2023/2841

18.12.2023

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ, Euratom) 2023/2841

z 13. decembra 2023,

ktorým sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 298,

so zreteľom na Zmluvu o založení Európskeho spoločenstva pre atómovú energiu, a najmä na jej článok 106a,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

konajúc v súlade s riadnym legislatívnym postupom ([1]),

keďže:

(1) V digitálnom veku sú informačné a komunikačné technológie základom otvorenej, efektívnej a nezávislej európskej administratívy. Vyvíjajúce sa technológie, zvýšená zložitosť a vzájomná prepojenosť digitálnych systémov zväčšujú kybernetickobezpečnostné riziká, a preto sú subjekty Únie zraniteľnejšie voči kybernetickým hrozbám a incidentom, čo predstavuje hrozbu pre ich kontinuitu činnosti a schopnosť zabezpečiť ich údaje. Kým intenzívnejšie používanie cloudových služieb, všadeprítomné používanie informačných a komunikačných technológií (ďalej len „IKT“), vysoká miera digitalizácie, práca na diaľku a vyvíjajúce sa technológie a pripojiteľnosť sú hlavnými prvkami všetkých činností subjektov Únie, digitálna odolnosť zatiaľ nie je dostatočne vybudovaná.

(2) Panoráma kybernetických hrozieb, ktorým čelia subjekty Únie, sa neustále vyvíja. Taktiky, techniky a postupy, ktoré aktéri hrozby využívajú, sa neustále vyvíjajú, pričom hlavné motívy týchto útokov sa takmer nemenia, a to od krádeže cenných nesprístupnených informácií až po zarábanie peňazí, manipuláciu verejnej mienky alebo narušanie digitálnej infraštruktúry. Tempo, akým vykonávajú aktéri hrozby svoje kybernetické útoky, sa zrýchľuje a ich operácie sú čoraz sofistikovanejšie a automatizovanejšie, zacielené na stále sa zväčšujúce plochy nechránené voči útoku a promptne využíva zraniteľnosti.

(3) Prostredia IKT subjektov Únie sú vzájomne previazané a majú integrované toky údajov a ich používatelia úzko spolupracujú. Takéto prepojenie znamená, že každé narušenie dokonca aj také, ktoré sa spočiatku obmedzuje na jeden subjekt Únie, môže mať širšie kaskádovité účinky a mať ďalekosiahly a dlhotrvajúci negatívny vplyv na ostatné subjekty Únie. Prostredia IKT niektorých subjektov Únie sú navyše prepojené s prostrediami IKT členských štátov, čo spôsobuje, že incident u jedného subjektu Únie predstavuje kybernetickobezpečnostné riziko pre prostredia IKT členských štátov a naopak. Zdieľanie informácií o konkrétnom incidente môže uľahčiť odhalenie podobných kybernetických hrozieb alebo incidentov v členských štátoch.

(4) Subjekty Únie sú atraktívne ciele, ktoré čelia kvalifikovaným aktérom hrozieb s dostatočnými zdrojmi, ako aj ďalším hrozbám. Úroveň a vyspelosť kybernetickej odolnosti a schopnosť odhaľovať škodlivé kybernetické činnosti a reagovať na ne sa v týchto subjektoch zároveň výrazne líši. Z hľadiska fungovania subjektov Únie je preto potrebné, aby dosahovali vysokú spoločnú úroveň kybernetickej bezpečnosti prostredníctvom vykonávania opatrení v oblasti kybernetickej bezpečnosti úmerným identifikovaným kybernetickobezpečnostným rizikám, výmeny informácií a spolupráce.

([1]) Pozícia Európskeho parlamentu z 21. novembra 2023 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 8. decembra 2023.

(5) Cieľom smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 ([2]) je ďalšie zvyšovanie kybernetickej odolnosti a zlepšovanie schopností verejných a súkromných subjektov, príslušných orgánov a subjektov, ako aj Únie ako celku reagovať na incidenty. Preto treba zabezpečiť, aby ich príklad nasledovali aj subjekty Únie, a to stanovením pravidiel, ktoré budú v súlade so smernicou (EÚ) 2022/2555 a budú rovnako ambiciózne.

(6) Dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti si vyžaduje, aby si každý subjekt Únie vytvoril vnútorný rámec riadenia, správy a kontroly kybernetickobezpečnostných rizík (ďalej len „rámec“), ktorým sa zabezpečí účinné a obozretné riadenie všetkých kybernetickobezpečnostných rizík a v ktorom sa zohľadní kontinuita činností a krízové riadenie. V rámci by sa mali stanoviť politiky kybernetickej bezpečnosti vrátane cieľov a priorít v oblasti bezpečnosti sietí a informačných systémov, ktoré sa budú vzťahovať na celé verejne prístupné prostredie IKT. Rámec by mal byť založený na prístupe zohľadňujúcom všetky riziká, ktorého cieľom je chrániť siete a informačné systémy a fyzické prostredie týchto systémov pred udalosťami, ako sú napríklad krádeže, požiare, záplavy, telekomunikačné výpadky alebo výpadky energie, alebo neoprávnený fyzický prístup do informačných zariadení subjektu Únie a jeho zariadení na spracúvanie informácií a ich poškodenie alebo narušanie, čo by mohlo ohroziť dostupnosť, pravosť, integritu alebo dôvernosť údajov, ktoré sa uchovávajú, prenášajú, spracúvajú alebo sprístupňujú prostredníctvom sietí a informačných systémov.

(7) Na riadenie kybernetickobezpečnostných rizík identifikovaných v rámci by mal každý subjekt Únie prijať vhodné a primerané technické, prevádzkové a organizačné opatrenia. Uvedené opatrenia by sa mali týkať oblastí a opatrení na riadenie kybernetickobezpečnostných rizík stanovených v tomto nariadení s cieľom posilniť kybernetickú bezpečnosť každého subjektu Únie.

(8) V pláne kybernetickej bezpečnosti, ktorý vypracuje každý subjekt Únie, by sa mali zohľadniť aktíva a kybernetickobezpečnostné riziká identifikované v rámci, ako aj závery vyplývajúce z pravidelných posúdení vyspelosti v oblasti kybernetickej bezpečnosti. Plán kybernetickej bezpečnosti by mal zahŕňať prijaté opatrenia na riadenie kybernetickobezpečnostných rizík.

(9) Keďže zabezpečenie kybernetickej bezpečnosti je nepretržitý proces, vhodnosť a účinnosť opatrení prijatých podľa tohto nariadenia by sa mala pravidelne revidovať vzhľadom na meniace sa kybernetickobezpečnostné riziká, aktíva a vyspelosť subjektov Únie v oblasti kybernetickej bezpečnosti. Rámec by sa mal pravidelne preskúmavať, a to aspoň každé štyri roky, pričom plán kybernetickej bezpečnosti by sa mal revidovať každé dva roky, alebo v prípade potreby častejšie, po posúdení vyspelosti v oblasti kybernetickej bezpečnosti alebo akomkoľvek podstatnom preskúmaní rámca.

(10) Opatrenia na riadenie kybernetickobezpečnostných rizík, ktoré zaviedli subjekty Únie, by mali v rámci možností zahŕňať politiky zamerané na zabezpečenie transparentnosti zdrojového kódu, pričom sa zohľadnia záruky týkajúce sa práv tretích strán alebo subjektov Únie. Uvedené politiky by mali byť primerané kybernetickobezpečnostným rizikám a ich cieľom je uľahčiť vykonávanie analýzy kybernetických hrozieb bez vytvorenia povinnosti zverejniť kód tretej strany alebo udeliť práva na prístup k nemu nad rámec uplatniteľných zmluvných podmienok.

(11) K vyššej miere otvorenosti môžu prispieť nástroje a aplikácie kybernetickej bezpečnosti s otvoreným zdrojovým kódom. Otvorené normy uľahčujú interoperabilitu bezpečnostných nástrojov, čo je prínosom pre bezpečnosť zainteresovaných strán. Nástrojmi a aplikáciami kybernetickej bezpečnosti s otvoreným zdrojovým kódom sa môže mobilizovať širšia komunita vývojárov a umožniť diverzifikácia dodávateľov. Otvorený zdrojový kód môže viesť k transparentnejšiemu postupu overovania nástrojov súvisiacich s kybernetickou bezpečnosťou a ku komunitnému procesu objavovania zraniteľností. Subjekty Únie by preto mali mať možnosť podporovať používanie softvéru s otvoreným zdrojovým kódom a otvorených noriem, a to uplatňovaním politík využívania otvorených údajov a otvoreného zdrojového kódu ako súčasti bezpečnosti prostredníctvom transparentnosti.

([2]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).

(12) Rozdiely medzi subjektmi Únie si vyžadujú flexibilitu pri vykonávaní tohto nariadenia. Opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti stanovené v tomto nariadení by nemali obsahovať žiadne povinnosti, ktorými by sa priamo zasahovalo do plnenia poslania subjektov Únie alebo by sa narúšala ich inštitucionálna autonómia. Uvedené subjekty by si preto mali vytvoriť vlastné rámce a mali by prijať vlastné opatrenia na riadenie kybernetickobezpečnostných rizík a plány kybernetickej bezpečnosti. Pri vykonávaní takýchto opatrení by sa mali náležite zohľadniť existujúce synergie medzi subjektmi Únie s cieľom riadneho hospodárenia so zdrojmi a optimalizácie nákladov. Náležitá pozornosť by sa mala venovať aj tomu, aby opatrenia nemali negatívny vplyv na efektívnu výmenu informácií a spoluprácu medzi subjektmi Únie a medzi subjektmi Únie a náprotivkami v členskom štáte.

(13) V záujme optimalizácie využívania zdrojov by sa v tomto nariadení mala stanoviť možnosť, aby dva alebo viaceré subjekty Únie s podobnými štruktúrami spolupracovali pri vykonávaní posúdení vyspelosti v oblasti kybernetickej bezpečnosti pre svoje príslušné subjekty.

(14) S cieľom vyhnúť sa neprimeranému finančnému a administratívnemu zaťaženiu subjektov Únie by požiadavky na riadenie kybernetickobezpečnostných rizík mali byť primerané kybernetickobezpečnostnému riziku, ktorým čelí daná sieť a informačné systémy, pričom by sa mal zohľadniť najnovší vývoj v oblasti takýchto opatrení. Cieľom každého subjektu Únie by malo byť pridelenie primeraného percentuálneho podielu ich rozpočtu na IKT na zlepšenie úrovne kybernetickej bezpečnosti. V dlhšom horizonte by malo byť snahou dosiahnuť orientačný cieľ na úrovni rádovo aspoň 10 %. V posúdení vyspelosti v oblasti kybernetickej bezpečnosti by sa malo hodnotiť, či sú výdavky subjektu Únie na kybernetickú bezpečnosť primerané kybernetickobezpečnostným rizikám, ktorým čelí. Bez toho, aby boli dotknuté pravidlá týkajúce sa ročného rozpočtu Únie podľa zmlúv, by Komisia vo svojom návrhu prvého ročného rozpočtu, ktorý sa má prijať po nadobudnutí účinnosti tohto nariadenia, mala zohľadniť povinnosti vyplývajúce z tohto nariadenia pri posudzovaní rozpočtových a personálnych potrieb subjektov Únie, ktoré vyplývajú z ich odhadov výdavkov.

(15) Vysoká spoločná úroveň kybernetickej bezpečnosti si vyžaduje, aby nad kybernetickou bezpečnosťou vykonával dohľad manažment najvyššej úrovne každého subjektu Únie. Manažment najvyššej úrovne subjektu Únie by mal byť zodpovedný za vykonávanie tohto nariadenia vrátane vytvorenia rámca, prijímania opatrení na riadenie kybernetickobezpečnostných rizík a schválenia plánu kybernetickej bezpečnosti. Neoddeliteľnou súčasťou rámca a zodpovedajúcich opatrení na riadenie kybernetickobezpečnostných rizík u všetkých subjektov Únie je riešenie kultúry kybernetickej bezpečnosti, konkrétne každodennej praxe v oblasti kybernetickej bezpečnosti.

(16) Bezpečnosť sietí a informačných systémov, v ktorých sa zaobchádza s utajovanými skutočnosťami EÚ, má zásadný význam. Od subjektov Únie, ktoré zaobchádzajú s utajovanými skutočnosťami EÚ, sa vyžaduje, aby uplatňovali zavedené komplexné regulačné rámce na ochranu takýchto informácií vrátane osobitnej správy, politík a postupov riadenia rizík. Je potrebné, aby siete a informačné systémy, v ktorých sa zaobchádza s utajovanými skutočnosťami EÚ, spĺňali prísnejšie bezpečnostné normy ako verejne prístupné siete a informačné systémy. Siete a informačné systémy, v ktorých sa zaobchádza s utajovanými skutočnosťami EÚ, sú teda odolnejšie voči kybernetickým hrozbám a incidentom. Toto nariadenie by sa preto nemalo vzťahovať na siete a informačné systémy, v ktorých sa zaobchádza s utajovanými skutočnosťami EÚ, hoci sa uznáva potreba spoločného rámca v tejto súvislosti. Ak však o to subjekt Únie výslovne požiada, tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (ďalej len „CERT-EU“) by mal byť schopný poskytnúť tomuto subjektu Únie pomoc v súvislosti s incidentmi v utajených prostrediach IKT.

(17) Subjekty Únie by mali posudzovať kybernetickobezpečnostné riziká vzťahov s dodávateľmi a poskytovateľmi služieb vrátane poskytovateľov služieb dátových úložísk a služieb spracúvania údajov alebo riadených bezpečnostných služieb a prijímať primerané opatrenia na ich riešenie. Opatrenia v oblasti kybernetickej bezpečnosti by sa mali podrobnejšie vymedziť v usmerneniach alebo odporúčaniach, ktoré vydá CERT-EU. Pri stanovovaní opatrení a usmernení by sa mal náležite zohľadniť najnovší technologický vývoj a v náležitých prípadoch relevantné európske a medzinárodné normy, ako aj relevantné právo a politiky Únie vrátane posúdení kybernetickobezpečnostných rizík a odporúčaní vydaných skupinou pre spoluprácu zriadenou podľa článku 14 smernice (EÚ) 2022/2555, ako je napríklad koordinované posúdenie rizík kybernetickej bezpečnosti sietí 5G na úrovni EÚ a súboru nástrojov EÚ pre kybernetickú bezpečnosť 5G. Okrem toho by sa vzhľadom na panorámu kybernetických

hrozieb a dôležitosť zvyšovania kybernetickej odolnosti subjektov Únie mala vyžadovať certifikácia relevantných produktov IKT, služieb IKT a postupov IKT, v rámci špecifických európskych systémov certifikácie kybernetickej bezpečnosti prijatých podľa článku 49 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 ([3]).

(18) V máji 2011 sa generálni tajomníci inštitúcií a orgánov Únie rozhodli vytvoriť v predbežnom zoskupení tím CERT-EU pod dohľadom medziinštitucionálnej riadiacej rady. V júli 2012 generálni tajomníci potvrdili praktické opatrenia a dohodli sa na zachovaní CERT-EU ako stáleho subjektu s cieľom pomôcť zlepšiť celkovú úroveň bezpečnosti informačných technológií inštitúcií, orgánov a agentúr Únie ako príklad viditeľnej medziinštitucionálnej spolupráce v oblasti kybernetickej bezpečnosti. V septembri 2012 bol CERT-EU zriadený ako pracovná skupina Komisie s medziinštitucionálnym mandátom. Medziinštitucionálnu dohodu o organizácii a fungovaní CERT-EU uzavreli inštitúcie a orgány Únie v decembri 2017 ([4]). Týmto nariadením by sa mal stanoviť ucelený súbor pravidiel týkajúcich sa organizácie a fungovania CERT-EU. Ustanovenia tohto nariadenia majú prednosť pred ustanoveniami medziinštitucionálnej dohody o organizácii a fungovaní tímu CERT-EU, ktorá bola uzavretá v decembri 2017.

(19) CERT-EU by sa mal premenovať na Službu kybernetickej bezpečnosti pre inštitúcie, orgány, úrady a agentúry Únie, no už známa skratka CERT-EU by sa mala zachovať.

(20) Okrem toho, že by sa CERT-EU malo zveriť viac povinností a mala by sa rozšíriť jeho úloha, týmto nariadením sa zriaďuje Medziinštitucionálna rada pre kybernetickú bezpečnosť (ďalej len „IICB“) s cieľom uľahčovať dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti subjektov Únie. IICB by mala mať výlučnú úlohu pri monitorovaní a podpore vykonávania tohto nariadenia subjektmi Únie, a pri dohľade nad vykonávaním všeobecných priorít a cieľov CERT-EU a pri jeho strategickom usmerňovaní. IICB by mala preto zabezpečiť zastúpenie inštitúcií Únie a zapojiť zástupcov orgánov, úradov a agentúr Únie prostredníctvom siete agentúr EÚ (ďalej len „EUAN“). Organizácia a fungovanie IICB by sa mali ďalej riadiť prostredníctvom vnútorného rokovacieho poriadku, ktorý môže zahŕňať ďalšiu špecifikáciu pravidelných zasadnutí IICB vrátane výročných zhromaždení na politickej úrovni, na ktorých by zástupcovia manažmentu najvyššej úrovne každého člena IICB umožnili, aby IICB viedla strategickú diskusiu a poskytovali jej strategické usmernenie. Okrem toho by IICB mala mať možnosť zriadiť výkonný výbor, ktorý jej bude pomáhať pri jej práci a delegovať naň niektoré z jej úloh a právomocí, najmä pokiaľ ide o úlohy, ktoré si vyžadujú osobitné odborné znalosti jej členov, napríklad schválenie katalógu služieb a akékoľvek jeho následné aktualizácie, dohody o úrovni poskytovaných služieb, posudzovanie dokumentov a správ, ktoré subjekty Únie predkladajú IICB podľa tohto nariadenia, alebo úlohy súvisiace s prípravou rozhodnutí o opatreniach na zabezpečenie dodržiavania povinností vydaných IICB a monitorovaním ich vykonávania. IICB by mala stanoviť rokovací poriadok výkonného výboru vrátane jeho úloh a právomocí.

(21) Cieľom IICB je podporovať subjekty Únie pri posilňovaní ich pozície v oblasti kybernetickej bezpečnosti prostredníctvom vykonávania tohto nariadenia. S cieľom podporiť subjekty Únie by IICB mala vedúcemu CERT-EU poskytovať usmernenia, prijať viacročnú stratégiu na zvýšenie úrovne kybernetickej bezpečnosti v subjektoch Únie, stanoviť metodiku a iné aspekty dobrovoľných partnerských preskúmaní a uľahčiť zriadenie neformálnej skupiny miestnych úradníkov pre kybernetickú bezpečnosť s podporou Agentúry Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) s cieľom vymieňať si najlepšie postupy a informácie v súvislosti s vykonávaním tohto nariadenia.

([3]) 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) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

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

(22) V záujme dosiahnutia vysokej úrovne kybernetickej bezpečnosti vo všetkých subjektoch Únie by záujmy orgánov, úradov a agentúr Únie, ktoré prevádzkujú vlastné prostredie IKT, mali v IICB zastupovať traja zástupcovia určení sieťou EUAN. Bezpečnosť spracúvania osobných údajov, a teda aj jeho kybernetická bezpečnosť, je základom ochrany osobných údajov. Vzhľadom na synergie medzi ochranou údajov a kybernetickou bezpečnosťou by mal byť európsky dozorný úradník pre ochranu údajov zastúpený v IICB ako subjekt Únie, na ktorý sa vzťahuje toto nariadenie, s osobitnými odbornými znalosťami v oblasti ochrany údajov vrátane bezpečnosti elektronických komunikačných sietí. Vzhľadom na význam inovácií a konkurencieschopnosti v oblasti kybernetickej bezpečnosti by v IICB malo byť zastúpené Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti. Vzhľadom na úlohu agentúry ENISA ako centra odborných znalostí v oblasti kybernetickej bezpečnosti a podporu, ktorú agentúra ENISA poskytuje, a vzhľadom na význam kybernetickej bezpečnosti vesmírnej infraštruktúry a služieb Únie by agentúra ENISA a Agentúra Európskej únie pre vesmírny program mali byť zastúpené v IICB. Vzhľadom na úlohu zverenú CERT-EU podľa tohto nariadenia by mal predseda IICB pozvať vedúceho CERT-EU na všetky zasadnutia IICB okrem prípadov, keď IICB rokuje o záležitostiach týkajúcich sa priamo vedúceho CERT-EU.

(23) IICB by mala monitorovať dodržiavanie tohto nariadenia, ako aj vykonávanie usmernení a odporúčaní, a výzvy na činnosť. V technických záležitostiach by IICB mala mať podporu technických poradných skupín v zložení podľa uváženia IICB. Uvedené technické poradné skupiny by mali podľa potreby úzko spolupracovať s CERT-EU, subjektmi Únie, ako aj s inými zainteresovanými stranami.

(24) Ak IICB zistí, že subjekt Únie účinne nevykonal toto nariadenie alebo usmernenia, odporúčania alebo výzvy na činnosť vydané podľa neho, mala by mať možnosť pristúpiť k opatreniam na zabezpečenie dodržiavania povinností bez toho, aby boli dotknuté vnútorné postupy dotknutého subjektu Únie. IICB by mala uplatňovať opatrenia na zabezpečenie dodržiavania povinností postupne, inými slovami, IICB by mala najskôr prijať najmenej prísne opatrenie, a to odôvodnené stanovisko, a len v prípade potreby čoraz prísnejšie opatrenia až najzávažnejšie opatrenie, a to odporúčanie na dočasné pozastavenie tokov údajov do dotknutého subjektu Únie. Takéto odporúčanie by sa malo uplatňovať len vo výnimočných prípadoch dlhodobých, úmyselných, opakovaných alebo závažných porušovaní tohto nariadenia dotknutým subjektom Únie.

(25) Odôvodnené stanovisko predstavuje najmenej závažné opatrenie na zabezpečenie dodržiavania povinností, ktorým sa riešia zistené nedostatky vo vykonávaní tohto nariadenia. IICB by mala mať možnosť nadviazať na odôvodnené stanovisko usmernením s cieľom pomôcť subjektu Únie zabezpečiť, aby jeho rámec, opatrenia na riadenie kybernetickobezpečnostných rizík, plán kybernetickej bezpečnosti a oznamovanie boli v súlade s týmto nariadením, a následne vydaním varovania na vyriešenie zistených nedostatkov subjektu Únie v stanovenej lehote. Ak nedostatky zistené vo varovaní neboli dostatočne vyriešené, IICB by mala mať možnosť vydať odôvodnené oznámenie.

(26) IICB by mala mať možnosť odporučiť, aby sa vykonal audit subjektu Únie. Subjekt Únie by mal mať možnosť využiť na tento účel svoju funkciu vnútorného auditu. IICB by mala mať tiež možnosť požadovať, aby audit vykonal audítorský útvar tretej strany, a to aj útvar vzájomne dohodnutého poskytovateľa služieb zo súkromného sektora.

(27) Vo výnimočných prípadoch dlhodobého, úmyselného, opakovaného alebo závažného porušovania tohto nariadenia subjektom Únie by IICB mala mať možnosť ako krajné opatrenie odporúčať všetkým členským štátom a subjektom Únie dočasne pozastaviť toky údajov do daného subjektu Únie, ktoré bude účinné až kým subjekt Únie neskončí porušovanie. Takéto odporúčanie by sa malo oznámiť prostredníctvom vhodných a bezpečných komunikačných kanálov.

(28) S cieľom zabezpečiť správne vykonávanie tohto nariadenia by IICB mala v prípade, že sa domnieva, že neustále porušovanie tohto nariadenia subjektom Únie bolo priamo spôsobené konaním alebo opomenutím jeho zamestnanca, a to aj z radov manažmentu najvyššej úrovne, požiadať dotknutý subjekt Únie, aby prijal primerané opatrenia a aby zvážil prijatie disciplinárneho opatrenia v súlade s pravidlami a postupmi stanovenými v Služobnom poriadku úradníkov Európskej únie a Podmienkach zamestnávania ostatných zamestnancov Európskej Únie stanovených v nariadení Rady (EHS, Euratom, ESUO) č. 259/68 ([5]) (ďalej len „služobný poriadok“) a akýmikoľvek inými uplatniteľnými pravidlami a postupmi.

(29) CERT-EU by mal prispievať k bezpečnosti prostredia IKT všetkých subjektov Únie. Pri zvažovaní, či na žiadosť subjektu Únie poskytnúť technické poradenstvo alebo informácie o relevantných politických záležitostiach, by CERT-EU mal zabezpečiť, aby to nebránilo plneniu ostatných úloh, ktoré mu boli zverené podľa tohto nariadenia. CERT-EU by mal konať v mene subjektov Únie ako ekvivalent koordinátora určeného na účely koordinovaného zverejňovania zraniteľností podľa článku 12 ods. 1 smernice (EÚ) 2022/2555.

(30) CERT-EU by mal podporovať vykonávanie opatrení na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti prostredníctvom návrhov usmernení a odporúčaní pre IICB alebo vydávaním výziev na činnosť. Takéto usmernenia a odporúčania by mala schvaľovať IICB. V prípade potreby by CERT-EU mal vydávať výzvy na činnosť s opisom naliehavých bezpečnostných opatrení a na subjekty Únie naliehať, aby tieto opatrenia prijali v stanovenej lehote. IICB by mala dať CERT-EU pokyn na vydanie, zrušenie alebo zmenu návrhu usmernení alebo odporúčaní alebo výzvy na činnosť.

(31) CERT-EU by mal plniť aj úlohu stanovenú v smernici (EÚ) 2022/2555, pokiaľ ide o spoluprácu a výmenu informácií so sieťou jednotiek pre riešenie incidentov počítačovej bezpečnosti (ďalej len „CSIRT“) zriadenou podľa článku 15 uvedenej smernice. V súlade s odporúčaním Komisie (EÚ) 2017/1584 ([6]) by CERT-EU mal tiež spolupracovať s relevantnými zainteresovanými stranami a s nimi koordinovať reakciu. S cieľom prispieť k vysokej úrovni kybernetickej bezpečnosti v celej Únii by CERT-EU mal zdieľať informácie o konkrétnych incidentoch s náprotivkami v členskom štáte. CERT-EU by mal tiež spolupracovať s ostatnými verejnými, ako aj súkromnými náprotivkami vrátane Organizácie Severoatlantickej zmluvy po predchádzajúcom povolení IICB.

(32) CERT-EU by na podporu operačnej kybernetickej bezpečnosti mal využívať dostupné odborné znalosti agentúry ENISA prostredníctvom štruktúrovanej spolupráce, ako sa stanovuje v nariadení (EÚ) 2019/881. V náležitých prípadoch by sa mali medzi oboma subjektmi uzavrieť účelové dohody o fungovaní takejto spolupráce v praxi a zabránení zdvojovaniu činností. CERT-EU by mal spolupracovať s agentúrou ENISA na analýze kybernetických hrozieb a pravidelne zdieľať s agentúrou ENISA svoju správu o panoráme hrozieb.

(33) CERT-EU by mal byť schopný spolupracovať a vymieňať si informácie s príslušnými komunitami v oblasti kybernetickej bezpečnosti v rámci Únie a jej členských štátov s cieľom posilniť operačnú spoluprácu a umožniť existujúcim sieťam naplno využiť ich potenciál pri ochrane Únie.

(34) Keďže služby a úlohy CERT-EU sú v záujme subjektov Únie, každý subjekt Únie s výdavkami v oblasti IKT by mal na tieto služby a úlohy primerane prispievať. Uvedenými príspevkami nie je dotknutá rozpočtová autonómia subjektov Únie.

([5]) Nariadenie Rady (EHS, Euratom, ESUO) č. 259/68 z 29. februára 1968, ktorým sa ustanovuje Služobný poriadok a Podmienky zamestnávania ostatných zamestnancov Európskych spoločenstiev a osobitné pravidlá, ktoré sa dočasne uplatňujú na úradníkov Komisie (Ú. v. ES L 56, 4.3.1968, s. 1).

([6]) 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).

(35) Mnohé kybernetické útoky sú súčasťou rozsiahlejších kampaní, ktoré sa zameriavajú na skupiny subjektov Únie alebo na významné komunity, do ktorých subjekty Únie patria. S cieľom umožniť proaktívne odhaľovanie, reakciu na incidenty alebo prijímanie zmierňujúcich opatrení a obnovu po incidentoch by subjekty Únie mali byť schopné CERT-EU oznamovať incidenty, kybernetické hrozby, zraniteľnosti a udalosti odvrátené v poslednej chvíli a zdieľať s CERT-EU primerané technické podrobnosti, ktoré umožnia odhaľovanie alebo zmierňovanie podobných incidentov, kybernetických hrozieb, zraniteľností a udalostí odvrátených v poslednej chvíli v iných subjektoch Únie, ako aj reakciu na ne. Na základe rovnakého prístupu, ako je prístup v smernici (EÚ) 2022/2555, by subjekty Únie mali byť povinné do 24 hodín od momentu, keď sa dozvedia o významnom incidente, podať CERT-EU včasné varovanie. Takouto výmenou informácií by sa CERT-EU malo umožniť poskytnúť tieto informácie ostatným subjektom Únie, ako aj relevantným náprotivkom s cieľom pomôcť chrániť prostredia IKT subjektov Únie a prostredia IKT náprotivkov Únie pred podobnými incidentmi.

(36) V tomto nariadení sa stanovuje viacfázový prístup k oznamovaniu významných incidentov s cieľom nájsť správnu rovnováhu medzi rýchlym oznamovaním, ktoré pomáha zmierniť potenciálne šírenie významných incidentov a umožňuje subjektom Únie hľadať pomoc, na jednej strane a podrobným oznamovaním, pri ktorom sa čerpajú cenné ponaučenia z jednotlivých incidentov a ktoré postupne zvyšujú kybernetickú odolnosť jednotlivých subjektov Únie a prispieva k zlepšeniu celkového stavu ich kybernetickej bezpečnosti na strane druhej. V tejto súvislosti by toto nariadenie malo zahŕňať oznamovanie incidentov, ktoré by na základe počiatočného posúdenia vykonaného dotknutým subjektom Únie mohli spôsobiť vážne prevádzkové narušenie fungovania dotknutého subjektu Únie alebo finančnú stratu tomuto subjektu alebo ovplyvniť iné fyzické alebo právnické osoby tým, že by im spôsobili značnú majetkovú alebo nemajetkovú ujmu. V takomto počiatočnom posúdení by sa okrem iného mali zohľadniť zasiahnuté siete a informačné systémy, najmä ich význam pre fungovanie subjektu Únie, závažnosť a technické charakteristiky kybernetickej hrozby a všetky súvisiace zraniteľnosti, ktoré sa využívajú, ako aj skúsenosti subjektu Únie s podobnými incidentmi. Pri určovaní toho, či ide o vážne prevádzkové narušenie, by dôležitú úlohu mohli zohrávať ukazovatele, ako je napríklad rozsah, v akom je ovplyvnené fungovanie subjektu Únie, trvanie incidentu alebo počet zasiahnutých fyzických alebo právnických osôb.

(37) Keďže infraštruktúra a siete a informačné systémy príslušného subjektu Únie a členského štátu, v ktorom sa daný subjekt Únie nachádza, sú prepojené, je nevyhnutné, aby bol tento členský štát bez zbytočného odkladu informovaný o významnom incidente v danom subjekte Únie. Na tento účel by mal dotknutý subjekt Únie informovať všetky relevantné náprotivky v členskom štáte určené alebo zriadené podľa článkov 8 a 10 smernice (EÚ) 2022/2555 o výskyte významného incidentu, ktorý oznamuje CERT-EU. Ak sa CERT-EU dozvie o významnom incidente, ktorý nastal v členskom štáte, mal by informovať všetky relevantné náprotivky v tomto členskom štáte.

(38) Mal by sa zaviesť mechanizmus na zabezpečenie účinnej výmeny informácií, koordinácie a spolupráce subjektov Únie v prípade závažných incidentov vrátane jasného určenia úloh a povinností zainteresovaných subjektov Únie. Zástupca Komisie v IICB by mal byť, s výhradou plánu riadenia kybernetických kríz, kontaktnou osobou na uľahčenie zdieľania relevantných informácií súvisiacich so závažnými incidentmi medzi IICB a Európskou sieťou styčných organizácií pre kybernetické krízy (ďalej len „EU-CyCLONe“) ako príspevok k spoločnej situačnej informovanosti. Úlohou zástupcu Komisie v IICB ako kontaktnej osoby by nemala byť dotknutá samostatná a odlišná úloha Komisie v sieti EU-CyCLONe podľa článku 16 ods. 2 smernice (EÚ) 2022/2555.

(39) Na spracúvanie osobných údajov vykonávané podľa tohto nariadenia sa uplatňuje nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 ([7]). Spracúvanie osobných údajov by sa mohlo uskutočňovať v súvislosti s opatreniami prijatými v kontexte riadenia kybernetickobezpečnostných rizík, riešenia zraniteľností a incidentov, zdieľania informácií o incidentoch, kybernetických hrozbách a zraniteľnostiach a v kontexte koordinácie a spolupráce v oblasti reakcie na incidenty. Takéto opatrenia by si mohli vyžadovať spracúvanie určitých kategórií osobných údajov, ako sú napríklad IP adresy, jednotné vyhľadávače zdrojov (URL), názvy domén, e-mailové adresy, organizačné úlohy dotknutej osoby, časové pečiatky, predmety e-mailov alebo názvy súborov. Všetky opatrenia

([7]) 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).

prijaté podľa tohto nariadenia by mali byť v súlade s rámcom ochrany údajov a súkromia a subjekty Únie, CERT-EU a v relevantných prípadoch IICB by mali prijať všetky relevantné technické a organizačné záruky na zabezpečenie takéhoto súladu zodpovedným spôsobom.

(40) Týmto nariadením sa stanovuje právny základ pre spracúvanie osobných údajov subjektmi Únie, CERT-EU a v relevantných prípadoch IICB na účely plnenia ich úloh a povinností podľa tohto nariadenia v súlade s článkom 5 ods. 1 písm. b) nariadenia (EÚ) 2018/1725. CERT-EU môže konať ako sprostredkovateľ alebo prevádzkovateľ v závislosti od úlohy, ktorú vykonáva podľa nariadenia (EÚ) 2018/1725.

(41) V určitých prípadoch a na účely plnenia svojich povinností podľa tohto nariadenia na zabezpečenie vysokej úrovne kybernetickej bezpečnosti, a najmä v kontexte riešenia zraniteľností a incidentov, môže byť potrebné, aby subjekty Únie a CERT-EU spracúvali osobitné kategórie osobných údajov uvedené v článku 10 ods. 1 nariadenia (EÚ) 2018/1725. Týmto nariadením sa stanovuje právny základ pre spracúvanie osobitných kategórií osobných údajov subjektmi Únie a CERT-EU v súlade s článkom 10 ods. 2 písm. g) nariadenia (EÚ) 2018/1725. Spracúvanie osobitných kategórií osobných údajov podľa tohto nariadenia by malo byť striktne primerané sledovanému cieľu. S výhradou podmienok stanovených v článku 10 ods. 2 písm. g) uvedeného nariadenia by subjekty Únie a CERT-EU mali mať možnosť spracúvať takéto údaje len v nevyhnutnom rozsahu a ak sa to výslovne stanovuje v tomto nariadení. Pri spracúvaní osobitných kategórií osobných údajov by subjekty Únie a CERT-EU mali rešpektovať podstatu práva na ochranu údajov a stanoviť vhodné a konkrétne opatrenia na ochranu základných práv a záujmov dotknutých osôb.

(42) Podľa článku 33 nariadenia (EÚ) 2018/1725 by subjekty Únie a CERT-EU mali so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb, zaviesť primerané technické a organizačné opatrenia s cieľom zaistiť primeranú úroveň bezpečnosti osobných údajov, ako je napríklad poskytovanie obmedzených prístupových práv na základe potreby informovanosti, uplatňovanie zásad audítorského záznamu, prijatie spracovateľského reťazca, uchovávanie neaktívnych údajov v kontrolovanom a kontrolovateľnom prostredí, štandardizované prevádzkové postupy a opatrenia na zachovanie súkromia, ako je napríklad pseudonymizácia alebo šifrovanie. Tieto opatrenia by sa nemali vykonávať spôsobom, ktorý by mal vplyv na účely riešenia incidentov a integrity dôkazov. Ak subjekt Únie alebo CERT-EU prenáša osobné údaje týkajúce sa incidentu vrátane osobitných kategórií osobných údajov protistrane alebo partnerovi na účely tohto nariadenia, takéto prenosy by mali byť v súlade s nariadením (EÚ) 2018/1725. Ak sa tretej strane prenášajú osobitné kategórie osobných údajov, subjekty Únie a CERT-EU by mali zabezpečiť, aby tretia strana uplatňovala opatrenia týkajúce sa ochrany osobných údajov na úrovni rovnocennej s nariadením (EÚ) 2018/1725.

(43) Osobné údaje spracúvané na účely tohto nariadenia by sa mali uchovávať len tak dlho, ako je to potrebné v súlade s nariadením (EÚ) 2018/1725. Subjekty Únie a v náležitých prípadoch CERT-EU konajúci ako prevádzkovateľ by mali stanoviť obdobia uchovávania, ktoré sa obmedzia na obdobia nevyhnutné na dosiahnutie konkrétnych účelov. Najmä v súvislosti s osobnými údajmi získanými na účely riešenia incidentov by subjekty Únie a CERT-EU mali rozlišovať medzi osobnými údajmi, ktoré sa získavajú na účely odhaľovania kybernetickej hrozby v ich prostrediach IKT s cieľom zabrániť incidentu, a osobnými údajmi, ktoré sa získavajú na zmiernenie incidentu, reakciu na naň a obnovu po ňom. Pri odhaľovaní kybernetickej hrozby je dôležité vziať do úvahy čas, počas ktorého môže aktér hrozby zostať v systéme neodhalený. Na zmiernenie incidentu, reakciu naň a obnovu po ňom je dôležité zvážiť, či sú osobné údaje potrebné na vysledovanie a riešenie opakujúceho sa incidentu alebo incidentu podobnej povahy, pri ktorom by sa mohla preukázať korelácia.

(44) Zaobchádzanie s údajmi zo strany subjektov Únie a CERT-EU by malo byť v súlade s príslušnými pravidlami o informačnej bezpečnosti. Začlenenie bezpečnosti ľudských zdrojov ako opatrenia na riadenie kybernetickobezpečnostných rizík by tiež malo byť v súlade s príslušnými pravidlami.

(45) Na účel zdieľania informácií sa na označenie toho, že príjemcovia informácií majú uplatňovať obmedzenia zdieľania informácií, používajú viditeľné označenia, a to najmä na základe dohôd o nezverejňovaní informácií alebo neformálnych dohôd o nezverejňovaní informácií, ako je napríklad semaforový protokol, alebo iné jasné označenia zo strany zdroja informácií. Semaforový protokol sa má chápať ako prostriedok na poskytovanie informácií o akýchkoľvek obmedzeniach, pokiaľ ide o ďalšie šírenie informácií. Používa sa takmer vo všetkých jednotkách CSIRT a v niektorých centrách na analýzu a zdieľanie informácií.

(46) Toto nariadenie by sa malo pravidelne hodnotiť vzhľadom na budúce rokovania o viacročných finančných rámcoch, ktoré umožnia prijať ďalšie rozhodnutia o fungovaní a inštitucionálnej úlohe CERT-EU vrátane možného stanovenia CERT-EU za úrad Únie.

(47) IICB by s pomocou CERT-EU mala skúmať a hodnotiť vykonávanie tohto nariadenia a o svojich zisteniach informovať Komisiu. Na základe týchto informácií by Komisia mala podať správu Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov. V uvedenej správe by sa na základe informácií od IICB mala vyhodnotiť vhodnosť zahrnutia sietí a informačných systémov, v ktorých sa zaobchádza s utajovanými skutočnosťami EÚ, do rozsahu pôsobnosti tohto nariadenia, najmä ak neexistujú spoločné pravidlá informačnej bezpečnosti pre subjekty Únie.

(48) V súlade so zásadou proporcionality je pre dosiahnutie základného cieľa, ktorým je dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v rámci subjektov Únie, potrebné a vhodné stanoviť pravidlá kybernetickej bezpečnosti pre subjekty Únie. V súlade s článkom 5 ods. 4 Zmluvy o Európskej únii toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie sledovaného cieľa.

(49) Toto nariadenie odráža skutočnosť, že subjekty Únie sa líšia veľkosťou a schopnosťami, a to aj pokiaľ ide o finančné a ľudské zdroje.

(50) V súlade s článkom 42 ods. 1 nariadenia (EÚ) 2018/1725 sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 17. mája 2022 svoje stanovisko ([8]),

PRIJALI TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

Týmto nariadením sa stanovujú opatrenia, ktorých cieľom je dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v subjektoch Únie, pokiaľ ide o:

a) zriadenie vnútorného rámca riadenia, správy a kontroly kybernetickobezpečnostných rizík každým subjektom Únie podľa článku 6;

b) riadenie kybernetickobezpečnostných rizík, ich oznamovanie a zdieľanie informácií;

c) organizáciu, fungovanie a činnosť Medziinštitucionálnej rady pre kybernetickú bezpečnosť zriadenej podľa článku 10, ako aj organizáciu a fungovanie Služby kybernetickej bezpečnosti pre inštitúcie, orgány, úrady a agentúry Únie (ďalej len „CERT-EU“);

d) monitorovanie vykonávania tohto nariadenia.

([8]) Ú. v. EÚ C 258, 5.7.2022, s. 10.

Článok 2

Rozsah pôsobnosti

1. Toto nariadenie sa vzťahuje na subjekty Únie, Medziinštitucionálnu radu pre kybernetickú bezpečnosť zriadenú podľa článku 10 a CERT-EU.

2. Toto nariadenie sa uplatňuje bez toho, aby bola dotknutá inštitucionálna autonómia podľa zmlúv.

3. S výnimkou článku 13 ods. 8 sa toto nariadenie nevzťahuje na siete a informačné systémy, v ktorých sa zaobchádza s utajovanými skutočnosťami EÚ (EUCI).

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňujú tieto vymedzenia pojmov:

1. „subjekty Únie“ sú inštitúcie, orgány, úrady a agentúry Únie zriadené Zmluvou o Európskej únii, Zmluvou o fungovaní Európskej únie (ďalej len „ZFEÚ“) alebo Zmluvou o založení Európskeho spoločenstva pre atómovú energiu alebo na ich základe;

2. „sieť a informačný systém“ je sieť a informačný systém v zmysle vymedzenia v článku 6 bode 1 smernice (EÚ) 2022/2555;

3. „bezpečnosť sietí a informačných systémov“ je bezpečnosť sietí a informačných systémov v zmysle vymedzenia v článku 6 bode 2 smernice (EÚ) 2022/2555;

4. „kybernetická bezpečnosť“ je kybernetická bezpečnosť v zmysle vymedzenia v článku 2 bode 1 nariadenia (EÚ) 2019/881;

5. „manažment najvyššej úrovne“ je manažér, riadiaci orgán alebo orgán koordinácie a dohľadu, ktorý je zodpovedný za fungovanie subjektu Únie na najvyššej administratívnej úrovni s mandátom prijímať alebo schvaľovať rozhodnutia podľa mechanizmu správy a riadenia na vysokej úrovni tohto subjektu Únie bez toho, aby boli dotknuté formálne povinnosti iných úrovní manažmentu za dodržiavanie povinností a riadenie kybernetickobezpečnostných rizík v im prislúchajúcich oblastiach zodpovednosti;

6. „udalosť odvrátená v poslednej chvíli“ je udalosť odvrátená v poslednej chvíli v zmysle vymedzenia v článku 6 bode 5 smernice (EÚ) 2022/2555;

7. „incident“ je incident v zmysle vymedzenia v článku 6 bode 6 smernice (EÚ) 2022/2555;

8. „závažný incident“ je incident, ktorý spôsobí takú úroveň narušenia, ktorá presahuje schopnosť subjektu Únie a CERT-EU reagovať naň, alebo ktorý má významný vplyv na najmenej dva subjekty Únie;

9. „rozsiahly kybernetický incident“ je rozsiahly kybernetický incident v zmysle vymedzenia v článku 6 bode 7 smernice (EÚ) 2022/2555;

10. „riešenie incidentov“ je riešenie incidentov v zmysle vymedzenia v článku 6 bode 8 smernice (EÚ) 2022/2555;

11. „kybernetická hrozba“ je kybernetická hrozba v zmysle vymedzenia v článku 2 bode 8 nariadenia (EÚ) 2019/881;

12. „významná kybernetická hrozba“ je významná kybernetická hrozba v zmysle vymedzenia v článku 6 bode 11 smernice (EÚ) 2022/2555;

13. „zraniteľnosť“ je zraniteľnosť v zmysle vymedzenia v článku 6 bode 15 smernice (EÚ) 2022/2555;

14. „kybernetickobezpečnostné riziko“ je riziko v zmysle vymedzenia v článku 6 bode 9 smernice (EÚ) 2022/2555;

15. „služba cloud computingu“ je služba cloud computingu v zmysle vymedzenia v článku 6 bode 30 smernice (EÚ) 2022/2555.

Článok 4

Spracúvanie osobných údajov

1. Spracúvanie osobných údajov podľa tohto nariadenia zo strany CERT-EU, Medziinštitucionálnej rady pre kybernetickú bezpečnosť zriadenej podľa článku 10 a subjektov Únie sa vykonáva v súlade s nariadením (EÚ) 2018/1725.

2. Ak CERT-EU, Medziinštitucionálna rada pre kybernetickú bezpečnosť zriadená podľa článku 10 a subjekty Únie vykonávajú úlohy alebo plnia povinnosti podľa tohto nariadenia, spracúvajú a vymieňajú si osobné údaje len v potrebnom rozsahu a výlučne na účely výkonu týchto úloh alebo plnenia týchto povinností.

3. Spracúvanie osobitných kategórií osobných údajov uvedených v článku 10 ods. 1 nariadenia (EÚ) 2018/1725 sa považuje za potrebné z dôvodov významného verejného záujmu v súlade s článkom 10 ods. 2 písm. g) uvedeného nariadenia. Takéto údaje sa môžu spracúvať len v rozsahu potrebnom na vykonávanie opatrení na riadenie kybernetickobezpečnostných rizík uvedených v článkoch 6 a 8, na poskytovanie služieb CERT-EU podľa článku 13, na zdieľanie informácií o incidentoch podľa článku 17 ods. 3 a článku 18 ods. 3, na zdieľanie informácií podľa článku 20, na oznamovacie povinnosti podľa článku 21, na koordináciu a spoluprácu v oblasti reakcie na incidenty podľa článku 22 a na riadenie závažných incidentov podľa článku 23 tohto nariadenia. Keď subjekty Únie a CERT-EU konajú ako prevádzkovatelia, uplatňujú technické opatrenia na zabránenie spracúvaniu osobitných kategórií osobných údajov na iné účely a stanovia vhodné a konkrétne opatrenia na ochranu základných práv a záujmov dotknutých osôb.

KAPITOLA II

OPATRENIA NA ZABEZPEČENIE VYSOKEJ SPOLOČNEJ ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

Článok 5

Vykonávanie opatrení

1. Medziinštitucionálna rada pre kybernetickú bezpečnosť zriadená podľa článku 10 po konzultácii s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) a po prijatí usmernení od CERT-EU vydá do 8. septembra 2024 usmernenia pre subjekty Únie na účely vykonania počiatočného preskúmania kybernetickej bezpečnosti a vytvorenia vnútorného rámca riadenia, správy a kontroly kybernetickobezpečnostných rizík podľa článku 6, vykonávania posúdení vyspelosti v oblasti kybernetickej bezpečnosti podľa článku 7, prijatia opatrení na riadenie kybernetickobezpečnostných rizík podľa článku 8 a prijatia plánu kybernetickej bezpečnosti podľa článku 9.

2. Pri vykonávaní článkov 6 až 9 subjekty Únie zohľadňujú usmernenia uvedené v odseku 1 tohto článku, ako aj príslušné usmernenia a odporúčania prijaté podľa článkov 11 a 14.

Článok 6

Rámec riadenia, správy a kontroly kybernetickobezpečnostných rizík

1. Každý subjekt Únie po vykonaní počiatočného preskúmania kybernetickej bezpečnosti, ako je napríklad audit, zriadi do 8. apríla 2025 vnútorný rámec riadenia, správy a kontroly kybernetickobezpečnostných rizík (ďalej len „rámec“). Nad vytvorením rámca dohliada a zodpovedá zaň manažment najvyššej úrovne subjektu Únie.

2. Rámec sa vzťahuje na celé verejne prístupné prostredie IKT dotknutého subjektu Únie vrátane akéhokoľvek prostredia IKT v jeho priestoroch, siete prevádzkovej technológie v jeho priestoroch, externe zabezpečovaných aktív a služieb v prostrediach cloud computingu alebo služieb s hostingom tretích strán, mobilných zariadení, korporátnych sietí, podnikových sietí, ktoré nie sú pripojené k internetu, a akýchkoľvek zariadení pripojených k týmto prostrediam (ďalej len „prostredie IKT“). Rámec je založený na prístupe zohľadňujúcom všetky riziká.

3. Rámcom sa zabezpečí vysoká úroveň kybernetickej bezpečnosti. V rámci sa stanovujú vnútorné politiky kybernetickej bezpečnosti, vrátane cieľov a priorít, pre bezpečnosť sietí a informačných systémov, ako aj úlohy a povinnosti zamestnancov subjektu Únie poverených zabezpečením účinného vykonávania tohto nariadenia. Rámec zahŕňa aj mechanizmy na meranie účinnosti vykonávania.

4. Rámec sa vzhľadom na meniace sa kybernetickobezpečnostné riziká pravidelne preskúma, a to aspoň každé štyri roky. V náležitých prípadoch a po podaní žiadosti Medziinštitucionálnej rady pre kybernetickú bezpečnosť zriadenej podľa článku 10 možno rámec subjektu Únie aktualizovať na základe usmernení CERT-EU vychádzajúcich zo zistených incidentov alebo možných nedostatkov vo vykonávaní tohto nariadenia.

5. Manažment najvyššej úrovne každého subjektu Únie zodpovedá za vykonávanie tohto nariadenia a dohliada na dodržiavanie povinností súvisiacich s rámcom zo strany jeho organizácie.

6. V náležitých prípadoch a bez toho, aby bola dotknutá jeho zodpovednosť za vykonávanie tohto nariadenia, môže manažment najvyššej úrovne každého subjektu Únie delegovať osobitné povinnosti podľa tohto nariadenia na riadiacich pracovníkov v zmysle článku 29 ods. 2 služobného poriadku alebo iných úradníkov na rovnocennej úrovni v rámci dotknutého subjektu Únie. Bez ohľadu na takéto delegovanie môže byť manažment najvyššej úrovne braný na zodpovednosť za porušenie tohto nariadenia dotknutým subjektom Únie.

7. Každý subjekt Únie má zavedené účinné mechanizmy s cieľom zabezpečiť, aby sa na kybernetickú bezpečnosť vynakladal primeraný percentuálny podiel z rozpočtu na IKT. Pri stanovení tohto percentuálneho podielu sa náležite zohľadní rámec.

8. Každý subjekt Únie menuje miestneho úradníka pre kybernetickú bezpečnosť alebo osobu v rovnocennej funkcii, ktorá koná ako jeho jednotné kontaktné miesto v súvislosti so všetkými aspektmi kybernetickej bezpečnosti. Miestny úradník pre kybernetickú bezpečnosť pomáha s vykonávaním tohto nariadenia a pravidelne podáva správy o stave vykonávania priamo manažmentu najvyššej úrovne. Bez toho, aby bola dotknutá skutočnosť, že miestny úradník pre kybernetickú bezpečnosť je jednotným kontaktným miestom v každom subjekte Únie, subjekt Únie môže delegovať určité úlohy miestneho pracovníka pre kybernetickú bezpečnosť v súvislosti s vykonávaním tohto nariadenia na CERT-EU na základe dohody o úrovni poskytovaných služieb uzavretej medzi daným subjektom Únie a CERT-EU, alebo tieto úlohy môžu spoločne vykonávať viaceré subjekty Únie. Ak sú tieto úlohy delegované na CERT-EU, Medziinštitucionálna rada pre kybernetickú bezpečnosť zriadená podľa článku 10 rozhodne, či poskytovanie takejto služby bude súčasťou základných služieb CERT-EU, pričom zohľadní ľudské a finančné zdroje dotknutého subjektu Únie. Každý subjekt Únie bez zbytočného odkladu oznámi CERT-EU vymenovaných miestnych úradníkov pre kybernetickú bezpečnosť a všetky následné vykonané zmeny.

CERT-EU zostaví a pravidelne aktualizuje zoznam vymenovaných miestnych úradníkov pre kybernetickú bezpečnosť.

9. Riadiaci pracovníci v zmysle článku 29 ods. 2 služobného poriadku alebo iní úradníci na rovnocennej úrovni každého subjektu Únie, ako aj všetci príslušní zamestnanci poverení výkonom opatrení a plnením povinností v oblasti riadenia kybernetickobezpečnostných rizík stanovených v tomto nariadení sa pravidelne zúčastňujú osobitnej odbornej prípravy s cieľom získať dostatočné vedomosti a zručnosti na pochopenie a posúdenie kybernetickobezpečnostných rizík a postupov ich riadenia, ako aj ich vplyvu na prevádzku subjektu Únie.

Článok 7

Posúdenia vyspelosti v oblasti kybernetickej bezpečnosti

1. Každý subjekt Únie vykoná do 8. júla 2025 a potom aspoň každé dva roky posúdenie vyspelosti v oblasti kybernetickej bezpečnosti zahŕňajúce všetky prvky jeho prostredia IKT.

2. Posúdenia vyspelosti v oblasti kybernetickej bezpečnosti sa v náležitých prípadoch vykonávajú s pomocou špecializovanej tretej strany.

3. Subjekty Únie s podobnými štruktúrami môžu spolupracovať pri vykonávaní posúdení vyspelosti v oblasti kybernetickej bezpečnosti pre svoje príslušné subjekty.

4. Na základe žiadosti Medziinštitucionálnej rady pre kybernetickú bezpečnosť zriadenej podľa článku 10 a s výslovným súhlasom dotknutého subjektu Únie môže výsledky posúdenia vyspelosti v oblasti kybernetickej bezpečnosti prerokovať táto rada alebo neformálna skupina miestnych úradníkov pre kybernetickú bezpečnosť s cieľom poučiť sa zo skúseností a zdieľať najlepšie postupy.

Článok 8

Opatrenia na riadenie kybernetickobezpečnostných rizík

1. Bez zbytočného odkladu a v každom prípade do 8. septembra 2025 prijme každý subjekt Únie pod dohľadom svojho manažmentu najvyššej úrovne vhodné a primerané technické, prevádzkové a organizačné opatrenia na riadenie kybernetickobezpečnostných rizík identifikovaných prostredníctvom rámca a na predchádzanie incidentom alebo minimalizáciu ich následkov. S ohľadom na najnovšie a v náležitých prípadoch relevantné európske a medzinárodné normy sa uvedenými opatreniami zabezpečí úroveň bezpečnosti sietí a informačných systémov v celom prostredí IKT zodpovedajúca identifikovaným kybernetickobezpečnostným rizikám. Pri posudzovaní primeranosti týchto opatrení sa náležite zohľadní stupeň vystavenia subjektu Únie kybernetickobezpečnostným rizikám, jeho veľkosť a pravdepodobnosť výskytu incidentov a ich závažnosť vrátane ich spoločenského, hospodárskeho a medziinštitucionálneho vplyvu.

2. Pri vykonávaní opatrení na riadenie kybernetickobezpečnostných rizík sa subjekty Únie zameriavajú aspoň na tieto oblasti:

a) politiku kybernetickej bezpečnosti vrátane opatrení potrebných na dosiahnutie cieľov a priorít uvedených v článku 6 a v odseku 3 tohto článku;

b) zásady analýzy kybernetickobezpečnostných rizík a bezpečnosti informačných systémov;

c) ciele politiky týkajúce sa využívania služieb cloud computingu;

d) v náležitých prípadoch audit kybernetickej bezpečnosti, ktorý môže zahŕňať posúdenie kybernetickobezpečnostných rizík, zraniteľností a kybernetických hrozieb, a penetračné testovanie, ktoré pravidelne vykonáva dôveryhodný súkromný poskytovateľ;

e) vykonávanie odporúčaní vyplývajúcich z auditov kybernetickej bezpečnosti uvedených v písmene d) prostredníctvom aktualizácií kybernetickej bezpečnosti a politiky;

f) organizáciu kybernetickej bezpečnosti vrátane vymedzenia úloh a povinností;

g) správu aktív vrátane inventára aktív IKT a kartografie sietí IKT;

h) bezpečnosť ľudských zdrojov a kontrolu prístupu;

i) bezpečnosť operácií;

j) komunikačnú bezpečnosť;

k) nadobudnutie, vývoj a údržbu systému vrátane zásad riešenia a zverejňovania zraniteľností;

l) ak je to možné, zásady transparentnosti zdrojového kódu;

m) bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom Únie a jeho priamymi dodávateľmi alebo poskytovateľmi služieb;

n) riešenie incidentov a spoluprácu s CERT-EU, ako je napríklad údržba monitorovania bezpečnosti a logovania;

o) riadenie kontinuity činností, ako je napríklad riadenie zálohovania a obnova systému po havárii, a krízové riadenie; a

p) propagáciu a vývoj programov, pokiaľ ide o vzdelávanie, nadobúdanie zručností, zvyšovanie informovanosti, cvičenia a odbornú prípravu v oblasti kybernetickej bezpečnosti.

Na účely prvého pododseku písm. m) subjekty Únie zohľadňujú zraniteľnosti špecifické pre každého priameho dodávateľa a poskytovateľa služieb a celkovú kvalitu produktov a postupy ich dodávateľov a poskytovateľov služieb v oblasti kybernetickej bezpečnosti vrátane ich postupov bezpečného vývoja.

3. Subjekty Únie prijmú aspoň tieto opatrenia na riadenie kybernetickobezpečnostných rizík:

a) technické opatrenia na umožnenie a udržanie telepráce;

b) konkrétne kroky na prechod k zásadám nulovej dôvery;

c) používanie dvojstupňovej autentifikácie ako normy v sieťach a informačných systémoch;

d) používanie kryptografie a šifrovania, najmä šifrovania bez medzifáz, ako aj bezpečných digitálnych podpisov;

e) v náležitých prípadoch zavedenie zabezpečenej hlasovej, video a textovej komunikácie a zabezpečených systémov tiesňovej komunikácie v rámci subjektu Únie;

f) proaktívne opatrenia na odhaľovanie a odstraňovanie malvéru a špionážneho softvéru;

g) zavedenie bezpečnosti dodávateľského reťazca softvéru prostredníctvom kritérií bezpečného vývoja a hodnotenia softvéru;

h) vypracovanie a schválenie učebných plánov odbornej prípravy v oblasti kybernetickej bezpečnosti zodpovedajúce predpísaným úlohám a očakávaným spôsobilostiam manažmentu najvyššej úrovne a zamestnancov subjektu Únie poverených zaistením účinného vykonávania tohto nariadenia;

i) pravidelná odborná príprava zamestnancov v oblasti kybernetickej bezpečnosti;

j) v relevantných prípadoch účasť na analýzach rizík prepojení medzi subjektmi Únie;

k) posilnenie pravidiel obstarávania s cieľom uľahčiť dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti prostredníctvom:

   i) odstránenia zmluvných prekážok, ktoré obmedzujú zdieľanie informácií CERT-EU o incidentoch, zraniteľnostiach a kybernetických hrozbách poskytovateľmi služieb IKT;

   ii) zmluvných povinností oznamovať incidenty, zraniteľnosti a kybernetické hrozby, ako aj mať zavedené mechanizmy primeranej reakcie na incidenty a monitorovania incidentov.

Článok 9

Plány kybernetickej bezpečnosti

1. V nadväznosti na záver posúdenia vyspelosti v oblasti kybernetickej bezpečnosti vykonaného podľa článku 7 a vzhľadom na aktíva a kybernetickobezpečnostné riziká identifikované v rámci, ako aj na opatrenia na riadenie kybernetickobezpečnostných rizík prijaté podľa článku 8 manažment najvyššej úrovne každého subjektu Únie bez zbytočného odkladu a najneskôr do 8. januára 2026 schváli plán kybernetickej bezpečnosti. Cieľom plánu kybernetickej bezpečnosti je zvýšiť celkovú kybernetickú bezpečnosť subjektu Únie, a tak prispieť k zlepšeniu vysokej spoločnej úrovne kybernetickej bezpečnosti v rámci subjektov Únie. Plán kybernetickej bezpečnosti obsahuje aspoň opatrenia na riadenie kybernetickobezpečnostných rizík prijaté podľa článku 8. Plán kybernetickej bezpečnosti sa reviduje každé dva roky, alebo v prípade potreby častejšie, po posúdeniach vyspelosti v oblasti kybernetickej bezpečnosti vykonaných podľa článku 7 alebo po akomkoľvek podstatnom preskúmaní rámca.

2. Súčasťou plánu kybernetickej bezpečnosti je plán riadenia kybernetických kríz subjektu Únie pre prípad závažných incidentov.

3. Subjekt Únie predloží vypracovaný plán kybernetickej bezpečnosti Medziinštitucionálnej rade pre kybernetickú bezpečnosť zriadenej podľa článku 10.

KAPITOLA III

MEDZIINŠTITUCIONÁLNA RADA PRE KYBERNETICKÚ BEZPEČNOSŤ

Článok 10

Medziinštitucionálna rada pre kybernetickú bezpečnosť

1. Zriaďuje sa Medziinštitucionálna rada pre kybernetickú bezpečnosť (ďalej len „IICB“).

2. IICB zodpovedá za:

a) monitorovanie a presadzovanie vykonávania tohto nariadenia subjektmi Únie;

b) dohľad nad vykonávaním všeobecných priorít a cieľov CERT-EU, ako aj strategické riadenie CERT-EU.

3. IICB tvoria:

a) jeden zástupca vymenovaný každým z týchto subjektov:

   i) Európsky parlament;

   ii) Európska rada

   iii) Rada Európskej únie;

   iv) Komisia;

   v) Súdny dvor Európskej únie;

   vi) Európska centrálna banka;

   vii) Dvor audítorov;

   viii) Európska služba pre vonkajšiu činnosť;

   ix) Európsky hospodársky a sociálny výbor;

   x) Európsky výbor regiónov;

   xi) Európska investičná banka;

   xii) Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti;

   xiii) agentúra ENISA;

   xiv) európsky dozorný úradník pre ochranu údajov;

   xv) Agentúra Európskej únie pre vesmírny program;

b) traja zástupcovia vymenovaní sieťou agentúr EÚ (ďalej len „EUAN“) na návrh jej poradného výboru pre IKT, ktorí zastupujú záujmy orgánov, úradov a agentúr Únie, ktoré prevádzkujú svoje vlastné prostredie IKT, ktoré sa líši od prostredí uvedených v písmene a).

Subjekty Únie zastúpené v IICB sa snažia dosiahnuť rodovú rovnováhu vymenovaných zástupcov.

4. Členom IICB môže pomáhať náhradník. Predseda môže pozvať iných zástupcov subjektov Únie uvedených v odseku 3 alebo iných subjektov Únie, aby sa zúčastnili na zasadnutiach IICB bez hlasovacieho práva.

5. Na zasadnutiach IICB sa ako pozorovatelia môžu zúčastňovať vedúci CERT-EU a predseda skupiny pre spoluprácu zriadenej podľa článku 14 smernice (EÚ) 2022/2555, predseda siete jednotiek CSIRT zriadenej podľa článku 15 smernice 2022/2555 a predseda siete EU-CyCLONe zriadenej podľa článku 16 smernice (EÚ) 2022/2555 alebo ich náhradníci. Vo výnimočných prípadoch môže IICB v súlade so svojim vnútorným rokovacím poriadkom rozhodnúť inak.

6. IICB prijme svoj vnútorný rokovací poriadok.

7. IICB v súlade so svojím vnútorným rokovacím poriadkom vymenuje spomedzi svojich členov predsedu na obdobie troch rokov. Náhradník predsedu sa na rovnaké obdobie stáva riadnym členom IICB.

8. IICB zasadá aspoň trikrát do roka z iniciatívy svojho predsedu, na žiadosť CERT-EU alebo na žiadosť ktoréhokoľvek zo svojich členov.

9. Každý člen IICB má jeden hlas. IICB prijíma rozhodnutia jednoduchou väčšinou, ak v tomto nariadení nie je stanovené inak. Predseda IICB nehlasuje, s výnimkou prípadov rovnosti hlasov, keď môže udeliť rozhodujúci hlas.

10. IICB môže konať prostredníctvom zjednodušeného písomného postupu iniciovaného v súlade s vnútorným rokovacím poriadkom IICB. Pri uvedenom postupe sa príslušné rozhodnutie považuje za schválené v lehote stanovenej predsedom, okrem prípadov, keď niektorý z členov vznesie námietku.

11. Sekretariát IICB zabezpečuje Komisia a zodpovedá sa predsedovi IICB.

12. Členom siete EUAN oznamujú rozhodnutia IICB zástupcovia vymenovaní sieťou EUAN. Ktorýkoľvek člen siete EUAN má právo obrátiť sa na týchto zástupcov alebo predsedu IICB s každou záležitosťou, na ktorú by podľa jeho názoru mala byť IICB upozornená.

13. IICB môže zriadiť výkonný výbor, ktorý jej pomáha pri práci, a delegovať mu niektoré svoje úlohy a právomoci. IICB stanoví rokovací poriadok výkonného výboru vrátane jeho úloh a právomocí, ako aj funkčné obdobie jeho členov.

14. IICB predloží Európskemu parlamentu a Rade do 8. januára 2025 a následne každoročne správu, v ktorej podrobne opíše pokrok dosiahnutý pri vykonávaní tohto nariadenia a v ktorej uvedie najmä rozsah spolupráce CERT-EU s náprotivkami v členskom štáte v každom členskom štáte. Táto správa sa použije ako zdroj informácií na vypracovanie správy o stave kybernetickej bezpečnosti v Únii prijímanej každé dva roky v súlade s článkom 18 smernice (EÚ) 2022/2555.

Článok 11

Úlohy IICB

IICB pri plnení svojich úloh predovšetkým:

a) poskytuje usmernenia vedúcemu CERT-EU;

b) účinne monitoruje vykonávanie tohto nariadenia, dohliada nad jeho vykonávaním a podporuje subjekty Únie pri posilňovaní ich kybernetickej bezpečnosti, a to v náležitých prípadoch aj vyžiadaním ad hoc správ od subjektov Únie a CERT-EU;

c) v nadväznosti na strategickú diskusiu prijíma viacročnú stratégiu na zvýšenie úrovne kybernetickej bezpečnosti v subjektoch Únie, pravidelne ju posudzuje, a to aspoň každých päť rokov, a v prípade potreby ju mení;

d) stanovuje metodiku a organizačné aspekty vykonávania dobrovoľných partnerských preskúmaní subjektmi Únie s cieľom čerpať sa zo spoločných skúseností, posilniť vzájomnú dôveru, dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti, ako aj posilniť spôsobilosti subjektov Únie v oblasti kybernetickej bezpečnosti, pričom sa zabezpečí, aby takéto partnerské preskúmania vykonávali odborníci na kybernetickú bezpečnosť určení iným subjektom Únie, než je subjekt Únie podstupujúci preskúmanie, a aby metodika vychádzala z článku 19 smernice (EÚ) 2022/2555 a v náležitých prípadoch bola prispôsobená subjektom Únie;

e) na základe návrhu vedúceho CERT-EU schvaľuje ročný pracovný program CERT-EU a monitoruje jeho vykonávanie;

f) na základe návrhu vedúceho CERT-EU schvaľuje katalóg služieb CERT-EU a všetky jeho aktualizácie;

g) na základe návrhu vedúceho CERT-EU schvaľuje ročný finančný plán príjmov a výdavkov súvisiacich s činnosťami CERT-EU, ktorý zahŕňa aj plán počtu zamestnancov;

h) na základe návrhu vedúceho CERT-EU schvaľuje postupy pre dohody o úrovni poskytovaných služieb;

i) preskúmava a schvaľuje výročnú správu o činnostiach CERT-EU a správe jeho finančných prostriedkov, ktorú vypracoval vedúci CERT-EU;

j) schvaľuje a monitoruje kľúčové ukazovatele výkonnosti (KPI) CERT-EU stanovené na základe návrhu vedúceho CERT-EU;

k) schvaľuje dohody o spolupráci, dohody o úrovni poskytovaných služieb alebo zmluvy medzi CERT-EU a inými subjektmi podľa článku 18;

l) prijíma usmernenia a odporúčania na základe návrhu CERT-EU v súlade s článkom 14 a dáva CERT-EU pokyn na vydanie, zrušenie alebo zmenu návrhu usmernení alebo odporúčaní, alebo výzvy na činnosť;

m) zriaďuje technické poradné skupiny poverené konkrétnymi úlohami na pomoc pri práci IICB, schvaľuje ich mandát a menuje ich predsedov;

n) prijíma a posudzuje dokumenty a správy predložené subjektmi Únie podľa tohto nariadenia, ako sú napríklad posúdenia vyspelosti v oblasti kybernetickej bezpečnosti;

o) umožní zriadenie neformálnej skupiny miestnych úradníkov pre kybernetickú bezpečnosť subjektov Únie, podporovanej agentúrou ENISA, s cieľom vymieňať si najlepšie postupy a informácie v súvislosti s vykonávaním tohto nariadenia;

p) s prihliadnutím na informácie o identifikovaných kybernetickobezpečnostných rizikách a získané poznatky, ktoré poskytuje CERT-EU, monitoruje primeranosť dohôd o prepojení medzi prostrediami IKT subjektov Únie a poskytuje poradenstvo o možných zlepšeniach;

q) vypracuje plán riadenia kybernetických kríz s cieľom podporiť koordinované riadenie závažných incidentov, ktoré majú vplyv na subjekty Únie, na operačnej úrovni a prispieť k pravidelnej výmene relevantných informácií, najmä pokiaľ ide o dosah a závažnosť závažných incidentov a možné spôsoby zmiernenia ich vplyvov;

r) koordinuje prijímanie plánov riadenia kybernetických kríz jednotlivých subjektov Únie uvedených v článku 9 ods. 2;

s) prijíma odporúčania týkajúce sa bezpečnosti dodávateľského reťazca uvedenej v článku 8 ods. 2 prvom pododseku písm. m), pričom prihliada na výsledky koordinovaných posúdení bezpečnostných rizík kritických dodávateľských reťazcov na úrovni Únie uvedených v článku 22 smernice (EÚ) 2022/2555, aby podporila subjekty Únie pri prijímaní účinných a primeraných opatrení na riadenie kybernetickobezpečnostných rizík.

Článok 12

Dodržiavanie povinností

1. IICB podľa článku 10 ods. 2 a článku 11 účinne monitoruje vykonávanie tohto nariadenia a prijatých usmernení, odporúčaní a výziev na činnosť subjektmi Únie. IICB môže od subjektov Únie požadovať informácie alebo dokumentáciu potrebné na tento účel. Na účely prijatia opatrení na zabezpečenie dodržiavania povinností podľa tohto článku nemá dotknutý subjekt Únie hlasovacie práva, ak je daný subjekt Únie priamo zastúpený v IICB.

2. Keď IICB zistí, že subjekt Únie toto nariadenie alebo usmernenia, odporúčania alebo výzvy na činnosť vydané podľa tohto nariadenia účinne nevykonáva, bez toho, aby boli dotknuté vnútorné postupy dotknutého subjektu Únie, a po poskytnutí možnosti dotknutému subjektu Únie predložiť svoje vyjadrenie, IICB môže:

a) dať dotknutému subjektu Únie na vedomie odôvodnené stanovisko so zistenými nedostatkami vo vykonávaní tohto nariadenia;

b) po porade s CERT-EU poskytnúť dotknutému subjektu Únie usmernenia s cieľom zabezpečiť súlad jeho rámca, opatrení na riadenie kybernetickobezpečnostných rizík, plánu kybernetickej bezpečnosti a oznamovania s týmto nariadením v stanovenej lehote;

c) vydať varovanie na vyriešenie zistených nedostatkov v stanovenej lehote, ktoré bude obsahovať aj odporúčania na zmenu opatrení prijatých dotknutým subjektom Únie podľa tohto nariadenia;

d) vydať odôvodnené oznámenie adresované dotknutému subjektu Únie v prípade, že nedostatky zistené vo varovaní vydanom podľa písmena c) neboli v stanovenej lehote dostatočne vyriešené;

e) vydať:

i) odporúčanie, aby sa vykonal audit; alebo

ii) žiadosť, aby audit vykonal audítorský útvar tretej strany;

f) v príslušných prípadoch informovať Dvor audítorov v rámci jeho mandátu o údajnom nedodržiavaní povinností;

g) vydať odporúčanie pre všetky členské štáty a subjekty Únie na dočasné pozastavenie tokov údajov do dotknutého subjektu Únie.

Na účely prvého pododseku písm. c) sa primerane obmedzia adresáti varovania, v prípade potreby vzhľadom na závažné kybernetickobezpečnostné riziko.

Varovania a odporúčania vydané podľa prvého pododseku sú adresované manažmentu najvyššej úrovne dotknutého subjektu Únie.

3. Ak IICB prijala opatrenia podľa odseku 2 prvého pododseku písm. a) až g), dotknutý subjekt Únie poskytne podrobný opis opatrení a krokov prijatých na vyriešenie údajných nedostatkov, ktoré IICB zistila. Subjekt Únie predloží tento podrobný opis v primeranej lehote, ktorú si dohodne s IICB.

4. Ak sa IICB domnieva, že subjekt Únie neustále porušuje toto nariadenie a že toto porušovanie vyplýva priamo z konania alebo opomenutia úradníka alebo iného zamestnanca Únie, a to aj z radov manažmentu najvyššej úrovne, IICB požiada dotknutý subjekt Únie, aby prijal primerané opatrenia a aby zvážil prijatie disciplinárneho opatrenia, a to v súlade s pravidlami a postupmi stanovenými v služobnom poriadku a akýmikoľvek inými uplatniteľnými pravidlami a postupmi. Na tento účel IICB postúpi potrebné informácie dotknutému subjektu Únie.

5. Ak subjekty Únie oznámia, že nie sú schopné dodržať lehoty stanovené v článku 6 ods. 1 a článku 8 ods. 1, IICB môže v riadne odôvodnených prípadoch a s prihliadnutím na veľkosť daného subjektu Únie povoliť predĺženie týchto lehôt.

KAPITOLA IV

CERT-EU

Článok 13

Poslanie a úlohy CERT-EU

1. Poslaním CERT-EU je prispievať k bezpečnosti verejne prístupných prostredí IKT subjektov Únie tým, že im poskytuje poradenstvo v oblasti kybernetickej bezpečnosti, pomáha im predchádzať incidentom, odhaľovať ich, riešiť ich, zmierňovať ich účinky, reagovať na ne a zotaviť sa z nich a koná ako ich centrum na výmenu informácií a koordináciu reakcie na incidenty v oblasti kybernetickej bezpečnosti.

2. CERT-EU získava, spravuje a analyzuje informácie o kybernetických hrozbách, zraniteľnostiach a incidentoch týkajúcich sa verejne prístupných infraštruktúr IKT a zdieľa ich so subjektmi Únie. Koordinuje reakcie na incidenty na medziinštitucionálnej úrovni a na úrovni subjektov Únie, a to aj poskytovaním špecializovanej operačnej pomoci alebo koordináciou jej poskytovania.

3. Ako pomoc pre subjekty Únie vykonáva CERT-EU tieto úlohy:

a) podporuje ich pri vykonávaní tohto nariadenia a prispieva ku koordinácii vykonávania tohto nariadenia prostredníctvom opatrení uvedených v článku 14 ods. 1 alebo prostredníctvom *ad hoc* správ požadovaných IICB;

b) ponúka štandardné služby jednotiek CSIRT subjektom Únie prostredníctvom balíka kybernetickobezpečnostných služieb opísaného vo svojom katalógu služieb (základné služby);

c) spravuje sieť partnerov na podporu služieb, ako sa uvádza v článkoch 17 a 18;

d) upozorňuje IICB na problémy súvisiace s vykonávaním tohto nariadenia a vykonávaním usmernení, odporúčaní a výziev na činnosť;

e) na základe informácií uvedených v odseku 2 prispieva v úzkej spolupráci s agentúrou ENISA k situačnej informovanosti o kybernetickej bezpečnosti v Únii.

f) koordinuje riadenie závažných incidentov;

g) v mene subjektov Únie koná ako ekvivalent koordinátora určeného na účely koordinovaného zverejňovania zraniteľností podľa článku 12 ods. 1 smernice (EÚ) 2022/2555.

h) na žiadosť subjektu Únie zabezpečuje proaktívne nerušivé skenovanie verejne prístupných sietí a informačných systémov tohto subjektu Únie.

Informácie uvedené v prvom pododseku písm. e) sa zdieľajú s IICB, sieťou jednotiek CSIRT a v náležitých a vhodných prípadoch so Spravodajským a situačným centrom Európskej únie (ďalej len „EU INTCEN“), a to pri dodržaní primeraných podmienok dôvernosti.

4. CERT-EU môže v súlade s článkom 17 alebo 18 spolupracovať s príslušnými komunitami kybernetickej bezpečnosti v Únii a jej členských štátoch, a to aj v týchto oblastiach:

a) pripravenosť, koordinácia pri incidentoch, výmena informácií a reakcia na krízu na technickej úrovni v prípadoch súvisiacich so subjektmi Únie;

b) operačná spolupráca týkajúca sa siete jednotiek CSIRT, a to aj pokiaľ ide o vzájomnú pomoc;

c) spravodajské informácie o kybernetických hrozbách vrátane situačnej informovanosti;

d) akákoľvek téma, ktorá si vyžaduje odborné technické znalosti CERT-EU v oblasti kybernetickej bezpečnosti.

5. CERT-EU v rámci svojich právomocí štruktúrovane spolupracuje s agentúrou ENISA pri budovaní kapacít, operačnej spolupráci a dlhodobých strategických analýzach kybernetických hrozieb v súlade s nariadením (EÚ) 2019/881. CERT-EU môže spolupracovať a vymieňať si informácie s Európskym centrom boja proti počítačovej kriminalite pri Europole.

6. CERT-EU môže poskytovať tieto služby, ktoré nie sú opísané v jeho katalógu služieb (spoplatnené služby):

a) iné služby na podporu kybernetickej bezpečnosti prostredia IKT subjektov Únie, než sú služby uvedené v odseku 3, na základe dohôd o úrovni poskytovaných služieb a podľa dostupných zdrojov, a to najmä širokospektrálne monitorovanie sietí vrátane bežného nepretržitého monitorovania kybernetických hrozieb s vysokou závažnosťou;

b) iné služby na podporu činností alebo projektov subjektov Únie v oblasti kybernetickej bezpečnosti, než sú služby na ochranu ich prostredia IKT, a to na základe písomných dohôd a s predchádzajúcim povolením IICB;

c) na požiadanie proaktívne skenovanie sietí a informačných systémov dotknutého subjektu Únie s cieľom odhaliť zraniteľnosti s potenciálnym významným vplyvom;

d) služby na podporu bezpečnosti prostredia IKT organizáciám, ktoré nie sú subjektmi Únie a ktoré so subjektmi Únie úzko spolupracujú, napríklad tak, že majú pridelené úlohy alebo povinnosti podľa práva Únie, a to na základe písomných dohôd a s predchádzajúcim povolením IICB.

S ohľadom na prvý pododsek písm. d) CERT-EU môže výnimočne uzavrieť dohody o úrovni poskytovaných služieb s inými subjektmi, než sú subjekty Únie, a to s predchádzajúcim povolením IICB.

7. CERT-EU organizuje cvičenia v oblasti kybernetickej bezpečnosti a môže sa na nich zúčastňovať alebo odporúčať účasť na existujúcich cvičeniach, a to v náležitých prípadoch v úzkej spolupráci s agentúrou ENISA, s cieľom testovať úroveň kybernetickej bezpečnosti subjektov Únie.

8. CERT-EU môže subjektom Únie poskytovať pomoc s incidentmi v sieťach a informačných systémoch, v ktorých sa zaobchádza s utajovanými skutočnosťami EÚ, ak o to dotknuté subjekty Únie výslovne požiadajú v súlade so svojimi príslušnými postupmi. Poskytovaním pomoci zo strany CERT-EU podľa tohto odseku nie sú dotknuté príslušné pravidlá týkajúce sa ochrany utajovaných skutočností.

9. CERT-EU informuje subjekty Únie o svojich postupoch a procesoch riešenia incidentov.

10. Zachovávajúc vysokú mieru dôvernosti a spoľahlivosti CERT-EU prispieva prostredníctvom vhodných mechanizmov spolupráce a hierarchických vzťahov k relevantným a anonymizovaným informáciám o závažných incidentoch a o spôsobe, akým boli riešené. Uvedené informácie sa zahrnú do správy uvedenej v článku 10 ods. 14.

11. CERT-EU v spolupráci s európsky dozorným úradníkom pre ochranu osobných údajov podporuje dotknuté subjekty Únie pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, bez toho, aby boli dotknuté kompetencie a úlohy európskeho dozorného úradníka pre ochranu osobných údajov ako orgánu dohľadu podľa nariadenia (EÚ) 2018/1725.

12. CERT-EU môže subjektom Únie poskytnúť technické poradenstvo alebo informácie o relevantných politických otázkach, ak o to politické oddelenia subjektov Únie výslovne požiadajú.

Článok 14

Usmernenia, odporúčania a výzvy na činnosť

1. CERT-EU podporuje vykonávanie tohto nariadenia vydávaním:

a) výziev na činnosť s opisom naliehavých bezpečnostných opatrení, v ktorých sa subjekty Únie naliehavo vyzývajú, aby tieto opatrenia prijali v stanovenej lehote;

b) návrhov usmernení pre IICB adresovaných všetkým subjektom Únie alebo ich časti;

c) návrhov odporúčaní pre IICB adresovaných jednotlivým subjektom Únie.

Pokiaľ ide o prvý pododsek písm. a), dotknutý subjekt Únie bez zbytočného odkladu po prijatí výzvy na činnosť informuje CERT-EU o tom, ako vykonal naliehavé bezpečnostné opatrenia.

2. Usmernenia a odporúčania môžu zahŕňať:

a) spoločné metodiky a model posudzovania vyspelosti v oblasti kybernetickej bezpečnosti subjektov Únie vrátane zodpovedajúcich stupníc alebo kľúčových ukazovateľov výkonnosti, ktoré slúžia ako referencia na podporu neustáleho zlepšovania kybernetickej bezpečnosti naprieč subjektmi Únie a uľahčujú uprednostňovanie kybernetickobezpečnostných oblastí a opatrení s prihliadnutím na stav kybernetickej bezpečnosti subjektov;

b) postupy alebo zlepšenia týkajúce sa riadenia kybernetickobezpečnostných rizík alebo opatrení na riadenie kybernetickobezpečnostných rizík;

c) postupy týkajúce sa posudzovania vyspelosti v oblasti kybernetickej bezpečnosti a plánov kybernetickej bezpečnosti;

d) vo vhodných prípadoch využívanie spoločných technológií, architektúry, otvoreného zdrojového kódu a súvisiacich najlepších postupov s cieľom dosiahnuť interoperabilitu a spoločné normy vrátane koordinovaného prístupu k bezpečnosti dodávateľského reťazca;

e) vo vhodných prípadoch informácie na umožnenie využívania nástrojov spoločného obstarávania na nákup príslušných služieb a produktov kybernetickej bezpečnosti od dodávateľov, ktorí sú tretími stranami;

f) dohody o zdieľaní informácií podľa článku 20.

Článok 15

Vedúci CERT-EU

1. Vedúceho CERT-EU vymenuje Komisia po jeho schválení dvojtretinovou väčšinou členov IICB. Vo všetkých fázach postupu vymenovania, najmä pri vypracúvaní oznámení o voľnom pracovnom mieste, posudzovaní prihlášok a vymenovaní výberových komisií v súvislosti s uvedeným miestom, sa uskutočňujú konzultácie s IICB. Vo výberovom konaní vrátane konečného užšieho zoznamu kandidátov, z ktorých sa vedúci CERT-EU má vymenovať, sa zabezpečí spravodlivé rodové zastúpenie, pričom sa zohľadnia predložené prihlášky.

2. Vedúci CERT-EU zodpovedá za riadne fungovanie CERT-EU a koná v rámci právomocí jeho funkcie a pod vedením IICB. Vedúci CERT-EU predkladá pravidelné správy predsedovi IICB a na požiadanie podáva IICB ad hoc správy.

3. Vedúci CERT-EU pomáha zodpovednému povoľujúcemu úradníkovi vymenovanému delegovaním pri vypracúvaní výročnej správy o činnosti, ktorá obsahuje finančné informácie a informácie o riadení vrátane výsledkov kontrol a ktorá sa vypracúva v súlade s článkom 74 ods. 9 nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) 2018/1046 ([9]), a pravidelne povoľujúcemu úradníkovi vymenovanému delegovaním podáva správy o vykonávaní opatrení, v súvislosti s ktorými sa na vedúceho CERT-EU subdelegovali právomoci.

4. Vedúci CERT-EU každoročne vypracuje finančné plánovanie administratívnych príjmov a výdavkov na jeho činnosti, návrh ročného pracovného programu, návrh katalógu služieb CERT-EU, návrh revízií katalógu služieb, návrh dohôd o úrovni poskytovaných služieb a návrh kľúčových ukazovateľov výkonnosti (KPI) pre CERT-EU, ktoré má schváliť IICB v súlade s článkom 11. Pri revízii zoznamu služieb v katalógu služieb CERT-EU vedúci CERT-EU zohľadní zdroje pridelené CERT-EU.

5. Vedúci CERT-EU aspoň raz ročne predkladá IICB a predsedovi IICB správy o činnostiach a výkonnosti CERT-EU počas referenčného obdobia, a to aj o plnení rozpočtu, dohodách o úrovni poskytovaných služieb a uzatvorených písomných dohodách, spolupráci s náprotivkami a partnermi, ako aj o služobných cestách zamestnancov, vrátane správ uvedených v článku 11. Uvedené správy zahŕňajú pracovný program na nasledujúce obdobie, finančný plán príjmov a výdavkov vrátane plánu počtu zamestnancov, plánované aktualizácie katalógu služieb CERT-EU a posúdenie očakávaného vplyvu, ktorý takéto aktualizácie môžu mať na finančné a ľudské zdroje.

Článok 16

Finančné a personálne záležitosti

1. CERT-EU sa začlení do administratívnej štruktúry generálneho riaditeľstva Komisie, aby mohol využívať administratívnu podpornú štruktúru a podpornú štruktúru finančného riadenia a účtovníctva Komisie a zároveň si zachovať svoje postavenie nezávislého medziinštitucionálneho poskytovateľa služieb pre všetky subjekty Únie. Komisia informuje IICB o administratívnom umiestnení CERT-EU a o všetkých jeho následných zmenách. Komisia pravidelne a v každom prípade pred vytvorením akéhokoľvek viacročného finančného rámca podľa článku 312 ZFEÚ preskúma správne dojednania týkajúce sa CERT-EU, aby bolo možné prijať vhodné opatrenia. Preskúmanie zahŕňa možnosť zriadiť CERT-EU ako úrad Únie.

2. Pri uplatňovaní administratívnych a finančných postupov koná vedúci CERT-EU pod vedením Komisie a pod dohľadom IICB.

([9]) 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).

3. Úlohy a činnosti CERT-EU vrátane služieb, ktoré CERT-EU poskytuje podľa článku 13 ods. 3, 4, 5 a 7 a článku 14 ods. 1 subjektom Únie financovaným v rámci okruhu viacročného finančného rámca určeného pre európsku verejnú administratívu, sa financujú zo samostatného rozpočtového riadku v rozpočte Komisie. Pracovné miesta vyčlenené pre CERT-EU sa detailne uvádzajú v poznámke pod čiarou plánu pracovných miest Komisie.

4. Iné subjekty Únie než subjekty uvedené v odseku 3 tohto článku poskytujú CERT-EU ročný finančný príspevok na úhradu služieb, ktoré CERT-EU poskytuje podľa daného odseku. Príspevky vychádzajú z usmernení IICB a každý subjekt Únie si ich dohodne s CERT-EU v dohodách o úrovni poskytovaných služieb. Príspevky predstavujú spravodlivý a primeraný podiel z celkových nákladov na poskytnuté služby. Započítajú sa do samostatného rozpočtového riadka uvedeného v odseku 3 tohto článku ako vnútorné pripísané príjmy, ako sa stanovuje v článku 21 ods. 3 písm. c) nariadenia (EÚ, Euratom) 2018/1046.

5. Náklady na služby vymedzené v článku 13 ods. 6 uhrádzajú subjekty Únie, ktorým CERT-EU poskytol služby. Príjmy sa pripíšu do rozpočtových riadkov na podporu nákladov.

Článok 17

Spolupráca CERT-EU s náprotivkami v členskom štáte

1. CERT-EU bezodkladne spolupracuje a vymieňa si informácie s náprotivkami v členskom štáte, najmä s jednotkami CSIRT určenými alebo zriadenými podľa článku 10 smernice (EÚ) 2022/2555 alebo v náležitých prípadoch s príslušnými orgánmi a jednotnými kontaktnými miestami určenými alebo zriadenými podľa článku 8 danej smernice, v súvislosti s incidentmi, kybernetickými hrozbami, zraniteľnosťami, udalosťami odvrátenými v poslednej chvíli, možnými protiopatreniami, ako aj v súvislosti s najlepšími postupmi a o všetkých otázkach relevantných pre zlepšenie ochrany prostredí IKT subjektov Únie, a to aj prostredníctvom siete jednotiek CSIRT zriadenej podľa článku 15 smernice (EÚ) 2022/2555. CERT-EU podporuje Komisiu v sieti EU-CyCLONe zriadenej podľa článku 16 smernice (EÚ) 2022/2555 o koordinovanom riadení rozsiahlych kybernetických incidentov a kríz.

2. Ak sa CERT-EU dozvie o významnom incidente, ku ktorému došlo na území členského štátu, bezodkladne informuje všetkých relevantných náprotivkov v tomto členskom štáte, v súlade s odsekom 1.

3. Za predpokladu, že osobné údaje sú chránené v súlade s príslušným právom Únie v oblasti ochrany údajov, si CERT-EU bez zbytočného odkladu vymieňa relevantné informácie o konkrétnom incidente s náprotivkami v členskom štáte s cieľom pomôcť odhaliť podobné kybernetické hrozby alebo incidenty alebo prispieť k analýze incidentu, a to bez povolenia zasiahnutého subjektu Únie. CERT-EU si vymieňa informácie o konkrétnom incidente, ktoré odhaľujú identitu cieľa incidentu len v prípade jednej z týchto možností:

a) zasiahnutý subjekt Únie súhlasí;

b) zasiahnutý subjekt Únie nesúhlasí, ako sa stanovuje v písmene a), ale zverejnením identity zasiahnutého subjektu Únie by sa zvýšila pravdepodobnosť, že sa zamedzí ďalším incidentom alebo sa zmiernia ich následky;

c) zasiahnutý subjekt Únie už zverejnil, že bol incidentom zasiahnutý.

Rozhodnutia o výmene informácií o konkrétnom incidente, ktoré odhaľujú totožnosť cieľa incidentu podľa prvého pododseku písm. b), schvaľuje vedúci CERT-EU. Pred vydaním takéhoto rozhodnutia sa CERT-EU písomne obráti na zasiahnutý subjekt Únie, pričom mu jasne vysvetlí, ako by zverejnenie jeho totožnosti pomohlo zamedziť ďalším incidentom alebo zmierniť ich následky. Vedúci CERT-EU poskytne vysvetlenie a výslovne požiada subjekt Únie, aby v stanovenej lehote uviedol, či súhlasí. Vedúci CERT-EU takisto informuje subjekt Únie o tom, že na základe poskytnutého vysvetlenia si vyhradzuje právo zverejniť dané informácie aj bez udelenia súhlasu. Zasiahnutý subjekt Únie musí byť informovaný pred tým, než sú informácie zverejnené.

Článok 18

Spolupráca CERT-EU s ostatnými náprotivkami

1. CERT-EU môže spolupracovať s inými náprotivkami v Únii, než sú tie, ktoré sú uvedené v článku 17 a na ktoré sa vzťahujú požiadavky Únie na kybernetickú bezpečnosť, vrátane náprotivkov z konkrétnych odvetví v oblasti nástrojov a metód, ako sú napríklad techniky, taktiky, postupy a najlepšie postupy, ako aj v oblasti kybernetických hrozieb a zraniteľností. Na každú spoluprácu s takýmito náprotivkami si CERT-EU v každom konkrétnom prípade vyžiada predchádzajúce povolenie IICB. Keď CERT-EU nadviaže spoluprácu s takýmito náprotivkami, informuje o tom všetky príslušné náprotivky v členskom štáte uvedené v článku 17 ods. 1 v členskom štáte, v ktorom sa náprotivok nachádza. V náležitých a vhodných prípadoch sa takáto spolupráca a jej podmienky, a to aj pokiaľ ide o kybernetickú bezpečnosť, ochranu údajov a zaobchádzanie s informáciami, stanovia v osobitných dohodách o zachovaní dôvernosti, ako sú napríklad zmluvy alebo správne dojednania. Dohody o zachovaní dôvernosti si nevyžadujú predchádzajúce povolenie zo strany IICB, ale predseda IICB o nich musí byť informovaný. V prípade naliehavej a bezprostrednej potreby výmeny informácií o kybernetickej bezpečnosti v záujme subjektov Únie alebo inej strany môže CERT-EU takúto výmenu urobiť so subjektom, ktorého osobitná spôsobilosť, kapacita a odborné znalosti sa oprávnene vyžadujú na pomoc s takouto naliehavou a bezprostrednou potrebou, a to aj v prípade, že CERT-EU nemá s daným subjektom uzavretú dohodu o zachovaní dôvernosti. V takýchto prípadoch CERT-EU bezodkladne informuje predsedu IICB a podáva IICB informácie prostredníctvom pravidelných správ alebo zasadnutí.

2. CERT-EU môže spolupracovať s partnermi, ako sú napríklad obchodné subjekty vrátane subjektov z konkrétnych odvetví, medzinárodné organizácie, vnútroštátne subjekty z tretích krajín alebo jednotliví odborníci, s cieľom zhromažďovať informácie o všeobecných a konkrétnych kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli, zraniteľnostiach a možných protiopatreniach. Na širšiu spoluprácu s týmito partnermi si CERT-EU v každom konkrétnom prípade vyžiada predchádzajúce povolenie IICB.

3. CERT-EU môže so súhlasom subjektu Únie zasiahnutého incidentom a pod podmienkou, že s relevantným náprotivkom alebo partnerom má uzavretú dohodu alebo zmluvu o nezverejňovaní informácií, poskytnúť informácie týkajúce sa konkrétneho incidentu náprotivkom alebo partnerom uvedeným v odsekoch 1 a 2 výlučne na účely príspevku k analýze incidentu.

KAPITOLA V

SPOLUPRÁCA A OZNAMOVACIE POVINNOSTI

Článok 19

Zaobchádzanie s informáciami

1. Subjekty Únie a CERT-EU rešpektujú povinnosť služobného tajomstva v súlade s článkom 339 ZFEÚ alebo s rovnocennými uplatniteľnými rámcami.

2. V súvislosti so žiadosťami o prístup verejnosti k dokumentom v držbe CERT-EU sa uplatňuje nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 ([10]) vrátane povinnosti podľa daného nariadenia poradiť sa s ďalšími subjektmi Únie alebo v relevantných prípadoch s členskými štátmi vždy, keď sa žiadosť týka ich dokumentov.

3. Zaobchádzanie s informáciami zo strany subjektov Únie a CERT-EU je v súlade s príslušnými pravidlami o informačnej bezpečnosti.

([10]) 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).

Článok 20

Dohody o zdieľaní informácií o kybernetickej bezpečnosti

1. Subjekty Únie môžu CERT-EU dobrovoľne oznamovať incidenty, kybernetické hrozby, udalosti odvrátené v poslednej chvíli a zraniteľnosti, ktoré majú na nich vplyv, a poskytovať o nich informácie. CERT-EU zabezpečuje, aby na účely umožnenia zdieľania informácií so subjektmi Únie boli k dispozícii účinné prostriedky komunikácie vyznačujúce sa vysokou úrovňou vysledovateľnosti, dôvernosti a spoľahlivosti. Pri spracúvaní oznámení môže CERT-EU uprednostniť spracovanie povinných oznámení pred dobrovoľnými oznámeniami. Bez toho, aby bol dotknutý článok 12, dobrovoľným oznámením nevznikajú oznamujúcemu subjektu Únie žiadne ďalšie povinnosti, ktoré by sa naň nevzťahovali, ak by oznámenie nepodal.

2. CERT-EU môže na účely vykonávania svojho poslania a úloh udelených podľa článku 13 požiadať subjekty Únie, aby mu poskytli informácie zo svojich príslušných inventárov systémov IKT vrátane informácií o kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli, zraniteľnostiach, ukazovateľoch narušenia, výstrahách a odporúčaniach týkajúcich sa konfigurácie nástrojov kybernetickej bezpečnosti na odhaľovanie incidentov. Dožiadaný subjekt Únie poskytne požadované informácie a všetky ich ďalšie aktualizácie bez zbytočného odkladu.

3. CERT-EU si môže so subjektmi Únie vymieňať informácie o konkrétnom incidente, ktorými sa odhaľuje identita subjektu Únie zasiahnutého incidentom pod podmienkou, že dotknutý subjekt Únie súhlasí. Ak subjekt Únie odmietne udeliť súhlas, poskytne CERT-EU dôvody tohto rozhodnutia.

4. Subjekty Únie na požiadanie zdieľajú s Európskym parlamentom a Radou informácie o dokončení plánov kybernetickej bezpečnosti.

5. IICB alebo CERT-EU na požiadanie zdieľa s Európskym parlamentom a Radou usmernenia, odporúčania a výzvy na činnosť.

6. Povinnosti v oblasti zdieľania informácií stanovené v tomto článku sa nevzťahujú na:

a) utajované skutočnosti EÚ;

b) informácie, ktorých ďalšie šírenie bolo vylúčené prostredníctvom viditeľného označenia, pokiaľ ich zdieľanie s CERT-EU nebolo výslovne povolené.

Článok 21

Oznamovacie povinnosti

1. Incident sa považuje za významný, ak:

a) spôsobil alebo môže spôsobiť vážne prevádzkové narušenie fungovania dotknutého subjektu Únie alebo finančnú stratu dotknutému subjektu Únie;

b) zasiahol alebo môže zasiahnuť iné fyzické alebo právnické osoby tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu.

2. Subjekty Únie podávajú CERT-EU:

a) bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia významného incidentu včasné varovanie, v ktorom v náležitých prípadoch uvedú, že významný incident pravdepodobne spôsobilo nezákonné konanie alebo konanie so zlým úmyslom, alebo že môže mať dosah na iný subjekt či cezhraničný dosah;

b) bez zbytočného odkladu a v každom prípade do 72 hodín po tom, ako sa dozvedeli o významnom incidente, oznámenie o incidente, ktorým v náležitých prípadoch aktualizujú informácie uvedené v písmene a) a uvedú prvotné posúdenie významného incidentu, vrátane jeho závažnosti a dosahu, ako aj v náležitých prípadoch ukazovatele narušenia;

c) na žiadosť CERT-EU priebežnú správu s relevantnou aktualizáciou daného stavu.

d) najneskôr jeden mesiac po podaní oznámenia o incidente podľa písmena b) záverečnú správu, ktorá obsahuje tieto informácie:

   i) podrobný opis incidentu vrátane jeho závažnosti a dosahu;

   ii) druh hrozby alebo hlavnú príčinu, ktorá pravdepodobne incident spôsobila;

   iii) zavedené a prebiehajúce zmierňujúce opatrenia;

   iv) v náležitých prípadoch cezhraničný dosah incidentu alebo jeho dosah na iný subjekt;

e) v prípade prebiehajúceho incidentu v čase podávania záverečnej správy uvedenej v písmene d), správu o pokroku v danom čase a záverečnú správu do jedného mesiaca po vyriešení incidentu.

3. Subjekt Únie bez zbytočného odkladu a v každom prípade do 24 hodín od zistenia významného incidentu informuje všetky príslušné náprotivky v členskom štáte uvedené v článku 17 ods. 1 v členskom štáte, v ktorom sa nachádza, o tom, že došlo k významnému incidentu.

4. Subjekty Únie oznamujú CERT-EU okrem iného všetky informácie, ktoré mu umožnia určiť akýkoľvek dosah na iný subjekt, dosah na hostiteľský členský štát alebo cezhraničný dosah po tom, čo došlo k významnému incidentu. Bez toho, aby bol dotknutý článok 12, samotný akt oznámenia nezakladá zvýšenú zodpovednosť subjektu Únie.

5. Subjekty Únie v náležitých prípadoch bez zbytočného odkladu informujú používateľov zasiahnutých sietí a informačných systémov alebo iných zložiek prostredia IKT, ktoré sú potenciálne zasiahnuté významným incidentom alebo významnou kybernetickou hrozbou a vo vhodných prípadoch si vyžadujú prijatie zmierňujúcich opatrení, o opatreniach alebo prostriedkoch nápravy, ktoré môžu prijať v reakcii na daný incident alebo danú hrozbu. Subjekty Únie vo vhodných prípadoch informujú týchto používateľov o samotnej významnej kybernetickej hrozbe.

6. Ak má významný incident alebo významná kybernetická hrozba vplyv na sieť a informačný systém alebo zložku prostredia IKT subjektu Únie, o ktorej je známe jej prepojenie s prostredím IKT iného subjektu Únie, CERT-EU vydá príslušnú výstrahu.

7. Subjekty Únie na žiadosť CERT-EU bez zbytočného odkladu poskytnú CERT-EU digitálne informácie vytvorené pomocou elektronických zariadení, ktorých sa príslušné incidenty týkali. CERT-EU môže poskytnúť ďalšie podrobnosti o type informácií, ktoré požaduje na účely situačnej informovanosti a reakcie na incident.

8. CERT-EU predkladá IICB, agentúre ENISA, centru EU INTCEN a sieti jednotiek CSIRT každé tri mesiace súhrnnú správu obsahujúcu anonymizované a súhrnné údaje o významných incidentoch, incidentoch, kybernetických hrozbách, udalostiach odvrátených v poslednej chvíli a zraniteľnostiach podľa článku 20 a významných incidentoch oznámených podľa odseku 2 tohto článku. Táto súhrnná správa sa použije ako zdroj informácií na vypracovanie správy o stave kybernetickej bezpečnosti v Únii prijímanej každé dva roky v súlade s článkom 18 smernice (EÚ) 2022/2555.

9. IICB do 8. júla 2024 vydá usmernenia alebo odporúčania, v ktorých bližšie určí spôsoby, formát a obsah oznamovania podľa tohto článku. Pri príprave takýchto usmernení alebo odporúčaní IICB zohľadní všetky vykonávacie akty prijaté podľa článku 23 ods. 11 smernice (EÚ) 2022/2555, v ktorých sa bližšie určuje druh informácií, formát a postup oznamovania. CERT-EU šíri náležité technické podrobnosti, aby subjektom Únie umožnil vykonať proaktívne odhaľovanie, reagovanie na incident alebo prijatie zmierňujúcich opatrení.

10. Oznamovacie povinnosti stanovené v tomto článku sa nevzťahujú na:

a) utajované skutočnosti EÚ;

b) informácie, ktorých ďalšie šírenie bolo vylúčené prostredníctvom viditeľného označenia, pokiaľ ich zdieľanie s CERT-EU nebolo výslovne povolené.

Článok 22

Koordinácia a spolupráca v rámci reakcie na incidenty

1. CERT-EU ako centrum na výmenu informácií a koordináciu reakcie na incidenty v oblasti kybernetickej bezpečnosti uľahčuje výmenu informácií o incidentoch, kybernetických hrozbách, zraniteľnostiach a udalostiach odvrátených v poslednej chvíli medzi:

a) subjektmi Únie;

b) náprotivkami uvedenými v článkoch 17 a 18.

2. CERT-EU, v relevantných prípadoch v úzkej spolupráci s agentúrou ENISA, uľahčuje koordináciu reakcií subjektov Únie na incidenty vrátane:

a) prispievania k sústavnej komunikácii navonok;

b) vzájomnej podpory, ako je napríklad zdieľanie relevantných informácií so subjektmi Únie, alebo v relevantných prípadoch poskytovania pomoci priamo na mieste;

c) optimálneho využívania operačných zdrojov;

d) koordinácie s inými mechanizmami reakcie na krízu na úrovni Únie.

3. CERT-EU v úzkej spolupráci s agentúrou ENISA podporuje subjekty Únie, pokiaľ ide o situačnú informovanosť o incidentoch, kybernetických hrozbách, zraniteľnostiach a udalostiach odvrátených v poslednej chvíli, ako aj zdieľanie informácií o relevantnom vývoji v oblasti kybernetickej bezpečnosti.

4. IICB do 8. januára 2025 na základe návrhu CERT-EU vydá usmernenia alebo odporúčania týkajúce sa koordinácie a spolupráce v rámci reakcie na incidenty v prípade významných incidentov. V prípade podozrenia na trestnoprávnu povahu incidentu, CERT-EU bez zbytočného odkladu poskytne rady o spôsoboch oznamovania incidentu orgánom presadzovania práva.

5. Na základe osobitnej žiadosti členského štátu a so súhlasom dotknutých subjektov Únie môže CERT-EU vyzvať odborníkov zo zoznamu uvedeného v článku 23 ods. 4, aby prispeli k reakcii na závažný incident, ktorý má dosah v danom členskom štáte, alebo na rozsiahly kybernetický incident v súlade s článkom 15 ods. 3 písm. g) smernice (EÚ) 2022/2555. IICB schváli na návrh CERT-EU osobitné pravidlá týkajúce sa prístupu k technickým odborníkom zo subjektov Únie a ich využívania.

Článok 23

Riadenie závažných incidentov

1. S cieľom podporiť koordinované riadenie závažných incidentov, ktoré majú vplyv na subjekty Únie, na operačnej úrovni a prispieť k pravidelnej výmene relevantných informácií medzi subjektmi Únie a s členskými štátmi vypracuje IICB podľa článku 11 písm. q) v úzkej spolupráci s CERT-EU a agentúrou ENISA plán riadenia kybernetických kríz založený na činnostiach uvedených v článku 22 ods. 2. Plán riadenia kybernetických kríz obsahuje aspoň tieto prvky:

a) postupy týkajúce sa koordinácie a toku informácií medzi subjektmi Únie na účely riadenia závažných incidentov na operačnej úrovni;

b) spoločné štandardné operačné postupy (SOPs);

c) spoločnú taxonómiu závažnosti závažných incidentov a spúšťacích bodov kríz;

d) pravidelné cvičenia;

e) bezpečné komunikačné kanály, ktoré sa majú používať.

2. Zástupca Komisie v IICB je v závislosti od plánu riadenia kybernetických kríz vypracovaného podľa odseku 1 tohto článku a bez toho, aby bol dotknutý článok 16 ods. 2 prvý pododsek smernice (EÚ) 2022/2555, kontaktnou osobou na zdieľanie relevantných informácií v súvislosti so závažnými incidentmi so sieťou EU-CyCLONe.

3. CERT-EU koordinuje riadenie závažných incidentov medzi subjektmi Únie. Vedie súpis dostupných odborných technických znalostí, ktoré by boli potrebné na reakciu na incident v prípade závažných incidentov, a pomáha IICB pri koordinácii plánov riadenia kybernetických kríz subjektov Únie pre prípad závažných incidentov uvedených v článku 9 ods. 2.

4. Subjekty Únie prispievajú do súpisu odborných technických znalostí poskytovaním každoročne aktualizovaného zoznamu odborníkov dostupných v jednotlivých organizáciách s podrobným opisom ich konkrétnych technických zručností.

KAPITOLA VI

ZÁVEREČNÉ USTANOVENIA

Článok 24

Počiatočné prerozdelenie rozpočtových prostriedkov

S cieľom zabezpečiť riadne a stabilné fungovanie CERT-EU môže Komisia navrhnúť prerozdelenie zamestnancov a finančných zdrojov do rozpočtu Komisie na použitie na činnosti CERT-EU. Prerozdelenie nadobudne účinnosť súčasne s prvým ročným rozpočtom Únie prijatým po nadobudnutí účinnosti tohto nariadenia.

Článok 25

Preskúmanie

1. IICB s pomocou CERT-EU do 8. januára 2025 a potom každoročne predloží Komisii správu o vykonávaní tohto nariadenia. IICB môže Komisii takisto odporučiť, aby toto nariadenie preskúmala.

2. Komisia do 8. januára 2027 a potom každé dva roky posúdi vykonávanie tohto nariadenia a predloží Európskemu parlamentu a Rade správu o jeho vykonávaní a o skúsenostiach získaných na strategickej a operačnej úrovni.

Správa uvedená v prvom pododseku tohto odseku obsahuje preskúmanie uvedené v článku 16 ods. 1 týkajúce sa možnosti zriadiť CERT-EU ako úrad Únie.

3. Komisia do 8. januára 2029 vyhodnotí fungovanie tohto nariadenia a predloží správu Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov. Komisia tiež vyhodnotí vhodnosť zahrnúť siete a informačné systémy, v ktorých sa zaobchádza s utajovanými skutočnosťami EÚ, do rozsahu pôsobnosti tohto nariadenia, pričom zohľadní iné legislatívne akty Únie uplatniteľné na tieto systémy. K správe sa v prípade potreby pripojí legislatívny návrh.

Článok 26

Nadobudnutie účinnosti

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

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

V Štrasburgu 13. decembra 2023

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda*
R. METSOLA	P. NAVARRO RÍOS