Rada
Evropské unie

Brusel 17. prosince 2020
(OR. en)

14150/20

Interinstitucionální spis:
2020/0359(COD)

CYBER 281
JAI 1119
DATAPROTECT 155
TELECOM 270
MI 581
CSC 368
CSCI 97

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	16. prosince 2020
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	COM(2020) 823 final
Předmět:	Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

Delegace naleznou v příloze dokument COM(2020) 823 final.

Příloha: COM(2020) 823 final

EVROPSKÁ
KOMISE

V Bruselu dne 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

(Text s významem pro EHP)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Tento návrh je součástí balíčku opatření, jež mají dále zlepšit odolnost veřejných a soukromých subjektů, příslušných orgánů a Unie jako celku v oblasti kybernetické bezpečnosti a ochrany kritické infrastruktury a jejich schopnost reagovat na bezpečnostní incidenty. Je v souladu s prioritami Evropské komise připravit Evropu na digitální věk a vybudovat hospodářství připravené na budoucnost, které bude pracovat pro lidi. Kybernetická bezpečnost je jednou z priorit Komise v rámci reakce na krizi COVID-19. Balíček zahrnuje novou strategii kybernetické bezpečnosti zaměřenou na posílení strategické autonomie Unie s cílem zlepšit její odolnost a kolektivní reakci a vytvářet otevřený a globální internet. Balíček rovněž obsahuje návrh směrnice o odolnosti klíčových provozovatelů základních služeb, což má za cíl snížit fyzické hrozby vůči nim.

Tento návrh navazuje na směrnici (EU) 2016/1148 o bezpečnosti sítí a informačních systémů (dále jen „směrnice o bezpečnosti sítí a informací“), která je prvním právním předpisem týkajícím se kybernetické bezpečnosti pro celou EU a poskytuje právní opatření k posílení celkové kybernetické bezpečnosti v Unii, a uvedenou směrnici ruší. Směrnice o bezpečnosti sítí a informací 1) přispěla ke zlepšení schopností v oblasti kybernetické bezpečnosti na úrovni členských států, neboť vyžadovala, aby členské státy přijaly národní strategie kybernetické bezpečnosti a určily orgány pro kybernetickou bezpečnost; 2) zvýšila spolupráci členských států na úrovni Unie zřízením různých fór usnadňujících výměnu strategických a operačních informací a 3) zlepšila kybernetickou odolnost veřejných a soukromých subjektů v sedmi konkrétních odvětvích (energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, dodávky a rozvody pitné vody a digitální infrastruktura) a ve třech oblastech digitálních služeb (on-line tržiště, internetové vyhledávače a služby cloud computingu) tím, že požadovala, aby členské státy zajistily, že provozovatelé základních služeb a poskytovatelé digitálních služeb zavedou požadavky kybernetické bezpečnosti a budou hlásit incidenty.

Návrh modernizuje stávající právní rámec a přitom zohledňuje zvýšenou digitalizaci vnitřního trhu v posledních letech a vyvíjející se prostředí kybernetických bezpečnostních hrozeb. Oba tyto vývojové trendy od vypuknutí krize COVID-19 dále zesílily. Návrh rovněž řeší některá slabá místa, jež bránila rozvinutí celého potenciálu směrnice o bezpečnosti sítí a informací.

I přes významné úspěchy směrnice o bezpečnosti sítí a informací, která připravila půdu pro významnou změnu v myšlení, pokud jde o institucionální a regulatorní přístup ke kybernetické bezpečnosti v mnoha členských státech, se projevila i její omezení. Digitální transformace společnosti (která se v důsledku krize COVID-19 ještě více zintenzivnila) rozšířila prostředí hrozeb a přináší nové výzvy, jež vyžadují přizpůsobené a inovativní reakce. Počet kybernetických útoků nadále roste a stále sofistikovanější útoky vycházejí z celé řady zdrojů v EU i mimo ni.

Hodnocení fungování směrnice o bezpečnosti sítí a informací, provedené pro účely posouzení dopadů, poukázalo na tyto problémy: 1) nízká úroveň kybernetické odolnosti podniků v EU; 2) nestejná odolnost členských států a odvětví a 3) nízká úroveň společného situačního povědomí a nedostatečná společná reakce na krize. Například některé velké nemocnice v jednom členském státě nespadají do oblasti působnosti směrnice o bezpečnosti sítí a informací, a nejsou tedy povinny provádět z ní vyplývající bezpečnostní opatření, zatímco v jiném členském státě se bezpečnostní požadavky směrnice vztahují téměř na každého poskytovatele zdravotní péče v zemi.

Vzhledem k tomu, že se jedná o iniciativu v rámci Programu pro účelnost a účinnost právních předpisů (REFIT), je cílem tohoto návrhu snížit regulační zátěž pro příslušné orgány a náklady na dodržování předpisů pro veřejné a soukromé subjekty. Zejména je pak třeba zdůraznit, že je toho dosahováno zrušením povinnosti příslušných orgánů určit provozovatele základních služeb a zvýšením úrovně harmonizace bezpečnostních požadavků a požadavků na hlášení s cílem usnadnit subjektům poskytujícím přeshraniční služby dodržování právních předpisů. Zároveň budou příslušným orgánům uloženy nové úkoly, včetně dohledu nad subjekty v odvětvích, na která se směrnice o bezpečnosti sítí a informací dosud nevztahovala.

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

Tento návrh je součástí širšího souboru stávajících právních předpisů a připravovaných iniciativ na úrovni Unie, jehož cílem je zvyšování odolnosti veřejných a soukromých subjektů vůči hrozbám.

V oblasti kybernetické bezpečnosti jsou to zejména směrnice (EU) 2018/1972, kterou se stanoví evropský kodex pro elektronické komunikace (jejíž ustanovení týkající se kybernetické bezpečnosti budou nahrazena ustanoveními tohoto návrhu) a návrh nařízení o digitální provozní odolnosti finančního sektoru (COM(2020) 595 final), jež bude považováno za *lex specialis* k tomuto návrhu, jakmile oba akty vstoupí v platnost.

V oblasti fyzické bezpečnosti tento návrh doplňuje návrh směrnice o odolnosti klíčových subjektů, který reviduje směrnici 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (dále jen „směrnice o evropských kritických infrastrukturách“), která zavádí postup Unie pro určování a označování evropských kritických infrastruktur a stanoví přístup ke zlepšení jejich ochrany. V červenci 2020 přijala Komise strategii bezpečnostní unie EU[1], která uznala rostoucí vzájemnou provázanost a vzájemnou závislost fyzické a digitální infrastruktury. Zdůraznila potřebu soudržnějšího a jednotnějšího přístupu mezi směrnicí o evropských kritických infrastrukturách a směrnicí (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Tento návrh proto úzce souvisí s návrhem směrnice o odolnosti klíčových subjektů, jejímž cílem je posílení odolnosti klíčových subjektů vůči fyzickým hrozbám ve velkém počtu odvětví. Tento návrh má zajistit, aby příslušné orgány podle obou právních aktů přijímaly vzájemně se doplňující opatření a podle potřeby si vyměňovaly informace týkající se kybernetické i nekybernetické odolnosti a aby zejména klíčoví provozovatelé v odvětvích, která jsou podle tohoto návrhu považována za „základní“, podléhali také obecnějším povinnostem zaměřeným na posilování odolnosti s důrazem na nekybernetická rizika.

- **Soulad s ostatními politikami Unie**

Jak se uvádí ve sdělení „Formování digitální budoucnosti Evropy“[2], pro Evropu je důležité, aby těžila ze všech výhod digitálního věku a posilovala svůj průmysl a inovační kapacitu v bezpečných a etických mezích. Evropská strategie pro data stanoví čtyři pilíře – ochranu údajů, základní práva, bezpečnost a kybernetickou bezpečnost – jako nezbytné předpoklady pro posílení společnosti díky využívání údajů.

---

[1] COM(2020) 605 final.
[2] COM(2020) 67 final.

Evropský parlament v usnesení ze dne 12. března 2019 vyzval „*[...] Komisi, aby posoudila, zda je nutné rozšířit působnost směrnice o bezpečnosti sítí a informací na další klíčové sektory a služby, které nejsou pokryty odvětvovými právními předpisy*“[3]. Rada ve svých závěrech ze dne 9. června 2020 uvítala „*[...] plány Komise na zajištění soudržných pravidel pro účastníky na trhu a k usnadnění bezpečného, spolehlivého a odpovídajícího sdílení informací o hrozbách i incidentech, mimo jiné prostřednictvím přezkumu směrnice o bezpečnosti sítě a informačních systémů (směrnice o bezpečnosti sítí a informací), s cílem usilovat o lepší kybernetickou odolnost a účinnější reakce na kybernetické útoky, zejména pokud jde o základní hospodářské a společenské činnosti, a to při respektování pravomocí členských států, včetně odpovědnosti za jejich národní bezpečnost.*“[4] Navrhovaným legislativním aktem dále není dotčeno uplatňování pravidel hospodářské soutěže stanovených ve Smlouvě o fungování Evropské unie (dále jen „SFEU“).

Vzhledem k tomu, že značná část kybernetických bezpečnostních hrozeb má původ mimo EU, je nutný soudržný přístup k mezinárodní spolupráci. Směrnice musí představovat referenční model, který je třeba prosazovat v rámci spolupráce EU se třetími zeměmi, a to zejména při poskytování vnější technické pomoci.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- **Právní základ**

Právní základ směrnice o bezpečnosti sítí a informací tvoří článek 114 Smlouvy o fungování Evropské unie, jehož cílem je vytvoření a fungování vnitřního trhu posílením opatření ke sbližování vnitrostátních předpisů. Jak rozhodl Soudní dvůr Evropské unie v rozsudku ve věci C-58/08 Vodafone a další, lze článek 114 SFEU využít zejména v případě rozdílů mezi vnitrostátními právními úpravami, které mohou mít přímý dopad na fungování vnitřního trhu. Stejně tak Soudní dvůr rozhodl, že jestliže akt založený na článku 114 SFEU již odstranil všechny překážky obchodu v oblasti, kterou harmonizuje, nemůže být zákonodárce Společenství zbaven možnosti přizpůsobit tento akt jakékoli změně okolností nebo jakémukoli vývoji znalostí s ohledem na úkol, který mu náleží, a to dbát na ochranu obecných zájmů uznaných ve Smlouvě. Dále pak Soudní dvůr rozhodl, že opatření ke sbližování uvedená v článku 114 SFEU mají v závislosti na obecném kontextu a zvláštních okolnostech harmonizované oblasti poskytnout určitý prostor pro uvážení, pokud jde o techniku sbližování, která je nejvhodnější pro dosažení požadovaného výsledku. Navrhovaný právní akt by odstranil překážky a zlepšil vytváření a fungování vnitřního trhu pro zásadní a důležité subjekty tím, že stanoví jasná, obecně použitelná pravidla o oblasti působnosti směrnice o bezpečnosti sítí a informací, která harmonizují pravidla platná v oblasti řízení kybernetických bezpečnostních rizik a hlášení incidentů. Rozdíly, které v této oblasti v současnosti existují jak na úrovni legislativně právní, tak na úrovni dohledu, představují překážky pro vnitřní trh, protože subjekty zapojené do přeshraničních činností narážejí na rozdílné, a možná překrývající se regulační požadavky a/nebo jejich uplatňování, a to na úkor jejich svobody usazování a poskytování služeb. Rozdílná pravidla mají také negativní dopad na podmínky hospodářské soutěže na vnitřním trhu, pokud jde o subjekty stejného druhu v různých členských státech.

[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_CS.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/cs/pdf

- **Subsidiarita (v případě nevýlučné pravomoci)**

Odolnost z hlediska kybernetické bezpečnosti v celé Unii nemůže být účinná, pokud by se k ní přistupovalo rozdílným způsobem prostřednictvím vnitrostátních nebo regionálních sil. Směrnice o bezpečnosti sítí a informací tento nedostatek částečně řešila zřízením rámce pro bezpečnost sítí a informačních systémů na úrovni členských států a Unie. Její provedení do vnitrostátního práva a provádění však odhalilo také přirozené nedostatky a limity některých ustanovení nebo přístupů, jako např. nejasné vymezení oblasti působnosti směrnice, jež vedlo ke značným rozdílům v rozsahu a hloubce faktických intervencí EU na úrovni členských států. Od vypuknutí krize COVID-19 navíc evropské hospodářství více než kdykoli předtím závisí na sítích a informačních systémech a provázanost odvětví a služeb je stále větší. To, že intervence EU přesahují rámec stávajících opatření podle směrnice o bezpečnosti sítí a informací, je odůvodněno hlavně: i) stále více přeshraniční povahou hrozeb a výzev souvisejících s bezpečností sítí a informací; ii) potenciálem opatření EU zlepšovat a usnadňovat účinné a koordinované vnitrostátní politiky; a iii) přínosem sladěných politických opatření a spolupráce k účinné ochraně údajů a soukromí.

- **Proporcionalita**

Pravidla navrhovaná v této směrnici nepřekračují rámec toho, co je nezbytné pro uspokojivé dosažení specifických cílů. Předpokládané sladění a zefektivnění bezpečnostních opatření a povinností hlášení souvisejí s požadavky členských států a podniků na zlepšení stávajícího rámce.

Návrh zohledňuje již existující postupy v členských státech. Zvýšená úroveň ochrany dosažená prostřednictvím takových efektivnějších a koordinovaných požadavků je přiměřená stále větším rizikům, kterým je třeba čelit, včetně rizik představujících přeshraniční prvek. Tyto požadavky jsou přiměřené a odpovídají zájmům subjektů usilujících o zajištění kontinuity a kvality svých služeb. Náklady na zajištění systematické spolupráce členských států by byly malé v porovnání s hospodářskými a společenskými ztrátami a škodami způsobenými kybernetickými bezpečnostními incidenty. Konzultace se zúčastněnými stranami provedené v souvislosti s přezkumem směrnice o bezpečnosti sítí a informací, včetně výsledků otevřené veřejné konzultace a cílených průzkumů, kromě toho potvrzují podporu pro revizi směrnice o bezpečnosti sítí a informací ve výše uvedených směrech.

- **Volba nástroje**

Návrh dále zjednoduší povinnosti podniků a zajistí vyšší úroveň jejich harmonizace. Zároveň je cílem návrhu poskytnout členským státům pružnost, kterou potřebují, aby mohly zohlednit vnitrostátní specifika (jako např. možnost určit další základní nebo důležité subjekty, které překračují základní linii stanovenou právním aktem). Budoucím právním nástrojem by proto měla být směrnice, neboť tento právní nástroj umožňuje cílenou lepší harmonizaci i určitý stupeň pružnosti pro příslušné orgány.

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

- **Hodnocení *ex-post* / kontroly účelnosti platných právních předpisů**

Komise vyhodnotila fungování směrnice o bezpečnosti sítí a informací[5]. Analyzovala relevantnost, přidanou hodnotu EU, soudržnost, účinnost a účelnost. Analýza dospěla k těmto hlavním zjištěním:

- Oblast působnosti směrnice o bezpečnosti sítí a informací je, pokud jde o odvětví, jež pokrývá, příliš omezená, zejména v důsledku: i) zvýšené digitalizace v posledních letech a vyššího stupně vzájemné propojenosti, ii) toho, že oblast působnosti směrnice o bezpečnosti sítí a informací již neodráží všechna digitalizovaná odvětví, jež poskytují klíčové služby hospodářství a společnosti jako celku.
- Směrnice o bezpečnosti sítí a informací není dostatečně jasná co do rozsahu provozovatelů základních služeb, na něž se vztahuje, a její ustanovení dostatečně jasně nevymezují pravomoci členských států vůči poskytovatelům digitálních služeb. To vedlo k situaci, kdy některé druhy subjektů nebyly určeny ve všech členských státech, a proto nebyly povinny zavádět bezpečností opatření a hlásit incidenty.
- Směrnice o bezpečnosti sítí a informací poskytovala členským státům velký prostor pro uvážení při stanovení požadavků v oblasti bezpečnosti a hlášení incidentů pro provozovatele základních služeb. Z hodnocení vyplývá, že v některých případech členské státy prováděly tyto požadavky značně různými způsoby, což vytvářelo další zátěž pro společnosti působící ve více než jednom členském státě.
- Režim dohledu a vymáhání směrnice o bezpečnosti sítí a informací není účinný. Například se členské státy stavěly velmi odmítavě k ukládání sankcí subjektům, které nezavedly bezpečnostní požadavky nebo nehlásily incidenty. To může mít negativní důsledky pro kybernetickou odolnost jednotlivých subjektů.
- Finanční a lidské zdroje, které členské státy vyčlenily pro splnění svých úkolů (jako je určování provozovatelů základních služeb nebo dohled nad nimi), a tedy i jednotlivé úrovně vyspělosti při řešení kybernetických bezpečnostních rizik se velmi liší. To rozdíly v kybernetické odolnosti členských států dále prohlubuje.
- Členské státy navzájem systematicky nesdílejí informace, což má negativní důsledky zejména pro účinnost opatření v oblasti kybernetické bezpečnosti a úroveň společného situačního povědomí na úrovni EU. Stejně je tomu v případě sdílení informací mezi soukromými subjekty a součinnosti struktur pro spolupráci na úrovni EU a soukromých subjektů.

- **Konzultace se zúčastněnými stranami**

Komise konzultovala širokou škálu zúčastněných stran. Členské státy a zúčastněné strany byly vyzvány k účasti na otevřené veřejné konzultaci a průzkumech a workshopech, jež organizovaly společnosti Wavestone, CEPS a ICF, které Komise najala k provedení podpůrné studie k přezkumu směrnice o bezpečnosti sítí a informací. Konzultované zúčastněné strany zahrnovaly příslušné orgány, instituce Unie zabývající se kybernetickou bezpečností, provozovatele základních služeb, poskytovatele digitálních služeb, subjekty poskytující služby mimo oblast působnosti stávající směrnice o bezpečnosti sítí a informací, obchodní sdružení, spotřebitelské organizace a občany.

---

[5] [Příloha 5 posouzení dopadů].

Komise byla kromě toho ve stálém kontaktu s příslušnými orgány odpovědnými za provádění směrnice o bezpečnosti sítí a informací. Skupina pro spolupráci se obsáhle zabývala různými průřezovými a odvětvovými prvky provádění. Během svých návštěv v jednotlivých zemích v souvislosti s bezpečností sítí a informací v letech 2019 a 2020 pak Komise provedla pohovory se 154 veřejnými a soukromými subjekty a se 117 příslušnými orgány.

- **Sběr a využití výsledků odborných konzultací**

Komise uzavřela smlouvu s konsorciem společností Wavestone, CEPS a ICF, aby ji podpořilo při přezkumu směrnice o bezpečnosti sítí a informací[6]. Smluvní partner oslovil nejen zúčastněné strany, kterých se směrnice o bezpečnosti sítí a informací přímo dotýká, prostřednictvím cílených průzkumů a workshopů, ale vedl rovněž konzultace s celou řadou odborníků na kybernetickou bezpečnost, jako jsou výzkumní pracovníci v oboru kybernetické bezpečnosti a profesionálové v odvětví kybernetické bezpečnosti.

- **Posouzení dopadů**

K tomuto návrhu je přiloženo posouzení dopadů[7], které bylo dne 23. října 2020 předloženo Výboru pro kontrolu regulace a dne 20. listopadu 2020 obdrželo od tohoto výboru kladné stanovisko. Výbor doporučil vylepšení v některých oblastech, a sice: 1) v analýze problému lépe zohlednit úlohu přeshraničního přesahu; 2) lépe vysvětlit, jak by úspěch této iniciativy vypadal; 3) podrobněji odůvodnit seznam možností politiky; 4) podrobněji rozvést náklady spojené s navrhovaným opatřením. Posouzení dopadů bylo v souladu s těmito body i podrobnějšími připomínkami Výboru upraveno. Nyní obsahuje podrobnější vysvětlení úlohy přeshraničních přesahů v oblasti kybernetické bezpečnosti, jasnější přehled toho, jak lze měřit úspěch, podrobnější vysvětlení koncepce a logiky, z níž vycházejí jednotlivé možnosti politiky a opatření zvažovaná v rámci těchto možností, podrobnější vysvětlení aspektů analyzovaných v souvislosti s odvětvovou oblastí působnosti směrnice o bezpečnosti sítí a informací a další objasnění týkající se nákladů.

Komise posoudila několik možností politiky zaměřených na zlepšení právního rámce v oblasti kybernetické odolnosti a reakce na incidenty:

- „Nedělat nic“: Směrnice o bezpečnosti sítí a informací by zůstala beze změny a nebyla by přijata ani žádná jiná opatření nelegislativní povahy s cílem řešit problémy zjištěné při hodnocení směrnice o bezpečnosti sítí a informací.
- Možnost 1: Nedošlo by k žádným změnám na úrovni legislativy. Komise by místo toho po konzultaci se skupinou pro spolupráci, s Agenturou EU pro kybernetickou bezpečnost (ENISA) a případně se sítí bezpečnostních týmů typu CSIRT („týmů CSIRT“) vydala doporučení a pokyny (např. týkající se určování provozovatelů základních služeb, bezpečnostních požadavků, postupů pro hlášení incidentů a dohledu).
- Možnost 2: Tato možnost zahrnuje cílené změny směrnice o bezpečnosti sítí a informací včetně rozšíření její oblasti působnosti a některých dalších změn, jejichž cílem by bylo zajištění některých okamžitých řešení zjištěných problémů, zajištění větší jasnosti a další harmonizace (např. ustanovení s cílem harmonizovat hranice pro

[6] Studie na podporu přezkumu směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice o bezpečnosti sítí a informací) – č. 2020-665. Wavestone, CEPS a ICF.

[7] **[Doplní se odkazy na konečný dokument a souhrnný přehled.]**

určování provozovatelů). Hlavní stavební prvky, přístup a odůvodnění změněné směrnice o bezpečnosti sítí a informací by však byly zachovány.

- Možnost 3: Tento scénář obsahuje systémové a strukturální změny směrnice o bezpečnosti sítí a informací (prostřednictvím nové směrnice), které předpokládají zásadnější změnu přístupu tak, aby směrnice pokrývala širší segment ekonomik v celé Unii, avšak s cílenějším dohledem zaměřeným na velké a klíčové aktéry. Zjednodušil by rovněž povinnosti podniků a zajistil by vyšší úroveň jejich harmonizace, přinesl by účinnější nastavení operačních prvků a stanovil by také jasný základ pro větší sdílení povinností a odpovědnosti různých zúčastněných stran, pokud jde o opatření v oblasti kybernetické bezpečnosti.

Posouzení dopadů dochází k závěru, že upřednostňovanou možností je možnost 3 (tj. systémové a strukturální změny rámce pro bezpečnost sítí a informací). Pokud jde o účinnost, upřednostňovaná možnost by jasně vymezila oblast působnosti směrnice o bezpečnosti sítí a informací, rozšířenou na reprezentativnější část ekonomik a společností EU, a zjednodušila požadavky, spolu s přesněji definovaným rámcem pro dohled a vymáhání zaměřeným na zvýšení úrovně dodržování právních předpisů. Obsahuje také opatření zaměřená na zlepšení přístupů k tvorbě politik na úrovni členských států a na změnu jejich paradigmatu, podporu nových rámců pro řízení rizik v oblasti dodavatelských vztahů a koordinované odhalování zranitelných míst. Upřednostňovaná možnost politiky zároveň stanoví jasný základ pro sdílení povinností a odpovědnosti a předpokládá mechanismy zaměřené na podporu větší důvěry mezi členskými státy (jak orgánů, tak průmyslu), motivaci ke sdílení informací a zajištění operativnějšího přístupu, jako je vzájemná pomoc a mechanismy vzájemného hodnocení. Tato možnost by také stanovila rámec EU pro krizové řízení v návaznosti na nedávno zřízenou operační síť EU a zajistila by větší zapojení agentury ENISA v rámci jejího stávajícího mandátu při udržování přesného přehledu o stavu kybernetické bezpečnosti v Unii.

Pokud jde o efektivitu, upřednostňovaná možnost by zahrnovala další náklady na dodržování a vymáhání předpisů pro podniky a členské státy, avšak vedla by také k účinným kompromisům a součinnosti, přičemž by mohla ze všech analyzovaných možností politiky nejlépe zajistit zvýšenou a konzistentní úroveň kybernetické odolnosti klíčových subjektů v celé Unii, která by nakonec vedla k úsporám nákladů pro podniky i společnost. Tato možnost politiky by vedla k určité další správní zátěži a nákladům na dodržování předpisů pro orgány členských států. Ve střednědobé a dlouhodobé perspektivě by však celkově znamenala podstatný přínos prostřednictvím zvýšení spolupráce členských států, a to i na operativní úrovni, a podnět k celkovému zvýšení schopností v oblasti kybernetické bezpečnosti na vnitrostátní a regionální úrovni prostřednictvím vzájemné pomoci, mechanismů vzájemného hodnocení a lepšího přehledu o klíčových podnicích a interakcí mezi těmito podniky. Upřednostňovaná možnost politiky by také ve značné míře zajistila soudržnost s jinými právními předpisy, iniciativami nebo politickými opatřeními, včetně *lex specialis* specifického pro jednotlivá odvětví.

Řešení v současnosti přetrvávající nedostatečné připravenosti v oblasti kybernetické bezpečnosti na úrovni členských států a na úrovni společností a jiných organizací by mohlo vést ke zvýšení účinnosti a snížení dalších nákladů vyplývajících z kybernetických bezpečnostních incidentů.

- Z hlediska základních a důležitých subjektů by zvýšení úrovně připravenosti v oblasti kybernetické bezpečnosti mohlo vést ke snížení potenciální ztráty příjmů v důsledku narušení hospodářské soutěže – včetně průmyslové špionáže – a mohlo by snížit velké výdaje na *ad hoc* zmírňování hrozeb. Tyto přínosy budou

pravděpodobně převažovat nad nezbytnými investičními náklady. Zmírnění roztříštěnosti vnitřního trhu by také pomohlo vyrovnat podmínky tržních subjektů.

- Z hlediska členských států by mohlo dále snížit riziko narůstajících rozpočtových výdajů na *ad hoc* zmírňování rizik a dalších nákladů v případě mimořádných situací souvisejících s kybernetickými bezpečnostními incidenty.
- Z hlediska občanů se očekává, že řešení kybernetických bezpečnostních incidentů povede ke snížení ztráty příjmů v důsledku narušení hospodářské soutěže.

Zvýšení úrovně kybernetické bezpečnosti v členských státech a schopnosti společností a orgánů rychle reagovat na incident a zmírnit jeho dopad s největší pravděpodobností povede ke zvýšení celkové důvěry občanů v digitální ekonomiku, což by mohlo mít pozitivní dopad na růst a investice.

Zvyšování celkové úrovně kybernetické bezpečnosti pravděpodobně povede k větší celkové bezpečnosti a hladkému a nerušenému fungování základních služeb, které mají pro společnost kritický význam. Tato iniciativa též může přispět k dalším sociálním dopadům, jako je snížení úrovně kybernetické kriminality a terorismu a zvýšení civilní ochrany. Zvyšování úrovně kybernetické připravenosti podniků a jiných organizací může zabránit potenciálním finančním ztrátám v důsledku kybernetických útoků, a předejít tak potřebě propouštění zaměstnanců.

Zvyšování celkové úrovně kybernetické bezpečnosti by rovněž mohlo vést k prevenci environmentálních rizik/škod v případě útoku na základní služby. To by mohlo obzvláště platit pro odvětví energetiky, dodávek a rozvodů vody nebo dopravy. Posilováním schopností v oblasti kybernetické bezpečnosti by tato iniciativa mohla vést k lepšímu využívání infrastruktury a služeb IKT nejnovější generace, které jsou udržitelnější i z hlediska životního prostředí, a k nahrazení starší neefektivní a méně bezpečné infrastruktury. To by rovněž mělo přispět ke snížení počtu nákladných kybernetických incidentů, a tím i k uvolnění zdrojů, které budou k dispozici na udržitelné investice.

- **Účelnost právních předpisů a zjednodušení**

Návrh předpokládá všeobecné vyloučení mikrosubjektů a malých subjektů z oblasti působnosti bezpečnosti sítí a informací a mírnější režim dohledu *ex post* uplatňovaný vůči velkému počtu nových subjektů v rámci revidované oblasti působnosti (takzvané důležité subjekty). Cílem těchto opatření je minimalizovat a vyvážit zátěž kladenou na společnosti a orgány veřejné správy. Návrh dále nahrazuje složitý systém určování provozovatelů základních služeb obecně platnou povinností a zavádí vyšší úroveň harmonizace povinností v oblasti bezpečnosti a hlášení, což by snížilo zátěž spojenou s dodržováním předpisů, zejména pro subjekty poskytující přeshraniční služby.

Návrh minimalizuje náklady na dodržování předpisů pro malé a střední podniky, neboť od subjektů se vyžaduje, aby přijímaly pouze ta opatření, která jsou nezbytná pro zajištění úrovně bezpečnosti sítě a informačních systémů a která odpovídají riziku, jemuž jsou tyto subjekty vystaveny.

- **Základní práva**

EU je odhodlána zajistit vysoké standardy ochrany základních práv. Veškerá dobrovolná ujednání zaměřená na sdílení informací mezi subjekty, jež tato směrnice podporuje, by byla

uzavírána v atmosféře důvěry, při plném dodržování pravidel Unie pro ochranu údajů a zejména nařízení Evropského parlamentu a Rady (EU) 2016/679[8].

4. ROZPOČTOVÉ DŮSLEDKY

Viz finanční výkaz.

5. OSTATNÍ PRVKY

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

Návrh obsahuje obecný plán sledování a hodnocení dopadu na specifické cíle a vyžaduje, aby Komise provedla přezkum alespoň [54 měsíců] po vstupu v platnost a aby o svých zjištěních podala zprávu Evropskému parlamentu a Radě.

Přezkum bude proveden v souladu s pokyny Komise pro zlepšování právní úpravy.

- **Podrobné vysvětlení konkrétních ustanovení návrhu**

Návrh je rozvržen do několika hlavních oblastí politiky, které spolu navzájem souvisejí a slouží ke zvyšování úrovně kybernetické bezpečnosti v Unii.

Předmět a oblast působnosti (článek 1 a článek 2)

Směrnice zejména: a) stanoví povinnosti členských států přijmout národní strategii kybernetické bezpečnosti, určit příslušné vnitrostátní orgány, jednotná kontaktní místa a týmy CSIRT; b) stanoví, že členské státy vymezí subjektům uvedeným v příloze I jako základní subjekty a uvedeným v příloze II jako důležité subjekty povinnosti v oblasti řízení kybernetických bezpečnostních rizik a hlášení; c) stanoví, že členské státy vymezí povinnosti týkající se výměny informací o kybernetické bezpečnosti.

Vztahuje se na určité veřejné nebo soukromé základní subjekty, které působí v odvětvích uvedených v příloze I (energetika, doprava, bankovnictví, infrastruktury finančních trhů, zdravotnictví, pitná voda, odpadní voda, digitální infrastruktura, veřejná správa a vesmír) a určité důležité subjekty, které působí v odvětvích uvedených v příloze II (poštovní a kurýrní služby, nakládání s odpady, výroba, produkce a distribuce chemických látek, výroba, zpracování a distribuce potravin, výroba a poskytovatelé digitálních služeb). Z oblasti působnosti směrnice jsou vyjmuty mikropodniky a malé podniky ve smyslu doporučení Komise 2003/361/ES ze dne 6. května 2003 kromě poskytovatelů sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací, poskytovatelů služeb vytvářejících důvěru, registrů internetových domén nejvyšší úrovně a veřejné správy a určitých dalších subjektů, jako např. jediného poskytovatele určité služby v členském státě.

Vnitropolitické rámce pro kybernetickou bezpečnost (články 5 až 11)

Členské státy jsou povinny přijmout národní strategii kybernetické bezpečnosti, ve které vymezí strategické cíle a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji.

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

Směrnice rovněž stanoví rámec pro koordinované odhalování zranitelných míst a vyžaduje, aby členské státy určily týmy CSIRT, které budou působit jako důvěryhodní zprostředkovatelé a usnadňovat interakci mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů IKT a služeb IKT. Od Agentury Evropské unie pro bezpečnost sítí a informací (ENISA) se vyžaduje, aby vyvinula a spravovala evropský registr zranitelností pro zaznamenávání odhalených zranitelných míst.

Od členských států se vyžaduje, aby zavedly vnitrostátní rámce pro řešení kybernetických bezpečnostních krizí, mimo jiné určením příslušných vnitrostátních orgánů odpovědných za řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí.

Členské státy jsou rovněž povinny určit jeden nebo více příslušných vnitrostátních orgánů v oblasti kybernetické bezpečnosti pro dohled nad plněním této směrnice a vnitrostátní jednotné kontaktní místo pro kybernetickou bezpečnost, které bude plnit styčnou funkci s cílem zajistit přeshraniční spolupráci orgánů členských států. Od členských států se též vyžaduje, aby určily týmy CSIRT.

Spolupráce (články 12 až 16)

Směrnice zřizuje skupinu pro spolupráci s cílem podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy a rozvíjet důvěru. Zavádí rovněž síť týmů CSIRT, která má přispívat k rozvoji důvěry mezi členskými státy a podporovat rychlou a účinnou operativní spolupráci.

Zřizuje se evropská síť styčných organizací pro kybernetické krize (EU-CyCLONe) na podporu koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí a k zajištění pravidelné výměny informací mezi členskými státy a orgány EU.

Agentuře ENISA se ukládá, aby ve spolupráci s Komisí vydávala každé dva roky zprávu o stavu kybernetické bezpečnosti v Unii.

Od Komise se vyžaduje, aby stanovila systém vzájemného hodnocení, který umožní pravidelné vzájemné hodnocení účinnosti politik členských států v oblasti kybernetické bezpečnosti.

Povinnosti v oblasti řízení kybernetických bezpečnostních rizik a hlášení (články 17 až 23)

Směrnice vyžaduje, aby členské státy zajistily, že vedoucí orgány všech subjektů v oblasti působnosti směrnice schválí opatření k řízení kybernetických bezpečnostních rizik přijatá příslušnými subjekty a absolvují zvláštní odbornou přípravu v oblasti kybernetické bezpečnosti.

Členské státy jsou povinny zajistit, aby subjekty v oblasti působnosti směrnice přijaly vhodná a přiměřená technická a organizační opatření k řízení kybernetických bezpečnostních rizik, jež mohou ohrozit bezpečnost sítí a informačních systémů. Jsou také povinny zajistit, aby subjekty oznamovaly příslušným vnitrostátním orgánům nebo týmům CSIRT každý kybernetický bezpečnostní incident, který má závažný dopad na poskytování služeb, jež poskytují.

Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně musí shromažďovat a uchovávat přesné a úplné údaje o registraci domén.

Tyto subjekty jsou dále povinny poskytnout oprávněným žadatelům o přístup účinný přístup k údajům o registraci domén.

Jurisdikce a registrace (články 24 a 25)

Zpravidla se má za to, že základní subjekty a důležité subjekty spadají do pravomoci členského státu, ve kterém poskytují své služby. U některých druhů subjektů (poskytovatelé služeb systému doménových jmen, registry internetových domén nejvyšší úrovně, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center a poskytovatelé sítí pro doručování obsahu, jakož i někteří poskytovatelé digitálních služeb) se však má za to, že patří do pravomoci členského státu, ve kterém mají hlavní provozovnu v Unii. To má zajistit, aby tyto subjekty nepodléhaly množství různých právních požadavků, pokud poskytují přeshraniční služby ve zvlášť velkém rozsahu. Agentura ENISA je povinna vytvořit a spravovat registr subjektů tohoto druhu.

Sdílení informací (články 26 a 27)

Členské státy stanoví pravidla, která umožní zapojení subjektů do sdílení informací o kybernetické bezpečnosti v rámci zvláštních ujednání o sdílení informací o kybernetické bezpečnosti, a to v souladu s článkem 101 SFEU. Členské státy dále umožní, aby subjekty, které nespadají do oblasti působnosti této směrnice, mohly dobrovolně hlásit závažné incidenty, kybernetické hrozby nebo případy, kdy téměř došlo k incidentu.

Dohled a vymáhání (články 28 až 34)

Příslušné orgány jsou povinny vykonávat dohled nad subjekty, které se nacházejí v oblasti působnosti směrnice, a zejména zajistit, aby tyto subjekty dodržovaly požadavky týkající se bezpečnosti a oznamování incidentů. Směrnice rozlišuje mezi režimem dohledu *ex ante* pro základní subjekty a režimem dohledu *ex post* pro důležité subjekty, přičemž dohled *ex post* vyžaduje, aby příslušné orgány přijímaly opatření, pokud jim byly poskytnuty důkazy nebo indicie, že určitý důležitý subjekt nesplňuje požadavky v oblasti bezpečnosti a oznamování incidentů.

Směrnice rovněž vyžaduje, aby členské státy ukládaly základním a důležitým subjektům správní pokuty, a stanoví určitou maximální výši pokut.

Členské státy jsou povinny spolupracovat a podle potřeby si navzájem pomáhat v případech, kdy subjekty poskytují služby ve více než jednom členském státě, nebo kdy je subjekt primárně usazen v určitém členském státě nebo zde má zástupce, ale jeho sítě a informační systémy se nacházejí v jednom nebo více jiných členských státech.

2020/0359 (COD)

Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

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

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[9],

s ohledem na stanovisko Výboru regionů[10],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Cílem směrnice Evropského parlamentu a Rady (EU) 2016/1148[11] bylo budovat schopnosti v oblasti kybernetické bezpečnosti v Unii, zmírňovat hrozby pro sítě a informační systémy užívané k poskytování základních služeb v klíčových odvětvích a zajišťovat kontinuitu takových služeb v případě kybernetických bezpečnostních incidentů, a přispívat tak k účinnému fungování hospodářství a společnosti v Unii.

(2) Od vstupu směrnice (EU) 2016/1148 v platnost bylo ve zvyšování úrovně odolnosti Unie v oblasti kybernetické bezpečnosti dosaženo významného pokroku. Z přezkumu uvedené směrnice vyplynulo, že posloužila jako katalyzátor institucionálního a regulačního přístupu ke kybernetické bezpečnosti v Unii, a současně připravila půdu pro významnou změnu v myšlení. Uvedená směrnice zajistila dokončení vnitrostátních rámců stanovením národních strategií kybernetické bezpečnosti, stanovením vnitrostátních schopností a prováděním regulačních opatření pokrývajících základní infrastruktury a subjekty určené každým členským státem. Přispěla rovněž ke spolupráci na úrovni Unie vytvořením skupiny pro spolupráci[12] a sítě vnitrostátních bezpečnostních týmů typu CSIRT (dále jen „síť CSIRT“)[13]. I přes tyto úspěchy odhalil přezkum směrnice (EU) 2016/1148 přirozené nedostatky, které jí brání v účinném řešení současných a vznikajících výzev v oblasti kybernetické bezpečnosti.

---

9 Úř. věst. C , , s. .

10 Úř. věst. C , , s. .

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

12 Článek 11 směrnice (EU) 2016/1148.

13 Článek 12 směrnice (EU) 2016/1148.

(3) Sítě a informační systémy se rozvinuly v ústřední prvek každodenního života s rychlou digitální transformací a vzájemnou propojeností společnosti, včetně přeshraniční výměny. Tento vývoj vedl k prudkému rozšíření prostředí kybernetických bezpečnostních hrozeb a přináší nové výzvy, které vyžadují přizpůsobené, koordinované a inovativní reakce ve všech členských státech. Počet, rozsah, sofistikovanost, četnost výskytu a dopad kybernetických bezpečnostních incidentů narůstají a představují značnou hrozbu pro fungování sítí a informačních systémů. V důsledku toho mohou kybernetické incidenty brzdit provádění hospodářských činností na vnitřním trhu, způsobovat finanční ztráty, narušovat důvěru uživatelů a způsobovat velké škody hospodářství a společnosti Unie. Připravenost a účinnost v oblasti kybernetické bezpečnosti jsou dnes proto pro řádné fungování vnitřního trhu důležitější než kdy předtím.

(4) Právním základem směrnice (EU) 1148/2016 byl článek 114 Smlouvy o fungování Evropské unie (SFEU), jehož cílem je vytvoření a fungování vnitřního trhu posílením opatření ke sbližování vnitrostátních předpisů. Požadavky kybernetické bezpečnosti kladené na subjekty poskytující služby nebo vyvíjející příslušné hospodářské činnosti se mezi členskými státy značně liší co do druhů požadavků, míry jejich podrobnosti a způsobu dohledu. Tyto rozdíly jsou spojeny s dalšími náklady a vytvářejí obtíže pro podniky, které nabízejí přeshraničně zboží nebo služby. Požadavky, jež ukládá jeden členský stát a které se liší od požadavků, jež ukládá jiný členský stát, nebo jsou s nimi dokonce v rozporu, mohou tyto přeshraniční činnosti podstatně ovlivnit. Dále je pravděpodobné, že možná neoptimální koncepce nebo neoptimální provádění norem kybernetické bezpečnosti v jednom členském státě může mít důsledky pro úroveň kybernetické bezpečnosti jiných členských států, zejména vzhledem k intenzivní přeshraniční výměně. Z přezkumu směrnice (EU) 2016/1148 vyplynuly velké rozdíly v jejím provádění členskými státy, a to i ve vztahu k její oblasti působnosti, jejíž vymezení bylo do značné míry ponecháno na uvážení členských států. Směrnice (EU) 2016/1148 rovněž dávala členským státům velmi široký prostor pro uvážení, pokud jde o provedení povinností v oblasti bezpečnosti a hlášení incidentů, které v ní byly stanoveny. Tyto povinnosti byly proto na úrovni členských států provedeny výrazně odlišnými způsoby. K podobným rozdílům v provádění docházelo ve vztahu k ustanovením uvedené směrnice týkajícím se dohledu a vymáhání.

(5) Všechny tyto rozdíly vyvolávají roztříštěnost vnitřního trhu a mohou mít škodlivý účinek na jeho fungování s tím, že ovlivňují zejména přeshraniční poskytování služeb a úroveň odolnosti v oblasti kybernetické bezpečnosti v důsledku uplatňování odlišných norem. Cílem této směrnice je takové značné rozdíly mezi členskými státy odstranit, zejména stanovením minimálních pravidel upravujících fungování koordinovaného regulačního rámce, stanovením mechanismů účinné spolupráce příslušných orgánů v každém členském státě, aktualizací seznamu odvětví a činností, na něž se vztahují povinnosti v oblasti kybernetické bezpečnosti, a zavedením účinných nápravných opatření a sankcí, jež napomáhají účinnému vymáhání těchto povinností. Směrnice (EU) 2016/1148 by proto měla být zrušena a nahrazena touto směrnicí.

(6) Tato směrnice ponechává nedotčenou schopnost členských států přijímat nezbytná opatření, aby zajistily ochranu svých základních bezpečnostních zájmů, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. V souladu s článkem 346 SFEU není žádný členský stát povinen poskytovat informace, jejichž zpřístupnění by bylo v rozporu se základními zájmy jeho veřejné bezpečnosti. V tomto ohledu jsou relevantní pravidla

členských států a Unie o ochraně utajovaných informací, dohody o zachování důvěrnosti údajů nebo neformální dohody o zachování důvěrnosti, jako je například tzv. „semaforový protokol“ (Traffic Light Protocol)[14].

(7) Se zrušením směrnice (EU) 2016/1148 by vzhledem k aspektům uvedeným ve 4. až 6. bodě odůvodnění měla být oblast působnosti podle odvětví rozšířena na větší část ekonomiky. Odvětví pokrytá směrnicí (EU) 2016/1148 by proto měla být rozšířena tak, aby bylo zajištěno komplexní pokrytí odvětví a služeb, které mají zásadní význam pro klíčové společenské a hospodářské činnosti v rámci vnitřního trhu. Pravidla by se neměla lišit podle toho, zda jsou subjekty provozovateli základních služeb nebo poskytovateli digitálních služeb. Toto rozlišení se ukázalo jako zastaralé, neboť nezohledňuje skutečnou důležitost odvětví nebo služeb z hlediska společenských a hospodářských činností na vnitřním trhu.

(8) V souladu se směrnicí (EU) 2016/1148 byly členské státy odpovědné za určení toho, které subjekty splňují kritéria pro zařazení mezi provozovatele základních služeb (dále jen „proces určování“). S cílem odstranit značné rozdíly mezi členskými státy v tomto ohledu a zajistit právní jistotu pro všechny příslušné subjekty, pokud jde o požadavky na řízení rizik a povinnosti hlášení, by mělo být stanoveno jednotné kritérium, které určí subjekty, jež spadají do oblasti působnosti této směrnice. Toto kritérium by mělo spočívat v uplatnění pravidla velikostního omezení, podle kterého by do oblasti působnosti této směrnice spadaly všechny střední a velké podniky ve smyslu doporučení Komise 2003/361/ES[15], které působí v odvětvích nebo poskytují druh služeb, na něž se vztahuje tato směrnice. Od členských států by nemělo být vyžadováno, aby stanovily seznam subjektů, které splňují toto obecně použitelné kritérium související s velikostí podniku.

(9) Tato směrnice by se však měla vztahovat i na malé subjekty nebo mikrosubjekty, které splňují určitá kritéria, jež naznačují klíčovou úlohu pro hospodářství nebo společnosti členských států nebo pro konkrétní odvětví či konkrétní druhy služeb. Členské státy by měly být odpovědné za stanovení seznamu takových subjektů a předložit ho Komisi.

(10) Komise může ve spolupráci se skupinou pro spolupráci vydávat pokyny ohledně plnění kritérií platných pro mikropodniky a malé podniky.

(11) Podle odvětví, v němž působí, nebo druhu služeb, jež poskytují, by subjekty spadající do oblasti působnosti této směrnice měly být zařazeny do dvou kategorií: základní a důležité. Tato kategorizace by měla zohlednit úroveň kritické důležitosti daného odvětví nebo druhu služby a také úroveň závislosti jiných odvětví nebo druhů služeb. Jak základní, tak důležité subjekty by měly podléhat stejným požadavkům na řízení rizik a povinnostem hlášení. Dohledové a sankční režimy by mezi těmito dvěma kategoriemi subjektů měly rozlišovat, aby byla zajištěna spravedlivá vyváženost mezi požadavky a povinnostmi na jedné straně a správní zátěží vyplývající z dohledu nad dodržováním směrnice na druhé straně.

(12) Právní předpisy a nástroje specifické pro jednotlivá odvětví mohou přispět k zajištění vysoké úrovně kybernetické bezpečnosti při současném plném zohlednění zvláštností a složitosti těchto odvětví. Pokud právní akt Unie specifický pro určité odvětví

---

[14] Semaforový protokol je prostředek pro toho, kdo sdílí informace, aby informoval své publikum o jakýchkoli omezeních dalšího šíření těchto informací. Používá se téměř ve všech komunitách CSIRT a některých střediscích pro sdílení a analýzu informací (ISAC).

[15] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

vyžaduje, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik, nebo aby oznamovaly incidenty nebo závažné kybernetické hrozby s alespoň rovnocenným účinkem jako povinnosti stanovené v této směrnici, měla by platit tato ustanovení specifická pro dané odvětví, včetně ustanovení o dohledu a vymáhání. Komise může vydávat pokyny v souvislosti s prováděním *lex specialis*. Tato směrnice nebrání přijetí dalších aktů Unie specifických pro určitá odvětví a týkajících se opatření k řízení kybernetických bezpečnostních rizik a oznamování incidentů. Touto směrnicí nejsou dotčeny stávající prováděcí pravomoci, jež byly Komisi svěřeny v řadě odvětví, včetně odvětví dopravy a energetiky.

(13) Nařízení Evropského parlamentu a Rady XXXX/XXXX[16] by mělo být považováno za právní akt specifický pro konkrétní odvětví ve vztahu k této směrnici, pokud jde o subjekty ve finančním odvětví. Ustanovení nařízení XXXX/XXXX, která se týkají opatření k řízení rizik v oblasti informačních a komunikačních technologií (IKT), řešení incidentů souvisejících s IKT, a zejména hlášení incidentů, jakož i ustanovení týkající se testování digitální provozní odolnosti, ujednání o sdílení informací a rizik v oblasti IKT spojených s třetími stranami by měla platit místo ustanovení stanovených podle této směrnice. Členské státy by proto neměly uplatňovat ustanovení této směrnice o řízení kybernetických bezpečnostních rizik a o povinnostech hlášení, o sdílení informací a o dohledu a vymáhání vůči jakýmkoli finančním subjektům, na něž se vztahuje nařízení XXXX/XXXX. Zároveň je důležité zachovat s finančním odvětvím silný vztah a výměnu informací podle této směrnice. Za tím účelem nařízení XXXX/XXXX umožňuje, aby se všechny orgány finančního dohledu, evropské orgány dohledu pro odvětví financí a příslušné vnitrostátní orgány podle nařízení XXXX/XXXX účastnily diskusí o strategické politice a technických prací skupiny pro spolupráci a aby si vyměňovaly informace a spolupracovaly s jednotnými kontaktními místy určenými podle této směrnice a s týmy CSIRT v členských státech. Příslušné orgány podle nařízení XXXX/XXXX by měly předávat údaje o závažných incidentech týkajících se IKT také jednotným kontaktním místům určeným podle této směrnice. Členské státy by kromě toho měly odvětví financí nadále zahrnovat do svých strategií kybernetické bezpečnosti a týmy CSIRT v členských státech mohou zahrnout finanční odvětví do svých činností.

(14) Vzhledem ke vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností subjektů by měl být zajištěn soudržný přístup ke směrnici Evropského parlamentu a Rady (EU) XXX/XXX[17] a k této směrnici. Za tímto účelem by členské státy měly zajistit, aby klíčové subjekty a rovnocenné subjekty podle směrnice (EU) XXX/XXX byly považovány za základní subjekty podle této směrnice. Členské státy by také měly zajistit, aby jejich strategie kybernetické bezpečnosti stanovily rámec politik pro posílení koordinace mezi příslušným orgánem podle této směrnice a příslušným orgánem podle směrnice (EU) XXX/XXX v souvislosti se sdílením informací o incidentech a kybernetických hrozbách a plněním úkolů v oblasti dohledu. Orgány by podle obou směrnic měly spolupracovat a vyměňovat si informace, zejména informace týkající se určení klíčových subjektů, kybernetických hrozeb, kybernetických bezpečnostních rizik, incidentů dotýkajících se klíčových subjektů a opatření v oblasti kybernetické bezpečnosti přijatých klíčovými subjekty. Příslušným orgánům podle této směrnice by mělo být umožněno, aby na žádost příslušných orgánů podle směrnice (EU) XXX/XXX vykonávaly své dohledové a vymáhací

---

16 *[vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]*

17 *[vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]*

pravomoci vůči subjektu, který byl označen jako klíčový. Oba orgány by za tímto účelem měly spolupracovat a vyměňovat si informace.

(15) Podpora a ochrana spolehlivého, odolného a bezpečného systému doménových jmen jsou klíčovým faktorem pro zachování integrity internetu a jsou nezbytné pro jeho nepřetržitý a stabilní provoz, na kterém závisí digitální ekonomika a společnost. Tato směrnice by se proto měla vztahovat na všechny poskytovatele služeb systému doménových jmen v celém řetězci řešení systému doménových jmen, včetně operátorů kořenových jmenných serverů, serverů internetových domén nejvyšší úrovně, autoritativních jmenných serverů pro doménová jména a rekurzivních resolverů.

(16) Služby cloud computingu by měly zahrnovat služby, které umožňují správu na vyžádání a široký dálkový přístup k rozšiřitelnému a přizpůsobitelnému úložišti distribuovaných výpočetních zdrojů, které je možno sdílet. Tyto výpočetní zdroje zahrnují zdroje, jako jsou sítě, servery nebo jiná infrastruktura, operační systémy, software, ukládání, aplikace a služby. Modely zavádění cloud computingu by měly zahrnovat soukromý, komunitní, veřejný a hybridní cloud. Uvedené služby a modely zavádění mají tentýž význam jako podmínky poskytování služeb a modely zavádění definované podle normy ISO/IEC 17788:2014. Schopnost uživatele cloud computingu jednostranně vlastními silami využívat výpočetní potenciál, jako je čas serveru nebo ukládání na síti, bez jakékoli interakce poskytovatele služeb cloud computingu s člověkem, by bylo možné popsat jako správu na vyžádání. Pojem „široký dálkový přístup“ se používá k popsání toho, že cloudová kapacita je poskytována po síti a přístup k ní se uskutečňuje prostřednictvím mechanismu podporujícího použití heterogenních platforem s tenkými nebo tlustými klienty (včetně mobilních telefonů, tabletů, laptopů a pracovních stanic). Pojem „rozšiřitelný“ poukazuje na skutečnost, že v zájmu pokrytí nerovnoměrné poptávky jsou výpočetní zdroje přidělovány poskytovatelem cloudových služeb flexibilně, bez ohledu na zeměpisnou polohu zdrojů. Pojem „přizpůsobitelné úložiště“ označuje skutečnost, že uvedené výpočetní zdroje jsou poskytovány a uvolňovány na základě poptávky, aby bylo možno urychleně zvyšovat i snižovat dostupné zdroje se zřetelem na zatížení. Pojmem „které je možno sdílet“ se rozumí, že tyto výpočetní zdroje jsou poskytovány vícero uživatelům, kteří k dané službě sdílejí společný přístup, avšak zpracování probíhá pro každého uživatele odděleně, byť je služba poskytována z téhož elektronického zařízení. Pojem „distribuovaný“ označuje ty výpočetní zdroje, které se nacházejí na různých sítově propojených počítačích nebo zařízeních a které mezi sebou komunikují a koordinují prostřednictvím předávání zpráv.

(17) Vzhledem ke vzniku inovativních technologií a nových obchodních modelů se předpokládá, že v reakci na vyvíjející se potřeby zákazníků se na trhu objeví nové modely zavádění a služeb cloud computingu. V této souvislosti lze služby cloud computingu poskytovat ve vysoce distribuované podobě, ještě blíže k místu, kde jsou data generována nebo shromažďována, a přejít tak od tradičního modelu k vysoce distribuovanému modelu (tzv. „edge computing“).

(18) Služby, jež nabízejí poskytovatelé služeb datových center, nemusí být vždy poskytovány ve formě služeb cloud computingu. Datová centra tedy ne vždy tvoří součást infrastruktury cloud computingu. Aby bylo možné řídit všechna rizika pro bezpečnost sítí a informačních systémů, měla by se tato směrnice vztahovat také na poskytovatele takových služeb datových center, které nejsou službami cloud computingu. Pro účely této směrnice by pojem „služba datových center“ měl zahrnovat poskytování služby, která zahrnuje struktury nebo skupiny struktur určené pro centralizované úpravy, vzájemné propojení a provozování informačních

technologií a síťových zařízení poskytujících služby ukládání, zpracování a přepravu dat spolu se všemi zařízeními a infrastrukturami pro rozvod energie a kontrolu životního prostředí. Pojem „služba datových center“ se nevztahuje na interní, firemní datová centra vlastněná a provozovaná pro vlastní potřebu dotyčného subjektu.

(19) Poskytovatelé poštovních služeb ve smyslu směrnice Evropského parlamentu a Rady 97/67/ES[18] a rovněž poskytovatelé expresních a kurýrních doručovacích služeb by měli této směrnici podléhat, pokud poskytují alespoň jeden z kroků v poštovním řetězci, a zejména výběr, třídění nebo dodání, včetně služeb souvisejících s vyzvedáváním. Přepravní služby, které nejsou poskytovány ve spojení s některým z těchto kroků, by neměly spadat do oblasti působnosti poštovních služeb.

(20) Tyto rostoucí vzájemné závislosti jsou výsledkem stále více přeshraniční a vzájemně propojené sítě poskytování služeb pomocí klíčových infrastruktur v celé Unii v odvětvích energetiky, dopravy, digitální infrastruktury, pitné a odpadní vody, zdravotnictví, některých prvků veřejné správy a rovněž vesmíru, pokud jde o poskytování určitých služeb závisejících na pozemních infrastrukturách, které vlastní, řídí a provozují buď členské státy, nebo soukromé subjekty, a proto nezahrnují infrastruktury vlastněné, řízené a provozované Unií nebo jménem Unie v rámci jejích vesmírných programů. Tyto vzájemné závislosti znamenají, že jakékoli narušení hospodářské soutěže, a dokonce i takové narušení, které je původně omezeno na jeden subjekt nebo jedno odvětví, může mít širší dominové účinky, jež mohou potenciálně mít dalekosáhlé negativní dopady na poskytování služeb na celém vnitřním trhu. Pandemie COVID-19 prokázala zranitelnost našich stále více vzájemně závislých společností, jsou-li vystaveny málo pravděpodobným rizikům.

(21) Vzhledem k odlišnostem jednotlivých vnitrostátních správních struktur a s cílem podpořit již existující odvětvová opatření nebo kontrolní a regulační orgány Unie by členské státy měly mít možnost určit více než jeden vnitrostátní příslušný orgán odpovědný za plnění úkolů spojených s bezpečností sítí a informačních systémů základních a důležitých subjektů podle této směrnice. Členským státům by mělo být umožněno, aby tuto úlohu svěřily již existujícímu orgánu.

(22) Pro usnadnění přeshraniční spolupráce a komunikace mezi orgány a za účelem účinného provedení této směrnice je nezbytné, aby každý členský stát určil na vnitrostátní úrovni jednotné kontaktní místo pověřené koordinací v oblasti bezpečnosti sítí a informačních systémů a přeshraniční spolupráce na úrovni Unie.

(23) Příslušné orgány nebo týmy CSIRT by měly od subjektů dostávat oznámení o incidentech účinným a efektivním způsobem. Jednotným kontaktním místům by mělo být uloženo, aby zasílala oznámení o incidentech jednotným kontaktním místům jiných dotčených členských států. Aby bylo zajištěno jedno jednotné kontaktní místo v každém členském státě, měly by být jednotným kontaktním místům na úrovni členských států zasílány příslušné informace o incidentech týkajících se subjektů ve finančním odvětví od příslušných orgánů podle nařízení XXXX/XXXX, které by tato kontaktní místa měla být podle této směrnice schopna případně zasílat příslušným vnitrostátním orgánům nebo týmům CSIRT.

---

[18] Směrnice Evropského parlamentu a Rady 97/67/ES ze dne 15. prosince 1997 o společných pravidlech pro rozvoj vnitřního trhu poštovních služeb Společenství a zvyšování kvality služby (Úř. věst. L 15, 21.1.1998, s. 14).

(24) Členské státy by měly být náležitě vybaveny jak po technické, tak po organizační stránce, aby mohly předcházet incidentům a rizikům spojeným se sítěmi a informačními systémy, odhalovat je, reagovat na ně a zmírňovat je. Členské státy by proto měly zajistit, aby dobře fungovaly jejich týmy CSIRT, rovněž označované jako týmy CERT (týmy pro reakci na počítačové hrozby), které budou splňovat základní požadavky, tak aby byly zaručeny jejich efektivní a kompatibilní schopnosti řešit incidenty a rizika a aby byla zajištěna účinná spolupráce na úrovni Unie. V zájmu posílení důvěry mezi subjekty a týmy CSIRT v případech, kdy je tým CSIRT součástí příslušného orgánu, by členské státy měly zvážit funkční oddělení operativních úkolů plněných týmy CSIRT, zejména v souvislosti se sdílením informací a podporou poskytovanou subjektům, od činností příslušných orgánů v oblasti dohledu.

(25) Pokud jde o osobní údaje, týmům CSIRT by mělo být umožněno, aby v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679[19] jménem a na žádost subjektu podle této směrnice aktivně prohledávaly sítě a informační systémy, které používá k poskytování svých služeb. Členské státy by se měly zaměřit na to, aby všem odvětvovým týmům CSIRT zajistily stejné technické podmínky. Při budování vnitrostátních týmů CSIRT mohou členské státy požádat o součinnost Agenturu Evropské unie pro kybernetickou bezpečnost (ENISA).

(26) S ohledem na význam mezinárodní spolupráce na poli kybernetické bezpečnosti by týmy CSIRT měly mít možnost účastnit se kromě sítě CSIRT zřízené touto směrnicí také dalších sítí pro mezinárodní spolupráci.

(27) V souladu s přílohou doporučení Komise (EU) 2017/1548 o koordinované reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize (dále jen „plán“)[20] by rozsáhlý incident měl označovat incident s významným dopadem na nejméně dva členské státy nebo takový incident, při kterém narušení přesahuje schopnost členského státu na něj reagovat. V závislosti na jejich příčině a dopadu mohou rozsáhlé incidenty eskalovat a přejít ve skutečné krize, jež neumožní řádné fungování vnitřního trhu. Vzhledem k širokému dopadu a ve většině případů i přeshraniční povaze takových incidentů by členské státy a příslušné orgány, instituce a agentury Unie měly na technické, operativní a politické úrovni spolupracovat a odpovídajícím způsobem koordinovat reakci v celé Unii.

(28) Využití zranitelných míst v sítích a informačních systémech může způsobit vážná narušení a škody, a rychlé určení a náprava těchto zranitelností je proto důležitým faktorem při snižování kybernetických bezpečnostních rizik. Subjekty, které takové systémy vyvíjejí, by proto měly stanovit vhodné postupy k řešení zranitelných míst, jakmile jsou zjištěna. Jelikož zranitelná místa jsou často zjištěna a ohlášena (odhalena) třetími stranami (subjekty ohlašujícími incidenty), výrobce nebo poskytovatel produktů nebo služeb IKT by měl rovněž zavést nezbytné postupy pro získávání informací o zranitelných místech od třetích stran. Vodítko pro řešení zranitelností a odhalování zranitelností v této souvislosti poskytují mezinárodní normy ISO/IEC 30111 a ISO/IEC 29417. Pokud jde o odhalování zranitelných míst, je obzvláště důležitá koordinace mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů nebo služeb IKT. Koordinované odhalování zranitelností specifikuje

---

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

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

strukturovaný proces, jehož prostřednictvím jsou zranitelná místa hlášena organizacím takovým způsobem, který organizaci umožní diagnostikovat a odstranit zranitelnost dříve, než budou podrobné informace o ní sděleny třetím stranám nebo veřejnosti. Koordinované odhalování zranitelností by také mělo zahrnovat koordinaci mezi subjektem ohlašujícím incidenty a organizací, pokud jde o načasování odstranění a zveřejnění zranitelných míst.

(29) Členské státy by proto měly stanovit příslušnou vnitrostátní politiku a přijmout tak opatření k usnadnění koordinovaného odhalování zranitelností. V této souvislosti by členské státy měly určit tým CSIRT, který převezme úlohu „koordinátora“ a v případě potřeby bude působit jako zprostředkovatel mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů nebo služeb IKT. Úkoly koordinátora týmů CSIRT by měly zahrnovat zejména určení a kontaktování dotčených subjektů, podporu subjektů ohlašujících incidenty, dojednávání harmonogramů odhalení a řízení zranitelností, které se dotýkají mnoha organizací (odhalování zranitelností ohrožujících více stran). Pokud se zranitelná místa dotýkají více výrobců nebo poskytovatelů produktů nebo služeb IKT, kteří jsou usazení ve více než jednom členském státě, určené týmy CSIRT z každého z dotčených členských států by měly spolupracovat v rámci sítě CSIRT.

(30) Přístup ke správným a včasným informacím o zranitelnostech dotýkajících se produktů a služeb IKT přispívá k zesílenému řízení kybernetických bezpečnostních rizik. V této souvislosti jsou zdroje veřejně přístupných informací o zranitelných místech důležitým nástrojem pro subjekty a jejich uživatele, ale i pro příslušné vnitrostátní orgány v Unii a týmy CSIRT. Z tohoto důvodu by agentura ENISA měla zavést registr zranitelností, kde základní a důležité subjekty a jejich dodavatelé, a stejně tak i subjekty, které nespadají do oblasti působnosti této směrnice, mohou na základě dobrovolnosti odhalovat zranitelná místa a poskytovat o nich informace, jež uživatelům umožní přijímat vhodná opatření ke zmírnění dopadů.

(31) Ačkoli podobné registry nebo databáze zranitelností existují, jsou hostovány a spravovány subjekty, které nejsou usazeny v Unii. Evropský registr zranitelností spravovaný agenturou ENISA by poskytl lepší transparentnost procesu odhalování předtím, než je zranitelné místo oficiálně zveřejněno, a odolnost v případech narušení nebo přerušení poskytování podobných služeb. S cílem zabránit zdvojení úsilí a v co největší možné míře usilovat o komplementaritu, by agentura ENISA měla zkoumat možnost uzavření strukturovaných dohod o spolupráci s podobnými registry v jurisdikcích třetích zemí.

(32) Skupina pro spolupráci by měla každé dva roky přijmout pracovní program včetně opatření, které má skupina podniknout ke splnění svých cílů a úkolů. Časový rámec prvního programu, který by byl podle této směrnice přijat, by byl sladěn s časovým rámcem posledního programu přijatého podle směrnice (EU) 2016/1148, aby se zabránilo možnému přerušení práce skupiny.

(33) Při vypracování pokynů by skupina pro spolupráci měla důsledně: mapovat vnitrostátní řešení a zkušenosti, posuzovat dopad výstupů skupiny pro spolupráci na přístupy členských států, diskutovat o problémech spojených s prováděním a formulovat konkrétní doporučení, která je třeba zohlednit prostřednictvím lepšího provádění stávajících pravidel.

(34) Skupina pro spolupráci by i nadále měla být flexibilním fórem a měla by být schopna reagovat na měnící se a nové priority a výzvy politik, a přitom brát v úvahu dostupnost zdrojů. Měla by organizovat pravidelná společná setkání s relevantními soukromými

zúčastněnými stranami z celé Unie za účelem projednání činností prováděných skupinou a shromažďování vstupů týkajících se vznikajících politických výzev. S cílem posílit spolupráci na úrovni Unie by skupina měla zvážit pozvání k účasti na její činnosti pro instituce a agentury Unie zapojené do politiky v oblasti kybernetické bezpečnosti, jako je Evropské centrum pro boj proti kyberkriminalitě (EC3), Agentura Evropské unie pro bezpečnost letectví (EASA) a Agentura Evropské unie pro kosmický program (EUSPA).

(35) Příslušné orgány a týmy CSIRT by měly být zmocněny se účastnit výměnných programů pro úředníky z jiných členských států za účelem zlepšení spolupráce. Příslušné orgány by měly přijmout nezbytná opatření, jež umožní úředníkům z jiných členských států účinně se zapojit do činností hostitelského příslušného orgánu.

(36) Unie by ve vhodných případech měla v souladu s článkem 218 SFEU uzavírat mezinárodní dohody s třetími zeměmi nebo mezinárodními organizacemi, které umožní a zorganizují jejich účast na některých činnostech skupiny pro spolupráci a sítě CSIRT. Takové dohody by měly zajistit odpovídající ochranu údajů.

(37) Členské státy by měly přispět k vytvoření rámce EU pro reakci na kybernetické bezpečnostní krize uvedeného v doporučení (EU) 2017/1584 prostřednictvím stávajících sítí pro spolupráci, zejména sítě styčných organizací pro kybernetické krize (EU-CyCLONe), sítě CSIRT a skupiny pro spolupráci. Sítě EU-CyCLONe a CSIRT by měly spolupracovat na základě procesních ujednání, jež vymezí podmínky této spolupráce. Jednací řád sítě EU-CyCLONe by měl dále vymezit podmínky, za nichž by měla síť fungovat, mimo jiné včetně úloh, způsobů spolupráce, interakcí s jinými relevantními subjekty a šablon pro sdílení informací, jakož i způsobů komunikace. Pokud jde o krizové řízení na úrovni Unie, měly by příslušné strany vycházet z integrovaných opatření pro politickou reakci na krize. Komise by za tímto účelem měla využít proces meziodvětvové koordinace na vysoké úrovni v krizových situacích ARGUS. Pokud má krize významný externí rozměr nebo rozměr společné bezpečnostní a obranné politiky (SBOP), měl by být aktivován mechanismus Evropské služby pro vnější činnost (ESVČ) pro reakce na krize.

(38) Pro účely této směrnice by pojem „riziko“ měl poukazovat na možnost ztráty nebo narušení způsobených kybernetickým bezpečnostním incidentem a měl by být vyjádřen jako kombinace rozsahu takové ztráty nebo narušení a pravděpodobnosti vzniku uvedeného incidentu.

(39) Pro účely této směrnice by pojem „případy, kdy téměř došlo k incidentu“ měl poukazovat na událost, která by mohla potenciálně způsobit škodu, ale jejímu plnému projevení bylo úspěšně zabráněno.

(40) Opatření pro řízení rizik by měla zahrnovat opatření pro určení veškerých rizik incidentů, předcházení incidentům, jejich odhalování a řešení a zmírňování jejich dopadu. Bezpečnost sítí a informačních systémů by měla zahrnovat bezpečnost uchovávaných, předávaných a zpracovávaných údajů.

(41) Požadavky na řízení kybernetických bezpečnostních rizik by měly být úměrné rizikům, jež daná síť nebo informační systém obnáší, aby na základní a důležité subjekty nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových opatření.

(42) Základní a důležité subjekty by měly zajistit bezpečnost sítí a informačních systémů, které užívají ve svých činnostech. Jedná se především o soukromé sítě a informační systémy, jež jsou buď řízeny jejich interními pracovníky IT, nebo jejichž bezpečnost

zajišťuje externí dodavatel. Požadavky týkající se řízení kybernetických bezpečnostních rizik a hlášení podle této směrnice by měly pro příslušné základní a důležité subjekty platit bez ohledu na to, zda správu svých sítí a informačních systémů provádějí interně, nebo s pomocí externího dodavatele.

(43) Řešení kybernetických bezpečnostních rizik vyplývajících z dodavatelského řetězce subjektu nebo jeho vztahů s dodavateli je zvlášť důležité vzhledem k počtu incidentů, kdy se subjekty staly obětí kybernetických útoků a kdy nepřátelské subjekty byly schopny narušit bezpečnost sítí a informačních systémů daného subjektu tím, že využily zranitelných míst v produktech a službách třetí strany. Subjekty by proto měly posoudit a zohlednit celkovou kvalitu produktů a postupů kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů k zajištění bezpečného vývoje.

(44) Mezi poskytovateli služeb mají zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí o odhalování a řešení incidentů poskytovatelé řízených bezpečnostních služeb v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Tito poskytovatelé řízených bezpečnostních služeb však jsou rovněž sami cíli kybernetických útoků a kvůli své úzké integraci do provozu operátorů představují zvlášť vysoké kybernetické bezpečnostní riziko. Subjekty by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat se zvýšenou pečlivostí.

(45) Subjekty by rovněž měly řešit kybernetická bezpečnostní rizika vyplývající z jejich interakcí a vztahů s jinými zúčastněnými stranami v rámci širšího ekosystému. Subjekty by zejména měly přijetím vhodných opatření zajistit, že jejich spolupráce s akademickými a výzkumnými institucemi probíhá v souladu s jejich politikami kybernetické bezpečnosti a řídí se osvědčenými postupy, pokud jde o bezpečný přístup a šíření informací obecně a ochranu duševního vlastnictví zvláště. Podobně by subjekty, jsou-li závislé na službách transformace dat a analýzy dat poskytovaných třetími stranami, vzhledem k důležitosti a hodnotě dat pro jejich činnost měly přijmout veškerá vhodná opatření v oblasti kybernetické bezpečnosti.

(46) K dalšímu řešení klíčových rizik dodavatelského řetězce a na pomoc subjektům působícím v odvětvích, na něž se vztahuje tato směrnice, aby odpovídajícím způsobem řídily dodavatelský řetězec a kybernetická bezpečnostní rizika související s dodavateli, by skupina pro spolupráci, jež zahrnuje příslušné vnitrostátní orgány, ve spolupráci s Komisí a agenturou ENISA měla provést koordinovaná posouzení rizik dodavatelských řetězců v jednotlivých odvětvích, jak bylo již provedeno pro sítě 5G v návaznosti na doporučení (EU) 2019/534 o kybernetické bezpečnosti sítí 5G[21], za účelem určení příslušných hrozeb a zranitelných míst v každém odvětví, v němž existují kritické služby IKT, systémy nebo produkty IKT.

(47) Posouzení rizik dodavatelského řetězce by s ohledem na charakteristické rysy dotčeného odvětví měla zohlednit jak technické, tak případné netechnické faktory včetně faktorů vymezených v doporučení (EU) 2019/534, v koordinovaném posouzení rizik pro bezpečnost sítí 5G v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci. K určení dodavatelských řetězců, které by měly podléhat koordinovanému posouzení rizik, by měla být vzata v úvahu tato kritéria: i) rozsah, v jakém základní a důležité subjekty

[21] Doporučení Komise (EU) 2019/534 ze dne 26. března 2019 Kybernetická bezpečnost sítí 5G (Úř. věst. L 88, 29.3.2019, s. 42).

využívají konkrétní kritické služby, systémy a produkty IKT a jsou na nich závislé; ii) relevantnost konkrétních služeb, systémů nebo produktů IKT pro plnění kritických nebo citlivých funkcí, včetně zpracování osobních údajů; iii) dostupnost alternativních služeb, systémů nebo produktů IKT; iv) odolnost celého dodavatelského řetězce služeb, systémů nebo produktů IKT vůči narušení a v) u vznikajících služeb, systémů nebo produktů IKT jejich budoucí význam pro činnost subjektů.

(48) S cílem zjednodušit právní povinnosti ukládané poskytovatelům veřejných sítí elektronické komunikace nebo veřejně dostupných služeb elektronické komunikace a poskytovatelům služeb vytvářejících důvěru a které se týkají bezpečnosti jejich sítí a informačních systémů, a s cílem umožnit těmto subjektům a jejich příslušným orgánům využívat právní rámec stanovený touto směrnicí (včetně určení týmu CSIRT odpovědného za zvládání rizik a incidentů, účasti příslušných orgánů a institucí na činnosti skupiny pro spolupráci a sítě CSIRT), by měly být zahrnuty do oblasti působnosti této směrnice. Příslušná ustanovení v nařízení Evropského parlamentu a Rady (EU) č. 910/2014[22] a směrnici Evropského parlamentu a Rady (EU) 2018/1972[23], které na tyto druhy subjektů kladou požadavky týkající se bezpečnosti a podávání zpráv, by proto měla být zrušena. Pravidly o povinnostech ohlašování by nemělo být dotčeno nařízení Evropského parlamentu a Rady (EU) 2016/679 a směrnice Evropského parlamentu a Rady 2002/58/ES[24].

(49) Pokud je to vhodné a s cílem zabránit zbytečným narušením by příslušné orgány odpovědné za dohled a vymáhání pro účely této směrnice měly i nadále používat stávající vnitrostátní pokyny a právní předpisy členských států přijaté k provedení pravidel týkajících se bezpečnostních opatření stanovených v čl. 40 odst. 1 směrnice (EU) 2018/1972, a rovněž požadavků čl. 40 odst. 2 uvedené směrnice týkajících se parametrů pro určení významnosti dopadu daného incidentu.

(50) Vzhledem k rostoucímu významu interpersonálních komunikačních služeb nezávislých na číslech je nutné zajistit, aby i tyto služby podléhaly odpovídajícím bezpečnostním požadavkům v souladu s jejich zvláštní povahou a ekonomickým významem. Provozovatelé takových služeb by tedy měli rovněž zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. Vzhledem k tomu, že poskytovatelé interpersonálních komunikačních služeb nezávislých na číslech obvykle nevykonávají skutečnou kontrolu nad přenosem signálů v sítích, lze míru rizika pro tyto služby v některých ohledech považovat za nižší než v případě tradičních služeb elektronických komunikací. Totéž platí o interpersonálních komunikačních službách, které využívají čísla a které nevykonávají skutečnou kontrolu nad přenosem signálů.

(51) Vnitřní trh více než kdy předtím spoléhá na fungování internetu. Na službách poskytovaných po internetu jsou závislé služby prakticky všech základních a důležitých subjektů. S cílem zajistit bezproblémové poskytování služeb základních a důležitých subjektů je důležité, aby veřejné sítě elektronických komunikací, jako jsou

---

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

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

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

například internetové páteřní sítě nebo podmořské komunikační kabely, měly zavedena odpovídající opatření v oblasti kybernetické bezpečnosti a hlásily incidenty, které se jich týkají.

(52) Ve vhodných případech by subjekty měly informovat příjemce svých služeb o konkrétních a závažných hrozbách a o opatřeních, která mohou přijmout, aby snížili riziko, jež jim z těchto hrozeb vyplývá. Požadavek na informování příjemců o hrozbách by subjekty neměl zbavovat povinnosti přijmout na své vlastní náklady přiměřená a okamžitá opatření s cílem zamezit jakýmkoli kybernetickým hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto informace o bezpečnostních hrozbách by měly být příjemcům poskytovány zdarma.

(53) Poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací by měli příjemce služby zejména informovat o konkrétních a závažných kybernetických hrozbách a o opatřeních, která mohou přijmout, aby chránili bezpečnost své komunikace, například použitím specifických druhů softwaru nebo šifrovacích technologií.

(54) S cílem zajistit bezpečnost sítí a služeb elektronické komunikace by mělo být podporováno použití šifrování, a zejména šifrování mezi koncovými body, a v případě nutnosti by pro poskytovatele těchto služeb a sítí v souladu se zásadami bezpečnosti a soukromí standardně a záměrně pro účely článku 18 mělo být povinné. Použití šifrování mezi koncovými body by mělo být v souladu s pravomocemi členských států zajistit ochranu podstatných zájmů své bezpečnosti a veřejné bezpečnosti a umožnit vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. Řešení k zajištění zákonného přístupu k informacím v rámci komunikace šifrované mezi koncovými body by měla zachovat účinnost šifrování při ochraně soukromí a bezpečnosti komunikací, a současně poskytnout účinnou reakci na trestnou činnost.

(55) Tato směrnice stanoví dvoustupňový přístup k hlášení incidentů, tak aby bylo dosaženo správné rovnováhy mezi rychlým hlášením, které pomáhá snížit potenciální šíření incidentů a umožňuje subjektům žádat o podporu, na jedné straně a podrobným hlášením, které čerpá cenná poučení z jednotlivých incidentů a s postupem času zvyšuje odolnost jednotlivých společností a celých odvětví vůči kybernetickým hrozbám, na straně druhé. Jakmile se subjekty dozvědí o incidentu, měly by být povinny předložit počáteční oznámení do 24 hodin a poté závěrečnou zprávu nejpozději do jednoho měsíce. Počáteční oznámení by mělo obsahovat pouze informace, které jsou zcela nezbytné, aby byl příslušný orgán zpraven o incidentu, a které subjektu umožňují v případě potřeby požádat o pomoc. V tomto oznámení by v daném případě mělo být uvedeno, zda je incident pravděpodobně způsoben protiprávním či zlovolným jednáním. Členské státy by měly zajistit, aby požadavek na předložení tohoto počátečního oznámení neodváděl zdroje ohlašujícího subjektu od činností souvisejících s řešením incidentu, které by měly mít přednost. Aby se dále zabránilo tomu, že by povinnosti hlášení incidentu odváděly zdroje od řešení reakce na incident nebo jinak narušovaly úsilí subjektů v tomto ohledu, členské státy by měly rovněž stanovit, že v řádně odůvodněných případech a po dohodě s příslušnými orgány nebo s týmy CSIRT se dotyčný subjekt může odchýlit od lhůt 24 hodin pro počáteční oznámení a jeden měsíc pro konečnou zprávu.

(56) Základní a důležité subjekty jsou často v situaci, kdy je konkrétní incident vzhledem k jeho povaze třeba v důsledku oznamovacích povinností uvedených v různých právních nástrojích ohlásit různým orgánům. Takové případy vytvářejí další zátěž a mohou také vést k nejasnostem, pokud jde o formát a postupy takových oznámení.

Vzhledem k tomu a za účelem zjednodušení hlášení o bezpečnostních incidentech by členské státy měly stanovit *jedno vstupní místo* pro všechna oznámení vyžadovaná podle této směrnice i podle jiných právních předpisů Unie, jako je nařízení (EU) 2016/679 a směrnice 2002/58/ES. Agentura ENISA by ve spolupráci se skupinou pro spolupráci měla vypracovat společné šablony hlášení prostřednictvím pokynů, které by zjednodušily a zefektivnily informace uvedené v hlášeních, jež vyžaduje právo Unie, a snížily zátěž pro společnosti.

(57) Existuje-li podezření, že určitý incident souvisí se závažnou trestnou činností podle unijního nebo vnitrostátního práva, měly by členské státy motivovat základní a důležité subjekty, aby na základě platných pravidel trestního řízení v souladu s právem Unie incidenty s podezřením na trestní povahu ohlašovaly z vlastní iniciativy donucovacím orgánům. V případě potřeby, a aniž jsou dotčena pravidla ochrany osobních údajů platná pro Europol, je žádoucí, aby koordinaci mezi příslušnými orgány a donucovacími orgány v různých členských státech usnadnily EC3 a agentura ENISA.

(58) V důsledku incidentů je v mnoha případech ohrožena ochrana osobních údajů. V této souvislosti by příslušné orgány měly spolupracovat s orgány pro ochranu osobních údajů a orgány dozoru podle směrnice 2002/58/ES a vyměňovat si s nimi informace o všech relevantních záležitostech

(59) Udržování přesných a úplných databází doménových jmen a registračních údajů (takzvaných „údajů WHOIS“) a poskytování zákonného přístupu k těmto údajům má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému doménových jmen (DNS), což na druhé straně přispívá k vyšší společné úrovni kybernetické bezpečnosti v Unii. Pokud zpracování údajů zahrnuje osobní údaje, musí takové zpracování být v souladu s právem Unie v oblasti ochrany údajů.

(60) Dostupnost a včasný přístup k těmto údajům pro orgány veřejné správy, včetně příslušných orgánů podle unijního nebo vnitrostátního práva za účelem prevence, vyšetřování či stíhání trestných činů, pro týmy CERT (týmy CSIRT) a, pokud jde o údaje jejich zákazníků, pro poskytovatele elektronických komunikačních sítí a služeb a poskytovatele technologií a služeb v oblasti kybernetické bezpečnosti jednající jménem těchto zákazníků, má zásadní význam pro prevenci a boj proti zneužívání systému doménových jmen, a zejména pro prevenci a odhalování kybernetických bezpečnostních incidentů a reakci na tyto incidenty. Pokud se takový přístup týká osobních údajů, měl by být v souladu s právem Unie v oblasti ochrany údajů.

(61) S cílem zajistit dostupnost přesných a úplných údajů o registraci domén by registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně (takzvaní registrátoři) měly shromažďovat údaje o registraci domén a zaručovat integritu a dostupnost těchto údajů. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně by zejména měly stanovit politiky a postupy pro shromažďování a uchovávání přesných a úplných registračních údajů a rovněž zamezit uvádění nesprávných registračních údajů a opravovat je v souladu s pravidly Unie o ochraně osobních údajů.

(62) Registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén by měly veřejně zpřístupnit údaje o registraci domén, které nespadají do oblasti působnosti pravidel Unie na ochranu osobních údajů, například údajů, které

se týkají právnických osob[25]. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně by také měly v souladu s právem Unie na ochranu osobních údajů umožnit oprávněným žadatelům o přístup zákonný přístup ke konkrétním údajům o registraci domén týkajícím se fyzických osob. Členské státy by měly zajistit, aby registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén bez zbytečného odkladu reagovaly na žádosti oprávněných žadatelů o přístup o zpřístupnění údajů o registraci domén. Registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén by měly stanovit politiky a postupy pro zveřejňování a zpřístupnění registračních údajů, včetně dohod o úrovni služeb k vyřizování žádostí o přístup od oprávněných žadatelů o přístup. Postup poskytování přístupu může také obsahovat užívání rozhraní, portálu nebo jiného technického nástroje k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům. Za účelem podpory harmonizovaných postupů na vnitřním trhu může Komise přijmout pokyny o takových postupech, aniž jsou dotčeny pravomoci Evropského sboru pro ochranu osobních údajů.

(63) Všechny základní a důležité subjekty podle této směrnice by měly podléhat pravomoci členského státu, ve kterém poskytují své služby. Poskytuje-li subjekt služby ve více než jednom členském státě, měl by podléhat samostatné a souběžné pravomoci každého z těchto členských států. Příslušné orgány těchto členských států by měly spolupracovat, poskytovat si navzájem pomoc a v případě potřeby provádět společné akce v oblasti dohledu.

(64) S cílem zohlednit přeshraniční povahu služeb a činností poskytovatelů služeb systému doménových jmen, registrů internetových domén nejvyšší úrovně, poskytovatelů sítí pro doručování obsahu, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center a poskytovatelů digitálních služeb by pravomoc nad těmito subjekty měl mít pouze jeden členský stát. Pravomoc by měl mít ten členský stát, v němž má daný subjekt v rámci Unie hlavní místo obchodní činnosti. Kritérium místa obchodní činnosti pro účely této směrnice předpokládá účinný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem. To, zda je toto kritérium splněno, by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou hlavního místa obchodní činnosti, a tudíž ani nejsou rozhodujícími kritérii pro jeho určení. Hlavní místo obchodní činnosti by mělo být místo v Unii, kde jsou přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa společnosti v Unii. Pokud taková rozhodnutí nejsou v Unii přijímána, mělo by se mít za to, že hlavní místo obchodní činnosti je v členském státě, ve kterém má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud jsou služby prováděny skupinou podniků, mělo by se za hlavní místo obchodní činnosti skupiny podniků považovat hlavní místo obchodní činnosti řídícího podniku.

(65) V případech, kdy poskytovatel služeb systému doménových jmen, registr internetových domén nejvyšší úrovně, poskytovatel sítí pro doručování obsahu,

[25] Viz 14. bod odůvodnění NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679, kde se uvádí, že „toto nařízení se nevztahuje na zpracování osobních údajů právnických osob, a zejména podniků vytvořených jako právnické osoby, včetně názvu, právní formy a kontaktních údajů právnické osoby“.

poskytovatel služeb cloud computingu, poskytovatel služeb datových center a poskytovatel digitálních služeb usazený mimo Unii nabízí služby v rámci Unie, měl by ustanovit svého zástupce. Aby bylo možno určit, zda takový subjekt nabízí služby v rámci Unie, mělo by být ověřeno, zda má dotyčný subjekt zjevně v úmyslu nabízet služby osobám v jednom nebo více členských státech. Pouhá dostupnost internetových stránek subjektu nebo jeho zprostředkovatele v Unii nebo dostupnost e-mailové adresy a dalších kontaktních údajů nebo používání jazyka obecně používaného ve třetí zemi, v níž je subjekt usazen, k ověření tohoto úmyslu nepostačují. Avšak faktory jako používání jazyka nebo měny obecně používaných v jednom nebo více členských státech, spolu s možností objednat služby v tomto jiném jazyce, nebo zmínka o zákaznících či uživatelích nacházejících se v Unii mohou být zjevným dokladem o tom, že subjekt má v úmyslu nabízet služby v rámci Unie. Zástupce by měl jednat jménem subjektu a příslušné orgány nebo týmy CSIRT by měly být oprávněny zástupce kontaktovat. Zástupce by měl být výslovně písemně pověřen subjektem, aby mohl jednat jeho jménem v otázkách jeho povinností podle této směrnice, včetně hlášení incidentů.

(66) Pokud jsou podle ustanovení této směrnice vyměňovány, hlášeny nebo jinak sdíleny informace, které jsou podle unijních nebo vnitrostátních předpisů považovány za utajované, měla by se použít odpovídající zvláštní pravidla o nakládání s utajovanými informacemi.

(67) S tím, jak se kybernetické hrozby stávají stále složitějšími a sofistikovanějšími, účinná opatření v oblasti odhalování a prevence závisejí do značné míry na pravidelném sdílení zpravodajských informací o hrozbách a zranitelnosti mezi subjekty. Sdílení informací přispívá k lepšímu povědomí o kybernetických hrozbách, což následně posiluje schopnost subjektů předcházet tomu, že tyto hrozby přerostou ve skutečné incidenty, a umožňuje subjektům lépe zachycovat dopady incidentů a efektivněji se zotavovat. Při neexistenci vedení na úrovni Unie, jak se zdá, bránily takovému sdílení zpravodajských informací některé faktory, a zejména nejistota ohledně slučitelnosti s pravidly hospodářské soutěže a pravidly odpovědnosti.

(68) Subjekty by měly být motivovány k tomu, aby společně využívaly pákového efektu svých individuálních znalostí a praktických zkušeností na strategické, taktické a operativní úrovni a tím posílit své schopnosti odpovídajícím způsobem posuzovat a sledovat kybernetické hrozby, bránit se jim a reagovat na ně. Je proto nezbytné umožnit vznik mechanismů na úrovni Unie pro dobrovolná ujednání o sdílení informací. Členské státy by za tímto účelem měly aktivně podporovat a motivovat také relevantní subjekty, jež nespadají do oblasti působnosti této směrnice, aby se účastnily takovýchto mechanismů pro sdílení informací. Tyto mechanismy by měly fungovat v plném souladu s pravidly Unie v oblasti hospodářské soutěže a s právními předpisy Unie o ochraně údajů.

(69) Zpracování osobních údajů v rozsahu nezbytně nutném a přiměřeném pro zajištění bezpečnosti sítí a informací ze strany subjektů, které provádějí orgány veřejné správy, týmy CERT, týmy CSIRT a poskytovatelé bezpečnostních technologií a služeb, by mělo představovat oprávněný zájem dotčeného správce údajů podle nařízení (EU) 2016/679. To by mělo zahrnovat opatření týkající se prevence, odhalování a analýzy incidentů a reakce na incidenty, opatření ke zvyšování povědomí o konkrétních kybernetických hrozbách, výměnu informací v rámci odstraňování a koordinovaného odhalování zranitelných míst, a také dobrovolnou výměnu informací o těchto incidentech, kybernetických hrozbách a zranitelných místech, indikátorech narušení, taktice, technikách a postupech, varováních v oblasti kybernetické bezpečnosti a

konfiguračních nástrojích. Taková opatření mohou vyžadovat zpracovávání těchto druhů osobních údajů: IP adres, jednotných adres zdroje (URL), doménových jmen a e-mailových adres.

(70) S cílem posílit pravomoci a činnosti dohledu, které pomáhají zajistit účinný soulad s předpisy, by tato směrnice měla stanovit minimální seznam opatření a prostředků dohledu, jejichž prostřednictvím mohou příslušné orgány uskutečňovat dohled nad základními a důležitými subjekty. Tato směrnice by kromě toho měla zavést rozlišení režimů dohledu mezi základními a důležitými subjekty s cílem zajistit spravedlivou rovnováhu povinností pro oba druhy subjektů a příslušné orgány. Základní subjekty by tak měly podléhat plnohodnotnému režimu dohledu (dohled *ex ante* a *ex post*), zatímco důležité subjekty by měly podléhat mírnému režimu dohledu, pouze dohledu *ex post*. Mírný režim znamená, že důležité subjekty by neměly systematicky dokumentovat soulad s požadavky na řízení kybernetických bezpečnostních rizik a příslušné orgány by měly provádět reaktivní *ex post* přístup k dohledu, a neměly by tedy obecnou povinnost dohlížet na tyto subjekty.

(71) K zajištění účinného vymáhání by měl být stanoven minimální seznam správních sankcí za porušení povinnosti v oblasti řízení kybernetických bezpečnostních rizik a hlášení, jež stanoví tato směrnice, čímž se vytvoří jasný a jednotný rámec pro takové sankce v celé Unii. Náležitá pozornost by měla být věnována povaze, závažnosti a době trvání protiprávního jednání, skutečné způsobené škodě či ztrátám nebo potenciálním škodám či ztrátám, které mohly být vyvolány, úmyslné nebo nedbalostní povaze protiprávního jednání, opatřením přijatým za účelem prevence nebo zmenšení způsobené škody nebo ztrát, míře odpovědnosti nebo jakémukoli relevantnímu protiprávnímu jednání v minulosti, míře spolupráce s příslušným orgánem a jakýmkoli jiným přitěžujícím nebo polehčujícím faktorům. Uložení sankcí včetně správních pokut by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listinou základních práv Evropské unie, včetně účinné právní ochrany a spravedlivého procesu.

(72) S cílem zajistit účinné vymáhání povinností stanovených v této směrnici by každý příslušný orgán měl mít pravomoc ukládat správní pokuty nebo požadovat uložení správních pokut.

(73) Jsou-li správní pokuty uloženy podniku, měl by se podnikem pro tyto účely rozumět podnik v souladu s články 101 a 102 SFEU. Jsou-li správní pokuty uloženy osobám, které nejsou podnikem, měl by dozorový úřad při rozhodování o odpovídající výši pokuty zohlednit obecnou úroveň příjmů v daném členském státě, jakož i ekonomickou situaci dané osoby. Mělo by být ponecháno na členských státech, aby určily, zda a v jaké míře by měly správním pokutám podléhat orgány veřejné správy. Uložením správní pokuty není dotčeno uplatnění jiných pravomocí příslušných orgánů nebo jiných sankcí stanovených ve vnitrostátních pravidlech provádějících tuto směrnici.

(74) Členským státům by mělo být umožněno, aby stanovily pravidla týkající se trestních sankcí za porušení vnitrostátních pravidel provádějících tuto směrnici. Uložení trestních sankcí za porušení těchto vnitrostátních pravidel a souvisejících správních sankcí by však nemělo vést k porušení zásady *ne bis in idem*, jak ji vykládá Soudní dvůr.

(75) Nejsou-li správní sankce harmonizovány touto směrnicí nebo v případě potřeby v jiných případech, jako jsou závažná porušení povinností stanovených v této směrnici, měly by členské státy zavést systém, který zajistí uložení účinných,

přiměřených a odrazujících sankcí. Povaha těchto trestních nebo správních sankcí by měla být stanovena právem členského státu.

(76) Aby se dále posílila účinnost a odrazující účinek sankcí, jež mají být uloženy za porušení povinností stanovených podle této směrnice, měly by být příslušné orgány oprávněny uplatňovat sankce spočívající v pozastavení osvědčení nebo povolení týkajícího se části nebo všech služeb, jež poskytuje základní subjekt, a uložení dočasného zákazu výkonu řídící funkce fyzické osoby. Vzhledem k závažnosti a dopadu těchto sankcí na činnost subjektů a v konečném důsledku na jejich zákazníky, měly by být uplatňovány pouze úměrně závažnosti porušení a s ohledem na konkrétní okolnosti každého případu, včetně úmyslné nebo nedbalostní povahy porušení, opatřením přijatým k zamezení nebo zmírnění způsobené škody nebo ztrát. Tyto sankce by se měly používat jen jako krajní prostředek, což znamená pouze po vyčerpání ostatních relevantních donucovacích opatření, jež stanoví tato směrnice, a pouze po dobu, než subjekty, vůči kterým jsou uplatněny, přijmou nezbytná opatření k nápravě nedostatků nebo k dosažení souladu s požadavky příslušného orgánu, kvůli kterým byly tyto sankce uloženy. Uložení takových sankcí musí podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny základních práv Evropské unie, včetně účinné právní ochrany, spravedlivého procesu, presumpce neviny a práva na obhajobu.

(77) Tato směrnice by měla stanovit pravidla spolupráce mezi příslušnými orgány a orgány dohledu v souladu s nařízením (EU) 2016/679 pro řešení případů porušení souvisejících s osobními údaji.

(78) Cílem této směrnice by mělo být zajištění vysoké míry odpovědnosti za opatření v oblasti řízení kybernetických bezpečnostních rizik a povinností v oblasti podávání zpráv na úrovni organizací. Z těchto důvodů by vedoucí orgány subjektů, jež spadají do oblasti působnosti této směrnice, měly schválit opatření pro řízení kybernetických bezpečnostních rizik a dohlížet na jejich provádění.

(79) Měl by být zaveden mechanismus vzájemného hodnocení, který umožní, aby provádění politik kybernetické bezpečnosti, včetně úrovně schopností a dostupných zdrojů členských států, posuzovali odborníci určení členskými státy.

(80) Za účelem zohlednění nových kybernetických hrozeb, technologického vývoje nebo odvětvových zvláštností by Komisi měla být svěřena pravomoc přijmout akty v souladu s článkem 290 SFEU, pokud jde o prvky související s opatřeními v oblasti řízení rizik, jež vyžaduje tato směrnice. Komise by rovněž měla být zmocněna přijmout akty v přenesené pravomoci, jimiž stanoví, které kategorie základních subjektů budou povinny získat osvědčení a podle kterých konkrétních evropských systémů certifikace kybernetické bezpečnosti. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[26]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na zasedání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

[26] Úř. věst. L 123, 12.5.2016, s. 1.

(81) Za účelem zajištění jednotných podmínek k provedení příslušných ustanovení této směrnice týkajících se procesních opatření nezbytných pro fungování skupiny pro spolupráci, technických prvků opatření k řízení rizik nebo druhu informací, formátu a postupu oznamování incidentů by Komisi měly být svěřeny prováděcí pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011[27].

(82) Komise by měla provádět pravidelný přezkum této směrnice za konzultace se zainteresovanými stranami, zejména pokud jde o nutnost změn s ohledem na měnící se společenské, politické, technologické nebo tržní podmínky.

(83) Jelikož cíle této směrnice, totiž dosažení vysoké společné úrovně kybernetické bezpečnosti v Unii, nemůže být uspokojivě dosaženo členskými státy, ale spíše jich z důvodu účinků této směrnice může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje tato směrnice rámec toho, co je pro dosažení tohoto cíle nezbytné.

(84) Tato směrnice dodržuje základní práva a ctí zásady uznané Listinou základních práv Evropské unie, zejména právo na respektování soukromého života a komunikace, právo na ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní ochranu a spravedlivý proces. Tato směrnice by měla být prováděna v souladu s těmito právy a zásadami,

PŘIJALY TUTO SMĚRNICI:

KAPITOLA I

Obecná ustanovení

Článek 1

Předmět

1. Touto směrnicí se stanoví opatření pro zajištění vysoké společné úrovně kybernetické bezpečnosti v rámci Unie.

2. Za tímto účelem tato směrnice:

   a) ukládá členským státům povinnost přijmout národní strategie kybernetické bezpečnosti, určit příslušné vnitrostátní orgány, jednotná kontaktní místa a bezpečnostní týmy typu CSIRT (týmy CSIRT);

   b) stanoví povinnost řízení rizik v oblasti kybernetické bezpečnosti a oznamovací povinnost pro subjekty druhu, který je v příloze I označován za základní a v příloze II za důležitý;

   c) stanoví povinnosti týkající se sdílení informací o kybernetické bezpečnosti.

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

Článek 2

Oblast působnosti

1. Tato směrnice se vztahuje na veřejné a soukromé subjekty druhu, který je v příloze I označován za základní a v příloze II za důležitý. Tato směrnice se nevztahuje na subjekty, které splňují definici mikropodniků a malých podniků ve smyslu doporučení Komise 2003/361/ES[28].

2. Tato směrnice se však vztahuje také na subjekty uvedené v přílohách I a II bez ohledu na jejich velikost, pokud:

   a) jsou služby poskytovány jedním z těchto subjektů:

      i) veřejnými sítěmi elektronických komunikací nebo veřejně dostupnými službami elektronických komunikací uvedenými v bodě 8 přílohy I;

      ii) poskytovateli služeb vytvářejících důvěru uvedenými v bodě 8 přílohy I;

      iii) poskytovateli služeb registrů internetových domén nejvyšší úrovně a systému doménových jmen uvedenými v bodě 8 přílohy I;

   b) je subjekt orgánem veřejné správy podle definice uvedené v čl. 4 bodě 23;

   c) je subjekt výhradním dodavatelem služeb v členském státě;

   d) by možné narušení služby poskytované tímto subjektem mohlo mít vliv na veřejný pořádek, veřejnou bezpečnost nebo ochranu zdraví;

   e) by možné narušení služby poskytované tímto subjektem mohlo vyvolat systémová rizika, zejména pro ta odvětví, kde by takové narušení mohlo mít přeshraniční dopad;

   f) je subjekt kritický vzhledem ke svému specifickému významu na regionální nebo vnitrostátní úrovni pro konkrétní odvětví nebo druh služby nebo pro jiná vzájemně závislá odvětví v členském státě;

   g) je subjekt označen za kritický podle směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX[29] [směrnice o odolnosti kritických subjektů] nebo za subjekt rovnocenný kritickému subjektu podle článku 7 této směrnice.

   Členské státy stanoví seznam subjektů určených podle písmen b) až f) a předloží jej je do [6 měsíců po uplynutí lhůty pro provedení] Komisi. Členské státy tento seznam pravidelně přezkoumávají, a to alespoň každé dva roky od předložení, a v případě potřeby jej aktualizují.

3. Touto směrnicí není dotčena příslušnost členských států, pokud jde o udržování veřejné bezpečnosti, obranu a národní bezpečnost v souladu s právem Unie.

4. Touto směrnicí nejsou dotčeny směrnice Rady 2008/114/ES[30] a směrnice Evropského parlamentu a Rady 2011/93/EU[31] a 2013/40/EU[32].

---

28 Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

29 *[vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]*

30 Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Úř. věst. L 345, 23.12.2008, s. 75).

5. Aniž je dotčen článek 346 Smlouvy o fungování EU, se informace, které jsou důvěrné podle unijních a vnitrostátních pravidel, jako jsou pravidla pro zachovávání důvěrnosti obchodních informací, vyměňují s Komisí a jinými příslušnými orgány pouze v případě, že je tato výměna nutná pro účely této směrnice. Vyměňované informace se omezí na informace, které jsou relevantní a přiměřené účelu této výměny. Při těchto výměnách informací se zachovává důvěrnost předmětných informací a jsou chráněny bezpečnost a obchodní zájmy základních nebo důležitých subjektů.

6. Pokud ustanovení právních aktů Unie pro konkrétní odvětví vyžadují, aby základní nebo důležité subjekty přijaly opatření k řízení rizik v oblasti kybernetické bezpečnosti nebo aby oznamovaly incidenty či významné kybernetické hrozby, a pokud je účinek těchto opatření alespoň rovnocenný účinku povinností stanovených v této směrnici, příslušná ustanovení této směrnice, včetně ustanovení o dohledu a vymáhání v kapitole VI, se neuplatní.

Článek 3

Minimální harmonizace

Aniž jsou dotčeny jiné povinnosti členských států podle práva Unie, mohou členské státy v souladu s touto směrnicí přijímat nebo ponechat v platnosti ustanovení zajišťující vyšší úroveň kybernetické bezpečnosti.

Článek 4

Definice

Pro účely této směrnice se rozumí:

1) „sítí a informačním systémem“:

   a) síť elektronických komunikací ve smyslu čl. 2 bodu 1 směrnice (EU) 2018/1972;

   b) zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování digitálních dat;

   c) digitální data, jež jsou prvky uvedenými v písmeni a) a b) uchovávána, zpracovávána, opětovně vyhledávána nebo předávána za účelem jejich provozu, použití, ochrany a údržby;

2) „bezpečností sítí a informačních systémů“ schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo

---

[31] Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV (Úř. věst. L 335, 17.12.2011, s. 1).

[32] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV (Úř. věst. L 218, 14.8.2013, s. 8).

zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné;

3) „kybernetickou bezpečností“ kybernetická bezpečnost ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady 2019/881[33];

4) „národní strategií kybernetické bezpečnosti“ soudržný rámec členského státu vymezující strategické cíle a priority v oblasti bezpečnosti sítí a informačních systémů v tomto členském státě;

5) „incidentem“ jakákoli událost narušující dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které nabízejí sítě a informační systémy nebo které jsou jejich prostřednictvím přístupné;

6) „řešením incidentu“ veškeré akce a postupy, jejichž cílem je incident odhalit, analyzovat, zamezit jeho šíření a reagovat na něj;

7) „kybernetickou hrozbou“ kybernetická hrozba ve smyslu čl. 2 bodu 8 nařízení (EU) č. 2019/881;

8) „zranitelností“ slabá stránka, snížená odolnost nebo chyba prostředku, systému, procesu nebo kontroly, která může být využita kybernetickou hrozbou;

9) „zástupcem“ fyzická či právnická osoba usazená v Unii, výslovně pověřená, aby jednala jménem i) poskytovatele služeb DNS, registru internetových domén nejvyšší úrovně (TLD), poskytovatele služby cloud computingu, poskytovatele služeb datového centra, poskytovatele sítě pro doručování obsahu podle bodu 8 přílohy I nebo ii) subjektů uvedených v bodě 6 přílohy II, které v Unii usazeny nejsou, přičemž vnitrostátní příslušný orgán nebo tým CSIRT může se zástupcem jednat namísto subjektu, pokud jde o povinnosti tohoto subjektu vyplývající z této směrnice;

10) „normou“ norma ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 1025/2012[34];

11) „technickou specifikací“ technická specifikace ve smyslu čl. 2 bodu 4 nařízení (EU) č. 1025/2012;

12) „výměnným uzlem internetu (IXP)“ síťové zařízení umožňující propojení více než dvou nezávislých sítí (autonomních systémů), a to primárně pro účely usnadnění výměny dat zasílaných prostřednictvím internetu; výměnný uzel internetu poskytuje propojení pouze autonomním systémům; výměnný uzel internetu nevyžaduje, aby data zasílaná prostřednictvím internetu mezi kterýmikoli dvěma zúčastněnými autonomními systémy procházela přes jakýkoli třetí autonomní systém, ani zasílaná data nemění ani žádným jiným způsobem do jejich zasílání nezasahuje;

---

33 Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

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

13) „systémem doménových jmen (DNS)“ hierarchický distribuovaný systém doménových jmen, který umožňuje koncovým uživatelům přístup ke službám a zdrojům na internetu;

14) „poskytovatelem služeb systému doménových jmen (DNS)“ subjekt, který poskytuje rekurzívní nebo autoritativní služby pro překlad doménových jmen koncovým uživatelům internetu a dalším poskytovatelům služeb DNS;

15) „registrem internetových domén nejvyšší úrovně“ subjekt, kterému byla delegována konkrétní TLD a je odpovědný za správu TLD, včetně registrace doménových jmen v rámci TLD a technického provozu TLD, včetně provozu jejích jmenných serverů, vedení jejích databází a distribuce souborů zón TLD mezi jmennými servery;

16) „digitální službou“ služba ve smyslu čl. 1 odst. 1 písm. b) směrnice Evropského parlamentu a Rady (EU) 2015/1535[35];

17) „on-line tržištěm“ digitální služba ve smyslu čl. 2 písm. n) směrnice Evropského parlamentu a Rady 2005/29/ES[36];

18) „internetovým vyhledávačem“ digitální služba ve smyslu čl. 2 odst. 5) nařízení Evropského parlamentu a Rady (EU) 2019/1150[37];

19) „službou cloud computingu“ digitální služba umožňující správu na vyžádání a široký dálkový přístup k rozšiřitelnému a přizpůsobitelnému úložišti distribuovaných výpočetních zdrojů, které je možno sdílet;

20) „službou datového centra“ služba, která zahrnuje struktury nebo skupiny struktur určené k centralizovanému umístění, propojení a provozu zařízení informační technologie a sítě, poskytující služby ukládání, zpracování a přepravy dat společně se všemi zařízeními a infrastrukturami pro distribuci energie a řízení prostředí;

21) „sítí pro doručování obsahu“ síť geograficky distribuovaných serverů za účelem zajištění vysoké dostupnosti, přístupnosti nebo rychlého poskytování digitálního obsahu a služeb uživatelům internetu jménem poskytovatelů obsahu a služeb;

22) „platformou sociálních sítí“ platforma, která koncovým uživatelům umožňuje vzájemné propojení, sdílení, objevování a komunikaci napříč různými zařízeními, zejména prostřednictvím chatů, příspěvků, videí a doporučení;

23) „subjektem veřejné správy“ subjekt v členském státě, který splňuje tato kritéria:

    (a) je založen za účelem naplňování potřeb veřejného zájmu a nemá průmyslovou nebo obchodní povahu;

    (b) má právní subjektivitu;

---

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

36 Směrnice Evropského parlamentu a Rady 2005/29/ES ze dne 11. května 2005 o nekalých obchodních praktikách vůči spotřebitelům na vnitřním trhu a o změně směrnice Rady 84/450/EHS, směrnic Evropského parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nařízení Evropského parlamentu a Rady (ES) č. 2006/2004 („směrnice o nekalých obchodních praktikách“) (Úř. věst. L 149, 11.6.2005, s. 22).

37 Nařízení Evropského parlamentu a Rady (EU) 2019/1150 ze dne 20. června 2019 o podpoře spravedlnosti a transparentnosti pro podnikatelské uživatele online zprostředkovatelských služeb (Úř. věst. L 186, 11.7.2019, s. 57).

(c) je financován převážně státem, regionálními orgány nebo jinými veřejnoprávními subjekty; nebo podléhá řídicímu dohledu těchto orgánů nebo subjektů; nebo v jehož správním, řídicím nebo dozorčím orgánu je více než polovina členů jmenována státem, regionálními orgány nebo jinými veřejnoprávními subjekty;

(d) má pravomoc vydávat fyzickým nebo právnickým osobám správní nebo regulační rozhodnutí ovlivňující jejich práva při přeshraničním pohybu osob, zboží, služeb nebo kapitálu.

Subjekty veřejné správy, které vykonávají činnosti v oblasti veřejné bezpečnosti, vymáhání práva, obrany nebo národní bezpečnosti, jsou vyloučeny.

24) „subjektem“ jakákoli fyzická nebo právnická osoba vytvořená a uznaná jako taková podle vnitrostátních právních předpisů v místě svého usazení, která může svým jménem vykonávat práva a podléhat povinnostem;

25) „základním subjektem“ jakýkoli subjekt druhu, který je v příloze I označován za základní subjekt;

26) „důležitým subjektem“ jakýkoli subjekt druhu, který je v příloze II označován za důležitý subjekt.

KAPITOLA II

Koordinované regulační rámce kybernetické bezpečnosti

Článek 5
Národní strategie kybernetické bezpečnosti

1. Každý členský stát přijme národní strategii kybernetické bezpečnosti, ve které vymezí strategické cíle a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji. Národní strategie kybernetické bezpečnosti zahrnuje zejména:

a) definici cílů a priorit strategie kybernetické bezpečnosti členských států;

b) správní rámec pro naplnění těchto cílů a priorit, včetně politik uvedených v odstavci 2 a úloh a povinností veřejných orgánů a subjektů i dalších relevantních subjektů;

c) hodnocení za účelem určení relevantních zařízení a kybernetických rizik v tomto členském státě;

d) určení opatření zajišťujících připravenost, reakci a obnovu při incidentech, včetně spolupráce veřejného a soukromého sektoru;

e) seznam různých orgánů a subjektů zapojených do provádění národní strategie kybernetické bezpečnosti;

f) politický rámec pro lepší koordinaci mezi příslušnými orgány podle této směrnice a směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX[38]

[38] *[vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]*

[směrnice o odolnosti kritických subjektů] pro účely sdílení informací o incidentech a kybernetických hrozbách pro výkon úkolů v oblasti dohledu.

2. V rámci národní strategie kybernetické bezpečnosti přijmou členské státy zejména tyto politiky:

   a) politiku zabývající se kybernetickou bezpečností v dodavatelském řetězci pro produkty a služby IKT využívané základními a důležitými subjekty k poskytování služeb;

   b) pokyny týkající se zařazení a specifikace požadavků na kybernetickou bezpečnost produktů a služeb IKT při zadávání veřejných zakázek;

   c) politiku za účelem prosazování a usnadňování koordinovaného odhalování zranitelných míst ve smyslu článku 6;

   d) politiku týkající se udržení celkové dostupnosti a integrity veřejného jádra otevřeného internetu;

   e) politiku za účelem prosazování a rozvíjení dovedností v oblasti kybernetické bezpečnosti, zvyšování informovanosti a výzkumných a vývojových iniciativ;

   f) politiku za účelem podpory akademických a výzkumných institucí při vývoji nástrojů kybernetické bezpečnosti a zabezpečené síťové infrastruktury;

   g) politiku, příslušné postupy a vhodné nástroje pro sdílení informací na podporu dobrovolného sdílení informací týkajících se kybernetické bezpečnosti mezi podniky v souladu s právem Unie;

   h) politiku řešící zvláštní potřeby malých a středních podniků, zejména těch, které nespadají do oblasti působnosti této směrnice, v souvislosti s pokyny a podporou při zlepšování jejich odolnosti vůči kybernetickým hrozbám.

3. Členské státy oznámí své národní strategie kybernetické bezpečnosti Komisi do tří měsíců od jejich přijetí. Členské státy mohou z oznámení vyloučit konkrétní informace, pokud je to naprosto nezbytné pro zachování národní bezpečnosti.

4. Členské státy posuzují své národní strategie kybernetické bezpečnosti alespoň každé čtyři roky podle klíčových ukazatelů výkonnosti a v případě potřeby je změní. Při zpracování národní strategie a klíčových ukazatelů výkonnosti pro posouzení strategie poskytuje členským státům na jejich žádost součinnost Evropská agentura pro bezpečnost sítí a informací (ENISA).

Článek 6

Koordinované zveřejňování informací o zranitelnostech a Evropský registr zranitelností

1. Každý členský stát určí jeden ze svých týmů CSIRT podle článku 9 jako koordinátora za účelem koordinovaného zveřejňování informací o zranitelnostech. Tento určený tým CSIRT vystupuje jako důvěryhodný zprostředkovatel, který v případě potřeby usnadňuje interakci mezi oznamujícím subjektem a výrobcem nebo poskytovatelem produktů nebo služeb IKT. Pokud se hlášená zranitelnost týká více výrobců nebo poskytovatelů produktů nebo služeb IKT v celé Unii, spolupracuje určený tým CSIRT z každého členského státu v rámci sítě CSIRT.

2. Agentura ENISA vytvoří a spravuje Evropský registr zranitelností. Za tímto účelem ENISA zřídí a spravuje informační systémy, politiky a postupy s cílem zejména

umožnit důležitým a základním subjektům a jejich dodavatelům sítí a informačních systémů odhalovat a registrovat zranitelná místa v produktech nebo službách IKT a poskytovat přístup k informacím o těchto zranitelnostech uvedeným v registru všem zúčastněným stranám. V registru jsou zejména uvedeny informace popisující slabé místo, dotčený produkt IKT nebo služby IKT a závažnost této zranitelnosti z hlediska okolností, za nichž může být využita, dostupnost příslušných oprav, a pokud opravy nejsou dostupné, pokyny pro uživatele zranitelných produktů a služeb, jak mohou být rizika vyplývající z odhalených slabých míst zmírněna.

Článek 7

Národní rámce krizového řízení kybernetické bezpečnosti

1. Každý členský stát určí jeden nebo více příslušných orgánů odpovědných za řešení rozsáhlých incidentů a krizí. Členské státy zajistí, aby příslušné orgány disponovaly odpovídajícími zdroji pro účinné a efektivní plnění svěřených úkolů.

2. Každý členský stát určí kapacity, prostředky a postupy, které mohou být nasazeny v případě krize pro účely této směrnice.

3. Každý členský stát přijme národní plán reakce na krizi a kybernetické bezpečnostní incidenty, v němž budou stanoveny cíle a způsoby řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí. V plánu se stanoví zejména:

   a) cíle vnitrostátních opatření a činností v oblasti připravenosti;

   b) úkoly a odpovědnost příslušných vnitrostátních orgánů;

   c) postupy krizového řízení a kanály pro výměnu informací;

   d) opatření v oblasti připravenosti včetně nácviku a školení;

   e) příslušné veřejné a soukromé zúčastněné strany a zapojená infrastruktura;

   f) vnitrostátní postupy a ujednání mezi příslušnými vnitrostátními orgány a subjekty, aby byla zajištěna účinná účast členského státu a podpora koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na úrovni Unie.

4. Členské státy oznámí Komisi své určené příslušné orgány podle odstavce 1 a předloží své národní plány reakce na kybernetické bezpečnostní incidenty a krize podle odstavce 3 do tří měsíců od tohoto určení a přijetí těchto plánů. Členské státy mohou z plánu vyloučit konkrétní informace, pokud je to naprosto nezbytné pro jejich národní bezpečnost.

Článek 8

Vnitrostátní příslušné orgány a jednotná kontaktní místa

1. Každý členský stát určí jeden nebo více příslušných orgánů odpovědných za kybernetickou bezpečnost a úkoly dohledu podle kapitoly VI této směrnice. Členské státy tím mohou pověřit stávající orgán nebo stávající orgány.

2. Příslušné orgány podle odstavce 1 dohlížejí na provádění této směrnice na vnitrostátní úrovni.

3. Každý členský stát určí jedno vnitrostátní jednotné kontaktní místo pro kybernetickou bezpečnost („jednotné kontaktní místo“). Určí-li členský stát pouze jeden příslušný orgán, je tento orgán rovněž jednotným kontaktním místem pro tento členský stát.

4. Každé jednotné kontaktní místo plní styčnou funkci pro účely přeshraniční spolupráce orgánů svého členského státu s příslušnými orgány v jiných členských státech a také meziodvětvové spolupráce s jinými příslušnými vnitrostátními orgány ve svém členském státě.

5. Členské státy zajistí, aby příslušné orgány podle odstavce 1 a jednotná kontaktní místa disponovaly odpovídajícími zdroji pro účinné a účelné plnění svěřených úkolů, a tím pro naplnění cílů této směrnice. Členské státy zajistí, aby jimi jmenovaní zástupci ve skupině pro spolupráci podle článku 12 účelně, účinně a spolehlivě spolupracovali.

6. Každý členský stát Komisi neprodleně oznámí určení příslušného orgánu podle odstavce 1 a jednotného kontaktního místa uvedeného v odstavci 3, jejich úkoly a jakékoli změny, které se jich týkají. Každý členský stát určení příslušného orgánu a jednotného kontaktního místa zveřejní. Komise zveřejní seznam určených jednotných kontaktních míst.

Článek 9

Bezpečnostní týmy typu CSIRT

1. Každý členský stát zřídí jeden nebo více bezpečnostních týmů typu CSIRT, které splňují požadavky uvedené v čl. 10 odst. 1, pokrývají alespoň odvětví, pododvětví nebo subjekty uvedené v přílohách I a II a jsou odpovědné za řešení incidentů podle řádně vymezeného postupu. Tým CSIRT může být zřízen v rámci příslušného orgánu uvedeného v článku 8.

2. Členské státy zajistí, aby měl každý tým CSIRT odpovídající zdroje pro účinné plnění svých úkolů podle čl. 10 odst. 2.

3. Členské státy zajistí, aby měl každý tým CSIRT k dispozici přístup k odpovídající, bezpečné a odolné komunikační a informační infrastruktuře pro výměnu informací se základními a důležitými subjekty a dalšími příslušnými zúčastněnými stranami. Za tímto účelem členské státy zajistí, aby týmy CSIRT přispívaly k zavedení nástrojů pro bezpečné sdílení informací.

4. Týmy CSIRT spolupracují a ve vhodných případech si vyměňují příslušné informace podle článku 26 s důvěryhodnými odvětvovými nebo meziodvětvovými komunitami základních a důležitých subjektů.

5. Týmy CSIRT se účastní vzájemného hodnocení pořádaného v souladu s článkem 16.

6. Členské státy zajistí, aby jejich týmy CSIRT v rámci sítě CSIRT uvedené v článku 13 účelně, účinně a spolehlivě spolupracovaly.

7. Členské státy bez zbytečného odkladu oznámí Komisi týmy CSIRT určené podle odstavce 1, koordinátora CSIRT určeného podle čl. 6 odst. 1 a jejich úkoly stanovené v souvislosti se subjekty uvedenými v přílohách I a II.

8. Členské státy si mohou při vytváření týmů CSIRT vyžádat pomoc agentury ENISA.

Článek 10

Požadavky na týmy CSIRT a jejich úkoly

1. Týmy CSIRT musí splňovat tyto požadavky:

   a) týmy CSIRT zajistí, aby v jejich komunikačních službách nebyla žádná kritická místa (tzv. single points of failure), a tyto služby tak byly široce dostupné, a disponují několika způsoby, jimiž budou kontaktovat ostatní a jimiž bude možné kontaktovat je, a to kdykoli. Týmy CSIRT jednoznačně specifikují komunikační kanály a oznámí je spolupracujícím partnerům a subjektům spadajícím do jejich působnosti;

   b) pracoviště týmů CSIRT a jejich podpůrné informační systémy se nacházejí na bezpečném místě;

   c) týmy CSIRT jsou vybaveny vhodným systémem řízení a směrování požadavků, zejména pro usnadnění účelného a efektivního předávání;

   d) týmy CSIRT jsou náležitě personálně obsazeny tak, aby byly kdykoli k dispozici;

   e) týmy CSIRT jsou vybaveny redundantními systémy a záložním pracovním prostorem pro zajištění kontinuity jejich služeb;

   f) týmy CSIRT musí mít možnost zapojovat se do mezinárodních sítí pro spolupráci.

2. Týmy CSIRT mají tyto úkoly:

   a) monitorování kybernetických hrozeb, zranitelností a incidentů na vnitrostátní úrovni;

   b) vydávání včasných varování a upozornění, oznamování a šíření informací o kybernetických hrozbách, zranitelnostech a incidentech základním a důležitým subjektům a dalším příslušným zúčastněným stranám;

   c) reakce na incidenty;

   d) poskytování dynamické analýzy rizik a incidentů a přehledu o situaci v oblasti kybernetické bezpečnosti;

   e) provádění aktivního skenování sítě a informačních systémů používaných k poskytování služeb subjektu, který o to požádal;

   f) účast v síti CSIRT a poskytování vzájemné pomoci dalším členům sítě na jejich žádost.

3. Týmy CSIRT navážou spolupráci s příslušnými subjekty v soukromém sektoru za účelem lepšího plnění cílů směrnice.

4. V zájmu usnadnění spolupráce prosazují týmy CSIRT přijetí a používání společných či standardních postupů, klasifikace a taxonomie v oblasti:

   a) postupů řešení incidentů;

   b) krizového řízení kybernetické bezpečnosti;

   c) koordinovaného zveřejňování informací o zranitelnostech.

Článek 11
Spolupráce na vnitrostátní úrovni

1. Pokud příslušné orgány podle článku 8, jednotné kontaktní místo a tým (týmy) CSIRT téhož členského státu existují odděleně, vzájemně spolupracují při plnění povinností stanovených touto směrnicí.

2. Členské státy zajistí, aby buď jejich příslušné orgány, nebo týmy CSIRT obdržely hlášení o incidentech a významných kybernetických hrozbách a o případech, kdy téměř došlo k incidentu, podaná podle této směrnice. Pokud členský stát rozhodne, že jeho týmy CSIRT nemají tato hlášení přijímat, bude týmům CSIRT v rozsahu nezbytném pro plnění jejich úkolů povolen přístup k údajům o incidentech hlášených základními nebo důležitými subjekty podle článku 20.

3. Každý členský stát zajistí, aby buď jejich příslušné orgány, nebo týmy CSIRT informovaly jeho jednotné kontaktní místo o hlášeních o incidentech, významných kybernetických hrozbách a případech, kdy téměř došlo k incidentu, podaných podle této směrnice.

4. V rozsahu nezbytném pro účelné plnění úkolů a povinností stanovených touto směrnicí zajistí členské státy vhodnou spolupráci mezi příslušnými orgány a jednotnými kontaktními místy a donucovacími orgány, úřady pro ochranu osobních údajů a orgány odpovědnými za kritickou infrastrukturu podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] a vnitrostátními finančními orgány určenými v souladu s nařízením Evropského parlamentu a Rady (EU) XXXX/XXXX[39] [nařízení DORA] v daném členském státě.

5. Členské státy zajistí, aby jejich příslušné orgány pravidelně poskytovaly informace příslušným orgánům určeným podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] o kybernetických bezpečnostních rizicích, kybernetických hrozbách a incidentech postihujících základní subjekty určené jako kritické nebo jako subjekty rovnocenné kritickým subjektům podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů], jakož i o opatřeních, jež příslušné orgány přijaly v reakci na tato rizika a incidenty.

KAPITOLA III

Spolupráce

Článek 12
Skupina pro spolupráci

1. S cílem podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy v oblasti uplatňování směrnice se zřizuje skupina pro spolupráci.

2. Skupina pro spolupráci vykonává své úkoly na základě dvouletých pracovních programů, jak je uvedeno v odstavci 6.

---

[39] *[vložte úplný název a údaje o vyhlášení v Úředním věstníku, až budou známy]*

3. Skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA. Činností skupiny pro spolupráci se jako pozorovatel účastní Evropská služba pro vnější činnost. Činností skupiny pro spolupráci se mohou účastnit evropské orgány dohledu v souladu s čl. 17 odst. 5 písm. c) nařízení (EU) XXXX/XXXX [nařízení DORA].

Tam, kde je to vhodné, může skupina pro spolupráci přizvat ke spolupráci zástupce příslušných zúčastněných stran.

Služby sekretariátu zajistí Komise.

4. Skupina pro spolupráci má tyto úkoly:

a) poskytovat příslušným orgánům doporučení v souvislosti s provedením této směrnice ve vnitrostátním právu a jejím uplatňováním;

b) vyměňovat si osvědčené postupy a informace související s uplatňováním této směrnice, včetně informací souvisejících s kybernetickými hrozbami, incidenty, zranitelnostmi, případy, kdy téměř došlo k incidentu, iniciativami zaměřenými na zvyšování informovanosti, školením, cvičením a dovednostmi, budováním kapacit, jakož i normami a technickými specifikacemi;

c) vyměňovat si doporučení a spolupracovat s Komisí na nových politických iniciativách v oblasti kybernetické bezpečnosti;

d) vyměňovat si doporučení a spolupracovat s Komisí na návrzích prováděcích aktů Komise nebo aktů v přenesené pravomoci přijatých podle této směrnice;

e) vyměňovat si osvědčené postupy a informace s příslušnými orgány, institucemi a jinými subjekty Unie;

f) projednávat zprávy o vzájemném hodnocení podle čl. 16 odst. 7;

g) projednávat výsledky ze společných dohledových činností v přeshraničních případech podle článku 34;

h) vydávat strategické pokyny síti CSIRT ke konkrétním novým problémům;

i) přispívat ke zlepšování schopností v oblasti kybernetické bezpečnosti v celé Unii usnadňováním výměny státních úředníků prostřednictvím programu budování kapacit zahrnujícího pracovníky z příslušných orgánů nebo týmů CSIRT v členských státech;

j) pořádat pravidelná společná setkání s příslušnými soukromými zainteresovanými stranami z celé Unie za účelem projednávání činností vykonávaných skupinou a shromažďování poznatků o nových výzvách v oblasti této politiky;

k) projednávat práci vykonávanou ve vztahu ke cvičením v oblasti kybernetické bezpečnosti, včetně práce prováděné agenturou ENISA.

5. Skupina pro spolupráci si může od sítě CSIRT vyžádat odbornou zprávu o vybraných tématech.

6. Do … [24 měsíců od data vstupu této směrnice v platnost] a poté každé dva roky vypracuje skupina pro spolupráci pracovní program týkající se akcí, jež mají být realizovány za účelem plnění jejích cílů a úkolů. Časový rámec prvního programu

přijatého podle této směrnice se sladí s časovým rámcem posledního programu přijatého podle směrnice (EU) 2016/1148.

7. Komise může přijmout prováděcí akty, kterými stanoví procesní pravidla nezbytná pro fungování skupiny pro spolupráci. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 37 odst. 2.

8. Skupina pro spolupráci se schází pravidelně, alespoň jednou ročně, se skupinou pro odolnost kritických subjektů zřízenou podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za účelem podpory strategické spolupráce a výměny informací.

Článek 13

Síť CSIRT

1. Zřizuje se síť vnitrostátních týmů CSIRT s cílem přispívat k budování důvěry mezi členskými státy a podporovat jejich rychlou a účinnou operativní spolupráci.

2. Síť CSIRT tvoří zástupci týmů CSIRT z členských států a týmu CERT–EU. Komise se účastní sítě CSIRT jako pozorovatel. Agentura ENISA zajistí služby sekretariátu a aktivně podporuje spolupráci mezi týmy CSIRT.

3. Síť CSIRT má tyto úkoly:

   a) zajišťuje výměnu informací o schopnostech týmů CSIRT;

   b) zajišťuje výměnu příslušných informací o incidentech, případech, kdy téměř došlo k incidentu, kybernetických hrozbách, rizicích a zranitelnostech;

   c) na žádost zástupce sítě CSIRT potenciálně zasaženého incidentem zajišťuje výměnu informací o tomto incidentu a souvisejících kybernetických hrozbách, rizicích a zranitelnostech;

   d) na žádost zástupce sítě CSIRT projedná a pokud možno realizuje koordinovanou reakci na incident, který byl zjištěn v oblasti spadající do pravomoci tohoto členského státu;

   e) poskytuje členským státům podporu při řešení přeshraničních incidentů podle této směrnice;

   f) spolupracuje a poskytuje součinnost určeným týmům CSIRT uvedeným v článku 6 v souvislosti s řízením vícestranného koordinovaného odhalování zranitelností postihujících více výrobců nebo poskytovatelů produktů IKT, služeb IKT a procesů IKT v různých členských státech;

   g) projednává a vymezuje další formy operativní spolupráce, a to mimo jiné ve vztahu k:

      i) kategoriím kybernetických hrozeb a incidentů;

      ii) včasným varováním;

      iii) vzájemné pomoci;

      iv) zásadám a způsobům koordinace při reakci na přeshraniční rizika a incidenty;

v) příspěvku k národnímu plánu reakce na kybernetické bezpečnostní incidenty a krizi uvedenému v čl. 7 odst. 3;

h) informuje skupinu pro spolupráci o svých činnostech a o dalších formách operativní spolupráce projednávaných podle písmene g) a v případě potřeby žádá v tomto ohledu odpovídající pokyny;

i) bilancuje cvičení v oblasti kybernetické bezpečnosti, včetně cvičení pořádaných agenturou ENISA;

j) na žádost jednotlivých týmů CSIRT jedná o jejich schopnostech a připravenosti;

k) spolupracuje a zajišťuje výměnu informací s regionálními bezpečnostními operačními středisky a bezpečnostními operačními středisky na úrovni Unie za účelem zlepšení společné informovanosti o situaci u incidentů a hrozeb v celé Unii;

l) projednává zprávy o vzájemném hodnocení podle čl. 16 odst. 7;

m) vydává pokyny s cílem usnadnit sbližování operativních postupů ve vztahu k uplatňování ustanovení tohoto článku o operativní spolupráci.

4. Pro účely přezkumu podle článku 35 a do [24 měsíců od data vstupu této směrnice v platnost] a poté každé dva roky posoudí síť CSIRT pokrok dosažený v provozní spolupráci a vypracuje zprávu. Ve zprávě se zejména uvedou závěry o výsledcích vzájemného hodnocení podle článku 16 provedeného ve vztahu k národním týmům CSIRT, včetně závěrů a doporučení podle tohoto článku. Tato zpráva bude rovněž předložena skupině pro spolupráci.

5. Síť CSIRT přijme svůj jednací řád.

Článek 14

Evropská síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe)

1. Za účelem podpory koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operační úrovni a pro zajištění pravidelné výměny informací mezi členskými státy a institucemi, orgány a agenturami Unie se tímto zřizuje Evropská síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe).

2. Síť EU-CyCLONe je tvořena zástupci orgánů krizového řízení členských států určených podle článku 7, Komise a agentury ENISA. Agentura ENISA zajišťuje služby sekretariátu a podporuje bezpečnou výměnu informací.

3. Úkoly sítě EU-CyCLONE jsou:

a) zvýšit úroveň připravenosti na řešení rozsáhlých incidentů a krizí;

b) rozvíjet společnou informovanost o důležitých událostech v oblasti kybernetické bezpečnosti;

c) koordinovat řešení rozsáhlých incidentů a krizí a podporovat rozhodování na politické úrovni týkající se těchto incidentů a krizí;

d) projednávat národní plány reakce na kybernetické bezpečnostní incidenty uvedené v čl. 7 odst. 2.

4. Síť EU-CyCLONe přijme svůj jednací řád.

5. Síť EU-CyCLONe pravidelně podává skupině pro spolupráci zprávy o kybernetických hrozbách, incidentech a trendech, se zvláštním zaměřením na jejich dopad na základní a důležité subjekty.

6. Síť EU-CyCLONe spolupracuje se sítí CSIRT podle sjednaných procesních pravidel.

Článek 15

Zpráva o stavu kybernetické bezpečnosti v Unii

1. Agentura ENISA ve spolupráci s Komisí vydává jednou za dva roky zprávu o stavu kybernetické bezpečnosti v Unii. Ve zprávě uvede zejména posouzení:

   a) vývoje kapacit v oblasti kybernetické bezpečnosti v celé Unii;

   b) technických, finančních a lidských zdrojů dostupných pro příslušné orgány a politiky v oblasti kybernetické bezpečnosti a plnění dohledových a donucovacích opatření v návaznosti na výsledky vzájemných hodnocení podle článku 16;

   c) indexu kybernetické bezpečnosti umožňující agregované posouzení úrovně vyspělosti kapacit v oblasti kybernetické bezpečnosti.

2. Ve zprávě uvede konkrétní doporučení k této oblasti politiky zaměřená na zvýšení úrovně kybernetické bezpečnosti v celé Unii a shrne zjištění za dané období z technických situačních zpráv EU v oblasti kybernetické bezpečnosti vydaných agenturou ENISA podle čl. 7 odst. 6 nařízení (EU) 2019/881.

Článek 16

Vzájemná hodnocení

1. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA stanoví nejpozději do 18 měsíců po vstupu této směrnice v platnost metodiku a obsah vzájemných hodnocení pro posuzování účelnosti politik členských států v oblasti kybernetické bezpečnosti. Hodnocení provádějí techničtí odborníci na kybernetickou bezpečnost z členských států jiných, než je posuzovaný členský stát, přičemž hodnocení zahrnují alespoň:

   i) účelnost uplatňování požadavků na řízení kybernetických bezpečnostních rizik a plnění oznamovacích povinností uvedených v článcích 18 a 20;

   ii) úroveň kapacit, včetně dostupných finančních, technických a lidských zdrojů, a účelnost plnění úkolů příslušných vnitrostátních orgánů;

   iii) provozní kapacity a účelnost týmů CSIRT;

   iv) účelnost vzájemné pomoci podle článku 34;

   v) účelnost rámce sdílení informací podle článku 26 této směrnice.

2. Metodika zahrnuje objektivní, nediskriminační, korektní a transparentní kritéria, na jejichž základě určí členské státy odborníky způsobilé provádět vzájemná hodnocení. Agentura ENISA a Komise určí odborníky, kteří se budou vzájemných hodnocení

účastnit jako pozorovatelé. Komise za podpory agentury ENISA stanoví v rámci metodiky podle odstavce 1 objektivní, nediskriminační, korektní a transparentní systém výběru a náhodného přidělování odborníků ke každému vzájemnému hodnocení.

3. O organizačních aspektech vzájemných hodnocení rozhoduje Komise za podpory agentury ENISA a po konzultaci se skupinou pro spolupráci je stanoví podle kritérií definovaných v metodice uvedené v odstavci 1. Při vzájemných hodnoceních se posuzují aspekty uvedené v odstavci 1 u všech členských států a odvětví, včetně cílené problematiky, která je specifická pro jeden nebo několik členských států nebo pro jedno nebo několik odvětví.

4. Vzájemná hodnocení zahrnují skutečné nebo virtuální návštěvy na místě i externí výměny. S ohledem na zásadu dobré spolupráce poskytnou posuzované členské státy určeným odborníkům požadované informace potřebné k posouzení kontrolovaných aspektů. Veškeré informace získané v rámci procesu vzájemného hodnocení lze použít pouze pro tento účel. Odborníci účastnící se vzájemného hodnocení nesmí sdělit žádné citlivé nebo důvěrné informace získané v průběhu tohoto hodnocení žádným třetím stranám.

5. Tytéž aspekty, které již byly v členském státě posuzovány, nepodléhají v tomto členském státě v průběhu dvou let po ukončení vzájemného hodnocení dalšímu posuzování, pokud Komise po konzultaci s agenturou ENISA a skupinou pro spolupráci nerozhodne jinak.

6. Členský stát zajistí, aby byly ostatní členské státy, Komise a agentura ENISA bez zbytečného odkladu informovány o případném riziku střetu zájmů týkajícím se určených odborníků.

7. Odborníci účastnící se vzájemných hodnocení vypracují návrhy zpráv o zjištěních a závěrech hodnocení. Zprávy předloží Komisi, skupině pro spolupráci, síti CSIRT a agentuře ENISA. Zprávy se projednají ve skupině pro spolupráci a v síti CSIRT. Zprávy mohou být zveřejněny na vyhrazených internetových stránkách skupiny pro spolupráci.

KAPITOLA IV

Řízení kybernetických bezpečnostních rizik a oznamovací povinnosti

ODDÍL I

Řízení a oznamování kybernetických bezpečnostních rizik

Článek 17

Správa a řízení

1. Členské státy zajistí, aby vedoucí orgány základních a důležitých subjektů schválily opatření k řízení rizik v oblasti kybernetické bezpečnosti přijatá těmito subjekty za

účelem splnění požadavků článku 18, dohlížely nad jejich uplatňováním a nesly odpovědnost za neplnění povinností subjektů podle tohoto článku.

2. Členské státy zajistí, aby členové vedoucího orgánu pravidelně absolvovali zvláštní školení, a získali tak dostatečné znalosti a dovednosti, aby mohli posoudit a vyhodnotit kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na provoz subjektu.

Článek 18

Opatření k řízení rizik v oblasti kybernetické bezpečnosti

1. Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto subjekty používají pro poskytování svých služeb. S ohledem na nejnovější technický vývoj musí tato opatření zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika.

2. Opatření uvedená v odstavci 1 zahrnují alespoň:

   a) analýzu rizik a politiku bezpečnosti informačních systémů;

   b) řešení incidentů (prevence a odhalování incidentů a reakce na ně);

   c) řízení kontinuity provozu a krizové řízení;

   d) zabezpečení dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho dodavateli nebo poskytovateli služeb, jako jsou poskytovatelé služeb ukládání a zpracování dat nebo řízených bezpečnostních služeb;

   e) zabezpečení pořizování, vývoje a údržby sítě a informačních systémů, včetně zveřejňování informací o zranitelnostech a jejich řešení;

   f) politiky a postupy (testování a audit) za účelem posouzení účelnosti opatření k řízení rizik v oblasti kybernetické bezpečnosti;

   g) používání kryptografie a šifrování.

3. Členské státy zajistí, aby při zvažování vhodných opatření uvedených v odst. 2 písm. d) subjekty zohlednily zranitelnosti specifické pro každého dodavatele a poskytovatele služeb a celkovou kvalitu produktů a praktik v oblasti kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje.

4. Členské státy zajistí, aby v případě, že subjekt zjistí, že jeho služby nebo úkoly neodpovídají požadavkům stanoveným v odstavci 2, neprodleně přijal všechna nezbytná nápravná opatření, aby dotčená služba požadavky splňovala.

5. Komise může přijmout prováděcí akty, aby stanovila technické a metodické specifikace prvků uvedených v odstavci 2. Při přípravě těchto aktů postupuje Komise v souladu s přezkumným postupem uvedeným v čl. 37 odst. 2 a v maximální možné míře dodržuje mezinárodní a evropské normy, jakož i příslušné technické specifikace.

6. Komisi je svěřena pravomoc přijmout v souladu s článkem 36 akty v přenesené pravomoci, kterými doplní prvky stanovené v odstavci 2, aby zohledňovaly nové kybernetické hrozby, technologický vývoj nebo specifičnosti daného odvětví.

Článek 19

Koordinované posouzení rizik kritických dodavatelských řetězců v EU

1. Skupina pro spolupráci může v součinnosti s Komisí a agenturou ENISA provést koordinované posouzení rizik dodavatelských řetězců u specifických kritických služeb, systémů nebo produktů IKT, přičemž zohlední technické, případně netechnické rizikové faktory.

2. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA určí specifické kritické služby, systémy nebo produkty IKT, jež mohou být předmětem koordinovaného posouzení rizik uvedeného v odstavci 1.

Článek 20

Oznamovací povinnosti

1. Členské státy zajistí, aby základní a důležité subjekty neprodleně oznamovaly příslušným orgánům nebo týmu CSIRT v souladu s odstavci 3 a 4 každý incident, který má závažný dopad na poskytování jejich služeb. Ve vhodných případech tyto subjekty neprodleně informují příjemce svých služeb o incidentech, které by mohly negativně ovlivnit poskytování dané služby. Členské státy zajistí, aby tyto subjekty oznamovaly mimo jiné všechny informace, které příslušným orgánům nebo týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu.

2. Členské státy zajistí, aby základní a důležité subjekty neprodleně oznamovaly příslušným orgánům nebo týmu CSIRT každou významnou kybernetickou hrozbu, kterou tyto subjekty zjistí a která by mohla mít za následek významný incident.

   Ve vhodných případech tyto subjekty neprodleně informují příjemce svých služeb, které mohou být ovlivněny významnou kybernetickou hrozbou, o všech krocích nebo nápravných opatřeních, jež příjemci mohou učinit v reakci na danou hrozbu. Ve vhodných případech subjekty příjemce uvědomí také o hrozbě samotné. Ohlášení nezakládá u oznamujícího subjektu vyšší míru právní odpovědnosti.

3. Incident se považuje za významný, jestliže:

   a) incident dotčenému subjektu způsobil nebo může způsobit podstatné provozní narušení nebo finanční ztráty;

   b) incident způsobil nebo může způsobit jiným fyzickým nebo právnickým osobám značné hmotné nebo nehmotné ztráty.

4. Členské státy zajistí, aby za účelem oznámení podle odstavce 1 dotčené subjekty předložily příslušným orgánům nebo týmu CSIRT:

   a) neprodleně, nejpozději však do 24 hodin po zjištění incidentu, první oznámení, v němž případně uvedou, zda byl incident pravděpodobně způsoben neoprávněným nebo svévolným zásahem;

b) na žádost příslušného orgánu nebo týmu CSIRT průběžnou zprávu o podstatných změnách stavu;

c) nejpozději do jednoho měsíce od předložení oznámení podle písmene a) závěrečnou zprávu zahrnující alespoň:

i) podrobný popis incidentu, jeho závažnost a dopad;

ii) druh hrozby nebo základní příčinu, která incident pravděpodobně spustila;

iii) učiněná a probíhající opatření ke zmírnění následků.

Členské státy zajistí, aby se dotčený subjekt mohl v odůvodněných případech a po dohodě s příslušnými orgány nebo týmem CSIRT odchýlit od lhůt stanovených v písmeni a) a c).

5. Příslušné vnitrostátní orgány nebo tým CSIRT poskytnou do 24 hodin po obdržení prvního oznámení podle odst. 4 písm. a) oznamujícímu subjektu své vyjádření, včetně prvních připomínek k incidentu, a na žádost subjektu doporučí možná zmírňující opatření. Pokud tým CSIRT neobdržel oznámení podle odstavce 1, doporučení vydá příslušný orgán ve spolupráci s týmem CSIRT. Pokud o to dotčený subjekt požádá, poskytne mu tým CSIRT další technickou podporu. Jestliže existuje podezření, že má incident povahu trestného činu, doporučí příslušné vnitrostátní orgány nebo tým CSIRT také ohlášení tohoto incidentu orgánům činným v trestním řízení.

6. Tam, kde je to vhodné, a zejména pokud se incident podle odstavce 1 týká dvou nebo více členských států, informuje příslušný orgán nebo tým CSIRT, jimž byl incident ohlášen, ostatní dotčené členské státy a agenturu ENISA. Příslušné orgány, týmy CSIRT a jednotná kontaktní místa přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachovávají bezpečnost a obchodní zájmy subjektu, jakož i důvěrnost poskytnutých informací.

7. Pokud je nezbytné informovat veřejnost, aby se incidentu zabránilo nebo aby se probíhající incident vyřešil, nebo pokud je zveřejnění incidentu jinak ve veřejném zájmu, může příslušný orgán nebo tým CSIRT, případně orgány nebo týmy CSIRT jiných dotčených členských států po konzultaci s dotčeným subjektem informovat veřejnost o incidentu nebo požadovat, aby tak učinil daný subjekt.

8. Na žádost příslušného orgánu nebo týmu CSIRT postoupí jednotné kontaktní místo hlášení obdržená podle odstavce 1 a 2 jednotným kontaktním místům dalších dotčených členských států.

9. Jednotné kontaktní místo předkládá každý měsíc agentuře ENISA souhrnnou zprávu zahrnující anonymizovaná a agregovaná data o incidentech, závažných kybernetických hrozbách a případech, kdy téměř došlo k incidentu, oznámených podle odstavce 1 a 2 a podle článku 27. V zájmu větší srovnatelnosti poskytovaných informací může agentura ENISA vydat technické pokyny k parametrům informací, jež mají být v souhrnné zprávě uvedeny.

10. Příslušné orgány poskytnou příslušným orgánům určeným podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] informace o incidentech a kybernetických hrozbách oznámených podle odstavců 1 a 2 základními subjekty určenými jako kritické subjekty nebo subjekty, které jsou rovnocenné kritickým subjektům, podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů].

11. Komise může přijmout prováděcí akty dále upřesňující druh informací, formát a postup oznámení předkládaných podle odstavce 1 a 2. Komise může rovněž přijmout prováděcí akty dále upřesňující případy, kdy se incident považuje za významný, jak je uvedeno v odstavci 3. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 37 odst. 2.

Článek 21

Použití evropských systémů certifikace kybernetické bezpečnosti

1. K prokázání splnění některých požadavků článku 18 mohou členské státy požadovat, aby základní a důležité subjekty certifikovaly některé produkty IKT, služby IKT a procesy IKT podle zvláštních evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881. Produkty, služby a procesy podléhající certifikaci mohou být vyvinuty základním nebo důležitým subjektem nebo pořízeny od třetích stran.

2. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci upřesňující, které kategorie základních subjektů budou povinny obstarat si certifikát a podle kterých konkrétních evropských systémů certifikace kybernetické bezpečnosti podle odstavce 1. Akty v přenesené pravomoci se přijímají v souladu s článkem 36.

3. Komise může požádat agenturu ENISA, aby v případech, kdy není k dispozici žádný vhodný evropský systém certifikace kybernetické bezpečnosti pro účely odstavce 2, připravila návrh systému podle čl. 48 odst. 2 nařízení (EU) 2019/881.

Článek 22

Standardizace

1. Členské státy za účelem harmonizovaného provádění čl. 18 odst. 1 a 2 podporují používání evropských nebo mezinárodně uznávaných norem nebo specifikací upravujících bezpečnost sítí a informačních systémů, aniž by přitom vyžadovaly používání konkrétního druhu technologie nebo diskriminujícím způsobem prosazovaly jeho používání.

2. Agentura ENISA ve spolupráci se členskými státy vydá doporučení a pokyny týkající se technických oblastí, které by měly být zohledněny ve vztahu k odstavci 1, jakož i s ohledem na již existující normy, včetně vnitrostátních norem členských států, které by umožnily tyto oblasti pokrýt.

Článek 23

Databáze doménových jmen a registračních údajů

1. Aby členské státy přispěly k bezpečnosti, stabilitě a odolnosti DNS, zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD shromažďovaly a uchovávaly přesné a úplné údaje o registraci doménových jmen ve vyhrazeném databázovém zařízení, a to s náležitou péčí podle právních předpisů Unie o ochraně osobních údajů, pokud jde o data, jež jsou osobními údaji.

2. Členské státy zajistí, aby databáze údajů o registraci doménových jmen uvedené v odstavci 1 obsahovaly podstatné informace umožňující identifikaci a kontaktování držitelů doménových jmen a kontaktní místa spravující doménová jména v registrech TLD.

3. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD měly zavedeny zásady a postupy zajišťující, aby databáze zahrnovaly přesné a úplné informace. Členské státy zajistí, aby byly tyto zásady a postupy veřejně dostupné.

4. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD zveřejnily neprodleně po registraci doménového jména údaje o registraci domény, které nejsou osobními údaji.

5. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD poskytovaly přístup ke konkrétním údajům o registraci doménových jmen na oprávněnou a řádně odůvodněnou žádost oprávněných žadatelů o přístup, a to v souladu s právními předpisy Unie o ochraně osobních údajů. Členské státy zajistí, aby registry TLD a subjekty poskytující služby registrace doménových jmen pro TLD neprodleně reagovaly na všechny žádosti o přístup. Členské státy zajistí, aby byly zásady a postupy zveřejňování těchto údajů veřejně dostupné.

Oddíl II

Pravomoc a registrace

Článek 24

Pravomoc a územní působnost

1. Poskytovatele služeb DNS, registry doménových jmen TLD, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center a poskytovatelé sítí pro doručování obsahu uvedení v bodě 8 přílohy I, jakož i digitální poskytovatelé uvedení v bodě 6 přílohy II se považují za spadající pod pravomoc členského státu, který je hlavním místem jejich obchodní činnosti v Unii.

2. Pro účely této směrnice se má za to, že hlavním místem obchodní činnosti subjektů uvedených v odstavci 1 v Unii je členský stát, v němž přijímají rozhodnutí týkající se opatření k řízení rizik v oblasti kybernetické bezpečnosti. Jestliže tato rozhodnutí nejsou přijímána v žádné provozovně v Unii, má se za to, že hlavní místo obchodní činnosti je v členském státě, kde mají subjekty provozovnu s nejvyšším počtem zaměstnanců v Unii.

3. Jestliže subjekt uvedený v odstavci 1 není v Unii usazen, ale nabízí v Unii služby, určí svého zástupce v Unii. Tento zástupce musí být usazen v jednom z členských států, v němž jsou služby nabízeny. Má se za to, že tento subjekt podléhá pravomoci členského státu, v němž je zástupce usazen. Neexistuje-li určený zástupce v Unii podle tohoto článku, může právní kroky proti subjektu za neplnění povinností podle této směrnice podniknout kterýkoli členský stát, v němž tento subjekt poskytuje služby.

4. Určí-li subjekt uvedený v odstavci 1 svého zástupce, není tím dotčena možnost zahájit právní řízení proti samotnému subjektu.

Článek 25

Registr základních a důležitých subjektů

1. Agentura ENISA vytvoří a vede registr základních a důležitých subjektů uvedených v čl. 24 odst. 1. Subjekty předloží [nejpozději do 12 měsíců od vstupu této směrnice v platnost] agentuře ENISA tyto informace:

   a) název subjektu;

   b) adresu své hlavní provozovny a svých dalších provozoven v Unii nebo, není-li subjekt v Unii usazen, svého zástupce určeného podle čl. 24 odst. 3;

   c) aktuální kontaktní údaje, včetně e-mailových adres a telefonních čísel subjektů.

2. Subjekty uvedené v odstavci 1 uvědomí agenturu ENISA o všech změnách údajů, které předložily podle odstavce 1, a to neprodleně, nejpozději však do tří měsíců od data, kdy změna začala platit.

3. Po obdržení informací podle odstavce 1 je agentura ENISA předá jednotným kontaktním místům v závislosti na uvedeném umístění hlavního místa obchodní činnosti každého subjektu nebo, pokud subjekt není v Unii usazen, sídle jeho určeného zástupce. Jestliže má subjekt uvedený v odstavci 1 vedle svého hlavního místa obchodní činnosti v Unii další provozovny v jiných členských státech, agentura ENISA informuje také jednotná kontaktní místa těchto členských států.

4. Pokud subjekt nezaregistruje svou činnost nebo neposkytne příslušné informace ve lhůtě stanovené v odstavci 1, má každý členský stát, v němž tento subjekt poskytuje služby, pravomoc zajistit, aby subjekt plnil povinnosti stanovené v této směrnici.

KAPITOLA V

Sdílení informací

Článek 26

Ujednání o sdílení informací o kybernetické bezpečnosti

1. Aniž je dotčeno nařízení (EU) 2016/679 členské státy zajistí, aby základní a důležité subjekty mohly mezi sebou sdílet podstatné informace o kybernetické bezpečnosti včetně informací týkajících se kybernetických hrozeb, zranitelností, indikátorů narušení, taktiky, technik a postupů, varování při ohrožení kybernetické bezpečnosti a konfiguračních nástrojů, pokud toto sdílení informací:

   a) má za cíl prevenci a odhalování incidentů a reakci na ně nebo jejich zmírnění;

   b) zvyšuje úroveň kybernetické bezpečnosti, zejména zvyšováním informovanosti o kybernetických hrozbách, omezováním nebo bráněním schopnosti těchto hrozeb šířit se, podporou obranných kapacit, zveřejňováním informací o zranitelnostech a jejich nápravou, prostřednictvím metod zjišťování hrozeb, strategií zmírňování nebo fází reakce a obnovy.

2. Členské státy zajistí, aby k výměně informací docházelo v důvěryhodných komunitách základních a důležitých subjektů. Tato výměna bude probíhat

prostřednictvím ujednání o sdílení informací s ohledem na potenciálně citlivou povahu sdílených informací v souladu s pravidly práva Unie uvedenými v odstavci 1.

3. Členské státy stanoví pravidla upřesňující postup, provozní prvky (včetně použití vyhrazených platforem IKT), obsah a podmínky ujednání o sdílení informací podle odstavce 2. Tato pravidla rovněž podrobně upravují zapojení veřejných orgánů do těchto ujednání, jakož i provozní prvky, včetně využití vyhrazených platforem IT. Členské státy nabídnou podporu při uplatňování těchto ujednání v souladu se svými politikami uvedenými v čl. 5 odst. 2 písm. g).

4. Po uzavření ujednání o sdílení informací podle odstavce 2, případně po odstoupení od těchto ujednání, jakmile nabude účinku, uvědomí základní a důležité subjekty příslušné orgány o své účasti na nich.

5. V souladu s právem Unie podporuje agentura ENISA vznik ujednání o sdílení informací o kybernetické bezpečnosti podle odstavce 2 poskytováním osvědčených postupů a doporučení.

Článek 27

Dobrovolné oznamování podstatných informací

Členské státy zajistí, aniž je dotčen článek 3, aby subjekty, které nespadají do oblasti působnosti této směrnice, mohly dobrovolně oznamovat významné incidenty, kybernetické hrozby nebo případy, kdy téměř došlo k incidentu. Při zpracování oznámení postupují členské státy postupem uvedeným v článku 20. Členské státy mohou dát přednost zpracování povinných oznámení před dobrovolnými oznámeními. Na základě dobrovolného oznámení nesmí být oznamujícímu subjektu uloženy žádné další povinnosti, které by mu nebyly uloženy, kdyby toto oznámení neučinil.

KAPITOLA VI

Dohled a vymáhání

Článek 28

Obecné aspekty týkající se dohledu a vymáhání

1. Členské státy zajistí, aby příslušné orgány účinně monitorovaly dodržování této směrnice a činily opatření nezbytná k zajištění jejího dodržování, zejména povinností stanovených v článcích 18 a 20.

2. Při řešení incidentů, v jejichž důsledku došlo k porušení ochrany osobních údajů, příslušné orgány úzce spolupracují s orgány pro ochranu osobních údajů.

Článek 29

Dohled a vymáhání u základních subjektů

1. Členské státy zajistí, aby byla opatření v oblasti dohledu nebo vymáhání uložená základním subjektům v souvislosti s povinnostmi stanovenými v této směrnici

účinná, přiměřená a odrazující, přičemž zohlední okolnosti každého jednotlivého případu.

2. Členské státy zajistí, aby příslušné orgány měly při výkonu svých dohledových úkolů v souvislosti se základními subjekty pravomoc podrobit tyto subjekty:

a) kontrolám na místě i externímu dohledu, včetně namátkových kontrol;

b) pravidelným auditům;

c) cíleným bezpečnostním auditům na základě posouzení rizik nebo dostupných informací týkajících se rizik;

d) bezpečnostním prověrkám na základě objektivních, nediskriminačních, korektních a transparentních kritérií posouzení rizik;

e) požadavkům na informace nezbytné k posouzení opatření v oblasti kybernetické bezpečnosti přijatých subjektem, včetně zadokumentovaných zásad kybernetické bezpečnosti, jakož i dodržování povinnosti informovat agenturu ENISA podle čl. 25 odst. 1 a 2;

f) požadavkům na přístup k údajům, dokumentům nebo veškerým informacím potřebným pro výkon jejich dohledových úkolů;

g) požadavkům na doložení provádění zásad kybernetické bezpečnosti, jako jsou výsledky bezpečnostních auditů provedených kvalifikovaným auditorem a příslušné podpůrné doklady.

3. Při výkonu svých pravomocí podle odst. 2 písm. e) až g) uvedou příslušné orgány účel žádosti a upřesní informace, které jsou požadovány.

4. Členské státy zajistí, aby příslušné orgány měly při výkonu svých donucovacích pravomocí v souvislosti se základními subjekty pravomoc:

a) vydat subjektům varování při nedodržení povinností stanovených v této směrnici;

b) vydat závazné pokyny nebo příkaz požadující, aby tyto subjekty napravily zjištěné nedostatky nebo porušení povinností stanovených v této směrnici;

c) nařídit těmto subjektům, aby ukončily jednání, které není v souladu s povinnostmi stanovenými v této směrnici a nadále se takového jednání zdržely;

d) nařídit těmto subjektům, aby uvedly svá opatření k řízení rizik anebo oznamovací povinnosti do souladu s povinnostmi stanovenými v článcích 18 a 20, a to určeným způsobem a ve stanovené lhůtě;

e) nařídit těmto subjektům, aby informovaly fyzické nebo právnické osoby, jimž poskytují služby nebo činnosti, které jsou potenciálně postiženy významnou kybernetickou hrozbou, o všech možných ochranných nebo nápravných opatřeních, jež by mohly tyto fyzické nebo právnické osoby učinit v reakci na tuto hrozbu;

f) nařídit těmto subjektům, aby v přiměřené lhůtě provedly doporučení vydané v důsledku bezpečnostního auditu;

g) určit na stanovenou dobu pracovníka pro monitorování s přesně vymezenými úkoly, který bude dohlížet na dodržování jejich povinností stanovených v článcích 18 a 20;

h) nařídit těmto subjektům, aby konkrétním způsobem zveřejnily aspekty nedodržování povinností stanovených v této směrnici;

i) učinit veřejné prohlášení, které identifikuje právnické a fyzické osoby odpovědné za porušení povinnosti stanovené v této směrnici a povahu tohoto porušení;

j) uložit nebo požádat o uložení správní pokuty podle vnitrostátních právních předpisů příslušnými orgány nebo soudy podle článku 31 vedle opatření uvedených v písmenech a) až i) tohoto odstavce nebo namísto těchto opatření, a to v závislosti na okolnostech každého jednotlivého případu.

5. Pokud se donucovací opatření přijatá podle odst. 4 písm. a) až d) a f) ukážou jako neúčinná, členské státy zajistí, aby příslušné orgány měly pravomoc stanovit lhůtu, v níž bude základní subjekt vyzván k přijetí nezbytných opatření k nápravě nedostatků nebo splnění požadavků těchto orgánů. Pokud požadovaná opatření nebudou přijata ve stanovené lhůtě, členské státy zajistí, aby příslušné orgány měly pravomoc:

a) pozastavit nebo požádat certifikační nebo schvalovací orgán o pozastavení certifikace nebo schválení týkající se všech nebo některých služeb nebo činností poskytovaných základním subjektem;

b) uložit nebo požadovat, aby příslušné orgány nebo soudy v souladu s vnitrostátními právními předpisy uložily dočasný zákaz výkonu manažerských funkcí v tomto subjektu jakékoli osobě, která má manažerskou odpovědnost na úrovni výkonného ředitele nebo zákonného zástupce v tomto základním subjektu, i jakékoli jiné fyzické osobě odpovědné za porušení.

Tato omezující opatření se použijí pouze do doby, než subjekt přijme opatření nezbytná k odstranění nedostatků nebo splnění požadavků příslušného orgánu, kvůli nimž byla tato omezující opatření uplatněna.

6. Členské státy zajistí, aby každá fyzická osoba odpovědná za základní subjekt nebo jednající jako zástupce základního subjektu na základě pravomoci jej zastupovat, oprávnění přijímat rozhodnutí jeho jménem nebo oprávnění vykonávat nad ním kontrolu měla pravomoc zajistit plnění povinností stanovených v této směrnici. Členské státy zajistí, aby tyto fyzické osoby mohly být volány k odpovědnosti za porušení svých úkolů zajistit dodržování povinností stanovených v této směrnici.

7. Při přijímání donucovacích opatření nebo uplatňování jakýchkoli omezujících opatření podle odstavců 4 a 5 dodržují příslušné orgány práva na obhajobu a zohlední okolnosti každého jednotlivého případu a v úvahu vezmou alespoň:

a) závažnost porušení a významnost porušených ustanovení. Mezi porušení, která by měla být považována za závažná, patří: opakovaná porušení, neoznámení nebo nezajištění nápravy incidentů s významným rušivým účinkem, neodstranění nedostatků podle závazných pokynů příslušných orgánů, maření auditů nebo monitorovací činnosti nařízené příslušným orgánem po zjištění porušení povinnosti, poskytnutí nepravdivých nebo hrubě nepřesných informací v souvislosti s požadavky na řízení rizik nebo oznamovacími povinnostmi stanovenými v článcích 18 a 20;

b) dobu trvání porušení povinnosti, včetně prvku opakovaného porušení povinnosti;

c) skutečně způsobené škody nebo vzniklé ztráty, případně potenciální škody nebo ztráty, které mohly být způsobeny, pokud je lze určit. Při hodnocení

tohoto aspektu je třeba zohlednit mimo jiné skutečné nebo potenciální finanční nebo ekonomické ztráty, účinky na jiné služby, počet postižených nebo potenciálně postižených uživatelů;

d) to, zda k porušení povinnosti došlo úmyslně nebo z nedbalosti;

e) opatření přijatá subjektem za účelem prevence nebo zmírnění škod anebo ztrát;

f) dodržování schválených kodexů chování nebo schválených certifikačních mechanismů;

g) míru spolupráce fyzické nebo právnické osoby považované za odpovědnou s příslušnými orgány.

8. Příslušné orgány svá rozhodnutí o výkonu podrobně odůvodní. Před přijetím těchto rozhodnutí příslušné orgány oznámí dotčeným subjektům svá předběžná zjištění a poskytnou těmto subjektům přiměřenou dobu na předložení připomínek.

9. Členské státy zajistí, aby jejich příslušné orgány při výkonu svých pravomocí v oblasti dohledu a vymáhání zaměřených na zajištění dodržování povinností podle této směrnice ze strany základního subjektu určeného podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za kritický subjekt nebo subjekt, který je rovnocenný kritickému subjektu, informovaly příslušné orgány daného členského státu určené podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]. Na žádost příslušných orgánů podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] mohou příslušné orgány vykonávat své dohledové a donucovací pravomoci u základního subjektu označeného jako kritický nebo rovnocenný kritickému subjektu.

Článek 30

Dohled a vymáhání u důležitých subjektů

1. Při předložení důkazů nebo informací naznačujících, že důležitý subjekt neplní povinnosti stanovené v této směrnici, zejména v článcích 18 a 20, členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření prostřednictvím dohledových opatření *ex post*.

2. Členské státy zajistí, aby příslušné orgány měly při výkonu svých dohledových úkolů v souvislosti s důležitými subjekty pravomoc podrobit tyto subjekty:

a) kontrolám na místě i externímu dohledu *ex post*;

b) cíleným bezpečnostním auditům na základě posouzení rizik nebo dostupných informací týkajících se rizik;

c) bezpečnostním prověrkám na základě objektivních, korektních a transparentních kritérií posouzení rizik;

d) požadavkům na veškeré informace nezbytné k posouzení opatření v oblasti kybernetické bezpečnosti *ex post*, včetně zadokumentovaných zásad kybernetické bezpečnosti, jakož i dodržování povinnosti informovat agenturu ENISA podle čl. 25 odst. 1 a 2;

e) požadavkům na přístup k údajům, dokumentům anebo veškerým informacím potřebným pro výkon dohledových úkolů.

3. Při výkonu svých pravomocí podle odst. 2 písm. d) nebo e) uvedou příslušné orgány účel žádosti a upřesní informace, které jsou požadovány.

4. Členské státy zajistí, aby příslušné orgány měly při výkonu svých donucovacích pravomocí v souvislosti s důležitými subjekty pravomoc:

   a) vydat subjektům varování při nedodržení povinností stanovených v této směrnici;

   b) vydat závazné pokyny nebo příkaz požadující, aby tyto subjekty napravily zjištěné nedostatky nebo porušení povinností stanovených v této směrnici;

   c) nařídit těmto subjektům, aby ukončily jednání, které není v souladu s povinnostmi stanovenými v této směrnici, a nadále se takového jednání zdržely;

   d) nařídit těmto subjektům, aby uvedly svá opatření k řízení rizik nebo oznamovací povinnosti do souladu s povinnostmi stanovenými v článcích 18 a 20, a to určeným způsobem a ve stanovené lhůtě;

   e) nařídit těmto subjektům, aby informovaly fyzické nebo právnické osoby, jimž poskytují služby nebo činnosti, které jsou potenciálně postiženy významnou kybernetickou hrozbou, o všech možných ochranných nebo nápravných opatřeních, jež by mohly tyto fyzické nebo právnické osoby učinit v reakci na tuto hrozbu;

   f) nařídit těmto subjektům, aby v přiměřené lhůtě provedly doporučení dané v důsledku bezpečnostního auditu;

   g) nařídit těmto subjektům, aby konkrétním způsobem zveřejnily aspekty nedodržování jejich povinností stanovených v této směrnici;

   h) učinit veřejné prohlášení, které identifikuje právnické a fyzické osoby odpovědné za porušení povinnosti stanovené v této směrnici a povahu tohoto porušení;

   i) uložit nebo požádat o uložení správní pokuty podle vnitrostátních právních předpisů příslušnými orgány nebo soudy podle článku 31 vedle opatření uvedených v písmenech a) až h) tohoto odstavce nebo namísto těchto opatření, a to v závislosti na okolnostech každého jednotlivého případu.

5. Ustanovení čl. 29 odst. 6 až 8 se rovněž použijí na opatření v oblasti dohledu a vymáhání stanovená v tomto článku pro důležité subjekty uvedené v příloze II.

Článek 31

Obecné podmínky ukládání správních pokut základním a důležitým subjektům

1. Členské státy zajistí, aby ukládání správních pokut základním a důležitým subjektům podle tohoto článku za porušení povinností stanovených v této směrnici bylo v každém jednotlivém případě účinné, přiměřené a odrazující.

2. Správní pokuty se ukládají podle okolností každého jednotlivého případu kromě opatření uvedených v čl. 29 odst. 4 písm. a) až i), čl. 29 odst. 5 a čl. 30 odst. 4 písm. a) až h) či místo nich.

3. Při rozhodování o uložení správní pokuty a při rozhodování o její výši se v každém jednotlivém případě náležitě přihlédne alespoň k prvkům uvedeným v čl. 29 odst. 7.

4. Členské státy zajistí, aby za porušení povinností stanovených v článku 18 nebo článku 20 byly v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty, jejichž maximální výše bude stanovena na nejméně 10 000 000 EUR nebo 2 % celkového celosvětového ročního obratu podniku, ke kterému patřil základní nebo důležitý subjekt v předchozím rozpočtovém roce, podle toho, co je vyšší.

5. Členské státy mohou stanovit pravomoc ukládat penále s cílem přimět základní nebo důležitý subjekt, aby přestal porušovat povinnosti podle předchozího rozhodnutí příslušného orgánu.

6. Aniž jsou dotčeny pravomoci příslušných orgánů podle článků 29 a 30, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty subjektům veřejné správy uvedeným v čl. 4 odst. 23, na něž se vztahují povinnosti stanovené v této směrnici.

Článek 32

Porušení povinností spočívající v porušení zabezpečení osobních údajů

1. Pokud mají příslušné orgány informace naznačující, že porušení povinností stanovených v článcích 18 a 20 základním nebo důležitým subjektem má za následek porušení zabezpečení osobních údajů ve smyslu čl. 4 odst. 12 nařízení (EU) 2016/679, které musí být oznámeno podle článku 33 uvedeného nařízení, uvědomí v přiměřené lhůtě orgány dohledu příslušné podle článků 55 a 56 uvedeného nařízení.

2. Pokud se orgány dohledu příslušné podle článků 55 a 56 nařízení (EU) 2016/679 rozhodnou vykonat své pravomoci podle čl. 58 písm. i) uvedeného nařízení a uložit správní pokutu, příslušné orgány neuloží za stejné porušení správní pokutu podle článku 31 této směrnice. Příslušné orgány však mohou uplatnit donucovací opatření nebo sankční pravomoci stanovené v čl. 29 odst. 4 písm. a) až i), čl. 29 odst. 5 a v čl. 30 odst. 4 písm. a) až h) této směrnice.

3. Pokud má dozorový úřad příslušný podle nařízení (EU) 2016/679 sídlo v jiném členském státě než příslušný orgán, může příslušný orgán informovat dozorový úřad se sídlem ve stejném členském státě.

Článek 33

Sankce

1. Členské státy stanoví sankce za porušení vnitrostátních ustanovení přijatých podle této směrnice a přijmou veškerá opatření nezbytná k zajištění jejich uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující.

2. Členské státy nejpozději do [dvou] let od vstupu této směrnice v platnost oznámí stanovené sankce a opatření Komisi a budou ji neprodleně informovat o všech následných změnách, které se jich budou týkat.

Článek 34

Vzájemná pomoc

1. Pokud základní nebo důležitý subjekt poskytuje služby ve více než jednom členském státě nebo má svou hlavní provozovnu nebo zástupce v členském státě, ale jeho sítě a informační systémy se nacházejí v jednom či více jiných členských státech, příslušný orgán členského státu, v němž se nachází hlavní místo obchodní činnosti nebo jiná provozovna, případně zástupce, a příslušné orgány těchto jiných členských států podle potřeby spolupracují a jsou si navzájem nápomocny. Tato spolupráce spočívá alespoň v tomto:

   a) příslušné orgány uplatňující opatření v oblasti dohledu nebo vymáhání v členském státě konzultují prostřednictvím jednotného kontaktního místa s příslušnými orgány v ostatních dotčených členských státech a informují je o přijatých opatřeních v oblasti dohledu a vymáhání a o svých následných opatřeních podle článků 29 a 30;

   b) příslušný orgán může požádat jiný příslušný orgán, aby učinil opatření v oblasti dohledu nebo vymáhání uvedená v článcích 29 a 30;

   c) po obdržení odůvodněné žádosti jiného příslušného orgánu poskytne příslušný orgán druhému příslušnému orgánu pomoc, aby bylo možné provést opatření v oblasti dohledu nebo vymáhání uvedená v článcích 29 a 30 účelně, efektivně a důsledně. Tato vzájemná pomoc může zahrnovat žádosti o informace a opatření v oblasti dohledu, včetně žádostí o provedení kontrol na místě nebo externího dohledu, případně cílených bezpečnostních auditů. Příslušný orgán, kterému je určena žádost o pomoc, nemůže tuto žádost odmítnout, ledaže se po výměně informací s ostatními dotčenými orgány, agenturou ENISA a Komisí prokáže, že tento orgán není příslušný k poskytnutí požadované pomoci nebo požadovaná pomoc není úměrná úkolům dohledu příslušného orgánu prováděným v souladu s články 29 nebo 30.

2. Je-li to vhodné, mohou se příslušné orgány z různých členských států vzájemně dohodnout, že budou provádět společné kontrolní akce uvedené v článcích 29 a 30.

KAPITOLA VII

Přechodná a závěrečná ustanovení

Článek 35

Přezkum

Komise pravidelně přezkoumává fungování této směrnice a podává zprávu Evropskému parlamentu a Radě. Ve zprávě se zejména posoudí význam odvětví, pododvětví, velikosti a druhu subjektů uvedených v přílohách I a II pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností. Za tímto účelem a s cílem dále rozvíjet strategickou a operativní spolupráci Komise zohlední zprávy skupiny pro spolupráci a sítě CSIRT z hlediska zkušeností získaných na strategické a operativní úrovni. První zprávu předloží do ... [54 měsíců od data vstupu této směrnice v platnost].

Článek 36

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 18 odst. 6 a v čl. 21 odst. 2 je svěřena Komisi na dobu pěti let ode dne […]

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 18 odst. 6 a v čl. 21 odst. 2 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie*, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Před přijetím aktu v přenesené pravomoci vede Komise konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů.

5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle čl. 18 odst. 6 a čl. 21 odst. 2 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 37

Postup projednávání ve výboru

1. Komisi je nápomocen výbor. Uvedený výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

3. Má-li být stanovisko výboru získáno písemným postupem, je tento postup ukončen bez výsledku, pokud tak o tom ve lhůtě stanovené pro vydání stanoviska rozhodne předseda výboru nebo pokud o to požádá člen výboru.

Článek 38

Provedení ve vnitrostátním právu

1. Členské státy přijmou a zveřejní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději… [18 měsíců po vstupu této směrnice v platnost]. Neprodleně o nich uvědomí Komisi. Začnou tato opatření uplatňovat ode dne ... [jeden den ode dne uvedeného v prvním pododstavci].

2. Tyto předpisy přijaté členskými státy musí obsahovat odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob odkazu si stanoví členské státy.

Článek 39

Změna nařízení (EU) č. 910/2014

Článek 19 nařízení (EU) č. 910/2014 se zrušuje.

Článek 40

Změna směrnice (EU) 2018/1972

Články 40 a 41 směrnice (EU) 2018/1972 se zrušují.

Článek 41

Zrušení

Směrnice (EU) 2016/1148 se zrušuje s účinností od ... [datum provedení směrnice ve vnitrostátním právu].

Odkazy na směrnici (EU) 2016/1148 se považují za odkazy na tuto směrnici v souladu se srovnávací tabulkou obsaženou v příloze III.

Článek 42

Vstup v platnost

Tato směrnice vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Článek 43

Určení

Tato směrnice je určena členským státům.

V Bruselu dne

Za Evropský parlament
předseda

Za Radu
předseda/předsedkyně

LEGISLATIVNÍ FINANČNÍ VÝKAZ

Obsah

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Návrh směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

1.2. Příslušné oblasti politik *(skupina programů)*

Komunikační sítě, obsah a technologie

1.3. Návrh/podnět se týká:

☐ **nové akce**

☐ **nové akce následující po pilotním projektu / přípravné akci**[40]

☒ **prodloužení stávající akce**

☐ **sloučení jedné či více akcí v jinou/novou akci nebo přesměrování jedné či více akcí na jinou/novou akci**

1.4. Odůvodnění návrhu/podnětu

1.4.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu

Cílem revize je zvýšit úroveň kybernetické odolnosti celého souboru podniků působících v Evropské unii ve všech příslušných odvětvích, snížit rozdíly v odolnosti na vnitřním trhu v odvětvích, na něž se směrnice již vztahuje, a zlepšit úroveň společné znalosti situace a kolektivní schopnosti připravit se a reagovat.

1.4.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

Odolnost v oblasti kybernetické bezpečnosti v celé Unii nemůže být účinná, pokud k ní bude přistupováno rozdílně prostřednictvím národních nebo regionálních izolovaných sil. Směrnice o bezpečnosti sítí a informací začala tento nedostatek řešit stanovením rámce pro bezpečnost sítí a informačních systémů na vnitrostátní úrovni a na úrovni Unie. První pravidelný přezkum této směrnice však poukázal na řadu neodmyslitelných nedostatků, které nakonec vedly ke značným rozdílům v jednotlivých členských státech, pokud jde o schopnosti, plánování a úroveň ochrany, které současně ovlivňují rovné podmínky pro podobné společnosti na vnitřním trhu. Intervence EU, která jde nad rámec současných opatření směrnice o bezpečnosti sítí a informací, je odůvodněna zejména: i) přeshraniční povahou problému; ii) potenciálem opatření EU zlepšit a usnadnit účinné vnitrostátní politiky; iii) přínosem koordinovaných a společných politických opatření v oblasti bezpečnosti sítí a informací k účinnému zajištění ochrany údajů a soukromí. Uvedených cílů lze proto dosáhnout snáze, dojde-li k akci na úrovni EU, než budou-li členské státy postupovat samostatně.

[40] Uvedené v čl. 58 odst. 2 písm. a) nebo b) finančního nařízení.

1.4.3. Závěry vyvozené z podobných zkušeností v minulosti

Směrnice o bezpečnosti sítí a informací je prvním horizontálním nástrojem vnitřního trhu, jehož cílem je zlepšit odolnost sítí a systémů v Unii vůči kybernetickým bezpečnostním rizikům. Již významně přispěla ke zvýšení společné úrovně kybernetické bezpečnosti v členských státech. Přezkum fungování a provádění směrnice však poukázal na řadu nedostatků, které je třeba spolu s rostoucí digitalizací a potřebou aktuálnější reakce řešit v revidovaném právním aktu.

1.4.4. Slučitelnost a možná součinnost s dalšími vhodnými nástroji

Nový návrh je zcela v souladu s dalšími souvisejícími iniciativami, jako je návrh nařízení o digitální provozní odolnosti finančního sektoru („DORA“) a návrh směrnice o odolnosti kritických provozovatelů základních služeb. Je rovněž v souladu s evropským kodexem pro elektronické komunikace, obecným nařízením o ochraně údajů a nařízením eIDAS.

Návrh tvoří nezbytnou část strategie bezpečnostní unie EU.

1.5. Doba trvání akce a finanční dopad

☐ **časově omezená doba trvání**

– ☐ s platností od [DD.MM.]RRRR do [DD.MM.]RRRR

– ☐ finanční dopad od RRRR do RRRR u prostředků na závazky a od RRRR do RRRR u prostředků na platby

☒ **časově neomezená doba trvání**

– Provádění s obdobím rozběhu od roku 2022 do roku 2025,

– poté plné fungování.

1.6. Předpokládaný způsob řízení[41]

Přímé řízení Komisí

– ☒ prostřednictvím jejích útvarů, včetně jejích zaměstnanců v delegacích Unie,

– ☐prostřednictvím výkonných agentur

☐ **Sdílené řízení** s členskými státy

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

– ☐ třetí země nebo subjekty určené těmito zeměmi,

– ☐ mezinárodní organizace a jejich agentury (upřesněte),

– ☐ EIB a Evropský investiční fond,

– X☐ subjekty uvedené v článcích 70 a 71 finančního nařízení,

– ☐ veřejnoprávní subjekty,

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

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

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

– *Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.*

Poznámky

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), jíž byl aktem o kybernetické bezpečnosti udělen nový trvalý mandát, by členským státům a Komisi pomohla v provádění revidované směrnice o bezpečnosti sítí a informací.

V důsledku revidované směrnice o bezpečnosti sítí a informací bude mít agentura ENISA od roku 2022/23 další oblasti činnosti. I když budou tyto oblasti činnosti podle mandátu agentury ENISA spadat pod její obecné úkoly, budou pro agenturu znamenat další pracovní zátěž. Přesněji řečeno, kromě současných oblastí činnosti bude agentura ENISA muset podle návrhu Komise na revidovanou směrnici o bezpečnosti sítí a informací výslovně zařadit do svého pracovního programu mimo jiné tyto činnosti: i) vytvořit a spravovat evropský registr

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

zranitelnosti (čl. 6 odst. 2 návrhu); ii) poskytnout sekretariát evropské síti styčných organizací pro kybernetické krize (CyCLONe) (článek 14 návrhu) a vydávat roční zprávu o stavu kybernetické bezpečnosti v EU (článek 15 návrhu); iii) podporovat organizaci vzájemných hodnocení mezi členskými státy (článek 16 návrhu); iv) shromažďovat souhrnné údaje o incidentech z členských států a vydávat technické pokyny (čl. 20 odst. 9 návrhu); v) vytvořit a spravovat registr pro subjekty poskytující přeshraniční služby (článek 25 návrhu).

Z tohoto důvodu bude požádáno o dalších pět zaměstnanců na plný pracovní úvazek od roku 2022 s odpovídajícím rozpočtem přibližně 0,61 milionu EUR ročně, jenž tato nová pracovní místa pokryje (viz oddělený finanční výkaz pro agentury).

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Komise bude pravidelně přezkoumávat uplatňování této směrnice a podávat zprávy Evropskému parlamentu a Radě, poprvé tři roky po vstupu v platnost.

Komise rovněž posoudí správnost provedení směrnice do vnitrostátního práva členských států.

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

Provádění směrnice bude řídit útvar v rámci GŘ CNECT odpovědný za tuto oblast politiky.

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

Velmi nízké riziko, protože ekosystém směrnice o bezpečnosti sítí a informací je již zaveden.

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

Nevztahuje se na tento návrh. Použití pouze administrativního rozpočtu („celkový rámec“).

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření, např. opatření uvedená ve strategii pro boj proti podvodům.

Nevztahuje se na tento návrh. Použití pouze administrativního rozpočtu („celkový rámec“).

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruh víceletého finančního rámce a nově navržené výdajové rozpočtové položky

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdajů	Příspěvek			
	Číslo [Okruh…7……...……]	RP/NRP[42]	zemí ESVO[43]	kandidátských zemí[44]	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
	20 02 06 výdaje na řízení 20 02 06	NRP	NE	NE	NE	NE

42 RP = rozlišené prostředky / NRP = nerozlišené prostředky.
43 ESVO: Evropské sdružení volného obchodu.
44 Kandidátské země a případně potenciální kandidáti ze západního Balkánu.

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	**<…>**	[Okruh……..……]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Po roce 2027***	**CELKEM**
Operační prostředky (rozdělené podle rozpočtových položek uvedených v bodě 3.1)	Závazky	(1)									
	Platby	(2)									
Prostředky správní povahy financované z krytí programu[45]	Závazky = Platby	(3)									
Prostředky na krytí programu CELKEM	Závazky	=1+3									
	Platby	=2+3									

Okruh víceletého finančního rámce	7	Správní výdaje Zasedání: plenární zasedání skupiny pro spolupráci v oblasti bezpečnosti sítí a informací se konají obvykle čtyřikrát ročně. Komise pokrývá náklady související s cateringem a cestovními výdaji zástupců 27 členských států (jeden zástupce na členský stát). Náklady na jedno zasedání by mohly dosáhnout až 15 000 EUR. Služební cesty: Služební cesty souvisejí s monitorováním provádění směrnice o bezpečnosti sítí a informací. Příklad: Za jeden rok (květen 2019 – červenec 2020) jsme měli uspořádat takzvané „návštěvy zemí NIS“ a navštívit všech 27 členských států, abychom projednali provádění směrnice o bezpečnosti sítí a informací v celé

[45] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

		EU.

Tento oddíl se vyplní pomocí „rozpočtových údajů správní povahy“, jež se nejprve uvedou v příloze legislativního finančního výkazu, která se pro účely konzultace mezi útvary vloží do aplikace DECIDE.

v milionech EUR (zaokrouhleno na tři desetinná místa)

		2021	2022	2023	2024	2025	2026	2027	*Po roce 2027*	CELKEM
Lidské zdroje		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Ostatní správní výdaje		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
CELKEM prostředky na OKRUH 7 víceletého finančního rámce	(Závazky celkem = platby celkem)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

v milionech EUR (zaokrouhleno na tři desetinná místa)

		2021	2022	2023	2024	2025	2026	2027	*Po roce 2027*	CELKEM
CELKEM prostředky ze všech OKRUHŮ víceletého finančního rámce	Závazky									
	Platby									

3.2.2. Odhadovaný souhrnný dopad na prostředky správní povahy

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy

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

v milionech EUR (zaokrouhleno na tři desetinná místa)

Roky	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**CELKEM**
OKRUH 7 víceletého finančního rámce								
Lidské zdroje	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Ostatní správní výdaje	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Mezisoučet OKRUH 7 víceletého finančního rámce	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**
Mimo OKRUH 7[46] víceletého finančního rámce								
Lidské zdroje								
Ostatní správní výdaje								
Mezisoučet mimo OKRUH 7 víceletého finančního rámce								
CELKEM	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy budou pokryty z prostředků GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny v rámci GŘ a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

[46] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

3.2.2.1. Odhadované potřeby v oblasti lidských zdrojů

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.

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

Odhad vyjádřete v přepočtu na plné pracovní úvazky

Roky		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)								
Ústředí a zastoupení Komise		6	6	6	6	6	6	6
Delegace								
Výzkum								
• Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE) - SZ, MZ, VNO, ZAP a MOD[47] Okruh 7								
Financováno z OKRUHU 7 víceletého finančního rámce	– v ústředí	3	3	3	3	3	3	3
	– při delegacích							
Financováno z krytí programu [48]	– v ústředí							
	– při delegacích							
Výzkum								
Jiné (uveďte)								
CELKEM		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci	• příprava aktů v přenesené pravomoci podle čl. 18 odst. 6, čl. 21 odst. 2, článku 36, • příprava prováděcích aktů podle čl. 12 odst. 8, čl. 18 odst. 5, čl. 20 odst. 11, • poskytnutí sekretariátu skupině pro spolupráci v oblasti bezpečnosti sítí a informací, • organizace plenárních zasedání a pracovních schůzí skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, • koordinace práce členských států na různých dokumentech (pokyny, sady nástrojů atd.), • spolupráce s ostatními útvary Komise, agenturou ENISA a vnitrostátními orgány s ohledem na provádění směrnice o bezpečnosti sítí a informací, • analýza vnitrostátních metod a osvědčených postupů souvisejících s prováděním směrnice o bezpečnosti sítí a informací.
Externí zaměstnanci	Podpora při plnění všech výše uvedených úkolů dle potřeby

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

48 Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

3.2.3. Příspěvky třetích stran

Návrh/podnět:

– X☐ nepočítá se spolufinancováním od třetích stran.

– ☐ počítá se spolufinancováním od třetích stran podle následujícího odhadu:

prostředky v milionech EUR (zaokrouhleno na tři desetinná místa)

Roky	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**CELKEM**
Upřesněte spolufinancující subjekt								
Spolufinancované prostředky CELKEM								

3.3. Odhadovaný dopad na příjmy

– ☐X Návrh/podnět nemá žádný finanční dopad na příjmy.

– ☐ Návrh/podnět má tento finanční dopad:

☐ na vlastní zdroje

☐ na jiné příjmy

uveďte, zda je příjem účelově vázán na výdajové položky ☐

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová rozpočtová položka:	Dopad návrhu/podnětu[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Článek …….							

U účelově vázaných příjmů upřesněte dotčené výdajové rozpočtové položky.

Jiné poznámky (např. způsob/vzorec výpočtu dopadu na příjmy nebo jiné údaje).

[49] Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.

PŘÍLOHA
LEGISLATIVNÍHO FINANČNÍHO VÝKAZU

Název návrhu/podnětu:

Návrh směrnice, kterou se reviduje směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

……
……

1. POTŘEBNÉ LIDSKÉ ZDROJE A NÁKLADY NA TYTO ZDROJE

2. VÝŠE OSTATNÍCH SPRÁVNÍCH VÝDAJŮ

3. METODY VÝPOČTU POUŽITÉ K ODHADU NÁKLADŮ

3.1 Lidské zdroje

3.2 Ostatní správní výdaje

*Tato příloha, **kterou vyplní každé GŘ/útvar, jež se na návrhu/podnětu podílí**, musí být přiložena k legislativnímu finančnímu výkazu při zahájení konzultací mezi útvary.*

Tabulky s údaji slouží jako zdroj pro tabulky obsažené v legislativním finančním výkazu. Jsou určeny pouze pro interní použití v Komisi.

1. Náklady na potřebné lidské zdroje

☐ Návrh/podnět nevyžaduje využití lidských zdrojů

X☐ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

OKRUH 7 víceletého finančního rámce		**2021**		**2022**		**2023**		**2024**		**2025**		**2026**		**2027**		**CELKEM**	
		Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky
• Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)																	
Ústředí a zastoupení Komise	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
při delegacích Unie	AD																
	AST																
• Externí zaměstnanci [50]0,24																	
Celkové krytí	SZ	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	VNO																
	ZAP																
při delegacích Unie	SZ																
	MZ																

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

	VNO																
	ZAP																
	MOD																
Jiné rozpočtové položky (*upřesněte*)																	
Mezisoučet – za OKRUH 7 víceletého finančního rámce		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Mimo OKRUH 7 víceletého finančního rámce			2021		2022		2023		2024		2025		2025		2025		CELKEM	
			Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky	Plný pracovní úvazek	Prostředky
• Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)																		
Výzkum		AD																
		AST																
• Externí zaměstnanci [51]																		
Externí zaměstnanci financovaní z operačních prostředků (bývalé položky „BA“).	– v ústředí	SZ																
		VNO																
		ZAP																
	– při delegacích Unie	SZ																
		MZ																
		VNO																
		ZAP																
		MOD																
Výzkum		SZ																
		VNO																
		ZAP																

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

Jiné rozpočtové položky (*upřesněte*)																	
Mezisoučet – mimo OKRUH 7 víceletého finančního rámce																	

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Odhadovaný dopad na lidské zdroje agentury ENISA

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), jíž byl aktem o kybernetické bezpečnosti udělen nový trvalý mandát, by členským státům a Komisi pomohla v provádění revidované směrnice o bezpečnosti sítí a informací. V důsledku revidované směrnice o bezpečnosti sítí a informací bude mít agentura ENISA od roku 2022/2023 další oblasti činnosti. I když se tyto oblasti činnosti budou vykonávat v rámci obecných úkolů agentury ENISA v souladu s jejím mandátem, budou pro agenturu znamenat další pracovní zátěž. Přesněji řečeno by se od agentury ENISA v rámci návrhu Komise revidované směrnice o bezpečnosti sítí a informací vyžadovalo, aby do svého pracovního programu kromě svých současných oblastí činnosti výslovně zahrnula mimo jiné také tyto činnosti: i) vytvořit a spravovat evropský registr zranitelnosti (čl. 6 odst. 2 návrhu); ii) poskytnout sekretariát evropské síti styčných organizací pro kybernetické krize (CyCLONe) (článek 14 návrhu) a vydávat roční zprávu o stavu kybernetické bezpečnosti v EU (článek 15 návrhu); iii) podporovat organizaci vzájemných hodnocení mezi členskými státy (článek 16 návrhu); iv) shromažďovat souhrnné údaje o incidentech z členských států a vydávat technické pokyny (čl. 20 odst. 9 návrhu); v) vytvořit a spravovat registr pro subjekty poskytující přeshraniční služby (článek 25 návrhu). Z tohoto důvodu bude požádáno o dalších pět zaměstnanců na plný pracovní úvazek od roku 2022 s odpovídajícím rozpočtem přibližně 0,61 milionu EUR ročně, jenž tato nová pracovní místa pokryje (viz oddělený finanční výkaz pro agentury).

Z tohoto důvodu bude požádáno o dalších pět zaměstnanců na plný pracovní úvazek od roku 2022 s odpovídajícím rozpočtem, jenž tato nová pracovní místa pokryje.

☐ Návrh/podnět nevyžaduje využití prostředků správní povahy

☐X Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **N** [52] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)	**CELKEM**

[52] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

Dočasní zaměstnanci (třídy AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Dočasní zaměstnanci (třídy AST)								
Smluvní zaměstnanci	0,160	0,160	0,160	0,160	0,160	0,160		
Vyslaní národní odborníci								**0,96**

CELKEM	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Požadavky na zaměstnance (FTE):

	Rok **N** [53] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**CELKEM**
Dočasní zaměstnanci (třídy AD)	3	3	3	3	3	3		**18**
Dočasní zaměstnanci (třídy AST)								

[53] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

Smluvní zaměstnanci	2	2	2	2	2	2		**12**
Vyslaní národní odborníci								

CELKEM	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Výše ostatních správních výdajů

☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.
X☐ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

OKRUH 7 víceletého finančního rámce	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Celkem**
V ústředí:								
Náklady na služební cesty a reprezentaci	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Náklady na konference a zasedání	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Výbory[54]								
Studie a konzultace								

[54] Upřesněte druh výboru a skupinu, do níž náleží.

Informační a řídicí systémy								
Zařízení a služby IKT[55]								
Jiné rozpočtové položky (*podle potřeby upřesněte*)								
Při delegacích Unie								
Náklady na služební cesty, konference a reprezentaci								
Další odborné vzdělávání zaměstnanců								
Pořízení a pronájem budov a související výdaje								
Zařízení, nábytek, dodávky a služby								
Mezisoučet za OKRUH 7 víceletého finančního rámce	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

[55] IKT: Informační a komunikační technologie: musí být konzultováno GŘ DIGIT.

v milionech EUR (zaokrouhleno na tři desetinná místa)

Mimo OKRUH 7 víceletého finančního rámce	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**Celkem**
Výdaje na technickou a administrativní pomoc (mimo externí zaměstnance) z operačních prostředků (bývalé položky „BA“)								
– v ústředí								
– při delegacích Unie								
Ostatní výdaje na řízení v oblasti výzkumu								
Jiné rozpočtové položky (*podle potřeby upřesněte*)								
Mezisoučet – mimo OKRUH 7 víceletého finančního rámce								

CELKEM **OKRUH 7 a mimo OKRUH 7** víceletého finančního rámce	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Potřeby v oblasti správních prostředků budou pokryty z prostředků, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na stávající rozpočtová omezení.

3. Metody výpočtu použité k odhadu nákladů

3.1 Lidské zdroje

Tato část objasňuje metodu výpočtu použitou k odhadu potřebných lidských zdrojů (předpokládané pracovní vytížení, včetně konkrétních pracovních míst (pracovní profily Sysper 2), kategorie zaměstnanců a příslušné průměrné náklady)

OKRUH 7 víceletého finančního rámce

POZN.: Průměrné náklady pro každou kategorii zaměstnanců v ústředí jsou k dispozici na stránkách BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx

• Úředníci a dočasní zaměstnanci

6 úředníků na plný úvazek (průměrné náklady 0,150) = 0,9 za rok

- příprava aktů v přenesené pravomoci podle čl. 18 odst. 6, čl. 21 odst. 2, článku 36,
- příprava prováděcích aktů podle čl. 12 odst. 8, čl. 18 odst. 5, čl. 20 odst. 11,
- poskytnutí sekretariátu skupině pro spolupráci v oblasti bezpečnosti sítí a informací,
- organizace plenárních zasedání a pracovních schůzí skupiny pro spolupráci v oblasti bezpečnosti sítí a informací,
- koordinace práce členských států na různých dokumentech (pokyny, sady nástrojů atd.),
- spolupráce s ostatními útvary Komise, agenturou ENISA a vnitrostátními orgány s ohledem na provádění směrnice o bezpečnosti sítí a informací,
- analýza vnitrostátních metod a osvědčených postupů souvisejících s prováděním směrnice o bezpečnosti sítí a informací.

• Externí zaměstnanci

3 smluvní zaměstnanci (průměrné náklady 0,08) = 0,24 za rok

- Podpora při plnění všech výše uvedených úkolů dle potřeby

Mimo OKRUH 7 víceletého finančního rámce

• Pouze pracovní místa financovaná z rozpočtu na výzkum

• Externí zaměstnanci

3.2 Ostatní správní výdaje

Uveďte podrobnosti o metodě výpočtu použité pro jednotlivé rozpočtové položky,

a zejména příslušné předpoklady (např. počet zasedání za rok, průměrné náklady atd.).

OKRUH 7 víceletého finančního rámce

Zasedání: Plenární zasedání skupiny pro spolupráci v oblasti bezpečnosti sítí a informací se pořádají obvykle čtyřikrát ročně. Komise pokrývá náklady související s cateringem a cestovními výdaji zástupců 27 členských států (jeden zástupce na členský stát). Náklady jednoho zasedání mohou dosáhnout až 15 000 EUR, což znamená 60 000 EUR ročně.

Služební cesty: Služební cesty souvisejí s monitorováním provádění směrnice o bezpečnosti sítí a informací. Příklad: V jednom roce (květen 2019 – červenec 2020) jsme měli uspořádat takzvané „návštěvy zemí související s bezpečností sítí a informací“ a navštívit všech 27 členských států s cílem jednat

o provádění směrnice o bezpečnosti sítí a informací v EU.

Mimo OKRUH 7 víceletého finančního rámce

PŘÍLOHA 7

ROZHODNUTÍ KOMISE

o vnitřních pravidlech pro plnění souhrnného rozpočtu Evropské unie (oddíl Evropská komise), určené útvarům Komise

LEGISLATIVNÍ FINANČNÍ VÝKAZ „AGENTURY“

Tento legislativní finanční výkaz se vztahuje na požadavek zvýšit počet zaměstnanců agentury ENISA o pět zaměstnanců na plný pracovní úvazek od roku 2022, kteří mají vykonávat doplňkové činnosti spojené s prováděním směrnice o bezpečnosti sítí a informací. Na tyto činnosti se již vztahuje mandát agentury ENISA.

Obsah

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Návrh směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

1.2. Příslušné oblasti politik

Komunikační sítě, obsah a technologie

1.3. Návrh se týká:

☐ **nové akce**

☐ **nové akce následující po pilotním projektu / přípravné akci**[56]

☒ **prodloužení stávající akce**

☐ **sloučení jedné nebo více akcí za účelem jiné/nové akce**

1.4. Cíle

1.4.1. Obecné cíle

Cílem revize je zvýšit úroveň kybernetické odolnosti celého souboru podniků působících v Evropské unii ve všech příslušných odvětvích, snížit rozdíly v odolnosti na vnitřním trhu v odvětvích, na něž se směrnice již vztahuje, a zlepšit úroveň společné znalosti situace a kolektivní schopnosti připravit se a reagovat.

1.4.2. Specifické cíle

S cílem řešit problém nízké úrovně kybernetické odolnosti podniků činných v Evropské unii je specifickým cílem zajistit, aby subjekty ve všech odvětvích, jež jsou závislé na síti a informačních systémech a jež poskytují klíčové služby hospodářství a společnosti jako celku, měly povinnost přijmout opatření v oblasti kybernetické bezpečnosti a hlásit incidenty za účelem zvýšení celkové úrovně kybernetické odolnosti na vnitřním trhu.

Aby bylo možné řešit problém nejednotné úrovně odolnosti v členských státech a odvětvích, je specifickým cílem zajistit, aby všechny subjekty, jež jsou činné v odvětvích, na něž se vztahuje právní rámec pro bezpečnost sítí a informací, měly podobnou velikost a srovnatelnou roli, spadaly pod stejný regulační režim (jsou buď v mezích jeho působnosti, nebo mimo něj), bez ohledu na to, do jaké jurisdikce v rámci EU spadají.

Aby bylo zajištěno, že všechny subjekty, jež jsou činné v odvětvích, na něž se vztahuje právní rámec pro bezpečnost sítí a informací, budou muset dodržovat stejné povinnosti na základě konceptu řízení rizik, pokud jde o bezpečnostní opatření, a budou muset hlásit všechny incidenty na základě jednotného souboru kritérií, je specifickým cílem zajištění toho, aby příslušné orgány prosazovaly pravidla stanovená právním nástrojem účinněji prostřednictvím sladěných dohledových a donucovacích opatření, a zajištění srovnatelné úrovně zdrojů napříč členskými státy, jež jsou příslušným orgánům přiděleny a které jim umožní splnit základní úkoly stanovené rámcem pro bezpečnost sítí a informací.

[56] Uvedené v čl. 58 odst. 2 písm. a) nebo b) finančního nařízení.

Aby byl řešen problém společné informovanosti o situaci a nedostatečné společné reakce na krizi, je specifickým cílem zajistit, aby podstatné informace byly mezi členskými státy vyměňovány, a to zavedením jasných povinností pro příslušné orgány týkajících se sdílení informací a spolupráce, co se týče kybernetických hrozeb a incidentů, a vytvořením společné unijní operační kapacity pro reakci na krizi.

1.4.3. Očekávané výsledky a dopady

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

Očekává se, že návrh přinese významné výhody: odhady naznačují, že může vést ke snížení nákladů na kybernetické bezpečnostní incidenty o 11,3 miliardy EUR. Došlo by k významnému rozšíření množství odvětví, na něž se rámec pro bezpečnost sítí a informací vztahuje, ale vedle zmíněných přínosů by zátěž, kterou mohou požadavky v oblasti bezpečnosti sítí a informací představovat, zejména z perspektivy dohledu, byla zároveň vyvážena jak pro nové subjekty, na něž se rámec bude vztahovat, tak pro příslušné orgány. Důvodem je to, že tento nový rámec pro bezpečnost sítí a informací by vytvořil dvouvrstvový přístup se zaměřením na velké a klíčové subjekty a s rozlišením režimu dohledu, který umožňuje pouze následné kontroly u velkého počtu z nich, zejména u těch považovaných za „důležité“, ale ne za „nezbytné“.

Celkově lze říct, že by návrh vedl k efektivním kompromisům a součinnosti a má nejlepší potenciál ze všech analyzovaných možností politiky k zajištění zvýšené a jednotné úrovně kybernetické odolnosti klíčových subjektů v Unii, která by nakonec vedla k úspoře nákladů pro podniky i společnost.

Návrh by rovněž vedl k určitým nákladům na plnění a prosazování předpisů pro příslušné orgány členských států (odhaduje se celkový nárůst prostředků přibližně o 20–30 %). Nový rámec by však také přinesl významné výhody prostřednictvím lepšího přehledu klíčových podniků a interakce s nimi, zlepšené přeshraniční operativní spolupráce a také vzájemné pomoci a mechanismů vzájemného hodnocení. To by vedlo k celkovému zvýšení kapacity v oblasti kybernetické bezpečnosti v členských státech.

U společností, které již spadají do působnosti rámce pro bezpečnost sítí a informací, se odhaduje, že by na první roky po zavedení nového rámce pro bezpečnost sítí a informací potřebovaly zvýšit své současné výdaje na bezpečnost IKT o maximálně 22 % (u společností, které již spadají do oblasti působnosti současné směrnice o bezpečnosti sítí a informací, by se jednalo o 12 %). Toto průměrné zvýšení výdajů na bezpečnost IKT by však vedlo k přiměřenému přínosu těchto investic, zejména kvůli významnému snížení výdajů na kybernetické bezpečnostní incidenty (odhadují se na 118 miliard EUR během deseti let).

Malé podniky a mikropodniky by byly z oblasti působnosti rámce pro bezpečnost sítí a informací vyňaty. U středních podniků lze očekávat, že v prvních letech po zavedení nového rámce pro bezpečnost sítí a informací by došlo ke zvýšení úrovně výdajů na bezpečnost IKT. Zároveň platí, že zvýšení úrovně bezpečnostních požadavků pro tyto subjekty by rovněž stimulovalo jejich kapacitu v oblasti kybernetické bezpečnosti a pomohlo by zlepšit jejich řízení rizik v oblasti IKT.

Očekávají se dopady na vnitrostátní rozpočty a správní orgány: v krátkodobém a střednědobém horizontu se očekává zvýšení zdrojů odhadované na přibližně 20–30 %.

Neočekávají se žádné jiné významné negativní dopady. Očekává se, že návrh povede k odolnější kapacitě v oblasti kybernetické bezpečnosti a následně bude mít výraznější zmírňující dopad na množství a závažnost incidentů, včetně porušení zabezpečení ochrany údajů. Pravděpodobně také bude mít pozitivní dopad na zajištění rovných podmínek v členských státech pro všechny subjekty spadající do oblasti působnosti rámce pro bezpečnost sítí a informací a snížení informačních asymetrií v oblasti kybernetické bezpečnosti.

1.4.4. Ukazatele výkonnosti

Upřesněte ukazatele pro sledování pokroku a dosažených výsledků.

Posouzení ukazatelů provede Komise s podporou agentury ENISA a skupinou pro spolupráci, a to tři roky po vstupu nového právního aktu pro bezpečnost sítí a informací v platnost. Mezi některé ukazatele monitorování, na jejichž základě bude posuzován úspěch přezkumu směrnice o bezpečnosti sítí a informací, patří:

• Vylepšené řešení incidentů: přijímáním opatření v oblasti kybernetické bezpečnosti společnosti zlepšují nejen svou schopnost zcela se vyhnout určitým incidentům, ale také svou schopnost na incidenty reagovat. Mezi měřítka úspěšnosti proto patří i) snížení průměrné doby potřebné k odhalení incidentu; ii) doba, kterou organizace v průměru potřebují k překonání účinků incidentu a iii) průměrné výdaje na škodu způsobenou incidentem.

• Vyšší informovanost o kybernetických bezpečnostních rizicích u vrcholného vedení společností: tím, že se od společností bude vyžadovat přijetí opatření, by revidovaná směrnice o bezpečnosti sítí a informací přispěla ke zvyšování povědomí vrcholného vedení o rizicích souvisejících s kybernetickou bezpečností. To lze měřit zkoumáním toho, do jaké míry společnosti spadající do oblasti působnosti bezpečnost sítí a informací upřednostňují kybernetickou bezpečnost v interních firemních zásadách a postupech, což dokládají jejich interní dokumenty, příslušné školicí programy a činnosti pro zvyšování povědomí pro zaměstnance a upřednostňování investic do IKT v souvislosti s bezpečností. Vedení všech nezbytných a důležitých subjektů by rovněž mělo znát pravidla stanovená směrnicí o bezpečnosti sítí a informací.

• Vyrovnání výdajů pro konkrétní odvětví: výdaje na bezpečnost IKT se mezi jednotlivými odvětvími v EU výrazně liší. Pokud se od společností ve více odvětvích bude vyžadovat přijetí opatření, pak by mělo mezi odvětvími a členskými státy dojít ke snížení odchylek od průměrných výdajů na bezpečnost IKT v konkrétním odvětví vyjádřených jako procento celkových výdajů na IKT.

• Silnější příslušné orgány a větší spolupráce: revidovaná směrnice o bezpečnosti sítí a informací příslušným orgánům možná svěří další úkoly. To by mělo měřitelný dopad na finanční a lidské zdroje věnované agenturám pro kybernetickou bezpečnost na vnitrostátní úrovni a rovněž pozitivní dopad na schopnost příslušných orgánů proaktivně spolupracovat, a tedy zvýšit počet případů, kdy příslušné orgány spolupracují za účelem řešení přeshraničních incidentů nebo provádění společných činností v oblasti dohledu.

• Intenzívnější sdílení informací: revidovaná směrnice o bezpečnosti sítí a informací by rovněž zlepšila sdílení informací mezi společnostmi a s příslušnými orgány. Jedním z cílů přezkumu by mohlo být zvýšení počtu subjektů podílejících se na různých formách sdílení informací.

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu

Cílem návrhu je zvýšit úroveň kybernetické odolnosti celého souboru podniků působících v Evropské unii ve všech příslušných odvětvích, snížit rozdíly v odolnosti na vnitřním trhu v odvětvích, na něž se směrnice již vztahuje, a zlepšit úroveň společné znalosti situace a kolektivní schopnosti připravit se a reagovat. Bude vycházet z toho, čeho bylo dosaženo prováděním směrnice (EU) 2016/1148 během uplynulých čtyř let.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

Odolnost v oblasti kybernetické bezpečnosti v Unii nemůže být účinná, pokud k ní bude přistupováno rozdílně prostřednictvím národních nebo regionálních izolovaných sil. Směrnice o bezpečnosti sítí a informací začala tento nedostatek řešit stanovením rámce pro bezpečnost sítí a informačních systémů na vnitrostátní úrovni a na úrovni Unie. První pravidelný přezkum této směrnice však poukázal na řadu neodmyslitelných nedostatků, které nakonec vedly ke značným rozdílům v jednotlivých členských státech, pokud jde o schopnosti, plánování a úroveň ochrany, které současně ovlivňují rovné podmínky pro podobné společnosti na vnitřním trhu.

Intervence EU, která jde nad rámec současných opatření směrnice o bezpečnosti sítí a informací, je odůvodněna zejména: i) přeshraniční povahou problému; ii) potenciálem opatření EU zlepšit a usnadnit účinné vnitrostátní politiky; iii) přínosem koordinovaných a společných politických opatření v oblasti bezpečnosti sítí a informací k účinnému zajištění ochrany údajů a soukromí.

Uvedených cílů lze proto dosáhnout snáze, dojde-li k akci na úrovni EU, než budou-li členské státy postupovat samostatně.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Směrnice o bezpečnosti sítí a informací je prvním horizontálním nástrojem vnitřního trhu, jehož cílem je zlepšit odolnost sítí a systémů v Unii vůči kybernetickým bezpečnostním rizikům. Od svého vstupu v platnost v roce 2016 již velkou měrou přispěla ke zvýšení společné úrovně kybernetické bezpečnosti v členských státech. Přezkum fungování a provádění směrnice však poukázal na řadu nedostatků, které je třeba spolu s rostoucí digitalizací a potřebou aktuálnější reakce řešit v revidovaném právním aktu.

1.5.4. Slučitelnost s víceletým finančním rámcem a možná součinnost s dalšími vhodnými nástroji

Nový návrh je zcela v souladu s dalšími souvisejícími iniciativami, jako je návrh nařízení o digitální provozní odolnosti finančního sektoru („DORA“) a návrh směrnice o odolnosti kritických provozovatelů základních služeb. Rovněž je v souladu s evropským kodexem pro elektronické komunikace, obecným nařízením o ochraně osobních údajů a nařízením eIDAS.

Návrh tvoří nezbytnou část strategie bezpečnostní unie EU.

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

Správa těchto úkolů ze strany agentury ENISA vyžaduje specifické profily a další pracovní zátěž, kterou nelze absorbovat bez zvýšení lidských zdrojů.

1.6. Doba trvání a finanční dopad návrhu/podnětu

☐ **časově omezená doba trvání**

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

– ☐ Finanční dopad od RRRR do RRRR

☒ **časově neomezená doba trvání**

– Provádění s obdobím rozběhu od roku 2022 do roku 2025,

– poté plné fungování.

1.7. Předpokládaný způsob řízení[57]

☒ **Přímé řízení** Komisí

prostřednictvím

– ☐ výkonných agentur

☐ **Sdílené řízení** s členskými státy

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

☐ mezinárodní organizace a jejich agentury (upřesněte),

☐ EIB a Evropský investiční fond,

☒ subjekty uvedené v článcích 70 a 71,

☐ veřejnoprávní subjekty,

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

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

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

Poznámky

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), jíž byl aktem o kybernetické bezpečnosti udělen nový trvalý mandát, by členským státům a Komisi pomohla v provádění revidované směrnice o bezpečnosti sítí a informací.

V důsledku revidované směrnice o bezpečnosti sítí a informací bude mít agentura ENISA od roku 2022/2023 další oblasti činnosti. I když se tyto oblasti činnosti budou vykonávat v rámci obecných úkolů agentury ENISA v souladu s jejím mandátem, budou pro agenturu znamenat další pracovní zátěž. Přesněji řečeno by se od agentury ENISA v rámci návrhu Komise revidované směrnice o bezpečnosti sítí a informací vyžadovalo, aby do svého pracovního programu kromě svých současných oblastí činnosti výslovně zahrnula mimo jiné také tyto činnosti: i) vytvořit a spravovat evropský registr zranitelnosti (čl. 6 odst. 2 návrhu); ii) poskytnout sekretariát evropské síti styčných organizací pro kybernetické krize (CyCLONe) (článek 14 návrhu) a vydávat roční zprávu o stavu kybernetické

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

bezpečnosti v EU (článek 15 návrhu); iii) podporovat organizaci vzájemných hodnocení mezi členskými státy (článek 16 návrhu); iv) shromažďovat agregované údaje o incidentech z členských států a vydávat technické pokyny (čl. 20 odst. 9 návrhu); v) vytvořit a spravovat registr pro subjekty poskytující přeshraniční služby (článek 25 návrhu).

Z tohoto důvodu bude požádáno o dalších pět zaměstnanců na plný pracovní úvazek od roku 2022 s odpovídajícím rozpočtem ve výši přibližně 0,61 milionu EUR ročně, jenž tato nová pracovní místa pokryje.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Komise bude pravidelně přezkoumávat uplatňování této směrnice a podávat zprávy Evropskému parlamentu a Radě, poprvé tři roky po vstupu v platnost.

Komise rovněž posoudí správnost provedení směrnice do vnitrostátního práva členských států.

Sledování návrhu a podávání zpráv o něm bude prováděno v souladu se zásadami uvedenými v trvalém mandátu agentury ENISA podle nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti).

Zdroje údajů použité pro plánované sledování budou pocházet zejména od agentury ENISA, skupiny pro spolupráci, sítě CSIRT a orgánů členských států. Kromě údajů získaných ze zpráv (včetně výročních zpráv o činnosti) agentury ENISA, skupiny pro spolupráci a sítě CSIRT se v případě potřeby použijí konkrétní nástroje pro shromažďování údajů (například průzkumy prováděné u vnitrostátních orgánů, Eurobarometr a zprávy z kampaně Evropský měsíc kybernetické bezpečnosti a z celoevropských cvičení).

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

Provádění směrnice bude řídit útvar v rámci GŘ CNECT odpovědný za tuto oblast politiky.

Co se týče správy agentury ENISA, uvádí článek 15 aktu o kybernetické bezpečnosti podrobný seznam kontrolních funkcí správní rady agentury ENISA.

Podle článku 31 aktu o kybernetické bezpečnosti je výkonný ředitel agentury ENISA odpovědný za provádění rozpočtu agentury a interní auditor Komise vykonává nad agenturou ENISA stejné pravomoci jako nad útvary Komise. Správní rada agentury ENISA vydá stanovisko ke konečné účetní závěrce agentury ENISA.

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

Velmi nízké riziko, jelikož je již zaveden ekosystém směrnice o bezpečnosti sítí a informací, který se již vztahuje na agenturu ENISA, jež má trvalý mandát od vstupu aktu o kybernetické bezpečnosti v platnost v roce 2019.

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

Požadované navýšení rozpočtu uplatňuje Hlavu 1 a má financovat platy. To znamená velmi nízké riziko chyby na úrovni platby.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření, např. opatření uvedená ve strategii pro boj proti podvodům.

Použijí se preventivní a ochranná opatření agentury ENISA, konkrétně:

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

– V zájmu boje proti podvodům, korupci a jiným protiprávním činnostem se na agenturu bez omezení vztahuje nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 a nařízení Rady ze dne 25. května 1999 o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF).

– Podle článku 33 aktu o kybernetické bezpečnosti přistoupila agentura ENISA dne 28. prosince 2019 k interinstitucionální dohodě ze dne 25. května 1999 mezi Evropským parlamentem, Radou Evropské unie a Komisí Evropských společenství o vnitřním vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF). ENISA neprodleně vydá odpovídající předpisy vztahující se na veškeré její zaměstnance.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

- Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdajů	Příspěvek			
	Číslo	RP/NRP[58]	zemí ESVO[59]	kandidátských zemí[60]	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
2	02 10 04	/NRP	ANO	NE	NE	/NE

- Nové rozpočtové položky, jejichž vytvoření se požaduje

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdajů	Příspěvek			
	Číslo	RP/NRP	zemí ESVO	kandidátských zemí	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b)

[58] RP = rozlišené prostředky / NRP = nerozlišené prostředky.
[59] ESVO: Evropské sdružení volného obchodu.
[60] Kandidátské země a případně potenciální kandidáti ze západního Balkánu.

						finančního nařízení
	[XX.YY.YY.YY]		ANO/NE	ANO/NE	ANO/NE	ANO/NE

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	Číslo	[Okruh…2 Jednotný trh, inovace a digitální agenda……...……]

[Subjekt]: <…ENISA….>			Rok **N**[61] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6) **2026**	**2027**		**CELKEM**
Hlava 1:	Závazky	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Platby	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Hlava 2:	Závazky	(1a)								
	Platby	(2a)								
Hlava 3:	Závazky	(3a)								
	Platby	(3b)								
CELKEM prostředky pro [subjekt] <ENISA…….>	Závazky	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Platby	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

Okruh víceletého finančního rámce	**5**	Správní výdaje

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			**CELKEM**
GŘ: <…….>									
• Lidské zdroje									
• Ostatní správní výdaje									
GŘ <…….> CELKEM	Prostředky								

CELKEM prostředky na OKRUH 5 víceletého finančního rámce	(Závazky celkem = platby celkem)								

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **N**[62] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6) **2026**	**2027**		**CELKEM**
CELKEM prostředky na OKRUHY 1 až 5 víceletého finančního rámce	Závazky	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Platby	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

3.2.2. Odhadovaný dopad na prostředky [subjektu]

– ☐x Návrh/podnět nevyžaduje využití operačních prostředků.

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

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

Uveďte cíle a výstupy ⇩			Rok **N**		Rok **N+1**		Rok **N+2**		Rok **N+3**		Vložit počet let podle trvání finančního dopadu (viz bod 1.6)						**CELKEM**	
	VÝSTUPY																	
	Druh[63]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Celkové náklady
SPECIFICKÝ CÍL č. 1[64]…																		
– Výstup																		
– Výstup																		
– Výstup																		
Mezisoučet za specifický cíl č. 1																		
SPECIFICKÝ CÍL č. 2 …																		
– Výstup																		
Mezisoučet za specifický cíl č. 2																		
CELKOVÉ NÁKLADY																		

63 Výstupy se rozumí produkty a služby, které mají být dodány (např. počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

64 Popsaný v bodě 1.4.2. „Specifické cíle…“

3.2.3. Odhadovaný dopad na lidské zdroje agentury ENISA

3.2.3.1. Shrnutí

V důsledku revidované směrnice o bezpečnosti sítí a informací bude mít ENISA od roku 2022/2023 další úkoly. I když se tyto úkoly budou vykonávat v rámci mandátu agentury ENISA, budou pro agenturu znamenat další pracovní zátěž. Přesněji řečeno bude mít agentura ENISA vedle svých současných úkolů podle návrhu Komise na revidovanou směrnici o bezpečnosti sítí a informací za úkol mimo jiné i) vytvořit a spravovat evropský registr zranitelností (čl. 6 odst. 2); ii) poskytnout sekretariát evropské síti styčných organizací pro kybernetické krize (CyCLONe) (článek 14) a vydávat roční zprávu o stavu kybernetické bezpečnosti v EU (článek 15); iii) podporovat organizaci vzájemných hodnocení mezi členskými státy (článek 16); iv) shromažďovat souhrnné údaje o incidentech z členských států a vydávat technické pokyny (čl. 20 odst. 9); v) vytvořit a spravovat registr pro subjekty poskytující přeshraniční služby (článek 25).

Z tohoto důvodu bude požádáno o dalších pět zaměstnanců na plný pracovní úvazek od roku 2022 s odpovídajícím rozpočtem, jenž tato nová pracovní místa pokryje.

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy

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

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **N** [65] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6) **2026**	**2027**		**CELKEM**
Dočasní zaměstnanci (třídy AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Dočasní zaměstnanci (třídy AST)								
Smluvní zaměstnanci	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Vyslaní národní odborníci								
CELKEM	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Požadavky na zaměstnance (FTE):

[65] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

	Rok **N** [66] **2022**	Rok **N+1** **2023**	Rok **N+2** **2024**	Rok **N+3** **2025**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6) **2026**	**2027**		**CELKEM**
Dočasní zaměstnanci (třídy AD)	3	3	3	3	3	3		**18**
Dočasní zaměstnanci (třídy AST)								
Smluvní zaměstnanci	2	2	2	2	2	2		**12**
Vyslaní národní odborníci								
CELKEM	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Odhadované potřeby v oblasti lidských zdrojů pro mateřské GŘ.

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.

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

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

	Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
• **Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)**							
XX 01 01 01 (v ústředí a v zastoupeních Komise)							
XX 01 01 02 (při delegacích)							
XX 01 05 01 (v nepřímém výzkumu)							
10 01 05 01 (v přímém výzkumu)							
• **Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)**[67]							

[66] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

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

XX 01 02 01 (SZ, VNO, ZAP z celkového rámce)								
XX 01 02 02 (SZ, MZ, VNO, ZAP a MOD při delegacích)								
XX 01 04 ***rr***[68]	– v ústředí[69]							
	– při delegacích							
XX 01 05 02 (SZ, VNO, ZAP – v nepřímém výzkumu)								
10 01 05 02 (SZ, VNO, ZAP – v přímém výzkumu)								
Jiné rozpočtové položky (upřesněte)								
CELKEM								

XX je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci	
Externí zaměstnanci	

Popis výpočtu nákladů na jednotky FTE by měl být zahrnut v příloze V, oddíle 3.

68 Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

69 Zejména pro strukturální fondy, Evropský zemědělský fond pro rozvoj venkova (EZFRV) a Evropský rybářský fond (ERF).

3.2.4. *Slučitelnost se stávajícím víceletým finančním rámcem*

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

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

Upřesněte, jaká úprava se požaduje, příslušné rozpočtové položky a odpovídající částky. Návrh je kompatibilní s víceletým finančním rámcem na období 2021–2027. Vyrovnání rozpočtu požadovaného k pokrytí nárůstu lidských zdrojů v agentuře ENISA se provede snížením rozpočtu programu Digitální Evropa ve stejném okruhu o stejnou částku.

– ☐ Návrh/podnět vyžaduje použití nástroje pružnosti nebo revizi víceletého finančního rámce[70].

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky a odpovídající částky.

3.2.5. *Příspěvky třetích stran*

– Návrh/podnět nepočítá se spolufinancováním od třetích stran.

– Návrh/podnět počítá se spolufinancováním podle následujícího odhadu:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			Celkem
Upřesněte spolufinancující subjekt								
Spolufinancované prostředky CELKEM								

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

3.3. Odhadovaný dopad na příjmy

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

– ☐ Návrh/podnět má tento finanční dopad:

☐ na vlastní zdroje

☐ na jiné příjmy

☐ uveďte, zda je příjem účelově vázán na výdajové položky

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová rozpočtová položka:	Prostředky dostupné v běžném rozpočtovém roce	Dopad návrhu/podnětu[71]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
Článek …….								

U účelově vázaných různých příjmů upřesněte dotčené výdajové rozpočtové položky.

Upřesněte způsob výpočtu dopadu na příjmy.

[71] Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.