NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2019/881

zo 17. apríla 2019

o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru ([1]),

so zreteľom na stanovisko Výboru regiónov ([2]),

konajúc v súlade s riadnym legislatívnym postupom ([3]),

keďže:

(1) Siete a informačné systémy a elektronické komunikačné siete a služby sú pre spoločnosť kľúčové a stali sa oporným pilierom hospodárskeho rastu. Na informačných a komunikačných technológiách (ďalej len „IKT“) sú založené komplexné systémy, ktoré podporujú každodenné činnosti spoločnosti, udržujú chod kľúčových odvetví hospodárstva, ako je zdravotníctvo, energetika, financie či doprava, a najmä podporujú fungovanie vnútorného trhu.

(2) Občania, organizácie a podniky v Únii dnes využívajú siete a informačné systémy na každom kroku. Digitalizácia a pripojiteľnosť sa stávajú základnými vlastnosťami čoraz väčšieho množstva produktov a služieb, pričom sa očakáva, že s nástupom internetu vecí (ďalej len „IoT“ – Internet of Things) sa v Únii bude v najbližšom desaťročí využívať mimoriadne vysoký počet pripojených digitálnych zariadení. Na internet je pripojených čoraz viac zariadení, no ich bezpečnosť a odolnosť nie je do nich dostatočne zabudovaná už vo fáze ich návrhu, čo vedie k nedostatočnej kybernetickej bezpečnosti. Certifikácia sa využíva obmedzene, čo v tejto situácii vedie k tomu, že užívatelia z radov jednotlivcov, organizácií a podnikov nie sú dostatočne informovaní o prvkoch kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT, čo znižuje dôveru v digitálne riešenia. Siete a informačné systémy sú schopné podporovať všetky aspekty nášho života a poháňať hospodársky rast Únie. Sú základným kameňom pre dosiahnutie jednotného digitálneho trhu.

(3) Rastúca digitalizácia a pripojiteľnosť zvyšujú kybernetickobezpečnostné riziká, takže spoločnosť ako celok sa stáva zraniteľnejšou z hľadiska kybernetických hrozieb a zvyšuje sa nebezpečenstvo, ktorému čelia fyzické osoby, vrátane zraniteľných osôb, ako sú napríklad deti. V záujme zmiernenia uvedených rizík treba prijať všetky potrebné kroky na zvýšenie kybernetickej bezpečnosti v Únii, aby boli siete a informačné systémy, komunikačné siete, digitálne produkty, služby a zariadenia, ktoré využívajú občania, organizácie i podniky – od malých a stredných podnikov (ďalej len „MSP“) v zmysle vymedzenia v odporúčaní Komisie 2003/361/ES ([4]), až po prevádzkovateľov kritických infraštruktúr lepšie chránené pred kybernetickými hrozbami.

([1]) Ú. v. EÚ C 227, 28.6.2018, s. 86.
([2]) Ú. v. EÚ C 176, 23.5.2018, s. 29.
([3]) Pozícia Európskeho parlamentu z 12. marca 2019 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 9. apríla 2019.
([4]) Odporúčanie Komisie zo 6. mája 2003 o definícii mikropodnikov, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003, s. 36).

(4) Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ďalej len „ENISA“) zriadená nariadením Európskeho parlamentu a Rady (EÚ) č. 526/2013 ([5]) sprístupňuje verejnosti relevantné informácie, čím prispieva k rozvoju odvetvia kybernetickej bezpečnosti v Únii, najmä MSP a startupov. Agentúra ENISA by sa mala usilovať o užšiu spoluprácu s univerzitami a výskumnými subjektmi, aby prispela k znižovaniu závislosti od kybernetickobezpečnostných produktov a služieb z krajín mimo Únie a k posilňovaniu dodávateľských reťazcov v Únii.

(5) Kybernetické útoky sú na vzostupe a prepojené hospodárstvo a spoločnosť, ktoré sú zraniteľnejšie z hľadiska kybernetických hrozieb a útokov, si vyžadujú silnejšiu obranu. Kybernetické útoky sú často cezhraničné, ale právomoc a politická reakcia orgánov zodpovedných za kybernetickú bezpečnosť a presadzovanie práva majú prevažne vnútroštátnu povahu. Rozsiahle incidenty by mohli narušiť poskytovanie základných služieb v celej Únii. To si vyžaduje účinné a koordinované reakcie a krízové riadenie na úrovni Únie, ktoré vychádzajú z osobitných politík a všeobecnejších nástrojov pre európsku solidaritu a vzájomnú pomoc. Okrem toho je pre tvorcov politík, priemysel a používateľov dôležité pravidelné posudzovanie stavu kybernetickej bezpečnosti a odolnosti v Únii založené na spoľahlivých údajoch Únie, ako aj systematických predpovediach budúceho vývoja, výziev a hrozieb na úrovni Únie aj celosvetovo.

(6) Keďže výzvy, ktorým Únia čelí v oblasti kybernetickej bezpečnosti, sa stupňujú, je potrebný komplexný súbor opatrení, ktorými by sa nadviazalo na predošlé kroky Únie a ktorými by sa podporil synergický účinok cieľov. Uvedené ciele zahŕňajú aj ďalšie posilňovanie spôsobilosti a pripravenosti členských štátov a podnikov, ako aj zlepšovanie spolupráce, výmeny informácií a koordinácie medzi členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie. Okrem toho, keďže kybernetické hrozby nepoznajú hranice, treba posilniť spôsobilosť na úrovni Únie, ktorá by doplnila opatrenia členských štátov, najmä pri rozsiahlych cezhraničných incidentoch a krízach, a zároveň zohľadniť dôležitosť zachovania a ďalšieho posilnenia vnútroštátnej spôsobilosti reagovať na kybernetické hrozby akýchkoľvek rozmerov.

(7) Väčšie úsilie je potrebné vyvinúť aj v oblasti informovanosti občanov, organizácií a podnikov o otázkach kybernetickej bezpečnosti. Navyše, vzhľadom na to, že incidenty oslabujú dôveru v poskytovateľov digitálnych služieb a v samotný jednotný digitálny trh, najmä medzi spotrebiteľmi, dôvera by sa mala ešte posilniť transparentným poskytovaním informácií o úrovni bezpečnosti produktov IKT, služieb IKT a procesov IKT, ktoré by malo zdôrazňovať, že dokonca ani vysoká úroveň certifikácie kybernetickej bezpečnosti nezaručuje, že produkt IKT, služba IKT alebo proces IKT sú absolútne bezpečné. Zvýšenie dôvery môže uľahčiť celoúnijná certifikácia, ktorou sa zabezpečia spoločné požiadavky kybernetickej bezpečnosti a hodnotiace kritériá naprieč vnútroštátnymi trhmi a odvetviami.

(8) Kybernetická bezpečnosť nie je len otázkou technológie, ale rovnako dôležité je aj správanie ľudí. Mala by sa preto významne podporovať tzv. kybernetická hygiena, konkrétne jednoduché rutinné opatrenia, ktoré minimalizujú vystavenie sa rizikám kybernetických hrozieb, ak ich občania, organizácie a podniky vykonávajú pravidelne.

(9) Pre účely posilnenia kybernetickobezpečnostných štruktúr Únie je dôležité udržiavať a rozvíjať spôsobilosť členských štátov s cieľom komplexne reagovať na kybernetické hrozby vrátane cezhraničných incidentov.

(10) Podniky a jednotliví spotrebitelia by mali mať presné informácie o stupni dôveryhodnosti, na aký bola certifikovaná bezpečnosť ich produktov IKT, služieb IKT a procesov IKT. Zároveň žiadny produkt nie je úplne kyberneticky bezpečný a treba podporovať a uprednostňovať základné pravidlá kybernetickej hygieny. Vzhľadom na rastúcu dostupnosť zariadení IoT je k dispozícii viacero dobrovoľných opatrení, ktoré môže súkromný sektor prijať na posilnenie dôvery v bezpečnosť produktov IKT, služieb IKT a procesov IKT.

(11) Moderné produkty a systémy IKT často obsahujú jednu alebo viaceré technológie a komponenty tretích strán, ako napríklad softvérové moduly, knižnice alebo aplikačné programovacie rozhrania, a často sú na ne odkázané. Táto odkázanosť, ktorá sa nazýva „závislosť“, by mohla predstavovať dodatočné kybernetickobezpečnostné riziká, keďže zraniteľnosti komponentov tretích strán by mohli mať vplyv aj na bezpečnosť produktov IKT, služieb IKT a procesov IKT. Určenie a zdokumentovanie takýchto závislostí v mnohých prípadoch umožňuje koncovým užívateľom produktov IKT, služieb IKT a procesov IKT zlepšiť ich činnosť v oblasti riadenia kybernetickobezpečnostných rizík, napríklad tým, že zlepšia riadenie zraniteľnosti užívateľov v oblasti kybernetickej bezpečnosti a nápravné postupy.

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

(12) Organizácie, výrobcovia alebo poskytovatelia podieľajúci sa na navrhovaní a vývoji produktov IKT, služieb IKT a procesov IKT by sa mali nabádať na uplatňovanie opatrení počas čo najskorších etáp navrhovania a vývoja, aby sa bezpečnosť týchto produktov, služieb a procesov chránila v najvyššej možnej miere takým spôsobom, že výskyt kybernetických útokov sa bude predpokladať a ich následky sa budú očakávať a minimalizovať („bezpečnosť už v štádiu návrhu“). Bezpečnosť by mala byť zabezpečená počas celej životnosti produktu IKT, služby IKT a procesu IKT prostredníctvom procesov navrhovania a vývoja, ktoré sa neustále vyvíjajú, aby znížili riziko škody spôsobenej zámerným zneužitím.

(13) Podniky, organizácie a verejný sektor by mali nastaviť produkty IKT, služby IKT alebo procesy IKT, ktoré navrhujú, tak, aby zaistili vyšší stupeň bezpečnosti, ktorým by sa malo umožniť, že ich prvý užívateľ dostane v rámci predvolenej konfigurácie čo najbezpečnejšie nastavenia („bezpečnosť ako štandard“), čím sa zníži zaťaženie užívateľov musieť si produkt IKT, službu IKT alebo proces IKT správne nastaviť. Bezpečnosť ako štandard by si nemala vyžadovať rozsiahle nastavovanie ani osobitné technické znalosti alebo neintuitívne správanie zo strany užívateľa a mala by pri používaní ľahko a spoľahlivo fungovať. Ak sa analýzou rizík a použiteľnosti v konkrétnych prípadoch preukáže, že takéto štandardné nastavenie nie je možné, užívatelia by mali byť vyzvaní, aby sa rozhodli pre najbezpečnejšie nastavenie.

(14) Nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 ([6]) zriadilo agentúru ENISA so zámerom prispieť k cieľom v oblasti zabezpečenia vysokej a účinnej úrovne sieťovej a informačnej bezpečnosti v Únii a k vybudovaniu kultúry sieťovej a informačnej bezpečnosti v prospech občanov, spotrebiteľov, podnikov a verejnej správy. Nariadenie Európskeho parlamentu a Rady (ES) č. 1007/2008 ([7]) predĺžilo mandát agentúry ENISA do marca 2012. Nariadením Európskeho parlamentu a Rady (EÚ) č. 580/2011 ([8]) sa mandát agentúry ENISA ďalej predĺžil do 13. septembra 2013. Nariadenie (EÚ) č. 526/2013 predĺžilo mandát agentúry ENISA do 19. júna 2020.

(15) Únia už prijala dôležité kroky na zaistenie kybernetickej bezpečnosti a zvýšenie dôvery v digitálne technológie. V roku 2013 bola prijatá Stratégia kybernetickej bezpečnosti Európskej únie pre usmerňovanie politickej reakcie Únie na kybernetické hrozby a riziká. V snahe o lepšiu ochranu občanov online prijala Únia v roku 2016 prvý právny akt v oblasti kybernetickej bezpečnosti v podobe smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 ([9]). V smernici (EÚ) 2016/1148 sa stanovujú požiadavky na vnútroštátnu spôsobilosť v oblasti kybernetickej bezpečnosti, zriaďujú sa prvé mechanizmy na posilnenie strategickej a operačnej spolupráce medzi členskými štátmi a zavádzajú sa povinnosti týkajúce sa bezpečnostných opatrení a oznamovania incidentov v odvetviach, ktoré sú pre hospodárstvo a spoločnosť kľúčové (ako energetika, doprava, dodávka a distribúcia pitnej vody, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, digitálna infraštruktúra), ako aj povinnosti kľúčových poskytovateľov digitálnych služieb (vyhľadávače, služby cloud computingu a online trhoviská).

Agentúre ENISA bola priradená kľúčová úloha podpory pri vykonávaní uvedenej smernice. Účinný boj proti počítačovej kriminalite je navyše dôležitou prioritou Európskeho programu v oblasti bezpečnosti a prispieva k celkovému cieľu vysokej úrovne kybernetickej bezpečnosti. Ďalšie právne akty, ako je nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 ([10]) a smernice Európskeho parlamentu a Rady 2002/58/ES ([11]) a (EÚ) 2018/1972 ([12]), takisto prispievajú k vysokej úrovni kybernetickej bezpečnosti na jednotnom digitálnom trhu.

([6]) Nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií (Ú. v. EÚ L 77, 13.3.2004, s. 1).

([7]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1007/2008 z 24. septembra 2008, ktorým sa mení a dopĺňa nariadenie (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, pokiaľ ide o dobu jej trvania (Ú. v. EÚ L 293, 31.10.2008, s. 1).

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

([9]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

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

([11]) Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002, s. 37).

([12]) Smernica Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (Ú. v. EÚ L 321, 17.12.2018, s. 36).

(16) Od prijatia Stratégie kybernetickej bezpečnosti Európskej únie v roku 2013 a od posledného prehodnotenia mandátu agentúry ENISA sa celkový politický kontext výrazne zmenil, keďže globálne prostredie sa stalo neistejším a menej bezpečným. Vzhľadom na uvedený kontext a v súvislosti s pozitívnym vývojom úlohy agentúry ENISA ako referenčného bodu pre poradenstvo a odborné znalosti a ako subjektu, ktorý uľahčuje spoluprácu a budovanie kapacít v rámci novej kybernetickobezpečnostnej politiky Únie, treba mandát agentúry ENISA zrevidovať s cieľom vymedziť jej úlohu v zmenenom ekosystéme kybernetickej bezpečnosti a zaistiť, aby účinne prispievala k reakcii Únie na výzvy v oblasti kybernetickej bezpečnosti vyplývajúce z radikálne zmenenej povahy kybernetických hrozieb, keďže ako sa potvrdilo v rámci hodnotenia agentúry ENISA, jej súčasný mandát na to nestačí.

(17) Agentúra ENISA zriadená týmto nariadením by mala byť nástupcom agentúry ENISA zriadenej nariadením (EÚ) č. 526/2013. Agentúra ENISA by mala vykonávať úlohy zverené jej týmto nariadením a inými právnymi aktmi Únie v oblasti kybernetickej bezpečnosti, okrem iného ako zdroj poradenstva a odborných znalostí, a aj ako stredisko Únie pre informácie a znalosti. Mala by podporovať výmenu najlepších postupov medzi členskými štátmi a súkromnými aktérmi, ponúkať Komisii a členským štátom politické návrhy, pôsobiť ako referenčný bod pre iniciatívy v rámci odvetvových politík Únie, pokiaľ ide o otázky kybernetickej bezpečnosti, a podporovať operačnú spoluprácu medzi členskými štátmi navzájom i v ich vzťahu k inštitúciám, orgánom, úradom a agentúram Únie.

(18) V jednomyseľnom rozhodnutí 2004/97/ES, Euratom prijatom predstaviteľmi členských štátov zasadajúcich na najvyššej štátnej a vládnej úrovni ([13]) zástupcovia členských štátov rozhodli, že agentúra ENISA bude mať sídlo v gréckom meste, ktoré určí grécka vláda. Hostiteľský členský štát agentúry ENISA by mal zabezpečiť čo najlepšie podmienky pre bezproblémové a efektívne fungovanie agentúry ENISA. Pre riadne a efektívne plnenie jej úloh, nábor a udržanie zamestnancov a zvýšenie efektívnosti budovania sietí vzťahov je nevyhnutné, aby agentúra ENISA sídlila na vhodnom mieste, ktoré okrem iného poskytuje vhodné dopravné spojenia a zariadenia pre manželských partnerov a deti sprevádzajúce personál agentúry ENISA. Potrebné dojednania by sa mali stanoviť v dohode medzi agentúrou ENISA a hostiteľským členským štátom, ktorá sa uzavrie po získaní súhlasu správnej rady agentúry ENISA.

(19) Keďže Únia čelí narastajúcim kybernetickobezpečnostným rizikám a výzvam, mal by sa zvýšiť objem finančných a ľudských zdrojov pridelených agentúre ENISA, aby sa odzrkadlilo jej posilnené poslanie a úlohy a jej rozhodujúce postavenie v ekosystéme organizácií brániacich digitálny ekosystém Únie a aby sa agentúre ENISA umožnilo účinne plniť úlohy zverené týmto nariadením.

(20) Agentúra ENISA by mala dosiahnuť a udržiavať si vysokú úroveň odborných znalostí a pôsobiť ako referenčný bod, ktorý buduje dôveru v jednotný trh svojou nezávislosťou, kvalitou poskytovaného poradenstva a šírených informácií, transparentnosťou svojich postupov a pracovných metód a dôslednosťou pri plnení svojich úloh. Agentúra ENISA by mala aktívne podporovať vnútroštátne úsilie a proaktívne prispievať k úsiliu Únie, pričom by mala vykonávať svoje úlohy v plnej spolupráci s inštitúciami, orgánmi, úradmi a agentúrami Únie a s členskými štátmi a zároveň podporovať synergiu a predchádzať akémukoľvek zdvojovaniu práce. Okrem toho by agentúra ENISA mala využívať vstupy od súkromného sektora a od ďalších relevantných zainteresovaných strán a spoluprácu s nimi. Mal by sa stanoviť súbor úloh, ktorým sa určí, ako agentúra ENISA dosiahne svoje ciele, ktorý by však umožnil flexibilitu jej činnosti.

(21) Aby agentúra ENISA mohla primerane podporovať operačnú spoluprácu medzi členskými štátmi, mala by ďalej posilňovať svoje vlastné technické a ľudské spôsobilosti a zručnosti. Agentúra ENISA by mala zvýšiť svoje odborné znalosti a spôsobilosť. Agentúra ENISA a členské štáty by na dobrovoľnom základe mohli vypracovať programy pre vysielanie národných expertov do agentúry ENISA, združovanie expertov a výmenu personálu.

(22) Agentúra ENISA by mala pomáhať Komisii poskytovaním poradenstva, stanovísk a analýz týkajúcich sa všetkých záležitostí Únie súvisiacich s vypracúvaním, aktualizáciou a revíziou politík a právnych predpisov v oblasti kybernetickej bezpečnosti a jej odvetvových aspektov s cieľom posilniť relevantnosť politík a právnych predpisov Únie s kybernetickobezpečnostným rozmerom a umožniť konzistentnosť pri vykonávaní uvedených politík a právnych predpisov na vnútroštátnej úrovni. Agentúra ENISA by mala byť referenčným bodom, pokiaľ ide o poradenstvo a odborné znalosti pre iniciatívy v rámci odvetvových politík a právnych predpisov Únie zahŕňajúcich rozmer kybernetickej bezpečnosti. Agentúra ENISA by mala pravidelne informovať Európsky parlament o svojej činnosti.

([13]) Jednomyseľné rozhodnutie 2004/97/ES, Euratom prijaté predstaviteľmi členských štátov zasadajúcich na najvyššej štátnej a vládnej úrovni z 13. decembra 2003 o rozmiestnení sídel určitých úradov a agentúr Európskej únie (Ú. v. EÚ L 29, 3.2.2004, s. 15).

(23) Verejným jadrom otvoreného internetu, najmä jeho hlavnými protokolmi a infraštruktúrou, ktoré sú celosvetovým verejným statkom, sa zabezpečuje základná funkčnosť internetu ako celku a jeho bežná prevádzka. Agentúra ENISA by mala podporovať bezpečnosť verejného jadra otvoreného internetu a stabilitu jeho fungovania vrátane napríklad kľúčových protokolov (najmä DNS, BGP a IPv6), prevádzky systému názvov domén (napríklad prevádzky všetkých domén najvyššej úrovne) a prevádzky koreňovej zóny.

(24) Základnou úlohou agentúry ENISA je presadzovať dôsledné vykonávanie príslušného právneho rámca, najmä účinné vykonávanie smernice (EÚ) 2016/1148 a iných príslušných právnych nástrojov s kybernetickobezpečnostnými aspektmi, čo je kľúčom k posilneniu kybernetickej odolnosti. Keďže situácia v oblasti kybernetickobezpečnostných hrozieb sa rýchlo mení, je jasné, že členské štáty potrebujú podporu v podobe komplexnejšieho, prierezového prístupu k budovaniu kybernetickej odolnosti.

(25) Agentúra ENISA by mala pomáhať členským štátom a inštitúciám, orgánom, úradom a agentúram Únie v ich úsilí vybudovať a zdokonaľovať spôsobilosť a pripravenosť predchádzať kybernetickým hrozbám a incidentom, odhaľovať ich a reagovať na ne, ako aj vo vzťahu k bezpečnosti sietí a informačných systémov. Agentúra ENISA by mala najmä podporovať rozvoj a posilňovanie vnútroštátnych jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „CSIRT“) a jednotiek CSIRT Únie stanovených v smernici (EÚ) 2016/1148, aby v rámci Únie všetky dosiahli vysoký stupeň vývoja. Činnosťami, ktoré vykonáva agentúra ENISA a ktoré sa týkajú operačných kapacít členských štátov, by sa mali aktívne podporovať opatrenia, ktoré členské štáty prijali, aby si splnili svoje povinnosti podľa smernice (EÚ) 2016/1148, a preto by ich nemali nahrádzať.

(26) Agentúra ENISA by mala zároveň pomáhať pri príprave a aktualizácii stratégií v oblasti bezpečnosti sietí a informačných systémov na úrovni Únie a na požiadanie na úrovni členských štátov, najmä pokiaľ ide o kybernetickú bezpečnosť, a podporovať šírenie takých stratégií a sledovať pokrok pri ich vykonávaní. Agentúra ENISA by tiež mala prispievať k pokrytiu potrieb v oblasti odbornej prípravy a vzdelávacích materiálov, a to aj potrieb verejných orgánov, a podľa vhodnosti do vysokej miery „školiť školiteľov“ na základe Rámca digitálnych kompetencií pre občanov a s cieľom pomôcť členským štátom a inštitúciám, orgánom, úradom a agentúram Únie pri rozvoji ich vlastných kapacít odbornej prípravy.

(27) Agentúra ENISA by mala podporovať členské štáty v oblasti zvyšovania povedomia a vzdelávania o kybernetickej bezpečnosti tým, že umožní užšiu koordináciu a výmenu najlepších postupov medzi členskými štátmi. Táto podpora by mohla zahŕňať vytvorenie siete kontaktných miest vnútroštátneho vzdelávania a platformy pre odbornú prípravu v oblasti kybernetickej bezpečnosti. Sieť kontaktných miest vnútroštátneho vzdelávania by mohla fungovať v rámci siete národných styčných úradníkov a byť začiatkom budúcej koordinácie v rámci členských štátov.

(28) Agentúra ENISA by mala pomáhať skupine pre spoluprácu zriadenej smernicou (EÚ) 2016/1148 pri výkone jej úloh, a to najmä poskytovaním odborných znalostí, poradenstva a uľahčovaním výmeny najlepších postupov, okrem iného pokiaľ ide o určenie prevádzkovateľov základných služieb členskými štátmi z hľadiska rizík a incidentov, a to aj v súvislosti s cezhraničnou previazanosťou.

(29) Na stimulovanie spolupráce verejného a súkromného sektora a v rámci súkromného sektora, najmä pokiaľ ide o podporu ochrany kritických infraštruktúr, by agentúra ENISA mala podporovať výmenu informácií v odvetviach a medzi nimi, obzvlášť v odvetviach uvedených v prílohe II k smernici (EÚ) 2016/1148, a to poskytovaním najlepších postupov a usmernení k existujúcim nástrojom a postupom, ako aj usmerňovaním v otázke riešenia regulačných problémov spojených s výmenou informácií, napríklad uľahčovaním zriaďovania odvetvových stredísk pre výmenu a analýzu informácií.

(30) Keďže potenciálny negatívny vplyv zraniteľností produktov IKT, služieb IKT a procesov IKT sa neustále zvyšuje, ich odhalenie a náprava zohrávajú dôležitú úlohu pri znižovaní celkového rizika v oblasti kybernetickej bezpečnosti. Spolupráca medzi organizáciami, výrobcami alebo poskytovateľmi zraniteľných produktov IKT, služieb IKT a procesov IKT a členmi kybernetickobezpečnostnej výskumnej komunity a sektorom verejnej správy, ktorí zraniteľnosti odhaľujú, preukázateľne a výrazne zvyšuje mieru odhaľovania a nápravy zraniteľnosti produktov IKT, služieb IKT a procesov IKT. Koordinované zverejňovanie informácií o zraniteľnosti sa riadi štruktúrovaným procesom spolupráce, v rámci ktorého sa zraniteľnosti hlásia vlastníkovi informačného systému, čím sa danej organizácii dáva príležitosť diagnostikovať zraniteľnosť a zabezpečiť jej nápravu pred tým, ako sa podrobné informácie o zraniteľnosti poskytnú tretím stranám alebo verejnosti. Tento proces tiež upravuje koordináciu objaviteľa a organizácie, pokiaľ ide o zverejnenie uvedenej zraniteľnosti. Politiky koordinovaného zverejňovania informácií o zraniteľnosti by mohli zohrávať dôležitú úlohu v úsilí členských štátov o zvýšenie kybernetickej bezpečnosti.

(31) Agentúra ENISA by mala zhromažďovať a analyzovať dobrovoľne zdieľané správy vnútroštátnych jednotiek CSIRT a medziinštitucionálneho tímu reakcie na núdzové počítačové situácie v inštitúciách, orgánoch a agentúrach Únie zriadeného Dohodou medzi Európskym parlamentom, Európskou radou, Radou Európskej únie, Európskou komisiou, Súdnym dvorom Európskej únie, Európskou centrálnou bankou, Európskym dvorom audítorov, Európskou službou pre vonkajšiu činnosť, Európskym hospodárskym a sociálnym výborom, Európskym výborom regiónov a Európskou investičnou bankou o organizácii a fungovaní tímu reakcie na núdzové počítačové situácie v inštitúciách, orgánoch a agentúrach Únie (CERT-EU) ([14]), s cieľom prispievať k stanovovaniu spoločných postupov, jazyka a terminológie na výmenu informácií. V uvedenom kontexte by agentúra ENISA mala zapojiť súkromný sektor v rámci smernice (EÚ) 2016/1148, ktorou sa stanovuje základ pre dobrovoľnú výmenu technických informácií na operačnej úrovni v sieti jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „sieť jednotiek CSIRT“).

(32) Agentúra ENISA by mala prispievať k reakciám na úrovni Únie v prípade rozsiahlych cezhraničných incidentov a kríz v oblasti kybernetickej bezpečnosti. Uvedená úloha by sa mala vykonávať v súlade s mandátom agentúry ENISA podľa tohto nariadenia a prístupom, na ktorom sa dohodnú členské štáty v kontexte odporúčania Komisie (EÚ) 2017/1584 ([15]) a záverov Rady z 26. júna 2018 o koordinovanej reakcii EÚ na kybernetické bezpečnostné incidenty a krízy veľkého rozsahu. Uvedená úloha by mohla zahŕňať aj zhromažďovanie relevantných informácií a uľahčovanie interakcie medzi sieťou jednotiek CSIRT a technickou komunitou či subjektmi zodpovednými za krízové riadenie, ktoré prijímajú rozhodnutia. Okrem toho by agentúra ENISA mala podporovať operačnú spoluprácu medzi členskými štátmi na žiadosť jedného alebo viacerých členských štátov pri riešení incidentov z technickej stránky uľahčovaním výmeny relevantných technických riešení medzi členskými štátmi a vypracúvaním príspevkov pre komunikáciu s verejnosťou. Agentúra ENISA by mala podporovať operačnú spoluprácu skúšaním rôznych spôsobov takejto spolupráce na pravidelných kybernetickobezpečnostných cvičeniach.

(33) Agentúra ENISA by na podporu operačnej spolupráce mala prostredníctvom štruktúrovanej spolupráce využívať dostupné technické a operačné odborné znalosti tímu CERT-EU. Takáto štruktúrovaná spolupráca by mohla viesť k budovaniu odborných znalostí agentúry ENISA. Podľa potreby by sa mali medzi oboma subjektmi vytvoriť účelové dohody o fungovaní tejto spolupráce v praxi a zabránení zdvojovaniu činností.

(34) Pri plnení svojej úlohy na podporu operačnej spolupráce v rámci siete jednotiek CSIRT by agentúra ENISA mala byť schopná poskytovať členským štátom na ich požiadanie podporu, napríklad tým, že bude poskytovať poradenstvo o tom, ako zlepšiť ich spôsobilosti predchádzať incidentom, odhaľovať ich a reagovať na ne, že bude uľahčovať technické riešenie incidentov, ktoré majú významný alebo závažný vplyv, alebo že zabezpečí analýzy kybernetických hrozieb a incidentov. ENISA by mala uľahčovať technické riešenia incidentov, ktoré majú významný alebo závažný vplyv, najmä podporou zameranou na dobrovoľnú výmenu technických riešení medzi členskými štátmi alebo tým, že bude vypracúvať kombinované technické informácie, ako napríklad technické riešenia, ktoré dali dobrovoľne k dispozícii členské štáty. V odporúčaní (EÚ) 2017/1584 sa odporúča, aby členské štáty v dobrej viere spolupracovali a bez zbytočného odkladu sa vzájomne i s agentúrou ENISA delili o informácie o rozsiahlych incidentoch a krízach v oblasti kybernetickej bezpečnosti. Aj tieto informácie by agentúre ENISA pomohli pri plnení jej úlohy, pokiaľ ide o podporu operačnej spolupráce.

(35) V rámci bežnej technickej spolupráce na podporu situačného povedomia Únie by mala agentúra ENISA v úzkej spolupráci s členskými štátmi vypracúvať pravidelné podrobné technické situačné správy o kybernetickej bezpečnosti v EÚ, ktoré sa týkajú incidentov a kybernetických hrozieb, a ktoré vychádzajú z verejne dostupných informácií, jej vlastných analýz a správ, ktoré jej poskytli jednotky CSIRT členských štátov alebo národné jednotné kontaktné miesta pre bezpečnosť sietí a informačných systémov (ďalej len „jednotné kontaktné miesta“) stanovené v smernici (EÚ) 2016/1148, v oboch prípadoch na dobrovoľnom základe, Európske centrum boja proti počítačovej kriminalite (EC3) pri Europole, CERT-EU a v náležitých prípadoch spravodajské a situačné centrum Európskej únie (EU INTCEN) v rámci Európskej služby pre vonkajšiu činnosť. Uvedená správa by sa mala sprístupniť Rade, Komisii, vysokému predstaviteľovi Únie pre zahraničné veci a bezpečnostnú politiku a sieti jednotiek CSIRT.

(36) Podpora pri ex post technickom skúmaní incidentov s významným alebo závažným vplyvom, ktorú agentúra ENISA poskytuje na žiadosť dotknutých členských štátov, by sa mala zameriavať na predchádzanie incidentom v budúcnosti. Dotknuté členské štáty by mali agentúre ENISA poskytnúť potrebné informácie a pomoc, aby mohla účinne podporiť ex post technické skúmanie.

([14]) Ú. v. EÚ C 12, 13.1.2018, s. 1.

([15]) Odporúčanie Komisie (EÚ) 2017/1584 z 13. septembra 2017 o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu (Ú. v. EÚ L 239, 19.9.2017, s. 36).

(37) Členské štáty môžu prizvať podniky dotknuté daným incidentom k spolupráci v podobe poskytnutia potrebných informácií a pomoci agentúre ENISA bez toho, aby tým bolo dotknuté ich právo na ochranu citlivých obchodných informácií a informácií dôležitých z hľadiska verejnej bezpečnosti.

(38) Na lepšie pochopenie výziev v oblasti kybernetickej bezpečnosti a v záujme dlhodobého strategického poradenstva pre členské štáty a inštitúcie, orgány, úrady a agentúry Únie musí agentúra ENISA analyzovať existujúce i nové kybernetickobezpečnostné riziká. Na to by agentúra ENISA mala v spolupráci s členskými štátmi a podľa potreby so štatistickými orgánmi a ďalšími orgánmi zbierať relevantné verejne dostupné alebo dobrovoľne zdieľané informácie, analyzovať nové technológie a poskytovať tematické posúdenie o očakávanom spoločenskom, právnom, hospodárskom a regulačnom vplyve technologických inovácií na sieťovú a informačnú bezpečnosť, najmä kybernetickú bezpečnosť. Agentúra ENISA by navyše mala členské štáty a inštitúcie, orgány, úrady a agentúry Únie podporovať pri identifikácii nových kybernetickobezpečnostných rizík a pri predchádzaní incidentom, a to analýzou kybernetických hrozieb, zraniteľnosti a incidentov.

(39) V záujme posilnenia odolnosti Únie by agentúra ENISA mala rozvíjať odborné znalosti v oblasti kybernetickej bezpečnosti infraštruktúr, najmä s cieľom podpory odvetví uvedených v prílohe II k smernici (EÚ) 2016/1148, a infraštruktúr, ktoré používajú poskytovatelia digitálnych služieb uvedených v prílohe III k uvedenej smernici, a to poskytovaním poradenstva, vydávaním usmernení a výmenou najlepších postupov. S cieľom uľahčiť prístup k lepšie štruktúrovaným informáciám o kybernetickobezpečnostných rizikách a možných nápravách by agentúra ENISA mala zriadiť a udržiavať „informačné centrum“ Únie – portál s funkciou jednotného kontaktného miesta, ktorý bude verejnosti sprístupňovať informácie o kybernetickej bezpečnosti pochádzajúce od únijných a vnútroštátnych inštitúcií, orgánov, úradov a agentúr. Uľahčovanie prístupu k lepšie štruktúrovaným informáciám o kybernetickobezpečnostných rizikách a možných nápravách by mohlo tiež pomôcť členským štátom pri posilňovaní ich kapacít a zosúlaďovaní postupov, čo by zvýšilo ich celkovú odolnosť proti kybernetickým útokom.

(40) Agentúra ENISA by mala prispievať k zvyšovaniu verejného povedomia o kybernetickobezpečnostných rizikách, a to aj celoúnijnou kampaňou a podporou vzdelávania, a poskytovaniu poradenstva o osvedčených postupoch pre jednotlivých užívateľov zameraného na občanov, organizácie a podniky. Agentúra ENISA by mala prispievať aj k propagácii najlepších postupov a riešení vrátane kybernetickej hygieny a kybernetickej gramotnosti na úrovni občanov, organizácií a podnikov, a to zhromažďovaním a analýzou verejne dostupných informácií o významných incidentoch a vypracúvaním a uverejňovaním správ a poradenstva pre občanov, organizácie a podniky s cieľom zvýšiť ich celkovú úroveň pripravenosti a odolnosti. Agentúra ENISA by sa mala takisto usilovať o to, aby spotrebiteľom poskytovala relevantné informácie o platných certifikačných systémoch, napríklad poskytovaním usmernení a odporúčaní. Agentúra ENISA by navyše mala v súlade s Akčným plánom digitálneho vzdelávania stanoveným v oznámení Komisie zo 17. januára 2018 a v spolupráci s členskými štátmi a inštitúciami, orgánmi, úradmi a agentúrami Únie organizovať pravidelné osvetové a vzdelávacie kampane pre verejnosť určené koncovým užívateľom a zamerané na propagáciu bezpečnejšieho správania jednotlivcov na internete a digitálnej gramotnosti, na zvyšovanie povedomia o možných kybernetických hrozbách vrátane internetovej trestnej činnosti, ako sú phishingové útoky, botnety, finančné a bankové podvody, incidenty zahŕňajúce podvody s údajmi, a na propagáciu základných rád v oblasti viacfaktorovej autentifikácie, aplikovania bezpečnostných záplat, šifrovania, anonymizácie a ochrany údajov.

(41) Agentúra ENISA by mala zohrávať ústrednú úlohu pri urýchlení zvyšovania povedomia koncových užívateľov o bezpečnosti zariadení a bezpečnom využívaní služieb, a mala by na úrovni Únie propagovať zásady „bezpečnosť už v štádiu návrhu“ a „ochrana súkromia už v štádiu návrhu“. Pri sledovaní tohto cieľa by agentúra ENISA mala využívať dostupné najlepšie postupy a skúsenosti, najmä akademických inštitúcií a výskumných pracovníkov v oblasti bezpečnosti informačných technológií.

(42) Na podporu podnikov pôsobiacich v odvetví kybernetickej bezpečnosti, ako aj užívateľov kybernetickobezpečnostných riešení by agentúra ENISA mala vytvoriť a udržiavať „monitor trhu“, ktorý bude pravidelne analyzovať a šíriť informácie o hlavných trendoch na trhu kybernetickej bezpečnosti, a to na strane dopytu, ako aj ponuky.

(43) Agentúra ENISA by mala prispievať k úsiliu Únie v oblasti spolupráce s medzinárodnými organizáciami, ako aj v rámci príslušných medzinárodných rámcov spolupráce v oblasti kybernetickej bezpečnosti. Agentúra ENISA by predovšetkým mala podľa vhodnosti prispievať k spolupráci s organizáciami, ako je NATO, OBSE a OECD. Takáto spolupráca by mohla zahŕňať spoločné kybernetickobezpečnostné cvičenia a koordináciu spoločnej reakcie na incidenty. Uvedené činnosti sa majú vykonávať pri plnom rešpektovaní zásad inkluzívnosti, reciprocity a rozhodovacej autonómie Únie bez toho, aby bola dotknutá osobitná povaha bezpečnostnej a obrannej politiky ktoréhokoľvek členského štátu.

(44) S cieľom zaistiť úplné splnenie svojich cieľov by agentúra ENISA mala udržiavať kontakty s relevantnými dozornými orgánmi Únie a inými príslušnými orgánmi v Únii, inštitúciami, orgánmi, úradmi a agentúrami Únie vrátane tímu CERT-EU, EC3, Európskej obrannej agentúry (EDA), Agentúry pre európsky globálny navigačný satelitný systém (Agentúry pre európsky GNSS), Orgánu európskych regulátorov pre elektronické komunikácie (BEREC), Európskej agentúry na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti (eu-LISA), Európskej centrálnej banky (ECB), Európskeho orgánu pre bankovníctvo (EBA), Európskeho výboru pre ochranu údajov, Agentúry pre spoluprácu regulačných orgánov v oblasti energetiky (ACER), Agentúry Európskej únie pre bezpečnosť letectva (EASA) a všetkých ďalších agentúr Únie angažovaných v otázkach kybernetickej bezpečnosti. Okrem toho by agentúra ENISA mala udržiavať kontakty aj s orgánmi zodpovednými za ochranu údajov s cieľom vymieňať si know-how a najlepšie postupy a poskytovať poradenstvo o otázkach kybernetickej bezpečnosti, ktoré môžu ovplyvniť ich prácu. Zástupcovia vnútroštátnych orgánov a orgánov Únie v oblasti presadzovania práva a ochrany údajov by mali byť oprávnení na zastúpenie v poradnej skupine agentúry ENISA. Pri styku s orgánmi presadzovania práva v otázkach sieťovej a informačnej bezpečnosti, ktoré by mohli mať vplyv na ich prácu, by agentúra ENISA mala rešpektovať existujúce informačné kanály a zavedené siete.

(45) Mohli by sa vytvárať partnerstvá s akademickými inštitúciami, ktoré majú výskumné iniciatívy v relevantných oblastiach, pričom pre vstupy od spotrebiteľských a iných organizácií by mali byť k dispozícii vhodné kanály a mali by sa zohľadňovať.

(46) Agentúra ENISA by vo svojej funkcii sekretariátu siete jednotiek CSIRT mala podporovať jednotky CSIRT členských štátov a tím CERT-EU v operačnej spolupráci v súvislosti s relevantnými úlohami siete jednotiek CSIRT uvedenými v smernici (EÚ) 2016/1148. Ďalej by agentúra ENISA mala presadzovať a podporovať spoluprácu medzi príslušnými jednotkami CSIRT v prípade incidentov, útokov alebo narušení sietí alebo infraštruktúr pod ich správou alebo ochranou, ktoré zahŕňajú alebo môžu zahŕňať aspoň dve jednotky CSIRT, pričom sa riadne zohľadnia štandardné operačné postupy siete jednotiek CSIRT.

(47) V záujme lepšej pripravenosti Únie reagovať na incidenty by agentúra ENISA mala pravidelne organizovať kybernetickobezpečnostné cvičenia na úrovni Únie a na žiadosť by mala podporovať členské štáty a inštitúcie, orgány, úrady a agentúry Únie pri organizácii takých cvičení. Raz za dva roky by sa mali organizovať rozsiahle komplexné cvičenia, ktoré by zahŕňali technické, operačné alebo strategické prvky. Okrem toho agentúra ENISA by mala pravidelne organizovať menej komplexné cvičenia s rovnakým cieľom lepšej pripravenosti Únie reagovať na incidenty.

(48) Agentúra ENISA by mala ďalej rozvíjať a udržiavať odborné znalosti, ktoré sa týkajú certifikácie kybernetickej bezpečnosti, v záujme podpory politiky Únie v tejto oblasti. Agentúra ENISA by mala stavať na existujúcich najlepších postupoch a podporovať zavádzanie certifikácie kybernetickej bezpečnosti v Únii, a to aj tým, že prispeje k vytvoreniu a udržiavaniu rámca certifikácie kybernetickej bezpečnosti na úrovni Únie (Európsky rámec certifikácie kybernetickej bezpečnosti), aby sa posilnila transparentnosť dôveryhodnosti kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT, a tým sa posilnila dôvera v digitálny vnútorný trh a jeho konkurencieschopnosť.

(49) Účinné politiky kybernetickej bezpečnosti by mali vychádzať z podrobne vyvinutých metód posudzovania rizika vo verejnom i v súkromnom sektore. Metódy posudzovania rizika sa používajú na rôznych úrovniach bez spoločného postupu ich účinného uplatňovania. Podpora a vývoj najlepších postupov v oblasti posudzovania rizika a interoperabilných riešení riadenia rizika v organizáciách verejného a súkromného sektora zvýšia úroveň kybernetickej bezpečnosti v Únii. S týmto cieľom by agentúra ENISA mala podporovať spoluprácu zainteresovaných strán na úrovni Únie a uľahčovať ich úsilie o tvorbu a zavádzanie európskych a medzinárodných noriem pre riadenie rizika a merateľnú bezpečnosť elektronických produktov, systémov, sietí a služieb, ktoré spolu so softvérom tvoria sieťové a informačné systémy.

(50) Agentúra ENISA by mala podnecovať členské štáty, výrobcov alebo poskytovateľov produktov IKT, služieb IKT alebo procesov IKT k sprísňovaniu ich všeobecných bezpečnostných noriem tak, aby všetci užívatelia internetu mohli podniknúť kroky potrebné na zaistenie svojej osobnej kybernetickej bezpečnosti a boli k tomu motivovaní. Najmä výrobcovia a poskytovatelia produktov IKT, služieb IKT alebo procesov IKT by mali poskytovať potrebné aktualizácie a sťahovať od spotrebiteľov alebo z trhu či prepracúvať produkty IKT, služby IKT alebo procesy IKT, ktoré nespĺňajú kybernetickobezpečnostné normy, zatiaľ čo dovozcovia a distribútori by mali zabezpečiť, aby produkty IKT, služby IKT a procesy IKT, ktoré uvádzajú na trh Únie, boli v súlade s príslušnými požiadavkami a nepredstavovali riziko pre spotrebiteľov Únie.

(51) V spolupráci s príslušnými orgánmi by agentúra ENISA mala šíriť informácie o úrovni kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT ponúkaných na vnútornom trhu, varovať pred určitými výrobcami alebo poskytovateľmi produktov IKT, služieb IKT alebo procesov IKT a žiadať ich o zvýšenie bezpečnosti ich produktov IKT, služieb IKT a procesov IKT vrátane kybernetickej bezpečnosti.

(52) Pri poskytovaní poradenstva inštitúciám, orgánom, úradom a agentúram Únie a na požiadanie prípadne aj členským štátom o potrebách a prioritách výskumu v oblasti kybernetickej bezpečnosti by agentúra ENISA mala plne zohľadňovať výskum, vývoj a technologické posudzovanie, ktoré prebiehajú najmä v rámci rôznych výskumných iniciatív Únie. S cieľom určiť výskumné potreby a priority by agentúra ENISA mala konzultovať aj príslušné skupiny užívateľov. Konkrétnejšie by sa mohla nadviazať spolupráca s Európskou radou pre výskum, Európskym inovačným a technologickým inštitútom a Inštitútom Európskej únie pre bezpečnostné štúdie.

(53) Agentúra ENISA by mala pri príprave európskych systémov certifikácie kybernetickej bezpečnosti pravidelne viesť konzultácie s normalizačnými organizáciami, najmä európskymi normalizačnými organizáciami.

(54) Kybernetické hrozby sú globálnym problémom. Je potrebná užšia medzinárodná spolupráca s cieľom zlepšiť kybernetickobezpečnostné normy vrátane potreby vymedzenia spoločných noriem správania, prijatia kódexov správania, uplatňovania medzinárodných noriem a výmeny informácií, presadzovania rýchlejšej medzinárodnej spolupráce pri reakcii na problémy týkajúce sa sieťovej a informačnej bezpečnosti, ako aj presadzovania spoločného globálneho prístupu k týmto problémom. Agentúra ENISA by na tento účel mala podporovať výraznejšie kontakty a spoluprácu Únie s tretími krajinami a medzinárodnými organizáciami tým, že vo vhodných prípadoch poskytne potrebné odborné znalosti a analýzu príslušným inštitúciám, orgánom, úradom a agentúram Únie.

(55) Agentúra ENISA by mala byť schopná reagovať na ad hoc žiadosti členských štátov a inštitúcií, orgánov, úradov a agentúr Únie o poradenstvo a pomoc v záležitostiach, na ktoré sa vzťahuje mandát agentúry ENISA.

(56) Je rozumné a odporúča sa uplatňovať určité zásady týkajúce sa správy agentúry ENISA s cieľom dodržiavať spoločné vyhlásenie a spoločný prístupu, ktoré boli dohodnuté medziinštitucionálnou pracovnou skupinou pre decentralizované agentúry EÚ v júli 2012, ktorých cieľom je zefektívniť činnosti decentralizovaných agentúr a zlepšiť ich výkonnosť. Odporúčania v spoločnom vyhlásení a spoločnom prístupe by sa mali podľa potreby odraziť aj v pracovných programoch agentúry ENISA, jej hodnoteniach a jej praxi v oblasti podávania správ a administratívy.

(57) Správna rada zložená zo zástupcov členských štátov a Komisie by mala stanoviť všeobecné smerovanie činnosti agentúry ENISA a zabezpečiť, aby agentúra ENISA vykonávala svoje úlohy v súlade s týmto nariadením. Správna rada by mala mať potrebné právomoci na zostavovanie rozpočtu, overovanie plnenia rozpočtu, prijatie vhodných rozpočtových pravidiel, stanovenie transparentných pracovných postupov rozhodovania agentúry ENISA, prijatie jednotného programového dokumentu agentúry ENISA, prijatie vlastného rokovacieho poriadku, menovanie výkonného riaditeľa a rozhodovanie o predĺžení a ukončení jeho funkčného obdobia.

(58) Aby agentúra ENISA mohla riadne a efektívne fungovať, Komisia a členské štáty by mali zabezpečiť, aby osoby, ktoré majú byť vymenované za členov správnej rady, mali zodpovedajúce odborné znalosti a skúsenosti. Komisia a členské štáty by mali vynaložiť úsilie aj na obmedzenie obmeny svojich zástupcov v správnej rade s cieľom zabezpečiť kontinuitu jej práce.

(59) V záujme bezproblémového fungovania agentúry ENISA je nevyhnutné, aby bol jej výkonný riaditeľ vymenovaný na základe zásluh a zdokumentovaných administratívnych a riadiacich schopností, ako aj na základe spôsobilosti a skúseností v oblasti kybernetickej bezpečnosti. Výkonný riaditeľ by mal vykonávať svoje povinnosti úplne nezávisle. Výkonný riaditeľ by mal pripraviť návrh ročného pracovného programu agentúry ENISA po predchádzajúcej konzultácii s Komisiou a prijať všetky potrebné opatrenia na zabezpečenie riadneho vykonávania uvedeného pracovného programu. Výkonný riaditeľ by mal vypracovať výročnú správu, ktorej súčasťou bude plnenie ročného pracovného programu agentúry ENISA a ktorá sa predloží správnej rade, vypracovať návrh výkazu odhadov príjmov a výdavkov agentúry ENISA a plniť rozpočet. Výkonný riaditeľ by okrem toho mal mať možnosť zriadiť ad hoc pracovné skupiny zamerané na osobitné záležitosti najmä vedeckej, technickej, právnej či sociálno-ekonomickej povahy. Zriadenie ad hoc pracovnej skupiny sa považuje za potrebné najmä v súvislosti s vypracovaním konkrétneho kandidátskeho európskeho systému certifikácie kybernetickej bezpečnosti (ďalej len „kandidátsky systém“). Výkonný riaditeľ by mal zabezpečiť, aby sa členovia ad hoc pracovných skupín vyberali podľa najprísnejších požiadaviek na odbornosť s cieľom zabezpečiť rodovú rovnováhu a primeranú rovnováhu medzi

verejnými správami členských štátov, inštitúciami, orgánmi, úradmi a agentúrami Únie, súkromným sektorom vrátane príslušného priemyselného odvetvia, užívateľmi a akademickými expertmi v oblasti sieťovej a informačnej bezpečnosti, a to podľa konkrétnej tematiky.

(60) Výkonná rada by mala prispievať k efektívnej činnosti správnej rady. V rámci prípravných prác spojených s rozhodnutiami správnej rady by výkonná rada mala podrobne skúmať relevantné informácie a dostupné možnosti, radiť a ponúkať riešenia na prípravu rozhodnutí správnej rady.

(61) Agentúra ENISA by mala mať poradnú skupinu ENISA ako poradný orgán s cieľom zabezpečiť pravidelný dialóg so súkromným sektorom, spotrebiteľskými organizáciami a inými príslušnými zainteresovanými stranami. Poradná skupina ENISA zriadená správnou radou na návrh výkonného riaditeľa by sa mala zameriavať na otázky dôležité pre zainteresované strany a mala by na ne upriamovať pozornosť agentúry ENISA. Poradná skupina ENISA by mala byť konzultovaná najmä v súvislosti s návrhom ročného pracovného programu agentúry ENISA. Zloženie poradnej skupiny ENISA a úlohy zverené tejto skupine by mali zabezpečiť dostatočné zastúpenie zainteresovaných strán na práci agentúry ENISA.

(62) S cieľom pomáhať agentúre ENISA a Komisii pri uľahčovaní konzultácií s príslušnými zainteresovanými stranami by sa mala zriadiť skupina zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti. Skupina zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti by mala byť zložená z členov, ktorí vo vyváženom pomere zastupujú príslušné priemyselné odvetvie vrátane najmä malých a stredných podnikov, a to tak na strane dopytu, ako aj na strane ponuky produktov IKT a služieb IKT, poskytovateľov digitálnych služieb, európske a medzinárodné normalizačné orgány, vnútroštátne akreditačné orgány, dozorné orgány pre ochranu údajov a orgány posudzovania zhody podľa nariadenia Európskeho parlamentu a Rady (ES) č. 765/2008 ([16]), a akademickú obec, ako aj spotrebiteľské organizácie.

(63) Agentúra ENISA by mala zaviesť pravidlá na predchádzanie konfliktov záujmov a ich riešenie. Agentúra ENISA by mala tiež uplatňovať príslušné pravidlá Únie týkajúce sa prístupu verejnosti k dokumentom, ako sa stanovujú v nariadení Európskeho parlamentu a Rady (ES) č. 1049/2001 ([17]). Na spracúvanie osobných údajov agentúrou ENISA by sa malo vzťahovať nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 ([18]). Agentúra ENISA by mala dodržiavať ustanovenia platné pre inštitúcie, orgány, úrady a agentúry Únie, ako aj vnútroštátne právne predpisy o manipulácii s informáciami, najmä s citlivými neutajovanými skutočnosťami a utajovanými skutočnosťami Európskej únie.

(64) S cieľom zaručiť úplnú autonómiu a nezávislosť agentúry ENISA a umožniť jej plniť ďalšie úlohy vrátane nepredvídaných naliehavých úloh by sa mal agentúre ENISA udeliť dostatočný a nezávislý rozpočet, ktorého príjmy by mali pochádzať predovšetkým z príspevku Únie a príspevkov tretích krajín, ktoré sa podieľajú na práci agentúry ENISA. Primeraný rozpočet je rozhodujúci na zabezpečenie toho, aby agentúra ENISA mala dostatočné kapacity na plnenie všetkých svojich pribúdajúcich úloh a na dosahovanie svojich cieľov. Väčšina personálu agentúry ENISA by mala byť priamo zapojená do operačného plnenia mandátu agentúry ENISA. Hostiteľský členský štát a akýkoľvek iný členský štát by mali mať možnosť dobrovoľne prispievať do rozpočtu agentúry ENISA. Pokiaľ ide o akékoľvek dotácie hradené zo všeobecného rozpočtu Únie, naďalej by sa mal uplatňovať rozpočtový postup Únie. Okrem toho by Dvor audítorov mal vykonávať audit účtov agentúry ENISA v záujme transparentnosti a zodpovednosti.

(65) Certifikácia kybernetickej bezpečnosti zohráva významnú úlohu pri posilňovaní dôvery v produkty IKT, služby IKT a procesy IKT, ako aj ich bezpečnosti. Digitálny jednotný trh, a najmä dátové hospodárstvo a IoT môžu prosperovať, iba ak široká verejnosť verí, že takéto produkty, služby a procesy zaručujú určitú mieru kybernetickej bezpečnosti. Prepojené a automatizované vozidlá, elektronické zdravotnícke pomôcky, riadiace systémy priemyselnej automatizácie a inteligentné siete sú iba niekoľkými príkladmi odvetví, kde už sa certifikácia bežne využíva alebo sa začne využívať v blízkej budúcnosti. Aj v odvetviach, ktoré upravuje smernica (EÚ) 2016/1148, je certifikácia kybernetickej bezpečnosti kľúčová.

([16]) Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93 (Ú. v. EÚ L 218, 13.8.2008, s. 30).

([17]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (Ú. v. ES L 145, 31.5.2001, s. 43).

([18]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

(66) Vo svojom oznámení s názvom Posilnenie odolnosti kybernetického systému a podpora konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe z roku 2016 Komisia načrtla potrebu kvalitných, cenovo dostupných a interoperabilných produktov a riešení v oblasti kybernetickej bezpečnosti. Ponuka produktov IKT, služieb IKT a procesov IKT na jednotnom trhu je geograficky stále veľmi fragmentovaná. Dôvodom je, že vývoj odvetvia kybernetickej bezpečnosti v Európe sa do značnej miery riadil dopytom verejných správ jednotlivých štátov. Medzi ďalšie nedostatky ovplyvňujúce jednotný trh v oblasti kybernetickej bezpečnosti patrí absencia interoperabilných riešení (technických noriem), postupov a celoúnijných mechanizmov certifikácie. Európskym podnikom to sťažuje možnosť konkurovať si na národnej úrovni, na úrovni Únie i na svetovej úrovni. Na druhej sa tým okliešťuje ponuka reálne využiteľných technológií kybernetickej bezpečnosti, ku ktorým majú fyzické osoby a podniky prístup. Podobne Komisia vo svojom oznámení z roku 2017 o preskúmaní vykonávania stratégie digitálneho jednotného trhu v polovici trvania – Prepojený digitálny jednotný trh pre všetkých zdôraznila potrebu bezpečných pripojených produktov a systémov a naznačila, že vytvorenie európskeho rámca bezpečnosti IKT, v ktorom sa stanovia pravidlá organizovania certifikácie bezpečnosti IKT v Únii, by mohlo zachovať dôveru v internet a zároveň vyriešiť súčasnú fragmentáciu vnútorného trhu.

(67) Certifikácia kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT sa v súčasnosti využíva iba obmedzene. Ak sa uplatňuje, je to zväčša na úrovni členských štátov alebo z iniciatívy príslušného priemyselného odvetvia. V tejto súvislosti certifikát vystavený niektorým vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti v zásade iné členské štáty neuznávajú. Môže sa teda stať, že spoločnosti musia svoje produkty IKT, služby IKT a procesy IKT certifikovať v niekoľkých členských štátoch, v ktorých pôsobia, napríklad ak sa chcú zapojiť do ich vnútroštátnych postupov obstarávania, čím sa im zvyšujú náklady. Okrem toho, hoci sa objavujú nové systémy, zdá sa, že neexistuje koherentný a holistický prístup k horizontálnym otázkam kybernetickej bezpečnosti, ako napríklad v oblasti IoT. Existujúce systémy vykazujú výrazné nedostatky a rozdiely z hľadiska škály pokrytia produktov, stupňov dôveryhodnosti, vecných kritérií a samotného využitia, v dôsledku čoho sa v rámci Únie nemôžu využívať mechanizmy vzájomného uznávania.

(68) Boli určité snahy s cieľom zabezpečiť vzájomné uznávanie certifikátov v Únii. Úspešné však boli iba sčasti. Najvýznamnejším príkladom v tomto smere je dohoda skupiny vysokých úradníkov pre bezpečnosť informačných systémov (SOG-IS) o vzájomnom uznávaní (DVU). Hoci ide o najvýznamnejší model spolupráce a vzájomného uznávania v oblasti bezpečnostnej certifikácie, do SOG-IS je zapojených len niekoľko členských štátov. Táto skutočnosť obmedzila účinnosť dohody SOG-IS DVU z hľadiska vnútorného trhu.

(69) Je preto potrebné zaujať spoločný prístup a zriadiť európsky rámec certifikácie kybernetickej bezpečnosti, v ktorom sa stanovia základné horizontálne požiadavky kladené na európske systémy certifikácie kybernetickej bezpečnosti, ktoré sa majú vytvoriť, a ktorým sa umožní uznávanie a využívanie európskych certifikátov kybernetickej bezpečnosti a EÚ vyhlásení o zhode pre produkty IKT, služby IKT alebo procesy IKT vo všetkých členských štátoch. Pri tom je nevyhnutné stavať na súčasných vnútroštátnych a medzinárodných systémoch, ako aj na systémoch vzájomného uznávania, najmä na SOG-IS, a umožniť plynulý prechod z týchto existujúcich systémov na systémy v novom európskom rámci certifikácie kybernetickej bezpečnosti. Tento európsky rámec certifikácie kybernetickej bezpečnosti by mal plniť dvojaký účel. Po prvé, mal by prispievať k posilneniu dôvery v produkty IKT, služby IKT a procesy IKT certifikované podľa európskych systémov certifikácie kybernetickej bezpečnosti. Po druhé, mal by pomôcť zabrániť množeniu odporujúcich si či prekrývajúcich sa vnútroštátnych systémov certifikácie kybernetickej bezpečnosti, čím by sa znížili náklady podnikov pôsobiacich na digitálnom jednotnom trhu. Európske systémy certifikácie kybernetickej bezpečnosti by mali byť nediskriminačné a založené na európskych alebo medzinárodných normách, pokiaľ tieto normy nie sú neúčinné alebo nevhodné na plnenie legitímnych cieľov Únie v tomto ohľade.

(70) Európsky rámec certifikácie kybernetickej bezpečnosti by sa mal zaviesť jednotne vo všetkých členských štátoch, aby sa zabránilo praxi tzv. nakupovania certifikátov v dôsledku rozdielnych úrovní prísnosti v rôznych členských štátoch.

(71) Európske systémy certifikácie kybernetickej bezpečnosti by mali vychádzať z toho, čo už existuje na medzinárodnej a vnútroštátnej úrovni, a v prípade potreby z technických špecifikácií z fór a konzorcií, pričom by sa zužitkovali skúseností zo súčasných silných stránok a tiež posúdili a odstránili nedostatky.

(72) Aby si dané odvetvie udržiavalo náskok pred kybernetickými hrozbami, sú potrebné pružné riešenia v oblasti kybernetickej bezpečnosti, a preto by každý systém certifikácie mal byť navrhnutý tak, aby nemohol byť skoro zastaraný.

(73) Komisia by mala byť splnomocnená na prijímanie európskych systémov certifikácie kybernetickej bezpečnosti v súvislosti s konkrétnymi skupinami produktov IKT, služieb IKT a procesov IKT. Implementáciu týchto systémov a dozor nad nimi by mali vykonávať vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti, pričom certifikáty vydané podľa týchto systémov by mali byť platné a uznávané v celej Únii. Toto nariadenie by sa nemalo vzťahovať na certifikačné systémy, ktoré prevádzkuje príslušné odvetvie alebo iné súkromné organizácie. Orgánom, ktoré takéto systémy prevádzkujú, by sa však malo umožniť Komisii navrhnúť, aby zvážila použitie týchto systémov ako základu pre ich schválenie ako európskeho systému certifikácie kybernetickej bezpečnosti.

(74) Ustanoveniami tohto nariadenia by nemali byť dotknuté právne predpisy Únie stanovujúce konkrétne pravidlá certifikácie produktov IKT, služieb IKT a procesov IKT. Konkrétne v nariadení (EÚ) 2016/679 sa stanovuje zavedenie certifikačných mechanizmov, ako aj pečatí a značiek ochrany údajov na preukázanie súladu spracovateľských operácií prevádzkovateľov a sprostredkovateľov s uvedeným nariadením. Tieto certifikačné mechanizmy, ako aj pečate a značky ochrany údajov, by mali dotknutým osobám umožniť rýchle vyhodnotiť, nakoľko príslušné produkty IKT, služby IKT a procesy IKT chránia údaje. Týmto nariadením nie je dotknutá certifikácia operácií spracúvania údajov podľa nariadenia (EÚ) 2016/679, čo platí aj pre prípady, keď sú takéto operácie súčasťou produktov IKT, služieb IKT a procesov IKT.

(75) Účelom európskych systémov certifikácie kybernetickej bezpečnosti by malo byť, že sa zabezpečí, aby produkty IKT, služby IKT a procesy IKT, ktoré boli certifikované takýmto systémom, spĺňali uvedené požiadavky s cieľom chrániť dostupnosť, pravosť, integritu a dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich funkcií či služieb, ktoré tieto produkty, služby a procesy poskytujú alebo sprístupňujú, a to počas ich celého životného cyklu. V tomto nariadení nie je možné stanoviť podrobné požiadavky kybernetickej bezpečnosti pre všetky produkty IKT, služby IKT a procesy IKT. Produkty IKT, služby IKT a procesy IKT, ako aj potreby v oblasti kybernetickej bezpečnosti týkajúce sa uvedených produktov, služieb a procesov, sú také rozmanité, že je veľmi ťažké stanoviť všeobecné požiadavky kybernetickej bezpečnosti, ktoré by sa dali uplatniť za každých okolností. Je preto potrebné prijať široký a všeobecný koncept kybernetickej bezpečnosti na účely certifikácie, ktorý by mal byť doplnený súborom špecifických cieľov kybernetickej bezpečnosti, ktoré treba zohľadniť pri navrhovaní európskych systémov certifikácie kybernetickej bezpečnosti. Spôsoby, ktorými sa tieto ciele majú dosiahnuť pri konkrétnych produktoch IKT, službách IKT a procesoch IKT, by sa potom mali podrobne vymedziť na úrovni príslušného certifikačného systému prijatého Komisiou, napríklad odkazom na normy alebo technické špecifikácie, ak vhodné normy nie sú k dispozícii.

(76) Pri určovaní technických špecifikácií, ktoré sa majú použiť v európskych systémoch certifikácie kybernetickej bezpečnosti, by sa mali dodržiavať požiadavky stanovené v prílohe II k nariadeniu Európskeho parlamentu a Rady (EÚ) č. 1025/2012 ([19]). Niektoré odchýlky od týchto požiadaviek by sa však mohli považovať za potrebné v riadne odôvodnených prípadoch, ak sa tieto technické špecifikácie majú využívať v európskom systéme certifikácie kybernetickej bezpečnosti, ktorý sa vzťahuje na stupeň dôveryhodnosti „vysoký“. Dôvody týchto odchýlok by sa mali zverejniť.

(77) Certifikované posudzovanie zhody je proces hodnotenia, či boli uvedené požiadavky týkajúce sa produktu IKT, služby IKT alebo procesu IKT splnené. Tento proces vykonáva nezávislá tretia strana, ktorá nie je výrobcom ani poskytovateľom produktov IKT, služieb IKT alebo procesov IKT, ktoré sa posudzujú. Európsky certifikát kybernetickej bezpečnosti by mal byť vydaný po úspešnom hodnotení produktu IKT, služby IKT alebo procesu IKT. Európsky certifikát kybernetickej bezpečnosti by sa mal považovať za potvrdenie, že hodnotenie bolo vykonané správne. V závislosti od stupňa dôveryhodnosti by mal európsky systém certifikácie kybernetickej bezpečnosti uvádzať, či európsky certifikát kybernetickej bezpečnosti vydal súkromný alebo verejný subjekt. Posudzovanie zhody a certifikácia nemôžu samy osebe zaručiť, že certifikované produkty IKT, služby IKT a procesy IKT sú kyberneticky bezpečné. Namiesto toho ide o postupy a technické metodiky na potvrdenie toho, že produkty IKT, služby IKT a procesy IKT boli preskúšané a spĺňajú určité požiadavky kybernetickej bezpečnosti stanovené inde, napríklad v technických normách.

(78) Užívatelia európskych certifikátov kybernetickej bezpečnosti by si mali vhodnú certifikáciu a súvisiace bezpečnostné požiadavky vyberať na základe analýzy rizika spojeného s využívaním produktu IKT, služby IKT alebo procesu IKT. Stupeň dôveryhodnosti by mal zodpovedať úrovni rizika spojeného s plánovaným využívaním daného produktu IKT, služby IKT alebo procesu IKT.

([19]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho 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 ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12).

(79) Európske systémy certifikácie kybernetickej bezpečnosti by mohli umožňovať, aby sa posudzovanie zhody vykonávalo na výhradnú zodpovednosť výrobcu alebo poskytovateľa produktov IKT, služieb IKT alebo procesov IKT (ďalej len „vlastné posúdenie zhody“). V takýchto prípadoch by malo stačiť, aby výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT vykonal všetky kontroly sám s cieľom zabezpečiť zhodu produktov IKT, služieb IKT alebo procesov IKT s európskym systémom certifikácie kybernetickej bezpečnosti. Vlastné posúdenie zhody by sa malo považovať za vhodné pre menej zložité produkty IKT, služby IKT alebo procesy IKT, ktoré predstavujú nízke riziko z hľadiska verejného záujmu, napríklad z dôvodu jednoduchého dizajnu a produkčných mechanizmov. Okrem toho by vlastné posúdenie zhody malo byť dovolené len pre produkty IKT, služby IKT alebo procesy IKT, ktoré zodpovedajú stupňu dôveryhodnosti „základný“.

(80) Európske systémy certifikácie kybernetickej bezpečnosti by mohli umožňovať vlastné posúdenia zhody a certifikácie produktov IKT, služieb IKT alebo procesov IKT. V takomto prípade by mal systém poskytovať jasné a zrozumiteľné prostriedky, ktoré by spotrebiteľom alebo iným užívateľom umožnili rozlišovať medzi produktmi IKT, službami IKT alebo procesmi IKT, v súvislosti s ktorými je výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT zodpovedný za posúdenie, a produktmi IKT, službami IKT a procesmi IKT, ktoré certifikuje tretia strana.

(81) Výrobcovi alebo poskytovateľovi produktov IKT, služieb IKT alebo procesov IKT, ktorý vykonáva vlastné posúdenie zhody, by sa malo umožniť vydávať a podpisovať EÚ vyhlásenie o zhode ako súčasť postupu posudzovania zhody. EÚ vyhlásenie o zhode je dokument, v ktorom sa uvádza, že konkrétny produkt IKT, služba IKT alebo proces IKT spĺňa požiadavky európskeho systému certifikácie kybernetickej bezpečnosti. Vydaním a podpisom EÚ vyhlásenia o zhode preberá výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT zodpovednosť za súlad produktu IKT, služby IKT alebo procesu IKT s právnymi požiadavkami európskeho systému certifikácie kybernetickej bezpečnosti. Kópia EÚ vyhlásenia o zhode by sa mala odovzdať vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti a agentúre ENISA.

(82) Výrobcovia alebo poskytovatelia produktov IKT, služieb IKT alebo procesov IKT by mali mať EÚ vyhlásenie o zhode, technickú dokumentáciu a všetky ďalšie relevantné informácie, ktoré sa týkajú zhody produktov IKT, služieb IKT alebo procesov IKT s európskym systémom certifikácie kybernetickej bezpečnosti, k dispozícii pre príslušný vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti počas obdobia stanoveného v príslušnom európskom systéme certifikácie kybernetickej bezpečnosti. V technickej dokumentácii by sa mali uviesť uplatniteľné požiadavky podľa systému a mala by zahŕňať návrh, výrobu a používanie produktu IKT, služby IKT alebo procesu IKT v rozsahu relevantnom pre vlastné posúdenie zhody. Technická dokumentácia by mala byť zostavená tak, aby bolo možné vykonať posúdenie súladu produktu IKT, služby IKT alebo procesu IKT s požiadavkami uplatniteľnými podľa uvedeného systému.

(83) Pri správe európskeho rámca certifikácie kybernetickej bezpečnosti sa zohľadňuje zapojenie členských štátov, ako aj vhodné zapojenie zainteresovaných strán a stanovuje sa úloha Komisie počas plánovania a navrhovania európskych systémov certifikácie kybernetickej bezpečnosti, podávania žiadosti o ne, ich prípravy, prijímania a preskúmavania.

(84) Komisia by mala pripraviť priebežný pracovný program Únie pre európske systémy certifikácie kybernetickej bezpečnosti, a to s podporou európskej skupiny pre certifikáciu kybernetickej bezpečnosti (ďalej len „ECCG“ – European Cybersecurity Certification Group) a skupiny zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti a po otvorených a rozsiahlych konzultáciách, a mala by ho uverejniť vo forme nezáväzného nástroja. Priebežný pracovný program Únie by mal byť strategickým dokumentom, ktorý by najmä príslušnému odvetviu, vnútroštátnym orgánom a orgánom pre normalizáciu umožnil vopred sa pripraviť na budúce európske systémy certifikácie kybernetickej bezpečnosti. Priebežný pracovný program Únie by mal zahŕňať viacročný prehľad žiadostí, ktoré sa týkajú kandidátskych systémov a ktoré má Komisia v úmysle predložiť agentúre ENISA na účely prípravy na základe špecifických dôvodov. Komisia by mala priebežný pracovný program Únie zohľadniť pri príprave priebežného plánu normalizácie IKT a normalizačných žiadostí adresovaných európskym normalizačným organizáciám. Vzhľadom na rýchle zavádzanie nových technológií a ich využívanie užívateľmi a spoločnosťami, vznik predtým neznámych kybernetickobezpečnostných rizík a legislatívny vývoj a vývoj trhu by Komisia alebo ECCG mala byť oprávnená požiadať agentúru ENISA o prípravu kandidátskych systémov, ktoré neboli zahrnuté do priebežného pracovného programu Únie. V takýchto prípadoch by Komisia a ECCG mali tiež posúdiť nevyhnutnosť takejto žiadosti, pričom zohľadnia celkové zámery a ciele tohto nariadenia a potrebu zabezpečiť kontinuitu agentúry ENISA z hľadiska plánovania a využívania zdrojov.

Po predložení takej žiadosti by agentúra ENISA mala bez zbytočného odkladu pripraviť kandidátske systémy pre konkrétne produkty IKT, služby IKT a procesy IKT. Komisia by mala vyhodnotiť pozitívny a negatívny vplyv svojej žiadosti na konkrétny dotknutý trh, najmä na MSP, inováciu, prekážky vstupu na uvedený trh a náklady koncových užívateľov. Komisia by mala byť splnomocnená prijať prostredníctvom vykonávacích aktov európsky systém certifikácie kybernetickej bezpečnosti, ktorý by sa zakladal na kandidátskom systéme pripravenom agentúrou ENISA. Európske systémy certifikácie kybernetickej bezpečnosti prijaté Komisiou by mali uvádzať minimálny súbor prvkov, ktoré sa vzťahujú na zameranie, rozsah a fungovanie daného systému, pričom sa v nich zohľadní všeobecný účel a bezpečnostné ciele stanovené v tomto nariadení. Medzi uvedené prvky by mal okrem iného patriť rozsah a predmet certifikácie kybernetickej bezpečnosti vrátane kategórií pokrytých produktov IKT, služieb IKT a procesov IKT, podrobného vymedzenia požiadaviek kybernetickej bezpečnosti (napríklad v podobe odkazu na normy alebo technické špecifikácie), konkrétnych hodnotiacich kritérií a hodnotiacich metód, ako aj cieľového stupňa dôveryhodnosti („základný“, „pokročilý“ alebo „vysoký“) a prípadných stupňov hodnotenia. Agentúre ENISA by sa malo umožniť odmietnuť žiadosť ECCG. Takéto rozhodnutia by mala prijímať správna rada a malo by byť riadne odôvodnené.

(85) Agentúra ENISA by mala udržiavať webové sídlo, na ktorom by sa poskytovali informácie o európskych systémoch certifikácie kybernetickej bezpečnosti a prostredníctvom ktorého by sa propagovali, pričom by sa na ňom okrem iného uvádzali žiadosti o prípravu kandidátskeho systému, ako aj spätná väzba v rámci procesu konzultácií, ktorý uskutočňuje agentúra ENISA v prípravnej fáze. Toto webové sídlo by malo poskytovať aj informácie o európskych certifikátoch kybernetickej bezpečnosti a EÚ vyhláseniach o zhode vydaných podľa tohto nariadenia vrátane informácií o odňatí a skončení platnosti takýchto európskych certifikátov kybernetickej bezpečnosti a EÚ vyhlásení o zhode. Na tomto webovom sídle by sa tiež mali uvádzať vnútroštátne systémy certifikácie kybernetickej bezpečnosti, ktoré boli nahradené európskym systémom certifikácie kybernetickej bezpečnosti.

(86) Stupeň dôveryhodnosti európskeho systému certifikácie je základ pre presvedčenie, že produkt IKT, služba IKT alebo proces IKT spĺňa bezpečnostné požiadavky konkrétneho európskeho systému certifikácie kybernetickej bezpečnosti. S cieľom zabezpečiť konzistentnosť európskeho rámca certifikácie kybernetickej bezpečnosti by sa európskemu systému certifikácie kybernetickej bezpečnosti malo umožniť špecifikovať stupne dôveryhodnosti pre európske certifikáty kybernetickej bezpečnosti a EÚ vyhlásenia o zhode vydané v rámci daného systému. Každý európsky certifikát kybernetickej bezpečnosti by mohol uvádzať jeden zo stupňov dôveryhodnosti: „základný“, „pokročilý“ alebo „vysoký“, pričom EÚ vyhlásenie o zhode by mohlo uvádzať len stupeň dôveryhodnosti „základný“. Stupne dôveryhodnosti by uvádzali zodpovedajúcu prísnosť a hĺbku hodnotenia produktu IKT, služby IKT alebo procesu IKT a boli by charakterizované odkazom na súvisiace technické špecifikácie, normy a postupy vrátane technických kontrol, ktorých účelom je predchádzať incidentom alebo zmierňovať ich následky. Všetky stupne dôveryhodnosti by sa mali používať konzistentne v jednotlivých sektorových oblastiach, v ktorých sa uplatňuje certifikácia.

(87) Európsky systém certifikácie kybernetickej bezpečnosti by mohol špecifikovať niekoľko stupňov hodnotenia v závislosti od prísnosti a hĺbky použitej metodiky hodnotenia. Stupne hodnotenia by mali zodpovedať jednému zo stupňov dôveryhodnosti a mali by byť spojené s vhodnou kombináciou zložiek dôveryhodnosti. Produkt IKT, služba IKT alebo proces IKT by mali v prípade všetkých stupňov dôveryhodnosti obsahovať niekoľko zabezpečených funkcií stanovených v systéme, ktoré by mohli zahŕňať: konfiguráciu zabezpečenia na priame použitie, podpísaný programovací kód, zabezpečenú aktualizáciu a zmierňovanie následkov zneužitia bezpečnostných dier (exploits) a plnú ochranu dynamicky alebo staticky prideľovanej pamäte (stack/heap). Tieto funkcie by sa mali vyvinúť a potom udržiavať vývojovým prístupom zameraným na bezpečnosť a súvisiacimi nástrojmi s cieľom zaručiť spoľahlivé zapracovanie účinných softvérových a hardvérových mechanizmov.

(88) Pri stupni dôveryhodnosti „základný“ by sa hodnotenie malo riadiť aspoň týmito zložkami dôveryhodnosti: hodnotenie by malo zahŕňať aspoň preskúmanie technickej dokumentácie k produktu IKT, službe IKT alebo procesu IKT orgánom posudzovania zhody. Ak certifikácia zahŕňa procesy IKT, technické preskúmanie by sa malo vzťahovať aj na proces navrhovania, vývoja a údržby produktu IKT alebo služby IKT. Ak európsky systém certifikácie kybernetickej bezpečnosti stanovuje vlastné posúdenie zhody, malo by stačiť, že výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT vykonal vlastné posúdenie súladu produktu IKT, služby IKT alebo procesu IKT s certifikačným systémom.

(89) Pri stupni dôveryhodnosti „pokročilý“ by sa hodnotenie malo okrem požiadaviek stupňa dôveryhodnosti „základný“ riadiť aspoň overením súladu bezpečnostných funkcií produktu IKT, služby IKT alebo procesu IKT s ich technickou dokumentáciou.

(90) Pri stupni dôveryhodnosti „vysoký“ by sa hodnotenie malo okrem požiadaviek stupňa dôveryhodnosti „pokročilý“ riadiť aspoň skúškou účinnosti, ktorou sa posúdi odolnosť bezpečnostných funkcií produktu IKT, služby IKT alebo procesu IKT proti zložitým kybernetickým útokom, ktoré sú vedené osobami s významnými zručnosťami a zdrojmi.

(91) Využívanie európskej certifikácie kybernetickej bezpečnosti a EÚ vyhlásenia o zhode by malo ostať dobrovoľné, pokiaľ sa nestanovuje inak v práve Únie alebo v práve členských štátov prijatom v súlade s právom Únie. Ak neexistuje harmonizované právo Únie, členským štátom by sa malo umožniť prijať vnútroštátne technické predpisy, ktorými stanovia povinnú certifikáciu podľa európskeho systému certifikácie kybernetickej bezpečnosti v súlade so smernicou Európskeho parlamentu a Rady (EÚ) 2015/1535 ([20]). Členské štáty tiež majú k dispozícii európsku certifikáciu kybernetickej bezpečnosti aj v súvislosti s verejným obstarávaním a so smernicou Európskeho parlamentu a Rady 2014/24/EÚ ([21]).

(92) V niektorých oblastiach by mohlo byť v budúcnosti nevyhnutné v prípade určitých produktov IKT, služieb IKT alebo procesov IKT stanoviť špecifické požiadavky kybernetickej bezpečnosti a stanoviť povinnosť ich certifikácie s cieľom zvýšiť úroveň kybernetickej bezpečnosti v Únii. Komisia by mala pravidelne sledovať vplyv prijatých európskych systémov certifikácie kybernetickej bezpečnosti na dostupnosť bezpečných produktov IKT, služieb IKT a procesov IKT na vnútornom trhu a vyhodnocovať úroveň využívania certifikačných systémov výrobcami alebo poskytovateľmi produktov IKT, služieb IKT alebo procesov IKT v Únii. Účinnosť európskych systémov certifikácie kybernetickej bezpečnosti a to, či by konkrétne systémy mali byť záväzné, by sa malo posudzovať z hľadiska právnych predpisov Únie týkajúcich sa kybernetickej bezpečnosti, najmä smernice (EÚ) 2016/1148, pričom sa zohľadní bezpečnosť sietí a informačných systémov, ktoré používajú prevádzkovatelia základných služieb.

(93) Európske certifikáty kybernetickej bezpečnosti a EÚ vyhlásenia o zhode by mali pomôcť koncovým užívateľom robiť informované rozhodnutia. K produktom IKT, službám IKT a procesom IKT, ktoré boli certifikované alebo pre ktoré bolo vydané EÚ vyhlásenie o zhode, by mali byť pripojené štruktúrované informácie prispôsobené očakávanej technickej úrovni koncového užívateľa, ktorému sú určené. Všetky takéto informácie by mali byť k dispozícii online a prípadne vo fyzickej podobe. Koncový užívateľ by mal mať prístup k informáciám týkajúcim sa referenčného čísla certifikačného systému, stupňa dôveryhodnosti, opisu kybernetickobezpečnostných rizík spojených s produktom IKT, službou IKT alebo procesom IKT a vydávajúceho orgánu alebo subjektu, alebo by sa mu malo umožniť získať kópiu európskeho certifikátu kybernetickej bezpečnosti. Okrem toho by koncový užívateľ mal byť informovaný o podpornom programe výrobcu alebo poskytovateľa produktov IKT, služieb IKT alebo procesov IKT v oblasti kybernetickej bezpečnosti, najmä ako dlho bude môcť koncový užívateľ dostávať kybernetickobezpečnostné aktualizácie alebo opravy. V príslušných prípadoch by sa malo poskytovať poradenstvo o opatreniach alebo nastaveniach, ktoré môže koncový užívateľ vykonať na zachovanie alebo posilnenie kybernetickej bezpečnosti produktu IKT alebo služby IKT, a kontaktné informácie o jednotnom kontaktnom mieste na oznamovanie kybernetických útokov a získanie podpory, keď sa vyskytnú (okrem automatického oznamovania). Uvedené informácie by sa mali pravidelne aktualizovať a sprístupňovať na webovom sídle poskytujúcom informácie o európskych systémoch certifikácie kybernetickej bezpečnosti.

(94) Aby sa dosiahli ciele tohto nariadenia a aby sa predišlo fragmentácii vnútorného trhu, účinnosť vnútroštátnych systémov alebo postupov certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT alebo procesov IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, by mala skončiť k dátumu, ktorý stanoví Komisia vo vykonávacích aktoch. Okrem toho by členské štáty nemali zavádzať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT alebo procesov IKT, na ktoré sa už vzťahuje existujúci európsky systém certifikácie kybernetickej bezpečnosti. Členským štátom by sa však nemalo brániť prijímať alebo zachovať vnútroštátne systémy certifikácie kybernetickej bezpečnosti na účely národnej bezpečnosti. Členské štáty by mali informovať Komisiu a ECCG o každom úmysle vypracovať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti. Komisia a ECCG by mali posúdiť vplyv nových vnútroštátnych systémov certifikácie kybernetickej bezpečnosti na riadne fungovanie vnútorného trhu a vzhľadom na strategický záujem požadovať namiesto nich európsky systém certifikácie kybernetickej bezpečnosti.

(95) Európske systémy certifikácie kybernetickej bezpečnosti sú určené na harmonizáciu postupov kybernetickej bezpečnosti v Únii. Majú prispieť k zvýšeniu úrovne kybernetickej bezpečnosti v Únii. Koncepcia európskych systémov certifikácie kybernetickej bezpečnosti by mala zohľadňovať a umožňovať rozvoj inovácií v oblasti kybernetickej bezpečnosti.

([20]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/1535 z 9. septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (Ú. v. EÚ L 241, 17.9.2015, s. 1).

([21]) Smernica Európskeho parlamentu a Rady 2014/24/EÚ z 26. februára 2014 o verejnom obstarávaní a o zrušení smernice 2004/18/ES (Ú. v. EÚ L 94, 28.3.2014, s. 65).

(96) Európske systémy certifikácie kybernetickej bezpečnosti by mali zohľadňovať súčasné metódy vývoja softvéru a hardvéru, a najmä vplyv častých softvérových alebo firmvérových aktualizácií na jednotlivé európske certifikáty kybernetickej bezpečnosti. Európske systémy certifikácie kybernetickej bezpečnosti by mali špecifikovať podmienky, za ktorých si môže aktualizácia vyžadovať novú certifikáciu produktu IKT, služby IKT alebo procesu IKT alebo zúženie rozsahu konkrétneho európskeho certifikátu kybernetickej bezpečnosti pri zohľadnení akýchkoľvek nepriaznivých účinkov aktualizácie na súlad s bezpečnostnými požiadavkami uvedeného certifikátu.

(97) Po prijatí európskeho systému certifikácie kybernetickej bezpečnosti by výrobcovia alebo poskytovatelia produktov IKT, služieb IKT alebo procesov IKT mali mať možnosť podávať žiadosti o certifikáciu svojich produktov IKT alebo služieb IKT ktorémukoľvek nimi zvolenému orgánu posudzovania zhody kdekoľvek v Únii. Orgány posudzovania zhody by mal akreditovať vnútroštátny akreditačný orgán, ak spĺňajú určité konkrétne požiadavky stanovené v tomto nariadení. Akreditácia by sa mala vydávať najviac na päť rokov a malo by byť možné ju obnoviť za rovnakých podmienok, pokiaľ orgán posudzovania zhody naďalej spĺňa požiadavky. Vnútroštátne akreditačné orgány by mali akreditáciu orgánu posudzovania zhody obmedziť, pozastaviť jej platnosť alebo ju zrušiť, ak orgán posudzovania zhody nespĺňa alebo prestal spĺňať akreditačné podmienky, alebo ak porušuje toto nariadenie.

(98) Existencia odkazov vo vnútroštátnych právnych predpisoch na vnútroštátne normy, ktorých účinnosť sa skončila v dôsledku nadobudnutia účinnosti európskeho systému certifikácie kybernetickej bezpečnosti, môže byť zdrojom nejasností. Členské štáty by preto mali prijatie európskeho systému certifikácie kybernetickej bezpečnosti premietnuť do svojich vnútroštátnych právnych predpisov.

(99) S cieľom dosiahnuť uplatňovanie rovnocenných noriem v celej Únii, uľahčiť vzájomné uznávanie a podporovať celkovú akceptáciu európskych certifikátov kybernetickej bezpečnosti a EÚ vyhlásení o zhode je potrebné zaviesť systém partnerského preskúmania medzi vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti. Partnerské preskúmanie by sa malo vzťahovať na postupy pre dozor nad súladom produktov IKT, služieb IKT a procesov IKT s európskymi certifikátmi kybernetickej bezpečnosti, pre monitorovanie povinností výrobcov alebo poskytovateľov produktov IKT, služieb IKT alebo procesov IKT, ktorí vykonávajú vlastné posúdenie zhody, pre monitorovanie orgánov posudzovania zhody, ako aj primeranosti odborných znalostí personálu orgánov, ktoré vydávajú certifikáty pre stupeň dôveryhodnosti „vysoký“. Komisii by sa malo umožniť vo vykonávacích aktoch stanoviť minimálne päťročný plán pre partnerské preskúmanie a tiež stanoviť kritéria a metodiky fungovania systému partnerského preskúmania.

(100) Bez toho, aby bol dotknutý všeobecný systém partnerského preskúmania, ktorý majú v rámci európskeho rámca certifikácie kybernetickej bezpečnosti zaviesť všetky vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti, niektoré európske systémy certifikácie kybernetickej bezpečnosti môžu zahŕňať mechanizmus partnerského preskúmania určený orgánom, ktoré v rámci týchto systémov vydávajú európske certifikáty kybernetickej bezpečnosti pre produkty IKT, služby IKT a procesy IKT so stupňom dôveryhodnosti „vysoký“. ECCG by mala podporovať implementáciu takýchto mechanizmov partnerského preskúmania. Takýmito partnerskými preskúmaniami by sa malo najmä posudzovať, či dotknuté orgány vykonávajú svoje úlohy harmonizovane, pričom môžu zahŕňať mechanizmy odvolania. Výsledky partnerských preskúmaní by sa mali uverejniť. Dotknuté orgány môžu prijať vhodné opatrenia na prispôsobenie svojich postupov a odborných znalostí.

(101) Členské štáty by mali určiť jeden alebo viacero vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti na účely dozoru nad plnením povinností vyplývajúcich z tohto nariadenia. Vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti môže byť existujúci alebo novozriadený orgán. Členský štát by tiež mal mať možnosť určiť po vzájomnej dohode s iným členským štátom jeden alebo viacero vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti na území takéhoto iného členského štátu.

(102) Vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti by mali najmä monitorovať a presadzovať plnenie povinností výrobcov alebo poskytovateľov produktov IKT, služieb IKT alebo procesov IKT usadených na ich príslušných územiach, ktoré súvisia s EÚ vyhlásením o zhode, mali by pomáhať vnútroštátnym akreditačným orgánom pri monitorovaní činnosti orgánov posudzovania zhody a dozore nad nimi tým, že im poskytujú odborné znalosti a relevantné informácie, mali by oprávňovať orgány posudzovania zhody vykonávať ich úlohy, ak orgány posudzovania zhody spĺňajú dodatočné požiadavky stanovené v európskom systéme certifikácie kybernetickej bezpečnosti, a mali by monitorovať relevantný vývoj v oblasti certifikácie kybernetickej bezpečnosti. Vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti by tiež mali vybavovať sťažnosti fyzických alebo právnických osôb v súvislosti s európskymi certifikátmi kybernetickej bezpečnosti, ktoré uvedené orgány vydali,

alebo v súvislosti s európskymi certifikátmi kybernetickej bezpečnosti, ktoré vydali orgány posudzovania zhody, ak takéto certifikáty uvádzajú stupeň dôveryhodnosti „vysoký“, mali by v primeranom rozsahu prešetriť predmet danej sťažnosti a sťažovateľa v primeranej lehote informovať o pokroku a výsledku tohto prešetrenia. Okrem toho by vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti mali spolupracovať s inými vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti alebo ďalšími orgánmi verejnej moci vrátane poskytovania informácií o možnom nesúlade produktov IKT, služieb IKT a procesov IKT s požiadavkami tohto nariadenia alebo konkrétnymi európskymi systémami certifikácie kybernetickej bezpečnosti. Komisia by mala uľahčiť toto zdieľanie informácií tým, že sprístupní všeobecný elektronický podporný informačný systém, napríklad Informačný a komunikačný systém pre dohľad nad trhom (ICSMS) a systém na rýchlu výmenu informácií o nebezpečných nepotravinových výrobkoch (RAPEX), ktoré už používajú orgány dohľadu nad trhom podľa nariadenia (ES) č. 765/2008.

(103) V záujme konzistentného uplatňovania európskeho rámca certifikácie kybernetickej bezpečnosti by sa mala zriadiť ECCG zložená zo zástupcov vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti alebo iných príslušných vnútroštátnych orgánov. Medzi hlavné úlohy ECCG by mali patriť poradenstvo a pomoc Komisii v jej úsilí o zabezpečenie konzistentného vykonávania a uplatňovania európskeho rámca certifikácie kybernetickej bezpečnosti, pomoc agentúre ENISA a úzka spolupráca s ňou pri príprave kandidátskych systémov certifikácie kybernetickej bezpečnosti, v riadne odôvodnených prípadoch požadovanie od agentúry ENISA, aby pripravila kandidátsky systém, prijímanie stanovísk pre agentúru ENISA, pokiaľ ide o kandidátske systémy, a prijímanie stanovísk pre Komisiu k udržiavaniu a prehodnocovaniu existujúcich európskych systémov certifikácie kybernetickej bezpečnosti. ECCG by mala uľahčovať výmenu osvedčených postupov a odborných znalostí medzi rôznymi vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti zodpovednými za oprávňovanie orgánov posudzovania zhody a vydávanie európskych certifikátov kybernetickej bezpečnosti.

(104) Na zvýšenie povedomia o budúcich európskych systémoch certifikácie kybernetickej bezpečnosti a uľahčenie ich akceptácie môže Komisia vydať všeobecné či odvetvové kybernetickobezpečnostné usmernenia, napríklad o osvedčených postupoch alebo zodpovednom správaní sa v oblasti kybernetickej bezpečnosti, pričom sa zdôrazní pozitívny účinok využívania certifikovaných produktov IKT, služieb IKT a procesov IKT.

(105) S cieľom ďalej uľahčovať obchod a uznávajúc, že dodávateľské reťazce IKT sú globálne, môže Únia v súlade s článkom 218 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“) uzatvárať dohody o vzájomnom uznávaní týkajúce sa európskych certifikátov kybernetickej bezpečnosti. Komisia môže s prihliadnutím na poradenstvo od agentúry ENISA a európskej skupiny pre certifikáciu kybernetickej bezpečnosti odporučiť začatie príslušných rokovaní. V rámci každého európskeho systému certifikácie kybernetickej bezpečnosti by sa mali stanoviť konkrétne podmienky takéhoto vzájomného uznávania dohôd s tretími krajinami.

(106) S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia by sa mali na Komisiu preniesť vykonávacie právomoci. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011 ([22]).

(107) Postup preskúmania by sa mal uplatniť pri prijímaní vykonávacích aktov o európskych systémoch certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT alebo procesov IKT; pri prijímaní vykonávacích aktov o spôsoboch vykonávania šetrenia zo strany agentúry ENISA; pri prijímaní vykonávacích aktov o pláne partnerského preskúmania vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti, ako aj pri prijímaní vykonávacích aktov o okolnostiach, formátoch a postupoch, ktoré uplatňujú vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti, keď Komisii oznamujú akreditované orgány posudzovania zhody.

(108) Činnosť agentúry ENISA by sa mala pravidelne a nezávisle vyhodnocovať. Toto hodnotenie by sa malo vzťahovať na plnenie cieľov agentúry ENISA, jej pracovné postupy a relevantnosť jej úloh, najmä tých, ktoré sa týkajú operačnej spolupráce na úrovni Únie. Zároveň by sa v uvedenom hodnotení mal posúdiť dosah, efektívnosť a účinnosť európskeho rámca certifikácie kybernetickej bezpečnosti. V prípade preskúmania by Komisia mala posúdiť, akým spôsobom možno posilniť úlohu agentúry ENISA ako referenčného bodu pre poradenstvo a odborné znalosti a tiež by mala posúdiť možnú úlohu agentúry ENISA pri podpore hodnotenia produktov IKT, služieb IKT a procesov IKT tretích krajín, keď takéto produkty, služby a procesy vstupujú do Únie a nie sú v súlade s pravidlami Únie.

([22]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

(109) Keďže ciele tohto nariadenia nie je možné uspokojivo dosiahnuť na úrovni členských štátov, ale z dôvodu ich rozsahu a dôsledkov ich možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii (ďalej len „Zmluva o EÚ“). V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie týchto cieľov.

(110) Nariadenie (EÚ) č. 526/2013 by sa malo zrušiť,

PRIJALI TOTO NARIADENIE:

HLAVA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

1. S cieľom zaistiť riadne fungovanie vnútorného trhu a zároveň usilovať sa o dosiahnutie vysokej úrovne kybernetickej bezpečnosti, kybernetickej odolnosti a dôvery v rámci Únie, sa týmto nariadením stanovujú:

a) ciele, úlohy a organizačné aspekty týkajúce sa agentúry ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a

b) rámec pre zavádzanie európskych systémov certifikácie kybernetickej bezpečnosti na zabezpečenie primeranej úrovne kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT v Únii, ako aj na predídenie fragmentácii vnútorného trhu z hľadiska systémov certifikácie kybernetickej bezpečnosti v Únii.

Rámec uvedený v písmene b) prvého pododseku sa uplatňuje bez toho, aby mal vplyv na konkrétne ustanovenia v iných právnych aktoch Únie, ktoré sa týkajú dobrovoľnej alebo povinnej certifikácie.

2. Týmto nariadením nie sú dotknuté právomoci členských štátov týkajúce sa činností spojených s verejnou bezpečnosťou, obranou, národnou bezpečnosťou a činností štátu v oblasti trestného práva.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňujú tieto vymedzenia pojmov:

1. „kybernetická bezpečnosť“ sú činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami;

2. „sieť a informačný systém“ je sieť a informačný systém vymedzený v článku 4 bode 1 smernice (EÚ) 2016/1148;

3. „národná stratégia v oblasti bezpečnosti sietí a informačných systémov“ je národná stratégia v oblasti bezpečnosti sietí a informačných systémov vymedzená v článku 4 bode 3 smernice (EÚ) 2016/1148;

4. „prevádzkovateľ základných služieb“ je prevádzkovateľ základných služieb vymedzený v článku 4 bode 4 smernice (EÚ) 2016/1148;

5. „poskytovateľ digitálnych služieb“ je poskytovateľ digitálnych služieb vymedzený v článku 4 bode 6 smernice (EÚ) 2016/1148;

6. „incident“ je incident vymedzený v článku 4 bode 7 smernice (EÚ) 2016/1148;

7. „riešenie incidentov“ je riešenie incidentov vymedzené v článku 4 bode 8 smernice (EÚ) 2016/1148;

8. „kybernetická hrozba“ je každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby;

9. „európsky systém certifikácie kybernetickej bezpečnosti“ je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov, ktoré sú stanovené na úrovni Únie a ktoré sa uplatňujú na certifikáciu alebo posudzovanie zhody konkrétnych produktov IKT, služieb IKT alebo procesov IKT;

10. „vnútroštátny systém certifikácie kybernetickej bezpečnosti“ je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov vypracovaných a prijatých vnútroštátnym orgánom verejnej moci a uplatňovaných pri certifikácii alebo posudzovaní zhody produktov IKT, služieb IKT a procesov IKT v rozsahu pôsobnosti príslušného systému;

11. „európsky certifikát kybernetickej bezpečnosti“ je dokument, ktorý vydal príslušný orgán a ktorým sa potvrdzuje, že daný produkt IKT, služba IKT alebo proces IKT bol predmetom hodnotenia, pokiaľ ide o súlad s konkrétnymi bezpečnostnými požiadavkami stanovenými v európskom systéme certifikácie kybernetickej bezpečnosti;

12. „produkt IKT“ je prvok alebo skupina prvkov siete alebo informačného systému;

13. „služba IKT“ je služba pozostávajúca úplne alebo prevažne z prenosu, ukladania, získavania alebo spracúvania informácií prostredníctvom sietí a informačných systémov;

14. „proces IKT“ je súbor činností vykonávaných pre navrhnutie, vyvinutie, poskytnutie alebo údržbu produktu IKT alebo služby IKT;

15. „akreditácia“ je akreditácia vymedzená v článku 2 bode 10 nariadenia (ES) č. 765/2008;

16. „vnútroštátny akreditačný orgán“ je vnútroštátny akreditačný orgán vymedzený v článku 2 bode 11 nariadenia (ES) č. 765/2008;

17. „posudzovanie zhody“ je posudzovanie zhody vymedzené v článku 2 bode 12 nariadenia (ES) č. 765/2008;

18. „orgán posudzovania zhody“ je orgán posudzovania zhody vymedzený v článku 2 bode 13 nariadenia (ES) č. 765/2008;

19. „norma“ je norma vymedzená v článku 2 bode 1 nariadenia (EÚ) č. 1025/2012;

20. „technická špecifikácia“ je dokument, v ktorom sa predpisujú technické požiadavky, ktoré musí spĺňať produkt IKT, služba IKT alebo proces IKT, alebo postupy posudzovania zhody týkajúce sa produktu IKT, služby IKT alebo procesu IKT;

21. „stupeň dôveryhodnosti“ je základ pre presvedčenie, že produkt IKT, služba IKT alebo proces IKT spĺňa bezpečnostné požiadavky konkrétneho európskeho systému certifikácie kybernetickej bezpečnosti, uvádza úroveň, na akej sa produkt IKT, služba IKT alebo proces IKT hodnotil, ale ako taký nemeria bezpečnosť produktu IKT, služby IKT alebo procesu IKT;

22. „vlastné posúdenie zhody“ je činnosť vykonávaná výrobcom alebo poskytovateľom produktov IKT, služieb IKT alebo procesov IKT, ktorý hodnotí, či tieto produkty IKT, služby IKT alebo procesy IKT spĺňajú požiadavky konkrétneho európskeho systému certifikácie kybernetickej bezpečnosti.

HLAVA II

ENISA (AGENTÚRA EURÓPSKEJ ÚNIE PRE KYBERNETICKÚ BEZPEČNOSŤ)

KAPITOLA I

Mandát a ciele

Článok 3

Mandát

1. Agentúra ENISA plní úlohy, ktoré jej boli zverené týmto nariadením, s cieľom dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii, a to aj tým, že aktívne podporuje členské štáty a inštitúcie, orgány, úrady a agentúry Únie pri zlepšovaní kybernetickej bezpečnosti. Agentúra ENISA pôsobí ako referenčné miesto pre poradenstvo a odborné znalosti v oblasti kybernetickej bezpečnosti pre inštitúcie, orgány, úrady a agentúry Únie, ako aj pre iné príslušné zainteresované strany v Únii.

Vykonávaním úloh, ktoré boli agentúre ENISA zverené týmto nariadením, prispieva k zníženiu fragmentácie vnútorného trhu.

2. Agentúra ENISA plní úlohy, ktoré jej boli zverené v právnych aktoch Únie, v ktorých sa stanovujú opatrenia na aproximáciu zákonov, iných právnych predpisov a správnych opatrení členského štátu v oblasti kybernetickej bezpečnosti.

3. Pri vykonávaní svojich úloh agentúra ENISA koná nezávisle, pričom sa vyhýba zdvojovaniu činností členského štátu a zohľadňuje existujúce odborné znalosti členského štátu.

4. Agentúra ENISA vyvíja svoje vlastné zdroje vrátane technických a ľudských spôsobilostí a zručností potrebných na plnenie úloh, ktoré jej boli zverené týmto nariadením.

Článok 4

Ciele

1. Agentúra ENISA pôsobí ako stredisko odborných znalostí v oblasti kybernetickej bezpečnosti na základe svojej nezávislosti, vedeckej a technickej kvality poskytovaného poradenstva, pomoci a informácií, transparentnosti svojich prevádzkových postupov a pracovných metód a dôslednosti pri vykonávaní svojich úloh.

2. Agentúra ENISA pomáha inštitúciám, orgánom, úradom a agentúram Únie, ako aj členským štátom pri vypracúvaní a vykonávaní politík Únie súvisiacich s kybernetickou bezpečnosťou vrátane odvetvových politík v oblasti kybernetickej bezpečnosti.

3. Agentúra ENISA podporuje budovanie kapacít a pripravenosť v celej Únii tým, že inštitúciám, orgánom, úradom a agentúram Únie, ako aj členským štátom a verejným a súkromným zainteresovaným stranám pomáha pri zvyšovaní ochrany ich sietí a informačných systémov, pri rozvoji a zlepšovaní kybernetickej odolnosti a kapacít v oblasti reakcie, ako aj pri rozvoji zručností a spôsobilosti v oblasti kybernetickej bezpečnosti.

4. Agentúra ENISA presadzuje na úrovni Únie spoluprácu vrátane výmeny informácií a koordináciu medzi členskými štátmi, inštitúciami, orgánmi, úradmi a agentúrami Únie, ako aj príslušnými súkromnými a verejnými zainteresovanými stranami v otázkach týkajúcich sa kybernetickej bezpečnosti.

5. Agentúra ENISA prispieva k posilňovaniu spôsobilostí v oblasti kybernetickej bezpečnosti na úrovni Únie s cieľom podporiť činnosť členských štátov pri predchádzaní kybernetickým hrozbám a reakcii na ne, najmä v prípadoch cezhraničných incidentov.

6. Agentúra ENISA presadzuje používanie európskej certifikácie kybernetickej bezpečnosti, aby predišla fragmentácii vnútorného trhu. Agentúra ENISA prispieva k zriadeniu a udržiavaniu európskeho rámca certifikácie kybernetickej bezpečnosti v súlade s hlavou III tohto nariadenia, aby sa posilnila transparentnosť kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT, a tým sa posilnila dôvera v digitálny vnútorný trh a jeho konkurencieschopnosť.

7. Agentúra ENISA presadzuje vysokú úroveň povedomia o kybernetickej bezpečnosti vrátane kybernetickej hygieny a kybernetickej gramotnosti občanov, organizácii a podnikov.

KAPITOLA II

Úlohy

Článok 5

Tvorba a vykonávanie politiky a práva Únie

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

1. pomáha a radí pri tvorbe a prehodnocovaní politiky a práva Únie v oblasti kybernetickej bezpečnosti a odvetvovej politiky a legislatívnych iniciatív, ktoré sa týkajú kybernetickej bezpečnosti, najmä poskytovaním nezávislých stanovísk a analýz, ako aj vykonávaním prípravných prác;

2. pomáha členským štátom pri konzistentnom vykonávaní politiky a práva Únie v oblasti kybernetickej bezpečnosti, najmä v súvislosti so smernicou (EÚ) 2016/1148, a to aj vydávaním stanovísk, usmernení, poskytovaním poradenstva a najlepších postupov v oblastiach, ako je riadenie rizík, oznamovanie incidentov a zdieľanie informácií, ako aj uľahčovaním výmeny najlepších postupov medzi príslušnými orgánmi v tomto smere;

3. pomáha členským štátom a inštitúciám, orgánom, úradom a agentúram Únie pri tvorbe a presadzovaní politík v oblasti kybernetickej bezpečnosti vo vzťahu k udržaniu všeobecnej dostupnosti alebo integrity verejného jadra otvoreného internetu;

4. prispieva k práci skupiny pre spoluprácu v zmysle článku 11 smernice (EÚ) 2016/1148 v podobe odborných znalostí a poradenstva;

5. podporuje:

   a) tvorbu a vykonávanie politiky Únie v oblasti elektronickej totožnosti a dôveryhodných služieb, najmä formou poradenstva a vydávaním technických usmernení, ako aj uľahčovaním výmeny najlepších postupov medzi príslušnými orgánmi;

   b) presadzovanie zvýšenej úrovne bezpečnosti elektronických komunikácií, a to aj formou poradenstva a odborných znalostí, ako aj uľahčovaním výmeny najlepších postupov medzi príslušnými orgánmi;

   c) členské štáty pri vykonávaní konkrétnych kybernetickobezpečnostných aspektov politiky a práva Únie, ktoré sa týkajú ochrany údajov a súkromia, vrátane poskytovania poradenstva Európskemu výboru pre ochranu údajov na požiadanie;

6. podporuje pravidelné preskúmanie politickej činnosti Únie prípravou výročnej správy o stave vykonávania príslušného právneho rámca z hľadiska:

   a) informácií o oznámeniach členských štátov o incidentoch, ktoré podľa článku 10 ods. 3 smernice (EÚ) 2016/1148 poskytujú skupine pre spoluprácu jednotné kontaktné miesta;

   b) súhrnov oznámení o narušeniach bezpečnosti alebo integrity získavaných od poskytovateľov dôveryhodných služieb, ktoré agentúre ENISA poskytujú orgány dohľadu podľa článku 19 ods. 3 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([23]);

   c) oznámení o bezpečnostných incidentoch, ktoré podávajú poskytovatelia verejných elektronických komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb a ktoré agentúre ENISA poskytujú príslušné orgány podľa článku 40 smernice (EÚ) 2018/1972.

([23]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).

Článok 6

Budovanie kapacít

1. Agentúra ENISA pomáha:

a) členským štátom v ich úsilí zlepšovať prevenciu, odhaľovanie a analýzu kybernetických hrozieb a incidentov a schopnosť reagovať na ne tým, že im poskytuje vedomosti a odborné znalosti;

b) členským štátom a inštitúciám, orgánom, úradom a agentúram Únie pri zavádzaní a vykonávaní politík v oblasti zverejňovania informácií o zraniteľnosti na dobrovoľnom základe;

c) inštitúciám, orgánom, úradom a agentúram Únie v ich úsilí zlepšovať prevenciu, odhaľovanie a analýzu kybernetických hrozieb a incidentov a zlepšovať ich spôsobilosť reagovať na takéto kybernetické hrozby a incidenty, a to najmä primeranou podporou tímu CERT-EU;

d) členským štátom na požiadanie pri tvorbe vnútroštátnych jednotiek CSIRT podľa článku 9 ods. 5 smernice (EÚ) 2016/1148;

e) členským štátom na požiadanie pri vypracúvaní národných stratégií v oblasti bezpečnosti sietí a informačných systémov podľa článku 7 ods. 2 smernice (EÚ) 2016/1148 a v záujme propagácie najlepších postupov podporuje šírenie týchto stratégií v Únii a berie na vedomie pokrok v ich vykonávaní;

f) inštitúciám Únie pri tvorbe a revízii kybernetickobezpečnostných stratégií Únie, podpore ich šírenia a monitorovaní pokroku v ich vykonávaní;

g) vnútroštátnym jednotkám CSIRT a jednotkám CSIRT Únie pri zdokonaľovaní ich spôsobilosti, a to i presadzovaním dialógu a výmeny informácií, aby s ohľadom na aktuálny stupeň vývoja každá jednotka CSIRT mala spoločnú sadu minimálnej spôsobilosti a aby fungovala v súlade s najlepšími postupmi;

h) členským štátom pravidelným organizovaním kybernetickobezpečnostných cvičení na úrovni Únie podľa článku 7 ods. 5 aspoň raz za dva roky a vypracúvaním politických odporúčaní na základe hodnotenia týchto cvičení a takto získaných poznatkov;

i) príslušným verejným orgánom poskytovaním školení v oblasti kybernetickej bezpečnosti, podľa potreby v spolupráci so zainteresovanými stranami;

j) skupine pre spoluprácu pri výmene najlepších postupov podľa článku 11 ods. 3 písm. l) smernice (EÚ) 2016/1148, najmä z hľadiska identifikácie prevádzkovateľov základných služieb členskými štátmi, z hľadiska rizík a incidentov, a to aj v súvislosti s cezhraničnou previazanosťou.

2. Agentúra ENISA podporuje výmenu informácií v odvetviach a medzi nimi, a to najmä v odvetviach uvedených v prílohe II k smernici (EÚ) 2016/1148, poskytovaním najlepších postupov a poradenstva, ktoré sa týkajú dostupných nástrojov, postupov i riešení regulačných otázok spojených s výmenou informácií.

Článok 7

Operačná spolupráca na úrovni Únie

1. Agentúra ENISA podporuje operačnú spoluprácu medzi členskými štátmi, inštitúciami, orgánmi, úradmi a agentúrami Únie a medzi zainteresovanými stranami.

2. Agentúra ENISA na operačnej úrovni spolupracuje a vytvára synergie s inštitúciami, orgánmi, úradmi a agentúrami Únie vrátane tímu CERT-EU, útvarmi, ktoré sa zaoberajú počítačovou kriminalitou, a dozornými orgánmi v oblasti ochrany súkromia a osobných údajov na účely riešenia otázok spoločného záujmu, a to aj prostredníctvom:

a) výmeny know-how a osvedčených postupov;

b) poskytovania poradenstva a vydávania usmernení k relevantným otázkam spojeným s kybernetickou bezpečnosťou;

c) ustanovenia praktických dohôd na výkon konkrétnych úloh po konzultácii s Komisiou.

3. Agentúra ENISA zabezpečuje sekretariát siete jednotiek CSIRT podľa článku 12 ods. 2 smernice (EÚ) 2016/1148 a v tomto postavení aktívne podporuje výmenu informácií a spoluprácu medzi členmi siete jednotiek CSIRT.

4. Agentúra ENISA podporuje členské štáty v operačnej spolupráci v rámci siete jednotiek CSIRT tým, že:

a) im radí, ako zlepšiť svoju spôsobilosť predchádzať incidentom, odhaľovať ich a reagovať na ne, a na žiadosť jedného alebo viacerých členských štátov poskytne poradenstvo v súvislosti s konkrétnou kybernetickou hrozbou;

b) na žiadosť jedného alebo viacerých členských štátov im pomáha pri posúdení incidentov, ktoré majú významný alebo závažný vplyv, a to prostredníctvom poskytnutia odborných znalostí a uľahčením technického riešenia takýchto incidentov, okrem iného najmä podporou dobrovoľnej výmeny príslušných informácií a technických riešení medzi členskými štátmi;

c) analyzuje zraniteľnosti a incidenty na základe verejne dostupných informácií alebo informácií, ktoré na tento účel dobrovoľne poskytli členské štáty, a

d) na žiadosť jedného alebo viacerých členských štátov poskytuje podporu v súvislosti s ex post technickým skúmaním incidentov, ktoré majú významný alebo závažný vplyv v zmysle smernice (EÚ) 2016/1148.

Pri výkone týchto úloh agentúra ENISA a tím CERT-EU štruktúrovane spolupracujú s cieľom využiť synergie a predchádzať zdvojovaniu činností.

5. Agentúra ENISA pravidelne organizuje kybernetickobezpečnostné cvičenia na úrovni Únie a na požiadanie podporuje členské štáty a inštitúcie, orgány, úrady a agentúry Únie pri organizácií kybernetickobezpečnostných cvičení. Súčasťou takýchto kybernetickobezpečnostných cvičení na úrovni Únie môžu byť technické, operačné alebo strategické prvky. Raz za dva roky agentúra ENISA zorganizuje rozsiahle komplexné cvičenie.

Agentúra ENISA vo vhodnom prípade tiež prispieva k odvetvovým kybernetickobezpečnostným cvičeniam, pričom ich pomáha organizovať, spolu s relevantnými organizáciami, ktoré sa tiež zúčastňujú na kybernetickobezpečnostných cvičeniach na úrovni Únie.

6. Agentúra ENISA vypracúva v úzkej spolupráci s členskými štátmi pravidelnú podrobnú technickú správu EÚ o situácií v oblasti incidentov a kybernetických hrozieb, pri ktorej vychádza z verejne dostupných informácií, zo svojich vlastných analýz a zo správ, ktoré okrem iného poskytli jednotky CSIRT členských štátov alebo jednotné kontaktné miesta zriadené podľa smernice (EÚ) 2016/1148, v oboch prípadoch dobrovoľne, EC3 a tím CERT-EU.

7. Agentúra ENISA prispieva k vypracovaniu spoločnej reakcie na úrovni Únie a členských štátov na rozsiahle cezhraničné incidenty alebo krízy v oblasti kybernetickej bezpečnosti, a to najmä:

a) zhromažďovaním a analýzou správ z národných zdrojov, ktoré sú verejne dostupné alebo sa poskytujú dobrovoľne, s cieľom prispieť k vytvoreniu spoločného situačného povedomia;

b) zaistením efektívneho toku informácií a zabezpečením eskalačných mechanizmov medzi sieťou jednotiek CSIRT a subjektmi zodpovednými za technické a politické rozhodnutia na úrovni Únie;

c) na žiadosť uľahčovaním technického riešenia takýchto incidentov alebo kríz, a to najmä podporou dobrovoľnej výmeny technických riešení medzi členskými štátmi;

d) podporou inštitúcií, orgánov, úradov a agentúr Únie a na žiadosť členských štátov aj ich podporou pri verejnej komunikácii o takýchto incidentoch alebo krízach;

e) testovaním plánov spolupráce pri reakcii na takéto incidenty alebo krízy na úrovni Únie a na žiadosť členských štátov poskytovaním im podpory pri testovaní takýchto plánov na vnútroštátnej úrovni.

Článok 8

Trh, certifikácia kybernetickej bezpečnosti a normalizácia

1. Agentúra ENISA podporuje a presadzuje tvorbu a vykonávanie politiky Únie v oblasti certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT v zmysle hlavy III tohto nariadenia, a to tak, že:

a) neustále monitoruje vývoj v súvisiacich oblastiach normalizácie a odporúča vhodné technické špecifikácie na použitie pri rozvoji európskych systémov certifikácie kybernetickej bezpečnosti podľa článku 54 ods. 1 písm. c) v prípadoch, keď normy nie sú k dispozícii;

b) vypracúva kandidátske európske systémy certifikácie kybernetickej bezpečnosti (ďalej len „kandidátske systémy“) produktov IKT, služieb IKT a procesov IKT v súlade s článkom 49;

c) hodnotí prijaté európske systémy certifikácie kybernetickej bezpečnosti v súlade s článkom 49 ods. 8;

d) zapája sa do partnerských preskúmaní podľa článku 59 ods. 4;

e) pomáha Komisii pri poskytovaní sekretariátu skupine ECCG podľa článku 62 ods. 5.

2. Agentúra ENISA poskytuje sekretariát skupine zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti podľa článku 22 ods. 4.

3. Agentúra ENISA zostavuje a uverejňuje usmernenia a vypracúva osvedčené postupy, ktoré sa týkajú požiadaviek kybernetickej bezpečnosti na produkty IKT, služby IKT a procesy IKT, a to v spolupráci s vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti a s príslušným odvetvím formálnym, štandardizovaným a transparentným spôsobom.

4. Agentúra ENISA prispieva k vybudovaniu kapacity pre procesy hodnotenia a certifikácie tým, že zostavuje a vydáva usmernenia, a tiež poskytuje podporu členským štátom na ich žiadosť.

5. Agentúra ENISA uľahčuje zavádzanie a využívanie európskych i medzinárodných noriem v oblasti riadenia rizika a v oblasti bezpečnosti produktov IKT, služieb IKT a procesov IKT.

6. Agentúra ENISA v spolupráci s členskými štátmi a príslušným odvetvím vypracúva podľa článku 19 ods. 2 smernice (EÚ) 2016/1148 odporúčania a usmernenia, ktoré sa týkajú technických oblastí spojených s bezpečnostnými požiadavkami kladenými na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, ako aj odporúčania a usmernenia, ktoré sa týkajú už existujúcich noriem vrátane vnútroštátnych noriem členských štátov.

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

Článok 9

Znalosti a informácie

Agentúra ENISA:

a) analyzuje nastupujúce technológie a poskytuje tematicky zamerané posúdenia očakávaných spoločenských, právnych, hospodárskych a regulačných vplyvov technologických inovácií na kybernetickú bezpečnosť;

b) vykonáva dlhodobé strategické analýzy kybernetických hrozieb a incidentov s cieľom identifikovať nové trendy a pomôcť predchádzať incidentom;

c) v spolupráci s expertmi orgánov členských štátov a príslušných zainteresovaných strán poskytuje poradenstvo, usmernenia a osvedčené postupy v oblasti bezpečnosti sietí a informačných systémov, a najmä bezpečnosti infraštruktúr, o ktoré sa opierajú odvetvia uvedené v prílohe II k smernici (EÚ) 2016/1148 a ktoré využívajú poskytovatelia digitálnych služieb uvedených v prílohe III k uvedenej smernici;

d) prostredníctvom vyhradeného portálu zhromažďuje, organizuje a uverejňuje informácie o kybernetickej bezpečnosti, ktoré poskytli inštitúcie, orgány, úrady a agentúry Únie, a informácie o kybernetickej bezpečnosti, ktoré poskytli na dobrovoľnom základe členské štáty a súkromné a verejné zainteresované strany;

e) zhromažďuje a analyzuje verejne dostupné informácie o významných incidentoch a pripravuje správy s cieľom poskytnúť poradenstvo pre občanov, organizácie a podniky v celej Únii.

Článok 10

Zvyšovanie povedomia a vzdelávanie

Agentúra ENISA:

a) zvyšuje verejné povedomie o kybernetickobezpečnostných rizikách a poskytuje poradenstvo o osvedčených postupoch pre jednotlivých užívateľov, ktoré sú zamerané na občanov, organizácie a podniky a ktoré sa týkajú aj kybernetickej hygieny a kybernetickej gramotnosti;

b) v spolupráci s členskými štátmi, inštitúciami, orgánmi, úradmi a agentúrami Únie, ako aj príslušným odvetvím, organizuje pravidelné osvetové kampane na zvýšenie kybernetickej bezpečnosti a jej viditeľnosti v Únii a podporuje diskusiu so širokou verejnosťou;

c) pomáha členským štátom v ich úsilí zvyšovať povedomie o kybernetickej bezpečnosti a podporovať vzdelávanie v oblasti kybernetickej bezpečnosti;

d) podporuje užšiu koordináciu a výmenu najlepších postupov medzi členskými štátmi, pokiaľ ide o povedomie a vzdelávanie v oblasti kybernetickej bezpečnosti.

Článok 11

Výskum a inovácia

V oblasti výskumu a inovácie agentúra ENISA:

a) radí inštitúciám, orgánom, úradom a agentúram Únie a členským štátom o potrebách a prioritách výskumu v oblasti kybernetickej bezpečnosti s cieľom umožniť účinnú reakciu na existujúce i nové riziká a kybernetické hrozby, a to i v súvislosti s novými a nastupujúcimi informačnými a komunikačnými technológiami, a s cieľom účinne používať technológie na prevenciu rizika;

b) podieľa sa na implementačnej fáze programov financovania výskumu a inovácie, ak jej Komisia udelila príslušné právomoci, alebo sa na nich zúčastňuje ako príjemca;

c) v oblasti kybernetickej bezpečnosti prispieva do strategického programu pre výskum a inováciu na úrovni Únie.

Článok 12

Medzinárodná spolupráca

Agentúra ENISA prispieva k úsiliu Únie o spoluprácu s tretími krajinami a medzinárodnými organizáciami, ako aj v rámci príslušných medzinárodných rámcov spolupráce s cieľom podporiť medzinárodnú spoluprácu v kybernetickobezpečnostných otázkach, a to tým, že:

a) sa v náležitých prípadoch zapája ako pozorovateľ pri organizácii medzinárodných cvičení, analyzuje ich výsledky a podáva o nich správy správnej rade;

b) na žiadosť Komisie sprostredkúva výmenu najlepších postupov;

c) na žiadosť Komisie jej poskytuje odborné znalosti;

d) poskytuje poradenstvo a podporu Komisii v záležitostiach týkajúcich sa dohôd o vzájomnom uznávaní certifikátov kybernetickej bezpečnosti s tretími krajinami v spolupráci s ECCG zriadenou podľa článku 62.

KAPITOLA III

Organizácia agentúry ENISA

Článok 13

Štruktúra agentúry ENISA

Administratívna a riadiaca štruktúra agentúry ENISA pozostáva z týchto prvkov:

a) správna rada;

b) výkonná rada;

c) výkonný riaditeľ;

d) poradná skupina agentúry ENISA;

e) sieť národných styčných dôstojníkov.

Oddiel 1

Správna rada

Článok 14

Zloženie správnej rady

1. Správnu radu tvorí jeden člen vymenovaný za každý členský štát a dvaja členovia vymenovaní Komisiou. Všetci členovia majú hlasovacie právo.

2. Každý člen správnej rady má náhradníka. Tento náhradník zastupuje člena v jeho neprítomnosti.

3. Členovia správnej rady a ich náhradníci sa vymenúvajú na základe ich znalostí v oblasti kybernetickej bezpečnosti s prihliadnutím na ich relevantné riadiace, administratívne a rozpočtové zručnosti. Komisia a členské štáty sa vynasnažia obmedziť fluktuáciu svojich zástupcov v správnej rade s cieľom zabezpečiť kontinuitu práce správnej rady. Komisia a členské štáty sa usilujú o rodovú vyváženosť v správnej rade.

4. Funkčné obdobie členov správnej rady a ich náhradníkov je štyri roky. Toto obdobie je obnoviteľné.

Článok 15

Funkcie správnej rady

1. Správna rada:

a) stanovuje všeobecné smerovanie činnosti agentúry ENISA a zabezpečuje, aby agentúra ENISA pracovala v súlade s pravidlami a zásadami stanovenými v tomto nariadení; zabezpečuje aj súlad práce agentúry ENISA s činnosťami vykonávanými členskými štátmi i na úrovni Únie;

b) prijíma návrh jednotného programového dokumentu agentúry ENISA uvedeného v článku 24 pred jeho predložením Komisii na vydanie stanoviska;

c) prijíma jednotný programový dokument agentúry ENISA, pričom zohľadňuje stanovisko Komisie;

d) dozerá na vykonávanie viacročného a ročného plánovania začleneného do jednotného programového dokumentu;

e) prijíma ročný rozpočet agentúry ENISA a vykonáva ostatné funkcie spojené s rozpočtom agentúry ENISA podľa kapitoly IV;

f) posudzuje a prijíma konsolidovanú výročnú správu o činnosti agentúry ENISA vrátane účtovných výkazov a opisu toho, do akej miery agentúra ENISA splnila svoje ukazovatele výkonnosti, predkladá výročnú správu i jej posúdenie do 1. júla nasledujúceho roka Európskemu parlamentu, Rade, Komisii a Dvoru audítorov a výročnú správu zverejňuje;

g) prijíma rozpočtové pravidlá platné pre agentúru ENISA v súlade s článkom 32;

h) prijíma stratégiu boja proti podvodom, ktorá musí byť primeraná riziku podvodov so zreteľom na analýzu efektívnosti nákladov a prínosov vo vzťahu k opatreniam, ktoré sa majú vykonávať;

i) prijíma pravidlá predchádzania konfliktom záujmov svojich členov a ich riešenia;

j) zabezpečuje primerané opatrenia nadväzujúce na zistenia a odporúčania, ktoré vyplývajú z vyšetrovania Európskeho úradu pre boj proti podvodom (OLAF) a rôznych správ a hodnotení interného alebo externého auditu;

k) prijíma svoj rokovací poriadok vrátane pravidiel pre prijímanie predbežných rozhodnutí o delegovaní osobitných úloh podľa článku 19 ods. 7;

l) v súlade s odsekom 2 tohto článku vykonáva vo vzťahu k zamestnancom agentúry ENISA právomoci zverené Služobným poriadkom úradníkov Európskej únie (ďalej len „služobný poriadok úradníkov“) a Podmienkami zamestnávania ostatných zamestnancov Európskej únie (ďalej len „podmienky zamestnávania ostatných zamestnancov“), stanovenými v nariadení Rady (EHS, Euratom, ESUO) č. 259/68 ([24]), menovaciemu orgánu a orgánu oprávnenému uzatvárať pracovné zmluvy (ďalej len „právomoci menovacieho orgánu“);

m) prijíma predpisy vykonávajúce Služobný poriadok úradníkov a Podmienky zamestnávania ostatných zamestnancov v súlade s postupom uvedeným v článku 110 služobného poriadku úradníkov;

n) vymenúva výkonného riaditeľa a v náležitých prípadoch predlžuje jeho funkčné obdobie alebo ho z funkcie odvoláva v súlade s článkom 36;

o) vymenúva účtovníka, ktorým môže byť účtovníkom Komisie a ktorý musí byť pri výkone svojich povinností úplne nezávislý;

p) prijíma všetky rozhodnutia o zriaďovaní vnútorných štruktúr agentúry ENISA a v prípade potreby o zmene uvedených vnútorných štruktúr, pričom prihliada na potreby činnosti agentúry ENISA a zásadu správneho rozpočtového riadenia;

q) schvaľuje stanovenie pracovných dojednaní podľa článku 7;

r) schvaľuje stanovenie alebo uzavretie pracovných dojednaní podľa článku 42.

2. Správna rada v súlade s článkom 110 služobného poriadku úradníkov prijíma rozhodnutie na základe článku 2 ods. 1 služobného poriadku úradníkov a článku 6 podmienok zamestnávania ostatných zamestnancov, ktorým deleguje príslušné právomoci menovacieho orgánu na výkonného riaditeľa a ktorým určuje podmienky, za ktorých možno toto delegovanie právomoci pozastaviť. Výkonný riaditeľ môže tieto právomoci delegovať ďalej.

([24]) Ú. v. ES L 56, 4.3.1968, s. 1.

3. Ak si to vyžadujú mimoriadne okolnosti, správna rada môže prijať rozhodnutie o dočasnom pozastavení delegovania právomocí menovacieho orgánu na výkonného riaditeľa a akýchkoľvek právomocí menovacieho orgánu ďalej delegovaných výkonným riaditeľom, a tieto právomoci vykonávať sama alebo ich delegovať na jedného zo svojich členov alebo na zamestnanca, ktorý nie je výkonným riaditeľom.

Článok 16

Predseda správnej rady

Správna rada volí spomedzi svojich členov dvojtretinovou väčšinou hlasov členov svojho predsedu a podpredsedu. Ich funkčné obdobie je štvorročné a je obnoviteľné raz. Ak sa však ich členstvo v správnej rade kedykoľvek počas ich funkčného obdobia skončí, ich funkčné obdobie sa automaticky končí k danému dátumu. Ak predseda nie je schopný plniť si svoje povinnosti, podpredseda ho nahradí *ex officio*.

Článok 17

Zasadnutia správnej rady

1. Zasadnutia správnej rady zvoláva jej predseda.

2. Riadne zasadnutia správnej rady sa konajú aspoň dvakrát ročne. Na žiadosť jej predsedu, Komisie alebo najmenej tretiny svojich členov zasadá správna rada aj mimoriadne.

3. Výkonný riaditeľ sa zúčastňuje na zasadnutiach správnej rady, avšak nemá hlasovacie právo.

4. Na zasadnutiach správnej rady sa môžu na pozvanie predsedu zúčastniť členovia poradnej skupiny agentúry ENISA, avšak nemajú hlasovacie právo.

5. Členom správnej rady a ich náhradníkom môžu v súlade s jej rokovacím poriadkom pomáhať na zasadnutiach správnej rady poradcovia alebo experti.

6. Sekretariát pre správnu radu zabezpečuje agentúra ENISA.

Článok 18

Pravidlá hlasovania správnej rady

1. Správna rada prijíma svoje rozhodnutia väčšinou hlasov svojich členov.

2. Dvojtretinová väčšina hlasov členov správnej rady sa vyžaduje na prijatie jednotného programového dokumentu a ročného rozpočtu a na vymenovania a odvolania výkonného riaditeľa či predĺženia jeho funkčného obdobia.

3. Každý člen má jeden hlas. Ak je člen správnej rady neprítomný, hlasovacie právo tohto člena uplatňuje jeho náhradník.

4. Predseda správnej rady sa na hlasovaní zúčastňuje.

5. Výkonný riaditeľ sa na hlasovaní nezúčastňuje.

6. V rokovacom poriadku správnej rady sa stanovia podrobnejšie pravidlá hlasovania, najmä podmienky, za ktorých môže člen konať v mene iného člena.

Oddiel 2

Výkonná rada

Článok 19

Výkonná rada

1. Správnej rade pomáha výkonná rada.

2. Výkonná rada:

a) pripravuje rozhodnutia, ktoré má prijať správna rada;

b) spolu so správnou radou zabezpečuje prijatie vhodných opatrení v nadväznosti na zistenia a odporúčania vyplývajúce z vyšetrovaní úradu OLAF a z rôznych správ z interného alebo externého auditu a hodnotení;

c) bez toho, aby boli dotknuté povinnosti výkonného riaditeľa stanovené v článku 20, pomáha a radí výkonnému riaditeľovi pri vykonávaní rozhodnutí správnej rady v administratívnej a rozpočtovej oblasti podľa článku 20.

3. Výkonná rada je zložená z piatich členov. Členovia výkonnej rady sa vymenujú spomedzi členov správnej rady. Jeden z členov je predseda správnej rady, ktorý môže predsedať aj výkonnej rade, a ďalším je jeden zo zástupcov Komisie. Pri vymenovaniach členov výkonnej rady sa dbá na zabezpečenie vyváženého rodového zastúpenia vo výkonnej rade. Výkonný riaditeľ sa zúčastňuje na zasadnutiach výkonnej rady, ale nemá hlasovacie právo.

4. Funkčné obdobie členov výkonnej rady je štyri roky. Toto obdobie je obnoviteľné.

5. Výkonná rada zasadá aspoň raz za tri mesiace. Predseda výkonnej rady zvoláva ďalšie zasadnutia na žiadosť jej členov.

6. Rokovací poriadok výkonnej rady stanovuje správna rada.

7. Ak je to potrebné z dôvodu naliehavosti, výkonná rada môže prijať určité predbežné rozhodnutia v mene správnej rady, a to najmä o otázkach administratívneho riadenia vrátane rozhodnutí o pozastavení delegovania právomocí menovacieho orgánu a o rozpočtových záležitostiach. Akékoľvek takéto predbežné rozhodnutia sa bez zbytočného odkladu oznámia správnej rade. Správna rada potom rozhodne, či predbežné rozhodnutie schváli alebo zamietne najneskôr do troch mesiacov po jeho prijatí. Výkonná rada nesmie prijímať rozhodnutia v mene správnej rady, ktoré si vyžadujú schválenie dvojtretinovou väčšinou členov správnej rady.

Oddiel 3

Výkonný riaditeľ

Článok 20

Povinnosti výkonného riaditeľa

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

2. Výkonný riaditeľ podáva Európskemu parlamentu na jeho vyzvanie správu o plnení svojich povinností. Rada môže vyzvať výkonného riaditeľa, aby podal správu o plnení svojich povinností.

3. Výkonný riaditeľ je zodpovedný za:

a) každodennú správu agentúry ENISA;

b) vykonávanie rozhodnutí, ktoré prijme správna rada;

c) prípravu návrhu jednotného programového dokumentu a jeho predloženie správnej rade na schválenie pred tým, než sa predloží Komisii;

d) vykonávanie jednotného programového dokumentu a zodpovedajúce informovanie správnej rady;

e) vypracovanie konsolidovanej výročnej správy o činnosti agentúry ENISA vrátane plnenia ročného pracovného programu agentúry ENISA a jej predloženie správnej rade na posúdenie a prijatie;

f) vypracovanie akčného plánu v nadväznosti na závery spätných hodnotení a predloženie správy o pokroku Komisii každé dva roky;

g) vypracovanie akčného plánu v nadväznosti na závery správ z interného alebo externého auditu, ako aj na vyšetrovania úradu OLA a za predkladanie správ o pokroku dvakrát ročne Komisii a pravidelne správnej rade;

h) vypracovanie návrhu rozpočtových pravidiel uplatniteľných na agentúru ENISA podľa článku 32;

i) vypracovanie návrhu výkazu odhadov príjmov a výdavkov agentúry ENISA a plnenie jej rozpočtu;

j) ochranu finančných záujmov Únie prostredníctvom uplatňovania preventívnych opatrení na zamedzenie podvodov, korupcie a iných nezákonných činností, prostredníctvom účinných kontrol a v prípade, že sa zistia nezrovnalosti, prostredníctvom vymáhania neoprávnene vyplatených súm a prípadne prostredníctvom účinných, primeraných a odradzujúcich administratívnych a finančných sankcií;

k) vypracovanie stratégie agentúry ENISA pre boj proti podvodom a jej predloženie správnej rade na schválenie;

l) nadviazanie a udržiavanie kontaktov s podnikateľskou komunitou a so spotrebiteľskými organizáciami na zabezpečenie pravidelného dialógu s príslušnými zainteresovanými stranami;

m) pravidelnú výmenu názorov a informácií s inštitúciami, orgánmi, úradmi a agentúrami Únie, pokiaľ ide o ich činnosti týkajúce sa kybernetickej bezpečnosti, na účely zabezpečenia koherentnosti pri vypracúvaní a vykonávaní politiky Únie;

n) vykonávanie ostatných úloh, ktoré sú výkonnému riaditeľovi zverené týmto nariadením.

4. V prípade potreby a v súlade s cieľmi a úlohami agentúry ENISA môže výkonný riaditeľ zriaďovať ad hoc pracovné skupiny zložené z expertov vrátane expertov z príslušných orgánov členských štátov. Výkonný riaditeľ o tom musí vopred informovať správnu radu. Postupy týkajúce sa najmä zloženia týchto pracovných skupín, menovania expertov týchto pracovných skupín výkonným riaditeľom a fungovania týchto pracovných skupín sa spresnia vo vnútorných pravidlách činnosti agentúry ENISA.

5. Na účely efektívneho a účinného plnenia úloh agentúry ENISA a na základe primeranej analýzy nákladov a prínosov môže výkonný riaditeľ v prípade potreby rozhodnúť, že zriadi jednu alebo viacero miestnych kancelárií v jednom alebo viacerých členských štátoch. Pred rozhodnutím o zriadení miestnej kancelárie výkonný riaditeľ požiada o stanovisko dotknuté členské štáty vrátane členského štátu, v ktorom sa nachádza sídlo agentúry ENISA, a musí vopred získať súhlas Komisie a správnej rady. V prípade nezhody medzi výkonným riaditeľom a dotknutými členskými štátmi v priebehu konzultačného procesu sa záležitosť predloží na prerokovanie v Rade. Celkový počet členov personálu v miestnych kanceláriách musí byť minimálny a neprekročiť 40 % celkového počtu členov personálu agentúry ENISA v členskom štáte, v ktorom sa nachádza jej sídlo. Počet členov personálu v žiadnej miestnej kancelárii neprekročí 10 % celkového počtu členov personálu agentúry ENISA v členskom štáte, v ktorom sa nachádza jej sídlo.

V rozhodnutí o zriadení miestnej kancelárie sa vymedzí rozsah činností, ktoré sa majú v miestnej kancelárii vykonávať, a to tak, aby sa zabránilo vzniku zbytočných nákladov a zdvojeniu administratívnych funkcií agentúry ENISA.

Oddiel 4

Poradná skupina agentúry ENISA, skupina zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti a sieť národných styčných úradníkov

Článok 21

Poradná skupina agentúry ENISA

1. Správna rada konajúca na návrh výkonného riaditeľa transparentným spôsobom zriadi poradnú skupinu agentúry ENISA zloženú z uznávaných expertov zastupujúcich príslušné zainteresované strany, ako sú odvetvie IKT, poskytovatelia verejne dostupných elektronických komunikačných sietí alebo služieb, MSP, prevádzkovatelia základných služieb, spotrebiteľské skupiny, akademickí experti na kybernetickú bezpečnosť a zástupcovia príslušných orgánov, voči ktorým sa plní oznamovacia povinnosť podľa smernice (EÚ) 2018/1972, európske normalizačné organizácie, ako aj orgány presadzovania práva a dozorné orgány v oblasti ochrany údajov. Správna rada sa usiluje o zabezpečenie vhodnej vyváženosti rodového zastúpenia a vhodnej geografickej vyváženosti, ako aj rovnováhy medzi rôznymi skupinami zainteresovaných strán.

2. Postupy poradnej skupiny agentúry ENISA, najmä z hľadiska jej zloženia, návrhu výkonného riaditeľa uvedeného v odseku 1, počtu a menovania jej členov a činnosti poradnej skupiny agentúry ENISA sa vymedzia vo vnútorných pravidlách činnosti agentúry ENISA a zverejnia sa.

3. Poradnej skupine agentúry ENISA predsedá výkonný riaditeľ alebo ktokoľvek, koho výkonný riaditeľ v jednotlivých prípadoch vymenuje.

4. Funkčné obdobie členov poradnej skupiny agentúry ENISA je dva a pol roka. Členovia správnej rady nie sú členmi poradnej skupiny agentúry ENISA. Experti z Komisie a členských štátov sú oprávnení zúčastňovať sa na zasadnutiach poradnej skupiny agentúry ENISA a podieľať sa na jej práci. Na zasadnutia poradnej skupiny agentúry ENISA a k účasti na jej práci možno prizvať aj zástupcov iných orgánov, ktoré výkonný riaditeľ považuje za relevantné a ktoré nie sú členmi poradnej skupiny agentúry ENISA.

5. Poradná skupina agentúry ENISA radí agentúre ENISA v súvislosti s vykonávaním úloh agentúry ENISA s výnimkou uplatňovania ustanovení hlavy III tohto nariadenia. Predovšetkým radí výkonnému riaditeľovi pri vypracúvaní návrhu ročného pracovného programu agentúry ENISA a pri zabezpečovaní komunikácie s príslušnými zainteresovanými stranami o otázkach týkajúcich sa ročného pracovného programu.

6. Poradná skupina agentúry ENISA pravidelne informuje správnu radu o svojich činnostiach.

Článok 22

Skupina zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti

1. Zriadi sa skupina zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti.

2. Skupina zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti sa skladá z členov vybraných spomedzi uznávaných expertov zastupujúcich príslušné zainteresované strany. Komisia vyberie členov skupiny zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti na základe návrhu agentúry ENISA prostredníctvom transparentnej a otvorenej súťaže a zabezpečí rovnováhu medzi rôznymi skupinami zainteresovaných strán, ako aj vhodnú rodovú a geografickú vyváženosť.

3. Skupina zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti:

a) radí Komisii o strategických otázkach, pokiaľ ide o európsky rámec certifikácie kybernetickej bezpečnosti;

b) na požiadanie radí agentúre ENISA o všeobecných a strategických otázkach týkajúcich sa úloh agentúry ENISA, pokiaľ ide o trh, certifikáciu kybernetickej bezpečnosti a normalizáciu;

c) pomáha Komisii pri príprave priebežného pracovného programu Únie podľa článku 47;

d) vydáva stanovisko k priebežnému pracovnému programu Únie podľa článku 47 ods. 4 a

e) v naliehavých prípadoch radí Komisii a ECCG o potrebe ďalších certifikačných systémov, ktoré nie sú zahrnuté do priebežného pracovného programu Únie, ako je uvedené v článkoch 47 a 48.

4. Skupine zainteresovaných strán pre certifikáciu kybernetickej bezpečnosti spoločne predsedajú zástupcovia Komisie a agentúry ENISA a jej sekretariát zabezpečí agentúra ENISA.

Článok 23

Sieť národných styčných úradníkov

1. Správna rada konajúca na návrh výkonného riaditeľa zriadi sieť národných styčných úradníkov zloženú zo zástupcov všetkých členských štátov (ďalej len „národní styční úradníci“). Každý členský štát vymenuje jedného zástupcu do siete národných styčných úradníkov. Zasadnutia siete národných styčných úradníkov sa môžu konať v rôznych expertných zloženiach.

2. Sieť národných styčných úradníkov najmä uľahčuje výmenu informácií medzi agentúrou ENISA a členskými štátmi a podporuje agentúru ENISA pri šírení jej činností, zistení a odporúčaní príslušným zainteresovaným stranám v celej Únii.

3. Národní styční úradníci pôsobia ako kontaktné miesto na vnútroštátnej úrovni s cieľom uľahčiť spoluprácu medzi agentúrou ENISA a národnými expertmi pri plnení ročného pracovného programu agentúry ENISA.

4. Národní styční úradníci síce úzko spolupracujú so zástupcami správnej rady z ich príslušných členských štátov, ale sieť národných styčných úradníkov samotná nesmie zdvojovať prácu správnej rady ani iných fór Únie.

5. Funkcie a postupy siete národných styčných úradníkov sa stanovia vo vnútorných pravidlách činnosti agentúry ENISA a zverejnia sa.

Oddiel 5

Činnosť

Článok 24

Jednotný programový dokument

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

2. Výkonný riaditeľ každý rok vypracúva návrh jednotného programového dokumentu, ktorý obsahuje ročné a viacročné plánovanie vrátane plánovania zodpovedajúcich finančných a ľudských zdrojov v súlade s článkom 32 delegovaného nariadenia Komisie (EÚ) č. 1271/2013 ([25]), pričom zohľadní usmernenia stanovené Komisiou.

3. Správna rada každoročne prijme do 30. novembra jednotný programový dokument uvedený v odseku 1 a zašle ho Európskemu parlamentu, Rade a Komisii do 31. januára nasledujúceho roka, ako aj všetky neskôr aktualizované verzie uvedeného dokumentu.

4. Jednotný programový dokument nadobudne konečné znenie po konečnom prijatí všeobecného rozpočtu Únie, na základe ktorého sa podľa potreby upraví.

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

5. Ročný pracovný program zahŕňa podrobné ciele a očakávané výsledky vrátane ukazovateľov výkonnosti. Obsahuje aj opis opatrení, ktoré sa majú financovať, a informáciu o finančných a ľudských zdrojoch vyčlenených na každé opatrenie v súlade so zásadami zostavovania rozpočtu a riadenia podľa činností. Ročný pracovný program musí byť súlade s viacročným pracovným programom uvedeným v odseku 7. Jasne sa v ňom vymedzia úlohy, ktoré sa oproti predchádzajúcemu rozpočtovému roku pridali, zmenili alebo vypustili.

6. Ak sa agentúre ENISA zverí nová úloha, správna rada prijatý ročný pracovný program zmení. Každá podstatná zmena ročného pracovného programu sa prijíma rovnakým postupom ako pôvodný ročný pracovný program. Právomoc vykonávať nepodstatné zmeny ročného pracovného programu môže správna rada delegovať na výkonného riaditeľa.

7. Vo viacročnom pracovnom programe sa stanovuje všeobecné strategické plánovanie vrátane cieľov, očakávaných výsledkov a ukazovateľov výkonnosti. Zároveň sa v ňom uvádza plánovanie zdrojov vrátane viacročného rozpočtu a personálu.

8. Plánovanie zdrojov sa každoročne aktualizuje. Strategické plánovanie sa aktualizuje podľa potreby, najmä so zámerom zohľadniť výsledky hodnotenia uvedeného v článku 67.

Článok 25

Vyhlásenie o záujmoch

1. Členovia správnej rady, výkonný riaditeľ a úradníci dočasne vyslaní členskými štátmi vydajú vyhlásenie o záväzkoch a vyhlásenie o absencii alebo existencii akýchkoľvek priamych alebo nepriamych záujmov, ktoré by sa mohli považovať za záujmy, ktoré ovplyvňujú ich nezávislosť. Vyhlásenia musia byť presné a úplné, vyhotovené každoročne v písomnej forme a v prípade potreby sa aktualizujú.

2. Členovia správnej rady, výkonný riaditeľ a externí experti, ktorí sa zúčastňujú v ad hoc pracovných skupinách, presne a úplne oznámia najneskôr na začiatku každého zasadnutia akékoľvek záujmy, ktoré by sa mohli považovať za záujmy, ktoré ovplyvňujú ich nezávislosť v súvislosti s bodmi programu, a zdržia sa účasti na diskusiách k týmto bodom a na hlasovaní o nich.

3. Agentúra ENISA vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia pre pravidlá, ktoré sa týkajú vyhlásení o záujmoch uvedených v odsekoch 1 a 2.

Článok 26

Transparentnosť

1. Agentúra ENISA vykonáva svoje činnosti s vysokým stupňom transparentnosti a v súlade s článkom 28.

2. Agentúra ENISA zabezpečí, aby verejnosť a všetky strany, ktoré prejavia záujem, dostávali náležité, objektívne, spoľahlivé a ľahko dostupné informácie, najmä o výsledkoch jej práce. Agentúra takisto uverejňuje vyhlásenia o záujmoch podľa článku 25.

3. Správna rada konajúc na návrh výkonného riaditeľa môže stranám, ktoré prejavia záujem, povoliť pozorovanie postupov niektorých činností agentúry ENISA.

4. Agentúra ENISA vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia na vykonávanie pravidiel transparentnosti uvedených v odsekoch 1 a 2.

Článok 27

Povinnosť mlčanlivosti

1. Bez toho, aby bol dotknutý článok 28, agentúra ENISA nevyzradí tretím stranám informácie, ktoré spracúva alebo získava a v súvislosti s ktorými bola podaná odôvodnená žiadosť o dôverné zaobchádzanie.

2. Členovia správnej rady, výkonný riaditeľ, členovia poradnej skupiny agentúry ENISA, externí experti zúčastňujúci sa ad hoc pracovných skupín a personál agentúry ENISA vrátane úradníkov dočasne vyslaných členskými štátmi musia spĺňať požiadavky na povinnosť mlčanlivosti podľa článku 339 ZFEÚ, a to aj po skončení ich povinností.

3. Agentúra ENISA vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia na vykonávanie pravidiel týkajúcich sa povinnosti mlčanlivosti uvedených v odsekoch 1 a 2.

4. Ak je to potrebné pre vykonávanie úloh agentúry ENISA, správna rada rozhodne, že agentúre ENISA povolí pracovať s utajovanými skutočnosťami. V takom prípade agentúra ENISA po dohode s útvarmi Komisie prijme bezpečnostné predpisy, ktorými sa uplatňujú zásady bezpečnosti stanovené v rozhodnutiach Komisie (EÚ, Euratom) 2015/443 ([26]) a 2015/444 ([27]). Tieto bezpečnostné predpisy musia zahŕňať ustanovenia týkajúce sa výmeny, spracúvania a uchovávania utajovaných skutočností.

Článok 28

Prístup k dokumentom

1. Na dokumenty, ktoré má agentúra ENISA v držbe, sa vzťahuje nariadenie (ES) č. 1049/2001.

2. Správna rada prijme opatrenia na vykonanie nariadenia (ES) č. 1049/2001 do 28. decembra 2019.

3. Rozhodnutia, ktoré agentúra ENISA prijme podľa článku 8 nariadenia (ES) č. 1049/2001, môžu byť predmetom sťažnosti podanej európskemu ombudsmanovi podľa článku 228 ZFEÚ alebo žaloby podanej na Súdnom dvore Európskej únie podľa článku 263 ZFEÚ.

KAPITOLA IV

Zostavovanie a štruktúra rozpočtu agentúry ENISA

Článok 29

Zostavovanie rozpočtu agentúry ENISA

1. Výkonný riaditeľ každoročne vypracúva návrh výkazu odhadov príjmov a výdavkov agentúry ENISA na nasledujúci rozpočtový rok a postupuje ho správnej rade spolu s návrhom plánu pracovných miest. Príjmy a výdavky musia byť v rovnováhe.

2. Správna rada každý rok na základe návrhu výkazu odhadov vypracuje výkaz odhadov príjmov a výdavkov agentúry ENISA na nasledujúci rozpočtový rok.

3. Výkaz odhadov, ktorý je súčasťou návrhu jednotného programového dokumentu, správna rada každoročne do 31. januára zasiela Komisii a tretím krajinám, s ktorými Únia uzatvorila dohody podľa článku 42 ods. 2.

4. Komisia na základe výkazu odhadov zaradí do návrhu všeobecného rozpočtu Únie odhady, ktoré pokladá za potrebné pre plán pracovných miest, a výšku príspevku, ktorý sa má uhradiť zo všeobecného rozpočtu Únie, ktoré predloží Európskemu parlamentu a Rade v súlade s článkom 314 ZFEÚ.

5. Európsky parlament a Rada schvaľujú rozpočtové prostriedky na príspevok Únie agentúre ENISA.

6. Európsky parlament a Rada prijímajú plán pracovných miest agentúry ENISA.

([26]) Rozhodnutie Komisie (EÚ, Euratom) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii (Ú. v. EÚ L 72, 17.3.2015, s. 41).
([27]) Rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53).

7. Správna rada prijíma rozpočet agentúry ENISA spolu s jednotným programovým dokumentom. Rozpočet agentúry ENISA sa stáva konečným po tom, čo sa všeobecný rozpočet Únie prijme s konečnou platnosťou. Správna rada v prípade potreby upraví rozpočet a jednotný programový dokument agentúry ENISA v súlade so všeobecným rozpočtom Únie.

Článok 30

Štruktúra rozpočtu agentúry ENISA

1. Bez toho, aby boli dotknuté iné zdroje, príjmy agentúry ENISA zahŕňajú:

a) príspevok zo všeobecného rozpočtu Únie;

b) príjmy určené na krytie konkrétnych výdavkových položiek v súlade s jej rozpočtovými pravidlami uvedenými v článku 32;

c) finančné prostriedky Únie na základe dohôd o delegovaní alebo ad hoc grantov v súlade s jej rozpočtovými pravidlami uvedenými v článku 32 a s ustanoveniami príslušných nástrojov na podporu politík Únie;

d) príspevky tretích krajín podieľajúcich sa na činnosti agentúry ENISA podľa článku 42;

e) prípadné peňažné či nepeňažné dobrovoľné príspevky členských štátov.

Členským štátom, ktoré poskytujú dobrovoľné príspevky podľa písmena e) prvého pododseku, za ne nevzniká nárok na žiadne osobitné práva alebo služby.

2. Medzi výdavky agentúry ENISA patria výdavky na personál, administratívnu a technickú podporu, infraštruktúru a prevádzku a výdavky vyplývajúce zo zmlúv s tretími stranami.

Článok 31

Plnenie rozpočtu agentúry ENISA

1. Za plnenie rozpočtu agentúry ENISA je zodpovedný výkonný riaditeľ.

2. Vnútorný audítor Komisie má rovnaké právomoci nad agentúrou ENISA ako nad odbormi Komisie.

3. Účtovník agentúry ENISA zasiela predbežnú účtovnú závierku za rozpočtový rok (rok N) účtovníkovi Komisie a Dvoru audítorov do 1. marca nasledujúceho rozpočtového roka (rok N+1).

4. Po doručení pripomienok Dvora audítorov k predbežnej účtovnej závierke agentúry ENISA podľa článku 246 nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046 ([28]) vypracuje účtovník agentúry ENISA na vlastnú zodpovednosť konečnú účtovnú závierku agentúry ENISA a predloží ju správnej rade na vyjadrenie stanoviska.

5. Správna rada vydáva stanovisko ku konečnej účtovnej závierke agentúry ENISA.

6. Výkonný riaditeľ zasiela do 31. marca roku N + 1 Európskemu parlamentu, Rade, Komisii a Dvoru audítorov správu o rozpočtovom a finančnom hospodárení.

7. Účtovník agentúry ENISA do 1. júla roku N + 1 zasiela konečnú účtovnú závierku agentúry ENISA Európskemu parlamentu, Rade, účtovníkovi Komisie a Dvoru audítorov spolu so stanoviskom správnej rady.

([28]) Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046 z 18. júla 2018 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Únie, o zmene nariadení (EÚ) č. 1296/2013, (EÚ) č. 1301/2013, (EÚ) č. 1303/2013, (EÚ) č. 1304/2013, (EÚ) č. 1309/2013, (EÚ) č. 1316/2013, (EÚ) č. 223/2014, (EÚ) č. 283/2014 a rozhodnutia č. 541/2014/EÚ a o zrušení nariadenia (EÚ, Euratom) č. 966/2012 (Ú. v. EÚ L 193, 30.7.2018, s. 1).

8. V deň zaslania konečnej účtovnej závierky agentúry ENISA účtovník agentúry ENISA zároveň zašle Dvoru audítorov vyhlásenie k tejto konečnej účtovnej závierke a jeho kópiu zašle účtovníkovi Komisie.

9. Výkonný riaditeľ uverejňuje konečnú účtovnú závierku agentúry ENISA do 15. novembra roku N + 1 v *Úradnom vestníku Európskej únie*.

10. Výkonný riaditeľ zasiela Dvoru audítorov do 30. septembra roku N + 1 odpoveď na jeho pripomienky, pričom kópiu tejto odpovede zašle správnej rade a Komisii.

11. Výkonný riaditeľ predloží Európskemu parlamentu na jeho žiadosť všetky informácie potrebné na bezproblémové uplatnenie postupu udelenia absolutória za dotknutý rozpočtový rok v súlade s článkom 261 ods. 3 nariadenia (EÚ, Euratom) 2018/1046.

12. Európsky parlament na odporúčanie Rady udelí do 15. mája roku N + 2 výkonnému riaditeľovi absolutórium za plnenie rozpočtu za rok N.

Článok 32

Rozpočtové pravidlá

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

Článok 33

Boj proti podvodom

1. V záujme uľahčenia boja proti podvodom, korupcii a iným nezákonným činnostiam podľa nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013 ([29]) agentúra ENISA do 28. decembra 2019 pristúpi k Medziinštitucionálnej dohode z 25. mája 1999 medzi Európskym parlamentom, Radou Európskej únie a Komisiou Európskych spoločenstiev, ktorá sa týka vnútorných vyšetrovaní Európskym úradom pre boj proti podvodom (OLAF) ([30]). Agentúra ENISA prijme vhodné ustanovenia uplatniteľné na všetkých zamestnancov agentúry ENISA, pričom použije vzor uvedený v prílohe k uvedenej dohode.

2. Dvor audítorov má právomoc na základe kontrol dokumentov a kontrol na mieste vykonať audit u všetkých príjemcov grantov, dodávateľov a subdodávateľov, ktorým boli poskytnuté finančné prostriedky Únie od agentúry ENISA.

3. Úrad OLAF môže vykonávať vyšetrovania vrátane kontrol a inšpekcií na mieste v súlade s ustanoveniami a postupmi stanovenými v nariadení (EÚ, Euratom) č. 883/2013 a v nariadení Rady (Euratom, ES) č. 2185/96 ([31])s cieľom zistiť, či v súvislosti s grantom alebo zmluvou financovanými agentúrou ENISA nedošlo k podvodu, korupcii alebo akémukoľvek inému protiprávnemu konaniu poškodzujúcemu finančné záujmy Únie.

4. Bez toho, aby boli dotknuté odseky 1, 2 a 3, dohody o spolupráci s tretími krajinami alebo s medzinárodnými organizáciami, zmluvy, dohody o grante a rozhodnutia o grante uzatvorené alebo prijaté agentúrou ENISA obsahujú ustanovenia, ktoré výslovne udeľujú Dvoru audítorov a úradu OLAF právomoc vykonávať takéto audity a vyšetrovania v súlade s ich príslušnými právomocami.

([29]) Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013 z 11. septembra 2013 o vyšetrovaniach vykonávaných Európskym úradom pre boj proti podvodom (OLAF), ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady (ES) č. 1073/1999 a nariadenie Rady (Euratom) č. 1074/1999 (Ú. v. EÚ L 248, 18.9.2013, s. 1).

([30]) Ú. v. ES L 136, 31.5.1999, s. 15.

([31]) Nariadenie Rady (Euratom, ES) č. 2185/96 z 11 novembra 1996 o kontrolchách a inšpekciách na mieste, vykonávaných Komisiou s cieľom ocharany finančn ých záujmov Európskych spoločenstiev pred spreneverou a inými podvodmi (Ú. v. ES L 292, 15.11.1996, s. 2).

KAPITOLA V

Zamestnanci

Článok 34

Všeobecné ustanovenia

Na zamestnancov agentúry ENISA sa vzťahuje služobný poriadok úradníkov a podmienky zamestnávania ostatných zamestnancov, ako aj pravidlá prijaté na základe dohody medzi inštitúciami Únie na účely uvedenia služobného poriadku úradníkov a podmienok zamestnávania ostatných zamestnancov do platnosti.

Článok 35

Výsady a imunity

Na agentúru ENISA a jej personál sa vzťahuje Protokol č. 7 o výsadách a imunitách Európskej únie pripojený k Zmluve o EÚ a k ZFEÚ.

Článok 36

Výkonný riaditeľ

1. Výkonný riaditeľ pôsobí ako dočasný zamestnanec agentúry ENISA podľa článku 2 písm. a) podmienok zamestnávania ostatných zamestnancov.

2. Výkonného riaditeľa vymenúva správna rada zo zoznamu kandidátov navrhnutých Komisiou na základe otvoreného a transparentného výberového konania.

3. Na účely uzatvorenia pracovnej zmluvy s výkonným riaditeľom zastupuje agentúru ENISA predseda správnej rady.

4. Kandidát, ktorého vybrala správna rada, sa pred vymenovaním vyjadrí pred príslušným výborom Európskeho parlamentu a odpovie na otázky jeho členov.

5. Funkčné obdobie výkonného riaditeľa je päť rokov. Pred koncom tohto obdobia Komisia vykoná posúdenie výsledkov činnosti výkonného riaditeľa a budúcich úloh a výziev agentúry ENISA.

6. Správna rada prijíma rozhodnutia o vymenovaní výkonného riaditeľa, predĺžení jeho funkčného obdobia alebo jeho odvolaní z funkcie v súlade s článkom 18 ods. 2.

7. Správna rada konajúc na návrh Komisie, v ktorom sa zohľadní posúdenie uvedené v odseku 5, môže jedenkrát predĺžiť funkčné obdobie výkonného riaditeľa o päť rokov.

8. Správna rada informuje Európsky parlament o svojom úmysle predĺžiť funkčné obdobie výkonného riaditeľa. Počas troch mesiacov pred takýmto predĺžením funkčného obdobia sa výkonný riaditeľ, ak k tomu bude vyzvaný, vyjadrí pred príslušným výborom Európskeho parlamentu a odpovie na otázky jeho členov.

9. Výkonný riaditeľ, ktorého funkčné obdobie sa predĺžilo, sa nemôže zúčastniť na ďalšom výberovom konaní na rovnakú funkciu.

10. Výkonný riaditeľ môže byť odvolaný z funkcie len na základe rozhodnutia správnej rady, ktorá koná na návrh Komisie.

Článok 37

Vyslaní národní experti a ďalší personál

1. Agentúra ENISA môže využívať vyslaných národných expertov alebo ďalší personál, ktorý agentúra ENISA nezamestnáva. Služobný poriadok úradníkov a podmienky zamestnávania ostatných zamestnancov sa na takýto personál nevzťahujú.

2. Správna rada prijme rozhodnutie, v ktorom stanoví pravidlá vysielania národných expertov do agentúry ENISA.

KAPITOLA VI

Všeobecné ustanovenia týkajúce sa agentúry ENISA

Článok 38

Právne postavenie agentúry ENISA

1. Agentúra ENISA je orgánom Únie a má právnu subjektivitu.

2. Agentúra ENISA má v každom členskom štáte najširšiu právnu spôsobilosť, akú jeho právo priznáva právnickým osobám. Môže najmä nadobúdať hnuteľný a nehnuteľný majetok a scudzovať ho, ako aj byť účastníkom súdnych konaní.

3. Agentúru ENISA zastupuje výkonný riaditeľ.

Článok 39

Zodpovednosť agentúry ENISA

1. Zmluvná zodpovednosť agentúry ENISA sa spravuje rozhodným právom pre danú zmluvu.

2. Súdny dvor Európskej únie má právomoc rozhodovať podľa akejkoľvek rozhodcovskej doložky obsiahnutej v zmluve uzatvorenej agentúrou ENISA.

3. V prípade mimozmluvnej zodpovednosti agentúra ENISA nahradí v súlade so všeobecnými zásadami spoločnými pre práva členských štátov všetky škody, ktoré spôsobila alebo ktoré spôsobil jej personál pri vykonávaní svojich povinností.

4. Vo všetkých sporoch súvisiacich s náhradou škody podľa odseku 3 má právomoc rozhodovať Súdny dvor Európskej únie.

5. Osobná zodpovednosť personálu agentúry ENISA voči nej sa riadi príslušnými podmienkami uplatniteľnými na personál agentúry ENISA.

Článok 40

Jazykový režim

1. Na agentúru ENISA sa vzťahuje nariadenie Rady č. 1 ([32]). Členské štáty a ostatné nimi menované orgány sa môžu obrátiť na agentúru ENISA a dostať odpoveď v úradnom jazyku inštitúcií Únie podľa vlastného výberu.

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

Článok 41

Ochrana osobných údajov

1. Na spracúvanie osobných údajov agentúrou ENISA sa vzťahuje nariadenie (EÚ) 2018/1725.

2. Správna rada prijme vykonávacie predpisy uvedené v článku 45 ods. 3 nariadenia (EÚ) 2018/1725. Správna rada môže prijať dodatočné opatrenia potrebné na uplatňovanie nariadenia (EÚ) 2018/1725 agentúrou ENISA.

([32]) Nariadenie Rady č. 1 o používaní jazykov v Európskom hospodárskom spoločenstve (Ú. v. ES 17, 6.10.1958, s. 385/58).

Článok 42

Spolupráca s tretími krajinami a medzinárodnými organizáciami

1. V rozsahu potrebnom na dosiahnutie cieľov stanovených v tomto nariadení môže agentúra ENISA spolupracovať s príslušnými orgánmi tretích krajín alebo s medzinárodnými organizáciami. Na tento účel môže agentúra ENISA za podmienky predchádzajúceho schválenia Komisiou dohodnúť pracovné dojednania s orgánmi tretích krajín a medzinárodnými organizáciami. Uvedenými pracovnými dojednaniami nevznikajú Únii ani jej členským štátom žiadne právne záväzky.

2. Agentúra ENISA je otvorená účasti tretích krajín, ktoré na tento účel uzavreli dohody s Úniou. Podľa príslušných ustanovení takýchto dohôd sa stanovia pracovné dojednania, v ktorých sa stanoví najmä povaha, rozsah a spôsob účasti týchto tretích krajín na práci agentúry ENISA, vrátane ustanovení týkajúcich sa účasti na iniciatívach uskutočňovaných agentúrou ENISA, finančných príspevkov a personálnych otázok. Pokiaľ ide o personálne otázky, musia byť uvedené pracovné dojednania za každých okolností v súlade so služobným poriadkom úradníkov a podmienkami zamestnávania ostatných zamestnancov.

3. Správna rada prijme stratégiu pre vzťahy s tretími krajinami a medzinárodnými organizáciami v otázkach spadajúcich do právomoci agentúry ENISA. Komisia zabezpečí, aby agentúra ENISA vykonávala činnosti v rámci svojho mandátu a existujúceho inštitucionálneho rámca, a to uzavretím náležitých pracovných dojednaní s výkonným riaditeľom.

Článok 43

Bezpečnostné predpisy v oblasti ochrany citlivých neutajovaných skutočností a utajovaných skutočností

Agentúra ENISA po porade s Komisiou prijme bezpečnostné predpisy, v ktorých uplatní bezpečnostné zásady obsiahnuté v bezpečnostných predpisoch Komisie na ochranu citlivých neutajovaných skutočností a utajovaných skutočností Európskej únie podľa rozhodnutí (EÚ, Euratom) 2015/443 a 2015/444. Bezpečnostné predpisy agentúry ENISA zahŕňajú ustanovenia týkajúce sa výmeny, spracúvania a uchovávania takýchto skutočností.

Článok 44

Dohoda o sídle a prevádzkové podmienky

1. Potrebné dojednania o poskytnutí sídla agentúre ENISA v hostiteľskom členskom štáte a o zariadeniach, ktoré má daný členský štát sprístupniť, ako aj osobitné pravidlá, ktoré sa v hostiteľskom členskom štáte vzťahujú na výkonného riaditeľa, členov správnej rady, personál agentúry ENISA a členov ich rodín, sa stanovia v dohode o sídle, ktorá sa uzavrie medzi agentúrou ENISA a hostiteľským členským štátom po tom, ako ju schváli správna rada.

2. Hostiteľský členský štát agentúry ENISA vytvorí najlepšie možné podmienky s cieľom zabezpečiť riadne fungovanie agentúry ENISA so zreteľom na dostupnosť jej umiestnenia, zabezpečenie primeraných vzdelávacích zariadení pre deti členov personálu, vhodný prístup na trh práce, k sociálnemu zabezpečeniu a zdravotnej starostlivosti pre deti aj manželských partnerov členov personálu.

Článok 45

Administratívna kontrola

Na činnosť agentúry ENISA dohliada v súlade s článkom 228 ZFEÚ európsky ombudsman.

HLAVA III

RÁMEC CERTIFIKÁCIE KYBERNETICKEJ BEZPEČNOSTI

Článok 46

Európsky rámec certifikácie kybernetickej bezpečnosti

1. V záujme vytvorenia digitálneho jednotného trhu s produktmi IKT, službami IKT a procesmi IKT sa zriadi európsky rámec certifikácie kybernetickej bezpečnosti s cieľom zlepšiť podmienky fungovania vnútorného trhu zvýšením úrovne kybernetickej bezpečnosti v Únii a umožnením harmonizovaného prístupu na úrovni Únie k európskym systémom certifikácie kybernetickej bezpečnosti.

2. Európskym rámcom certifikácie kybernetickej bezpečnosti sa zabezpečuje mechanizmus zavádzania európskych systémov certifikácie kybernetickej bezpečnosti a osvedčovania, že produkty IKT, služby IKT a procesy IKT vyhodnotené v súlade s týmito systémami spĺňajú špecifikované bezpečnostné požiadavky s cieľom chrániť dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo funkcií či služieb, ktoré tieto produkty, služby a procesy poskytujú alebo sprístupňujú, a to počas ich celého životného cyklu.

Článok 47

Priebežný pracovný program Únie pre európsku certifikáciu kybernetickej bezpečnosti

1. Komisia uverejní priebežný pracovný program Únie pre európsku certifikáciu kybernetickej bezpečnosti (ďalej len „priebežný pracovný program Únie"), v ktorom sa určia strategické priority budúcich európskych systémov certifikácie kybernetickej bezpečnosti.

2. Priebežný pracovný program Únie obsahuje najmä zoznam produktov IKT, služieb IKT a procesov IKT alebo ich kategórií, ktoré sú spôsobilé mať prospech zo zahrnutia do rozsahu pôsobnosti európskeho systému certifikácie kybernetickej bezpečnosti.

3. Zahrnutie konkrétneho produktu IKT, služby IKT a procesu IKT alebo ich kategórií do priebežného pracovného programu Únie sa zakladá na jednom či viacerých z týchto dôvodov:

a) dostupnosť a rozvoj vnútroštátnych systémov certifikácie kybernetickej bezpečnosti, ktoré sa vzťahujú na konkrétnu kategóriu produktov IKT, služieb IKT alebo procesov IKT, a najmä pokiaľ ide o riziko fragmentácie;

b) príslušné právo alebo politika Únie alebo členského štátu;

c) dopyt na trhu;

d) vývoj v oblasti kybernetických hrozieb;

e) žiadosť o vypracovanie konkrétneho kandidátskeho systému zo strany ECCG.

4. Komisia náležite zohľadňuje stanoviská, ktoré k návrhu priebežného pracovného programu Únie vydala ECCG a skupina zainteresovaných strán pre certifikáciu.

5. Prvý priebežný pracovný program Únie sa uverejní do 28. júna 2020. Priebežný pracovný program Únie sa aktualizuje aspoň raz za tri roky a podľa potreby aj častejšie.

Článok 48

Žiadosť o európsky systém certifikácie kybernetickej bezpečnosti

1. Komisia môže požiadať agentúru ENISA, aby vypracovala kandidátsky systém alebo preskúmala existujúci európsky systém certifikácie kybernetickej bezpečnosti na základe priebežného pracovného programu Únie.

2. V riadne odôvodnených prípadoch môže Komisia alebo ECCG požiadať agentúru ENISA, aby vypracovala kandidátsky systém alebo preskúmala existujúci európsky systém certifikácie kybernetickej bezpečnosti, ktorý nie je zahrnutý v priebežnom pracovnom programe Únie. Priebežný pracovný program Únie sa zodpovedajúcim spôsobom aktualizuje.

Článok 49

Vypracovanie, prijatie a preskúmanie európskeho systému certifikácie kybernetickej bezpečnosti

1. Na žiadosť Komisie podľa článku 48 vypracuje agentúra ENISA kandidátsky systém, ktorý spĺňa požiadavky stanovené v článkoch 51, 52 a 54.

2. Na žiadosť ECCG podľa článku 48 ods. 2 môže agentúra ENISA vypracovať kandidátsky systém, ktorý spĺňa požiadavky stanovené v článkoch 51, 52 a 54. Ak agentúra ENISA takúto žiadosť zamietne, musí toto zamietnutie odôvodniť. Rozhodnutie o zamietnutí takejto žiadosti prijíma správna rada.

3. Keď agentúra ENISA vypracúva kandidátsky systém, vedie so všetkými príslušnými zainteresovanými stranami formálne, otvorené, transparentné a inkluzívne konzultácie.

4. Pre každý kandidátsky systém agentúra ENISA zriadi ad hoc pracovnú skupinu v súlade s článkom 20 ods. 4, ktorej účelom je poskytovať agentúre ENISA špecifické poradenstvo a odborné znalosti.

5. Agentúra ENISA úzko spolupracuje s ECCG. ECCG poskytuje agentúre ENISA pri vypracúvaní kandidátskeho systému pomoc a odborné poradenstvo a prijíma stanovisko ku kandidátskemu systému.

6. Pred tým, než agentúra ENISA zašle kandidátsky systém vypracovaný podľa odsekov 3, 4 a 5 Komisii, v čo najväčšej miere zohľadní stanovisko ECCG. Stanovisko ECCG nie je pre agentúru ENISA záväzné a ani skutočnosť, že nebolo vydané, nebráni agentúre ENISA v zaslaní kandidátskeho systému Komisii.

7. Komisia môže na základe kandidátskeho systému pripraveného agentúrou ENISA prijať vykonávacie akty, v ktorých sa stanoví európsky systém certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT, ktoré spĺňa požiadavky stanovené v článkoch 51, 52 a 54. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 66 ods. 2.

8. Agentúra ENISA aspoň každých päť rokov preskúma každý prijatý európsky systém certifikácie kybernetickej bezpečnosti, pričom berie do úvahy spätnú väzbu zainteresovaných strán. Ak je to potrebné, Komisia alebo ECCG môžu požiadať agentúru ENISA, aby začala proces vypracovania revidovaného kandidátskeho systému v súlade s článkom 48 a týmto článkom.

Článok 50

Webové sídlo pre európske systémy certifikácie kybernetickej bezpečnosti

1. Agentúra ENISA udržiava vyhradené webové sídlo, ktoré propaguje a poskytuje informácie o európskych systémoch certifikácie kybernetickej bezpečnosti, európskych certifikátoch kybernetickej bezpečnosti a EÚ vyhláseniach o zhode, vrátane informácií o európskych systémoch certifikácie kybernetickej bezpečnosti, ktoré už nie sú platné, o európskych certifikátoch kybernetickej bezpečnosti a EÚ vyhláseniach o zhode, ktoré boli odňaté alebo ktorým uplynula platnosť, a o registri odkazov na informácie o kybernetickej bezpečnosti poskytované v súlade s článkom 55.

2. Na webovom sídle uvedenom v odseku 1 sa uvádzajú aj vnútroštátne systémy certifikácie kybernetickej bezpečnosti, ktoré boli nahradené európskym systémom certifikácie kybernetickej bezpečnosti.

Článok 51

Bezpečnostné ciele európskych systémov certifikácie kybernetickej bezpečnosti

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

a) chrániť uchovávané, prenášané alebo inak spracúvané údaje pred náhodným či neoprávneným uchovávaním, spracúvaním, prístupom alebo poskytnutím počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;

b) chrániť uchovávané, prenášané alebo inak spracúvané údaje pred náhodným či neoprávneným zničením, stratou alebo zmenou alebo nedostatočnou dostupnosťou počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;

c) umožňovať oprávneným osobám, programom alebo zariadeniam prístup výlučne k tým údajom, službám alebo funkciám, na ktoré sa vzťahujú ich prístupové práva;

d) identifikovať a dokumentovať známe závislosti a zraniteľnosti;

e) zaznamenávať, ktoré údaje, služby alebo funkcie boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;

f) umožňovať overenie, ktoré údaje, služby alebo funkcie boli predmetom prístupu, použité alebo inak spracúvané, kedy a kým;

g) overovať, či produkty IKT, služby IKT a procesy IKT neobsahujú známe zraniteľnosti;

h) v prípade fyzického alebo technického incidentu včas obnoviť dostupnosť údajov, služieb a funkcií a prístup k nim;

i) aby produkty IKT, služby IKT a procesy IKT boli bezpečné štandardne a už v štádiu návrhu;

j) aby sa produkty IKT, služby IKT a procesy IKT dodávali alebo poskytovali s aktualizovaným softvérom a hardvérom, ktoré neobsahujú verejne známe zraniteľnosti, a dodávali alebo poskytovali s mechanizmami na bezpečnú aktualizáciu.

Článok 52

Stupne dôveryhodnosti európskych systémov certifikácie kybernetickej bezpečnosti

1. Európsky systém certifikácie kybernetickej bezpečnosti môže uvádzať jeden alebo viacero z týchto stupňov dôveryhodnosti pre produkty IKT, služby IKT a procesy IKT: „základný“, „pokročilý“ alebo „vysoký“. Stupeň dôveryhodnosti zodpovedá úrovni rizika spojeného s plánovaným využívaním daného produktu IKT, služby IKT alebo procesu IKT z hľadiska pravdepodobnosti a vplyvu incidentu.

2. Európske certifikáty kybernetickej bezpečnosti a EÚ vyhlásenia o zhode odkazujú na stupeň dôveryhodnosti uvedený v európskom systéme certifikácie kybernetickej bezpečnosti, podľa ktorého je vydaný európsky certifikát kybernetickej bezpečnosti alebo EÚ vyhlásenie o zhode.

3. Bezpečnostné požiadavky zodpovedajúce každému stupňu dôveryhodnosti sa uvádzajú v príslušnom európskom systéme certifikácie kybernetickej bezpečnosti vrátane zodpovedajúcich bezpečnostných funkcií a zodpovedajúcej prísnosti a hĺbky hodnotenia, ktorým má produkt IKT, služba IKT alebo proces IKT prejsť.

4. Certifikát alebo EÚ vyhlásenie o zhode odkazujú na súvisiace technické špecifikácie, normy a postupy vrátane technických kontrol, ktorých účelom je znížiť riziko kybernetických bezpečnostných incidentov alebo týmto incidentom predísť.

5. Európsky certifikát kybernetickej bezpečnosti alebo EÚ vyhlásenie o zhode, v ktorom sa odkazuje na stupeň dôveryhodnosti „základný“, poskytuje uistenie, že produkty IKT, služby IKT a procesy IKT, pre ktoré je vydaný uvedený certifikát alebo uvedené EÚ vyhlásenie o zhode, spĺňajú zodpovedajúce bezpečnostné požiadavky vrátane bezpečnostných funkcií a že boli hodnotené na úrovni určenej na minimalizovanie známych základných rizík incidentov a kybernetických útokov. Hodnotiace činnosti, ktoré sa majú vykonať, zahŕňajú aspoň preskúmanie technickej dokumentácie. V prípade, keď takéto preskúmanie nie je vhodné, vykonajú sa náhradné hodnotiace činnosti s rovnocenným účinkom.

6. Európsky certifikát kybernetickej bezpečnosti, v ktorom sa odkazuje na stupeň dôveryhodnosti „pokročilý“, poskytuje uistenie, že produkty IKT, služby IKT a procesy IKT, pre ktoré je vydaný uvedený certifikát, spĺňajú zodpovedajúce bezpečnostné požiadavky vrátane bezpečnostných funkcií a že boli hodnotené na úrovni určenej na minimalizovanie známych kybernetickobezpečnostných rizík a rizík incidentov a kybernetických útokov, ktoré vykonávajú subjekty s obmedzenými zručnosťami a zdrojmi. Hodnotiace činnosti, ktoré sa majú vykonať, zahŕňajú aspoň preskúmanie na preukázanie neexistencie verejne známych zraniteľností a skúšku na preukázanie, že produkty IKT, procesy IKT alebo služby IKT správne plnia potrebné bezpečnostné funkcie. V prípade, keď takéto hodnotiace činnosti nie sú vhodné, vykonajú sa náhradné hodnotiace činnosti s rovnocenným účinkom.

7. Európsky certifikát kybernetickej bezpečnosti, v ktorom sa odkazuje na stupeň dôveryhodnosti „vysoký“, poskytuje uistenie, že produkty IKT, služby IKT a procesy IKT, pre ktoré je vydaný uvedený certifikát, spĺňajú zodpovedajúce bezpečnostné požiadavky vrátane bezpečnostných funkcií a že boli hodnotené na úrovni určenej na minimalizovanie rizika najpokročilejších kybernetických útokov, ktoré vykonávajú subjekty so značnými zručnosťami a zdrojmi. Hodnotiace činnosti, ktoré sa majú vykonať, zahŕňajú aspoň preskúmanie na preukázanie neexistencie verejne známych zraniteľností, skúšku na preukázanie, že produkty IKT, služby IKT alebo procesy IKT správne plnia najpokročilejšie potrebné bezpečnostné funkcie, a posúdenie ich odolnosti proti zručným útočníkom prostredníctvom skúšky prieniku. V prípade, keď takéto hodnotiace činnosti nie sú vhodné, vykonajú sa náhradné hodnotiace činnosti s rovnocenným účinkom.

8. Európsky systém certifikácie kybernetickej bezpečnosti môže špecifikovať viaceré úrovne hodnotenia v závislosti od prísnosti a hĺbky použitej metodiky hodnotenia. Každá z úrovní hodnotenia zodpovedá jednému zo stupňov dôveryhodnosti a je vymedzená vhodnou kombináciou zložiek dôveryhodnosti.

Článok 53

Vlastné posúdenie zhody

1. Európsky systém certifikácie kybernetickej bezpečnosti môže povoliť vlastné posúdenie zhody, za ktoré nesie výhradnú zodpovednosť výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT. Vlastné posúdenie zhody je povolené iba v súvislosti s produktmi IKT, službami IKT a procesmi IKT, ktoré predstavujú nízke riziko zodpovedajúce stupňu dôveryhodnosti „základný“.

2. Výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT môže vydať EÚ vyhlásenie o zhode, ktorým potvrdí, že sa preukázalo splnenie požiadaviek stanovených v systéme. Vydaním takéhoto vyhlásenia preberá výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT zodpovednosť za súlad produktu IKT, služby IKT alebo procesu IKT s požiadavkami stanovenými v uvedenom systéme.

3. Výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT uchováva EÚ vyhlásenie o zhode, technickú dokumentáciu a všetky ďalšie relevantné informácie, ktoré sa týkajú zhody produktov IKT alebo služieb IKT so systémom, k dispozícii pre vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti uvedený v článku 58 počas obdobia stanoveného v príslušnom európskom systéme certifikácie kybernetickej bezpečnosti. Kópia EÚ vyhlásenia o zhode sa predloží vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti a agentúre ENISA.

4. Vydanie EÚ vyhlásenia o zhode je dobrovoľné, pokiaľ nie je stanovené inak v práve Únie alebo v práve členského štátu.

5. EÚ vyhlásenia o zhode sa uznávajú vo všetkých členských štátoch.

Článok 54

Prvky európskych systémov certifikácie kybernetickej bezpečnosti

1. Európsky systém certifikácie kybernetickej bezpečnosti zahŕňa minimálne tieto prvky:

a) predmet úpravy a rozsah pôsobnosti daného certifikačného systému vrátane typu alebo kategórií produktov IKT, služieb IKT a procesov IKT, na ktoré sa vzťahuje;

b) jasný opis účelu systému a toho, ako zvolené normy, metódy hodnotenia a stupne dôveryhodnosti zodpovedajú potrebám užívateľov, ktorým je systém určený;

c) odkaz na medzinárodné, európske alebo vnútroštátne normy používané pri hodnotení alebo, ak také normy nie sú k dispozícii alebo nie sú vhodné, na technické špecifikácie, ktoré spĺňajú požiadavky stanovené v prílohe II k nariadeniu (EÚ) č. 1025/2012, alebo ak takéto špecifikácie nie sú k dispozícii, na technické špecifikácie alebo iné požiadavky kybernetickej bezpečnosti vymedzené európskom systéme certifikácie kybernetickej bezpečnosti;

d) podľa potreby jeden alebo viacero stupňov dôveryhodnosti;

e) informáciu o tom, či je v rámci daného systému povolené vlastné posúdenie zhody;

f) prípadné osobitné alebo dodatočné požiadavky na orgány posudzovania zhody s cieľom zabezpečiť ich technickú spôsobilosť na hodnotenie požiadaviek kybernetickej bezpečnosti;

g) konkrétne hodnotiace kritériá a metódy, ktoré sa majú použiť vrátane typov hodnotenia s cieľom preukázať, že sa dosiahli bezpečnostné ciele uvedené v článku 51;

h) prípadné informácie, ktoré sú potrebné na certifikáciu a ktoré má orgánom posudzovania zhody poskytnúť alebo inak sprístupniť žiadateľ;

i) ak systém zahŕňa označenia alebo značky, podmienky, za ktorých možno takéto označenia alebo značky použiť;

j) pravidlá monitorovania súladu produktov IKT, služieb IKT a procesov IKT s požiadavkami európskych certifikátov kybernetickej bezpečnosti alebo EÚ vyhlásení o zhode vrátane mechanizmov na preukázanie trvalého súladu so stanovenými požiadavkami kybernetickej bezpečnosti;

k) prípadné podmienky vydania, zachovania, pokračovania platnosti a obnovenia európskych certifikátov kybernetickej bezpečnosti, ako aj podmienky pre rozšírenie alebo zúženie rozsahu certifikácie;

l) pravidlá týkajúce sa dôsledkov pre produkty IKT, služby IKT a procesy IKT, ktoré boli certifikované alebo pre ktoré bolo vydané EÚ vyhlásenie o zhode, ale ktoré nespĺňajú požiadavky systému;

m) pravidlá nahlasovania a riešenia predtým nezistených zraniteľností produktov IKT, služieb IKT a procesov IKT z hľadiska kybernetickej bezpečnosti;

n) prípadné pravidlá uchovávania záznamov orgánmi posudzovania zhody;

o) určenie vnútroštátnych alebo medzinárodných systémov certifikácie kybernetickej bezpečnosti, ktoré sa vzťahujú na rovnaký typ alebo kategóriu produktov IKT, služieb IKT a procesov IKT, bezpečnostných požiadaviek, kritérií a metód hodnotenia a stupňov dôveryhodnosti;

p) obsah a podoba európskych certifikátov kybernetickej bezpečnosti a EÚ vyhlásení o zhode, ktoré majú byť vydané;

q) obdobie, počas ktorého výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT má uchovávať k dispozícii EÚ vyhlásenie o zhode, technickú dokumentáciu a všetky ďalšie relevantné informácie;

r) maximálne obdobie platnosti európskych certifikátov kybernetickej bezpečnosti vydaných v rámci systému;

s) politiku zverejňovania informácií o európskych certifikátoch kybernetickej bezpečnosti, ktoré boli vydané, zmenené alebo odňaté v rámci systému;

t) podmienky vzájomného uznávania systémov certifikácie s tretími krajinami;

u) prípadné pravidlá týkajúce sa mechanizmu partnerského preskúmania, ktorý je stanovený systémom pre orgány alebo subjekty vydávajúce európske certifikáty kybernetickej bezpečnosti pre stupeň dôveryhodnosti „vysoký“ podľa článku 56 ods. 6 Tento mechanizmus sa uplatňuje bez toho, aby bolo dotknuté partnerské preskúmanie stanovené v článku 59;

v) formát a postupy, ktoré musia dodržiavať výrobcovia alebo poskytovatelia produktov IKT, služieb IKT alebo procesov IKT pri poskytovaní a aktualizácii doplňujúcich informácií o kybernetickej bezpečnosti v súlade s článkom 55.

2. Stanovené požiadavky európskeho systému certifikácie kybernetickej bezpečnosti musia byť v súlade s akýmikoľvek platnými právnymi požiadavkami, najmä s požiadavkami, ktoré vyplývajú z harmonizovaného práva Únie.

3. Ak sa to stanovuje v osobitnom právnom akte Únie, certifikát alebo EÚ vyhlásenie o zhode vydané v rámci európskeho systému certifikácie kybernetickej bezpečnosti možno použiť na preukázanie predpokladu zhody s požiadavkami daného právneho aktu.

4. Ak harmonizované právo Únie neexistuje, v práve členských štátov možno tiež stanoviť, že európsky systém certifikácie kybernetickej bezpečnosti možno použiť na stanovenie predpokladu zhody s právnymi požiadavkami.

Článok 55

Doplňujúce informácie o kybernetickej bezpečnosti týkajúce sa certifikovaných produktov IKT, služieb IKT a procesov IKT

1. Výrobca alebo poskytovateľ certifikovaných produktov IKT, služieb IKT alebo procesov IKT alebo produktov IKT, služieb IKT a procesov IKT, pre ktoré bolo vydané EÚ vyhlásenie o zhode, zverejňuje tieto doplňujúce informácie o kybernetickej bezpečnosti:

a) poradenstvo a odporúčania s cieľom pomôcť koncovým užívateľom s bezpečnou konfiguráciou, inštaláciou, zavedením, prevádzkou a údržbou výrobkov IKT alebo služieb IKT;

b) obdobie, počas ktorého sa bude koncovým užívateľom poskytovať bezpečnostná podpora, a to najmä pokiaľ ide o dostupnosť aktualizácií, ktoré sa týkajú kybernetickej bezpečnosti;

c) kontaktné informácie výrobcu alebo poskytovateľa a akceptované metódy na prijímanie informácií o zraniteľnosti od koncových užívateľov a výskumníkov v oblasti bezpečnosti;

d) odkaz na registre online, ktoré uvádzajú zverejnené zraniteľnosti týkajúce sa daného produktu IKT, služby IKT alebo procesu IKT a všetky príslušné kybernetickobezpečnostné rady.

2. Informácie uvedené v odseku 1 musia byť k dispozícii v elektronickej forme a zostávajú k dispozícii a podľa potreby sa aktualizujú aspoň do skončenia platnosti príslušného európskeho certifikátu kybernetickej bezpečnosti alebo EÚ vyhlásenia o zhode.

Článok 56

Certifikácia kybernetickej bezpečnosti

1. Produkty IKT, služby IKT a procesy IKT certifikované v rámci európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa článku 49 sa považujú za vyhovujúce požiadavkám daného systému.

2. Pokiaľ sa v práve Únie alebo práve členského štátu nestanovuje inak, certifikácia kybernetickej bezpečnosti je dobrovoľná.

3. Komisia pravidelne posúdi účinnosť a využívanie prijatých európskych systémov certifikácie kybernetickej bezpečnosti a či sa niektorý konkrétny európsky systém certifikácie kybernetickej bezpečnosti má stať záväzným prostredníctvom príslušného práva Únie s cieľom zaistiť primeranú úroveň kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT v Únii a zlepšiť fungovanie vnútorného trhu. Prvé takéto posúdenie sa vykoná do 31. decembra 2023 a následné posúdenia sa potom vykonávajú aspoň každé dva roky. Komisia na základe výsledkov uvedených posúdení určí produkty IKT, služby IKT a procesy IKT, na ktoré sa vzťahuje existujúci certifikačný systém a na ktoré sa má vzťahovať povinný certifikačný systém.

Prioritne sa Komisia zameria na odvetvia uvedené v prílohe II k smernici (EÚ) 2016/1148, ktoré sa posúdia najneskôr do dvoch rokov po prijatí prvého európskeho systému certifikácie kybernetickej bezpečnosti.

Pri príprave posúdenia Komisia:

a) zohľadní vplyv opatrení na výrobcov alebo poskytovateľov takýchto produktov IKT, služieb IKT alebo procesov IKT a na užívateľov z hľadiska nákladov uvedených opatrení a spoločenských alebo ekonomických prínosov vyplývajúcich z predpokladanej zvýšenej úrovne bezpečnosti cielených produktov IKT, služieb IKT alebo procesov IKT;

b) zohľadní existenciu a vykonávanie príslušného práva členského štátu alebo práva tretej krajiny;

c) vykoná otvorené, transparentné a inkluzívne konzultácie so všetkými príslušnými zainteresovanými stranami a členskými štátmi;

d) zohľadní všetky lehoty na vykonávanie, prechodné opatrenia a obdobia, najmä s ohľadom na možný vplyv daného opatrenia na výrobcov alebo poskytovateľov produktov IKT, služieb IKT a procesov IKT vrátane MSP;

e) navrhne najrýchlejší a najefektívnejší spôsob vykonania prechodu z dobrovoľných na povinné certifikačné systémy.

4. Európske certifikáty kybernetickej bezpečnosti podľa tohto článku, ktoré odkazujú na stupeň dôveryhodnosti „základný“ alebo „pokročilý“, vydávajú orgány posudzovania zhody uvedené v článku 60 na základe kritérií zahrnutých v európskom systéme certifikácie kybernetickej bezpečnosti prijatom Komisiou podľa článku 49.

5. Odchylne od odseku 4 sa v riadne odôvodnených prípadoch môže v európskom systéme certifikácie kybernetickej bezpečnosti stanoviť, že európske certifikáty kybernetickej bezpečnosti podľa daného systému má vydávať len verejný subjekt. Takýmto subjektom je:

a) vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti uvedený v článku 58 ods. 1 alebo

b) verejný subjekt, ktorý je akreditovaný ako orgán posudzovania zhody podľa článku 60 ods. 1.

6. Ak európsky systém certifikácie kybernetickej bezpečnosti prijatý podľa článku 49 vyžaduje stupeň dôveryhodnosti „vysoký“, európsky certifikát kybernetickej bezpečnosti podľa uvedeného systému má vydávať len vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti alebo v týchto prípadoch orgán posudzovania zhody:

a) vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti najprv schváli každý jednotlivý európsky certifikát kybernetickej bezpečnosti, ktorý vydal orgán posudzovania zhody, alebo

b) vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti poveril úlohou vydávať takéto európske certifikáty kybernetickej bezpečnosti orgán posudzovania zhody na základe všeobecného delegovania.

7. Fyzická či právnická osoba, ktorá predkladá produkty IKT, služby IKT alebo procesy IKT na certifikáciu, sprístupní vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti uvedenému v článku 58, ak tento orgán vydáva európsky certifikát kybernetickej bezpečnosti, alebo orgánu posudzovania zhody uvedenému v článku 60 všetky informácie potrebné pre certifikáciu.

8. Držiteľ európskeho certifikátu kybernetickej bezpečnosti informuje orgán uvedený v odseku 7 o všetkých následne zistených zraniteľnostiach alebo nezrovnalostiach týkajúcich sa bezpečnosti certifikovaného produktu IKT, služby IKT alebo procesu IKT, ktoré môžu mať vplyv na ich súlad s požiadavkami týkajúcimi sa certifikácie. Uvedený orgán bez zbytočného odkladu postúpi uvedené informácie dotknutému vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti.

9. Európsky certifikát kybernetickej bezpečnosti sa vydáva na obdobie stanovené v európskom systéme certifikácie kybernetickej bezpečnosti a možno ho obnoviť, pokiaľ sa naďalej plnia relevantné požiadavky.

10. Európsky certifikát kybernetickej bezpečnosti vydaný podľa tohto článku sa uznáva vo všetkých členských štátoch.

Článok 57

Vnútroštátne systémy certifikácie a certifikáty kybernetickej bezpečnosti

1. Bez toho, aby bol dotknutý odsek 3 tohto článku, vnútroštátne systémy certifikácie kybernetickej bezpečnosti a súvisiace postupy týkajúce sa produktov IKT, služieb IKT a procesov IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, strácajú účinnosť k dátumu stanovenému vo vykonávacom akte prijatom podľa článku 49 ods. 7 Vnútroštátne systémy certifikácie kybernetickej bezpečnosti a súvisiace postupy týkajúce sa produktov IKT, služieb IKT a procesov IKT, na ktoré sa európsky systém certifikácie kybernetickej bezpečnosti nevzťahuje, existujú naďalej.

2. Členské štáty nezavedú nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT, na ktoré sa už vzťahuje platný európsky systém certifikácie kybernetickej bezpečnosti.

3. Existujúce certifikáty, ktoré boli vydané v rámci vnútroštátnych systémov certifikácie kybernetickej bezpečnosti a na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, platia naďalej až do konca doby ich platnosti.

4. S cieľom predísť fragmentácii vnútorného trhu členské štáty informujú Komisiu a ECCG o akomkoľvek zámere vypracovať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti.

Článok 58

Vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti

1. Každý členský štát určí jeden alebo viacero vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti na svojom území alebo určí po dohode s iným členským štátom jeden alebo viacero vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti zriadených v tomto inom členskom štáte, ktoré budú zodpovedné za dozor v určujúcom členskom štáte.

2. Každý členský štát oznámi Komisii určené vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti. Ak členský štát určí viac orgánov, informuje Komisiu aj o úlohách zverených každému z nich.

3. Bez toho, aby bol dotknutý článok 56 ods. 5 písm. a) a článok 56 ods. 6, každý vnútroštátny orgány pre certifikáciu kybernetickej bezpečnosti je z hľadiska svojej organizácie, rozhodnutí o financovaní, právnej štruktúry a rozhodovania nezávislý od subjektov, nad ktorými vykonáva dozor.

4. Členské štáty zabezpečia, aby činnosti vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti, ktoré sa týkajú vydávania európskych certifikátov kybernetickej bezpečnosti podľa článku 56 ods. 5 písm. a) a článku 56 ods. 6, boli prísne oddelené od ich činností dohľadu stanovených v tomto článku, a aby uvedené činnosti boli vykonávané nezávisle od seba.

5. Členské štáty zabezpečia, aby vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti mali primerané zdroje na výkon svojich právomocí a aby svoje úlohy vykonávali účinne a efektívne.

6. V záujme účinného vykonávania tohto nariadenia je vhodné, aby sa vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti aktívne, účinne, efektívne a bezpečne zapájali do práce ECCG.

7. Vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti:

a) dozerajú nad pravidlami uvedenými v európskych systémoch certifikácie kybernetickej bezpečnosti podľa článku 54 ods. 1 písm. j), ktoré sa týkajú monitorovania súladu produktov IKT, služieb IKT a procesov IKT s požiadavkami európskych certifikátov kybernetickej bezpečnosti, ktoré boli vydané na ich príslušných územiach, a tieto pravidlá presadzujú, a to v spolupráci s ďalšími príslušnými orgánmi dohľadu nad trhom;

b) monitorujú dodržiavanie povinností výrobcov alebo poskytovateľov produktov IKT, služieb IKT alebo procesov IKT, ktorí sú usadení na ich príslušných územiach a vykonávajú vlastné posúdenie zhody, a tieto povinnosti presadzujú, a najmä monitorujú dodržiavanie povinností takýchto výrobcov alebo poskytovateľov stanovených v článku 53 ods. 2 a 3 a v príslušnom európskom systéme certifikácie kybernetickej bezpečnosti, a tieto povinnosti presadzujú;

c) bez toho, aby bol dotknutý článok 60 ods. 3, na účely tohto nariadenia aktívne pomáhajú vnútroštátnym akreditačným orgánom a podporujú ich pri monitorovaní činností orgánov posudzovania zhody a pri dozore nad týmito činnosťami;

d) monitorujú a dozerajú na činnosti verejných orgánov uvedených v článku 56 ods. 5;

e) prípadne splnomocňujú orgány posudzovania zhody v súlade s článkom 60 ods. 3 a obmedzujú, pozastavujú alebo odnímajú existujúce splnomocnenie, keď orgány posudzovania zhody nespĺňajú požiadavky tohto nariadenia;

f) vybavujú sťažnosti fyzických alebo právnických osôb v súvislosti s európskymi certifikátmi kybernetickej bezpečnosti vydanými vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti, alebo v súvislosti s európskymi certifikátmi kybernetickej bezpečnosti vydanými orgánmi posudzovania zhody v súlade s článkom 56 ods. 6, alebo v súvislosti s EÚ vyhláseniami o zhode vydanými podľa článku 53, a v primeranom rozsahu prešetrujú predmet takýchto sťažností a sťažovateľa v primeranej lehote informujú o pokroku a výsledku tohto prešetrenia;

g) agentúre ENISA a ECCG poskytujú výročnú súhrnnú správu o činnostiach vykonaných podľa písmen b), c) a d) tohto odseku alebo podľa odseku 8;

h) spolupracujú s inými vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti alebo inými orgánmi verejnej moci, čo zahŕňa poskytovanie informácií o možnom nesúlade produktov IKT, služieb IKT a procesov IKT s požiadavkami tohto nariadenia alebo s požiadavkami konkrétnych európskych systémov certifikácie kybernetickej bezpečnosti, a

i) monitorujú relevantný vývoj v oblasti certifikácie kybernetickej bezpečnosti.

8. Každý vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti má prinajmenšom tieto právomoci:

a) žiadať od orgánov posudzovania zhody, držiteľov európskych certifikátov kybernetickej bezpečnosti a vydavateľov EÚ vyhlásení o zhode akékoľvek informácie, ktoré potrebuje na plnenie svojich úloh;

b) viesť vyšetrovanie v podobe auditov orgánov posudzovania zhody, držiteľov európskych certifikátov kybernetickej bezpečnosti a vydavateľov EÚ vyhlásení o zhode na overenie, či dodržiavajú ustanovenia tejto hlavy;

c) prijímať primerané opatrenia v súlade s vnútroštátnym právom s cieľom zabezpečiť, aby orgány posudzovania zhody, držitelia európskych certifikátov kybernetickej bezpečnosti a vydavatelia EÚ vyhlásení o zhode dodržiavali toto nariadenie alebo európsky systém certifikácie kybernetickej bezpečnosti;

d) získať prístup do priestorov akýchkoľvek orgánov posudzovania zhody alebo držiteľov európskych certifikátov kybernetickej bezpečnosti na účely vykonávania vyšetrovaní v súlade s procesným právom Únie alebo členského štátu;

e) v súlade s vnútroštátnym právom odnímať európske certifikáty kybernetickej bezpečnosti, ktoré vydali vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti, alebo európske certifikáty kybernetickej bezpečnosti, ktoré v súlade s článkom 56 ods. 6 vydali orgány posudzovania zhody, ak takéto certifikáty nie sú v súlade s týmto nariadením alebo európskym systémom certifikácie kybernetickej bezpečnosti;

f) ukladať v súlade s vnútroštátnym právom sankcie podľa článku 65 a vyžadovať okamžité ukončenie porušovania povinností stanovených v tomto nariadení.

9. Vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti navzájom i s Komisiou spolupracujú, najmä si vymieňajú informácie, skúsenosti a osvedčené postupy, pokiaľ ide o certifikáciu kybernetickej bezpečnosti a technické otázky súvisiace s kybernetickou bezpečnosťou produktov IKT, služieb IKT a procesov IKT.

Článok 59

Partnerské preskúmanie

1. S cieľom dosiahnuť v súvislosti s európskymi certifikátmi kybernetickej bezpečnosti a EÚ vyhláseniami o zhode rovnaké normy v celej Únii podliehajú vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti partnerskému preskúmaniu.

2. Partnerské preskúmanie sa vykonáva na základe riadnych a transparentných hodnotiacich kritérií a postupov, ktoré sa vzťahujú najmä na štrukturálne požiadavky, požiadavky na ľudské zdroje a postupy, povinnosť mlčanlivosti a sťažnosti.

3. Partnerské preskúmanie posudzuje:

a) ak je to relevantné, či sú činnosti vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti, ktoré sa týkajú vydávania európskych certifikátov kybernetickej bezpečnosti podľa článku 56 ods. 5 písm. a) a článku 56 ods. 6, prísne oddelené od ich činností dozoru stanovených v článku 58 a či sa uvedené činnosti vykonávajú nezávisle od seba;

b) postupy dozoru a presadzovania pravidiel monitorovania súladu produktov IKT, služieb IKT a procesov IKT s európskymi certifikátmi kybernetickej bezpečnosti podľa článku 58 ods. 7 písm. a);

c) postupy monitorovania a presadzovania povinností výrobcov a poskytovateľov produktov IKT, služieb IKT alebo procesov IKT podľa článku 58 ods. 7 písm. b);

d) postupy monitorovania, splnomocňovania a dozoru, pokiaľ ide o činnosti orgánov posudzovania zhody;

e) ak je to relevantné, či personál orgánov, ktoré vydávajú certifikáty pre stupeň dôveryhodnosti „vysoký“ podľa článku 56 ods. 6, má primerané odborné znalosti.

4. Partnerské preskúmanie vykonávajú najmenej dva vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti iných členských štátov a Komisia a vykonáva sa aspoň raz za päť rokov. Agentúra ENISA sa môže zúčastňovať na partnerskom preskúmaní.

5. Komisia môže prijímať vykonávacie akty, v ktorých stanoví plán partnerského preskúmania na obdobie najmenej piatich rokov, kritériá zloženia tímu partnerského preskúmania, metodiku partnerského preskúmania a časový harmonogram, periodicitu a ďalšie úlohy súvisiace s partnerským preskúmaním. Pri prijímaní uvedených vykonávacích aktov Komisia náležite zohľadňuje názory ECCG. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 66 ods. 2

6. Výsledky partnerského preskúmania preskúma ECCG, ktorá vypracuje súhrnnú správu, ktorá sa môže sprístupniť verejnosti, a v prípade potreby vydá usmernenia alebo odporúčania týkajúce sa krokov alebo opatrení, ktoré majú prijať dotknuté subjekty.

Článok 60

Orgány posudzovania zhody

1. Orgány posudzovania zhody akreditujú vnútroštátne akreditačné orgány vymenované podľa nariadenia (ES) č. 765/2008. Takáto akreditácia sa vydá, len ak orgán posudzovania zhody spĺňa požiadavky stanovené v prílohe k tomuto nariadeniu.

2. Ak vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti vydal v súlade s článkom 56 ods. 5 písm. a) a článkom 56 ods. 6 európsky certifikát kybernetickej bezpečnosti, certifikačný orgán vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti sa akredituje ako orgán posudzovania zhody podľa odseku 1 tohto článku.

3. Ak sa v európskych systémoch certifikácie kybernetickej bezpečnosti stanovujú osobitné alebo dodatočné požiadavky podľa článku 54 ods. 1 písm. f), vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti splnomocňuje len orgány posudzovania zhody, ktoré spĺňajú uvedené požiadavky, aby vykonávali úlohy podľa takýchto systémov.

4. Akreditácia uvedená v odseku 1 sa udeľuje orgánom posudzovania zhody najviac na päť rokov a možno ju obnoviť za rovnakých podmienok, pokiaľ orgán posudzovania zhody naďalej spĺňa požiadavky stanovené v tomto článku. Vnútroštátne akreditačné orgány prijmú v primeranom časovom rámci všetky vhodné opatrenia s cieľom obmedziť, pozastaviť alebo zrušiť akreditáciu orgánu posudzovania zhody udelenú podľa odseku 1, ak orgán posudzovania zhody nespĺňa alebo prestal spĺňať akreditačné podmienky, alebo porušuje toto nariadenie

Článok 61

Oznamovanie

1. V súvislosti s každým európskym systémom certifikácie kybernetickej bezpečnosti oznámia vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti Komisii orgány posudzovania zhody akreditované a prípadne splnomocnené podľa článku 60 ods. 3 na vydávanie európskych certifikátov kybernetickej bezpečnosti v rámci určených stupňov dôveryhodnosti, ako sa uvádzajú článku 52. Vnútroštátne orgány pre certifikáciu kybernetickej bezpečnosti oznamujú Komisii bez zbytočného odkladu akékoľvek následné zmeny v tejto súvislosti.

2. Jeden rok po nadobudnutí účinnosti európskeho systému certifikácie kybernetickej bezpečnosti Komisia uverejní v *Úradnom vestníku Európskej únie* zoznam orgánov posudzovania zhody oznámených v rámci uvedeného systému.

3. Ak sa Komisii doručí oznámenie po lehote stanovenej v odseku 2, uverejní v *Úradnom vestníku Európskej únie* zmeny zoznamu oznámených orgánov posudzovania zhody do dvoch mesiacov od doručenia daného oznámenia.

4. Vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti môže Komisii predložiť žiadosť o vyňatie orgánu posudzovania zhody, ktorý daný vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti oznámil, zo zoznamu uvedeného v odseku 2. Komisia uverejní v *Úradnom vestníku Európskej únie* príslušné zmeny uvedeného zoznamu do jedného mesiaca od doručenia žiadosti vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti.

5. Komisia môže prijať vykonávacie akty stanovujúce okolnosti, podobu a postupy oznamovania uvedeného v odseku 1 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 66 ods. 2.

Článok 62

Európska skupina pre certifikáciu kybernetickej bezpečnosti

1. Zriadi sa európska skupina pre certifikáciu kybernetickej bezpečnosti (ďalej len „ECCG“ – European Cybersecurity Certification Group).

2. ECCG sa skladá zo zástupcov vnútroštátnych orgánov pre certifikáciu kybernetickej bezpečnosti alebo zástupcov iných príslušných vnútroštátnych orgánov. Žiaden člen ECCG nesmie zastupovať viac ako dva členské štáty.

3. Zainteresované strany a príslušné tretie strany môžu byť prizvané zúčastniť sa na stretnutiach ECCG a podieľať sa na jej práci.

4. ECCG má tieto úlohy:

a) radiť a pomáhať Komisii v jej úsilí o zabezpečenie konzistentného vykonávania a uplatňovania tejto hlavy, najmä pokiaľ ide o priebežný pracovný program Únie, politické otázky spojené s certifikáciou kybernetickej bezpečnosti, koordináciu politických prístupov a vypracovanie európskych systémov certifikácie kybernetickej bezpečnosti;

b) pomáhať a radiť agentúre ENISA a spolupracovať s ňou pri vypracúvaní kandidátskeho systému podľa článku 49;

c) prijímať stanovisko ku kandidátskym systémom vypracovaným agentúrou ENISA podľa článku 49;

d) požiadať agentúru ENISA o vypracovanie kandidátskych systémov podľa článku 48 ods. 2;

e) prijímať stanoviská určené Komisii, ktoré sa týkajú udržiavania a preskúmania existujúcich európskych systémov certifikácie kybernetickej bezpečnosti;

f) skúmať relevantný vývoj v oblasti certifikácie kybernetickej bezpečnosti a vymieňať si informácie a osvedčené postupy v oblasti systémov certifikácie kybernetickej bezpečnosti;

g) uľahčovať spoluprácu medzi vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti podľa tejto hlavy, a to budovaním kapacít a výmenou informácií, najmä zavedením metód efektívnej výmeny informácií o otázkach spojených s certifikáciou kybernetickej bezpečnosti;

h) podporovať vykonávanie mechanizmov partnerského preskúmania v súlade s pravidlami stanovenými v európskom systéme certifikácie kybernetickej bezpečnosti podľa článku 54 ods. 1 písm. u) tohto nariadenia;

i) uľahčovať zosúlaďovanie európskych systémov certifikácie kybernetickej bezpečnosti s medzinárodne uznanými normami, a to aj preskúmaním súčasných európskych systémov certifikácie kybernetickej bezpečnosti a prípadne vydaním odporúčaní pre agentúru ENISA, aby spolupracovala s príslušnými medzinárodnými normalizačnými organizáciami s cieľom riešiť nedostatky alebo rozdiely v dostupných medzinárodne uznávaných normách.

5. Komisia za pomoci agentúry ENISA predsedá ECCG a zabezpečuje pre ECCG sekretariát v súlade s článkom 8 ods. 1 písm. e).

Článok 63

Právo na podanie sťažnosti

1. Fyzické a právnické osoby majú právo podať sťažnosť vydavateľovi európskeho certifikátu kybernetickej bezpečnosti, alebo ak sťažnosť súvisí s európskym certifikátom kybernetickej bezpečnosti, ktorý vydal orgán posudzovania zhody konajúci v súlade s článkom 56 ods. 6, príslušnému vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti.

2. Orgán, ktorému sa sťažnosť podala, informuje sťažovateľa o pokroku daného konania a prijatom rozhodnutí a o práve na účinný súdny prostriedok nápravy podľa článku 64.

Článok 64

Právo na účinný súdny prostriedok nápravy

1. Bez ohľadu na akékoľvek administratívne alebo iné mimosúdne prostriedky nápravy, fyzické osoby a právnické osoby majú právo na účinný súdny prostriedok nápravy, pokiaľ ide o:

a) rozhodnutia prijaté orgánom uvedeným v článku 63 ods. 1, a to prípadne aj v súvislosti s nesprávnym vydaním, nevydaním alebo uznaním európskeho certifikátu kybernetickej bezpečnosti, ktorého držiteľmi sú uvedené fyzické a právnické osoby;

b) nekonanie vo veci sťažnosti podanej orgánu uvedenému v článku 63 ods. 1.

2. Konanie podľa tohto článku sa vedie na súdoch členského štátu, v ktorom sa nachádza orgán, proti ktorému súdny prostriedok nápravy smeruje.

Článok 65

Sankcie

Členské štáty stanovia pravidlá pokiaľ ide o sankcie uplatniteľné pri porušení tejto hlavy a porušení európskych systémov certifikácie kybernetickej bezpečnosti a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty bezodkladne oznámia uvedené pravidlá a opatrenia Komisii a informujú ju o všetkých následných zmenách, ktoré na ne majú vplyv.

HLAVA IV

ZÁVEREČNÉ USTANOVENIA

Článok 66

Postup výboru

1. Komisii pomáha výbor. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 ods. 4 písm. b) nariadenia (EÚ) č. 182/2011.

Článok 67

Hodnotenie a preskúmanie

1. Komisia do 28. júna 2024 a následne každých päť rokov vyhodnotí vplyv, účinnosť a efektívnosť agentúry ENISA a jej pracovných postupov, prípadnú potrebu upraviť mandát agentúry ENISA a finančné dôsledky takýchto prípadných úprav. Pri tomto hodnotení sa zohľadní každá spätná väzba, ktorú agentúra ENISA dostala v nadväznosti na svoje činnosti. Ak sa Komisia domnieva, že ďalšie fungovanie agentúry ENISA už nie je odôvodnené vzhľadom na ciele, mandát a úlohy jej zverené, môže navrhnúť zmenu tohto nariadenia z hľadiska ustanovení, ktoré sa týkajú agentúry ENISA.

2. V hodnotení sa zároveň posúdi vplyv, účinnosť a efektívnosť ustanovení hlavy III tohto nariadenia z hľadiska cieľov zabezpečiť primeranú úroveň kybernetickej bezpečnosti produktov IKT, služieb IKT a procesov IKT v Únii a zlepšiť fungovanie vnútorného trhu.

3. V hodnotení sa posúdi, či sú základné požiadavky kybernetickej bezpečnosti na prístup na vnútorný trh potrebné na to, aby sa zabránilo vstupu produktov IKT, služieb IKT a procesov IKT, ktoré nespĺňajú základné požiadavky kybernetickej bezpečnosti, na trh Únie.

4. Komisia do 28. júna 2024 a následne každých päť rokov zašle správu o hodnotení spolu s jej závermi Európskemu parlamentu, Rade a správnej rade. Zistenia uvedené v tejto správe sa zverejnia.

Článok 68

Zrušenie a nástupníctvo

1. Nariadenie (EÚ) č. 526/2013 sa zrušuje s účinnosťou od 27. júna 2019.

2. Odkazy na nariadenie (EÚ) č. 526/2013 a na agentúru ENISA zriadenú uvedeným nariadením sa považujú za odkazy na toto nariadenie a na agentúru ENISA zriadenú týmto nariadením.

3. Agentúra ENISA zriadená týmto nariadením je nástupcom agentúry ENISA, ktorá bola zriadená nariadením (EÚ) č. 526/2013, pokiaľ ide o vlastníctvo, dohody, právne záväzky, pracovné zmluvy, finančné záväzky a povinnosti. Všetky rozhodnutia správnej rady a výkonnej rady prijaté v súlade s nariadením (EÚ) č. 526/2013 zostávajú v platnosti, pokiaľ sú v súlade s týmto nariadením.

4. Agentúra ENISA sa zriaďuje na dobu neurčitú od 27. júna 2019.

5. Výkonný riaditeľ vymenovaný podľa článku 24 ods. 4 nariadenia (EÚ) č. 526/2013 zostáva vo svojej funkcii a plní povinnosti výkonného riaditeľa, ako je uvedené v článku 20 tohto nariadenia, do konca zostatku funkčného obdobia výkonného riaditeľa. Ostatné podmienky jeho zmluvy zostávajú nezmenené.

6. Členovia správnej rady a ich náhradníci vymenovaní podľa článku 6 nariadenia (EÚ) č. 526/2013 zostávajú vo svojej funkcii a plnia povinnosti správnej rady, ako je uvedené v článku 15 tohto nariadenia, do konca zostatku svojho funkčného obdobia.

Článok 69

Nadobudnutie účinnosti

1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

2. Články 58, 60, 61, 63, 64, a 65 sa uplatňujú od 28. júna 2021.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Štrasburgu 17. apríla 2019.

Za Európsky parlament	*Za Radu*
predseda	*predseda*
A. TAJANI	G. CIAMBA

PRÍLOHA

POŽIADAVKY, KTORÉ MUSIA SPĹŇAŤ ORGÁNY POSUDZOVANIA ZHODY

Orgány posudzovania zhody žiadajúce o akreditáciu musia spĺňať tieto požiadavky:

1. Orgán posudzovania zhody je zriadený podľa vnútroštátneho práva a má právnu subjektivitu.

2. Orgán posudzovania zhody je orgánom tretej strany, ktorá je nezávislá od organizácie alebo produktov IKT, služieb IKT alebo procesov IKT, ktoré posudzuje.

3. Za orgán posudzovania zhody možno považovať subjekt, ktorý patrí do obchodného alebo profesijného združenia, ktoré zastupuje podniky, ktoré sa podieľajú na navrhovaní, produkcii, poskytovaní, inštalácii, používaní alebo údržbe produktov IKT, služieb IKT alebo procesov IKT, ktoré tento subjekt posudzuje, ak sa preukáže jeho nezávislosť a absencia konfliktu záujmov.

4. Orgány posudzovania zhody, ich vrcholový manažment a osoby zodpovedné za výkon úloh posudzovania zhody nesmú byť návrhármi, výrobcami, dodávateľmi, subjektmi, ktoré vykonávajú inštaláciu alebo údržbu, obstarávateľmi, vlastníkmi ani užívateľmi posudzovaného produktu IKT, služby IKT alebo procesu IKT, ani splnomocnenými zástupcami žiadnej z uvedených strán. Uvedený zákaz nevylučuje používanie posudzovaných produktov IKT, ktoré sú potrebné na vykonávanie činností orgánu posudzovania zhody, ani používanie takých produktov IKT na osobné účely.

5. Orgány posudzovania zhody, ich vrcholový manažment a osoby zodpovedné za vykonávanie úloh posudzovania zhody sa nesmú priamo podieľať na navrhovaní, zhotovovaní alebo výrobe, marketingu, inštalácii, používaní alebo údržbe posudzovaných produktov IKT, služieb IKT alebo procesov IKT, ani zastupovať strany, ktoré sa na takýchto činnostiach podieľajú. Orgány posudzovania zhody, ich vrcholový manažment a osoby zodpovedné za vykonávanie úloh posudzovania zhody sa nesmú podieľať na žiadnych činnostiach, ktoré môžu ovplyvniť ich nezávislý úsudok alebo bezúhonnosť v súvislosti s ich činnosťami posudzovania zhody. Uvedený zákaz sa vzťahuje najmä na poradenské služby.

6. Ak orgán posudzovania zhody vlastní alebo prevádzkuje verejný subjekt alebo verejná inštitúcia, musí sa zabezpečiť a zdokumentovať nezávislosť a absencia akéhokoľvek konfliktu záujmov medzi vnútroštátnym orgánom pre certifikáciu kybernetickej bezpečnosti a orgánom posudzovania zhody.

7. Orgány posudzovania zhody zabezpečia, aby činnosti ich dcérskych spoločností a subdodávateľov nemali vplyv na povinnosť mlčanlivosti, objektivitu a nestrannosť ich činností posudzovania zhody.

8. Orgány posudzovania zhody a ich personál vykonávajú činnosti posudzovania zhody na najvyššej úrovni profesionálnej čestnosti a požadovanej technickej spôsobilosti v danej oblasti a nepodliehajú žiadnym tlakom ani stimulom vrátane tlakov a stimulov finančnej povahy, ktoré by mohli ovplyvniť ich úsudok alebo výsledky ich činností posudzovania zhody, najmä zo strany osôb alebo skupín osôb, ktoré majú záujem na výsledku týchto činností.

9. Orgán posudzovania zhody musí byť schopný vykonať všetky úlohy posudzovania zhody, ktoré sú mu zverené týmto nariadením, bez ohľadu na to, či ich vykoná sám, alebo sa vykonajú v jeho mene a na jeho zodpovednosť. Všetky subdodávateľské zmluvy alebo konzultácie s externým personálom musia byť riadne zdokumentované, ich súčasťou nesmú byť žiadni sprostredkovatelia a musia mať podobu písomnej dohody, v ktorej sa okrem iného upraví povinnosť mlčanlivosti a konflikt záujmov. Za vykonané úlohy nesie plnú zodpovednosť orgán posudzovania zhody.

10. Orgán posudzovania zhody má neustále, pre každý postup posudzovania zhody a pre každý druh a každú kategóriu alebo podkategóriu produktov IKT, služieb IKT alebo procesov IKT v potrebnej miere k dispozícii:

    a) personál s odbornými znalosťami a dostatočnými a primeranými skúsenosťami na výkon úloh posudzovania zhody;

    b) opisy postupov, podľa ktorých sa má vykonávať posudzovanie zhody a ktorými sa zabezpečuje transparentnosť a opakovateľnosť uvedených postupov. Musí mať zavedené vhodné politiky a postupy, ktorými sa rozlišujú úlohy, ktoré vykonáva ako orgán oznámený podľa článku 61, od ostatných jeho činností;

c) postupy na výkon činností, ktorými sa náležite zohľadňuje veľkosť každého podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúra, stupeň zložitosti technológie daného produktu IKT, služby IKT alebo procesu IKT a hromadný či sériový charakter produkčného procesu.

11. Orgán posudzovania zhody musí mať prostriedky potrebné na riadne plnenie technických a administratívnych úloh spojených s posudzovaním zhody, ako aj prístup k všetkým potrebným zariadeniam a vybaveniu.

12. Osoby zodpovedné za výkon činností posudzovania zhody musí mať:

a) absolvovanú dôkladnú technickú a odbornú prípravu pokrývajúcu všetky činnosti posudzovania zhody;

b) dostatočné znalosti požiadaviek posudzovaní zhody, ktoré vykonávajú, a primeranú právomoc vykonávať tieto posudzovania;

c) primerané znalosti a chápanie platných požiadaviek a skúšobných noriem;

d) schopnosť vypracúvať certifikáty, záznamy a protokoly preukazujúce, že sa vykonalo posúdenie zhody.

13. Musí byť zaručená nestrannosť orgánov posudzovania zhody, ich vrcholového manažmentu a osôb zodpovedných za výkon činností posudzovania zhody, ako aj subdodávateľov.

14. Odmeňovanie vrcholového manažmentu a osôb zodpovedných za výkon činností posudzovania zhody nezávisí od počtu vykonaných posúdení zhody ani od výsledkov týchto posúdení.

15. Orgány posudzovania zhody musia uzavrieť poistenie zodpovednosti za škodu, ak túto zodpovednosť podľa svojho vnútroštátneho práva nenesie členský štát, alebo ak nie je za posudzovanie zhody priamo zodpovedný samotný členský štát.

16. Orgán posudzovania zhody a jeho personál, výbory, dcérske spoločnosti, subdodávatelia a akýkoľvek pridružený subjekt alebo personál externých subjektov orgánu posudzovania zhody zachovávajú povinnosť mlčanlivosti a služobné tajomstvo, pokiaľ ide o všetky informácie získané pri výkone svojich úloh posudzovania zhody podľa tohto nariadenia alebo akéhokoľvek ustanovenia vnútroštátneho práva, ktorým sa toto nariadenie vykonáva, okrem prípadov, keď sa ich poskytnutie vyžaduje podľa práva Únie alebo členského štátu, ktoré sa na tieto osoby vzťahuje, a okrem styku s príslušnými orgánmi členských štátov, v ktorých vykonávajú svoju činnosť. Práva duševného vlastníctva sú chránené. Orgán posudzovania zhody musí mať zavedené zdokumentované postupy, pokiaľ ide o požiadavky tohto bodu.

17. S výnimkou bodu 16 sa požiadavkami tejto prílohy nevylučuje výmenu technických informácií a regulačného poradenstva medzi orgánom posudzovania zhody a osobou, ktorá požiada o certifikáciu alebo ktorá o žiadosti uvažuje.

18. Orgány posudzovania zhody vykonávajú svoju činnosť v súlade so súborom konzistentných, spravodlivých a primeraných podmienok, pričom, pokiaľ ide o poplatky, zohľadňujú záujmy MSP.

19. Orgány posudzovania zhody spĺňajú požiadavky príslušnej normy harmonizovanej podľa nariadenia (ES) č. 765/2008 a týkajúcej sa akreditácie orgánov posudzovania zhody, ktoré vykonávajú certifikáciu produktov IKT, služieb IKT alebo procesov IKT.

20. Orgány posudzovania zhody zabezpečia, aby skúšobné laboratóriá používané na účely posudzovania zhody spĺňali požiadavky príslušnej normy harmonizovanej podľa nariadenia (ES) č. 765/2008 a týkajúcej sa akreditácie laboratórií, ktoré vykonávajú skúšky.