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.

(30) Vzhledem k tomu, že možný negativní dopad zranitelností v produktech, službách a procesech IKT trvale narůstá, zjišťování a odstraňování těchto zranitelností hraje důležitou roli při snižování celkového kybernetického bezpečnostního rizika. Spolupráce mezi organizacemi, výrobci nebo poskytovateli takto zranitelných produktů, služeb a procesů IKT a členy výzkumné obce v oblasti kybernetické bezpečnosti a vládami, které zranitelnosti naleznou, prokazatelně značně zvyšuje míru zjištěných a odstraněných zranitelností v produktech, službách a procesech IKT. Koordinované zveřejňování zranitelností specifikuje strukturovaný proces spolupráce, v jehož rámci je o zranitelnostech informován vlastník informačního systému, čímž se organizaci umožní diagnostikovat a odstranit zranitelnost dříve, než budou podrobné informace o ní sděleny třetím stranám nebo veřejnosti. V rámci tohoto procesu je rovněž zajištěna koordinace mezi tím, kdo zranitelnost nalezl, a organizací, pokud jde o zveřejnění uvedených zranitelností. Politika koordinovaného zveřejňování zranitelností by mohla hrát významnou roli v úsilí členských států o zlepšení kybernetické bezpečnosti.

(31) Agentura ENISA by měla agregovat a analyzovat dobrovolně sdílené vnitrostátní zprávy od týmů CSIRT a interinstitucionálního týmu pro reakci na počítačové hrozby pro orgány, instituce a jiné subjekty Unie zřízeného na základě ujednání mezi Evropským parlamentem, Evropskou radou, Radou Evropské unie, Evropskou komisí, Soudním dvorem Evropské unie, Evropskou centrální bankou, Evropským účetním dvorem, Evropskou službou pro vnější činnost, Evropským hospodářským a sociálním výborem, Evropským výborem regionů a Evropskou investiční bankou o organizaci a fungování týmu pro reakci na počítačové hrozby pro orgány, instituce a jiné subjekty Unie (CERT-EU) ([14]), s cílem přispět ke stanovování společných postupů, jazyka a terminologie pro výměnu informací. Agentura ENISA by v této souvislosti rovněž měla zapojit soukromý sektor v rámci směrnice (EU) 2016/1148, která stanoví základ pro dobrovolnou výměnu technických informací na operativní úrovni v rámci sítě týmů CSIRT (dále jen „síť CSIRT“) vytvořené uvedenou směrnicí.

(32) V případě rozsáhlých přeshraničních incidentů a krizí v oblasti kybernetické bezpečnosti by agentura ENISA měla přispět k reakci na úrovni Unie. Tato úloha by měla být vykonávána v souladu s mandátem agentury ENISA podle tohoto nařízení a členské státy by měly dohodnout přístup v rámci doporučení Komise (EU) 2017/1584 ([15]) a v rámci závěrů Rady ze dne 26. června 2018 o koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize. Úloha by mohla zahrnovat shromažďování příslušných informací a působení jako zprostředkovatel mezi sítí CSIRT a technickou komunitou a mezi subjekty s rozhodovací pravomocí příslušnými pro krizové řízení. Agentura ENISA by dále měla podporovat operativní spolupráci mezi členskými státy, pokud o to jeden či více členských států žádá, při řešení incidentů po technické stránce, a to usnadňováním příslušné výměny technických řešení mezi členskými státy a poskytováním vstupů do veřejných komunikací. Agentura ENISA by měla tuto operativní spolupráci podporovat testováním způsobů takové spolupráce prostřednictvím pravidelných cvičení v oblasti kybernetické bezpečnosti.

(33) Při podpoře operativní spolupráce by agentura ENISA měla využít dostupné technické a operativní odborné znalosti týmu CERT-EU, a to prostřednictvím strukturované spolupráce. Tato strukturovaná spolupráce by mohla vycházet z odborných znalostí agentury ENISA. V případě potřeby by měla být učiněna speciální ujednání mezi oběma subjekty o praktické podobě takové spolupráce a mělo by se zabránit zdvojování činností.

(34) Při plnění svých úkolů pro podporu operativní spolupráce v rámci sítě týmů CSIRT by agentura ENISA 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 kybernetických hrozeb a incidentů. Agentura ENISA by měla usnadňovat technické řešení incidentů, které mají závažný nebo významný dopad, zejména podporou dobrovolného sdílení technických řešení mezi členskými státy nebo aby vytvářela kombinované technické informace, jako jsou technická řešení dobrovolně sdílená členskými státy. Doporučení (EU) 2017/1584 doporučuje, aby členské státy spolupracovaly v dobré víře a aby mezi sebou a s agenturou ENISA bez zbytečného odkladu sdílely informace o rozsáhlých incidentech a krizích v oblasti kybernetické bezpečnosti. Tyto informace by agentuře ENISA dále pomohly při plnění jejích úkolů na podporu operativní spolupráce.

(35) Jako součást pravidelné spolupráce na technické úrovni na podporu informovanosti Unie o aktuální situaci by agentura ENISA měla v úzké spolupráci s členskými státy připravovat pravidelné podrobné technické zprávy EU o situaci v oblasti kybernetické bezpečnosti týkající se incidentů a kybernetických 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 pro oblast bezpečnosti sítí a informačních systémů (dále jen „jednotná kontaktní místa“) zřízená podle směrnice (EU) 2016/1148 (v obou případech dobrovolně), Evropské centrum pro boj proti kyberkriminalitě (EC3) při Europolu, tým CERT-EU a případně Středisko Evropské unie pro analýzu zpravodajských informací (EU INTCEN) při Evropské službě pro vnější činnost. Zpráva by měla být k dispozici Radě, Komisi, vysokému představiteli Unie pro zahraniční věci a bezpečnostní politiku a síti CSIRT.

(36) Podpora agentury ENISA ve vztahu k následným technickým šetřením incidentů se závažným nebo významným dopadem prováděným na základě žádosti dotčených členských států by se měla zaměřovat na předcházení budoucím incidentům. Dotčené členské státy by měly poskytnout nezbytné informace a pomoc s cílem umožnit agentuře ENISA následné technické šetření účinně podpořit.

([14]) Úř. věst. C 12, 13.1.2018, s. 1.

([15]) Doporučení Komise (EU) 2017/1584 ze dne 13. září 2017 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (Úř. věst. L 239, 19.9.2017, s. 36).

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

(38) K lepšímu pochopení výzev v oblasti kybernetické bezpečnosti a s cílem poskytovat členským státům a orgánům, institucích a jiným subjektům Unie dlouhodobé strategické poradenství je třeba, aby agentura ENISA analyzovala současná a nově se objevující kybernetická bezpečnostní rizika. Za tímto účelem by agentura ENISA 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 ENISA by měla také podporovat členské státy a orgány, instituce a jiné subjekty Unie při určování nových kybernetických bezpečnostních rizik a při předcházení incidentům tak, že bude provádět analýzy kybernetických hrozeb, zranitelností a incidentů.

(39) Za účelem zvýšení odolnosti Unie by agentura ENISA měla rozvíjet odborné znalosti v oblasti kybernetické bezpečnosti infrastruktur, zejména na podporu odvětví uvedených v příloze II směrnice (EU) 2016/1148 a odvětví využitých poskytovateli digitálních služeb uvedených v příloze III uvedené směrnice, a to poskytováním poradenství, vydáváním pokynů a výměnou osvědčených postupů. S cílem zajistit snazší přístup k lépe strukturovaným informacím o kybernetických bezpečnostních rizicích a o možných prostředcích nápravy by agentura ENISA měla vytvořit a spravovat „informační centrum“ Unie, jednotný portál („one-stop-shop“) poskytující veřejnosti informace o kybernetické bezpečnosti získané od unijních a vnitrostátních organizací, institucí a subjektů. Usnadnění přístupu k lépe strukturovaným informacím o kybernetických bezpečnostních rizicích a o možných prostředcích nápravy rovněž může pomoci členským státům rozvíjet jejich schopnosti a sladit jejich postupy, aby došlo ke zvýšení jejich celkové odolnosti vůči kybernetickým útokům.

(40) Agentura ENISA by měla přispívat ke zvyšování informovanosti veřejnosti ohledně kybernetických bezpečnostních rizik, rovněž prostřednictvím celounijních informačních kampaní, podpory vzdělávání a poskytování pokynů a osvědčených postupů pro jednotlivé uživatele zaměřených na občany, organizace a podniky. Agentura ENISA by rovněž měla přispívat k podpoře osvědčených postupů a řešení, včetně kybernetické hygieny a počítačové gramotnosti na úrovni občanů, organizací a podniků, a to shromažďováním a analyzováním veřejně dostupných informací týkajících se závažných incidentů a sestavováním a zveřejňováním zpráv a pokynů pro občany, organizace a podniky ke zlepšení celkové úrovně jejich připravenosti a odolnosti. Agentura ENISA by se měla rovněž snažit poskytovat spotřebitelům příslušné informace o platných systémech certifikace, například poskytnutím pokynů a doporučení. Agentura ENISA by dále měla v souladu s akčním plánem digitálního vzdělávání stanoveným sdělením Komise ze dne 17. ledna 2018 a 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 digitální gramotnost a informovanost o potenciálních kybernetických hrozbách, včetně počítačové kriminality jako phishingové útoky, botnety, finanční a bankovní podvody, incidenty s datovými podvody, a podporovat základní multifaktoriální ověřování, patching, šifrování, anonymizaci a ochranu údajů.

(41) Agentura by měla hrát ústřední úlohu při urychlování informovanosti koncových uživatelů o bezpečnosti zařízení a bezpečném používání služeb a měla by na úrovni Unie prosazovat bezpečnost a ochranu soukromí již od fáze návrhu. Při sledování tohoto cíle by agentura ENISA měla využít dostupné osvědčené postupy a zkušenosti získané zejména od akademických institucí a výzkumných pracovníků v oblasti bezpečnosti informačních technologií.

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

(43) Agentura ENISA by měla přispět k úsilí Unie o spolupráci s mezinárodními organizacemi, jakož i v rámci příslušných mezinárodních rámců spolupráce v oblasti kybernetické bezpečnosti. Agentura ENISA by měla zejména případně přispět ke spolupráci s organizacemi, jako je OECD, OBSE a NATO. Taková spolupráce by mohla zahrnovat společná cvičení v oblasti kybernetické bezpečnosti a koordinaci společné reakce na incidenty. Tyto činnosti mají být vykonávány při plném dodržení zásad inkluzivnosti, reciprocity a rozhodovací samostatnosti Unie, aniž je dotčena zvláštní povaha bezpečnostní a obranné politiky kteréhokoliv členského státu.

(44) Aby bylo zajištěno, že agentura ENISA plně dosahuje svých cílů, měla by spolupracovat s příslušnými orgány dohledu Unie a jinými příslušnými orgány v Unii, s orgány, institucemi a jinými subjekty Unie, včetně týmu CERT-EU, EC3, Evropské obranné agentury (EDA), Agentury pro evropský globální navigační družicový systém (Agentura pro evropský GNSS), Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC), Evropské agentury pro provozní řízení rozsáhlých informačních systémů v oblasti svobody, bezpečnosti a práva (eu-LISA), Evropské centrální banky (ECB), Evropského orgánu pro bankovnictví (EBA), Evropského sboru pro ochranu osobních údajů, Agentury pro spolupráci energetických regulačních orgánů (ACER), Agentury Evropské unie pro bezpečnost letectví (EASA) a všech dalších agentur Unie zapojených do kybernetické bezpečnosti. Agentura ENISA by měla rovněž spolupracovat s orgány zabývajícími se ochranou údajů, a to za účelem výměny know-how a osvědčených postupů a měla by poskytovat poradenství ohledně otázek 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 v poradní skupině agentury ENISA. Při spolupráci s donucovacími orgány týkající se otázek bezpečnosti sítí a informací, které by mohly mít dopad na jejich práci, by agentura ENISA měla respektovat stávající informační kanály a zavedené sítě.

(45) Mohla by být navázána partnerství s akademickými institucemi, které realizují výzkumné iniciativy v příslušných oblastech, a měly by existovat příslušné kanály k předávání podnětů spotřebitelských a dalších organizací, které by měly být zohledněny.

(46) Agentura ENISA ve funkci sekretariátu sítě CSIRT by měla podporovat týmy CSIRT členských států a tým CERT-EU při operativní spolupráci ve vztahu ke všem příslušným úkolům sítě CSIRT, jak jsou vymezeny ve směrnici (EU) 2016/1148. Agentura ENISA 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 mohou postihnout alespoň dva týmy CSIRT, přičemž by měla náležitě zohlednit standardní operační postupy sítě CSIRT.

(47) Za účelem zvýšení připravenosti Unie v oblasti reakce na incidenty by agentura ENISA měla pořádat pravidelná cvičení v oblasti kybernetické bezpečnosti na úrovni Unie a poskytovat na žádost podporu členským státům a institucím, orgánům a jiným subjektům Unie při pořádání takových cvičení. Jednou za dva roky by se měla pořádat rozsáhlá komplexní cvičení, která zahrnují technické, operativní nebo strategické prvky. Agentura ENISA by navíc měla mít možnost pravidelně pořádat méně komplexní cvičení se stejným cílem zvýšit připravenost Unie v reakci na incidenty.

(48) Agentura ENISA by měla dále rozvíjet a udržovat svoji odbornost v oblasti certifikace kybernetické bezpečnosti s cílem podporovat politiku Unie v této oblasti. Agentura ENISA by měla za účelem zvýšení transparentnosti záruk kybernetické bezpečnosti produktů, služeb a procesů IKT a s tím souvisejícího posílení důvěry v digitální vnitřní trh a jeho konkurenceschopnosti navazovat na stávající osvědčené postupy a 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 (evropský rámec pro certifikaci kybernetické bezpečnosti).

(49) 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 ENISA 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.

(50) Agentura ENISA by měla vybízet členské státy a výrobce a poskytovatele produktů, služeb a procesů IKT, aby zvýšili své obecné standardy v oblasti bezpečnosti, a umožnili tak všem uživatelům internetu podniknout potřebné kroky k zajištění své vlastní kybernetické bezpečnosti, a měla by k tomu poskytovat podněty. Výrobci a poskytovatelé produktů, služeb a procesů IKT by měli zejména poskytnout nezbytné aktualizace a stáhnout z trhu nebo z oběhu či recyklovat produkty, služby a procesy IKT, které nesplňují základní normy v oblasti kybernetické bezpečnosti, a dovozci a distributoři by měli zajistit, aby produkty, služby a procesy IKT, které uvádějí na trh Unie, odpovídaly platným požadavkům a nepředstavovaly pro spotřebitele v Unii riziko.

(51) Agentura ENISA by měla mít možnost ve spolupráci s příslušnými orgány šířit informace týkající se úrovně kybernetické bezpečnosti produktů, služeb a procesů IKT nabízených na vnitřním trhu a měla by vydávat varování, která jsou určená výrobcům a poskytovatelům produktů, služeb a procesů IKT a která od nich požadují, aby zvýšili bezpečnost svých produktů, služeb a procesů IKT, včetně kybernetické bezpečnosti.

(52) Agentura ENISA 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 a priorit výzkumu v oblasti kybernetické bezpečnosti. S cílem určit potřeby a priority v oblasti výzkumu by agentura ENISA měla rovněž konzultovat příslušné skupiny uživatelů. Konkrétně je možno navázat spolupráci s Evropskou radou pro výzkum a Evropským inovačním a technologickým institutem, jakož i s Ústavem Evropské unie pro studium bezpečnosti.

(53) Agentura ENISA by měla pravidelně konzultovat s organizacemi pro normalizaci, zejména s evropskými normalizačními organizacemi, při vypracovávání evropských systémů certifikace kybernetické bezpečnosti.

(54) Kybernetické hrozby jsou globální záležitostí. Je nutná užší mezinárodní spolupráce pro zvýšení standardů kybernetické bezpečnosti, včetně stanovení společných norem chování, přijetí kodexů chování a používání mezinárodních norem, a lepší výměna informací, jež by podpořila pružnější mezinárodní spolupráci v reakci na problémy týkající se bezpečnosti sítí a informací a prosazování společného globálního přístupu k nim. Agentura ENISA 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.

(55) Agentura ENISA by měla být schopna reagovat na žádosti ad hoc o poradenství a pomoc od členských států a orgánů, institucí a jiných subjektů Unie, které se týkají záležitostí spadajících do mandátu agentury ENISA.

(56) Je opodstatněné a doporučuje se zavést určité zásady týkající se řízení agentury ENISA, aby bylo naplněno společné prohlášení a společný přístupu, na nichž se v červenci 2012 dohodla interinstitucionální pracovní skupina pro decentralizované agentury EU a jejichž účelem je zjednodušit činnost decentralizovaných agentur a zlepšit jejich výkonnost. Doporučení ze společného prohlášení a společného přístupu by rovněž měla být odpovídajícím způsobem zohledněna v pracovních programech agentury ENISA, hodnoceních agentury ENISA a v postupech, které agentura ENISA používá pro podávání zpráv a v administrativě.

(57) Správní rada složená ze zástupců členských států a Komise by měla vymezit obecné směry činnosti agentury ENISA 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 pravidel, stanovení transparentních pracovních postupů pro přijímání rozhodnutí agentury ENISA, schvalování jednotného programového dokumentu agentury ENISA, přijímání jejího jednacího řádu, jmenování výkonného ředitele a rozhodování o prodloužení a ukončení funkčního období výkonného ředitele.

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

(59) Řádné fungování agentury ENISA 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. Výkonný ředitel by měl své povinnosti vykonávat zcela nezávisle. Výkonný ředitel by měl za tímto účelem po předchozích konzultacích s Komisí zpracovat návrh ročního pracovního programu agentury ENISA a učinit veškeré kroky nezbytné k zajištění jeho řádného plnění. Výkonný ředitel by měl vypracovávat výroční zprávy o provádění ročního pracovního programu agentury ENISA, které se předloží správní radě, a návrh odhadu příjmů a výdajů agentury ENISA 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. Zřízení ad hoc pracovní skupiny je považováno za nezbytné zejména v souvislosti s vypracováním konkrétního návrhu evropského systému certifikace kybernetické bezpečnosti (dále jen „návrh systému“). Výkonný ředitel by měl zajistit, aby byli členové ad hoc pracovní skupiny vybráni na základě

nejvyšších standardů odborných znalostí a při snaze řádně zohlednit genderovou vyváženost a rovnovážné zastoupení podle obsahu činnosti mezi zástupci veřejné správy členských států, zástupci orgánů, institucí a jiných subjektů Unie, zástupci soukromého sektoru, včetně průmyslového odvětví, a zástupci uživatelů a vědeckých odborníků v oblasti bezpečnosti sítí a informací.

(60) 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 rozhodnutí správní rady.

(61) Pro pravidelný dialog se soukromým sektorem, organizacemi spotřebitelů a ostatními významnými zúčastněnými stranami by agentura ENISA měla mít poradní skupinu agentury ENISA jako svůj poradní orgán. Tato skupina, ustavená správní radou na návrh výkonného ředitele, by se měla věnovat otázkám, které mají význam pro zúčastněné strany, a měla by je předkládat agentuře ENISA. Poradní skupina agentury ENISA by měla být zejména konzultována k návrhu ročního pracovního programu agentury ENISA. Složení poradní skupiny agentury ENISA a úkoly, jimiž je pověřena, by měly zajistit dostatečné zastoupení zúčastněných stran na činnosti agentury ENISA.

(62) Měla by být zřízena Skupina zúčastněných stran pro certifikaci kybernetické bezpečnosti, aby agentuře ENISA a Komisi pomohla usnadňovat konzultace s příslušnými zúčastněnými stranami. Skupina zúčastněných stran pro certifikaci kybernetické bezpečnosti by měla být složena z členů zastupujících vyváženě a přiměřeně průmyslové odvětví, a to na straně poptávky i nabídky produktů a služeb IKT, a zahrnující zejména malé a střední podniky, poskytovatele digitálních služeb, evropské a mezinárodní normalizační orgány, vnitrostátní akreditační orgány, orgány dozoru pro ochranu údajů a subjekty posuzování shody podle nařízení Evropského parlamentu a Rady(ES) č. 765/2008 ([16]), akademickou obec i spotřebitelské organizace.

(63) Agentura ENISA by měla mít zavedena pravidla týkající se prevence a řešení střetu zájmů. Agentura ENISA by rovněž měla uplatňovat odpovídající ustanovení práva Unie týkající se přístupu veřejnosti k dokumentům podle nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ([17]). Osobní údaje by měly být agenturou ENISA zpracovávány v souladu s nařízením Evropského parlamentu a Rady (EU) 2018/1725 ([18]). Agentura ENISA by měla zejména dodržovat předpisy vztahující se na orgány, instituce a jiné subjekty Unie a rovněž vnitrostátní předpisy o nakládání s informacemi, zejména s citlivými neutajovanými informacemi a utajovanými informacemi Evropské unie.

(64) Aby byla zaručena plná autonomie a nezávislost agentury ENISA a bylo jí umožněno vykonávat další 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 ENISA. Aby mohla agentura ENISA plnit rostoucí objem svých úkolů a dosahovat své cíle, je mimořádně důležité, aby měla k dispozici přiměřený rozpočet. Většina zaměstnanců agentury ENISA by se měla přímo podílet na operativním plnění mandátu agentury ENISA. Hostitelský nebo jakýkoli jiný členský stát by měl mít možnost poskytnout dobrovolné příspěvky do rozpočtu agentury ENISA. Všechny subvence ze souhrnného rozpočtu Unie by měly podléhat rozpočtovému procesu Unie. Účetní dvůr by měl navíc provádět audit účetnictví agentury ENISA s cílem zajistit transparentnost a odpovědnost.

(65) Certifikace kybernetické bezpečnosti hraje důležitou úlohu při zvyšování důvěry v produkty, služby a procesy IKT a při zvyšování 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, služby a procesy poskytují určitou úroveň kybernetické bezpečnosti. Propojené a automatizované automobily, elektronické zdravotnické prostředky, 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 (EU) 2016/1148 jsou zároveň odvětvími, v nichž má certifikace kybernetické bezpečnosti zásadní význam.

([16]) Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

([17]) 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).

([18]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

(66) 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 produktů a řešení v oblasti kybernetické bezpečnosti. Dodávky produktů, služeb a procesů 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 v oblasti kybernetické bezpečnosti, patří dále absence interoperabilních řešení (technických norem), postupů a unijních mechanismů pro certifikaci. To snižuje konkurenceschopnost podniků Unie na vnitrostátní, unijní i celosvětové úrovni. Rovněž to omezuje výběr funkčních a užitečných technologií kybernetické bezpečnosti, ke kterým mají občané a podniky přístup. Podobně Komise ve svém sdělení k přezkumu v polovině období provádění strategie pro jednotný digitální trh – propojený jednotný digitální trh pro všechny z roku 2017 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 mohlo zachovat důvěru v internet a řešit stávající roztříštěnost vnitřního trhu.

(67) Certifikace kybernetické bezpečnosti produktů, služeb a procesů IKT je v současné době využívána pouze v omezené míře. Pokud existuje, pak převážně na úrovni členských států nebo v rámci systémů definovaných potřebami průmyslového odvětví. V této souvislosti není certifikát vydaný jedním vnitrostátním orgánem pro certifikaci kybernetické bezpečnosti v zásadě není uznáván v jiných členských státech. Společnosti proto musí své produkty, služby a procesy IKT certifikovat v několika členských státech, v nichž působí, například s cílem účastnit se vnitrostátních zadávacích řízení, a tím se zvyšují jejich náklady. 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, což je na překážku mechanismům vzájemného uznávání v rámci Unie.

(68) Bylo vynaloženo určité úsilí k zajištění vzájemného uznávání certifikátů v Unii. Toto úsilí však bylo úspěšné pouze částečně. Nejdůležitějším příkladem je v tomto ohledu dohoda skupiny vyšších úředníků – bezpečnost informačních systémů (SOG-IS) o vzájemném uznávání. Ačkoliv dohoda skupiny SOG-IS o vzájemném uznávání představuje nejdůležitější model spolupráce a vzájemného uznávání v oblasti certifikace bezpečnosti, zahrnuje tato skupina pouze některé členské státy. To z pohledu vnitřního trhu účinnost dohody skupiny SOG-IS o vzájemném uznávání omezuje.

(69) Je tedy nezbytné přijmout společný přístup a zřídit evropský rámec certifikace kybernetické bezpečnosti, který stanoví hlavní horizontální požadavky pro evropské systémy certifikace kybernetické bezpečnosti, které mají být vypracovány, a umožní, aby byly evropské certifikáty kybernetické bezpečnosti a EU prohlášení o shodě pro produkty, služby a procesy IKT uznávané a používané ve všech členských státech. Zásadní přitom je stavět na stávajících vnitrostátních a mezinárodních systémech a rovněž na systémech vzájemného uznávání, zejména systému skupiny SOG-IS, a umožnit hladký přechod ze stávajících systémů v rámci těchto systémů na systémy podle tohoto nového evropského rámce pro certifikaci kybernetické bezpečnosti. Evropský rámec pro certifikaci kybernetické bezpečnosti by měl mít dvojí účel. Za prvé by měl pomoci zvýšit důvěru v produkty, služby a procesy IKT, které byly certifikovány podle evropských systémů certifikace kybernetické bezpečnosti. Za druhé by měl pomoci zabránit násobení protichůdných nebo odporujících si vnitrostátních systémů pro certifikací kybernetické bezpečnosti, a tím snížit náklady podniků působících na jednotném digitálním trhu. Evropské systémy certifikace kybernetické bezpečnosti by měly být nediskriminační a měly by být založeny na evropských nebo mezinárodních normách, pokud tyto normy nejsou neúčinné nebo nevhodné k dosažení cílů Unie, které jsou v tomto ohledu oprávněné.

(70) Evropský rámec pro certifikaci kybernetické bezpečnosti by měl být jednotně zaveden ve všech členských státech, aby se zabránilo spekulativnímu výběru místa pro certifikaci v závislosti na rozdílné přísnosti požadavků v různých členských státech.

(71) Evropské systémy certifikace kybernetické bezpečnosti by měly vycházet z toho, co již existuje na mezinárodní i vnitrostátní úrovni, a v případě nutnosti z technických specifikací z fór a konsorcií a měly by využít poznatků o stávajících silných stránkách a poznatků z vyhodnocování a oprav zranitelností.

(72) Flexibilní řešení v oblasti kybernetické bezpečnosti jsou nezbytná pro to, aby si průmyslové odvětví udržovalo náskok před kybernetickými hrozbami, a proto by měl být každý systém certifikace navržen tak, aby se vyhnul riziku rychlé ztráty aktuálnosti.

(73) Komisi by měla být svěřena pravomoc přijímat evropské systémy certifikace kybernetické bezpečnosti týkající se konkrétních skupin produktů, služeb a procesů 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 průmyslovým odvětvím nebo jinými soukromými organizacemi by měly spadat mimo oblast působnosti tohoto nařízení. Subjekty provozující tyto systémy by však měly mít možnost Komisi navrhnout, aby tyto systémy zvážila jako základ pro jejich schválení jakožto evropského systému certifikace kybernetické bezpečnosti.

(74) Ustanoveními tohoto nařízení by neměly být dotčeno Unie stanovující zvláštní pravidla týkající se certifikace produktů, služeb a procesů IKT. Zejména nařízení (EU) 2016/679 stanoví pravidla pro zavedení mechanismů pro vydávání osvědčení o ochraně údajů a zavedení pečetí a známek dokládajících ochranu údajů pro účely prokázání souladu s uvedeným 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, služeb a procesů IKT umožnit rychlé posouzení úrovně ochrany údajů. Tímto nařízením není dotčeno vydávání osvědčení pro operace zpracování údajů podle nařízení (EU) 2016/679, včetně situací, kdy jsou tyto operace již zahrnuty v produktech, službách a procesech IKT.

(75) Účelem evropských systémů certifikace kybernetické bezpečnosti by mělo být zajistit, aby produkty, služby a procesy IKT certifikované podle takového systému splňovaly konkrétní požadavky, které mají za cíl chránit dostupnost, autentičnost, integritu a důvěrnost uchovávaných, předávaných nebo zpracovávaných údajů nebo souvisejících funkcí nebo služeb nabízených nebo dostupných prostřednictvím těchto produktů, služeb a procesů v rámci jejich životního cyklu. V tomto nařízení není možné podrobně stanovit požadavky na kybernetickou bezpečnosti týkající se všech produktů, služeb a procesů IKT. Produkty, služby a procesy IKT a s nimi související potřeby v oblasti kybernetické bezpečnosti jsou natolik rozmanité, že je velmi obtížné vypracovat obecné požadavky na kybernetickou bezpečnost, které by byly platné za všech okolností. Proto je pro účely certifikace nutné přijmout obecný a široký obsah pojmu kybernetická bezpečnost, který by měl být doplněn souborem konkrétních cílů v oblasti kybernetické bezpečnosti, které je třeba zohlednit při navrhování evropských systémů certifikace kybernetické bezpečnosti. Způsoby, jimiž bude těchto cílů u konkrétních produktů, služeb a procesů 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.

(76) Technické specifikace, které by měly být využity v evropských systémech certifikace kybernetické bezpečnosti, by měly dodržovat požadavky stanovené v příloze II nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ([19]). Některé odchylky od těchto požadavků 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 by měly být zveřejněny.

(77) Posuzování shody je procesem zhodnocení, zda byly splněny stanovené požadavky týkající se produktu, služby nebo procesu IKT. Tento proces provádí nezávislá třetí strana, odlišná od výrobce posuzovaného produktu IKT nebo poskytovatele posuzované služby či procesu IKT. V návaznosti na úspěšné hodnocení produktu, služby nebo procesu IKT by měl být vydán evropský certifikát kybernetické bezpečnosti. Evropský certifikát kybernetické bezpečnosti je třeba považovat za potvrzení toho, že posouzení bylo řádně provedeno. V závislosti na úrovni záruky by evropský systém certifikace kybernetické bezpečnosti měl uvádět, zda evropský certifikát kybernetické bezpečnosti vydal soukromý nebo veřejný subjekt. Posuzování shody a certifikace nemohou samy o sobě zaručit, že certifikované produkty, služby a procesy IKT jsou kyberneticky bezpečné. Jsou to procesy a technické metodiky sloužící k potvrzení, že produkty, služby a procesy IKT byly testovány a že splňují určité jinde stanovené požadavky na kybernetickou bezpečnost, např. požadavky technických norem.

(78) Uživatelé evropských certifikátů kybernetické bezpečnosti by měli vybírat odpovídající certifikaci a s ní spojené bezpečnostní požadavky na základě analýzy rizik souvisejících s použitím produktů, služeb nebo procesů IKT. Úroveň záruky by tak měla být přiměřená úrovni rizika spojeného se zamýšleným použitím produktu, služby nebo procesu IKT.

([19]) Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

(79) Evropské systémy certifikace kybernetické bezpečnosti by mohly stanovit posuzování shody, které má být provedeno v rámci výhradní odpovědnosti výrobce produktu IKT nebo poskytovatele služby či procesu IKT (vlastní posuzování shody). V takových případech by mělo být postačující, že výrobce produktu IKT nebo poskytovatel služby či procesu IKT provede sám všechny kontroly pro zajištění souladu produktů, služeb nebo procesů IKT s evropským systémem certifikace kybernetické bezpečnosti. Vlastní posuzování shody by mělo být považováno za vhodné pro produkty, služby a procesy IKT s nízkou složitostí, jako je jednoduchý projekční a výrobní mechanismus, které představují nízké riziko pro veřejnost. Navíc by vlastní posuzování shody mělo být umožněno pouze pro produkty, služby a procesy IKT odpovídající úrovni záruky „základní".

(80) Evropské systémy certifikace kybernetické bezpečnosti by mohly umožňovat vlastní posuzování shody i certifikaci produktů, služeb a procesů IKT. V takovém případě by systém měl stanovit jasné a srozumitelné prostředky pro spotřebitele nebo jiné uživatele pro rozlišení mezi produkty, službami a procesy IKT, za jejichž posuzování odpovídá výrobce nebo poskytovatel, a produkty, službami a procesy IKT, které jsou certifikovány třetí stranou.

(81) Výrobce nebo poskytovatel produktů, služeb či procesů IKT, který provádí vlastní posuzování shody, by měl mít možnost vydat a podepsat EU prohlášení o shodě jako součást postupu posuzování shody. EU prohlášení o shodě je dokumentem, který uvádí, že určitý produkt, služba nebo proces IKT splňuje požadavky evropského systému certifikace kybernetické bezpečnosti. Vydáním a podepsáním EU prohlášení o shodě výrobce produktu IKT nebo poskytovatel služby či procesu IKT přebírá odpovědnost za to, že produkt, služba nebo proces IKT splňuje právní požadavky evropského systému certifikace kybernetické bezpečnosti. Kopie EU prohlášení o shodě by měla být předložena vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a agentuře ENISA.

(82) Výrobci nebo poskytovatelé produktů, služeb či procesů IKT by měli uchovávat EU prohlášení o shodě, technickou dokumentaci a veškeré další důležité informace týkající se shody produktů, služeb nebo procesů IKT s evropským systémem certifikace kybernetické bezpečnosti k dispozici příslušnému vnitrostátnímu orgánu certifikace kybernetické bezpečnosti po dobu stanovenou v příslušném evropském systému certifikace kybernetické bezpečnosti. Technická dokumentace by měla upřesňovat požadavky použitelné podle daného systému a v rozsahu odpovídajícím vlastnímu posuzování shody pokrývat návrh, výrobu a provoz produktu, služby nebo procesu IKT. Složení technické dokumentace by mělo být takové, aby umožnilo posoudit. zda produkt, služba nebo proces IKT splňuje požadavky použitelné podle daného systému.

(83) Řízení evropského rámce pro certifikaci kybernetické bezpečnosti zohledňuje zapojení členských států, jakož i odpovídající zapojení zúčastněných stran a vymezuje úlohu Komise během plánování a navrhování, podávání žádosti, přípravy, přijímání a provádění přezkumů evropských systémů kybernetické bezpečnosti.

(84) Komise by měla připravit, za podpory Evropské skupiny pro certifikaci kybernetické bezpečnosti a Skupiny zúčastněných stran pro certifikaci kybernetické bezpečnosti a po otevřené a široké konzultaci, průběžný pracovní program Unie pro evropské systémy certifikace kybernetické bezpečnosti a zveřejnit jej v podobě nezávazného nástroje. Průběžný pracovní program Unie by měl být strategický dokument umožňující průmyslovému odvětví, vnitrostátním orgánům a normalizačním orgánům zejména připravit s předstihem do budoucna evropské systémy certifikace kybernetické bezpečnosti. Průběžný pracovní program Unie by měl zahrnovat víceletý přehled žádostí o návrhy systémů, které má Komise v úmyslu předložit agentuře ENISA k přípravě na základě konkrétních důvodů. Komise by měla vzít průběžný pracovní program Unie v úvahu při přípravě průběžného plánu pro normalizaci IKT a žádostí o vypracování norem určených evropským normalizačním organizacím. S ohledem na rychlé zavádění a přijímání nových technologií, výskyt dříve neznámých kybernetických bezpečnostních rizik a legislativní vývoj a vývoj na trhu by Komise nebo Evropská skupina pro certifikaci kybernetické bezpečnosti měly být oprávněny požádat agenturu ENISA, aby vypracovala návrhy systémů, které nebyly zahrnuty do průběžného pracovního programu Unie. V takových případech by Komise a Evropská skupina pro certifikaci kybernetické bezpečnosti měly rovněž posoudit nezbytnost takové žádosti tím, že zohlední celkové záměry a cíle tohoto nařízení a potřebu zajištění kontinuity, pokud jde o plánování a použití zdrojů agentury ENISA.

V návaznosti na takovou žádost by agentura ENISA měla neprodleně vypracovat návrhy systémů pro konkrétní produkty, služby a procesy IKT. Komise by měla vyhodnotit pozitivní a negativní dopad své žádosti na daný zvláštní trh, zejména její dopad na malé a střední podniky, inovace, překážky vstupu na tento trh a náklady pro koncové uživatele. Komisi by 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. Tyto prvky by měly mimo jiné zahrnovat rozsah a předmět certifikace kybernetické bezpečnosti včetně kategorií produktů, služeb a procesů IKT, na které se certifikace vztahuje, podrobnou specifikaci požadavků na kybernetickou bezpečnost, například prostřednictvím odkazu na příslušné normy nebo technické specifikace, konkrétní kritéria a metody hodnocení a úroveň záruky („základní“, „podstatná“ nebo „vysoká“), kterou mají zajistit, a případně úroveň hodnocení. Agentura ENISA by měla mít možnost žádost Evropské skupiny pro certifikaci kybernetické bezpečnosti odmítnout. Takové rozhodnutí by měla přijmout správní rada a mělo by být řádně zdůvodněno.

(85) 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 systému, jakož i zpětnou vazbu získanou v přípravné fázi agenturou ENISA v rámci konzultačního procesu. Internetová stránka by měla rovněž poskytovat informace o evropských certifikátech kybernetické bezpečnosti a EU prohlášeních o shodě vydaných podle tohoto nařízení, včetně informací o zrušení a pozbytí platnosti těchto certifikátů a prohlášení. Internetová stránka by rovněž měla uvádět vnitrostátní systémy certifikace kybernetické bezpečnosti, které byly nahrazeny evropským systémem certifikace kybernetické bezpečnosti.

(86) Úroveň záruky evropského systému certifikace je podkladem pro důvěru, že produkt, služba či proces IKT splňuje bezpečnostní požadavky konkrétního evropského systému certifikace kybernetické bezpečnosti. V zájmu zajištění soudržnosti evropského rámce pro certifikaci kybernetické bezpečnosti by mělo být možné stanovit pro evropský systém certifikace kybernetické bezpečnosti úrovně záruky evropských certifikátů kybernetické bezpečnosti a EU prohlášení o shodě vydávaných podle tohoto systému. Každý evropský certifikát kybernetické bezpečnosti by mohl uvádět jednu z úrovní záruky „základní“, „podstatná“ či „vysoká“, zatímco EU prohlášení o shodě by se mohlo vztahovat pouze na úroveň záruky „základní“. Úrovně záruky odráží odpovídající náročnost a podrobnosti hodnocení produktu, služby nebo procesu IKT a jsou charakterizovány odkazem na související technické specifikace, normy a postupy včetně technických kontrol, jejichž účelem je zmírnit dopady incidentů nebo jim zabránit. Každá úroveň záruky by měla být konzistentní v rámci jednotlivých odvětvových oblastí, v nichž se certifikace používá.

(87) Evropský systém certifikace kybernetické bezpečnosti by mohl specifikovat několik úrovní hodnocení v závislosti na náročnosti a zevrubnosti použité hodnotící metodiky. Úrovně hodnocení by měly odpovídat jedné z úrovní záruk a být navázány na příslušnou kombinaci složek záruky. Pro každou úroveň záruky by produkt, služba nebo proces IKT měly obsahovat řadu bezpečných funkcí stanovených v systému, jež mohou zahrnovat: bezpečnou přednastavenou konfiguraci, digitální podpis kódu, bezpečnou aktualizaci a ochranu před zneužitím zranitelností v zabezpečení a ochranu proti 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.

(88) Pro úroveň záruky „základní“ by mělo hodnocení vycházet alespoň z následujících složek záruky: hodnocení by mělo přinejmenším zahrnovat přezkum technické dokumentace produktu, služby či procesu IKT ze strany subjektu posuzování shody. Zahrnuje-li certifikace procesy IKT, měl by do předmětu technického přezkumu spadat též proces použitý k návrhu, vývoji a provozu produktu či služby IKT. V případech, kdy evropský systém certifikace kybernetické bezpečnosti stanoví vlastní posuzování shody, by mělo postačovat, že výrobce produktu IKT nebo poskytovatel služby či procesu IKT provedl vlastní posuzování shody dotyčného produktu, služby či procesu IKT se systémem certifikace.

(89) Pro úroveň záruky „podstatná“ by hodnocení mělo navíc k požadavkům na úroveň záruky „základní“ vycházet přinejmenším z ověření souladu bezpečnostních funkcí produktu, služby či procesu IKT s příslušnou technickou dokumentací.

(90) Pro úroveň záruky „vysoká“ by hodnocení mělo navíc k požadavkům na úroveň záruky „podstatná“ vycházet přinejmenším ze zkoušky účinnosti, která hodnotí odolnost bezpečnostních funkcí produktu, služby či procesu IKT vůči propracovaným kybernetickým útokům vedeným osobami se značnými dovednostmi a zdroji.

(91) Využití evropské certifikace kybernetické bezpečnosti a EU prohlášení o shodě by mělo zůstat dobrovolné, pokud právo Unie nebo právní předpisy členských států přijaté v souladu s právem Unie nestanoví jinak. V případě neexistence harmonizovaného práva Unie mohou členské státy přijímat vnitrostátní technické předpisy, jimiž stanoví povinnou certifikaci podle evropského systému certifikace kybernetické bezpečnosti, v souladu se směrnicí Evropského parlamentu a Rady (EU) 2015/1535 ([20]). Členské státy by mohly rovněž využít evropské certifikace kybernetické bezpečnosti v souvislosti se zadáváním veřejných zakázek a se směrnicí Evropského parlamentu a Rady 2014/24/EU ([21])

(92) V některých oblastech by mohlo být nezbytné v budoucnu stanovit konkrétní požadavky na kybernetickou bezpečnost a učinit jejich certifikaci u některých produktů, služeb a procesů IKT povinnou s cílem zlepšit úroveň kybernetické bezpečnosti v Unii. Komise by měla pravidelně sledovat dopady přijatých evropských systémů certifikace kybernetické bezpečnosti na dostupnost bezpečných produktů, služeb a procesů IKT na vnitřním trhu a měla by pravidelně posuzovat míru využití systémů certifikace výrobci a poskytovateli produktů, služeb či procesů IKT v Unii. Účinnost evropských systémů certifikace kybernetické bezpečnosti a otázka, zda by konkrétní systémy měly být stanoveny jako povinné, by měly být posouzeny s ohledem na právní předpisy Unie týkající se kybernetické bezpečnosti, zejména směrnici (EU) 2016/1148, při zohlednění bezpečnosti sítí a informačních systémů používaných provozovateli základních služeb.

(93) Evropské certifikáty kybernetické bezpečnosti a EU prohlášení o shodě by měly napomoci koncovým uživatelům činit informované volby. Proto by produkty, služby a procesy IKT, které byly certifikovány nebo pro které bylo vydáno EU prohlášení o shodě, měly být doplněny o strukturované informace upravené podle předpokládané technické úrovně zamýšleného koncového uživatele. Veškeré takové informace by měly být k dispozici online a případně též ve fyzické podobě. Koncový uživatel by měl mít přístup k informacím o referenčním číslu systému certifikace, úrovni záruky, popisu kybernetických bezpečnostních rizik, které jsou s produktem, službou či procesem IKT spojené, a vydávajícím orgán nebo subjektu, nebo by měl mít možnost získat kopii evropského certifikátu kybernetické bezpečnosti. Koncový uživatel by měl být navíc informován o politice podpory kybernetické bezpečnosti výrobce produktu IKT nebo poskytovatele služby či procesu IKT, tedy jak dlouho může koncový uživatel očekávat, že bude dostávat aktualizace nebo opravy v oblasti kybernetické bezpečnosti. V příslušných případech by měl koncový uživatel obdržet pokyny ohledně kroků nebo nastavení, jež může provést, aby zachoval nebo zvýšil kybernetickou bezpečnost produktu nebo služby IKT, a kontaktní informace o jednotném kontaktním místě pro podávání zpráv a získávání podpory v případě kybernetických útoků (vedle automatického podávání zpráv). Tyto informace by měly být pravidelně aktualizovány a zpřístupňovány na internetové stránce s informacemi o evropských systémech certifikace kybernetické bezpečnosti.

(94) V zájmu dosažení cílů tohoto nařízení a zabránění roztříštěnosti vnitřního trhu by vnitrostátní systémy nebo postupy certifikace kybernetické bezpečnosti pro produkty, služby a procesy 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 certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT, které jsou již zahrnuty do stávajícího evropského systému certifikace kybernetické bezpečnosti. Členským státům by však nemělo být bráněno v přijímání či v zachování vnitrostátních systémů certifikace kybernetické bezpečnosti pro účely národní bezpečnosti. Členské státy by měly Komisi a Evropskou skupinu pro certifikaci kybernetické bezpečnosti informovat o jakémkoliv záměru vypracovat nové vnitrostátní systémy certifikace kybernetické bezpečnosti. Komise a Evropská skupina pro certifikaci kybernetické bezpečnosti by měla posoudit dopady nového vnitrostátního systému certifikace kybernetické bezpečnosti na řádné fungování vnitřního trhu a s ohledem na strategický zájem požádat namísto toho o evropský systém certifikace kybernetické bezpečnosti.

(95) Evropské systémy certifikace kybernetické bezpečnosti mají v rámci Unie pomoci harmonizovat a sjednotit postupy v oblasti kybernetické bezpečnosti. Mají přispět ke zvýšení úrovně kybernetické bezpečnosti v rámci Unie. Návrhy evropských systémů certifikace kybernetické bezpečnosti by měly zohlednit a umožnit vývoj nových inovací v oblasti kybernetické bezpečnosti.

([20]) Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti (Úř. věst. L 241, 17.9.2015, s. 1).

([21]) Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. února 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES (Úř. věst. L 94, 28.3.2014, s. 65).

(96) Evropské systémy certifikace kybernetické bezpečnosti by měly zohlednit stávající metody vývoje softwaru a hardwaru, a zejména dopad častých aktualizací softwaru nebo firmwaru na jednotlivé evropské certifikáty kybernetické bezpečnosti. Evropské systémy certifikace kybernetické bezpečnosti by měly stanovit podmínky, za nichž může být v důsledku aktualizace nezbytné produkt, službu nebo proces IKT opětovně certifikovat nebo omezit rozsah určitého evropského certifikátu kybernetické bezpečnosti, s ohledem jakýkoliv možný nepříznivý dopad aktualizace na plnění bezpečnostních požadavků daného certifikátu.

(97) Jakmile je přijat určitý evropský systém certifikace kybernetické bezpečnosti, výrobci nebo poskytovatelé produktů, služeb či procesů IKT by měli být schopni subjektu posuzování shody podlé své volby kdekoli v Unii předložit žádost o certifikaci svých produktů nebo služeb. Subjekty posuzování shody by měly být akreditovány vnitrostátním akreditačním orgánem, splňují-li určité konkrétní požadavky stanovené v tomto nařízení. Akreditace by měla být vydávána na období nejvýše pěti let a mělo by být možné ji obnovit za stejných podmínek, pokud daný subjekt posuzování shody stále splňuje příslušné požadavky. Vnitrostátní akreditační orgány by měly omezit, pozastavit či zrušit akreditaci subjektu posuzování shody, pokud podmínky pro akreditaci nejsou nebo přestanou být splňovány, nebo pokud subjekt posuzování shody porušuje toto nařízení.

(98) Odkazy ve vnitrostátních právních předpisech na vnitrostátní normám, které v důsledku vstupu evropského systému certifikace kybernetické bezpečnosti v platnost přestaly být účinné, by mohly způsobovat nejasnosti. Členské státy by proto měly přijetí evropského systému certifikace kybernetické bezpečnosti ve svých vnitrostátních právních předpisech zohlednit.

(99) S cílem dosáhnout rovnocenných norem po celé Unii, usnadnit vzájemné uznávání a podpořit celkové přijímání evropských certifikátů kybernetické bezpečnosti a EU prohlášení o shodě je nezbytné zavést systém pro vzájemné hodnocení mezi vnitrostátními orgány certifikace kybernetické bezpečnosti. Vzájemná hodnocení by se měla vztahovat na postupy pro dohled nad shodou produktů, služeb a procesů IKT s evropskými certifikáty kybernetické bezpečnosti, na monitorování povinností výrobců nebo poskytovatelů produktů, služeb či procesů IKT, kteří provádějí vlastní posuzování shody, na monitorování subjektů posuzování shody, jakož i na přiměřenost odborných znalostí zaměstnanců orgánů, které vydávají osvědčení pro úroveň záruky „vysoká“. Komise by měla mít možnost prostřednictvím prováděcích aktů stanovit alespoň pětiletý plán pro vzájemné hodnocení, jakož i pro stanovení kritérií a metodik pro fungování systému vzájemného hodnocení.

(100) Aniž je dotčen obecný systém vzájemného hodnocení, jenž má být zaveden u všech vnitrostátních orgánů certifikace kybernetické bezpečnosti v evropském rámci pro certifikaci kybernetické bezpečnosti, mohou některé evropské systémy certifikace kybernetické bezpečnosti zahrnovat mechanismy vzájemného hodnocení pro orgány, které vydávají v rámci těchto systémů pro produkty, služby a procesy IKT evropské certifikáty kybernetické bezpečnosti na úrovni záruky „vysoká“. Evropská skupina pro certifikaci kybernetické bezpečnosti by měla podporovat provádění takových mechanismů vzájemného hodnocení. Vzájemná hodnocení by měla zejména posoudit, zda dotčené orgány plní své úkoly harmonizovaně, a mohou zahrnout mechanismy opravného prostředku proti rozhodnutí. Výsledky vzájemných hodnocení by měly být zpřístupněny veřejnosti. Dotčené orgány mohou přijmout vhodná opatření s cílem přizpůsobit své postupy a odborné znalosti.

(101) Členské státy by měly určit jeden nebo více vnitrostátních orgánů certifikace kybernetické bezpečnosti s cílem dohlížet na soulad s povinnostmi vyplývajícími z tohoto nařízení. Vnitrostátní orgán certifikace kybernetické bezpečnosti může být stávajícím i novým orgánem. Po dohodě s jiným členským státem by měl mít členský stát rovněž možnost určit jeden nebo více vnitrostátních orgánů certifikace kybernetické bezpečnosti na území tohoto jiného členského státu.

(102) Vnitrostátní orgány certifikace kybernetické bezpečnosti by měly zejména monitorovat a vymáhat povinnosti výrobců nebo poskytovatelů produktů, služeb či procesů IKT usazených na jejich území, pokud jde o EU prohlášení o shodě, měly by pomáhat vnitrostátním akreditačním orgánům při sledování a dohledu nad činnostmi subjektů posuzování shody tím, že jim poskytují odborné znalosti a relevantní informace, měly by pověřovat subjekty posuzování shody prováděním svých úkolů, pokud tyto subjekty plní dodatečné požadavky stanovené v evropském systému certifikace kybernetické bezpečnosti, a měly by sledovat příslušný vývoj v oblasti certifikace kybernetické bezpečnosti. Vnitrostátní orgány certifikace kybernetické bezpečnosti by měly také řešit stížnosti podané fyzickými nebo právnickými osobami v souvislosti s jimi vydanými evropskými certifikáty kybernetické bezpečnosti nebo v souvislosti evropskými certifikáty kybernetické bezpečnosti vydanými subjekty posuzování shody, uvádějí-li tyto certifikáty úroveň záruky „vysoká“, měly by v přiměřeném rozsahu šetřit předmět stížnosti a v přiměřené lhůtě informovat stěžovatele o pokroku a výsledku šetření. Kromě toho by vnitrostátní orgány

certifikace kybernetické bezpečnosti měly spolupracovat s dalšími vnitrostátními orgány certifikace kybernetické bezpečnosti nebo jinými veřejnými orgány, a to i prostřednictvím sdílení informací o možných případech, kdy produkty, služby či procesy IKT nesplňují požadavky tohoto nařízení nebo konkrétních evropských systémů certifikace kybernetické bezpečnosti. Komise by měla tuto sdílení informací usnadnit zpřístupněním obecného elektronického systému pro výměnu informací, například prostřednictvím systému pro výměnu informací v rámci dohledu nad trhem (ICSMS) a systému rychlého varování pro nebezpečné nepotravinářské výrobky (RAPEX), které již dnes využívají orgány dozoru nad trhem podle nařízení (ES) č. 765/2008.

(103) S cílem zajistit jednotné uplatňování evropského rámce pro certifikaci kybernetické bezpečnosti by měla být zřízena Evropská skupina pro certifikaci kybernetické bezpečnosti 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 ENISA a úzce s ní spolupracovat při vypracování návrhů systémů certifikace kybernetické bezpečnosti, v řádně odůvodněných případech žádat agenturu ENISA, aby vypracovala návrh systému, přijímat stanoviska určená agentuře ENISA ohledně návrhů systémů a Komisi ohledně zachování a přezkumu stávajících evropských systémů certifikace kybernetické bezpečnosti. Evropská skupina pro certifikaci kybernetické bezpečnosti by měla usnadnit sdílení osvědčených postupů a odborných znalostí mezi různými vnitrostátními orgány certifikace kybernetické bezpečnosti odpovědnými za pověřování subjektů posuzování shody a vydávání evropských certifikátů kybernetické bezpečnosti.

(104) Evropská komise může za účelem zvyšování informovanosti a usnadnění přijetí budoucích evropských systémů certifikace kybernetické bezpečnosti vydávat obecné či sektorové kybernetické bezpečnostní pokyny, např. osvědčené postupy v oblasti kybernetické bezpečnosti nebo pokyny týkající se odpovědného chování v oblasti kybernetické bezpečnosti zdůrazňující pozitivní účinek používání certifikovaných produktů, služeb a procesů IKT.

(105) V zájmu dalšího usnadnění obchodu a s vědomím, že dodavatelské řetězce IKT jsou globální, může Unie v souladu s článkem 218 Smlouvy o fungování EU uzavírat dohody o vzájemném uznávání týkající se evropských certifikátů kybernetické bezpečnosti. Komise při zohlednění poradenství ze strany agentury ENISA a Evropské skupiny pro certifikaci kybernetické bezpečnosti může doporučit zahájení příslušných jednání. Každý evropský systém certifikace kybernetické bezpečnosti by měl poskytovat konkrétní podmínky pro takové dohody o vzájemném uznávání se třetími zeměmi.

(106) V zájmu zajištění jednotných podmínek pro provádění tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ([22]).

(107) Přezkumný postup by měl být použit pro přijímání prováděcích aktů týkajících se evropských systémů certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT; pro přijímání prováděcích aktů týkajících se způsobů, jakými agentura ENISA provádí šetření; pro přijímání prováděcích aktů týkajících se plánů pro vzájemné hodnocení vnitrostátních orgánů certifikace kybernetické bezpečnosti; jakož i pro přijímání prováděcích aktů týkajících se okolností, formátů a postupů oznamování akreditovaných subjektů posuzování shody podávaných vnitrostátními orgány certifikace kybernetické bezpečnosti Komisi.

(108) Působení agentury ENISA by mělo podléhat pravidelnému a nezávislému hodnocení. Toto hodnocení by mělo zohledňovat cíle agentury ENISA, její pracovní postupy a relevantnost jejích úkolů, zejména pak jejích úkolů souvisejících s operativní spoluprací na úrovni Unie. Toto hodnocení by rovněž mělo posuzovat dopad, účinnost a účelnost evropského rámce pro certifikaci kybernetické bezpečnosti. V případě přezkumu by Komise měla posoudit, jak je možno posílit úlohu agentury ENISA jako referenčního bodu pro poradenství a odborné znalosti, a měla by rovněž zhodnotit možnost uplatnění agentury ENISA při podpoře hodnocení produktů, služeb a procesů IKT třetích zemí, které nesplňují pravidla Unie.

([22]) Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

(109) Jelikož cílů tohoto nařízení nemůže být dosaženo uspokojivě členskými státy, ale spíše jich, z důvodu jejich rozsahu a účinků, 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 uvedených cílů.

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

PŘIJALY TOTO NAŘÍZENÍ:

HLAVA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět a oblast působnosti

1. Za účelem zajištění řádného fungování vnitřního trhu a současně s cílem dosáhnout v rámci Unie vysoké úrovně kybernetické bezpečnosti, kybernetické odolnosti a důvěry toto nařízení stanoví:

a) cíle, úkoly a organizační aspekty agentury ENISA – (Agentury Evropské unie pro kybernetickou bezpečnost); a

b) rámec pro zavedení evropského systému certifikace kybernetické bezpečnosti, jehož účelem je zajistit odpovídající úroveň kybernetické bezpečnosti produktů, služeb a procesů IKT v Unii a zabránit roztříštění vnitřního trhu, pokud jde o systémy certifikace kybernetické bezpečnosti v Unii.

Rámec uvedený v prvním pododstavci písm. b) se použije, aniž jsou dotčena zvláštní ustanovení v jiných právních aktech Unie týkající se dobrovolné nebo povinné certifikace.

2. Tímto nařízením nejsou dotčeny pravomoci členských států ohledně činností týkajících 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“ činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a dalších osob dotčených kybernetickými hrozbami;

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

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

4) „provozovatelem základních služeb“ provozovatel základních služeb ve smyslu čl. 4 bodu 4 směrnice (EU) 2016/1148;

5) „poskytovatelem digitálních služeb“ poskytovatel digitálních služeb ve smyslu čl. 4 bodu 6 směrnice (EU) 2016/1148;

6) „incidentem“ incident ve smyslu čl. 4 bodu 7 směrnice (EU) 2016/1148;

7) „řešením incidentu“ řešení incidentu ve smyslu čl. 4 bodu 8 směrnice (EU) 2016/1148;

8) „kybernetickou hrozbou“ jakákoliv potenciální okolnost, událost nebo čin, které mohou poškodit, narušit nebo jinak nepříznivě ovlivnit sítě a informační systémy, jejich uživatele a další osoby;

9) „evropským systémem certifikace kybernetické bezpečnosti“ komplexní soubor pravidel, technických požadavků, norem a postupů, které jsou stanoveny na úrovni Unie a které se uplatňují na certifikaci nebo posuzování shody určitých produktů, služeb a procesů IKT;

10) „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 posuzování shody produktů, služeb a procesů IKT spadajících do oblasti působnosti konkrétního systému;

11) „evropským certifikátem kybernetické bezpečnosti“ dokument vydaný příslušným orgánem a osvědčující, že byl hodnocen soulad daného produktu, služby nebo procesu IKT s konkrétními bezpečnostními požadavky stanovenými v evropském systému certifikace kybernetické bezpečnosti;

12) „produktem IKT“ prvek nebo skupina prvků sítě nebo informačního systému;

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

14) „procesem IKT“ soubor činností prováděných za účelem navrhování, vývoje, poskytování nebo údržby produktů nebo služeb IKT;

15) „akreditací“ akreditace ve smyslu čl. 2 bodu 10 nařízení (ES) č. 765/2008;

16) „vnitrostátním akreditačním orgánem“ vnitrostátní akreditační orgán ve smyslu čl. 2 bodu 11 nařízení (ES) č. 765/2008;

17) „posuzováním shody“ posuzování shody ve smyslu čl. 2 bodu 12 nařízení (ES) č. 765/2008;

18) „subjektem posuzování shody“ subjekt posuzování shody ve smyslu čl. 2 bodu 13 nařízení (ES) č. 765/2008;

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

20) „technickou specifikací“ dokument, který předepisuje technické požadavky, které má produkt, služba nebo proces IKT splňovat, nebo postup posuzování shody produktu, služby nebo procesu IKT;

21) „úrovní záruky“ podklad pro důvěru, že produkt, služba nebo proces IKT splňuje bezpečnostní požadavky konkrétního evropského systému certifikace kybernetické bezpečnosti, přičemž uvádí, na jakou úroveň bylo hodnocení produktu, služby nebo procesu IKT provedeno, avšak jako taková neměří bezpečnost dotyčného produktu, služby nebo procesu IKT.

22) „vlastním posuzováním shody“ úkon provedený výrobcem nebo poskytovatelem produktů, služeb či procesů IKT, jímž se vyhodnocuje, zda tyto produkty, služby či procesy IKT splňují požadavky konkrétního evropského systému certifikace kybernetické bezpečnosti.

HLAVA II

ENISA (AGENTURA EVROPSKÉ UNIE PRO KYBERNETICKOU BEZPEČNOST)

KAPITOLA I

Mandát a cíle

Článek 3

Mandát

1. Agentura ENISA plní úkoly, které jsou jí uloženy tímto nařízením za účelem dosažení vysoké společné úrovně kybernetické bezpečnosti v celé Unii, a to i aktivní podporou členských států, orgánů, institucí a jiných subjektů Unie, pokud jde o zlepšování kybernetické bezpečnosti. Agentura ENISA funguje jako referenční bod pro poradenství a odborné znalosti v oblasti kybernetické bezpečnosti pro orgány, instituce a jiné subjekty Unie, jakož i jiné zúčastněné strany Unie.

Agentura ENISA přispívá plněním úkolů, které jsou jí uloženy tímto nařízením, ke snížení roztříštěnosti vnitřního trhu.

2. Agentura ENISA plní úkoly, které jsou jí uloženy právními akty Unie, jež stanoví opatření pro sbližování právních a správních předpisů členských států týkajících se kybernetické bezpečnosti.

3. Agentura ENISA při plnění svých úkolů postupuje nezávisle, současně však předchází zdvojování činností členských států a zohledňuje již nabyté odborné znalosti členských států.

4. Agentura ENISA rozvíjí vlastní zdroje, včetně technických a lidských schopností a dovedností, které jsou nezbytné k plnění úkolů, které jsou jí uloženy tímto nařízením.

Článek 4

Cíle

1. Agentura ENISA 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 ENISA 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 ENISA 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 ENISA podporuje spolupráci, včetně sdílení informací a koordinace 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 ENISA přispívá ke zvyšování schopností v oblasti kybernetické bezpečnosti na úrovni Unie s cílem podporovat opatření členských států v oblasti předcházení kybernetickým hrozbám a reakce na ně, zejména v případě přeshraničních incidentů.

6. Agentura ENISA prosazuje využívání evropské certifikace kybernetické bezpečnosti, aby se zabránilo roztříštěnosti vnitřního trhu. S cílem zvýšit transparentnost kybernetické bezpečnosti produktů, služeb a procesů IKT, a posílit tak důvěru v digitální vnitřní trh a jeho konkurenceschopnost, přispívá agentura ENISA k zavedení a správě evropského rámce pro certifikaci kybernetické bezpečnosti v souladu s hlavou III tohoto nařízení.

7. Agentura ENISA prosazuje vysokou úroveň informovanosti o kybernetické bezpečnosti, včetně kybernetické hygieny a počítačové gramotnosti mezi občany, organizacemi a podniky.

KAPITOLA II

Úkoly

Článek 5

Tvorba a provádění politiky a práva Unie

Agentura ENISA 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 analýz 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 vydáváním stanovisek a pokynů a poskytováním 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) je nápomocna členským státům a orgánům, institucím a jiným subjektům Unie při tvorbě a prosazování politik kybernetické bezpečnosti v souvislosti se zachováním obecné dostupnosti nebo integrity veřejného jádra otevřeného internetu;

4) přispívá k činnosti skupiny pro spolupráci podle článku 11 směrnice (EU) 2016/1148 poskytováním svých odborných poznatků a pomoci;

5) podporuje:

   a) tvorbu a provádění politiky Unie v oblasti elektronické identity a služeb vytvářejících důvěru, zejména poskytováním poradenství a vydáváním technických pokynů, jakož i usnadňováním výměny osvědčených postupů mezi příslušnými orgány;

   b) prosazování vyšší úrovně bezpečnosti elektronických komunikací, mimo jiné poskytováním poradenství a odborných znalostí, jakož i usnadňováním výměny osvědčených postupů mezi příslušnými orgány;

   c) členské státy při provádění konkrétních aspektů kybernetické bezpečnosti v rámci politiky a práva Unie ve vztahu k ochraně údajů a soukromí a to též poskytováním poradenství Evropskému sboru pro ochranu osobních údajů na jeho žádost;

6) podporuje pravidelný přezkum činností v oblasti politiky Unie tím, že vypracovává výroční zprávu o stavu provádění příslušného právního rámce, pokud jde o:

   a) informace o hlášení členských států o incidentech, poskytnuté jednotnými kontaktními místy skupině pro spolupráci podle čl. 10 odst. 3 směrnice (EU) 2016/1148;

   b) shrnutí oznámení o narušení bezpečnosti nebo ztrátě integrity obdržených od poskytovatelů služeb vytvářejících důvěru, které agentuře ENISA poskytly orgány dohledu podle čl. 19 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([23]);

   c) oznámení o bezpečnostních incidentech předaných poskytovateli veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací, které agentuře ENISA poskytly příslušné orgány podle článku 40 směrnice (EU) 2018/1972.

([23]) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 73).

Článek 6

Budování kapacit

1. Agentura ENISA je nápomocna:

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

b) členským státům a orgánům, institucím a jiným subjektům Unie při dobrovolném vytváření a provádění politik zveřejňování zranitelností;

c) orgánům, institucím a jiným subjektům Unie v jejich úsilí zdokonalovat prevenci, odhalování a analýzu kybernetických hrozeb a incidentů a schopnost na tyto hrozby a incidenty reagovat, zejména tím, že poskytuje odpovídající podporu týmu CERT-EU;

d) členským státům na jejich žádost při budování vnitrostátních týmů CSIRT podle čl. 9 odst. 5 směrnice (EU) 2016/1148;

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

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

g) 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;

h) členským státům tím, že pravidelně a alespoň jednou za dva roky organizuje cvičení v oblasti kybernetické bezpečnosti na úrovni EU podle čl. 7 odst. 5 a na základě hodnocení těchto cvičení a poznatků z těchto cvičení předkládá politická doporučení;

i) příslušným veřejným orgánům tím, že jim nabízí školení v oblasti kybernetické bezpečnosti, a to případně ve spolupráci se zúčastněnými stranami;

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

2. Agentura ENISA 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 ENISA podporuje operativní spolupráci mezi členskými státy, orgány, institucemi a jinými subjekty Unie, jakož i mezi zúčastněnými stranami.

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

a) výměny know-how a osvědčených postupů;

b) poskytování poradenství a vydávání pokynů týkajících se příslušných otázek souvisejících s kybernetickou bezpečnostní;

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

3. Agentura ENISA zajišťuje služby sekretariátu sítě CSIRT podle čl. 12 odst. 2 směrnice (EU) 2016/1148 a v této funkci aktivně podporuje sdílení informací a spolupráci mezi jejími členy.

4. Agentura ENISA podporuje členské státy v operativní spolupráci v rámci sítě CSIRT tím, že:

a) poskytuje poradenství, jak zlepšit jejich schopnosti předcházet a odhalovat incidenty a reagovat na ně a na žádost jednoho nebo více členských států poskytuje poradenství v souvislosti s konkrétní kybernetickou hrozbou;

b) pomáhá na žádost jednoho nebo více členských států při posuzování incidentů, které mají závažný nebo významný dopad, a to poskytováním odborných znalostí a usnadňováním technického zpracování těchto incidentů, zejména prostřednictvím podpory dobrovolného sdílení příslušných informací a technických řešení mezi členskými státy;

c) analyzuje zranitelnosti a incidenty na základě veřejně dostupných informací nebo informací poskytnutých dobrovolně za tímto účelem členskými státy; a

d) na žádost jednoho nebo více členských států poskytuje podporu ve vztahu k následným technickým šetřením incidentů, které mají závažný či významný dopad ve smyslu směrnice (EU) 2016/1148.

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

5. Agentura ENISA pravidelně organizuje 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 v oblasti kybernetické bezpečnosti na úrovni Unie mohou zahrnovat technické, operativní či strategické prvky. Každé dva roky agentura ENISA uspořádá rozsáhlé komplexní cvičení.

Agentura ENISA případně rovněž přispívá spolu s příslušnými organizacemi, které se rovněž účastní cvičení v oblasti kybernetické bezpečnosti na úrovni Unie, k odvětvovým cvičením v oblasti kybernetické bezpečnosti a pomáhá je organizovat.

6. Agentura ENISA v úzké spolupráci s členskými státy vypracovává pravidelnou podrobnou technickou situační zprávu EU v oblasti kybernetické bezpečnosti týkající se incidentů a kybernetických hrozeb na základě veřejně dostupných informací, vlastní analýzy a zpráv, které s ní dobrovolně sdílejí mimo jiné týmy CSIRT členských států nebo jednotná kontaktní místa určená podle směrnice (EU) 2016/1148 nebo které jí poskytly Evropské centrum pro boj proti kyberkriminalitě (EC3) při Europolu a tým CERT-EU.

7. Agentura ENISA 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 a analyzuje zprávy z vnitrostátních zdrojů, jež jsou veřejně přístupné nebo dobrovolně sdílené, aby přispěla k vytvoření společného povědomí o situaci;

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

c) na žádost usnadňuje technické zpracování incidentů nebo krizí, zejména podporou dobrovolného sdílení technických řešení mezi členskými státy;

d) podporuje orgány, instituce a jiné subjekty Unie a na žádost i členské státy v komunikaci s veřejností ohledně těchto incidentů nebo krizí;

e) testuje plány spolupráce pro reakci na tyto incidenty nebo krize na úrovni Unie a na žádost podporuje členské státy v testování těchto plánů na vnitrostátní úrovni.

Článek 8

Trh, certifikace kybernetické bezpečnosti a normalizace

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

a) průběžně monitoruje vývoj v příslušných oblastech normalizace a doporučuje vhodné technické specifikace k použití při vypracovávání evropských systémů certifikace kybernetické bezpečnosti podle čl. 54 odst. 1 písm. c) v případech, kdy normy nejsou k dispozici;

b) vypracovává návrhy evropských systémů certifikace kybernetické bezpečnosti (dále jen „návrhy systémů“) pro produkty, služby a procesy IKT v souladu s článkem 49;

c) vyhodnocuje přijaté evropské systémy certifikace kybernetické bezpečnosti v souladu s čl. 49 odst. 8.

d) se účastní vzájemných hodnocení podle čl. 59 odst. 4;

e) je nápomocna Komisi při zajišťování služeb sekretariátu pro Evropskou skupinu pro certifikaci kybernetické bezpečnosti podle čl. 62 odst. 5.

2. Agentura ENISA zajišťuje služby sekretariátu pro Skupinu zúčastněných stran pro certifikaci kybernetické bezpečnosti podle čl. 22 odst. 4.

3. Agentura ENISA ve spolupráci s vnitrostátními orgány certifikace kybernetické bezpečnosti a průmyslovým odvětvím oficiálním, strukturovaným a transparentním způsobem sestavuje a zveřejňuje pokyny a vypracovává osvědčené postupy, týkající se požadavků na kybernetickou bezpečnost produktů, služeb a procesů IKT.

4. Agentura ENISA přispívá k budování kapacit souvisejících s hodnotícími a certifikačními procesy tím, že sestavuje a vydává pokyny a poskytuje členským státům na jejich žádost podporu.

5. Agentura ENISA usnadňuje stanovení a zavádění evropských a mezinárodních norem pro řízení rizik a pro bezpečnost produktů, služeb a procesů IKT.

6. Agentura ENISA ve spolupráci s členskými státy a průmyslovým odvětvím vydává podle čl. 19 odst. 2 směrnice (EU) 2016/1148 doporučení a pokyny týkající se technických oblastí souvisejících s bezpečnostními požadavky pro provozovatele základních služeb a poskytovatele digitálních služeb, jakož i již existujících norem, včetně vnitrostátních norem členských států.

7. Agentura ENISA 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

Poznatky a informace

Agentura ENISA:

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 hrozeb a incidentů za účelem odhalení nových trendů a pomoci při předcházení incidentům;

c) ve spolupráci s odborníky z orgánů členských států a zúčastněných stran 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 zmíněné směrnice;

d) prostřednictvím specializovaného portálu shromažďuje, uspořádává a zpřístupňuje veřejnosti informace o kybernetické bezpečnosti poskytnuté orgány, institucemi a jinými subjekty Unie a dobrovolně poskytnuté členskými státy a zúčastněnými stranami z veřejného i soukromého sektoru;

e) shromažďuje a analyzuje veřejně dostupné informace o významných incidentech a sestavuje zprávy s cílem poskytnout pokyny občanům, organizacím a podnikům v celé Unii.

Článek 10

Zvyšování informovanosti a vzdělávání

Agentura ENISA:

a) zvyšuje informovanost veřejnosti ohledně kybernetických bezpečnostních rizik a poskytuje pokyny týkající se osvědčených postupů pro jednotlivé uživatele zaměřené na občany, organizace a podniky, včetně kybernetické hygieny a počítačové gramotnosti;

b) ve spolupráci s členskými státy, orgány, institucemi a jinými subjekty Unie a průmyslovým odvětvím organizuje pravidelné informační kampaně za účelem zvýšení kybernetické bezpečnosti a jejího zviditelnění v Unii a podněcuje veřejnou rozpravu;

c) pomáhá členským státům v jejich úsilí o zvyšování informovanosti o kybernetické bezpečnosti a prosazování vzdělávání v oblasti kybernetické bezpečnosti;

d) podporuje užší koordinaci a výměnu osvědčených postupů mezi členskými státy v souvislosti s informovaností a vzděláváním v oblasti kybernetické bezpečnosti.

Článek 11

Výzkum a inovace

Ve vztahu k výzkumu a inovacím agentura ENISA:

a) poskytuje orgánům, institucím a jiným subjektům Unie 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 kybernetické hrozby, a to i pokud jde o nové a nově vznikající informační a komunikační technologie, a efektivně využívat technologie pro prevenci rizik;

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

c) přispívá ke strategickému programu pro výzkum a inovace na úrovni Unie v oblasti kybernetické bezpečnosti.

Článek 12

Mezinárodní spolupráce

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

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

b) na žádost Komise usnadňuje výměnu osvědčených postupů;

c) na žádost Komise jí poskytuje odborné znalosti;

d) poskytuje Komisi poradenství a podporu v otázkách týkajících se dohod se třetími zeměmi o vzájemném uznávání certifikátů kybernetické bezpečnosti, a to ve spolupráci s Evropskou skupinou pro certifikaci kybernetické bezpečnosti zřízenou podle článku 62.

KAPITOLA III

Organizace agentury ENISA

Článek 13

Struktura agentury ENISA

Správní a řídicí strukturu agentury ENISA tvoří:

a) správní rada;

b) výkonná rada;

c) výkonný ředitel;

d) poradní skupina agentury ENISA;

e) síť národních styčných úředníků.

Oddíl 1

Správní rada

Článek 14

Složení správní rady

1. Správní rada se skládá z jednoho člena jmenovaného každým členským státem a dvou členů jmenovaných Komisí. Všichni členové mají hlasovací právo.

2. Každý člen správní rady má náhradníka. Náhradník zastupuje daného člena v 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 správní rady. Komise a členské státy usilují o dosažení genderové vyváženosti ve správní radě.

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

Článek 15

Funkce správní rady

1. Správní rada:

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

b) přijímá návrh jednotného programového dokumentu agentury ENISA podle článku 24 před jeho předložením Komisi k vyjádření stanoviska;

c) s ohledem na stanovisko Komise přijímá jednotný programový dokument agentury ENISA;

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

e) přijímá roční rozpočet agentury ENISA a vykonává další funkce ve vztahu k rozpočtu agentury ENISA podle kapitoly IV;

f) posuzuje a přijímá souhrnnou výroční zprávu o činnosti agentury ENISA obsahující účetní výkaz a popis toho, jak agentura ENISA naplnila své ukazatele výkonnosti, do 1. července následujícího roku zprávu a její posouzení zasílá Evropskému parlamentu, Radě, Komisi a Účetnímu dvoru, a výroční zprávu zveřejňuje;

g) přijímá finanční pravidla použitelná na agenturu ENISA v souladu s článkem 32;

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

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

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

k) přijímá svůj jednací řád včetně pravidel pro prozatímní rozhodnutí o přenesení pravomocí k provádění zvláštních úkolů podle čl. 19 odst. 7;

l) v souladu s odstavcem 2 tohoto článku vykonává ve vztahu k zaměstnancům agentury ENISA pravomoci, které služební řád úředníků a pracovní řád ostatních zaměstnanců Evropské unie, jak jsou stanoveny v nařízení Rady (EHS, Euratom, ESUO) č. 259/68 ([24]), svěřují orgánu oprávněnému ke jmenování a orgánu oprávněnému uzavírat pracovní smlouvy (dále jen „pravomoci orgánu oprávněného ke jmenování“);

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

n) jmenuje výkonného ředitele a případně prodlužuje jeho funkční období nebo jej odvolává z funkce v souladu s článkem 36;

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

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

q) povoluje zavádění pracovní ujednání, pokud jde o článek 7;

r) povoluje zavádění nebo uzavírání pracovních ujednání v souladu s článkem 42.

2. Správní rada přijme v souladu s článkem 110 služebního řádu úředníků rozhodnutí na základě čl. 2 odst. 1 služebního řádu úředníků 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 může přenést tyto pravomoci na další osoby.

([24]) Úř. věst. L 56, 4.3.1968, s. 1.

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

Článek 16

Předseda správní rady

Správní rada si dvoutřetinovou většinou hlasů svých členů zvolí z řad svých členů předsedu a místopředsedu. Jejich funkční období je čtyři roky a lze je 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 17

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 účastní výkonný ředitel, avšak nemá hlasovací právo.

4. Zasedání správní rady se na pozvání předsedy mohou účastnit členové poradní skupiny agentury ENISA, avšak nemají hlasovací právo.

5. Členům správní rady a jejich náhradníkům mohou být s výhradou pravidel stanovených jednacím řádem na zasedáních správní rady nápomocni poradci nebo odborníci.

6. Služby sekretariátu pro správní radu zajišťuje agentura ENISA.

Článek 18

Pravidla hlasování ve správní radě

1. Správní rada přijímá rozhodnutí 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 členů správní rady.

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

4. Předseda správní rady 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 19

Výkonná rada

1. Správní radě je nápomocna výkonná rada.

2. Výkonná rada:

a) připravuje rozhodnutí přijímaná správní radou;

b) společně se správní radou zajišťuje vhodná následná opatření na základě zjištění a doporučení vyplývající z vyšetřování OLAF a z různých interních či externích auditních zpráv a hodnocení;

c) aniž jsou dotčeny povinnosti výkonného ředitele stanovené v článku 20, je nápomocna výkonnému řediteli a radí mu, pokud jde o provádění rozhodnutí správní rady v administrativních a rozpočtových záležitostech podle článku 20.

3. Výkonná rada se skládá z pěti členů. Členové výkonné rady jsou jmenování z řad členů správní rady. Jedním z členů je předseda správní rady, který smí předsedat i výkonné radě, a dalším je jeden ze zástupců Komise. Při jmenováních členů výkonné rady se usiluje zajištění genderové vyváženosti. Výkonný ředitel se účastní zasedání výkonné rady, avšak nemá hlasovací právo.

4. Funkční období členů výkonné rady je čtyři roky. Toto období lze prodloužit.

5. Zasedání výkonné rady se koná alespoň jednou za tři měsíce. Předseda výkonné rady svolává další zasedání na žádost členů této rady.

6. Správní rada stanoví jednací řád výkonné rady.

7. Je-li to z naléhavých důvodů nezbytné, může výkonná rada přijímat některá prozatímní rozhodnutí jménem správní rady, zejména ve věcech správního řízení, včetně pozastavení přenesení pravomocí orgánu oprávněného ke jmenování, a v rozpočtových záležitostech. Taková prozatímní rozhodnutí se bez zbytečného prodlení oznámí správní radě. Správní rada prozatímní rozhodnutí schválí, nebo zamítne do tří měsíců od přijetí daného rozhodnutí. Výkonná rada nepřijme jménem správní rady žádná rozhodnutí, která vyžadují schválení dvoutřetinovou většinou hlasů členů správní rady.

Oddíl 3

Výkonný ředitel

Článek 20

Povinnosti výkonného ředitele

1. Agenturu ENISA řídí výkonný ředitel, který je při výkonu svých povinností nezávislý. Výkonný ředitel se zodpovídá správní radě.

2. Výkonný ředitel předkládá Evropskému parlamentu na jeho výzvu 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 ENISA;

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 ENISA, včetně provádění jejího 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 vyšetřování OLAF, a předložení zprávy o pokroku Komisi dvakrát ročně a pravidelně správní radě;

h) vypracování návrhu finančních pravidel použitelných na agenturu ENISA podle článku 32;

i) vypracování návrhu odhadu příjmů a výdajů agentury ENISA 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 ENISA pro boj proti podvodům a její předložení správní radě ke schválení;

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

m) pravidelnou výměnu názorů a informací s orgány, institucemi a jinými subjekty Unie o jejich činnosti týkající se kybernetické bezpečnosti, aby byla zajištěna soudržnost při vývoji a provádění politiky Unie;

n) provádění jiných úkolů, které jsou výkonnému řediteli uloženy tímto nařízením.

4. Výkonný ředitel může v případě potřeby a v souladu s cíli a úkoly agentury ENISA zřizovat ad hoc pracovní skupiny složené z odborníků, mimo jiné z odborníků příslušných orgánů členských států. Výkonný ředitel o tom v předstihu 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 ENISA.

5. Je-li to nezbytné, může výkonný ředitel za účelem účinného a efektivního plnění úkolů agentury ENISA 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 dotčených členských států, včetně členského státu, v němž se nachází sídlo agentury ENISA, 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. Celkový počet zaměstnanců ve všech místních úřadech musí být omezen na minimum a nepřekročí 40 % celkového počtu zaměstnanců agentury ENISA umístěných v členském státě, v němž se nachází její sídlo. Počet zaměstnanců v každém místním úřadu nepřekročí 10 % celkového počtu zaměstnanců agentury ENISA umístěných v členském státě, v němž se nachází její sídlo.

Rozhodnutí o zřízení místního úřadu určí rozsah činností, jež mají být v daném místním úřadu prováděny, způsobem, který zabrání zbytečným nákladům a zdvojování správních funkcí agentury ENISA.

Oddíl 4

Poradní skupina agentury enisa, skupina zúčastněných stran pro certifikaci kybernetické bezpečnosti a síť národních styčných úředníků

Článek 21

Poradní skupina agentury ENISA

1. Správní rada na návrh výkonného ředitele zřídí transparentním způsobem poradní skupinu agentury ENISA složenou z uznávaných odborníků zastupujících příslušné zúčastněné strany, jako jsou odvětví informačních a komunikačních technologií, poskytovatelé veřejně dostupných sítí nebo služeb elektronických komunikací, malé a střední podniky, provozovatelé základních služeb, organizace spotřebitelů, akademičtí odborníci v oblasti kybernetické bezpečnosti a zástupci příslušných orgánů oznámených v souladu se směrnicí (EU) 2018/1972, evropských normalizačních organizací, jakož i donucovacích orgánů a orgánů dozoru pro ochranu údajů. Správní rada usiluje o zajištění patřičné genderové a zeměpisné vyváženosti a o zajištění vyváženého zastoupení různých skupin zúčastněných stran.

2. Postupy týkající se poradní skupiny agentury ENISA, zejména jejího složení, návrhu výkonného ředitele podle odstavce 1, počtu a jmenování jejích členů a činnosti poradní skupiny agentury ENISA jsou stanoveny ve vnitřních organizačních předpisech agentury ENISA a jsou zveřejňovány.

3. Poradní skupině agentury ENISA předsedá výkonný ředitel nebo osoba, kterou výkonný ředitel pro danou záležitost určí.

4. Funkční období členů poradní skupiny agentury ENISA je dva a půl roku. Členy poradní skupiny agentury ENISA nesmějí být členové správní rady. Odborníci z řad Komise a členských států jsou oprávněni účastnit se zasedání a podílet se na činnosti poradní skupiny agentury ENISA. K účasti na zasedáních a na činnosti poradní skupiny agentury ENISA mohou být přizváni zástupci dalších subjektů, kteří nejsou členy poradní skupiny agentury ENISA a jejichž účast považuje výkonný ředitel za důležitou.

5. Poradní skupina agentury ENISA poskytuje agentuře ENISA poradenství ohledně plnění jejích úkolů, s výjimkou případů, kdy se použijí ustanovení hlavy III tohoto nařízení. Poskytuje poradenství zejména výkonnému řediteli při vypracovávání návrhu ročního pracovního programu agentury ENISA a při zajišťování komunikace s příslušnými zúčastněnými stranami v otázkách souvisejících s ročním pracovním programem.

6. Poradní skupina agentury ENISA o své činnosti pravidelně informuje správní radu.

Článek 22

Skupina zúčastněných stran pro certifikaci kybernetické bezpečnosti

1. Zřizuje se Skupina zúčastněných stran pro certifikaci kybernetické bezpečnosti.

2. Členové Skupiny zúčastněných stran pro certifikaci kybernetické bezpečnosti jsou vybráni z řad uznávaných odborníků zastupujících příslušné zúčastněné strany. Tyto členy vybírá Komise na návrh agentury ENISA prostřednictvím transparentní a otevřené výzvy, přičemž zajišťuje vyvážené zastoupení různých skupin zúčastněných stran a patřičnou genderovou a zeměpisnou vyváženost.

3. Skupina zúčastněných stran pro certifikaci kybernetické bezpečnosti:

a) poskytuje poradenství Komisi ohledně strategických otázek souvisejících s evropským rámcem pro certifikaci kybernetické bezpečnosti;

b) na požádání poskytuje poradenství agentuře ENISA ohledně obecných i strategických záležitostí souvisejících s úkoly agentury ENISA v oblasti trhu, certifikace kybernetické bezpečnosti a normalizace;

c) je nápomocna Komisi při přípravě průběžného pracovního programu Unie podle článku 47;

d) vydává stanovisko k průběžnému pracovnímu programu Unie v souladu s čl. 47 odst. 4; a

e) v naléhavých případech poskytuje poradenství Komisi a Evropské skupině pro certifikaci kybernetické bezpečnosti ohledně potřeby dodatečných systémů certifikace mimo rámec průběžného pracovního programu Unie, jak je uvedeno v článcích 47 a 48.

4. Skupině zúčastněných stran pro certifikaci kybernetické bezpečnosti předsedají společně zástupci Komise a agentury ENISA a její sekretariát zajišťuje agentura ENISA.

Článek 23

Síť národních styčných úředníků

1. Správní rada zřídí na návrh výkonného ředitele síť národních styčných úředníků složenou ze zástupců všech členských států (národních styčných úředníků). Každý členský stát jmenuje do sítě národních styčných úředníků jednoho zástupce. Zasedání sítě národních styčných úředníků se mohou konat v různých odborných formátech.

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

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

4. Národní styční úředníci úzce spolupracují se zástupcem svého členského státu ve správní radě, avšak samotná síť národních styčných úředníků nesmí zdvojovat práci správní rady ani jiného fóra Unie.

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

Oddíl 5

Činnost

Článek 24

Jednotný programový dokument

1. Agentura ENISA vykonává svou činnost v souladu s jednotným programovým dokumentem obsahujícím její roční a víceletý program, které obsahují všechny plánované aktivity.

2. Výkonný ředitel každý rok vypracuje návrh jednotného programového dokumentu, který obsahuje roční a víceletý program spolu s odpovídajícím plánem finančních a lidských zdrojů v souladu s článkem 32 nařízení Komise v přenesené pravomoci (EU) č. 1271/2013 ([25]), 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 konečné podoby po přijetí souhrnného rozpočtu Unie s konečnou platností a podle potřeby se upraví.

([25]) 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).

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

6. Je-li agentuře ENISA uložen 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 každoročně aktualizován. Strategický plán je aktualizován podle potřeby, a zejména je-li nutno zohlednit výsledek hodnocení uvedeného v článku 67.

Článek 25

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 se účastní činnosti ad hoc pracovních skupin, 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 ENISA ve svých vnitřních organizačních předpisech stanoví praktická opatření upravující pravidla týkající se prohlášení o zájmech podle odstavců 1 a 2.

Článek 26

Transparentnost

1. Agentura ENISA vykonává své činnosti s vysokou mírou transparentnosti a v souladu s článkem 28.

2. Agentura ENISA zajistí, aby veřejnost a všechny zainteresované strany měly k dispozici náležité, objektivní, spolehlivé a snadno dostupné informace, zejména pokud jde o výsledky její činnosti. Zveřejní rovněž prohlášení o zájmech učiněná v souladu s článkem 25.

3. Správní rada může na návrh výkonného ředitele zainteresovaným stranám umožnit, aby se účastnily projednání některých činností agentury ENISA jako pozorovatelé.

4. Agentura ENISA ve svých vnitřních organizačních předpisech stanoví praktická opatření pro provádění pravidel transparentnosti podle odstavců 1 a 2.

Článek 27

Důvěrnost

1. Aniž je dotčen článek 28, agentura ENISA 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 poradní skupiny agentury ENISA, externí odborníci účastnící se ad hoc pracovních skupin a zaměstnanci agentury ENISA, včetně úředníků dočasně přidělených členskými státy, jsou povinni i po skončení svých funkcí dodržovat požadavky na důvěrnost podle článku 339 Smlouvy o fungování EU.

3. Agentura ENISA 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 ENISA, správní rada rozhodne, že agentuře ENISA umožní zpracovávat utajované informace. Agentura ENISA v tomto případě po dohodě s útvary Komise přijme bezpečnostní pravidla, v nichž se uplatňují bezpečnostní zásady stanovené v rozhodnutích Komise (EU, Euratom) 2015/443 ([26]) a 2015/444 ([27]). Tato bezpečnostní pravidla musí zahrnovat ustanovení o výměně, zpracování a ukládání utajovaných informací.

Článek 28

Přístup k dokumentům

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

2. Správní rada přijme do 28. prosince 2019 prováděcí pravidla k nařízení (ES) č. 1049/2001.

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

KAPITOLA IV

Sestavování a skladba rozpočtu agentury ENISA

Článek 29

Sestavování rozpočtu agentury ENISA

1. Výkonný ředitel každý rok sestaví návrh odhadu příjmů a výdajů agentury ENISA 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 odhad příjmů a výdajů agentury ENISA pro následující rozpočtový rok.

3. Správní rada zašle každý rok do 31. ledna odhad, který je součástí návrhu jednotného programového dokumentu, Komisi a třetím zemím, s nimiž Unie uzavřela dohody podle čl. 42 odst. 2.

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

5. Evropský parlament a Rada schválí prostředky, které Unie poskytne jako příspěvek agentuře ENISA.

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

([26]) Rozhodnutí Komise (EU, Euratom) 2015/443 ze dne 13. března 2015 o bezpečnosti v Komisi (Úř. věst. L 72, 17.3.2015, s. 41).
([27]) 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).

7. Správní rada přijme rozpočet agentury ENISA spolu s jednotným programovým dokumentem. Rozpočet agentury ENISA nabývá konečné podoby po přijetí souhrnného rozpočtu Unie s konečnou platností. Správní rada rozpočet a jednotný programový dokument agentury ENISA podle potřeby upraví v souladu se souhrnným rozpočtem Unie.

Článek 30

Skladba rozpočtu agentury ENISA

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

a) příspěvek ze souhrnného rozpočtu Unie;

b) příjmy účelově vázané na konkrétní položky výdajů v souladu s finančními pravidly uvedenými v článku 32;

c) finanční prostředky Unie ve formě dohod o přiznání příspěvku nebo grantů ad hoc v souladu s jejími finančními pravidly uvedenými v článku 32 a ustanoveními příslušných nástrojů na podporu politik Unie;

d) příspěvky třetích zemí, které se podílejí na činnosti agentury ENISA na základě článku 42;

e) dobrovolné finanční či věcné příspěvky členských států.

Členské státy, které poskytují dobrovolné příspěvky podle prvního pododstavce písm. e), nesmí na základě tohoto příspěvku požadovat žádné zvláštní právo nebo službu.

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

Článek 31

Plnění rozpočtu agentury ENISA

1. Za plnění rozpočtu agentury ENISA je odpovědný výkonný ředitel.

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

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

4. Po obdržení připomínek Účetního dvora k předběžné účetní závěrce agentury ENISA podle článku 246 nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ([28]) vypracuje účetní agentury ENISA na vlastní odpovědnost konečnou účetní závěrku agentury ENISA a předloží ji správní radě k vyjádření.

5. Správní rada zaujme stanovisko ke konečné účetní závěrce agentury ENISA.

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

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

([28]) Nařízení Evropského parlamentu a Rady (EU, Euratom) 2018/1046 ze dne 18. července 2018, kterým se stanoví finanční pravidla pro souhrnný rozpočet Unie, mění nařízení (EU) č. 1296/2013, (EU) č. 1301/2013, (EU) č. 1303/2013, (EU) č. 1304/2013, (EU) č. 1309/2013, (EU) č. 1316/2013, (EU) č. 223/2014 a (EU) č. 283/2014 a rozhodnutí č. 541/2014/EU a zrušuje nařízení (EU, Euratom) č. 966/2012 (Úř. věst. L 193, 30.7.2018, s. 1).

8. Účetní agentury ENISA 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 agentury ENISA zveřejní do 15. listopadu roku N+1 konečnou účetní závěrku v *Úředním věstníku Evropské unie*.

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 hladký průběh udílení absolutoria za příslušný rozpočtový rok v souladu s čl. 261 odst. 3 nařízení (EU, Euratom) 2018/1046.

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

Článek 32

Finanční pravidla

Finanční pravidla platná pro agenturu ENISA přijme správní rada po konzultaci s Komisí. Tato pravidla se nesmějí odchýlit od nařízení v přenesené pravomoci (EU) č. 1271/2013, ledaže je toto odchýlení zvlášť vyžadováno pro provoz agentury ENISA a Komise udělila předem souhlas.

Článek 33

Boj proti podvodům

1. V zájmu usnadnění boje proti podvodům, korupci a jinému protiprávnímu jednání podle nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 ([29]) přistoupí agentura ENISA do 28. prosince 2019 k interinstitucionální dohodě ze dne 25. května 1999 mezi Evropským parlamentem, Radou Evropské unie a Komisí Evropských společenství o vnitřním vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) ([30]). Agentura ENISA přijme vhodná ustanovení vztahující se na všechny zaměstnance agentury podle vzoru stanoveného v příloze uvedené dohody.

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

3. OLAF může provádět vyšetřování, včetně kontrol a inspekcí na místě, v souladu s ustanoveními a postupy uvedenými v nařízení (EU, Euratom) č. 883/2013 a v nařízení Rady (Euratom, ES) č. 2185/96 ([31]) s cílem zjistit, zda v souvislosti s grantem nebo smlouvou financovanou ze strany agentury ENISA nedošlo k podvodu, korupci nebo jinému protiprávnímu jednání poškozujícímu finanční zájmy Unie.

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

([29]) 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).

([30]) Úř. věst. L 136, 31.5.1999, s. 15.

([31]) 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).

KAPITOLA V

Zaměstnanci

Článek 34

Obecná ustanovení

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

Článek 35

Výsady a imunita

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

Článek 36

Výkonný ředitel

1. Výkonný ředitel je zaměstnán jako dočasný zaměstnanec agentury ENISA 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 pracovní smlouvy s výkonným ředitelem je agentura ENISA zastoupena předsedou správní rady.

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

5. Funkční období výkonného ředitele je pět let. Před koncem tohoto období Komise provede posouzení výsledků výkonného ředitele a budoucích úkolů a výzev agentury ENISA.

6. Správní rada přijímá rozhodnutí o jmenování, prodloužení funkčního období nebo odvolání výkonného ředitele v souladu s čl. 18 odst. 2.

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

8. Správní rada informuje o svém záměru prodloužit funkční období výkonného ředitele Evropský parlament. Do tří měsíců před tímto prodloužením výkonný ředitel, je-li k tomu vyzván, vystoupí 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 jednající na návrh Komise.

Článek 37

Vyslaní národní odborníci a další pracovníci

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

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

KAPITOLA VI

Obecná ustanovení týkající se agentury ENISA

Článek 38

Právní status agentury ENISA

1. Agentura ENISA je subjektem Unie a má právní subjektivitu.

2. Agentura ENISA 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 ENISA zastupuje výkonný ředitel.

Článek 39

Odpovědnost agentury ENISA

1. Smluvní odpovědnost agentury ENISA 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 ENISA.

3. V případě mimosmluvní odpovědnosti nahradí agentura ENISA 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 škody podle odstavce 3.

5. Osobní odpovědnost zaměstnanců vůči agentuře ENISA se řídí odpovídajícími předpisy vztahujícími se na zaměstnance agentury ENISA.

Článek 40

Jazykový režim

1. Na agenturu ENISA se vztahuje nařízení Rady č. 1 ([32]). Členské státy a ostatní jimi určené subjekty se mohou na agenturu ENISA obracet a přijímat odpovědi v libovolném úředním jazyce orgánů Unie.

2. Překladatelské služby potřebné pro činnost agentury ENISA zajišťuje Překladatelské středisko pro instituce Evropské unie.

Článek 41

Ochrana osobních údajů

1. Zpracování osobních údajů agenturou ENISA se řídí nařízením (EU) 2018/1725.

2. Správní rada přijme prováděcí pravidla uvedená v čl. 45 odst. 3 nařízení (EU) 2018/1725. Správní rada může přijmout další opatření nezbytná pro uplatňování nařízení (EU) 2018/1725 ze strany agentury ENISA.

([32]) Nařízení č. 1 o užívání jazyků v Evropském hospodářském společenství (Úř. věst. 17, 6.10.1958, s. 385).

Článek 42

Spolupráce s třetími zeměmi a mezinárodními organizacemi

1. V rozsahu nezbytném pro dosažení cílů stanovených v tomto nařízení může agentura ENISA spolupracovat s příslušnými orgány třetích zemí nebo s mezinárodními organizacemi. Za tímto účelem může agentura ENISA s výhradou předchozího schválení Komisí zavést s orgány třetích zemí a s mezinárodními organizacemi pracovní ujednání. Z těchto pracovních ujednání nevyplývají pro Unii ani její členské státy žádné právní závazky.

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

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

Článek 43

Bezpečnostní pravidla týkající se ochrany citlivých neutajovaných informací a utajovaných informací

Po konzultaci s Komisí agentura ENISA přijme svá bezpečnostní pravidla uplatňující bezpečnostní zásady obsažené v bezpečnostních pravidlech Komise pro ochranu citlivých neutajovaných informací a utajovaných informací Evropské unie, jak jsou obsažena v rozhodnutích (EU, Euratom) 2015/443 a 2015/444. Bezpečnostní pravidla agentury ENISA zahrnují ustanovení o výměně, zpracování a uchovávání těchto informací.

Článek 44

Dohoda o sídle a provozní podmínky

1. Nezbytná ujednání související s umístěním agentury ENISA v hostitelském členském státě a s prostory, které má tento členský stát dát k dispozici, a zvláštní pravidla, která se v hostitelském členském státě vztahují na výkonného ředitele, členy správní rady, zaměstnance agentury ENISA a jejich rodinné příslušníky, se stanoví v dohodě o sídle mezi agenturou ENISA a hostitelským členským státem uzavřené poté, co k tomu správní rada udělí souhlas.

2. Hostitelský členský stát agentury ENISA poskytuje pro zajištění řádného fungování agentury ENISA nejlepší možné podmínky, přičemž bere v úvahu přístupnost lokality, existenci vhodných vzdělávacích zařízení pro děti zaměstnanců, patřičný přístup na pracovní trh, sociální zabezpečení a zdravotní péči pro děti i pro manžely a manželky zaměstnanců.

Článek 45

Správní kontrola

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

HLAVA III

RÁMEC PRO CERTIFIKACI KYBERNETICKÉ BEZPEČNOSTI

Článek 46

Evropský rámec pro certifikaci kybernetické bezpečnosti

1. Zřizuje se evropský rámec pro certifikaci kybernetické bezpečnosti s cílem zlepšit podmínky fungování vnitřního trhu tím, že dojde ke zvýšení úrovně kybernetické bezpečnosti v Unii a umožní harmonizovaný přístup k evropským systémům certifikace kybernetické bezpečnosti na úrovni Unie, a to s výhledem na vytvoření jednotného digitálního trhu s produkty, službami a procesy IKT.

2. Evropský rámec pro certifikaci kybernetické bezpečnosti poskytne mechanismus pro zřizování evropských systémů certifikace kybernetické bezpečnosti a pro osvědčení, že produkty, služby a procesy IKT hodnocené v souladu s takovými systémy splňují stanovené bezpečnostní požadavky, pokud jde o ochranu dostupnosti, autentičnosti, integrity nebo důvěrnosti uchovávaných, předávaných či zpracovávaných údajů nebo funkcí či služeb nabízených nebo přístupných prostřednictvím těchto produktů, služeb a procesů během celého jejich životního cyklu.

Článek 47

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti

1. Komise zveřejní průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (dále jen „průběžný pracovní program Unie"), který určí strategické priority pro budoucí evropské systémy certifikace kybernetické bezpečnosti.

2. Průběžný pracovní program Unie obsahuje zejména seznam produktů, služeb a procesů IKT či jejich kategorií, pro něž by mohlo být zařazení do oblasti působnosti evropského systému kybernetické bezpečnosti prospěšné.

3. Zařazení každého konkrétního produktu, služby a procesu IKT či jejich kategorií do průběžného pracovního programu Unie musí být podloženo jedním či více z následujících důvodů:

a) dostupnost a rozvoj vnitrostátních systémů certifikace kybernetické bezpečnosti vztahujících se na konkrétní kategorii produktů, služeb nebo procesů IKT, zejména pokud jde o riziko roztříštěnosti;

b) relevantní politika nebo právo Unie či členského státu;

c) tržní poptávka;

d) vývoj v oblasti kybernetických hrozeb;

e) žádost o vypracování konkrétního návrhu systému ze strany Evropské skupiny pro certifikaci kybernetické bezpečnosti.

4. Komise bere řádný zřetel ke stanoviskům vydaným k průběžnému pracovnímu programu Unie Evropskou skupinou pro certifikaci kybernetické bezpečnosti a Skupinou zúčastněných stran pro certifikaci kybernetické bezpečnosti.

5. První průběžný pracovní program Unie se zveřejní do 28. června 2020. Průběžný pracovní program Unie je aktualizován alespoň každé tři roky a v případě potřeby častěji.

Článek 48

Žádost o evropský systém certifikace kybernetické bezpečnosti

1. Komise může agenturu ENISA požádat o vypracování návrhu systému nebo o přezkum stávajícího evropského systému certifikace kybernetické bezpečnosti na základě průběžného pracovního programu Unie.

2. V řádně odůvodněných případech může Komise nebo Evropská skupina pro certifikaci kybernetické bezpečnosti požádat agenturu ENISA o vypracování návrhu systému nebo o přezkum stávajícího systému certifikace kybernetické bezpečnosti, jenž není zahrnut do průběžného pracovního programu Unie. Průběžný pracovní program Unie se patřičně aktualizuje.

Článek 49

Vypracování, přijetí a přezkum evropského systému certifikace kybernetické bezpečnosti

1. Agentura ENISA na základě žádosti Komise podle článku 48 vypracuje návrh systému, který splňuje požadavky stanovené v článcích 51, 52 a 54.

2. Agentura ENISA může na základě žádosti Evropské skupiny pro certifikaci kybernetické bezpečnosti podle čl. 48 odst. 2 vypracovat návrh systému, který splňuje požadavky stanovené v článcích 51, 52 a 54. Pokud agentura ENISA takovou žádost odmítne, poskytne k tomu odůvodnění. Každé rozhodnutí o odmítnutí žádosti přijímá správní rada.

3. Při vypracovávání návrhu systému agentura ENISA konzultuje všechny příslušné zúčastněné strany prostřednictvím formálních, otevřených, transparentních a inkluzivních konzultačních postupů.

4. Pro každý návrh systému agentura ENISA zřídí ad hoc pracovní skupinu v souladu s čl. 20 odst. 4, která agentuře ENISA poskytuje konkrétní poradenství a odborné poznatky.

5. Agentura ENISA úzce spolupracuje s Evropskou skupinou pro certifikaci kybernetické bezpečnosti. Skupina poskytuje agentuře ENISA v souvislosti s vypracováním návrhu systému pomoc a odborné poradenství a k návrhu systému přijímá stanovisko.

6. Agentura ENISA stanovisko Evropské skupiny pro certifikaci kybernetické bezpečnosti v co největší míře zohlední před předložením návrhu systému vypracovaného v souladu s odstavci 3, 4 a 5 Komisi. Stanovisko Evropské skupiny pro certifikaci kybernetické bezpečnosti není pro agenturu ENISA závazné a neexistence takového stanoviska agentuře ENISA nebrání, aby návrh systému předložila Komisi.

7. Na základě návrhu systému vypracovaného agenturou ENISA může Komise přijmout prováděcí akty, kterými stanoví evropský systém certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT, splňující požadavky stanovené v článcích 51, 52 a 54. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 66 odst. 2.

8. Alespoň jednou za pět let agentura ENISA vyhodnotí každý přijatý evropský systém certifikace kybernetické bezpečnosti, přičemž zohlední zpětnou vazbu poskytnutou zúčastněnými stranami. V případně potřeby mohou Komise nebo Evropská skupina pro certifikaci kybernetické bezpečnosti požádat agenturu ENISA, aby zahájila postup vypracování revidovaného návrhu systému v souladu s článkem 48 a tímto článkem.

Článek 50

Internetové stránky o evropských systémech certifikace kybernetické bezpečnosti

1. Agentura ENISA provozuje internetové stránky, jejichž účelem je poskytovat informace a zvyšovat veřejné povědomí o evropských systémech certifikace kybernetické bezpečnosti, evropských certifikátech kybernetické bezpečnosti a EU prohlášeních o shodě, včetně informací týkajících se evropských systémů certifikace kybernetické bezpečnosti, které již nejsou platné, evropských certifikátů kybernetické bezpečnosti a EU prohlášení o shodě, jež byly zrušeny nebo jejichž platnost skončila, a úložišť internetových odkazů na informace o kybernetické bezpečnosti poskytnuté v souladu s článkem 55.

2. V příslušných případech internetové stránky uvedené v odstavci 1 rovněž uvádějí ty vnitrostátní systémy certifikace kybernetické bezpečnosti, které byly nahrazeny evropským systémem certifikace kybernetické bezpečnosti.

Článek 51

Bezpečnostní cíle evropských systémů certifikace kybernetické bezpečnosti

Evropský systém certifikace kybernetické bezpečnosti je navržen tak, aby dle okolností dosáhl alespoň těchto bezpečnostních cílů:

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

b) chránit ukládané, předávané nebo jinak zpracovávané údaje proti náhodnému nebo neoprávněnému zničení, ztrátě nebo změně nebo proti nedostupnosti, a to během celého životního cyklu produktu, služby nebo procesu IKT;

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

d) identifikovat a zdokumentovat známé případy závislosti a známé zranitelnosti;

e) zaznamenat, které údaje, služby nebo funkce byly předmětem přístupu, použití nebo jiného zpracování, kdy k tomu došlo a kdo tak učinil;

f) zajistit, aby bylo možné kontrolovat, které údaje, služby nebo funkce byly předmětem přístupu, použití nebo jiného zpracování, kdy k tomu došlo a kdo tak učinil;

g) ověřit, že produkty, služby a procesy IKT neobsahují žádné známé zranitelnosti;

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

i) zajistit, aby produkty, služby a procesy IKT byly zabezpečeny na úrovni standardního nastavení a výchozího návrhu;

j) zajistit, aby byly produkty, služby a procesy IKT poskytovány s aktualizovaným softwarem a hardwarem, které neobsahují veřejně známé zranitelnosti, a aby obsahovaly mechanismy pro bezpečné aktualizace.

Článek 52

Úrovně záruky evropských systémů certifikace kybernetické bezpečnosti

1. Evropský systém certifikace kybernetické bezpečnosti může u produktů, služeb a procesů IKT určit jednu nebo více těchto úrovní záruky: „základní“, „významná“ nebo „vysoká“. Úroveň záruky je přiměřená úrovni rizika z hlediska pravděpodobnosti a dopadu incidentu, jež je spojeno se zamýšleným použitím produktu, služby nebo procesu IKT.

2. Evropské certifikáty kybernetické bezpečnosti a EU prohlášení o shodě odkazují na úroveň záruky uvedenou v evropském systému certifikace kybernetické bezpečnosti, v jehož rámci byly dotyčné evropské certifikáty kybernetické bezpečnosti nebo EU prohlášení o shodě vydány.

3. Evropský systém certifikace bezpečnosti stanoví bezpečnostní požadavky, které odpovídají každé úrovni záruky, včetně odpovídajících bezpečnostních funkcí a odpovídající náročnosti a podrobnosti hodnocení, kterým má produkt, služba nebo proces IKT projít.

4. Certifikát nebo EU prohlášení o shodě odkazují na technické specifikace, normy a procesy s nimi související, včetně technických kontrol, jejichž účelem je snížit riziko kybernetických bezpečnostních incidentů nebo jim předcházet.

5. Evropský certifikát kybernetické bezpečnosti nebo EU prohlášení o shodě, které odkazují na úroveň záruky „základní“, poskytují záruku, že produkty, služby a procesy IKT, pro něž jsou tento certifikát nebo toto EU prohlášení o shodě vydány, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcionalit a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat známá základní rizika incidentů a kybernetických útoků. Prováděné hodnotící činnosti zahrnují alespoň přezkum technické dokumentace. Pokud takový přezkum není vhodný, provedou se náhradní hodnotící činnosti s rovnocenným účinkem.

6. Evropský certifikát kybernetické bezpečnosti, který odkazuje na úroveň záruky „významná“, poskytuje záruku, že produkty, služby a procesy IKT, pro něž je tento certifikát vydán, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcionalit a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat známá kybernetická rizika a rizika incidentů a kybernetických útoků prováděných subjekty s omezenými dovednostmi a zdroji. Prováděné hodnotící činnosti zahrnují alespoň: přezkum s cílem prokázat neexistenci veřejně známých zranitelností a zkouška k prokázání toho, že produkty, procesy a služby IKT náležitě uplatňují nezbytné bezpečnostní funkcionality. Pokud některá z těchto hodnotících činností není vhodná, provedou se náhradní hodnotící činnosti s rovnocenným účinkem

7. Evropský certifikát kybernetické bezpečnosti, který odkazuje na úroveň záruky „vysoká“, poskytuje záruku, že produkty, služby a procesy IKT, pro něž je tento certifikát vydán, splňují odpovídající bezpečnostní požadavky včetně bezpečnostních funkcionalit a že byly vyhodnoceny na úrovni, jejímž cílem je minimalizovat rizika sofistikovaných kybernetických útoků prováděných subjekty s významnými dovednostmi a zdroji. Prováděné hodnotící činnosti zahrnují alespoň: přezkum s cílem prokázat neexistenci veřejně známých zranitelností; zkouška k prokázání toho, že produkty, procesy a služby IKT náležitě uplatňují nezbytné nejnovější bezpečnostní funkcionality; a posouzení jejich odolnosti vůči zručným útočníkům prostřednictvím zkoušky penetrace. Pokud některá z těchto hodnotících činností není vhodná, provedou se náhradní hodnotící činnosti s rovnocenným účinkem.

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

Článek 53

Vlastní posuzování shody

1. Evropský systém certifikace kybernetické bezpečnosti může umožnit vlastní posuzování shody pod výhradní odpovědností výrobce nebo poskytovatele produktů, služeb či procesů IKT. Vlastní posuzování shody je přípustné pouze u produktů, služeb a procesů IKT, které vykazují nízké riziko odpovídající úrovni záruky „základní“.

2. Výrobce nebo poskytovatel produktů, služeb či procesů IKT může vydat EU prohlášení o shodě uvádějící, že bylo prokázáno plnění požadavků stanovených v příslušném systému. Vydáním tohoto prohlášení výrobce produktů IKT nebo poskytovatel služeb či procesů IKT přebírá odpovědnost za soulad produktu, služby nebo procesu IKT s požadavky stanovenými v daném systému.

3. Výrobce nebo poskytovatel produktů, služeb či procesů IKT uchovává EU prohlášení o shodě, technickou dokumentaci a veškeré ostatní důležité informace souvisejících se shodou produktů nebo služeb IKT se systémem k dispozici vnitrostátního orgánu certifikace kybernetické bezpečnosti uvedeného v čl. 58 po dobu stanovenou v odpovídajícím evropském systému certifikace kybernetické bezpečnosti. Jedno vyhotovení EU prohlášení o shodě se předkládá vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a jedno vyhotovení agentuře ENISA.

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

5. EU prohlášení o shodě je uznáváno ve všech členských státech.

Článek 54

Prvky evropských systémů certifikace kybernetické bezpečnosti

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

a) předmět a oblast působnosti systému certifikace včetně druhu nebo kategorií zahrnutých produktů, služeb a procesů IKT;

b) jasný popis účelu systému spolu s jasným vysvětlením, jak zvolené normy, metody hodnocení a úrovně záruky odpovídají potřebám zamýšlených uživatelů systému;

c) odkazy na mezinárodní, evropské nebo vnitrostátní normy používané při hodnocení, nebo pokud takové normy nejsou k dispozici nebo nejsou vhodné, odkazy na technické specifikace, které splňují požadavky stanovené v příloze II nařízení (EU) č. 1025/2012, nebo pokud takové specifikace nejsou k dispozici, odkazy na technické specifikace nebo požadavky kybernetické bezpečnosti definované v evropském systému certifikace kybernetické bezpečnosti;

d) v příslušných případech jednu nebo více úrovní záruky;

e) informace o tom, zda je v rámci systému přípustné vlastní posuzování shody;

f) v příslušných případech konkrétní nebo dodatečné požadavky na subjekty posuzování shody, s cílem zajistit jejich technickou způsobilost k hodnocení požadavků na kybernetickou bezpečnost;

g) konkrétní kritéria a metody hodnocení používané k prokázání toho, že bylo dosaženo bezpečnostních cílů uvedených v článku 51, včetně typů těchto hodnocení;

h) v příslušných případech informace nezbytné pro certifikaci, které žadatel předkládá nebo jinak zpřístupňuje subjektům posuzování shody;

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

j) pravidla pro monitorování souladu produktů, služeb a procesů IKT s požadavky evropských certifikátů kybernetické bezpečnosti nebo EU prohlášení o shodě, včetně mechanismů prokázání pokračujícího plnění specifikovaných požadavků kybernetické bezpečnosti;

k) v příslušných případech podmínky pro vydání, zachování, pokračování platnosti a obnovení evropských certifikátů kybernetické bezpečnosti, jakož i podmínky pro rozšíření nebo omezení rozsahu certifikace;

l) pravidla upravující důsledky pro produkty, služby a procesy IKT, jež jsou certifikovány nebo pro něž bylo vydáno EU prohlášení o shodě, avšak nesplňují požadavky systému;

m) pravidla upravující způsob oznamování a řešení dříve nezjištěných zranitelností v kybernetické bezpečnosti produktů, služeb a procesů IKT;

n) v příslušných případech pravidla upravující uchovávání záznamů subjekty posuzování shody;

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

p) obsah a formát vydávaných evropských certifikátů kybernetické bezpečnosti a EU prohlášení o shodě;

q) dobu dostupnosti EU prohlášení o shodě, technické dokumentace a veškerých dalších důležitých informací, které má výrobce nebo poskytovatele produktů, služeb či procesů IKT mít k dispozici;

r) maximální dobu platnosti evropských certifikátů kybernetické bezpečnosti vydaných v rámci systému;

s) politiku zveřejňování evropských certifikátů kybernetické bezpečnosti vydaných, pozměněných nebo zrušených v rámci systému;

t) podmínky pro vzájemné uznávání systémů certifikace s třetími zeměmi;

u) v příslušných případech pravidla týkající se mechanismu vzájemného posouzení zřízeného v rámci systému pro orgány nebo subjekty vydávající evropské certifikáty kybernetické bezpečnosti pro úroveň záruky „vysoká“ podle čl. 56 odst. 6. Tímto mechanismem není dotčeno vzájemné hodnocení podle článku 59;

v) formát a postupy, jež výrobci a poskytovatelé produktů, služeb či procesů IKT musejí dodržovat při poskytování a aktualizaci doplňujících informací o kybernetické bezpečnosti podle článku 55.

2. Specifikované požadavky evropského systému certifikace kybernetické bezpečnosti musí být v souladu s příslušnými právními požadavky, zejména s požadavky plynoucími z harmonizovaných právních předpisů Unie.

3. Pokud tak konkrétní právní akt Unie stanoví, lze certifikát nebo EU prohlášení o shodě vydané v rámci evropského systému certifikace kybernetické bezpečnosti použít k prokázání předpokladu shody s požadavky daného právního 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 55

Doplňující informace o kybernetické bezpečnosti týkající se certifikovaných produktů, služeb a procesů IKT

1. Výrobce nebo poskytovatel certifikovaných produktů, služeb či procesů IKT nebo produktů, služeb či procesů IKT, pro něž bylo vydáno EU prohlášení o shodě, zpřístupní veřejnosti tyto doplňující informace o kybernetické bezpečnosti:

a) pokyny a doporučení, jež koncovým uživatelům usnadní bezpečné nastavení, instalaci, uvedení do provozu, provoz samotný a údržbu produktů či služeb IKT;

b) období, během něhož bude koncovým uživatelům k dispozici bezpečnostní podpora, zejména pokud jde o dostupnost aktualizací souvisejících s kybernetickou bezpečností;

c) kontaktní údaje výrobce či poskytovatele a akceptované metody pro příjem informací o zranitelnostech ze strany koncových uživatelů nebo výzkumných pracovníků v oblasti bezpečnosti;

d) odkaz na internetová úložiště zveřejněných zranitelností souvisejících s produktem, službou či procesem IKT a na jakákoli relevantní upozornění v oblasti kybernetické bezpečnosti.

2. Informace uvedené v odstavci 1 se poskytují v elektronické podobě, přičemž zůstávají k dispozici a jsou podle potřeby aktualizovány přinejmenším do pozbytí platnosti odpovídajícího evropského certifikátu kybernetické bezpečnosti nebo EU prohlášení o shodě.

Článek 56

Certifikace kybernetické bezpečnosti

1. U produktů, služeb a procesů IKT, které byly certifikovány v rámci evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 49, se předpokládá, že splňují požadavky daného systému.

2. Certifikace kybernetické bezpečnosti je dobrovolná, nestanoví-li unijní nebo vnitrostátní právo jinak.

3. Komise pravidelně hodnotí účinnost a využití přijatých evropských systémů certifikace kybernetické bezpečnosti, přičemž rovněž posuzuje, zda by se určitý evropský systém certifikace kybernetické bezpečnosti měl na základě příslušných právních předpisů Unie stát povinným v zájmu zajištění patřičné úrovně kybernetické bezpečnosti produktů, služeb a procesů IKT v Unii a v zájmu zlepšení fungování vnitřního trhu. První takové hodnocení proběhne do 31. prosince 2023 a následná hodnocení se poté uskuteční alespoň každé dva roky. Na základě výsledku těchto hodnocení Komise z produktů, služeb a procesů IKT, na něž se již vztahuje stávající systém certifikace, určí ty, na něž by se měl vztahovat povinný systém certifikace.

Komise se prioritně zaměří na odvětví uvedená v příloze II směrnice (EU) 2016/1148, jež podrobí hodnocení do dvou let od přijetí prvního evropského systému certifikace kybernetické bezpečnosti.

V rámci přípravy hodnocení Komise:

a) zohlední dopad opatření na výrobce nebo poskytovatele daných produktů, služeb či procesů IKT a na uživatele z hlediska nákladů na tato opatření a společenských nebo hospodářských přínosů plynoucích z očekávaného zvýšení úrovně bezpečnosti pro dotyčné produkty, služby a procesy IKT;

b) bere zřetel na existenci příslušných právních předpisů členských států a třetích zemí a na jejich provádění;

c) uplatňuje otevřený, transparentní a inkluzivní proces konzultací se všemi relevantními zúčastněnými stranami a s členskými státy;

d) zohlední prováděcí lhůty, přechodná opatření nebo přechodná období, zejména se zřetelem na možný dopad daného opatření na výrobce nebo poskytovatele produktů, služeb či procesů IKT, včetně malých a středních podniků;

e) navrhne nejrychlejší a nejúčinnější způsob provedení přechodu od dobrovolných systémů certifikace k systémům povinným.

4. Subjekty posuzování shody uvedené v článku 60 vydávají evropské certifikáty kybernetické bezpečnosti podle tohoto článku, které odkazují na úrovně záruky „základní“ nebo „významná“, na základě kritérií obsažených v evropském systému certifikace kybernetické bezpečnosti přijatém Komisí podle článku 49.

5. Odchylně od odstavce 4 může evropský systém certifikace kybernetické bezpečnosti v řádně odůvodněných případech stanovit, že evropské certifikáty kybernetické bezpečnosti vyplývající z daného systému mohou vydávat pouze veřejné subjekty. Tímto subjektem je:

a) vnitrostátní orgán certifikace kybernetické bezpečnosti uvedený v čl. 58 odst. 1; nebo

b) veřejný subjekt, který je akreditován jako subjekt posuzování shody podle čl. 60 odst. 1;

6. Pokud evropský systém certifikace kybernetické bezpečnosti přijatý podle článku 49 požaduje úroveň záruky „vysoká“, může evropský certifikát kybernetické bezpečnosti v rámci tohoto systému vydat pouze vnitrostátní orgán certifikace kybernetické bezpečnosti, nebo v následujících případech subjekt posuzování shody:

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

b) na základě obecného pověření subjektu posuzování shody úkolem vydávat evropské certifikáty kybernetické bezpečnosti u ze strany vnitrostátního orgánu certifikace kybernetické bezpečnosti.

7. Fyzická nebo právnická osoba, která předkládá produkty, služby nebo procesy IKT k certifikaci, zpřístupní vnitrostátnímu orgánu certifikace kybernetické bezpečnosti podle článku 58, pokud je tento orgán subjektem vydávajícím evropský certifikát kybernetické bezpečnosti, nebo subjektu posuzování shody uvedenému v článku 60 veškeré informace nezbytné pro provedení certifikace.

8. Držitel evropského certifikátu kybernetické bezpečnosti informuje orgán či subjekt uvedený v odstavci 7 o veškerých později zjištěných zranitelnostech nebo nesrovnalostech týkajících se bezpečnosti certifikovaného produktu, služby nebo procesu IKT, které by mohly mít dopad na jejich souladu s požadavky souvisejícími s certifikací. Tento orgán či subjekt neprodleně tyto informace postoupí příslušnému vnitrostátnímu orgánu certifikace kybernetické bezpečnosti.

9. Evropský certifikát kybernetické bezpečnosti se vydává na dobu určenou evropským systémem certifikace kybernetické bezpečnosti a může být obnoven, budou-li nadále plněny příslušné požadavky.

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

Článek 57

Vnitrostátní systémy certifikace kybernetické bezpečnosti a certifikáty

1. Aniž je dotčen odstavec 3 tohoto článku, vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty, služby a procesy IKT zahrnuté do evropského systému certifikace kybernetické bezpečnosti pozbývají účinnosti ode dne stanoveného v prováděcím aktu přijatém podle čl. 49 odst. 7. Vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty, služby a procesy IKT, na něž se evropský systém certifikace kybernetické bezpečnosti nevztahuje, zůstávají v platnosti.

2. Členské státy nezavedou nové vnitrostátní systémy certifikace kybernetické bezpečnosti pro produkty, služby a procesy IKT, které jsou již 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.

4. Aby se zabránilo roztříštěnosti vnitřního trhu, vyrozumí členské státy Komisi a Evropskou skupinu pro certifikaci kybernetické bezpečnosti o každém záměru vypracovat nové vnitrostátní systémy certifikace kybernetické bezpečnosti.

Článek 58

Vnitrostátní orgány certifikace kybernetické bezpečnosti

1. Každý členský stát určí jeden nebo více vnitrostátních orgánů certifikace kybernetické bezpečnosti na svém území, nebo se souhlasem jiného členského státu určí jeden nebo více vnitrostátních orgánů certifikace kybernetické bezpečnosti zřízených v tomto jiném členském státě, které budou v určujícím členském státě odpovídat za dozor.

2. Každý členský stát informuje Komisi o určených vnitrostátních orgánech certifikace kybernetické bezpečnosti. Členský stát, jenž určí více než jeden orgán, informuje Komisi rovněž o úkolech, které byly každému z nich přiděleny.

3. Aniž je dotčen čl. 56 odst. 5 písm. a) a odst. 6, je každý vnitrostátní orgán certifikace kybernetické bezpečnosti ve své organizaci, finančních rozhodnutích, právní struktuře a rozhodovacím procesu nezávislý na subjektech, nad nimiž vykonává dohled.

4. Členské státy zajistí, aby činnosti vnitrostátního orgánu certifikace kybernetické bezpečnosti související s vydáváním evropských certifikátů kybernetické bezpečnosti podle čl. 56 odst. 5 písm. a) a odst. 6 byly striktně odděleny od činnosti dohledu podle tohoto článku a aby obě činnosti byly vykonávány na sobě nezávisle.

5. Členské státy zajistí, aby vnitrostátní orgány certifikace kybernetické bezpečnosti měly odpovídající zdroje pro výkon svých pravomocí a pro efektivní a účinné provádění svých úkolů.

6. Za účelem efektivního provádění tohoto nařízení je vhodné, aby se vnitrostátní orgány certifikace kybernetické bezpečnosti aktivním, efektivním, účinným a bezpečným způsobem podílely na činnosti Evropské skupiny pro certifikaci kybernetické bezpečnosti.

7. Vnitrostátní orgány certifikace kybernetické bezpečnosti:

a) dohlížejí na pravidla zahrnutá v evropských systémech certifikace kybernetické bezpečnosti podle čl. 54 odst. 1 písm. j) pro monitorování souladu produktů, procesů, služeb a procesů IKT s požadavky evropských certifikátů kybernetické bezpečnosti, jež byly vydány na území jejich států, a dodržování těchto pravidel vymáhají, přičemž spolupracují s dalšími příslušnými orgány dohledu nad trhem;

b) sledují dodržování povinností výrobců a poskytovatelů produktů, služeb nebo procesů IKT, kteří jsou usazeni na území jejich států a kteří provádějí vlastní posuzování shody, zejména pak povinností těchto výrobců a poskytovatelů stanovených v čl. 53 odst. 2 a 3 a v odpovídajícím evropském systému certifikace kybernetické bezpečnosti, a dodržování těchto povinností vymáhají;

c) aniž je dotčen čl. 60 odst. 3, pro účely tohoto nařízení aktivně napomáhají vnitrostátním subjektům akreditace při monitorování činnosti subjektů posuzování shody a při dozoru nad touto činností a poskytují uvedeným subjektům akreditace podporu;

d) sledují činnost veřejných subjektů uvedených v čl. 56 odst. 5 a dohlížejí na tyto aktivity;

e) v příslušných případech autorizují subjekty posuzování shody podle čl. 60 odst. 3 a omezují, pozastavují nebo odebírají stávající autorizaci, pokud subjekty posuzování shody porušují požadavky tohoto nařízení;

f) řeší stížnosti podané fyzickými nebo právnickými osobami v souvislosti s evropskými certifikáty kybernetické bezpečnosti vydanými vnitrostátními orgány certifikace kybernetické bezpečnosti či subjekty posuzování shody v souladu s čl. 56 odst. 6 nebo v souvislosti s EU prohlášeními o shodě vydanými podle článku 53, v přiměřeném rozsahu šetří předmět těchto stížností a v přiměřené lhůtě informují stěžovatele o průběhu a výsledku šetření;

g) každoročně předkládají agentuře ENISA a Evropské skupině pro certifikaci kybernetické bezpečnosti souhrnnou zprávu o činnostech uskutečněných podle písmen b), c) a d) tohoto odstavce nebo podle odstavce 8;

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

i) sledují příslušný vývoj v oblasti certifikace kybernetické bezpečnosti.

8. Každý vnitrostátní orgán certifikace kybernetické bezpečnosti má alespoň tyto pravomoci:

a) požadovat po subjektech posuzování shody, držitelích evropských certifikátů kybernetické bezpečnosti a vydavatelích EU prohlášení o shodě, aby poskytovali veškeré informace, které orgán potřebuje pro plnění svých úkolů;

b) za účelem ověření souladu s touto hlavou provádět šetření v podobě auditů u subjektů posuzování shody, držitelů evropských certifikátů kybernetické bezpečnosti a vydavatelů EU prohlášení o shodě;

c) v souladu s vnitrostátním právem přijímat vhodná opatření k zajištění toho, aby subjekty posuzování shody, držitelé evropských certifikátů kybernetické bezpečnosti a vydavatelé EU prohlášení o shodě dodržovali toto nařízení nebo některý evropský systém certifikace kybernetické bezpečnosti;

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

e) odebrat v souladu s vnitrostátním právem evropské certifikáty kybernetické bezpečnosti vydané vnitrostátními orgány certifikace kybernetické bezpečnosti nebo subjekty posuzování shody v souladu s čl. 56 odst. 6, pokud tyto certifikáty nejsou v souladu s tímto nařízením nebo s některým evropským systémem certifikace kybernetické bezpečnosti;

f) v souladu s vnitrostátním právem ukládat sankce podle článku 65 a požadovat okamžité zastavení porušování povinností stanovených v tomto nařízení.

9. 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 v oblasti kybernetické bezpečnosti, produktů, služeb a procesů IKT.

Článek 59

Vzájemné hodnocení

1. V zájmu dosažení rovnocenných norem v celé Unii, pokud jde o evropské certifikáty kybernetické bezpečnosti a EU prohlášení o shodě, podléhají vnitrostátní orgány certifikace kybernetické bezpečnosti vzájemnému hodnocení.

2. Vzájemné hodnocení se provádí na základě řádných a transparentních hodnotících kritérií a postupů, zejména pokud jde o požadavky na strukturu, lidské zdroje a o procedurální otázky, otázky důvěrnosti a stížnosti.

3. Vzájemné hodnocení posuzuje:

a) zda jsou v příslušných případech činnosti vnitrostátních orgánů certifikace kybernetické bezpečnosti související s vydáváním evropských certifikátů kybernetické bezpečnosti podle čl. 56 odst. 5 písm. a) a odst. 6 striktně odděleny od jejich činnosti dozoru podle článku 58 a zda jsou obě činnosti vykonávány na sobě nezávisle;

b) postupy dohledu nad pravidly pro monitorování souladu produktů, služeb a procesů IKT s evropskými certifikáty kybernetické bezpečnosti a vymáhání těchto pravidel, v souladu čl. 58 odst. 7 písm. a);

c) postupy pro sledování povinností výrobců a poskytovatelů produktů, služeb a procesů IKT a vymáhání těchto povinností, v souladu s čl. 58 odst. 7 písm. b);

d) postupy pro sledování a autorizaci činností subjektů posuzování shody a pro dohled nad nimi;

e) zda mají v příslušných případech zaměstnanci orgánů nebo subjektů, které vydávají osvědčení pro úroveň záruky „vysoká“ podle čl. 56 čl. 6, vhodnou odbornost.

4. Vzájemné hodnocení provádějí přinejmenším dva vnitrostátní orgány certifikace kybernetické bezpečnosti jiných členských států a Komise, a to přinejmenším jednou za pět let. Vzájemného hodnocení se může zúčastnit agentura ENISA.

5. Komise může přijímat prováděcí akty, jimiž stanoví plán vzájemného hodnocení na dobu nejméně pěti let, který stanoví kritéria týkající se složení týmu provádějícího vzájemné hodnocení, metodiku používanou pro vzájemné hodnocení, harmonogram, periodicitu a další úkoly související se vzájemným hodnocením. Při přijímání těchto prováděcích aktů Komise řádně zohlední názor Evropské skupiny pro certifikaci kybernetické bezpečnosti. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 66 odst. 2.

6. Výsledky vzájemných hodnocení přezkoumá Evropská skupina pro certifikaci kybernetické bezpečnosti a vypracuje shrnutí, jež mohou být zpřístupněna veřejnosti, přičemž v případě potřeby vydá pokyny či doporučení týkající se kroků či opatření, které by měly dotčené subjekty uskutečnit.

Článek 60

Subjekty posuzování shody

1. Subjekty posuzování shody jsou akreditovány vnitrostátními akreditačními orgány stanovenými podle nařízení (ES) č. 765/2008. Akreditace se vydá, pouze pokud subjekt posuzování shody splňuje požadavky stanovené v příloze tohoto nařízení.

2. Je-li evropský certifikát kybernetické bezpečnosti vydán vnitrostátním orgánem certifikace kybernetické bezpečnosti podle čl. 56 odst. 5 písm. a) a odst. 6, certifikační subjekt daného vnitrostátního orgánu certifikace kybernetické bezpečnosti musí být akreditován jako subjekt posuzování shody podle odstavce 1 tohoto článku.

3. Stanoví-li evropské systémy certifikace kybernetické bezpečnosti konkrétní nebo dodatečné požadavky podle čl. 54 odst. 1 písm. f), jsou k vykonávání úkolů v rámci těchto systémů vnitrostátním orgánem certifikace kybernetické bezpečnosti autorizovány pouze ty subjekty posuzování shody, které uvedené požadavky splňují.

4. Akreditace uvedená v odstavci 1se vydává subjektům posuzování shody na období nejvýše pěti let a lze ji za stejných podmínek obnovit, pokud daný subjekt posuzování shody stále splňuje požadavky stanovené v tomto článku. Vnitrostátní akreditační orgány přijmou v přiměřené lhůtě veškerá odpovídající opatření s cílem omezit, pozastavit nebo zrušit akreditaci subjektu posuzování shody vydanou podle odstavce 1, pokud podmínky pro udělení akreditace nebyly nebo již nejsou splněny nebo subjekt posuzování shody porušuje toto nařízení.

Článek 61

Oznámení

1. Ke každému evropskému systému certifikace kybernetické bezpečnosti vnitrostátní orgány certifikace kybernetické bezpečnosti oznámí Komisi subjekty posuzování shody akreditované a případně autorizované podle čl. 60 odst. 3 k vydávání evropských certifikátů kybernetické bezpečnosti s určenými úrovněmi záruky podle článku 52. Vnitrostátní orgány certifikace kybernetické bezpečnosti oznámí Komisi bez zbytečného prodlení jakékoliv jejich následné změny.

2. Do jednoho roku po vstupu evropského systému certifikace kybernetické bezpečnosti v platnost Komise zveřejní seznam subjektů posuzování shody oznámených pro daný systém v *Úředním věstníku Evropské unie*.

3. Obdrží-li Komise oznámení po uplynutí lhůty uvedené v odstavci 2, zveřejní změny v seznamu oznámených subjektů posuzování shody 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 tímto orgánem ze seznamu uvedeného v odstavci 2. Komise zveřejní odpovídající změny seznamu do jednoho měsíce ode dne přijetí žádosti vnitrostátního orgánu certifikace kybernetické bezpečnosti v *Úředním věstníku Evropské unie*.

5. Komise může přijmout prováděcí akty, jimiž stanoví okolnosti, formáty a postupy pro oznámení podle odstavce 1 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 66 odst. 2.

Článek 62

Evropská skupina pro certifikaci kybernetické bezpečnosti

1. Zřizuje se Evropská skupina pro certifikaci kybernetické bezpečnosti.

2. Evropská skupina pro certifikaci kybernetické bezpečnosti se skládá ze zástupců vnitrostátních orgánů certifikace kybernetické bezpečnosti nebo zástupců jiných příslušných vnitrostátních orgánů. Žádný člen Evropské skupiny pro certifikaci kybernetické bezpečnosti nesmí zastupovat více než dva členské státy.

3. Zúčastněné strany a relevantní třetí strany mohou být pozvány k účasti na zasedáních Evropské skupiny pro certifikaci kybernetické bezpečnosti a na její činnosti.

4. Evropská skupina pro certifikaci kybernetické bezpečnosti 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 průběžný pracovní program Unie, 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 podle článku 49;

c) přijmout stanovisko k návrhu systému vypracovanému agenturou ENISA podle článku 49;

d) požadovat po agentuře ENISA, aby vypracovala návrh systému v souladu s čl. 48 odst. 2;

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

f) zkoumat relevantní vývoj v oblasti certifikace kybernetické bezpečnosti a sdílet informace a osvědčené postupy týkající se systémů certifikace kybernetické bezpečnosti;

g) usnadňovat prostřednictvím budování kapacit a výměny informací spolupráci mezi vnitrostátními orgány certifikace kybernetické bezpečnosti podle této hlavy, zejména stanovením metod pro účinnou výměnu informací o veškerých otázkách týkajících se certifikace kybernetické bezpečnosti;

h) podporovat provádění mechanismu vzájemného hodnocení v souladu s pravidly stanovenými v evropském systému certifikace kybernetické bezpečnosti podle čl. 54 odst. 1 písm. u)

i) usnadňovat sbližování evropských systémů kybernetické bezpečnosti s mezinárodně uznávanými normami, a to i přezkumem stávajících evropských systémů certifikace kybernetické bezpečnosti a případně podáváním doporučení agentuře ENISA, aby navázala dialog s příslušnými mezinárodními normalizačními organizacemi s cílem společně řešit nedostatky nebo mezery v dostupných mezinárodně uznávaných normách.

5. Evropské skupině pro certifikaci kybernetické bezpečnosti předsedá Komise, s pomocí agentury ENISA, a Komise jí podle čl. 8 odst. 1) písm. e) zajišťuje služby sekretariátu.

Článek 63

Právo podat stížnost

1. Fyzické a právnické osoby mají právo podat stížnost u vydavatele evropského certifikátu kybernetické bezpečnosti, nebo týká-li se stížnost evropského certifikátu kybernetické bezpečnosti vydaného subjektem posuzování shody jednajícím podle čl. 56 odst. 6, u příslušného vnitrostátního orgánu certifikace kybernetické bezpečnosti.

2. Orgán nebo subjekt, u něhož byla stížnost podána, informuje stěžovatele o pokroku v řešení stížnosti a o přijatém rozhodnutí, jakož i o jeho právu využít soudního prostředku nápravy podle článku 64.

Článek 64

Právo na účinný soudní prostředek nápravy

1. Bez ohledu na jakékoli správní nebo jiné mimosoudní opravné prostředky mají fyzické i právnické osoby právo na účinný soudní prostředek nápravy, pokud jde o:

a) rozhodnutí orgánu nebo subjektu uvedeného v čl. 63 odst. 1, a to i pokud jde o případné chybné vydání či nečinnost ve vztahu k vydání nebo uznání evropského certifikátu kybernetické bezpečnosti, jehož jsou tyto fyzické či právnické osoby držiteli;

b) nečinnost v řešení stížnosti podané u orgánu nebo subjektu uvedeného v čl. 63 odst. 1.

2. Řízení podle tohoto článku se zahajuje u soudu členského státu, v němž se nachází orgán nebo subjekt, vůči kterému soudní prostředek nápravy směřuje.

Článek 65

Sankce

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

HLAVA IV

ZÁVĚREČNÁ USTANOVENÍ

Článek 66

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 67

Hodnocení a přezkum

1. Do 28. června 2024 a poté každých pět let Komise vyhodnotí dopad, efektivitu a účinnost agentury ENISA a jejích pracovních postupů, jakož i případnou potřebu změnit mandát agentury ENISA a finanční důsledky této změny. Hodnocení zohledňuje zpětnou vazbu, kterou agentura ENISA v reakci na svou činnost zaznamenala. Pokud se Komise domnívá, že pokračující fungování agentury ENISA již není s ohledem na cíle, mandát a úkoly, které jí byly uděleny, odůvodněné, může navrhnout, aby byla ustanovení tohoto nařízení týkající se agentury ENISA změněna.

2. Hodnocení rovněž posoudí dopad, efektivnost a účinnost ustanovení hlavy III tohoto nařízení s ohledem na cíle zajištění odpovídající úrovně kybernetické bezpečnosti produktů, služeb a procesů a v Unii a zlepšení fungování vnitřního trhu.

3. Hodnocení posoudí, zda jsou základní požadavky na kybernetickou bezpečnost pro přístup na vnitřní trh nezbytné k tomu, aby se zabránilo produktům, službám a procesům IKT, které nesplňují hlavní požadavky na kybernetickou bezpečnost, vstupovat na trh Unie.

4. Do 28. června 2024 a poté každých pět let předá Komise zprávu o hodnocení společně se svými závěry Evropskému parlamentu, Radě a správní radě. Zjištění této zprávy se zveřejní.

Článek 68

Zrušení a nástupnictví

1. Nařízení (EU) č. 526/2013 se zrušuje s účinkem od 27. června 2019.

2. Odkazy na nařízení (EU) č. 526/2013 a na agenturu ENISA zřízenou uvedeným nařízením se považují za odkazy na toto rozhodnutí a agenturu ENISA zřízenou tímto nařízením.

3. Agentura ENISA zřízená tímto nařízením je nástupkyní agentury ENISA zřízené nařízením (EU) č. 526/2013, pokud jde o veškeré vlastnictví, dohody, právní závazky, pracovní smlouvy, finanční závazky a odpovědnost. Všechna rozhodnutí správní a výkonné rady přijatá v souladu s nařízením (EU) č. 526/2013 zůstávají v platnosti, jsou-li v souladu s tímto nařízením.

4. Agentura ENISA se zřizuje na dobu neurčitou od 27. června 2019.

5. Výkonný ředitel jmenovaný podle čl. 24 odst. 4 nařízení (EU) č. 526/2013 zůstává ve funkci a vykonává povinnosti výkonného ředitele, jak jsou uvedeny v článku 20 tohoto nařízení, po zbývající část svého funkčního období. Ostatní podmínky jeho smlouvy se nemění.

6. Členové správní rady a jejich náhradníci jmenovaní podle článku 6 nařízení (EU) č. 526/2013 zůstávají ve funkci a vykonávají pravomoci správní rady, jak jsou uvedeny v článku 15 tohoto nařízení, po zbývající část svého funkčního období.

Článek 69

Vstup v platnost

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

2. Články 58, 60, 61, 63, 64 a 65 se použijí od 28. června 2021.

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

Ve Štrasburku dne 17. dubna 2019.

Za Evropský parlament	*Za Radu*
předseda	*předseda*
A. TAJANI	G. CIAMBA

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, službě či procesu 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, služeb nebo procesů IKT, které tento subjekt posuzuje, pokud je prokázána jeho nezávislost a neexistence jakéhokoli střetu zájmů.

4. Subjekty posuzování shody, jejich nejvyšší vedení a osoby odpovědné za plnění úkolů posuzování shody nesmí být osobami, které navrhují, vyrábějí, dodávají, instalují, nakupují, vlastní, používají nebo udržují posuzovaný produkt, službu či proces IKT, ani zplnomocněnými zástupci jakékoli z těchto stran. Tento zákaz nevylučuje používání posuzovaných produktů IKT, které jsou nezbytné pro činnost subjektu posuzování shody, ani používání takových produktů IKT k osobním účelům.

5. Subjekty posuzování shody, jejich nejvyšší vedení a osoby odpovědné za plnění úkolů posuzování shody se nesmí přímo podílet na navrhování, výrobě nebo konstrukci, uvádění na trh, instalaci, používání ani údržbě posuzovaných produktů, služeb či procesů IKT, ani nesmí zastupovat strany, které se těmito činnostmi zabývají. Subjekty posuzování shody, jejich nejvyšší vedení a osoby odpovědné za plnění úkolů posuzování shody nesmí vykonávat žádnou činnost, která by mohla ohrozit jejich nezávislý úsudek nebo důvěryhodnost ve vztahu k jejich činnostem posuzování shody. Tento zákaz platí zejména pro poradenské služby.

6. Je-li subjekt posuzování shody vlastněn nebo provozován veřejným subjektem nebo institucí, musí být zajištěna a zdokumentována nezávislost a neexistence jakéhokoli střetu zájmů mezi vnitrostátním orgánem certifikace kybernetické bezpečnosti a subjektem posuzování shody.

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

8. Subjekty posuzování shody a jejich zaměstnanci 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.

9. 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. Veškeré subdodávky nebo konzultace s externími pracovníky musí být řádně zdokumentovány, nesmějí zahrnovat žádné zprostředkovatele a podléhají písemné dohodě týkající se mimo jiné důvěrnosti a střetu zájmů. Dotyčný subjekt posuzování shody nese plnou odpovědnost za vykonávané úkoly.

10. Subjekt posuzování shody musí mít k dispozici vždy, pro každý postup posuzování shody a pro každý druh, kategorii nebo podkategorii produktů, služeb a procesů IKT potřebné:

    a) zaměstnance 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 subjekt oznámený podle článku 61, a dalšími činnostmi;

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

11. 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.

12. Osoby odpovědné za plnění úkolů posuzování 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 shody, 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 a zprávy prokazující provedení posuzování shody.

13. Musí být zaručena nestrannost subjektů posuzování shody, jejich nejvyššího vedení, osob odpovědných za plnění úkolů posuzování shody a jakýchkoli subdodavatelů.

14. Odměňování nejvyššího vedení a osob odpovědných za plnění úkolů posuzování shody nesmí záviset na počtu provedených posuzování shody ani na výsledcích těchto posuzování.

15. Subjekty posuzování shody uzavřou pojištění odpovědnosti za škodu, ledaže tuto odpovědnost převzal členský stát v souladu se svým vnitrostátním právem, nebo je za posuzování shody přímo odpovědný sám členský stát.

16. Subjekt posuzování shody a jeho zaměstnanci, výbory, dceřiné společnosti, subdodavatelé a jakýkoli přidružený subjekt nebo zaměstnanci externích orgánů subjektu posuzování shody jsou povinni zachovávat mlčenlivost a profesní tajemství, pokud jde o veškeré informace, které obdrželi při plnění svých úkolů posuzování shody podle tohoto nařízení nebo podle jakéhokoli ustanovení vnitrostátních právních předpisů, kterým se toto nařízení provádí, s výjimkou případů, kdy zveřejnění vyžadují právní předpisy Unie nebo členských států, které se na tyto osoby vztahují, a s výjimkou styku s příslušnými orgány členských států, v nichž vykonávají svou činnost. Práva duševního vlastnictví jsou chráněna. Pokud jde o požadavky tohoto bodu, subjekt posuzování shody musí mít zavedené zdokumentované postupy.

17. S výjimkou bodu 16 požadavky této přílohy nebrání výměně technických informací a regulačních pokynů mezi subjektem posuzování shody a osobou, která podává žádost o certifikaci nebo toto podání zvažuje.

18. Pokud jde o poplatky, subjekty posuzování shody působí v souladu se souborem důsledných, spravedlivých a přiměřených podmínek s přihlédnutím k zájmům malých a středních podniků.

19. Subjekty posuzování shody plní požadavky příslušné normy, která je harmonizována podle nařízení (ES) č. 765/2008 pro akreditaci subjektů posuzování shody provádějící certifikaci produktů, služeb nebo procesů IKT.

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