SMĚRNICE

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2555

ze dne 14. prosince 2022

o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

(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 Evropské centrální banky ([1]),

s ohledem na stanovisko Evropského hospodářského a sociálního výboru ([2]),

po konzultaci s Výborem regionů,

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

vzhledem k těmto důvodům:

(1) Cílem směrnice Evropského parlamentu a Rady (EU) 2016/1148 ([4]) bylo rozvíjet 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 incidentů, a přispívat tak k bezpečnosti Unie a k účinnému fungování jejího hospodářství a společnosti.

(2) Od vstupu směrnice (EU) 2016/1148 v platnost bylo ve zvyšování úrovně kybernetické odolnosti Unie 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 národních rámců pro bezpečnost sítí a informačních systémů stanovením národních strategií pro bezpečnost sítí a informačních systémů a stanovením vnitrostátních schopností a prováděním regulačních opatření pokrývajících základní infrastruktury a subjekty určené každým členským státem. Směrnice (EU) 2016/1148 rovněž přispěla ke spolupráci na úrovni Unie vytvořením skupiny pro spolupráci a sítě vnitrostátních bezpečnostních týmů typu CSIRT. 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.

(3) S rychlou digitální transformací a vzájemnou propojeností společnosti, včetně přeshraniční výměny, se sítě a informační systémy staly ústředním prvkem každodenního života. Tento vývoj vedl k prudkému rozšíření prostředí kybernetických hrozeb a přináší nové výzvy, které vyžadují přizpůsobené, koordinované a inovativní reakce ve všech členských státech. Počet, rozsah, sofistikovanost, četnost výskytu a dopad incidentů narůstají a představují značnou hrozbu pro fungování sítí a informačních systémů. V důsledku toho mohou 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

([1]) Úř. věst. C 233, 16.6.2022, s. 22.
([2]) Úř. věst. C 286, 16.7.2021, s. 170.
([3]) Postoj Evropského parlamentu ze dne 10. listopadu 2022 (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne 28. listopadu 2022.
([4]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

bezpečnosti jsou dnes proto pro řádné fungování vnitřního trhu důležitější než kdy předtím. Kybernetická bezpečnost je navíc klíčovým faktorem, který mnoha kritickým odvětvím umožňuje úspěšně podstoupit digitální transformaci a plně využívat hospodářských, sociálních a udržitelných přínosů digitalizace.

(4) Právním základem směrnice (EU) 2016/1148 byl článek 114 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“), jehož cílem je vytvoření a fungování vnitřního trhu posílením opatření ke sbližování vnitrostátních předpisů. Požadavky kybernetické bezpečnosti kladené na subjekty poskytující služby nebo vykonávající hospodářsky významné 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 subjekty, 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 neadekvátní koncepce nebo provádění požadavků na kybernetickou bezpečnost v jednom členském státě může mít důsledky pro úroveň kybernetické bezpečnosti jiných členských států, zejména vzhledem k intenzitě přeshraniční výměny. 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 oznamování incidentů, které v ní byly stanoveny. Tyto povinnosti byly proto na úrovni členských států provedeny výrazně odlišnými způsoby. Podobné rozdíly existují v provádění ustanovení směrnice (EU) 2016/1148 týkající 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 kybernetické odolnosti v důsledku uplatňování odlišných opatření. Tyto rozdíly by v konečném důsledku mohly vést k větší zranitelnosti některých členských států vůči kybernetickým hrozbám, které se mohou rozšířit na celou Unii. 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 a donucovacích opatření, jež jsou pro účinné vymáhání těchto povinností klíčové. Směrnice (EU) 2016/1148 by proto měla být zrušena a nahrazena touto směrnicí.

(6) Se zrušením směrnice (EU) 2016/1148 by měla být oblast působnosti podle odvětví rozšířena na větší část ekonomiky, aby bylo zajištěno komplexní pokrytí odvětví a služeb, které mají zásadní význam pro klíčové společenské a hospodářské činnosti v rámci vnitřního trhu. Cílem této směrnice je zejména odstranit nedostatky v souvislosti s rozlišováním mezi provozovateli základních služeb a poskytovateli digitálních služeb, které se ukázalo jako zastaralé, neboť nezohledňuje důležitost odvětví nebo služeb z hlediska společenských a hospodářských činností na vnitřním trhu.

(7) Podle směrnice (EU) 2016/1148 byly členské státy odpovědné za určení subjektů, které splňují kritéria pro zařazení mezi provozovatele základních služeb. S cílem odstranit značné rozdíly mezi členskými státy v tomto ohledu a zajistit právní jistotu pro všechny příslušné subjekty, pokud jde o opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti, by mělo být stanoveno jednotné kritérium, které určí subjekty, jež do oblasti působnosti této směrnice spadají. Toto kritérium by mělo spočívat v uplatnění pravidla velikostního omezení, podle kterého by do oblasti působnosti této směrnice spadaly všechny subjekty, které lze považovat za střední podniky podle článku 2 přílohy doporučení Komise 2003/361/ES ([5]), nebo které překračují stropy, jež jsou pro střední podniky stanoveny v odstavci 1 uvedeného článku a které působí v odvětvích nebo poskytují druhy služeb nebo vykonávají činnosti, na něž se vztahuje tato směrnice. Členské státy by měly rovněž stanovit, že do oblasti

([5]) 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).

působnosti této směrnice spadají některé malé podniky a mikropodniky ve smyslu čl. 2 odst. 2 a 3 uvedené přílohy, které splňují zvláštní kritéria poukazující na klíčovou úlohu pro společnost, ekonomiku, nebo pro konkrétní odvětví či druhy služeb.

(8) Vynětí subjektů veřejné správy z oblasti působnosti této směrnice by se mělo týkat subjektů, jež vykonávají svou činnost převážně v oblasti národní bezpečnosti, veřejné bezpečnosti, obrany nebo vymáhání práva, včetně prevence, vyšetřování, odhalování a stíhání trestných činů. Z oblasti působnosti této směrnice by však neměly být vyňaty subjekty veřejné správy, jejichž činnost s těmito oblastmi souvisí pouze okrajově. Subjekty s regulační pravomocí se pro účely této směrnice za subjekty vykonávající činnost v oblasti vymáhání práva nepovažují, a tudíž z oblasti působnosti této směrnice z tohoto důvodu vyňaty nejsou. Subjekty veřejné správy, které jsou zřízeny společně se třetí zemí v souladu s mezinárodní dohodou, jsou z oblasti působnosti této směrnice vyňaty. Tato směrnice se nevztahuje na diplomatické a konzulární mise členských států ve třetích zemích ani na jejich sítě a informační systémy, pokud jsou tyto systémy umístěny v prostorách mise nebo jsou provozovány pro uživatele ve třetí zemi.

(9) Členské státy by měly být schopny přijmout nezbytná opatření, aby zajistily ochranu základních zájmů národní bezpečnosti, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily prevenci, vyšetřování, odhalování a stíhání trestných činů. Za tímto účelem by členské státy měly mít možnost vyjmout konkrétní subjekty, které vykonávají činnosti v oblasti národní bezpečnosti, veřejné bezpečnosti, obrany, nebo vymáhání práva, včetně prevence, vyšetřování, odhalování a stíháním trestných činů, v souvislosti s uvedenými činnostmi z určitých povinností stanovených v této směrnici. Pokud subjekt poskytuje služby výhradně subjektu veřejné správy, který je vyňat z oblasti působnosti této směrnice, měly by mít členské státy možnost vyjmout uvedený subjekt z určitých povinností stanovených v této směrnici, pokud jde o tyto služby. Žádný členský stát by navíc neměl být povinen poskytovat informace, jejichž zpřístupnění by bylo v rozporu se základními zájmy jeho národní bezpečnosti, veřejné bezpečnosti či obrany. V uvedených souvislostech by měly být zohledněny vnitrostátní a unijní pravidla o ochraně utajovaných informací, dohody o zachování důvěrnosti údajů, nebo neformální dohody o zachování důvěrnosti, jako je například tzv. „TLP protokol“ (Traffic Light Protocol). TLP protokol je třeba chápat jako prostředek poskytování informací o jakýchkoli omezeních, pokud jde o další šíření informací. Používá se téměř ve všech týmech pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“) a některých střediscích pro sdílení a analýzu informací.

(10) I když se tato směrnice vztahuje na subjekty vykonávající činnosti v oblasti výroby elektřiny v jaderných elektrárnách, některé z těchto činnosti mohou nicméně souviset s národní bezpečností. V takovém případě by měl být členský stát schopen vykonávat svou odpovědnost za ochranu národní bezpečnosti, pokud jde o tyto činnosti, včetně činností v rámci jaderného hodnotového řetězce, v souladu se Smlouvami.

(11) Některé subjekty vykonávají činnost v oblastech národní bezpečnosti, veřejné bezpečnosti, obrany nebo vymáhání práva, včetně prevence, vyšetřování, odhalování a stíhání trestných činů, a zároveň poskytují služby vytvářející důvěru. Poskytovatelé služeb vytvářejících důvěru, kteří spadají do oblasti působnosti nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([6]), by měli spadat i do oblasti působnosti této směrnice, aby byla zajištěna stejná úroveň bezpečnostních požadavků a dohledu, jaká byla stanovena v uvedeném nařízení pro poskytovatele služeb vytvářejících důvěru. V souladu s tím, že některé konkrétní služby jsou vyňaty z působnosti nařízení (EU) č. 910/2014, by se tato směrnice neměla vztahovat na poskytování služeb vytvářejících důvěru, které jsou používány výhradně v rámci uzavřených systémů vyplývajících z vnitrostátního práva nebo z dohod mezi určeným okruhem účastníků.

([6]) 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).

(12) Poskytovatelé poštovních služeb ve smyslu směrnice Evropského parlamentu a Rady 97/67/ES ([7]), včetně poskytovatelů kurýrních doručovacích služeb, by měli této směrnici podléhat, pokud poskytují alespoň jeden z kroků v poštovním řetězci, zejména výběr, třídění, přepravu nebo dodání poštovních zásilek, včetně služeb souvisejících s vyzvedáváním, a současně by měla být zohledněna míra jejich závislosti na sítích a informačních systémech. Přepravní služby, které nejsou poskytovány ve spojení s některým z těchto kroků, by měly být vyňaty z oblasti působnosti poštovních služeb.

(13) Jelikož kybernetické hrozby jsou stále intenzivnější a důmyslnější, měly by se členské státy snažit zajistit, aby subjekty, které jsou vyňaty z oblasti působnosti této směrnice, dosáhly vysoké úrovně kybernetické bezpečnosti, a měly by podporovat provádění rovnocenných opatření k řízení kybernetických bezpečnostních rizik, která zohledňují citlivou povahu těchto subjektů.

(14) Na zpracování osobních údajů podle této směrnice se uplatní právo Unie v oblasti ochrany údajů a právo Unie v oblasti ochrany soukromí. Touto směrnicí není zejména dotčeno nařízení Evropského parlamentu a Rady (EU) 2016/679/ES ([8]) a směrnice Evropského parlamentu a Rady 2002/58/ES ([9]). Touto směrnicí by proto neměly být mimo jiné dotčeny úkoly a pravomoci orgánů příslušných ke sledování souladu s platným právem Unie v oblasti ochrany údajů a právem Unie v oblasti ochrany soukromí.

(15) Subjekty spadající do oblasti působnosti této směrnice pro účely dodržování opatření k řízení kybernetických bezpečnostních rizik a oznamovacích povinností by měly být zařazeny do dvou kategorií: základní subjekty a důležité subjekty, s přihlédnutím k míře kritické důležitosti, pokud jde o odvětví nebo druh služby, kterou poskytují, a také k jejich velikosti. V této souvislosti by se v případě potřeby měla náležitě zohlednit veškerá relevantní odvětvová posouzení rizik nebo pokyny příslušných orgánů. Dohledové a donucovací režimy pro tyto dvě kategorie subjektů by se měly odlišovat, aby byla zajištěna spravedlivá vyváženost mezi požadavky a povinnostmi založenými na riziku na jedné straně a správní zátěží vyplývající z dohledu nad dodržováním směrnice na druhé straně.

(16) Má-li se zabránit tomu, aby subjekty, které mají partnerské podniky nebo které jsou přidruženými podniky, byly považovány za základní nebo důležité subjekty, kde by to bylo nepřiměřené, mohou členské státy při uplatňování čl. 6 odst. 2 přílohy doporučení 2003/361/ES zohlednit míru nezávislosti, v níž se subjekt ve vztahu ke svým partnerským nebo přidruženým podnikům nachází. Členské státy mohou zejména zohlednit skutečnost, že subjekt je na svém partnerovi nebo přidružených podnicích nezávislý z hlediska sítě a informačních systémů, které tento subjekt používá při poskytování svých služeb, a pokud jde o služby, které tento subjekt poskytuje. Členské státy pak mohou mít v příslušném případě za to, že takový subjekt nesplňuje kritéria pro střední podnik podle článku 2 přílohy doporučení 2003/361/ES nebo nepřekračuje stropy pro střední podniky stanovené v odstavci 1 uvedeného článku, jestliže by se po zohlednění stupně nezávislosti uvedeného subjektu tento subjekt nepovažoval za subjekt, který je středním podnikem nebo za subjekt, který tyto stropy překračuje, pokud by se zohlednily pouze jeho vlastní údaje. Povinnosti, které směrnice stanovuje partnerským a přidruženým podnikům, které do oblasti působnosti této směrnice spadají, zůstávají nedotčeny.

(17) Členské státy by měly mít možnost rozhodnout, že subjekty určené před vstupem této směrnice v platnost jako provozovatelé základních služeb podle směrnice (EU) 2016/1148 mají být považovány za základní subjekty.

([7]) 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).

([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).

([9]) 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).

(18) Má-li být zajištěn jasný přehled o subjektech spadajících do oblasti působnosti této směrnice, měly by členské státy vytvořit seznam základních a důležitých subjektů, jakož i subjektů poskytujících služby registrace jmen domén. Za tímto účelem by členské státy měly od subjektů vyžadovat, aby příslušným orgánům předkládaly alespoň následující informace: název, adresu a aktuální kontaktní údaje, a to i e-mailové adresy, rozsah IP adres a telefonní čísla, případně i s uvedením příslušného odvětví a pododvětví podle příloh, a v příslušných případech i seznam členských států, v nichž poskytují služby spadající do oblasti působnosti této směrnice. Komise by bez zbytečného odkladu měla za tímto účelem za pomoci Agentury Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“) poskytnout pokyny a šablony týkající se povinnosti předkládat informace. Pro snazší sestavování a aktualizaci seznamu základních a důležitých subjektů, jakož i subjektů poskytujících služby registrace jmen domén by měly mít členské státy možnost zavést vnitrostátní mechanismy pro registraci těchto subjektů. Existují-li registry na vnitrostátní úrovni, mohou členské státy rozhodnout o vhodných mechanismech k určení subjektů, které do oblasti působnosti této směrnice spadají.

(19) Odpovědností členských států by mělo být předložit Komisi alespoň počet základních a důležitých subjektů pro každé odvětví a pododvětví uvedené v přílohách a také příslušné informace o počtu určených subjektů, o tom, na základě kterého z postupů stanovených v této směrnici byly určeny, a o typu služby, již poskytují. Členské státy se vyzývají k výměně informací s Komisí o základních a důležitých subjektech a v případě rozsáhlého incidentu v oblasti kybernetické bezpečnosti také k výměně příslušných informací, například názvu dotčeného subjektu.

(20) Komise by měla ve spolupráci se skupinou pro spolupráci a po konzultaci s relevantními zúčastněnými stranami poskytnout pokyny ohledně plnění kritérií platných pro mikropodniky a malé podniky za účelem posouzení toho, zda spadají do působnosti této směrnice. Komise by rovněž měla zajistit, že budou mikropodnikům a malým podnikům spadajícím do oblasti působnosti této směrnice poskytovány vhodné pokyny. V této souvislosti by Komise s pomocí členských států měla mikropodnikům a malým podnikům poskytovat informace.

(21) Komise může vydat pokyny s cílem pomoci členským státům provádět ustanovení této směrnice týkající se oblasti působnosti a vyhodnotit přiměřenost opatření, jež mají být podle této směrnice přijata, zejména pokud jde o subjekty s komplexními obchodními modely nebo podmínkami provozu, kdy určitý subjekt může současně splňovat kritéria stanovená pro základní i důležité subjekty nebo současně vykonávat činnosti, z nichž některé spadají do oblasti působnosti této směrnice, a některé jsou z ní vyňaty.

(22) Tato směrnice stanoví základ pro opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti napříč odvětvími, jež spadají do oblasti její působnosti. Budou-li v zájmu zajištění vysoké úrovně kybernetické bezpečnosti v celé Unii považovány za nezbytné další odvětvové právní akty Unie týkající se opatření k řízení kybernetických bezpečnostních rizik a oznamovacích povinností, měla by Komise posoudit, zda by mohla být taková další ustanovení stanovena v prováděcím aktu podle této směrnici, aby se zabránilo roztříštěnosti ustanovení o kybernetické bezpečnosti v rámci právních aktů Unie. V případě, že by tento prováděcí akt nebyl pro uvedený účel vhodný, mohly by k zajištění vysoké úrovně kybernetické bezpečnosti v celé Unii přispět odvětvové právní akty Unie při plném zohlednění specifik a složitosti dotčených odvětví. Tato směrnice za tímto účelem nebrání přijetí dalších odvětvových právních aktů Unie týkajících se opatření k řízení kybernetických bezpečnostních rizik a oznamovacích povinností, které řádně zohlední potřebu komplexního a soudržného rámce pro kybernetickou bezpečnost. Touto směrnicí nejsou dotčeny stávající prováděcí pravomoci, jež byly Komisi svěřeny v řadě odvětví, včetně odvětví dopravy a energetiky.

(23) Pokud odvětvový právní akt Unie obsahuje ustanovení, jež vyžadují, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik nebo aby oznamovaly významné incidenty, a pokud je účinek těchto opatření alespoň rovnocenný účinku povinností stanovených v této směrnici, měla by se tato

ustanovení, včetně těch o dohledu a vymáhání, na uvedené subjekty vztahovat. Pokud se odvětvový právní akt Unie nevztahuje na všechny subjekty v konkrétním odvětví, jež náleží do oblasti působnosti této směrnice, měla by se na subjekty, na něž se uvedený akt nevztahuje, vztahovat i nadále příslušná ustanovení této směrnice.

(24) Pokud ustanovení odvětvového právního aktu Unie vyžadují, aby základní nebo důležité subjekty dodržovaly oznamovací povinnosti, jejichž účinky jsou přinejmenším rovnocenné jako u povinností stanovených v této směrnici, měla by být při vyřizování oznámení o incidentech zajištěna soudržnost a účinnost. Za tímto účelem by ustanovení o oznamování incidentů odvětvového unijního právního aktu měla týmům CSIRT, příslušným orgánům nebo jednotným kontaktním místům pro kybernetickou bezpečnost (dále jen „jednotná kontaktní místa“) podle této směrnice poskytnout k oznámením o incidentech, jež byla učiněna v souladu s odvětvovým právním aktem Unie, okamžitý přístup. Tento okamžitý přístup lze zajistit zejména tak, že oznámení o incidentech budou týmu CSIRT, příslušnému orgánu nebo jednotnému kontaktnímu místu podle této směrnice předávána bez zbytečného odkladu. Členské státy by měly v příslušných případech zavést mechanismus automatického a přímého oznamování, který zajistí při vyřizování těchto oznámení o incidentech systematické a okamžité sdílení informací s týmy CSIRT, příslušnými orgány nebo jednotnými kontaktními místy. Pro zjednodušení oznamování a zavedení mechanismu automatického a přímého oznamování by členské státy mohly v souladu s odvětvovým právním aktem Unie využít jednotné kontaktní místo.

(25) Odvětvové právní akty Unie, které stanovují opatření k řízení kybernetických bezpečnostních rizik nebo oznamovací povinnosti, jež mají přinejmenším rovnocenný účinek jako ty, které jsou stanoveny v této směrnici, by mohly stanovit, že příslušné orgány podle těchto aktů vykonávají své dohledové a vymáhací pravomoci ve vztahu k těmto opatřením nebo povinnostem za pomoci příslušných orgánů ve smyslu této směrnice. Dotčené příslušné orgány by za tímto účelem mohly uzavřít ujednání o spolupráci. Tato ujednání o spolupráci mohou mimo jiné stanovit postupy týkající se koordinace činností v oblasti dohledu, včetně postupů šetření a kontrol na místě v souladu s vnitrostátním právem a mechanismu pro výměnu příslušných informací o dohledu a vymáhání mezi příslušnými orgány, a to i pokud jde o přístup ke kybernetickým údajům, které si vyžádaly příslušné orgány ve smyslu této směrnice.

(26) Pokud odvětvové právní akty Unie vyžadují nebo motivují subjekty k oznamování významných kybernetických hrozeb, měly by členské státy rovněž podporovat sdílení informací o významných kybernetických hrozbách s týmy CSIRT, příslušnými orgány nebo jednotnými kontaktními místy ve smyslu této směrnice, aby byly tyto orgány o bezpečnostních hrozbách na kybernetické scéně lépe informovány a mohly účinně a včas reagovat v případě, že se významné kybernetické hrozby naplní.

(27) Budoucí odvětvové právní akty Unie by měly náležitě zohledňovat definice a rámec pro dohled a vymáhání stanovené v této směrnici.

(28) Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ([10]) by mělo být považováno za odvětvový právní akt Unie ve vztahu k této směrnici, pokud jde o finanční subjekty. Ustanovení nařízení (EU) 2022/2554, která se týkají řízení rizik v oblasti informačních a komunikačních technologií (dále jen „IKT“), řešení incidentů souvisejících s IKT, a zejména oznamování 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 v této směrnici. Členské státy by proto neměly uplatňovat ustanovení této směrnice o řízení kybernetických bezpečnostních rizik a o oznamovacích povinnostech, a o dohledu a vymáhání vůči finančním subjektům, na něž se vztahuje nařízení (EU) 2022/2554. Zároveň je důležité zachovat s finančním odvětvím silný vztah a výměnu informací podle této směrnice. Za tím účelem nařízení (EU) 2022/2554 umožňuje, aby se evropské orgány dohledu a příslušné orgány podle uvedeného nařízení účastnily činností skupiny pro spolupráci a aby si vyměňovaly informace a spolupracovaly s jednotnými kontaktními místy, jakož i s týmy CSIRT a příslušnými orgány podle této směrnice. Příslušné orgány podle nařízení (EU) 2022/2554 by měly předávat rovněž údaje o významných incidentech týkajících se IKT a o významných kybernetických hrozbách týmům CSIRT, příslušným orgánům nebo jednotným kontaktním místům podle této směrnice. Toho lze dosáhnout poskytnutím okamžitého přístupu

([10]) Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (viz strana 1 v tomto čísle Úředního věstníku).

k oznámením o incidentu a jejich postoupením buď přímo, nebo prostřednictvím jednotného kontaktního místa. Členské státy by kromě toho měly odvětví financí nadále zahrnovat do svých strategií kybernetické bezpečnosti a týmy CSIRT mohou zahrnout finanční odvětví do svých činností.

(29) Má-li se zabránit rozdílům v povinnostech v oblasti kybernetické bezpečnosti uložených subjektům v odvětví letectví nebo jejich zdvojování, měly by vnitrostátní orgány podle nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ([11]) a (EU) 2018/1139 ([12]) a příslušné orgány podle této směrnice spolupracovat při provádění opatření k řízení kybernetických bezpečnostních rizik a dohledu nad dodržováním těchto opatření na vnitrostátní úrovni. Soulad subjektu s bezpečnostními požadavky stanovenými v nařízeních (ES) č. 300/2008 a (EU) 2018/1139 a v příslušných aktech v přenesené pravomoci a prováděcích aktech přijatých podle uvedených nařízení by mohly příslušné orgány podle této směrnice považovat za soulad s odpovídajícími požadavky stanovenými v této směrnici.

(30) Vzhledem ke vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností subjektů by měl být zajištěn soudržný přístup ke směrnici Evropského parlamentu a Rady (EU) 2022/2557 ([13]) a k této směrnici. Za tímto účelem by subjekty, které jsou určeny jakožto kritické subjekty podle směrnice (EU) 2022/2557, měly být považovány za základní subjekty podle této směrnice. Mimoto by každý členský stát měl zajistit, aby jeho národní strategie kybernetické bezpečnosti stanovila rámec politik pro posílení koordinace uvnitř uvedeného členského státu mezi jeho příslušnými orgány podle této směrnice a podle směrnice (EU) 2022/2557 v souvislosti se sdílením informací o rizicích, kybernetických hrozbách a incidentech a o jiných než kybernetických rizicích, hrozbách a incidentech a při výkonu úkolů dohledu. Příslušné orgány podle této směrnice a orgány příslušné podle směrnice (EU) 2022/2557 by měly spolupracovat a vyměňovat si informace bez zbytečného odkladu, zejména ve vztahu k určení kritických subjektů, rizik, kybernetických hrozeb a incidentů, jakož i ohledně jiných než kybernetických rizik, hrozeb nebo incidentů dotýkajících se kritických subjektů, včetně opatření v oblasti kybernetické bezpečnosti a fyzických opatření přijatých kritickými subjekty a výsledků činností v oblasti dohledu prováděných s ohledem na tyto subjekty.

V zájmu zefektivnění činností v oblasti dohledu mezi příslušnými orgány podle této směrnice a podle směrnice (EU) 2022/2557 a v zájmu minimalizace administrativní zátěže pro dotčené subjekty by uvedené příslušné orgány dále měly usilovat o harmonizaci šablon pro oznamování incidentů a postupů v oblasti dohledu. Příslušné orgány podle směrnice (EU) 2022/2557 by případně měly mít možnost požádat příslušné orgány podle této směrnice, aby vykonávaly své dohledové a vymáhací pravomoci ve vztahu k subjektu, který je určen jakožto kritický subjekt podle směrnice (EU) 2022/2557. Příslušné orgány podle této směrnice a podle směrnice (EU) 2022/2022/2557 by za tímto účelem měly, pokud možno v reálném čase, spolupracovat a vyměňovat si informace.

(31) Subjekty patřící do odvětví digitální infrastruktury jsou v zásadě založeny na sítích a informačních systémech, a proto by povinnosti uložené uvedeným subjektům touto směrnicí měly komplexně řešit fyzickou bezpečnost těchto systémů v rámci jejich opatření k řízení kybernetických bezpečnostních rizik a oznamovacích povinností. Jelikož se na tyto záležitosti vztahuje tato směrnice, povinnosti stanovené v kapitolách III, IV a VI směrnice (EU) 2022/2557 se na tyto subjekty nevztahují.

([11]) Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002 (Úř. věst. L 97, 9.4.2008, s. 72).

([12]) Nařízení Evropského parlamentu a Rady (EU) 2018/1139 ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se mění nařízení (ES) č. 2111/2005, (ES) č. 1008/2008, (EU) č. 996/2010, (EU) č. 376/2014 a směrnice Evropského parlamentu a Rady 2014/30/EU a 2014/53/EU a kterým se zrušuje nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 (Úř. věst. L 212, 22.8.2018, s. 1).

([13]) Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů, kterou se ruší směrnice Rady 2008/114/ES (viz strana 164 v tomto čísle Úředního věstníku).

(32) Podpora a ochrana spolehlivého, odolného a bezpečného systému jmen domén jsou klíčovými faktory 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 registry domén nejvyšší úrovně a provozovatele systému překladu jmen domén (dále jen „provozovatel DNS“) považované za subjekty poskytující veřejně dostupné rekurzívní služby pro překlad jmen domén pro koncové uživatele internetu nebo autoritativní služby pro překlad jmen domén pro použití třetími stranami. Tato směrnice by se neměla vztahovat na kořenové jmenné servery.

(33) Služby cloud computingu by měly zahrnovat digitální služby, které umožňují správu na vyžádání a široký dálkový přístup k rozšiřitelnému a přizpůsobitelnému úložišti distribuovaných výpočetních zdrojů, které je možno sdílet, včetně případů, kdy tyto zdroje mají několik různých umístění. Výpočetní zdroje zahrnují zdroje, jako jsou sítě, servery nebo jiná infrastruktura, operační systémy, software, úložiště, aplikace a služby. Modely služeb cloud computingu zahrnují mimo jiné infrastrukturu jako službu (IaaS), platformu jako službu (PaaS), software jako službu (SaaS) a síť jako službu (NaaA). Modely zavádění cloud computingu by měly zahrnovat soukromý, komunitní, veřejný a hybridní cloud. Služby a modely zavádění cloud computingu 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 výpočetní 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 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.

(34) Vzhledem ke vzniku inovativních technologií a nových obchodních modelů se předpokládá, že v reakci na vyvíjející se potřeby zákazníků se na vnitřním trhu objeví nové služby cloud computingu a modely zavádění. 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“).

(35) 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 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 přenos dat spolu se všemi zařízeními a infrastrukturami pro rozvod energie a kontrolu životního prostředí. Pojem „služba datových center“ by se neměl vztahovat na interní, firemní datová centra vlastněná a provozovaná pro vlastní potřebu dotčeného subjektu.

(36) Výzkumné činnosti hrají klíčovou úlohu při vývoji nových produktů a procesů. Mnohé z těchto činností provádějí subjekty, které výsledky svého výzkumu sdílejí, šíří nebo využívají pro komerční účely. Tyto subjekty proto mohou být důležitými hráči v hodnotových řetězcích, což činí bezpečnost jejich sítí a informačních systémů nedílnou součástí celkové kybernetické bezpečnosti vnitřního trhu. Výzkumné organizace by měly být chápány tak, že zahrnují subjekty, které se v podstatné části svých činností zaměřují na provádění aplikovaného výzkumu nebo experimentálního vývoje ve smyslu manuálu Frascati z roku 2015 vypracovaného Organizací pro hospodářskou

spolupráci a rozvoj: pokyny pro shromažďování a vykazování údajů o výzkumu a experimentálním vývoji za účelem využití jejich výsledků pro komerční účely, jako jsou výroba nebo vývoj produktu nebo procesu, poskytování služby, nebo jejich uvádění na trh.

(37) Rostoucí vzájemné závislosti jsou výsledkem stále více přeshraniční a vzájemně propojené sítě poskytování služeb pomocí klíčových infrastruktur v celé Unii v odvětvích, jako jsou energetika, doprava, digitální infrastruktura, pitná voda, odpadní voda, 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 jejího vesmírného programu. Tyto vzájemné závislosti znamenají, že jakékoli narušení, 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. Vystupňované kybernetické útoky během pandemie COVID-19 prokázaly zranitelnost stále více vzájemně závislých společností vůči rizikům s nízkou pravděpodobností.

(38) 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 nebo zřídit jeden nebo více příslušných orgánů odpovědných za kybernetickou bezpečnost a úkoly dohledu podle této směrnice.

(39) Pro usnadnění přeshraniční spolupráce a komunikace mezi orgány a za účelem účinného provedení této směrnice je nezbytné, aby každý členský stát určil jednotné kontaktní místo odpovědné za koordinaci záležitostí souvisejících s bezpečností sítí a informačních systémů a přeshraniční spoluprací na úrovni Unie.

(40) Jednotná kontaktní místa by měla zajistit účinnou přeshraniční spolupráci s příslušnými orgány jiných členských států a případně s Komisí a agenturou ENISA. Jednotná kontaktní místa by proto měla být pověřena postoupením oznámení o významných incidentech s přeshraničním dopadem jednotným kontaktním místům jiných dotčených členských států na žádost týmu CSIRT nebo příslušného orgánu. Na vnitrostátní úrovni by jednotná kontaktní místa měla zajišťovat hladkou meziodvětvovou spolupráci s ostatními příslušnými orgány. Jednotným kontaktním místům by mohly být také zasílány příslušné informace o incidentech týkajících se finančních subjektů od příslušných orgánů podle nařízení (EU) 2022/2554, které by tato místa měla být schopna případně zasílat týmům CSIRT nebo příslušným orgánům podle této směrnice.

(41) Členské státy by měly být náležitě vybaveny jak po technické, tak po organizační stránce, aby mohly incidentům a rizikům předcházet, odhalovat je, reagovat na ně, a zmírňovat jejich dopad. Členské státy by proto měly zřídit nebo určit jeden nebo více týmů CSIRT ve smyslu této směrnice a zajistit, aby měly odpovídající zdroje a technické kapacity. Týmy CSIRT by měly splňovat požadavky stanovené v této směrnici tak, aby zaručily efektivní a kompatibilní schopnosti řešit incidenty a rizika a zajistily účinnou spolupráci na úrovni Unie. Členské státy by měly mít možnost určit jako týmy CSIRT stávající týmy pro reakci na počítačové hrozby (dále jen „CERT“). V zájmu posílení důvěry mezi subjekty a týmy CSIRT v případech, kdy je tým CSIRT součástí příslušného orgánu, by členské státy měly mít možnost 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.

(42) Týmy CSIRT jsou pověřeny řešením incidentů. To zahrnuje zpracování velkého objemu údajů, které jsou někdy citlivé. Členské státy by měly zajistit, že týmy CSIRT budou mít infrastrukturu pro sdílení a zpracování informací, jakož i dobře vybavené pracovníky, což zajistí důvěrnost a důvěryhodnost jejich operací. Týmy CSIRT by v tomto ohledu rovněž mohly přijmout kodexy chování.

(43) Pokud jde o osobní údaje, týmům CSIRT by mělo být umožněno, aby v souladu s nařízením (EU) 2016/679 na žádost základního nebo důležitého subjektu aktivně skenovaly sítě a informační systémy, které tento subjekt používá k poskytování svých služeb. Členské státy by se měly v příslušných případech zaměřit na to, aby všem odvětvovým týmům CSIRT zajistily stejné technické podmínky. Členské státy by měly mít možnost si při vytváření svých týmů CSIRT vyžádat pomoc agentury ENISA.

(44) Týmy CSIRT by měly být na žádost základního nebo důležitého subjektu schopny sledovat veškerá jeho aktiva orientovaná na internet, a to jak na místě, tak mimo něj, aby určily, pochopily a řídily celková organizační rizika tohoto subjektu, pokud jde o nově zjištěné ohrožení dodavatelského řetězce nebo kritické zranitelnosti. Subjekt by měl být vyzván, aby tým CSIRT informoval o tom, zda provozuje rozhraní pro privilegovanou správu, neboť by to mohlo ovlivnit rychlost provádění zmírňujících opatření.

(45) 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 sítí pro mezinárodní spolupráci. Týmy CSIRT a příslušné orgány by proto pro účely plnění svých úkolů měly mít možnost vyměňovat si informace, včetně osobních údajů, s vnitrostátními týmy CSIRT nebo příslušnými orgány třetích zemí, pokud jsou splněny podmínky pro předávání osobních údajů do třetích zemí podle práva Unie v oblasti ochrany údajů, mimo jiné podmínky stanovené v článku 49 nařízení (EU) 2016/679.

(46) Je zásadní, aby byly zajištěny odpovídající zdroje pro dosažení cílů této směrnice a k tomu, aby mohly příslušné orgány a týmy CSIRT plnit úkoly, jež jsou v ní stanoveny. Členské státy mohou na vnitrostátní úrovni zavést mechanismus financování k pokrytí nezbytných výdajů pro plnění úkolů veřejných subjektů odpovědných za kybernetickou bezpečnost v daném členském státě podle této směrnice. Tento mechanismus by měl být v souladu s právem Unie, měl by být přiměřený a nediskriminační a měl by zohledňovat různé přístupy k poskytování bezpečných služeb.

(47) Síť CSIRT by měla i nadále přispívat k posilování důvěry a k podpoře rychlé a účinné operativní spolupráce mezi členskými státy. Za účelem posílení operativní spolupráce na úrovni Unie by síť CSIRT měla zvážit přizvání institucí a agentur Unie zapojených do politiky kybernetické bezpečnosti, jako je Europol, k účasti na své činnosti.

(48) Za účelem dosažení a udržení vysoké úrovně kybernetické bezpečnosti by národní strategie kybernetické bezpečnosti požadované touto směrnicí měly sestávat ze soudržných rámců se strategickými cíli a prioritami v oblasti kybernetické bezpečnosti a správy za účelem jejich dosažení. Tyto strategie se mohou skládat z jednoho nebo více legislativních či nelegislativních nástrojů.

(49) Politiky v oblasti kybernetické hygieny poskytují základy pro ochranu infrastruktury sítí a informačních systémů, hardwaru, softwaru a bezpečnosti aplikací on-line a údajů o podnicích nebo o koncových uživatelích, na něž se subjekty spoléhají. Politiky v oblasti kybernetické hygieny zahrnující společný základní soubor postupů, včetně aktualizace softwaru a hardwaru, změny hesel, řízení nových instalací, omezení přístupových účtů na úrovni administrátorů a zálohování údajů, zprostředkovávají proaktivní rámec připravenosti a celkové bezpečnosti a ochrany v případě incidentů nebo kybernetických hrozeb. Agentura ENISA by měla sledovat a analyzovat politiky členských států v oblasti kybernetické hygieny.

(50) Povědomí o kybernetické bezpečnosti a kybernetická hygiena mají zásadní význam pro zvýšení úrovně kybernetické bezpečnosti v Unii, zejména s ohledem na rostoucí počet připojených zařízení, která jsou stále častěji při kybernetických útocích využívána. Je třeba vyvinout úsilí o zvýšení celkového povědomí o rizicích spojených s těmito zařízeními, zatímco posouzení provedená na úrovni Unie by navíc mohla pomoci zajistit společné chápání těchto rizik v rámci vnitřního trhu.

(51) Členské státy by měly podporovat využívání jakékoli inovativní technologie, včetně umělé inteligence, jež by mohla zkvalitnit odhalování a prevenci kybernetických útoků a umožnit účinnější přesměrování zdrojů na řešení kybernetických útoků. Členské státy by proto měly ve svých národních strategiích kybernetické bezpečnosti podporovat činnosti v oblasti výzkumu a vývoje, jejímž cílem je usnadnit používání těchto technologií, zejména těch, které se týkají automatizovaných nebo poloautomatizovaných nástrojů v oblasti kybernetické bezpečnosti, a případně sdílení údajů potřebných pro zaškolení uživatelů těchto technologií a pro jejich zdokonalování. Používání jakékoli inovativní technologie, včetně umělé inteligence, by mělo být v souladu s právem Unie v oblasti ochrany údajů, včetně zásad ochrany údajů, minimalizace údajů, spravedlnosti a transparentnosti a bezpečnosti údajů, a to i pokud jde o nejmodernější metody šifrování. Požadavky na záměrnou a standardní ochranu údajů, jak jsou stanoveny v nařízení (EU) 2016/679, je třeba využít v plné míře.

(52) Nástroje a aplikace kybernetické bezpečnosti s otevřeným zdrojovým kódem mohou přispívat k vyšší míře otevřenosti a mohou mít pozitivní dopad na účinnost průmyslové inovace. Otevřené normy usnadňují interoperabilitu mezi bezpečnostními nástroji a přispívají k bezpečnosti odvětvových zúčastněných stran. Nástroje a aplikace kybernetické bezpečnosti s otevřeným zdrojovým kódem mohou podpořit širší komunitu vývojářů, a umožnit tak diverzifikaci dodavatelů. Otevřený zdrojový kód může vést k větší transparentnosti při ověřování nástrojů souvisejících s kybernetickou bezpečností a k postupu odhalování zranitelností řízeném komunitou. Členské státy by proto měly mít možnost podporovat používání softwaru s otevřeným zdrojovým kódem a otevřených standardů tím, že budou provádět politiky spojené s využíváním otevřených dat a otevřených zdrojů v rámci koncepce „bezpečnost prostřednictvím transparentnosti“. Politiky, které podporují zavádění a udržitelné využívání nástrojů kybernetické bezpečnosti s otevřeným zdrojovým kódem, mají zvláštní význam pro malé a střední podniky, které se potýkají se značnými realizačními náklady, jež by bylo možné minimalizovat snížením potřeby specifických aplikací nebo nástrojů.

(53) Veřejné služby jsou stále více propojeny s digitálními sítěmi ve městech kvůli zvyšování kvality městských dopravních sítí, modernizaci zásobování vodou a zařízení na likvidaci odpadu a zvyšování účinnosti osvětlení a vytápění budov. Tyto digitalizované veřejné služby mohou být snadným terčem kybernetických útoků a bude-li takový útok úspěšný, hrozí, že občané budou v důsledku propojenosti těchto služeb poškozeni ve velkém měřítku. Členské státy by měly v rámci své národní strategie kybernetické bezpečnosti vypracovat politiku, která se bude zabývat rozvojem těchto propojených nebo inteligentních měst a možnými dopady na společnost.

(54) V posledních letech čelila Unie exponenciálnímu nárůstu ransomwarových útoků, při nichž malware zašifruje údaje a systémy a za odblokování požaduje platbu výkupného. Rostoucí četnost a závažnost ransomwarových útoků může být dána několika faktory, jako jsou například různé vzorce útoků, nezákonné obchodní modely založené na „ransomware jako službě“ a kryptoměnách, požadavky na výkupné či nárůst útoků v dodavatelském řetězci. Členské státy by měly v rámci svých národních strategií kybernetické bezpečnosti vypracovat politiku, která bude nárůst ransomwarových útoků řešit.

(55) Partnerství veřejného a soukromého sektoru v oblasti kybernetické bezpečnosti mohou poskytnout vhodný rámec pro výměnu znalostí, sdílení osvědčených postupů a nastolení společné úrovně porozumění mezi zúčastněnými stranami. Členské státy by měly podporovat politiky na podporu vytváření partnerství veřejného a soukromého sektoru specificky zaměřených na kybernetickou bezpečnost. Tyto politiky by měly mimo jiné jasně specifikovat svou působnost a zúčastněné strany, model řízení, dostupné možnosti financování a interakci mezi zúčastněnými stranami ve vztahu k partnerství veřejného a soukromého sektoru. Partnerství veřejného a soukromého sektoru mohou využít odborné znalosti subjektů ze soukromého sektoru na pomoc příslušným orgánům při vývoji nejmodernějších služeb a procesů, včetně výměny informací, včasného varování, nácviků reakce při kybernetických hrozbách a incidentech, krizového řízení a plánování odolnosti.

(56) Členské státy by se měly ve svých národních strategiích kybernetické bezpečnosti zabývat tím, jaké specifické potřeby mají v oblasti kybernetické bezpečnosti malé a střední podniky. Malé a střední podniky mají v celé Unii významný podíl na průmyslovém a obchodním trhu a často mají problém přizpůsobit se novým obchodním postupům v propojenějším světě a digitálnímu prostředí, kdy zaměstnanci pracují z domova a obchodní činnost stále častěji probíhá on-line. Některé malé a střední podniky čelí v oblasti kybernetické bezpečnosti specifickým výzvám, v souvislosti s nimiž by měly obdržet pokyny a pomoc: nemají například o kybernetické bezpečnosti dostatečné povědomí, jejich systémy IT nejsou dostatečně zabezpečeny pro vzdálený přístup, mají v souvislosti s kybernetickou bezpečností vysoké náklady a jsou ve větším ohrožení, například vůči ransomwarovému útoku. Malé a střední podniky se čím dál častěji stávají terčem útoků skrze dodavatelský řetězec, a to kvůli tomu, že jejich opatření k řízení kybernetických bezpečnostních rizik a zvládání útoků jsou méně důkladná a že na bezpečnostní záležitosti mají k dispozici méně zdrojů. Tyto útoky skrze dodavatelský řetězec mají dopad nejen na malé a střední podniky a jejich izolovanou činnost, ale mohou mít také kaskádový účinek v rámci rozsáhlejších útoků na subjekty,

kterým poskytují své služby. Členské státy by měly prostřednictvím svých národních strategií kybernetické bezpečnosti pomoci malým a středním podnikům řešit výzvy, jimž ve svých dodavatelských řetězcích čelí. Členské státy by měly mít kontaktní místo pro malé a střední podniky na vnitrostátní nebo regionální úrovni, které bude poskytovat malým a středním podnikům pokyny a pomoc, nebo je za účelem poskytnutí pokynů a pomoci v otázkách kybernetické bezpečnosti nasměruje k patřičným subjektům. Členské státy se rovněž vybízí k tomu, aby mikropodnikům a malým podnikům, které nemají příslušné kapacity, poskytovaly služby, jako je konfigurace internetových stránek a vedení protokolů.

(57) Členské státy by měly v rámci svých národních strategií pro kybernetickou bezpečnost přijmout politiky na podporu aktivní kybernetické ochrany, které budou součástí širší obranné strategie. Aktivní kybernetická ochrana nefunguje reaktivně, ale zajišťuje aktivní prevenci, odhalování, sledování, analýzu a zmírňování případů narušení bezpečnosti sítě v kombinaci s využitím funkcí v síti, která je předmětem útoku, i mimo ni. V rámci této ochrany by mohly členské státy nabízet určitým způsobilým subjektům bezplatné služby nebo nástroje, včetně samoobslužných kontrol, detekčních nástrojů a služeb chránících před zneužitím korporátních značek a identity (takedown service). Pro jednotný postup v úsilí o úspěšnou prevenci, odhalování, řešení a blokování útoků proti sítím a informačním systémům je zásadně důležitá možnost rychle a automaticky sdílet a chápat údaje a analýzy týkající se hrozeb, varování v souvislosti s kybernetickými aktivitami a opatření reakce. Aktivní kybernetická ochrana spočívá na obranné strategii, která vylučuje útočná opatření.

(58) Využití zranitelností v sítích a informačních systémech může způsobit vážná narušení a škody, a rychlé určení a náprava těchto zranitelností je proto důležitým faktorem při snižování rizik. Subjekty, které sítě a informační systémy vyvíjejí nebo spravují, by proto měly stanovit vhodné postupy k řešení zranitelností, jakmile jsou zjištěny. Jelikož zranitelnosti jsou často zjištěny a odhaleny třetími stranami, výrobce nebo poskytovatel produktů IKT nebo služeb IKT by měl rovněž zavést nezbytné postupy pro získávání informací o zranitelnosti od třetích stran. Vodítko pro řešení zranitelnosti a zveřejňování zranitelností v této souvislosti poskytují mezinárodní normy ISO/IEC 30111 a ISO/IEC 29147. Pro účely usnadnění dobrovolného rámce pro zveřejňování informací o zranitelnostech je zvláště důležité posílení koordinace mezi fyzickými a právnickými osobami oznamujícími incidenty a výrobci nebo poskytovateli produktů IKT nebo služeb IKT. Koordinované zveřejňování zranitelností specifikuje strukturovaný proces, jehož prostřednictvím jsou zranitelnosti oznámeny výrobci nebo poskytovateli potenciálně zranitelných produktů IKT nebo služeb IKT takovým způsobem, který mu umožní diagnostikovat a odstranit zranitelnost dříve, než budou podrobné informace o ní sděleny třetím stranám nebo veřejnosti. Koordinované zveřejňování zranitelností by také mělo zahrnovat koordinaci mezi fyzickou a právnickou osobou oznamující incidenty a výrobcem nebo poskytovatelem potenciálně zranitelných produktů IKT nebo služeb IKT, pokud jde o načasování odstranění zranitelností a jejich zveřejnění.

(59) Komise, agentura ENISA a členské státy by měly i nadále podporovat sbližování s mezinárodními normami a stávajícími odvětvovými osvědčenými postupy v oblasti řízení kybernetických bezpečnostních rizik, například v oblastech posuzování bezpečnosti dodavatelského řetězce, sdílení informací a zveřejňování zranitelností.

(60) Členské státy by měly ve spolupráci s agenturou ENISA přijmout opatření k usnadnění koordinovaného zveřejňování zranitelností zavedením příslušné vnitrostátní politiky. V rámci své vnitrostátní politiky by členské státy měly usilovat o to, aby se v souladu s vnitrostátním právem v co největší míře zabývaly výzvami, jimž čelí objevovatelé zranitelností, kteří se touto problematikou zabývají, a to i pokud jde o jejich možné vystavení trestní odpovědnosti. Vzhledem k tomu, že fyzické a právnické osoby, které provádějí výzkum týkající se zranitelností, by v některých členských státech mohly být vystaveny trestní a občanskoprávní odpovědnosti, členské státy se vybízejí, aby přijaly pokyny týkající se nemožnosti stíhat osoby provádějících výzkum bezpečnosti informací a vyloučení vzniku občanskoprávní odpovědnosti v souvislosti s jejich činnostmi.

(61) Členské státy by měly určit jeden ze svých týmů CSIRT jakožto koordinátora, který v případě potřeby převezme úlohu důvěryhodného zprostředkovatele mezi oznamujícími fyzickými či právnickými osobami a výrobci nebo poskytovateli produktů IKT či služeb IKT, u nichž je pravděpodobné, že budou zranitelností dotčeny. Mezi úkoly týmu CSIRT, který byl určen jakožto koordinátor, by měla patřit identifikace a kontaktování dotčených subjektů,

pomoc fyzickým nebo právnickým osobám oznamujícím zranitelnost, jednání o lhůtách pro zveřejnění a řešení zranitelností, které mají dopad na více subjektů (vícestranné koordinované zveřejňování zranitelností). Pokud by oznámená zranitelnost mohla mít významný dopad na subjekty ve více než jednom členském státě, měly by týmy CSIRT určené jakožto koordinátoři v rámci sítě CSIRT případně spolupracovat.

(62) Přístup ke správným a včasným informacím o zranitelnostech dotýkajících se produktů IKT a služeb IKT přispívá k zesílenému řízení kybernetických bezpečnostních rizik. Zdroje veřejně přístupných informací o zranitelnostech jsou důležitým nástrojem pro subjekty a uživatele jejich služeb, ale i pro příslušné orgány a týmy CSIRT. Z tohoto důvodu by agentura ENISA měla zavést Evropskou databázi zranitelností, kde subjekty bez ohledu na to, zda se na ně tato směrnice vztahuje, a jejich dodavatelé sítí a informačních systémů a příslušné orgány a týmy CSIRT mohou veřejně známé zranitelnosti na základě dobrovolnosti zveřejňovat a zaznamenávat, aby uživatelům umožnili přijímat vhodná opatření ke zmírnění dopadů. Smyslem této databáze je řešit výzvy spojené s riziky příznačnými pro unijní subjekty. Agentura ENISA by nadto měla zavést vhodný postup pro zveřejňování informací, který poskytne subjektům čas k přijetí opatření zmírňujících jejich zranitelnosti, a uplatňovat nejmodernější opatření k řízení kybernetických bezpečnostních rizik a strojově čitelné datové soubory a odpovídající rozhraní. V zájmu podpory kultury zveřejňování zranitelností by odhalení nemělo způsobovat oznamující fyzické nebo právnické osobě žádnou újmu.

(63) Ačkoli podobné registry nebo databáze zranitelností existují, jsou hostovány a spravovány subjekty, které nejsou usazeny v Unii. Evropská databáze zranitelností spravovaná agenturou ENISA by poskytla lepší transparentnost procesu odhalování předtím, než je zranitelnost zveřejněna, a odolnost v případě narušení nebo přerušení poskytování podobných služeb. S cílem v co největší možné míře zabránit zdvojení úsilí a usilovat o komplementaritu by agentura ENISA měla zkoumat možnost uzavření strukturovaných dohod o spolupráci s podobnými registry nebo databázemi spadajícími do jurisdikce třetích zemí. Agentura ENISA by měla zejména prozkoumat možnost úzké spolupráce s provozovateli systému společných zranitelností a expozic (CVE).

(64) Skupina pro spolupráci by měla podporovat a usnadňovat strategickou spolupráci a výměnu informací, jakož i posilovat důvěru mezi členskými státy. Skupina pro spolupráci by měla každé dva roky přijmout pracovní program. Pracovní program by měl zahrnovat opatření, která má skupina pro spolupráci podniknout ke splnění svých cílů a úkolů. Časový rámec pro přijetí prvního programu podle této směrnice by měl být sladěn s časovým rámcem posledního pracovního programu stanoveného na základě směrnice (EU) 2016/1148, aby se zabránilo možnému přerušení práce skupiny pro spolupráci.

(65) 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, zejména pokud jde o usnadnění sladění při provádění této směrnice mezi členskými státy, která je třeba zohlednit prostřednictvím lepšího provádění stávajících pravidel. V zájmu podpory slaďování řešení v oblasti kybernetické bezpečnosti uplatňovaných v jednotlivých odvětvích v celé Unii by skupina pro spolupráci mohla rovněž mapovat vnitrostátní řešení. To je obzvláště důležité pro odvětví, která jsou ze své povahy mezinárodní nebo přeshraniční.

(66) 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. Mohla by organizovat pravidelná společná setkání s relevantními soukromými zúčastněnými stranami z celé Unie za účelem projednání činností prováděných skupinou pro spolupráci a shromažďování údajů a vstupů týkajících se vznikajících politických výzev. Kromě toho by skupina pro spolupráci měla pravidelně provádět hodnocení aktuálního stavu kybernetických hrozeb nebo

incidentů, například v souvislosti s ransomware. S cílem posílit spolupráci na úrovni Unie by skupina pro spolupráci měla zvážit, že k účasti na své činnosti přizve příslušné orgány, instituce a jiné subjekty Unie zapojené do politiky v oblasti kybernetické bezpečnosti, jako jsou Evropský parlament, Europol, Evropský sbor pro ochranu osobních údajů, Agentura Evropské unie pro bezpečnost letectví, zřízená nařízením (EU) 2018/1139, a Agentura Evropské unie pro Kosmický program, zřízená nařízením Evropského parlamentu a Rady (EU) 2021/696 ([14]).

(67) Za účelem zlepšení spolupráce a posílení důvěry mezi členskými státy by měly příslušné orgány a týmy CSIRT mít možnost účastnit se výměnných programů pro úředníky z jiných členských států, a to ve zvláštním rámci a případně pod podmínkou požadavku bezpečnostní prověrky úředníků účastnících se těchto výměnných programů, s cílem zlepšit spolupráci a posílit důvěru mezi členskými státy. Příslušné orgány by měly přijmout nezbytná opatření, jež umožní úředníkům z jiných členských států účinně se zapojit do činností hostitelského příslušného orgánu nebo hostitelského týmu CSIRT.

(68) Členské státy by měly přispět k vytvoření rámce EU pro reakci na kybernetické bezpečnostní krize uvedeného v doporučení Komise (EU) 2017/1584 ([15]) prostřednictvím stávajících sítí pro spolupráci, zejména Evropské sítě styčných organizací pro řešení kybernetických krizí (dále jen „síť EU-CyCLONe“), sítě CSIRT a skupiny pro spolupráci. Sítě EU-CyCLONe a CSIRT by měly spolupracovat na základě procesních opatření, jež vymezí podrobnosti této spolupráce, a zamezit zdvojování činnosti. Jednací řád sítě EU-CyCLONe by měl dále vymezit podmínky, za nichž by měla uvedená síť fungovat, včetně úloh této sítě, 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 opatření pro integrovanou politickou reakci na krize podle prováděcího rozhodnutí Rady (EU) 2018/1993 ([16]) (opatření IPRK). Komise by za tímto účelem měla využít proces meziodvětvové koordinace na vysoké úrovni v krizových situacích ARGUS. Pokud má krize významný externí rozměr nebo se týká společné bezpečnostní a obranné politiky, měl by být aktivován mechanismus Evropské služby pro vnější činnost pro reakce na krize.

(69) V souladu s přílohou doporučení (EU) 2017/1584 by rozsáhlý kybernetický bezpečnostní incident měl označovat incident, který způsobuje narušení přesahující schopnost členského státu na něj reagovat nebo incident, který má významný dopad na alespoň dva členské státy. V závislosti na jejich příčině a dopadu mohou rozsáhlé kybernetické bezpečnostní incidenty eskalovat a přejít ve skutečné krize, jež neumožní řádné fungování vnitřního trhu nebo budou představovat vážná rizika pro veřejnou bezpečnost a ochranu subjektů nebo občanů v několika členských státech nebo v Unii jako celku. Vzhledem k širokému dopadu a ve většině případů i přeshraniční povaze takových incidentů by členské státy a příslušné orgány, instituce a jiné subjekty Unie měly na technické, operativní a politické úrovni spolupracovat a odpovídajícím způsobem koordinovat reakci v celé Unii.

(70) Rozsáhlé kybernetické bezpečnostní incidenty a krize na úrovni Unie vyžadují koordinovanou činnost k zajištění rychlé a účinné reakce z důvodu vysokého stupně vzájemné závislosti mezi jednotlivými odvětvími a členskými státy. Dostupnost sítí a informačních systémů odolných vůči kybernetickým útokům a dostupnost, důvěrnost a integrita dat mají zásadní význam pro bezpečnost Unie a pro ochranu jejích občanů, podniků a institucí před incidenty a kybernetickými hrozbami, jakož i pro posílení důvěry jednotlivců a organizací ve schopnost Unie prosazovat a chránit globální, otevřený, svobodný, stabilní a bezpečný kyberprostor založený na lidských právech, základních svobodách, demokracii a právním státu.

([14]) Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zavádí Kosmický program Unie a zřizuje Agentura Evropské unie pro Kosmický program a zrušují nařízení (EU) č. 912/2010, (EU) č. 1285/2013 a (EU) č. 377/2014 a rozhodnutí č. 541/2014/EU (Úř. věst. L 170, 12.5.2021, s. 69).

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

([16]) Prováděcí rozhodnutí Rady (EU) 2018/1993 ze dne 11. prosince 2018 o opatřeních pro integrovanou politickou reakci EU na krize (Úř. věst. L 320, 17.12.2018, s. 28).

(71) Síť EU-CyCLONe by měla působit jako prostředník mezi technickou a politickou úrovní při rozsáhlých kybernetických bezpečnostních incidentech a krizích a měla by posilovat spolupráci na operační úrovni a podporovat rozhodování na politické úrovni. Ve spolupráci s Komisí a s ohledem na pravomoc Komise v oblasti řešení krizí by měla síť EU-CyCLONe vycházet ze zjištění sítě CSIRT a využívat své vlastní schopnosti k vypracování analýzy dopadů rozsáhlých kybernetických bezpečnostních incidentů a krizí.

(72) Kybernetické útoky jsou přeshraniční povahy a významný incident může narušit a poškodit kritickou informační infrastrukturu, na níž závisí hladké fungování vnitřního trhu. Doporučení (EU) 2017/1584 se zabývá úlohou všech příslušných aktérů. Kromě toho je Komise v rámci mechanismu civilní ochrany Unie zřízeného rozhodnutím Evropského parlamentu a Rady č. 1313/2013/EU [17] odpovědná za obecná opatření v oblasti připravenosti, včetně řízení Střediska pro koordinaci odezvy na mimořádné události a společného komunikačního a informačního systému pro mimořádné události, udržování a dalšího rozvoje situačního povědomí a schopnosti analýzy a vytvoření a řízení schopnosti mobilizovat a vyslat odborné týmy v případě žádosti členského státu nebo třetí země o pomoc. Komise je rovněž odpovědná za poskytování analytických zpráv pro opatření IPRK podle prováděcího rozhodnutí (EU) 2018/1993, a to i pokud jde o povědomí o situaci a připravenost v oblasti kybernetické bezpečnosti, jakož i za povědomí o situaci a reakci na krize v oblasti zemědělství, nepříznivých povětrnostních podmínek, mapování a prognóz konfliktů, systémů včasného varování v případě přírodních katastrof, mimořádných situací v oblasti zdraví, dozoru nad nakažlivými chorobami, zdraví rostlin, chemických incidentů, bezpečnosti potravin a krmiv, zdraví zvířat, migrace, cel, jaderných a radiologických mimořádných situací a v energetické oblasti.

(73) Unie může ve vhodných případech v souladu s článkem 218 Smlouvy o fungování EU uzavírat mezinárodní dohody s třetími zeměmi nebo mezinárodními organizacemi, které umožní a upraví jejich účast na některých činnostech skupiny pro spolupráci a sítě CSIRT a sítě EU-CyCLONe. Takové dohody by měly zajistit zájmy Unie a odpovídající ochranu údajů. Tím by nemělo být dotčeno právo členských států spolupracovat s třetími zeměmi na řízení zranitelností a řízení kybernetických bezpečnostních rizik, což usnadňuje podávání zpráv a obecné sdílení informací v souladu s právem Unie.

(74) V zájmu usnadnění účinného provádění této směrnice, s ohledem mimo jiné na řešení zranitelností, opatření k řízení kybernetických bezpečnostních rizik, oznamovací povinnosti a ujednání o sdílení informací o kybernetické bezpečnosti, mohou členské státy spolupracovat se třetími zeměmi a provádět činnosti, které jsou pro tento účel považovány za vhodné, včetně výměny informací o kybernetických hrozbách, incidentech, zranitelnostech, nástrojích a metodách, taktice, technikách a postupech, připravenosti a cvičeních pro řešení kybernetických bezpečnostních krizí, školení, budování důvěry a strukturovaných ujednáních o sdílení informací.

(75) Měla by být zavedena vzájemná hodnocení, díky nimž by bylo možné poučit se ze sdílených zkušeností, posílit vzájemnou důvěru a dosáhnout vysoké společné úrovně kybernetické bezpečnosti. Vzájemná hodnocení mohou přinést cenné poznatky a doporučení, posílit celkové schopnosti v oblasti kybernetické bezpečnosti, vytvořit další funkční způsob, jak sdílet osvědčené postupy mezi členskými státy, a přispět ke zvýšení úrovně vyspělosti členských států v oblasti kybernetické bezpečnosti. Kromě toho by vzájemná hodnocení měla zohledňovat výsledky obdobných mechanismů, například systému vzájemného hodnocení sítě CSIRT, a měla by vytvářet přidanou hodnotu a zamezit zdvojování činností. Zavedením vzájemných hodnocení by nemělo být dotčeno unijní ani vnitrostátní právo o ochraně důvěrných nebo utajovaných informací.

(76) Skupina pro spolupráci by měla pro členské státy vypracovat metodiku sebehodnocení, jejímž cílem bude pokrýt takové faktory, jako jsou úroveň provádění opatření k řízení kybernetických bezpečnostních rizik a oznamovacích povinností, úroveň schopností a účinnost plnění úkolů příslušných orgánů, provozní schopnosti týmů CSIRT, úroveň poskytování vzájemné pomoci, úroveň provádění ujednání o sdílení informací o kybernetické bezpečnosti nebo zvláštní přeshraniční či meziodvětvové otázky. Členské státy by měly být nabádány k tomu, aby sebehodnocení prováděly pravidelně a výsledky svého sebehodnocení předkládaly a projednávaly ve skupině pro spolupráci.

[17] Rozhodnutí Evropského parlamentu a Rady č. 1313/2013/EU ze dne 17. prosince 2013 o mechanismu civilní ochrany Unie (Úř. věst. L 347, 20.12.2013, s. 924).

(77) Povinnost zajistit bezpečnost sítě a informačního systému mají do značné míry základní a důležité subjekty. Měla by být prosazována a rozvíjena kultura řízení rizik zahrnující posuzování rizik a provádění opatření k řízení kybernetických bezpečnostních rizik úměrných hrozícím rizikům.

(78) Opatření k řízení kybernetických bezpečnostních rizik by měla zohledňovat míru závislosti základního nebo důležitého subjektu na sítích a informačních systémech a zahrnovat opatření pro určení veškerých rizik incidentů, předcházení incidentům, jejich odhalování, reakce na ně, zotavení se z nich a zmírňování jejich dopadu. Bezpečnost sítí a informačních systémů by měla zahrnovat bezpečnost uchovávaných, předávaných a zpracovávaných údajů. Opatření k řízení kybernetických bezpečnostních rizik by měla zajišťovat systémovou analýzu zohledňující lidský faktor s cílem získat úplný obraz o bezpečnosti sítě a informačního systému.

(79) Vzhledem k tomu, že hrozby pro bezpečnost sítí a informačních systémů mohou být různého původu, opatření k řízení kybernetických bezpečnostních rizik by měla být založena na přístupu zohledňujícím všechna rizika, jehož cílem je chránit sítě a informační systémy a jejich fyzické prostředí před událostmi, jako jsou krádež, požár, povodeň, výpadky telekomunikací nebo elektrického proudu, nebo před neoprávněným fyzickým přístupem k informacím a zařízením pro zpracování informací základního nebo důležitého subjektu a jejich poškozením a zásahům do nich, jež by mohly narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné. Opatření k řízení kybernetických bezpečnostních rizik by proto měla rovněž řešit fyzickou a environmentální bezpečnost sítí a informačních systémů tím, že budou zahrnovat opatření na ochranu těchto systémů před selháním systému, lidskou chybou, zlovolnými činy nebo přírodními jevy v souladu s evropskými a mezinárodními normami, jako jsou normy obsažené v řadě ISO/IEC 27000. V tomto ohledu by se základní a důležité subjekty měly v rámci svých opatření k řízení kybernetických bezpečnostních rizik zabývat rovněž bezpečností lidských zdrojů a zavést vhodné politiky kontroly přístupu. Tato opatření by měla být v souladu se směrnicí (EU) 2022/2557.

(80) Za účelem prokázání souladu s opatřeními k řízení kybernetických bezpečnostních rizik a v případě neexistence vhodných evropských systémů certifikace kybernetické bezpečnosti přijatých v souladu s nařízením Evropského parlamentu a Rady (EU) 2019/881 ([18]) by členské státy měly za konzultací se skupinou pro spolupráci a Evropskou skupinou pro certifikaci kybernetické bezpečnosti podporovat používání příslušných evropských a mezinárodních norem ze strany základních a důležitých subjektů nebo požadovat, aby subjekty používaly certifikované produkty IKT, služby IKT a procesy IKT.

(81) Aby se zabránilo nepřiměřené finanční a administrativní zátěži pro základní a důležité subjekty, měla by být opatření k řízení kybernetických bezpečnostních rizik úměrná rizikům, kterým jsou dotčená síť a informační systém vystaveny, s přihlédnutím k aktuálnímu stavu těchto opatření a případně k příslušným evropským a mezinárodním normám, jakož i k nákladům na jejich provádění.

(82) Opatření k řízení kybernetických bezpečnostních rizik by měla být úměrná míře vystavení základního nebo důležitého subjektu rizikům a společenskému a ekonomickému dopadu, který by měl incident. Při zavádění opatření k řízení kybernetických bezpečnostních rizik přizpůsobených pro základní a důležité subjekty by měla být náležitě zohledněna rozdílná expozice základních a důležitých subjektů rizikům, jako je kritičnost subjektu, rizika, včetně společenských rizik, jimž je vystaven, velikost subjektu a pravděpodobnost výskytu incidentů a jejich závažnost, včetně jejich společenského a ekonomického dopadu.

([18]) 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).

(83) Základní a důležité subjekty by měly zajistit bezpečnost sítí a informačních systémů, které užívají ve svých činnostech. Jedná se především o soukromé síťové a informační systémy, jež jsou buď řízeny interními pracovníky IT základních a důležitých subjektů, nebo jejichž bezpečnost zajišťuje externí dodavatel. Opatření k řízení kybernetických bezpečnostních rizik a povinnosti týkající se oznamování podle této směrnice by měly pro příslušné základní a důležité subjekty platit bez ohledu na to, zda správu svých sítí a informačních systémů provádějí tyto subjekty interně, nebo k tomu využívají externího dodavatele.

(84) S ohledem na jejich přeshraniční povahu by provozovatelé DNS, registry domén nejvyšší úrovně, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center, poskytovatelé sítí pro doručování obsahu, poskytovatelé řízených služeb, poskytovatelé řízených bezpečnostních služeb, poskytovatelé on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatelé služeb vytvářejících důvěru měli podléhat vysokému stupni harmonizace na úrovni Unie. Provádění opatření k řízení kybernetických bezpečnostních rizik ve vztahu k těmto subjektům by proto mělo být usnadněno prováděcím aktem.

(85) Řešení rizik vyplývajících z dodavatelského řetězce subjektu nebo jeho vztahů s dodavateli, jako jsou poskytovatelé služeb ukládání a zpracování dat nebo poskytovatelé řízených bezpečnostních služeb a vydavatelé softwaru, je zvlášť důležité vzhledem k počtu incidentů, v jejichž případě se subjekty staly obětí kybernetických útoků a pachatelé byli schopni narušit bezpečnost sítí a informačních systémů daného subjektu tím, že využili zranitelností v produktech a službách třetí strany. Základní a důležité subjekty by proto měly posoudit a zohlednit celkovou kvalitu a odolnost produktů a služeb, opatření v oblasti kybernetické bezpečnosti, která zahrnují, a postupů kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů k zajištění bezpečného vývoje. Základní a důležité subjekty by měly být zejména vybízeny, aby začlenily opatření k řízení kybernetických bezpečnostních rizik do smluvních ujednání se svými přímými dodavateli a poskytovateli služeb. Uvedené subjekty by mohly přihlížet k rizikům, jež mají původ u dodavatelů a poskytovatelů služeb dalších úrovní.

(86) Mezi poskytovateli služeb mají zvlášť důležitou úlohu v pomoci subjektům v jejich úsilí o předcházení incidentům, při jejich odhalování, reakci na ně nebo zotavení se z nich poskytovatelé řízených bezpečnostních služeb v oblastech jako reakce na incidenty, penetrační testování, bezpečnostní audity a konzultační činnost. Poskytovatelé řízených bezpečnostních služeb se však také sami stali terčem kybernetických útoků a vzhledem k jejich úzkému začlenění do provozu subjektů představují zvláštní riziko. Základní a důležité subjekty by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat s větší péčí.

(87) Příslušné orgány mohou v rámci svých úkolů v oblasti dohledu rovněž využívat služeb kybernetické bezpečnosti, jako jsou bezpečnostní audity, penetrační testování nebo reakce na incidenty.

(88) Základní a důležité subjekty by rovněž měly řešit rizika vyplývající z jejich interakcí a vztahů s jinými zúčastněnými stranami v rámci širšího ekosystému, včetně boje proti průmyslové špionáži a ochrany obchodního tajemství. Uvedené 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 základní a důležité 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 k řízení kybernetických bezpečnostních rizik.

(89) Základní a důležité subjekty by měly přijmout širokou škálu základních postupů v oblasti kybernetické hygieny, k nimž patří architektura nulové důvěry, aktualizace softwaru, konfigurace zařízení, segmentace sítě, řízení identity a přístupu nebo povědomí uživatelů, měly by pořádat školení pro své zaměstnance a zvyšovat povědomí o kybernetických hrozbách, phishingu či technikách sociálního inženýrství. Uvedené subjekty by dále měly hodnotit své vlastní schopnosti v oblasti kybernetické bezpečnosti a případně usilovat o integraci technologií zvyšujících kybernetickou bezpečnost, jako jsou umělá inteligence nebo systémy strojového učení, s cílem posílit své schopnosti a bezpečnost sítí a informačních systémů.

(90) Aby bylo možné dále řešit klíčová rizika dodavatelského řetězce a pomoci základním a důležitým subjektům působícím v odvětvích, na něž se vztahuje tato směrnice, náležitě řídit dodavatelský řetězec a rizika související s dodavateli, měla by skupina pro spolupráci ve spolupráci s Komisí a agenturou ENISA a případně po konzultaci s příslušnými zúčastněnými stranami, včetně průmyslu, provádět koordinovaná posouzení bezpečnostních rizik kritických dodavatelských řetězců, která byla provedena pro sítě 5G v souladu s doporučením Komise (EU) 2019/534 ([19]), s cílem určit kritické služby IKT, systémy IKT nebo produkty IKT, relevantní hrozby a zranitelnosti pro jednotlivá odvětví. Uvedená koordinovaná posouzení bezpečnostních rizik by měla určit opatření, plány zmírňování a osvědčené postupy ve vztahu ke kritickým závislostem, potenciálním jediným bodům selhání, hrozbám, zranitelnostem a dalším rizikům spojeným s dodavatelským řetězcem a měla by prozkoumat způsoby, jak základní a důležité subjekty dále podněcovat, aby je šířeji přijímaly. Potenciální netechnické rizikové faktory, jako je nepatřičný vliv třetí země na dodavatele a poskytovatele služeb, zejména v případě alternativních modelů správy, zahrnují skryté zranitelnosti nebo „zadní vrátka“ a možné systémové narušení dodávek, zejména v případě technologické závislosti nebo závislosti na poskytovateli.

(91) Koordinovaná posouzení bezpečnostních rizik kritických dodavatelských řetězců 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 kybernetickou bezpečnost sítí 5G v 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 bezpečnostních rizik, by měla být vzata v úvahu tato kritéria: i) rozsah, v jakém základní a důležité subjekty využívají konkrétní kritické služby IKT, systémy IKT a produkty IKT a jsou na nich závislé; ii) relevantnost konkrétních služeb IKT, systémů IKT nebo produktů IKT pro plnění kritických nebo citlivých funkcí, včetně zpracování osobních údajů; iii) dostupnost alternativních služeb IKT, systémů IKT nebo produktů IKT; iv) odolnost celého dodavatelského řetězce služeb IKT, systémů IKT nebo produktů IKT během jejich životního cyklu vůči narušení a v) u vznikajících služeb IKT, systémů IKT nebo produktů IKT jejich budoucí význam pro činnost subjektů. Zvláštní důraz je třeba dále klást na služby IKT, systémy IKT nebo produkty IKT, které podléhají specifickým požadavkům ze třetích zemí.

(92) S cílem zjednodušit 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 příslušným orgánům podle směrnice Evropského parlamentu a Rady (EU) 2018/1972 ([20]), nebo podle nařízení (EU) č. 910/2014, využívat právní rámec stanovený touto směrnicí, včetně určení týmu CSIRT odpovědného za řešení incidentů a účasti dotčených příslušných orgánů na činnostech skupiny pro spolupráci a sítě CSIRT, by tyto subjekty měly spadat do oblasti působnosti této směrnice. Příslušná ustanovení v nařízení (EU) č. 910/2014 a směrnici (EU) 2018/1972, které na tyto druhy subjektů kladou požadavky týkající se bezpečnosti a oznamování, by proto měla být zrušena. Pravidly týkajícími se oznamovacích povinností stanovenými v této směrnici by nemělo být dotčeno nařízení (EU) 2016/679 ani směrnice 2002/58/ES.

(93) Povinnosti k zajištění kybernetické bezpečnosti stanovené v této směrnici by měly být považovány za doplňkové k požadavkům kladeným na poskytovatele služeb vytvářejících důvěru podle nařízení (EU) č. 910/2014. Od poskytovatelů služeb vytvářejících důvěru by mělo být vyžadováno, aby přijali veškerá vhodná a přiměřená opatření k řízení rizik spojených s jejich službami, a to i ve vztahu k zákazníkům a spoléhajícím se třetím stranám, a aby oznamovali incidenty podle této směrnice. Tyto povinnosti k zajištění kybernetické bezpečnosti a povinnosti týkající se oznamování by se rovněž měly týkat fyzické ochrany poskytovaných služeb. Nadále platí požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru stanovené v článku 24 nařízení (EU) č. 910/2014.

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

([20]) 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).

(94) Členské státy mohou orgánům dohledu podle nařízení (EU) č. 910/2014 svěřit úlohu příslušných orgánů pro služby vytvářející důvěru s cílem zajistit pokračování stávajících postupů a využít znalostí a zkušeností získaných při uplatňování uvedeného nařízení. V takových případech by měly příslušné orgány podle této směrnice úzce a včas s těmito orgány dohledu spolupracovat formou výměny příslušných informací s cílem zajistit účinný dohled nad poskytovateli služeb vytvářejících důvěru a jejich dodržováním požadavků stanovených v této směrnici a nařízení (EU) č. 910/2014. Síť CSIRT nebo příslušný orgán podle této směrnice by měly v příslušných případech neprodleně informovat orgán dohledu podle nařízení (EU) č. 910/2014 o všech oznámených významných kybernetických hrozbách nebo incidentech s dopadem na služby vytvářející důvěru, jakož i o jakémkoli porušení této směrnice poskytovatelem služeb vytvářejících důvěru. Pro účely oznamování mohou členské státy případně využít jednotného kontaktního místa zřízeného za účelem dosažení společného a automatického oznamování incidentů jak orgánu dohledu podle nařízení (EU) č. 910/2014, tak týmu CSIRT nebo příslušnému orgánu podle této směrnice.

(95) Pokud je to vhodné a s cílem zabránit zbytečným narušením, by při provádění této směrnice měly být zohledněny stávající vnitrostátní pokyny přijaté pro provedení pravidel týkajících se bezpečnostních opatření stanovených v článcích 40 a 41 směrnice (EU) 2018/1972, a to na základě znalostí a dovedností již získaných podle směrnice (EU) 2018/1972, pokud jde o bezpečnostní opatření a oznamování incidentů. Agentura ENISA může rovněž pro poskytovatele veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací vypracovat pokyny týkající se bezpečnostních požadavků a povinností týkajících se oznamování s cílem usnadnit harmonizaci a přechod a minimalizovat narušení. Členské státy mohou úlohu příslušných orgánů pro elektronické komunikace svěřit vnitrostátním regulačním orgánům podle směrnice (EU) 2018/1972 s cílem zajistit pokračování stávajících postupů a využít znalostí a zkušeností získaných v důsledku provádění uvedené směrnice.

(96) Vzhledem k rostoucímu významu interpersonálních komunikačních služeb nezávislých na číslech ve smyslu směrnice (EU) 2018/1972 je nutné zajistit, aby i tyto služby podléhaly odpovídajícím bezpečnostním požadavkům v souladu s jejich zvláštní povahou a ekonomickým významem. Vzhledem k tomu, že se oblast útoku stále rozrůstá, interpersonální komunikační služby nezávislé na číslech, jako jsou služby zasílání zpráv, se stávají rozšířenými vektory útoků. Útočníci využívají platformy ke komunikaci, při níž se snaží nalákat oběti, aby otevřely napadené internetové stránky, tím se zvyšuje pravděpodobnost incidentů spojených s využíváním osobních údajů, což má pak důsledky pro bezpečnost sítí a informačních systémů. Provozovatelé interpersonálních komunikačních služeb nezávislých na číslech by měli 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 podle směrnice (EU) 2018/1972, které využívají čísla a nevykonávají skutečnou kontrolu nad přenosem signálů.

(97) Vnitřní trh více než kdy předtím spoléhá na fungování internetu. Na službách poskytovaných po internetu jsou závislé služby prakticky všech základních a důležitých subjektů. V zájmu zajištění hladkého poskytování služeb poskytovaných základními a důležitými subjekty je důležité, aby všichni poskytovatelé veřejných sítí elektronických komunikací zavedli vhodná opatření k řízení kybernetických bezpečnostních rizik a oznamovali související významné incidenty. Členské státy by měly zajistit zachování bezpečnosti veřejných sítí elektronických komunikací a ochranu jejich životně důležitých bezpečnostních zájmů před sabotáží a špionáží. Vzhledem k tomu, že mezinárodní propojení posiluje a urychluje konkurenceschopnou digitalizaci Unie a jejího hospodářství, incidenty postihující podmořské komunikační kabely by měly být hlášeny týmu CSIRT nebo případně příslušnému orgánu. Národní strategie kybernetické bezpečnosti by měla v příslušných případech zohledňovat kybernetickou bezpečnost podmořských komunikačních kabelů a zahrnovat mapování potenciálních kybernetických bezpečnostních rizik a zmírňující opatření k zajištění nejvyšší úrovně jejich ochrany.

(98) V zájmu zajištění bezpečnosti veřejných sítí elektronických komunikací a veřejně dostupných služeb elektronických komunikací by mělo být podporováno používání šifrovacích technologií, zejména šifrování mezi koncovými body, jakož i bezpečnostních koncepcí zaměřených na data, jako jsou kartografie, segmentace, označování, přístupová politika a správa přístupu, a rozhodnutí o automatizovaném přístupu. Je-li to nezbytné, mělo by být používání šifrování, zejména šifrování mezi koncovými body, povinné pro poskytovatele veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací v souladu se zásadami bezpečnosti a soukromí již od návrhu a standardně pro účely této směrnice. 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 prevenci, vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. To by však nemělo oslabit šifrování mezi koncovými body, které je zásadní technologií pro účinnou ochranu údajů a soukromí a bezpečnost komunikací.

(99) V zájmu zajištění bezpečnosti a zabránění zneužívání a manipulaci s veřejnými sítěmi elektronických komunikací a veřejně dostupnými službami elektronických komunikací je třeba podporovat používání interoperabilních standardů bezpečného směrování, jež zajistí integritu a spolehlivost směrovacích funkcí v celém ekosystému poskytovatelů služeb přístupu k internetu.

(100) V zájmu zajištění funkčnosti a integrity internetu a podpory bezpečnosti a odolnosti systému jmen domén by měly být příslušné zúčastněné strany, včetně subjektů soukromého sektoru v Unii, poskytovatelů veřejně dostupných služeb elektronických komunikací, zejména poskytovatelů služeb přístupu k internetu, a poskytovatelů internetových vyhledávačů vybízeny k přijetí strategie diverzifikace řešení systému jmen domén. Členské státy by nadto měly podporovat rozvoj a používání veřejné a bezpečné evropské služby resolverů systému jmen domén.

(101) Tato směrnice stanoví vícefázový přístup k oznamování významných incidentů, tak aby bylo dosaženo správné rovnováhy mezi rychlým oznamováním, které pomáhá snížit potenciální šíření významných incidentů a umožňuje základním a důležitým subjektům žádat o podporu, na jedné straně a podrobným oznamováním, které čerpá cenná poučení z jednotlivých incidentů a s postupem času zvyšuje kybernetickou odolnost jednotlivých subjektů a celých odvětví, na straně druhé. V tomto ohledu by tato směrnice měla zahrnovat oznamování incidentů, které by na základě prvotního posouzení provedeného dotčeným subjektem mohly uvedenému subjektu způsobit závažné provozní narušení služeb nebo finanční ztrátu nebo postihnout jiné fyzické nebo právnické osoby tím, že by jim způsobily značnou hmotnou nebo nehmotnou újmu. Při tomto prvotním posouzení by měly být mimo jiné zohledněny dotčené sítě a informační systémy, a zejména jejich význam při poskytování služeb subjektu, závažnost a technické charakteristiky kybernetické hrozby a veškeré související zranitelnosti, které jsou využívány, jakož i zkušenosti subjektu s podobnými incidenty. Ukazatele, jako jsou rozsah, v jakém je ovlivněno fungování služby, doba trvání incidentu nebo počet dotčených příjemců služeb, by mohly hrát důležitou úlohu při určování toho, zda je provozní narušení služby závažné.

(102) Pokud se základní nebo důležité subjekty dozvědí o významném incidentu, měly by mít povinnost bez zbytečného odkladu a v každém případě do 24 hodin podat včasné varování. Po tomto včasném varování by mělo následovat oznámení incidentu. Dotčené subjekty by měly oznámení o incidentu podat bez zbytečného odkladu a v každém případě do 72 hodin od okamžiku, kdy se o významném incidentu dozvěděly, zejména s cílem aktualizovat informace předložené prostřednictvím včasného varování a uvést prvotní posouzení významného incidentu, včetně jeho závažnosti a dopadu, jakož i indikátory narušení, jsou-li k dispozici. Nejpozději jeden měsíc po oznámení incidentu by měla být předložena závěrečná zpráva. Včasné varování by mělo zahrnovat pouze informace nezbytné k tomu, aby se tým CSIRT nebo případně příslušný orgán dozvěděly o významném incidentu a aby dotčený subjekt mohl v případě potřeby požádat o pomoc. Toto včasné varování by mělo případně uvádět, zda existuje podezření, že významný incident byl způsoben nezákonným nebo svévolným zásahem, a zda je pravděpodobné, že bude mít přeshraniční dopad. Členské státy by měly zajistit, aby povinnost podat toto včasné varování nebo následné

oznámení incidentu neodváděla zdroje oznamujícího subjektu od činností souvisejících s řešením incidentu, které by měly být upřednostněny, aby se zabránilo tomu, že kvůli povinnosti oznamování incidentů dojde buď k odvádění zdrojů z řešení reakce na významný incident, nebo se jinak naruší úsilí subjektů v tomto ohledu. V případě, že v okamžiku, kdy by měla být předložena závěrečná zpráva, incident stále trvá, členské státy zajistí, aby dotčené subjekty v uvedené lhůtě předložily zprávu o pokroku a poté nejpozději jeden měsíc po vyřešení významného incidentu závěrečnou zprávu.

(103) V příslušných případech by základní a důležité subjekty měly příjemcům svých služeb bez zbytečného odkladu sdělit veškerá opatření nebo nápravná opatření, která mohou přijmout ke zmírnění výsledných rizik vyplývajících z významné kybernetické hrozby. Uvedené subjekty by měly podle potřeby, a zejména, když je pravděpodobné, že se významná kybernetická hrozba naplní, rovněž informovat příjemce své služby o samotné hrozbě. Požadavek na informování těchto příjemců o významných kybernetických hrozbách by se měl splnit s vynaložením maximálního úsilí, ale tyto subjekty by neměl zbavovat povinnosti přijmout na vlastní náklady přiměřená a okamžitá opatření s cílem zamezit těmto hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto informace o významných kybernetických hrozbách by měly být příjemcům služby poskytovány zdarma a měly by být formulovány ve snadno srozumitelném jazyce.

(104) Poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací by měli zavádět bezpečnostní prvky standardně a záměrně a příjemce svých služeb informovat o významných kybernetických hrozbách a o opatřeních, která mohou přijmout, aby chránili bezpečnost svých zařízení a své komunikace, například použitím specifických druhů softwaru nebo šifrovacích technologií.

(105) Proaktivní přístup ke kybernetickým hrozbám je zásadní složkou opatření k řízení kybernetických bezpečnostních rizik, jenž by měl příslušným orgánům umožnit účinně předcházet tomu, aby kybernetické hrozby přerostly do incidentů, jež mohou způsobit značnou hmotnou či nehmotnou újmu. Za tímto účelem má ohlašování kybernetických hrozeb klíčový význam. S tímto záměrem jsou subjekty motivovány k dobrovolnému podávání zpráv o kybernetických hrozbách.

(106) Aby se zjednodušilo oznamování informací požadovaných podle této směrnice a snížila administrativní zátěž subjektů, měly by členské státy pro předkládání relevantních informací, jež se mají oznamovat, poskytnout technické prostředky, jako jsou jednotné kontaktní místo, automatizované systémy, on-line formuláře, uživatelsky přívětivá rozhraní, šablony a specializované platformy pro využívání ze strany subjektů bez ohledu na to, zda se na ně tato směrnice vztahuje. Finanční prostředky Unie na podporu provádění této směrnice, zejména v rámci programu Digitální Evropa zavedeného nařízením Evropského parlamentu a Rady (EU) 2021/694 ([21]), by mohly zahrnovat podporu pro jednotná kontaktní místa. Subjekty jsou navíc 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 administrativní zátěž a mohou také vést k nejasnostem, pokud jde o formát a postupy takových oznámení. Je-li zřízeno jednotné kontaktní místo, členské státy se rovněž vybízejí, aby toto jednotné kontaktní místo používaly pro oznamování bezpečnostních incidentů požadovaných podle jiných právních předpisů Unie, jako je nařízení (EU) 2016/679 a směrnice 2002/58/ES. Používáním tohoto jednotného kontaktního místa pro oznamování bezpečnostních incidentů podle nařízení (EU) 2016/679 a směrnice 2002/58/ES by nemělo být dotčeno uplatňování ustanovení nařízení (EU) 2016/679 a směrnice 2002/58/ES, zejména těch, která se týkají nezávislosti orgánů v nich uvedených. Agentura ENISA ve spolupráci se skupinou pro spolupráci vypracuje a neustále zdokonaluje společné šablony oznamování prostřednictvím pokynů, které zjednoduší a zefektivní informace, jež mají být oznamovány podle právních předpisů Unie, a sníží administrativní zátěž pro oznamující subjekty.

(107) 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 donucovacím orgánům z vlastního podnětu oznamovaly incidenty, v jejichž souvislosti existuje podezření o spáchání závažné trestné činnosti. 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 Evropské centrum pro boj proti kyberkriminalitě (EC3) a agentura ENISA.

([21]) Nařízení Evropského parlamentu a Rady (EU) 2021/694 ze dne 29. dubna 2021, kterým se zavádí program Digitální Evropa a zrušuje rozhodnutí (EU) 2015/2240 (Úř. věst. L 166, 11.5.2021, s. 1).

(108) V důsledku incidentů je v mnoha případech ohrožena ochrana osobních údajů. V této souvislosti by příslušné orgány měly spolupracovat a vyměňovat si informace o všech relevantních záležitostech s orgány uvedenými v nařízení (EU) 2016/679 a směrnici 2002/58/ES.

(109) Udržování přesných a úplných databází registračních údajů jmen domén (údajů WHOIS) a poskytování zákonného přístupu k těmto údajům má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému jmen domén, což na druhé straně přispívá k vyšší společné úrovni kybernetické bezpečnosti v celé Unii. Za tímto konkrétním účelem by registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén měly být povinny zpracovávat určité údaje nezbytné k dosažení tohoto účelu. Takové zpracování by mělo představovat právní povinnost ve smyslu čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679. Touto povinností není dotčena možnost shromažďovat údaje o registraci jmen domén pro jiné účely, například na základě smluvních ujednání nebo právních požadavků stanovených v jiných unijních nebo vnitrostátních právních předpisech. Cílem této povinnosti je dosáhnout úplnosti a přesnosti souboru registračních údajů a neměla by vést k vícenásobnému shromažďování stejných údajů. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by měly vzájemně spolupracovat, aby se zabránilo zdvojování tohoto úkolu.

(110) Dostupnost údajů o registraci jmen domén pro oprávněné žadatele o přístup a včasný přístup k uvedeným údajům má zásadní význam pro prevenci zneužívání systému překladu jmen domén a boj proti němu a pro prevenci a odhalování incidentů a reakci na ně. Oprávněnými žadateli o přístup se mají rozumět jakákoli fyzická nebo právnická osoba, která podává žádost podle unijního nebo vnitrostátního práva. Mezi tyto orgány mohou náležet orgány příslušné podle této směrnice a orgány, které jsou podle unijního nebo vnitrostátního práva příslušné pro prevenci, vyšetřování, odhalování či stíhání trestných činů, a skupiny CERT nebo týmy CSIRT. Registry jmen domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by měly mít povinnost umožnit oprávněným žadatelům o přístup zákonný přístup ke konkrétním údajům o registraci jmen domén, které jsou nezbytné pro účely žádosti o přístup, v souladu s právem Unie a vnitrostátním právem. K žádosti oprávněných žadatelů o přístup by mělo být přiloženo odůvodnění umožňující posoudit nezbytnost přístupu k údajům.

(111) S cílem zajistit dostupnost přesných a úplných údajů o registraci jmen domén by registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén měly shromažďovat údaje o registraci jmen domén a zaručovat integritu a dostupnost těchto údajů. Registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by zejména měly stanovit politiky a postupy pro shromažďování a uchovávání přesných a úplných registračních údajů doménového jména a rovněž zamezit uvádění nesprávných registračních údajů a opravovat je v souladu s právem Unie v oblasti ochrany údajů. Tyto politiky a postupy by měly v co největší míře zohledňovat normy vypracované řídícími strukturami s mnoha zúčastněnými stranami na mezinárodní úrovni. Registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by měly přijmout a zavést přiměřené postupy pro ověřování údajů souvisejících s registrací jmen domén. Tyto postupy by měly odrážet osvědčené postupy používané v daném odvětví a pokud možno pokrok dosažený v oblasti elektronické identifikace. Mezi příklady ověřovacích postupů mohou patřit kontroly *ex ante* prováděné v době registrace a kontroly *ex post* prováděné po registraci. Registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by měly zejména ověřit alespoň jeden způsob kontaktu žadatele o registraci.

(112) Registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by měly mít v souladu s body odůvodnění nařízení (EU) 2016/679 povinnost zveřejňovat takové údaje o registraci jmen domén, na které se nevztahuje oblast působnosti práva Unie v oblasti ochrany údajů, jako jsou údaje týkající se právnických osob. V případě právnických osob by registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén měly zveřejnit alespoň název žadatele o registraci a jeho kontaktní telefonní číslo. Kontaktní e-mailová adresa by měla být rovněž zveřejněna za předpokladu, že neobsahuje žádné osobní údaje, jako je tomu v případě používání e-mailových přezdívek nebo funkčních účtů. Registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by také měly v souladu s právem Unie v oblasti ochrany údajů umožnit oprávněným žadatelům o přístup zákonný přístup ke konkrétním údajům o registraci domén týkajícím se fyzických osob. Členské státy by měly požadovat, aby registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén reagovaly bez zbytečného odkladu na žádosti o zveřejnění údajů o registraci jmen domén oprávněných žadatelů o přístup. Registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by měly stanovit postupy a procesy pro zveřejňování a zpřístupnění registračních údajů, včetně dohod o úrovni služeb k vyřizování žádostí o přístup od oprávněných žadatelů o přístup. Tyto politiky a postupy by měly v co největší míře zohledňovat veškeré pokyny a normy vypracované správními strukturami mnoha zúčastněných stran na

mezinárodní úrovni. Postup poskytování přístupu by mohl také obsahovat užívání rozhraní, portálu nebo jiných technických nástrojů k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům S cílem podpořit harmonizované postupy na celém vnitřním trhu může Komise, aniž jsou dotčeny pravomoci Evropské rady pro ochranu údajů, poskytnout pokyny týkající se těchto postupů, které pokud možno zohlední normy vypracované správními strukturami mnoha zúčastněných stran na mezinárodní úrovni. Členské státy by měly zajistit, aby všechny druhy přístupu k osobním i neosobním údajům o registraci jmen domén byly bezplatné.

(113) Subjekty spadající do oblasti působnosti této směrnice by měly být považovány za subjekty podléhající pravomoci členského státu, v němž jsou usazeny. Avšak u poskytovatelů veřejných sítí elektronických komunikací nebo poskytovatelů veřejně dostupných služeb elektronických komunikací by se mělo mít za to, že podléhají pravomoci členského státu, v němž poskytují své služby. Provozovatelé DNS, registry domén nejvyšší úrovně, subjekty poskytující služby registrace jmen domén, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center, poskytovatelé sítí pro doručování obsahu, poskytovatelé řízených služeb, poskytovatelé řízených bezpečnostních služeb, poskytovatelé on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí by se měli považovat za spadající pod pravomoc členského státu, ve kterém mají hlavní provozovnu v Unii. Subjekty veřejné správy by měly spadat do pravomoci členského státu, který je zřídil. Poskytuje-li subjekt služby nebo je usazen 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. Pokud členské státy vykonávají pravomoc, neměly by za stejné jednání ukládat donucující opatření ani sankce více než jednou v souladu se zásadou zákazu dvojího trestání.

(114) S cílem zohlednit přeshraniční povahu služeb a činností provozovatelů DNS, registrů domén nejvyšší úrovně, subjektů poskytujících služby registrace jmen domén, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center, poskytovatelů sítí pro doručování obsahu, poskytovatelů řízených bezpečnostních služeb, poskytovatelů internetových tržišť, internetových vyhledávačů a služeb platforem sociálních sítí by měl mít pravomoc nad těmito subjekty pouze jeden členský stát. Pravomoc by měl mít ten členský stát, v němž má dotčený subjekt v rámci Unie hlavní provozovnu. Kritérium provozovny 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 hlavní provozovny, a tudíž ani nejsou rozhodujícími kritérii pro její určení. Mělo by se mít za to, že hlavní provozovna se nachází v členském státě, kde jsou v Unii převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa subjektu v Unii. Nelze-li takový členský stát určit nebo nejsou-li tato rozhodnutí přijímána v Unii, mělo by se mít se za to, že hlavní provozovna je v členském státě, v němž jsou prováděny operace v oblasti kybernetické bezpečnosti. Nelze-li takový členský stát určit, mělo by se mít za to, že hlavní provozovna se nachází v členském státě, v němž má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud jsou služby prováděny skupinou podniků, měla by se za hlavní provozovnu skupiny podniků považovat hlavní provozovna řídícího podniku.

(115) Pokud je veřejně přístupná rekurzivní služba systému pro překlad jmen domén poskytována poskytovatelem veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací pouze jako součást služby přístupu k internetu, měl by být daný subjekt považován za subjekt spadající do pravomoci všech členských států, v nichž jsou jeho služby poskytovány.

(116) Pokud provozovatel DNS, registr domén nejvyšší úrovně, subjekt poskytující služby registrace jmen domén, poskytovatel služeb cloud computingu, poskytovatel služeb datového centra, poskytovatel sítě pro doručování obsahu, poskytovatel řízených služeb, poskytovatel řízených bezpečnostních služeb, poskytovatel on-line tržišť, poskytovatel internetových vyhledávačů, nebo poskytovatel služeb platforem sociálních sítí, který není usazen v Unii, nabízí služby v Unii, měl by určit svého zástupce v Unii. Aby bylo možno určit, zda takový subjekt nabízí služby v rámci Unie, mělo by být ověřeno, zda má tento subjekt 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 nebo dalších kontaktních údajů nebo používání jazyka obecně používaného ve třetí zemi, v níž je subjekt usazen, by k ověření tohoto úmyslu postačovat neměla. Avšak faktory jako používání jazyka nebo měny obecně používaných v jednom nebo více členských státech, spolu s možností objednat služby v tomto jazyce, nebo zmínka o zákaznících či uživatelích nacházejících se v Unii by mohly 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 mít možnost se na něj obrátit. Zástupce by měl být výslovně písemně pověřen subjektem, aby mohl jednat jeho jménem v otázkách jeho povinností stanovených v této směrnici, včetně oznamování incidentů.

(117) Aby byl zajištěn jasný přehled provozovatelů DNS, registrů domén nejvyšší úrovně, subjektů poskytujících služby registrace jmen domén, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center, poskytovatelů sítí pro doručování obsahu, poskytovatelů řízených služeb, poskytovatelů řízených bezpečnostních služeb, poskytovatelů on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí, které poskytují služby v celé Unii spadající do oblasti působnosti této směrnice, měla by agentura ENISA vytvořit a vést registr těchto subjektů na základě informací, jež obdrží členské státy, případně prostřednictvím vnitrostátních mechanismů zřízených k tomu, aby se subjekty registrovaly samy. Jednotná kontaktní místa by měla předávat agentuře ENISA tyto informace a jejich veškeré změny. V zájmu zajištění přesnosti a úplnosti informací, které by měly být v tomto registru zahrnuty, by členské státy měly agentuře ENISA předložit informace o těchto subjektech, jež mají k dispozici ve svých vnitrostátních registrech. Agentura ENISA a členské státy by měly přijmout opatření s cílem usnadnit interoperabilitu těchto registrů a současně zajistit ochranu důvěrných nebo utajovaných informací. Agentura ENISA by měla zavést vhodné protokoly pro klasifikaci informací a řízení rizik s cílem zajistit bezpečnost a důvěrnost zpřístupněných informací, přičemž přístup k těmto informacím, jejich uchovávání a přenos by měla omezit na zamýšlené uživatele.

(118) Pokud jsou podle této směrnice vyměňovány, oznamovány nebo jinak sdíleny informace, které jsou v souladu s unijním nebo vnitrostátním právem v utajovaném režimu, měla by se použít odpovídající pravidla o nakládání s utajovanými informacemi. Kromě toho by agentura ENISA měla mít infrastrukturu a zavedené postupy a pravidla pro nakládání s citlivými a utajovanými informacemi v souladu s platnými bezpečnostními předpisy na ochranu utajovaných informací EU.

(119) S tím, jak se kybernetické hrozby stávají stále složitějšími a sofistikovanějšími, účinná opatření v oblasti odhalování těchto hrozeb a jejich 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 v incidenty, a umožňuje subjektům lépe zachycovat dopady incidentů a efektivněji se zotavovat. Jelikož na úrovni Unie příslušné pokyny neexistují, takovému sdílení zpravodajských informací, zdá se, brání různé faktory, zejména nejistota ohledně slučitelnosti s pravidly hospodářské soutěže a pravidly odpovědnosti.

(120) Členské státy by měly subjekty motivovat a pomáhat jim k tomu, aby společně využívaly svých individuálních znalostí a praktických zkušeností na strategické, taktické a operativní úrovni s cílem zlepšit své schopnosti předcházet incidentům, odhalovat je, reagovat na ně, zotavovat se z nich nebo zmírňovat jejich dopad. Je proto nezbytné umožnit na úrovni Unie vznik dobrovolných ujednání o sdílení informací o kybernetické bezpečnosti. Členské státy by za tímto účelem měly aktivně podporovat a motivovat subjekty, jako jsou subjekty zaměřené na poskytování služeb a výzkumu v oblasti kybernetické bezpečnosti, a relevantní subjekty, jež nespadají do oblasti působnosti této směrnice, aby se účastnily takovýchto opatření ujednání o sdílení informací o kybernetické bezpečnosti. Tato ujednání by měla být zavedena v souladu s pravidly Unie v oblasti hospodářské soutěže a právními předpisy Unie v oblasti ochrany údajů.

(121) Zpracování osobních údajů v rozsahu nutném a přiměřeném pro zajištění bezpečnosti sítí a informačních systémů ze strany základních a důležitých subjektů by mohlo být považováno za zákonné na základě toho, že takové zpracování splňuje právní povinnost, která se vztahuje na správce, v souladu s požadavky čl. 6 odst. 1 písm. c) a čl. 6 odst. 3 nařízení (EU) 2016/679. Zpracování osobních údajů by mohlo být rovněž nezbytné pro oprávněné zájmy základních a důležitých subjektů, jakož i poskytovatelů bezpečnostních technologií a služeb jednajících jménem těchto subjektů podle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679, včetně případů, kdy je takové zpracování nezbytné pro ujednání o sdílení informací o kybernetické bezpečnosti nebo dobrovolné oznamování příslušných informací v souladu s touto směrnicí. Opatření týkající se prevence, odhalování, identifikace, zamezení šíření, analýzy incidentů a reakce na incidenty, opatření ke zvyšování povědomí o konkrétních kybernetických hrozbách, výměny informací v rámci nápravy zranitelností a jejich koordinovaného zveřejňování, a také dobrovolné výměny informací o těchto incidentech, kybernetických hrozbách a zranitelnostech, indikátorech narušení, taktice, technikách a postupech, varováních v oblasti kybernetické bezpečnosti a konfiguračních nástrojích by mohla vyžadovat zpracovávání určitých kategorií osobních údajů, například IP adres, jednotných adres zdroje (URL), jmen domén, e-mailových adres a, odhalují-li osobní údaje, časových razítek. Zpracování osobních údajů příslušnými orgány, jednotnými kontaktními místy a týmy CSIRT by mohlo představovat právní povinnost nebo by mohlo být považováno za nezbytné pro plnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce údajů podle čl. 6 odst. 1 písm. c) nebo e) a čl. 6 odst. 3 nařízení (EU) 2016/679, nebo pro sledování oprávněného zájmu základních a důležitých subjektů, jak je uvedeno v čl. 6 odst. 1 písm. f) uvedeného nařízení.. Kromě toho by vnitrostátní právo mohlo stanovit pravidla, která příslušným orgánům, jednotným kontaktním místům a týmům CSIRT v rozsahu, který je nezbytný a přiměřený pro účely zajištění bezpečnosti sítí a informačních systémů základních a důležitých subjektů, umožní zpracovávat zvláštní kategorie osobních údajů v souladu s článkem 9 nařízení (EU) 2016/679, zejména stanovením vhodných a konkrétních opatření na ochranu základních práv a zájmů fyzických osob, včetně technických omezení opakovaného použití těchto údajů a používání nejmodernějších bezpečnostních opatření a opatření na ochranu soukromí, jako je pseudonymizace nebo šifrování, pokud může anonymizace mít významný vliv na sledovaný účel.

(122) S cílem posílit pravomoci a opatření v oblasti 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 těchto subjektů a povinností příslušných orgánů. Základní subjekty by tak měly podléhat komplexnímu režimu dohledu ex ante a ex post, zatímco důležité subjekty by měly podléhat mírnému režimu dohledu pouze ex post. Důležité subjekty by tedy neměly mít povinnost systematicky dokumentovat soulad s opatřeními k řízení kybernetických bezpečnostních rizik, zatímco příslušné orgány by měly provádět reaktivní ex post přístup k dohledu a neměly by tedy mít obecnou povinnost dohlížet na tyto subjekty. Dohled *ex post* nad důležitými subjekty může být zahájen na základě důkazů, indicií či informací, které byly příslušným orgánům oznámeny a o nichž mají tyto orgány za to, že nasvědčují možnému porušení této směrnice. Mohlo by se například jednat o takový druh důkazů, indicií nebo informací, jaký příslušným orgánům poskytují jiné orgány, subjekty, občané, sdělovací prostředky nebo jiné zdroje, nebo by se mohlo jednat o veřejně dostupné informace či o důkazy, indicie nebo informace, které by mohly vyplynout z jiných činností prováděných příslušnými orgány při plnění jejich úkolů.

(123) Provádění dohledu příslušnými orgány by nemělo zbytečně omezovat obchodní činnost dotčeného subjektu. Pokud příslušné orgány vykonávají úkoly v oblasti dohledu ve vztahu k základním subjektům, včetně kontrol na místě a externího dohledu, vyšetřování porušení této směrnice, a provádějí bezpečnostní audity nebo bezpečnostní prověrky, měly by minimalizovat dopad na obchodní činnosti dotčeného subjektu.

(124) Pokud jde o výkon dohledu *ex ante*, příslušné orgány by měly mít možnost rozhodnout o stanovení priorit při přiměřeném použití opatření a prostředků dohledu, jež mají k dispozici. To znamená, že příslušné orgány mohou o tomto stanovení priorit rozhodnout na základě metodik dohledu, které by se měly řídit přístupem založeným na posouzení rizik. Konkrétně by tyto metodiky mohly zahrnovat kritéria nebo referenční hodnoty pro zařazení základních subjektů do kategorií podle rizika a odpovídající opatření a prostředky dohledu doporučené pro jednotlivé kategorie podle rizika, jako jsou využití, četnost nebo druhy kontrol na místě, cílené bezpečnostní audity či bezpečnostní prověrky, druhy informací, jež mají být vyžadovány, a míra podrobnosti těchto informací. Tyto metodiky dohledu by mohly být rovněž doplněny o pracovní programy a pravidelně posuzovány a přezkoumávány,

a to i pokud jde o aspekty, jako jsou přidělování zdrojů a potřeby v této oblasti. Pokud jde o subjekty veřejné správy, měly by být pravomoci dohledu vykonávány v souladu s vnitrostátními právními předpisy a institucionálními rámci.

(125) Příslušné orgány by měly zajistit, aby jejich úkoly v oblasti dohledu nad základními a důležitými subjekty vykonávali vyškolení odborníci, kteří by měli mít nezbytné dovednosti k plnění těchto úkolů, zejména pro provádění kontrol na místě a externího dohledu, včetně zjišťování nedostatků v databázích, hardwaru, firewallech, šifrování a sítích. Tyto kontroly a tento dohled by měly být prováděny objektivně.

(126) V řádně odůvodněných případech, kdy si je příslušný orgán vědom podstatné kybernetické hrozby nebo bezprostředního rizika, měl by mít možnost okamžitě přijmout rozhodnutí o výkonu opatření, aby předešel incidentu nebo na něj reagoval.

(127) K zajištění účinného vymáhání by měl být stanoven minimální seznam pravomocí v oblasti vymáhání, jež lze uplatnit v případě porušení opatření k řízení kybernetických bezpečnostních rizik a oznamovacích povinností, jež stanoví tato směrnice, čímž se vytvoří jasný a jednotný rámec pro takové vymáhání v celé Unii. Náležitá pozornost by měla být věnována povaze, závažnosti a době trvání porušení této směrnice, způsobené hmotné či nehmotné újmě, úmyslné nebo nedbalostní povaze porušení, opatřením přijatým za účelem zamezení nebo zmenšení způsobené hmotné či nehmotné újmy, míře odpovědnosti nebo jakémukoli relevantnímu porušení v minulosti, míře spolupráce s příslušným orgánem a jakýmkoli jiným přitěžujícím nebo polehčujícím okolnostem. Opatření v oblasti vymáhání, včetně správních pokut, by měla být přiměřená a jejich uložení by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny základních práv Evropské unie (dále jen „Listina“), včetně práva na účinnou nápravu a spravedlivý proces, presumpce neviny a práva na obhajobu.

(128) Tato směrnice nevyžaduje, aby členské státy stanovily trestní nebo občanskoprávní odpovědnost fyzických osob, které nesou odpovědnost za zajištění dodržování této směrnice subjektem v souvislosti s újmou, kterou utrpěly třetí strany v důsledku porušení této směrnice.

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

(130) Pro účely uložení správní pokuty základnímu nebo důležitému subjektu, který je podnikem, by měl být podnik chápán ve smyslu článků 101 a 102 Smlouvy o fungování EU. Je-li správní pokuta uložena osobě, která není podnikem, měl by příslušný orgán 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.

(131) 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 Evropské unie.

(132) Nejsou-li správní sankce harmonizovány touto směrnicí nebo v případě potřeby v jiných případech, jako při závažném porušení této směrnice, měly by členské státy zavést systém, který zajistí uložení účinných, přiměřených a odrazujících sankcí. Povaha těchto sankcí a skutečnost, zda se jedná o trestní nebo správní sankce, by měla být stanovena vnitrostátním právem.

(133) Aby se dále posílila účinnost a odrazující účinek opatření v oblasti vymáhání, jež jsou uplatňována v případě porušení této směrnice, měly by být příslušné orgány oprávněny dočasně pozastavit certifikace nebo povolení týkající se části nebo všech relevantních služeb, jež poskytuje základní subjekt, nebo činností, jež vykonává, nebo požádat o jejich dočasné pozastavení, a požadovat uložení dočasného zákazu výkonu řídicích funkcí jakékoliv fyzické osobě, která má odpovědnost za výkon řídicích funkcí na úrovni výkonného ředitele nebo zákonného zástupce. Vzhledem k jejich závažnosti a dopadu na činnost subjektů a v konečném důsledku na uživatele by tato dočasná pozastavení nebo tyto zákazy měly být uplatňovány pouze úměrně závažnosti porušení a s ohledem na okolnosti každého jednotlivého případu, včetně úmyslné nebo nedbalostní povahy porušení, a úměrně k jakýmkoli opatřením přijatým k zamezení nebo zmírnění způsobené hmotné či nehmotné újmy. Tato dočasná pozastavení nebo tyto dočasné zákazy by se měly používat jen jako krajní prostředek, což znamená pouze po vyčerpání ostatních relevantních donucovacích opatření, jež stanoví tato směrnice, a pouze do té doby, než dotčený subjekt přijme nezbytná opatření k nápravě nedostatků nebo k dosažení souladu s požadavky příslušného orgánu, kvůli kterým byla uložena tato dočasná pozastavení nebo tyto dočasné zákazy. Uložení takových dočasných pozastavení nebo zákazů by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listinou, včetně práva na účinnou nápravu a na spravedlivý proces, presumpce neviny a práva na obhajobu.

(134) Za účelem zajištění toho, že subjekty budou plnit své povinnosti stanovené v této směrnici, by členské státy měly spolupracovat a měly by si být vzájemně nápomocny, pokud jde o opatření v oblasti dohledu a vymáhání, zejména pokud některý subjekt poskytuje služby ve více než jednom členském státě nebo pokud se jeho sítě a informační systémy nacházejí v jiném členském státě, než ve kterém poskytuje služby. Při poskytování pomoci by dožádaný příslušný orgán měl přijmout opatření v oblasti dohledu a vymáhání v souladu s vnitrostátním právem. V zájmu zajištění hladkého fungování vzájemné pomoci podle této směrnice by měly příslušné orgány využívat skupinu pro spolupráci jako fórum pro projednávání případů a konkrétních žádostí o pomoc.

(135) V zájmu zajištění účinného dohledu a vymáhání, zejména v situaci s přeshraničním rozměrem, by členský stát, který obdržel žádost o vzájemnou pomoc, měl v rozsahu dané žádosti přijmout vhodná opatření v oblasti dohledu a vymáhání ve vztahu k subjektu, jehož se uvedená žádost týká a který na území takového členského státu poskytuje služby nebo má na jeho území svou síť a informační systém.

(136) Tato směrnice by měla stanovit pravidla spolupráce mezi příslušnými orgány a dozorovými úřady na základě nařízení (EU) 2016/679 pro řešení případů porušení této směrnice souvisejících s osobními údaji.

(137) Cílem této směrnice by mělo být zajistit vysokou míru odpovědnosti za opatření k řízení kybernetických bezpečnostních rizik a v oblasti oznamovacích povinností na úrovni základních a důležitých subjektů. Řídící orgány základních a důležitých subjektů by proto měly schválit opatření k řízení kybernetických bezpečnostních rizik a dohlížet na jejich provádění.

(138) Za účelem zajištění vysoké společné úrovně kybernetické bezpečnosti v celé Unii na základě této směrnice by Komisi měla být svěřena pravomoc přijmout akty v souladu s článkem 290 Smlouvy o fungování EU, pokud jde o doplnění této směrnice upřesněním kategorií základních a důležitých subjektů, které mají být povinny používat určité certifikované produkty IKT, služby IKT a procesy IKT nebo získat osvědčení podle některého evropského systému 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 ([22]). 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 setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

([22]) Úř. věst. L 123, 12.5.2016, s. 1.

(139) Za účelem zajištění jednotných podmínek k provedení této směrnice by Komisi měly být svěřeny prováděcí pravomoci ke stanovení procesních opatření nezbytných pro fungování skupiny pro spolupráci a technických a metodických, jakož i odvětvových požadavků týkajících se opatření k řízení kybernetických bezpečnostních rizik, a k dalšímu upřesnění druhu informací, formátu a postupu oznamování incidentů, kybernetických hrozeb a významných událostí, a upřesnění komunikace o významných kybernetických hrozbách, jakož i případů, kdy je třeba považovat incident za významný. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ([23]).

(140) Komise by měla provádět pravidelný přezkum této směrnice po konzultaci se zúčastněnými stranami, zejména pokud jde o rozhodnutí, zda je vhodné navrhnout změny s ohledem na měnící se společenské, politické, technologické nebo tržní podmínky. V rámci přezkumů by Komise měla posoudit, jaký význam mají velikost dotčených subjektů a odvětví, pododvětví a druhy subjektu uvedené v přílohách této směrnice pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností. Komise by měla mimo jiné posoudit, zda by poskytovatelé, na které se vztahuje oblast působnosti této směrnice a již jsou označeni jakožto velmi velké on-line platformy ve smyslu článku 33 nařízení Evropského parlamentu a Rady (EU) 2022/2065 ([24]), mohli být podle této směrnice označeni za základní subjekty.

(141) Tato směrnice vytváří nové úkoly pro agenturu ENISA, čímž posiluje její úlohu, a může vést rovněž k požadavku, aby agentura ENISA plnila své stávající úkoly, které jí nyní stanoví nařízení (EU) 2019/881, na vyšší úrovni než dříve. S cílem zajistit, aby agentura ENISA měla potřebné finanční a lidské zdroje pro stávající a nové úkoly a aby splňovala veškeré vyšší úrovně plnění těchto úkolů vyplývající z její posílené úlohy, by měl být odpovídajícím způsobem navýšen její rozpočet. V zájmu zajištění účinného využívání zdrojů by navíc měla být agentuře ENISA poskytnuta větší flexibilita tak, aby mohla interně přidělovat zdroje za účelem účinného vykonávání svých úkolů a plnění očekávání.

(142) Jelikož cíle této směrnice, totiž dosažení vysoké společné úrovně kybernetické bezpečnosti v celé Unii, nemůže být dosaženo uspokojivě členskými státy, ale spíše jej 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 nezbytné pro dosažení tohoto cíle.

(143) Tato směrnice dodržuje základní práva a ctí zásady uznané Listinou, 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, presumpci neviny a právo na obhajobu. Právo na účinnou právní ochranu se vztahuje i na příjemce služeb poskytovaných základními a důležitými subjekty. Tato směrnice by měla být prováděna v souladu s těmito právy a zásadami.

(144) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([25]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 11. března 2021 ([26]),

([23]) 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).

([24]) Nařízení (EU) 2022/2065 Evropského parlamentu a Rady ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách) (Úř. věst. L 277, 27.10.2022, s. 1).

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

([26]) Úř. věst. C 183, 11.5.2021, s. 3.

PŘIJALY TUTO SMĚRNICI:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

1. Touto směrnicí se stanoví opatření, jejichž účelem je dosáhnout vysoké společné úrovně kybernetické bezpečnosti v rámci Unie s cílem zlepšit fungování vnitřního trhu.

2. Za tímto účelem tato směrnice stanoví:

a) povinnosti, jež vyžadují, aby členské státy přijaly národní strategie kybernetické bezpečnosti, určily nebo zřídily příslušné orgány, orgány pro řešení kybernetických krizí, jednotná kontaktní místa pro kybernetickou bezpečnost (dále jen „jednotná kontaktní místa“) a týmy pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“);

b) opatření k řízení kybernetických bezpečnostních rizik a oznamovací povinnosti pro subjekty, jejichž druhy jsou uvedeny v příloze I nebo II, jakož i pro subjekty, jež jsou určeny jakožto kritické subjekty podle směrnice (EU) 2022/2022/2557;

c) pravidla a povinnosti týkající se sdílení informací o kybernetické bezpečnosti;

d) povinnosti členských států v oblasti dohledu a vymáhání.

Článek 2

Oblast působnosti

1. Tato směrnice se vztahuje na veřejné a soukromé subjekty, jejichž druhy jsou uvedeny v příloze I nebo II a které jsou považovány podle článku 2 přílohy doporučení 2003/361/ES za střední podniky, nebo které překračují stropy pro střední podniky stanovené v odstavci 1 uvedeného článku a které poskytují služby nebo vykonávají činnosti v rámci Unie.

Ustanovení čl. 3 odst. 4 přílohy uvedeného doporučení se pro účely této směrnice nepoužije.

2. Bez ohledu na jejich velikost se tato směrnice vztahuje také na subjekty, jejichž druh je uveden v příloze I nebo II, pro něž platí, že:

a) služby jsou poskytovány:

   i) poskytovateli veřejné sítě elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací;

   ii) poskytovateli služeb vytvářejících důvěru;

   iii) registry domén nejvyšší úrovně a provozovateli DNS;

b) subjekt je v některém členském státě výhradním poskytovatelem služeb, jež mají zásadní význam pro zachování kritických společenských nebo hospodářských činností;

c) narušení služby poskytované tímto subjektem by mohlo mít významný dopad na veřejný pořádek, veřejnou bezpečnost nebo ochranu zdraví;

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

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

f) subjekt je subjektem veřejné správy:

i) ústřední vlády, jak je vymezena členským státem podle vnitrostátního práva; nebo

ii) na regionální úrovni, jak je vymezena členským státem podle vnitrostátního práva, a na základě posouzení rizik poskytuje služby, jejichž narušení by mohlo mít významný dopad na kritické společenské nebo hospodářské činnosti.

3. Bez ohledu na jejich velikost se tato směrnice použije na subjekty určené jakožto kritické subjekty podle směrnice (EU) 2022/2557.

4. Bez ohledu na jejich velikost se tato směrnice použije na subjekty poskytující služby registrace jmen domén.

5. Členské státy mohou stanovit, že se tato směrnice vztahuje na:

a) subjekty veřejné správy na místní úrovni;

b) vzdělávací instituce, zejména pokud vykonávají kritické výzkumné činnosti.

6. Touto směrnicí není dotčena odpovědnost členských států za ochranu národní bezpečnosti ani jejich pravomoc chránit jiné základní funkce státu, včetně zajišťování územní celistvosti státu a zachování veřejného pořádku.

7. Tato směrnice se nevztahuje na subjekty veřejné správy, které vykonávají činnosti v oblasti národní bezpečnosti, veřejné bezpečnosti, obrany nebo vymáhání práva, včetně prevence, vyšetřování, odhalování a stíhání trestných činů.

8. Členské státy mohou osvobodit konkrétní subjekty, které vykonávají činnosti v oblasti národní bezpečnosti, veřejné bezpečnosti, obrany nebo vymáhání práva, včetně činností souvisejících s prevencí, vyšetřováním, odhalováním a stíháním trestných činů, nebo které poskytují služby výhradně subjektům veřejné správy uvedeným v odstavci 7 tohoto článku, v souvislosti s těmito činnostmi nebo službami od povinností stanovených v článku 21 nebo 23. V takových případech se na tyto konkrétní činnosti nebo služby nevztahují opatření v oblasti dohledu a vymáhání uvedená v kapitole VII. Pokud subjekty vykonávají činnosti nebo poskytují služby výlučně takového druhu, jaký je uveden v tomto odstavci, mohou členské státy rovněž rozhodnout, že osvobodí tyto subjekty od povinností stanovených v článcích 3 a 27.

9. Odstavce 7 a 8 se nepoužijí, pokud subjekt jedná jako poskytovatel služeb vytvářejících důvěru.

10. Tato směrnice se nevztahuje na subjekty, které členské státy vyňaly z oblasti působnosti nařízení (EU) 2022/2554 v souladu s čl. 2 odst. 4 uvedeného nařízení.

11. Povinnosti stanovené v této směrnici nezahrnují poskytování informací, jejichž zpřístupnění by bylo v rozporu se zásadními zájmy členských států v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany.

12. Touto směrnicí není dotčeno nařízení (EU) 2016/679 a nejsou jí dotčeny směrnice Evropského parlamentu a Rady 2002/58/ES, 2011/93/EU ([27]) a 2013/40/EU ([28]) ani směrnice (EU) 2022/2557.

13. Aniž je dotčen článek 346 Smlouvy o fungování EU, informace, které jsou důvěrné podle unijních či vnitrostátních pravidel, jako jsou pravidla pro zachovávání důvěrnosti obchodních informací, se vyměňují s Komisí a jinými příslušnými orgány v souladu s touto směrnicí 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 dotčených subjektů.

([27]) 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).

([28]) 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).

14. Subjekty, příslušné orgány, jednotná kontaktní místa a týmy CSIRT zpracovávají osobní údaje pouze v rozsahu nezbytném pro účely této směrnice a v souladu s nařízením (EU) 2016/679 a takové zpracování se opírá o článek 6 uvedeného nařízení.

Zpracování osobních údajů podle této směrnice poskytovateli veřejných sítí elektronických komunikací nebo poskytovateli veřejně dostupných služeb elektronických komunikací se provádí v souladu s právem Unie v oblasti ochrany údajů a právem Unie v oblasti ochrany soukromí, zejména v souladu se směrnicí 2002/58/ES.

Článek 3

Základní a důležité subjekty

1. Pro účely této směrnice se za základní subjekty považují:

a) subjekty, jejichž druh je uveden v příloze I, které překračují stropy pro střední podniky stanovené v čl. 2 odst. 1 přílohy doporučení 2003/361/ES;

b) kvalifikovaní poskytovatelé služeb vytvářejících důvěru, registry domén nejvyšší úrovně a provozovatelé DNS bez ohledu na jejich velikost;

c) poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací, kteří jsou považováni za střední podniky podle článku 2 přílohy doporučení 2003/361/ES;

d) subjekty veřejné správy podle čl. 2 odst. 2 písm. f) bodu i);

e) jakékoli jiné subjekty druhu, který je uveden v příloze I nebo II, jež členský stát označí za základní subjekty podle čl. 2 odst. 2 písm. b) až e);

f) subjekty určené jakožto kritické subjekty podle směrnice (EU) 2022/2557, jež jsou uvedeny v čl. 2 odst. 3 této směrnice;

g) pokud tak členský stát stanoví, subjekty, které tento členský stát označil před 16. lednem 2023 za provozovatele základních služeb v souladu se směrnicí (EU) 2016/1148 nebo s vnitrostátním právem.

2. Pro účely této směrnice se za důležité subjekty považují subjekty druhu uvedeného v příloze I nebo II, které nelze považovat za základní subjekty podle odstavce 1 tohoto článku. Patří k nim i subjekty, jež členské státy označily za důležité podle čl. 2 odst. 2 písm. b) až e).

3. Členské státy stanoví do 17. dubna 2025 seznam základních a důležitých subjektů, jakož i subjektů poskytujících služby registrace jmen domén. Členské státy tento seznam pravidelně, a to alespoň každé dva roky, přezkoumávají a v případě potřeby jej aktualizují.

4. Pro účely stanovení seznamu uvedeného v odstavci 3 členské státy vyžadují, aby subjekty zmíněné v uvedeném odstavci příslušným orgánům předložily alespoň tyto informace:

a) název subjektu;

b) adresu a aktuální kontaktní údaje, včetně e-mailových adres, rozsahu IP adres a telefonních čísel;

c) případně příslušná odvětví a pododvětví podle přílohy I nebo II; a

d) případně seznam členských států, v nichž poskytují služby spadající do oblasti působnosti této směrnice.

Subjekty uvedené v odstavci 3 oznámí všechny změny údajů, které předložily podle prvního pododstavce tohoto odstavce, a to neprodleně, nejpozději však do dvou týdnů od data změny.

Komise za pomoci Agentury Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“) bez zbytečného odkladu poskytne pokyny a šablony týkající se povinností stanovených v tomto odstavci.

Členské státy mohou zřídit vnitrostátní mechanismy, jejichž pomocí by se subjekty mohly registrovat samy.

5. Příslušné orgány do 17. dubna 2025 a poté každé 2 roky oznámí:

a) Komisi a skupině pro spolupráci počet základních a důležitých subjektů uvedených na seznamu podle odstavce 3 v každém odvětví a pododvětví uvedeném v příloze I nebo II a

b) Komisi příslušné informace o počtu základních a důležitých subjektů, které jsou za takové označeny podle čl. 2 odst. 2 písm. b) až e), informace o odvětví a pododvětví uvedených v příloze I nebo II, do nichž subjekty patří, o druhu služeb, které poskytují, a o tom, podle kterého z ustanovení uvedených v čl. 2 odst. 2 písm. b) až e) byly označeny za základní či důležité.

6. Do 17. dubna 2025 a na žádost Komise mohou členské státy oznámit Komisi názvy základních a důležitých subjektů uvedených v odst. 5 písm. b).

Článek 4

Odvětvové právní akty Unie

1. Pokud ustanovení odvětvových právních aktů Unie vyžadují, aby základní nebo důležité subjekty přijaly opatření k řízení kybernetických bezpečnostních rizik nebo aby oznamovaly významné incidenty, 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 VII, se na takové subjekty nepoužijí. Pokud se odvětvové právní akty Unie nevztahují na všechny subjekty v konkrétním odvětví, jež náleží do oblasti působnosti této směrnice, použijí se nadále na subjekty, na něž se uvedené odvětvové právní akty Unie nevztahují, příslušná ustanovení této směrnice.

2. Účinek požadavků uvedených v odstavci 1 tohoto článku se považuje za rovnocenný účinku povinností stanovených v této směrnici, pokud:

a) účinek opatření k řízení kybernetických bezpečnostních rizik je přinejmenším rovnocenný účinku opatření stanovených v čl. 21 odst. 1 a 2; nebo

b) odvětvový právní akt Unie stanoví okamžitý, případně automatický a přímý přístup k oznámením o incidentech, která podle této směrnice vydávají týmy CSIRT, příslušné orgány nebo jednotná kontaktní místa, a účinky požadavků na oznamování významných incidentů jsou přinejmenším rovnocenné účinkům požadavků stanovených v čl. 23 odst. 1 až 6 této směrnice.

3. Komise poskytne do 17. července 2023 pokyny objasňující uplatňování odstavců 1 a 2. Komise provádí pravidelný přezkum těchto pokynů. Při přípravě těchto pokynů zohlední Komise veškeré postřehy skupiny pro spolupráci a agentury ENISA.

Článek 5

Minimální harmonizace

Tato směrnice nebrání členským státům v tom, aby přijímaly nebo ponechaly v platnosti ustanovení zajišťující vyšší úroveň kybernetické bezpečnosti, jsou-li tato ustanovení v souladu s jejich povinnostmi stanovenými v právu Unie.

Článek 6

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; nebo

c) digitální data, jež jsou prvky uvedenými v písmenech 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 událostem, které mohou narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které jsou nabízeny prostřednictvím sítí a informačních systémů nebo které jsou jejich prostřednictvím přístupné;

3) „kybernetickou bezpečností“ kybernetická bezpečnost ve smyslu čl. 2 bodu 1 nařízení (EU) 2019/881;

4) „národní strategií kybernetické bezpečnosti“ soudržný rámec členského státu vymezující strategické cíle a priority v oblasti kybernetické bezpečnosti a správy za účelem jejich dosažení v tomto členském státě;

5) „významnou událostí“ událost, která mohla narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které nabízejí sítě a informační systémy nebo které jsou jejich prostřednictvím přístupné, ale plnému vzniku takové události bylo úspěšně zabráněno nebo taková událost nenastala;

6) „incidentem“ událost narušující dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které jsou nabízeny prostřednictvím sítí a informačních systémů nebo které jsou jejich prostřednictvím přístupné;

7) „rozsáhlým kybernetickým bezpečnostním incidentem“ incident, který způsobí úroveň narušení, jež přesahuje schopnost členského státu na takový incident reagovat, nebo který má významný dopad na nejméně dva členské státy;

8) „řešením incidentu“ jakékoli akce a postupy, jejichž cílem je incidentu předejít, odhalit jej, analyzovat, zamezit jeho šíření nebo na něj reagovat a zotavit se z něj;

9) „rizikem“ potenciální ztráta nebo narušení v důsledku incidentu, přičemž toto riziko je vyjádřeno jako kombinace rozsahu takové ztráty nebo takového narušení a pravděpodobnosti vzniku incidentu;

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

11) „významnou kybernetickou hrozbou“ kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že má potenciál vážně ovlivnit sítě a informační systémy určitého subjektu nebo uživatelů služeb takového subjektu tím, že způsobí značnou hmotnou nebo nehmotnou újmu;

12) „produktem IKT“ produkt IKT ve smyslu čl. 2 bodu 12 nařízení (EU) 2019/881;

13) „službou IKT“ služba IKT ve smyslu čl. 2 bodu 13 nařízení (EU) 2019/881;

14) „procesem IKT“ proces IKT ve smyslu čl. 2 bodu 14 nařízení (EU) 2019/881;

15) „zranitelností“ slabá stránka, snížená odolnost nebo chyba produktů IKT nebo služeb IKT, která může být využita kybernetickou hrozbou;

16) „normou“ norma ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ([29]);

17) „technickou specifikací“ technická specifikace ve smyslu čl. 2 bodu4 nařízení (EU) č. 1025/2012;

([29]) 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).

18) „výměnným uzlem internetu“ síťové zařízení umožňující propojení více než dvou nezávislých sítí (autonomních systémů), a to primárně pro účely umožnění výměny dat zasílaných prostřednictvím internetu; výměnný uzel internetu poskytuje propojení pouze autonomním systémům a 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;

19) „systémem překladu jmen domén“ nebo „DNS“ hierarchický distribuovaný systém překladu jmen domén, který umožňuje identifikaci internetových služeb a zdrojů a současně umožňuje, aby zařízení koncových uživatelů využívala služby směrování a připojení k internetu za účelem přístupu k těmto službám a zdrojům;

20) „provozovatelem služeb systému překladu jmen domén (DNS)“ nebo „provozovatelem DNS“ subjekt, který poskytuje:

a) veřejně dostupné rekurzívní služby pro překlad jmen domén koncovým uživatelům internetu; nebo

b) autoritativní služby pro překlad jmen domén pro použití třetí stranou, s výjimkou kořenových jmenných serverů;

21) „registrem domén nejvyšší úrovně“ nebo „registrem TLD“ subjekt, kterému byla delegována konkrétní doména nejvyšší úrovně (TLD) a je odpovědný za správu domén nejvyšší úrovně, včetně registrace jmen domén v rámci domén nejvyšší úrovně a technického provozu domén nejvyšší úrovně, včetně provozu jejích jmenných serverů, vedení jejích databází a distribuce souborů zón domén nejvyšší úrovně mezi jmennými servery, bez ohledu na to, zda kteroukoli z těchto operací provádí subjekt sám nebo je zajišťována externě, avšak s výjimkou situací, kdy jsou jména domén nejvyšší úrovně používána registrem pouze pro vlastní potřebu;

22) „subjektem poskytujícím služby registrace jmen domén“ registrátor nebo zástupce jednající jménem registrátorů, jako je poskytovatel služeb ochrany soukromí nebo zprostředkovatel registračních služeb nebo přeprodeje;

23) „digitální službou“ služba ve smyslu čl. 1 odst. 1 písm. b) směrnice Evropského parlamentu a Rady (EU) 2015/1535 ([30]);

24) „službou vytvářející důvěru“ služba vytvářející důvěru ve smyslu čl. 3 bodu 16 nařízení (EU) č. 910/2014;

25) „poskytovatelem služby vytvářející důvěru“ poskytovatel služeb vytvářejících důvěru ve smyslu čl. 3 bodu 19 nařízení (EU) č. 910/2014;

26) „kvalifikovanou službou vytvářející důvěru“ kvalifikovaná služba vytvářející důvěru ve smyslu čl. 3 bodu 17 nařízení (EU) č. 910/2014;

27) „kvalifikovaným poskytovatelem služby vytvářející důvěru“ kvalifikovaný poskytovatel služby vytvářející důvěru podle definice v čl. 3 bodu 20 nařízení (EU) č. 910/2014;

28) „on-line tržištěm“ on-line tržiště ve smyslu čl. 2 písm. n) směrnice Evropského parlamentu a Rady 2005/29/ES ([31]);

29) „internetovým vyhledávačem“ internetový vyhledávač ve smyslu čl. 2 bodu 5 nařízení Evropského parlamentu a Rady (EU) 2019/1150 ([32]);

30) „službou cloud computingu“ digitální služba, která umožňuje samoobslužnou správu a široký vzdálený přístup k rozšiřitelnému a pružnému seskupení sdílitelných výpočetních zdrojů, včetně těch, které jsou rozmístěny na více místech;

([30]) 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).

([31]) 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).

([32]) 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).

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

32) „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;

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

34) „zástupcem“ fyzická či právnická osoba usazená v Unii, výslovně pověřená, aby jednala jménem provozovatele DNS, registru domén nejvyšší úrovně, subjektu poskytujícího služby registrace jmen domén, poskytovatele služby cloud computingu, poskytovatele služeb datového centra, poskytovatele sítě pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, nebo poskytovatele on-line tržiště, internetového vyhledávače nebo služeb platforem sociálních sítí, který není usazen v Unii, přičemž vnitrostátní příslušný orgán nebo tým CSIRT může se zástupcem jednat namísto subjektu, pokud jde o povinnosti tohoto subjektu vyplývající z této směrnice;

35) „subjektem veřejné správy“ subjekt uznaný jako takový v členském státě v souladu s vnitrostátním právem, s výjimkou soudnictví, parlamentů a centrálních bank, který splňuje tato kritéria:

   a) je založen za účelem spočívajícím v uspokojování potřeb veřejného zájmu a nemá průmyslovou nebo obchodní povahu;

   b) má právní subjektivitu nebo je ze zákona oprávněn jednat jménem jiného subjektu s právní subjektivitou;

   c) je financován převážně státem, regionálními orgány nebo jinými veřejnoprávními subjekty, podléhá řídicímu dohledu těchto orgánů nebo subjektů, nebo je v jeho správním, řídícím nebo dozorčím orgánu 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;

36) „veřejnou sítí elektronických komunikací“ veřejná síť elektronických komunikací ve smyslu čl. 2 bodu 8 směrnice (EU) 2018/1972;

37) „službou elektronických komunikací“ služba elektronických komunikací ve smyslu čl. 2 bodu 4 směrnice (EU) 2018/1972;

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

39) „poskytovatelem řízených služeb“ subjekt, který poskytuje služby související s instalací, správou, provozem nebo údržbou produktů IKT, sítí, infrastruktury, aplikací nebo jakýchkoli jiných sítí a informačních systémů, a to prostřednictvím asistence nebo aktivní správy, které jsou prováděny buď v prostorách zákazníků, nebo na dálku;

40) „poskytovatelem řízených bezpečnostních služeb“ poskytovatel řízených služeb, který provádí činnosti související s řízením kybernetických bezpečnostních rizik nebo poskytuje asistenci pro tyto činnosti;

41) „výzkumnou organizací“ subjekt, jehož hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití výsledků tohoto výzkumu pro komerční účely, který ovšem nezahrnuje vzdělávací instituce.

KAPITOLA II

KOORDINOVANÉ RÁMCE KYBERNETICKÉ BEZPEČNOSTI

Článek 7

Národní strategie kybernetické bezpečnosti

1. Každý členský stát přijme národní strategii kybernetické bezpečnosti, která stanovuje strategické cíle, zdroje potřebné k dosažení těchto cílů a příslušné politiky a regulační opatření s cílem dosáhnout vysoké úrovně kybernetické bezpečnosti a udržovat ji. Národní strategie kybernetické bezpečnosti zahrnuje:

a) cíle a priority strategie kybernetické bezpečnosti členského státu týkající se zejména odvětví uvedených v přílohách I a II;

b) rámec správy k dosažení těchto cílů a priorit uvedených v tomto odstavci písm. a), včetně politik uvedených v odstavci 2;

c) rámec správy, který vyjasňuje úlohy a povinnosti příslušných zúčastněných stran na vnitrostátní úrovni, na němž se zakládá spolupráce a koordinace na vnitrostátní úrovni mezi příslušnými orgány, jednotnými kontaktními místy a týmy CSIRT podle této směrnice, jakož i koordinace a spolupráce mezi těmito subjekty a příslušnými orgány podle odvětvových právních aktů Unie;

d) mechanismus za účelem určení relevantních zařízení a hodnocení rizik v tomto členském státě;

e) určení opatření zajišťujících připravenost, schopnost reakce a obnovu při incidentech, včetně spolupráce veřejného a soukromého sektoru;

f) seznam různých orgánů a zúčastněných stran zapojených do provádění národní strategie kybernetické bezpečnosti;

g) rámec politiky pro lepší koordinaci mezi příslušnými orgány podle této směrnice a příslušnými orgány podle směrnice (EU) 2022/2557 pro účely sdílení informací o rizicích, kybernetických hrozbách a incidentech a o jiných než kybernetických rizicích, hrozbách a incidentech, případně pro výkon úkolů v oblasti dohledu;

h) plán, včetně nezbytných opatření, ke zlepšení obecné úrovně povědomí občanů o kybernetické bezpečnosti.

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

a) zaměřené na kybernetickou bezpečnost v dodavatelském řetězci pro produkty IKT a služby IKT využívané subjekty k poskytování služeb;

b) týkající se zařazení a specifikace požadavků na kybernetickou bezpečnost produktů IKT a služeb IKT při zadávání veřejných zakázek, a to i pokud jde o certifikaci kybernetické bezpečnosti, šifrování a využívání produktů kybernetické bezpečnosti s otevřeným zdrojovým kódem;

c) týkající se řešení zranitelností, včetně prosazování a usnadňování koordinovaného zveřejňovaní zranitelností podle čl. 12 odst. 1;

d) týkající se udržení celkové dostupnosti, integrity a důvěrnosti veřejného jádra otevřeného internetu, případně včetně kybernetické bezpečnosti podmořských komunikačních kabelů;

e) podporující vývoj a integraci příslušných pokročilých technologií zaměřených na zavádění nejmodernějších opatření k řízení kybernetických bezpečnostních rizik;

f) prosazující a rozvíjející vzdělávání a školení v oblasti kybernetické bezpečnosti, dovedností v této oblasti, zvyšování informovanosti a výzkumné a vývojové iniciativy, jakož i pokyny k osvědčeným postupům a kontrolám v oblasti kybernetické hygieny, jež jsou určeny občanům, zúčastněným stranám a subjektům;

g) na podporu akademických a výzkumných institucí při vývoji, zlepšování a prosazování zavádění nástrojů kybernetické bezpečnosti a zabezpečené síťové infrastruktury;

h) zahrnující příslušné postupy a vhodné nástroje pro sdílení informací na podporu dobrovolného sdílení informací týkajících se kybernetické bezpečnosti mezi subjekty v souladu s právem Unie;

i) pro posílení kybernetické odolnosti a základní kybernetické hygieny malých a středních podniků, zejména těch, které nespadají do oblasti působnosti této směrnice, poskytováním snadno dostupných pokynů a pomoci pro jejich specifické potřeby;

j) prosazující aktivní kybernetickou ochranu.

3. Členské státy oznámí své národní strategie kybernetické bezpečnosti Komisi do tří měsíců od jejich přijetí. Členské státy mohou z těchto oznámení vyloučit informace, které se týkají jejich národní bezpečnosti.

4. Členské státy pravidelně a alespoň každých pět let posuzují své národní strategie kybernetické bezpečnosti podle klíčových ukazatelů výkonnosti a v případě potřeby je aktualizují. Při zpracování nebo aktualizaci národní strategie kybernetické bezpečnosti a klíčových ukazatelů výkonnosti pro posouzení strategie s cílem uvést je do souladu s požadavky a povinnostmi stanovenými v této směrnici poskytuje členským státům na jejich žádost součinnost agentura ENISA.

Článek 8

Příslušné orgány a jednotná kontaktní místa

1. Každý členský stát určí nebo zřídí jeden nebo více příslušných orgánů odpovědných za kybernetickou bezpečnost a úkoly dohledu podle kapitoly VII (dále jen „příslušné orgány“).

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

3. Každý členský stát určí nebo zřídí jednotné kontaktní místo. Určí-li nebo zřídí-li členský stát pouze jeden příslušný orgán podle odstavce 1, je tento orgán rovněž jednotným kontaktním místem pro tento členský stát.

4. Každé jednotné kontaktní místo plní styčnou funkci s cílem zajistit přeshraniční spolupráci orgánů svého členského státu s příslušnými orgány jiných členských států a případně s Komisí a agenturou ENISA, a také meziodvětvovou spolupráci s jinými příslušnými orgány ve svém členském státě.

5. Členské státy zajistí, aby jejich příslušné orgány a jednotná kontaktní místa disponovaly odpovídajícími zdroji pro účinné a účelné plnění svěřených úkolů, a tím pro naplnění cílů této směrnice.

6. Každý členský stát Komisi oznámí bez zbytečného odkladu, o jaký příslušný orgán určený podle odstavce 1 a jaké jednotné kontaktní místo určené podle odstavce 3 se jedná, oznámí úkoly těchto orgánů a jakékoli následné změny, které se jich týkají. Každý členský stát zveřejní, o jaký příslušný orgán se jedná. Komise zveřejní seznam jednotných kontaktních míst.

Článek 9

Národní rámce řešení kybernetických krizí

1. Každý členský stát určí nebo zřídí jeden nebo více příslušných orgánů odpovědných za řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí (dále jen „orgány pro řešení kybernetických krizí“). Členské státy zajistí, aby tyto orgány disponovaly odpovídajícími zdroji pro účinné a účelné plnění svěřených úkolů. Členské státy zajistí soudržnost se stávajícími rámci pro obecné vnitrostátní krizové řízení.

2. Pokud členský stát určí nebo zřídí více než jeden příslušný orgán pro řešení kybernetických krizí podle odstavce 1, jasně uvede, který z těchto orgánů bude působit jako koordinátor pro řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí.

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

4. Každý členský stát přijme národní plán reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize, v němž budou stanoveny cíle a ujednání řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí. V uvedeném plánu se stanoví zejména:

a) cíle vnitrostátních opatření a činností v oblasti připravenosti;

b) úkoly a odpovědnost orgánů pro řešení kybernetických krizí;

c) postupy řešení kybernetické krize, včetně jejich začlenění do obecných vnitrostátních rámců pro krizové řízení, a kanály pro výměnu informací;

d) vnitrostátní opatření v oblasti připravenosti včetně cvičení 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.

5. Do tří měsíců od určení nebo zřízení orgánu pro řešení kybernetických krizí podle odstavce 1 oznámí každý členský stát Komisi, o jaký orgán se jedná, a veškeré následné změny, které se ho týkají. Členské státy předloží Komisi a Evropské síti styčných organizací pro řešení kybernetických krizí (dále jen „EU-CyCLONe“) příslušné informace o požadavcích stanovených v odstavci 4, totiž o svých národních plánech reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize, do tří měsíců od přijetí těchto plánů. Členské státy mohou vyloučit informace, pokud je takové vyloučení nezbytné pro jejich národní bezpečnost.

Článek 10

Týmy pro reakce na počítačové bezpečnostní incidenty (týmy CSIRT)

1. Každý členský stát určí nebo zřídí jeden nebo více týmů CSIRT. Týmy CSIRT mohou být určeny nebo zřízeny v rámci příslušného orgánu. Týmy CSIRT splňují požadavky uvedené v čl. 11 odst. 1, pokrývají alespoň odvětví, pododvětví a druhy subjektů uvedené v přílohách I a II a jsou odpovědné za řešení incidentů podle řádně vymezeného postupu.

2. Členské státy zajistí, aby měl každý tým CSIRT odpovídající zdroje pro účinné plnění svých úkolů podle čl. 11 odst. 3.

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 každý tým CSIRT přispíval k zavedení bezpečných nástrojů pro sdílení informací.

4. Týmy CSIRT spolupracují a v příslušných případech si vyměňují příslušné informace podle článku 29 s odvětvovými nebo meziodvětvovými komunitami základních a důležitých subjektů.

5. Týmy CSIRT se účastní vzájemného hodnocení pořádaného v souladu s článkem 19.

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

7. Týmy CSIRT mohou navázat spolupráci s národními týmy pro reakce na počítačové bezpečnostní incidenty ze třetích zemí. Členské státy v rámci takové spolupráce usnadňují účinnou, účelnou a bezpečnou výměnu informací s těmito národními týmy pro reakce na počítačové bezpečnostní incidenty ze třetích zemí, a to za použití příslušných protokolů pro sdílení informací, včetně TLP protokolu. Týmy CSIRT si mohou v souladu s právem Unie v oblasti ochrany údajů vyměňovat relevantní informace s národními týmy pro reakce na počítačové bezpečnostní incidenty ze třetích zemí, včetně osobních údajů.

8. Týmy CSIRT mohou spolupracovat s národními týmy pro reakci na počítačové bezpečnostní incidenty ze třetích zemí nebo s obdobnými subjekty ze třetích zemí, zejména za účelem poskytování pomoci v oblasti kybernetické bezpečnosti.

9. Každý členský stát oznámí Komisi bez zbytečného odkladu identifikační údaje týmu CSIRT podle odstavce 1 tohoto článku a informuje ji o týmu CSIRT, který byl určen koordinátorem podle čl. 12 odst. 1, o úkolech, jimiž byly pověřeny v souvislosti se základními a důležitými subjekty a o jakýchkoli následných změnách, které se jich týkají.

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

Článek 11

Požadavky na týmy CSIRT, jejich technické dovednosti a úkoly

1. Týmy CSIRT splňují tyto požadavky:

a) týmy CSIRT zajišťují vysokou úroveň dostupnosti svých komunikačních kanálů tím, že předchází kritickým místům selhání a disponují několika způsoby, jimiž mohou kontaktovat ostatní a jimiž lze kontaktovat je, a to kdykoli; jednoznačně vymezí 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 zabezpečeném místě;

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

d) týmy CSIRT zajišťují důvěrnost a důvěryhodnost svých činností;

e) týmy CSIRT jsou náležitě personálně obsazeny tak, aby jejich služby byly kdykoli k dispozici, a zajistí odpovídající vyškolení svých pracovníků;

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

Týmy CSIRT se mohou zapojovat do mezinárodních sítí pro spolupráci.

2. Členské státy zajistí, aby jejich týmy CSIRT společně měly technické dovednosti potřebné k plnění úkolů uvedených v odstavci 3. Členské státy zajistí, aby byly jejich týmům CSIRT přiděleny dostatečné zdroje s cílem zajistit odpovídající personální obsazení, které jim umožní rozvoj jejich technických kapacit.

3. Týmy CSIRT mají tyto úkoly:

a) monitorovat a analyzovat kybernetické hrozby, zranitelnosti a incidenty na vnitrostátní úrovni a na žádost poskytovat pomoc dotčeným základním a důležitým subjektům s monitorováním jejich sítí a informačních systémů v reálném čase nebo v téměř reálném čase;

b) poskytovat včasná varování a upozornění, oznamovat a šířit informace o kybernetických hrozbách, zranitelnostech a incidentech určené dotčeným základním a důležitým subjektům, příslušným orgánům a dalším příslušným zúčastněným stranám, pokud možno v téměř reálném čase;

c) reagovat na incidenty a případně poskytovat pomoc dotčeným základním a důležitým subjektům;

d) shromažďovat a analyzovat forenzní data a poskytovat dynamické analýzy rizik a incidentů a přehled o situaci v oblasti kybernetické bezpečnosti;

e) provádět proaktivní skenování sítí a informačních systémů základního nebo důležitého subjektu, který o to požádal, s cílem odhalit zranitelnosti s potenciálním významným dopadem;

f) podílet se na síti CSIRT a poskytovat v rámci svých kapacit a pravomocí vzájemnou pomoc dalším členům sítě CSIRT na jejich žádost;

g) v příslušných případech působit jakožto koordinátor pro účely koordinovaného zveřejňování zranitelností podle čl. 12 odst. 1;

h) podporovat zavádění bezpečných nástrojů pro sdílení informací podle čl. 10 odst. 3.

Týmy CSIRT mohou provádět proaktivní a neintruzivní skenování veřejně přístupných sítí a informačních systémů základních a důležitých subjektů. Toto skenování se provádí s cílem odhalit zranitelné nebo nezabezpečeně konfigurované sítě a informační systémy a informovat dotčené subjekty. Toto skenování nesmí mít negativní dopad na fungování služeb subjektů.

Při plnění úkolů uvedených v prvním pododstavci mohou týmy CSIRT některé úkoly upřednostnit na základě přístupu založeného na posouzení rizik.

4. Týmy CSIRT navážou spolupráci s příslušnými zúčastněnými stranami v soukromém sektoru za účelem plnění cílů této směrnice.

5. V zájmu usnadnění spolupráce uvedené v odstavci 4 prosazují týmy CSIRT přijetí a používání společných či standardních postupů, klasifikačních schémat a taxonomií v oblasti:

a) postupů řešení incidentů;

b) krizového řízení a

c) koordinovaného zveřejňování zranitelností podle čl. 12 odst. 1.

Článek 12

Koordinované zveřejňování zranitelností a Evropská databáze zranitelností

1. Každý členský stát určí jeden ze svých týmů CSIRT jakožto koordinátora za účelem koordinovaného zveřejňování zranitelností. Tým CSIRT určený jakožto koordinátor vystupuje jako důvěryhodný zprostředkovatel, který v případě potřeby a na žádost kterékoli strany usnadňuje interakci mezi fyzickou nebo právnickou osobou oznamující zranitelnost a výrobcem nebo poskytovatelem případných zranitelných produktů IKT nebo služeb IKT. Mezi úkoly týmu CSIRT, který byl určen jakožto koordinátor, náleží:

a) identifikace a kontaktování dotčených subjektů;

b) pomoc fyzickým nebo právnickým osobám oznamujícím zranitelnost; a

c) jednání o lhůtách pro zveřejnění a řešení zranitelností, které mají dopad na více subjektů.

Členské státy zajistí, aby fyzické nebo právnické osoby mohly týmu CSIRT, který byl určen jakožto koordinátor, oznámit zranitelnost na požádání anonymně. Tým CSIRT, který byl určen jakožto koordinátor, zajistí, aby byla s ohledem na oznámenou zranitelnost provedena s náležitou péčí následná opatření, a zajistí anonymitu fyzické nebo právnické osoby oznamující zranitelnost. Pokud by oznámená zranitelnost mohla mít významný dopad na subjekty ve více než jednom členském státě, spolupracují týmy CSIRT, které byly určeny jakožto koordinátoři, z každého dotčeného členského státu v případě potřeby s ostatními týmy CSIRT, které byly určeny jakožto koordinátoři, v rámci sítě CSIRT.

2. Agentura ENISA po konzultaci se skupinou pro spolupráci vytvoří a spravuje Evropskou databázi zranitelností. Za tímto účelem agentura ENISA zřídí a spravuje informační systémy, politiky a postupy a přijme technická a organizační opatření nezbytná k zajištění bezpečnosti a integrity Evropské databáze zranitelností s cílem zejména umožnit subjektům bez ohledu na to, zda se na ně vztahuje oblast působnosti této směrnice, a jejich dodavatelům sítí a informačních systémů dobrovolně oznamovat a registrovat veřejně známé zranitelnosti v produktech IKT nebo službách IKT. Přístup k informacím o zranitelnostech uvedeným v Evropské databázi zranitelností je poskytnut všem zúčastněným stranám. V této databázi jsou uvedeny:

a) informace popisující zranitelnost;

b) zasažené produkty IKT nebo služby IKT, závažnost této zranitelnosti z hlediska okolností, za nichž může být využita;

c) dostupnost příslušných oprav, a pokud opravy nejsou dostupné, pokyny poskytnuté příslušnými orgány nebo týmy CSIRT a určené uživatelům zranitelných produktů IKT a služeb IKT ohledně toho, jak mohou být rizika vyplývající ze zveřejněných zranitelností zmírněna.

Článek 13

Spolupráce na vnitrostátní úrovni

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

2. Členské státy zajistí, aby jejich týmy CSIRT, nebo ve vhodných případech jejich příslušné orgány, obdržely oznámení o významných incidentech podle článku 23 a o incidentech, kybernetických hrozbách a významných událostech podle článku 30.

3. Členské státy zajistí, aby jejich týmy CSIRT, nebo ve vhodných případech jejich příslušné orgány, informovaly jejich jednotná kontaktní místa o oznámeních o incidentech, kybernetických hrozbách a významných událostech, která byla podána podle této směrnice.

4. S cílem zajistit účinné plnění úkolů a povinností příslušných orgánů, jednotných kontaktních míst a týmů CSIRT zajistí členské státy v co největší možné míře vhodnou spolupráci mezi těmito subjekty a donucovacími orgány, orgány pro ochranu osobních údajů, vnitrostátními orgány podle nařízení (ES) č. 300/2008 a (EU) 2018/1139, orgány dohledu podle nařízení (EU) č. 910/2014, příslušnými orgány podle nařízení (EU) 2022/2554, vnitrostátními regulačními orgány podle směrnice (EU) 2018/1972, příslušnými orgány podle směrnice (EU) 2022/2557, a příslušnými orgány podle dalších odvětvových právních aktů Unie v daném členském státě.

5. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice a jejich příslušné orgány podle směrnice (EU) 2022/2557spolupracovaly a pravidelně si vyměňovaly informace o určení kritických subjektů, o rizicích, kybernetických hrozbách a incidentech, jakož i o jiných než kybernetických rizicích, hrozbách a incidentech postihujících základní subjekty určené jakožto kritické podle směrnice (EU) 2022/2557, jakož i o opatřeních přijatých v reakci na tato rizika, hrozby a incidenty. Členské státy rovněž zajistí, aby si jejich příslušné orgány podle této směrnice a jejich příslušné orgány podle nařízení (EU) č. 910/2014, nařízení (EU) 2022/2554a směrnice (EU) 2018/1972 pravidelně vyměňovaly relevantní informace, včetně informací o příslušných incidentech a kybernetických hrozbách.

6. Členské státy zjednoduší poskytování informací technickými prostředky pro oznamování podle článků 23 a 30.

KAPITOLA III

SPOLUPRÁCE NA UNIJNÍ A MEZINÁRODNÍ ÚROVNI

Článek 14

Skupina pro spolupráci

1. S cílem podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy a posilovat důvěru se zřizuje skupina pro spolupráci.

2. Skupina pro spolupráci vykonává své úkoly na základě dvouletých pracovních programů, jak je uvedeno v odstavci 7.

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 v souladu s čl. 47 odst. 1 nařízení (EU) 2022/2554účastnit evropské orgány dohledu a příslušné orgány podle uvedeného nařízení.

V příslušném případě může skupina pro spolupráci přizvat ke spolupráci Evropský parlament a zástupce příslušných zúčastněných stran.

Sekretariát zajišťuje Komise.

4. Skupina pro spolupráci má tyto úkoly:

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

b) poskytovat pokyny příslušným orgánům v souvislosti s vypracováváním a prováděním politik v oblasti koordinovaného zveřejňování zranitelností, jak je uvedeno v čl. 7 odst. 2 písm. c);

c) vyměňovat si osvědčené postupy a informace související s uplatňováním této směrnice, včetně informací souvisejících s kybernetickými hrozbami, incidenty, zranitelnostmi, významnými událostmi, iniciativami zaměřenými na zvyšování povědomí, školením, cvičeními a dovednostmi, budováním kapacit, normami a technickými specifikacemi, jakož i s určováním základních a důležitých subjektů podle čl. 2 odst. 2 písm. b) až e);

d) vyměňovat si doporučení a spolupracovat s Komisí na nových politických iniciativách v oblasti kybernetické bezpečnosti a na celkové soudržnosti odvětvových požadavků na kybernetickou bezpečnost;

e) vyměňovat si rady a spolupracovat s Komisí na návrzích aktů v přenesené pravomoci či prováděcích aktů přijímaných podle této směrnice;

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

g) vyměňovat si názory na provádění odvětvových právních aktů Unie, které obsahují ustanovení o kybernetické bezpečnosti;

h) případně projednávat zprávy o vzájemném hodnocení uvedené v čl. 19 odst. 9 a vypracovávat závěry a doporučení;

i) provádět koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců v souladu s čl. 22 odst. 1;

j) projednávat případy vzájemné pomoci, včetně zkušeností a výsledků přeshraničních společných činností v oblasti dohledu uvedených v článku 37;

k) na žádost jednoho nebo více dotčených členských států projednávat konkrétní žádosti o vzájemnou pomoc podle článku 37;

l) poskytovat strategické pokyny síti CSIRT a EU-CyCLONe ke konkrétním nově vznikajícím problémům;

m) vyměňovat si názory na následná opatření po rozsáhlých kybernetických bezpečnostních incidentech a krizích na základě zkušeností získaných v rámci sítě CSIRT a EU-CyCLONe;

n) přispívat ke schopnostem v oblasti kybernetické bezpečnosti v celé Unii usnadňováním výměny úředníků členských států prostřednictvím programu budování kapacit zahrnujícího pracovníky z příslušných orgánů nebo týmů CSIRT;

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

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

q) stanovit metodiku a organizační aspekty vzájemných hodnocení uvedených v čl. 19 odst. 1 a vypracovat metodiku sebehodnocení pro členské státy v souladu s čl. 19 odst. 5 za pomoci Komise a agentury ENISA a ve spolupráci s Komisí a agenturou ENISA vypracovat kodexy chování, na nichž budou založeny pracovní metody určených odborníků na kybernetickou bezpečnost v souladu s čl. 19 odst. 6;

r) připravovat zprávy o zkušenostech získaných ze strategické úrovně a ze vzájemných hodnocení pro účely přezkumu uvedeného v článku 40;

s) pravidelně projednávat a provádět hodnocení aktuálního stavu kybernetických hrozeb nebo incidentů, například v souvislosti s ransomware.

Skupina pro spolupráci předkládá zprávy podle prvního pododstavce písm. r) Komisi, Evropskému parlamentu a Radě.

5. Členské státy zajistí, aby jejich zástupci ve skupině pro spolupráci účinně, účelně a spolehlivě spolupracovali.

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

7. Do 1. února 2024 a poté každé dva roky vypracuje skupina pro spolupráci pracovní program týkající se činností, jež mají být realizovány za účelem plnění jejích cílů a úkolů.

8. Komise může přijmout prováděcí akty, kterými stanoví procesní pravidla nezbytná pro fungování skupiny pro spolupráci.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Komise si v souladu s odst. 4 písm. e) poskytuje se skupinou pro spolupráci vzájemné poradenství a spolupracuje s ní, pokud jde o návrhy prováděcích aktů uvedených v prvním pododstavci tohoto odstavce.

9. Skupina pro spolupráci se schází pravidelně, a vždy alespoň jednou ročně, se skupinou pro odolnost kritických subjektů zřízenou podle směrnice (EU) 2022/2557za účelem podpory a usnadnění strategické spolupráce a výměny informací.

Článek 15

Síť CSIRT

1. Zřizuje se síť národních 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 určených nebo zřízených podle článku 10 a zástupci týmu pro reakci na počítačové hrozby pro orgány, instituce a jiné subjekty Unie (CERT-EU). Komise se účastní sítě CSIRT jako pozorovatel. Agentura ENISA zajišťuje sekretariát a aktivně podporuje spolupráci mezi týmy CSIRT.

3. Síť CSIRT má tyto úkoly:

a) vyměňovat si informace o schopnostech týmů CSIRT;

b) usnadňovat sdílení, přenos a výměnu technologií a příslušných opatření, politik, nástrojů, procesů, osvědčených postupů a rámců mezi týmy CSIRT;

c) vyměňovat si příslušné informace o incidentech, významných událostech, kybernetických hrozbách, rizicích a zranitelnostech;

d) vyměňovat si informace, pokud jde o publikace a doporučení v oblasti kybernetické bezpečnosti;

e) zajišťovat interoperabilitu, pokud jde o specifikace a protokoly týkající se sdílení informací;

f) na žádost člena sítě CSIRT potenciálně zasaženého incidentem si vyměňovat a projednávat informace o tomto incidentu a souvisejících kybernetických hrozbách, rizicích a zranitelnostech;

g) na žádost člena sítě CSIRT projednat a pokud možno realizovat koordinovanou reakci na incident, který byl zjištěn v oblasti spadající do pravomoci tohoto členského státu;

h) poskytovat členským státům pomoc při řešení přeshraničních incidentů podle této směrnice;

i) spolupracovat a poskytovat pomoc týmům CSIRT, které byly určeny jakožto koordinátoři, podle čl. 12 odst. 1 a vyměňovat si s nimi osvědčené postupy v souvislosti s řízením koordinovaného zveřejňování zranitelností, které by mohly mít významný dopad na subjekty ve více než jednom členském státě;

j) projednávat a vymezovat 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 ujednáním koordinace při reakci na přeshraniční rizika a incidenty;

   v) příspěvku k národnímu plánu reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize uvedenému v čl. 9 odst. 4 na žádost členského státu;

k) informovat skupinu pro spolupráci o svých činnostech a o dalších formách operativní spolupráce projednávaných podle písmene j) a v případě potřeby žádat v tomto ohledu odpovídající pokyny;

l) vyhodnocovat cvičení v oblasti kybernetické bezpečnosti, včetně cvičení pořádaných agenturou ENISA;

m) na žádost jednotlivých týmů CSIRT jednat o jejich schopnostech a připravenosti;

n) spolupracovat a vyměňovat si informace s regionálními bezpečnostními operačními středisky a bezpečnostními operačními středisky na úrovni Unie za účelem zlepšení společného situačního povědomí u incidentů a kybernetických hrozeb v celé Unii;

o) případně projednávat zprávy o vzájemném hodnocení uvedené v čl. 19 odst. 9;

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

4. Síť CSIRT do 17. ledna 2025 a poté každé dva roky pro účely přezkumu uvedeného v článku 40 posoudí pokrok dosažený s ohledem na operativní spolupráci a přijme zprávu. Ve zprávě se zejména uvedou závěry a doporučení vycházející z výsledků vzájemného hodnocení uvedeného v článku 19, provedeného ve vztahu k národním týmům CSIRT. Tato zpráva bude předložena skupině pro spolupráci.

5. Síť CSIRT přijme svůj jednací řád.

6. Síť CSIRT a síť EU-CyCLONe sjednají procesní pravidla, podle kterých spolupracují.

Článek 16

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

1. Za účelem podpory koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni a pro zajištění pravidelné výměny relevantních informací mezi členskými státy a orgány, institucemi a jinými subjekty Unie se zřizuje síť EU-CyCLONe.

2. Síť EU-CyCLONe je tvořena zástupci orgánů členských států pro řešení kybernetických krizí a v případech, kdy potenciální nebo probíhající rozsáhlý kybernetický bezpečnostní incident má nebo pravděpodobně bude mít významný dopad na služby a činnosti spadající do oblasti působnosti této směrnice, jsou jejími členy také zástupci Komise. V jiných případech se činností sítě EU-CyCLONe Komise účastní jako pozorovatel.

Agentura ENISA zajišťuje sekretariát pro síť EU-CyCLONe, podporuje bezpečnou výměnu informací a poskytuje nezbytné nástroje na podporu spolupráce mezi členskými státy zajištěním bezpečné výměny informací.

Tam, kde je to vhodné, může síť EU-CyCLONe přizvat zástupce příslušných zúčastněných stran, aby se podíleli na činnosti jako pozorovatelé.

3. Síť EU-CyCLONe má tyto úkoly:

a) zvýšit úroveň připravenosti pro řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí;

b) rozvíjet situační povědomí o rozsáhlých kybernetických bezpečnostních incidentech a krizích;

c) posuzovat důsledky a dopad příslušných rozsáhlých kybernetických bezpečnostních incidentů a krizí a navrhovat případná opatření k jejich zmírnění;

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

e) na žádost dotčeného členského státu projednávat národní plány reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize uvedené v čl. 9 odst. 4.

4. Síť EU-CyCLONe přijme svůj organizační řád.

5. Síť EU-CyCLONe pravidelně podává skupině pro spolupráci zprávy o řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí a o trendech, se zvláštním zaměřením na jejich dopad na základní a důležité subjekty.

6. Síť EU-CyCLONe spolupracuje se sítí CSIRT na základě sjednaných procesních pravidel podle čl. 15 odst. 6.

7. Síť EU-CyCLONe do 17. července 2024 a poté každých 18 měsíců předloží Evropskému parlamentu a Radě zprávu, v níž posoudí svou činnost.

Článek 17

Mezinárodní spolupráce

Unie může ve vhodných případech v souladu s článkem 218 Smlouvy o fungování EU uzavírat mezinárodní dohody se třetími zeměmi nebo mezinárodními organizacemi, které umožní a upraví jejich účast na určitých činnostech skupiny pro spolupráci, sítě CSIRT a sítě EU-CyCLONe. Tyto dohody musí být v souladu s právem Unie v oblasti ochrany údajů.

Článek 18

Zpráva o stavu kybernetické bezpečnosti v Unii

1. Agentura ENISA ve spolupráci s Komisí a skupinou pro spolupráci přijme jednou za dva roky zprávu o stavu kybernetické bezpečnosti v Unii a tuto zprávu předloží a představí Evropskému parlamentu. Zpráva musí být dostupná mimo jiné ve strojově čitelném formátu a zahrnuje:

a) posouzení kybernetických bezpečnostních rizik na úrovni Unie se zohledněním oblasti kybernetických hrozeb;

b) posouzení vývoje kapacit v oblasti kybernetické bezpečnosti ve veřejném i soukromém sektoru v celé Unii;

c) posouzení obecné úrovně povědomí o kybernetické bezpečnosti a kybernetické hygieny mezi občany a subjekty, včetně malých a středních podniků;

d) agregované posouzení výsledků vzájemných hodnocení uvedených v článku 19;

e) agregované posouzení úrovně vyspělosti kapacit a zdrojů v oblasti kybernetické bezpečnosti v celé Unii, a to i na úrovni odvětví, a toho, do jaké míry jsou národní strategie kybernetické bezpečnosti členských států sladěny.

2. Zpráva obsahuje konkrétní doporučení k této oblasti politiky zaměřená na řešení nedostatků a zvýšení úrovně kybernetické bezpečnosti v celé Unii a shrne zjištění za dané období z technických situačních zpráv EU v oblasti kybernetické bezpečnosti týkající se incidentů a kybernetických hrozeb vypracovaných agenturou ENISA podle čl. 7 odst. 6 nařízení (EU) 2019/881.

3. Agentura ENISA ve spolupráci s Komisí, skupinou pro spolupráci a sítí CSIRT vypracuje metodiku pro agregované posouzení uvedené v odst. 1 písm. e) a zahrne do ní příslušné proměnné, jako jsou kvantitativní a kvalitativní ukazatele.

Článek 19

Vzájemná hodnocení

1. Skupina pro spolupráci do 17. ledna 2025 s pomocí Komise a agentury ENISA a případně sítě CSIRT vypracuje metodiku a organizační aspekty vzájemných hodnocení s cílem poučit se ze společných zkušeností, posílit vzájemnou důvěru, dosáhnout společné vysoké úrovně kybernetické bezpečnosti a posílit schopnosti a politické strategie členských států v oblasti kybernetické bezpečnosti, které jsou nezbytné pro provádění této směrnice. Účast na vzájemných hodnoceních je dobrovolná. Vzájemná hodnocení provádějí odborníci na kybernetickou bezpečnost. Odborníky na kybernetickou bezpečnost určí nejméně dva členské státy, které nejsou posuzovanými členskými státy.

Vzájemná hodnocení musí zahrnovat alespoň jeden z následujících aspektů:

a) úroveň provádění opatření k řízení kybernetických bezpečnostních rizik a plnění oznamovacích povinností stanovených v článcích 21 a 23;

b) úroveň kapacit, včetně dostupných finančních, technických a lidských zdrojů, a účinnost plnění úkolů příslušných orgánů;

c) provozní kapacity týmů CSIRT;

d) úroveň uskutečňování vzájemné pomoci podle článku 37;

e) úroveň provádění ujednání o sdílení informací o kybernetické bezpečnosti podle článku 29;

f) specifické otázky přeshraniční nebo meziodvětvové povahy.

2. Metodika uvedená v odstavci 1 zahrnuje objektivní, nediskriminační, korektní a transparentní kritéria, na jejichž základě členské státy určí odborníky na kybernetickou bezpečnost způsobilé provádět vzájemná hodnocení. Komise a agentura ENISA se budou vzájemných hodnocení účastnit jako pozorovatelé.

3. Pro účely vzájemného hodnocení mohou členské státy určit konkrétní otázky, jak je uvedeno v odst. 1 písm. f).

4. Před zahájením vzájemného hodnocení podle odstavce 1 oznámí členské státy zúčastněným členským státům jeho rozsah, včetně konkrétních otázek, jež byly ve smyslu odstavce 3 určeny.

5. Před zahájením vzájemného hodnocení mohou členské státy provést sebehodnocení posuzovaných aspektů, které poté poskytnou určeným odborníkům na kybernetickou bezpečnost. Metodiku sebehodnocení členských států stanoví skupina pro spolupráci za pomoci Komise a agentury ENISA.

6. Vzájemná hodnocení zahrnují osobní nebo virtuální návštěvy na místě i externí výměny informací. S ohledem na zásadu dobré spolupráce poskytnou členské státy podléhající vzájemnému hodnocení určeným odborníkům na kybernetickou bezpečnost informace potřebné k posouzení, aniž by tím bylo dotčeno právo členských států nebo Unie týkající se ochrany důvěrných či utajovaných informací nebo plnění základních funkcí státu, jako je národní bezpečnost. Skupina pro spolupráci ve spolupráci s Komisí a agenturou ENISA vypracuje vhodné kodexy chování, které budou tvořit základ pracovních metod určených odborníků na kybernetickou bezpečnost. Veškeré informace získané v rámci vzájemného hodnocení lze použít pouze pro tento účel. Odborníci na kybernetickou bezpečnost účastnící se vzájemného hodnocení nesmí sdělit žádné citlivé nebo důvěrné informace získané v průběhu tohoto vzájemného hodnocení žádným třetím stranám.

7. Tytéž aspekty, které již byly v členském státě předmětem vzájemného hodnocení, nepodléhají v tomto členském státě v průběhu dvou let po ukončení vzájemného hodnocení dalšímu posuzování, pokud o to členský stát nepožádá nebo pokud to není výsledkem dohody na základě návrhu skupiny pro spolupráci.

8. Členské státy zajistí, aby byly ostatní členské státy, skupina pro spolupráci, Komise a agentura ENISA před zahájením vzájemného hodnocení informovány o jakémkoli riziku střetu zájmů týkajícím se určených odborníků na kybernetickou bezpečnost. Členský stát podléhající vzájemnému hodnocení může vznést námitku vůči určení konkrétních odborníků na kybernetickou bezpečnost, a to na základě řádného odůvodnění, které sdělí členskému státu, který tyto odborníky určil.

9. Odborníci na kybernetickou bezpečnost účastnící se vzájemných hodnocení vypracují návrhy zpráv o zjištěních a závěrech těchto vzájemných hodnocení. Členské státy podléhající vzájemnému hodnocení mohou předložit připomínky k návrhům zpráv, které se jich týkají, a tyto připomínky se poté ke zprávám připojí. Zprávy obsahují doporučení, jejichž cílem je dosáhnout zlepšení v aspektech, jichž se vzájemné hodnocení týká. Zprávy se předloží skupině pro spolupráci a v příslušném případě síti CSIRT. Členský stát podléhající vzájemnému hodnocení se může rozhodnout svou zprávu nebo její upravenou verzi zveřejnit.

KAPITOLA IV

OPATŘENÍ K ŘÍZENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH RIZIK A OZNAMOVACÍ POVINNOSTI

Článek 20

Řízení

1. Členské státy zajistí, aby řídící orgány základních a důležitých subjektů schválily opatření k řízení kybernetických bezpečnostních rizik přijatá těmito subjekty za účelem dosažení souladu s článkem 21, dohlížely nad jeho uplatňováním a mohly nést odpovědnost, poruší-li subjekty uvedený článek.

Uplatňováním tohoto odstavce není dotčeno vnitrostátní právo, pokud jde o pravidla odpovědnosti vztahující se na veřejné orgány, odpovědnost úředníků veřejné správy a odpovědnost volených veřejných činitelů nebo jmenovaných úředníků.

2. Členské státy zajistí, aby členové řídících orgánů základních a důležitých subjektů museli absolvovat školení, a vybízí základní a důležité subjekty, aby pravidelně nabízely podobné školení svým zaměstnancům, aby tak získali dostatečné znalosti a dovednosti, aby mohli identifikovat rizika a posoudit postupy řízení kybernetických bezpečnostních rizik a jejich dopad na služby poskytované subjektem.

Článek 21

Opatření k řízení kybernetických bezpečnostních rizik

1. Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická, provozní a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto subjekty používají pro svůj provoz nebo poskytování svých služeb, a k předcházení incidentům nebo minimalizaci jejich dopadů na příjemce jejich služeb a na další služby.

S ohledem na nejnovější technický vývoj a případně na příslušné evropské a mezinárodní normy a na náklady na provádění musí opatření uvedená v prvním pododstavci zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. Při posuzování přiměřenosti těchto opatření je třeba náležitě zohlednit míru vystavení subjektu rizikům, jeho velikost a pravděpodobnost výskytu incidentů, jejich závažnost a společenský a ekonomický dopad.

2. Opatření uvedená v odstavci 1 jsou založena na přístupu zohledňujícím všechny druhy rizik, jehož cílem je chránit sítě a informační systémy a fyzické prostředí těchto systémů před incidenty, a zahrnují alespoň:

a) politiku analýzy rizik a politiku bezpečnosti informačních systémů;

b) řešení incidentů;

c) řízení kontinuity provozu, jako je například správa zálohování a obnova provozu po havárii, a krizové řízení;

d) bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;

e) zabezpečení pořizování, vývoje a údržby sítí a informačních systémů, včetně zveřejňování zranitelností a jejich řešení;

f) politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik;

g) základní postupy kybernetické hygieny a školení v oblasti kybernetické bezpečnosti;

h) politiky a postupy týkající se používání kryptografie a případně šifrování;

i) bezpečnost lidských zdrojů, postupy kontroly přístupu a správa aktiv;

j) v příslušných případech používání vícefaktorových autentizačních řešení nebo trvalých autentizačních řešení, zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů nouzové komunikace v rámci subjektu.

3. Členské státy zajistí, aby při zvažování vhodných opatření uvedených v odst. 2 písm. d) tohoto článku subjekty zohlednily zranitelnosti specifické pro každého přímého dodavatele a poskytovatele služeb a celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje. Členské státy rovněž zajistí, aby při zvažování vhodných opatření podle uvedeného písmene subjekty měly povinnost zohlednit výsledky koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců, které bylo provedeno v souladu s čl. 22 odst. 1.

4. Členské státy zajistí, aby v případě, že subjekt zjistí, že neodpovídá požadavkům stanoveným v odstavci 2, přijal bez zbytečného odkladu všechna nezbytná, vhodná a přiměřená nápravná opatření.

5. Do 17. října 2024 přijme Komise prováděcí akty, kterými stanoví technické a metodické požadavky opatření uvedených v odstavci 2, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru.

Komise může přijmout prováděcí akty, kterými stanoví technické, metodické a případně odvětvové požadavky, pokud jde o opatření uvedená v odstavci 2, přičemž tyto požadavky se týkají jiných základních a důležitých subjektů než těch, které jsou uvedeny v prvním pododstavci tohoto odstavce.

Při přípravě prováděcích aktů uvedených v prvním a druhém pododstavci tohoto odstavce se Komise pokud možno řídí evropskými a mezinárodními normami, jakož i příslušnými technickými specifikacemi. Komise si v souladu s čl. 14 odst. 4 písm. e) poskytuje se skupinou pro spolupráci a agenturou ENISA vzájemné poradenství a spolupracuje s nimi, pokud jde o návrhy prováděcích aktů.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 22

Koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni

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

2. Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA a případně s příslušnými zúčastněnými stranami určí specifické kritické služby IKT, systémy IKT nebo produkty IKT, jež mohou být předmětem koordinovaného posouzení bezpečnostních rizik podle odstavce 1.

Článek 23

Oznamovací povinnosti

1. Členské státy zajistí, aby základní a důležité subjekty oznamovaly bez zbytečného odkladu svému týmu CSIRT nebo případně svému příslušnému orgánu v souladu s odstavcem 4 každý incident, který má významný dopad na poskytování jejich služeb, jak je uvedeno v odstavci 3 (významný incident). V příslušných případech dotčené subjekty oznámí bez zbytečného odkladu příjemci svých služeb významné incidenty, které by mohly negativně ovlivnit poskytování těchto služeb. Každý členský stát zajistí, aby tyto subjekty oznamovaly mimo jiné všechny informace, které týmu CSIRT nebo případně příslušnému orgánu umožní posoudit případný přeshraniční dopad daného incidentu. Pouhé oznámení nepředstavuje pro oznamující subjekt vyšší míru právní odpovědnosti.

Pokud dotčené subjekty oznámí příslušnému orgánu významný incident podle prvního pododstavce, členský stát zajistí, aby příslušný orgán toto oznámení po jeho obdržení předal týmu CSIRT.

V případě přeshraničního nebo meziodvětvového významného incidentu členské státy zajistí, aby jejich jednotná kontaktní místa včas obdržela příslušné informace v souladu s odstavcem 4.

2. Členské státy příslušně zajistí, aby základní a důležité subjekty informovaly bez zbytečného odkladu příjemce svých služeb, kteří mohou být ovlivněni významnou kybernetickou hrozbou, o všech krocích nebo nápravných opatřeních, jež příjemci mohou v reakci na danou hrozbu učinit. Subjekty příjemce příslušně uvědomí také o významné kybernetické hrozbě samotné.

3. Incident se považuje za významný, jestliže:

a) dotčenému subjektu způsobil nebo může způsobit závažné provozní narušení služeb nebo finanční ztráty;

b) způsobil nebo může způsobit jiným fyzickým nebo právnickým osobám značnou hmotnou nebo nehmotnou újmu.

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

a) bez zbytečného odkladu, nejpozději však do 24 hodin po zjištění významného incidentu, včasné varování, v němž případně uvedou, zda se domnívají, že byl významný incident způsoben nezákonným nebo svévolným zásahem nebo že by mohl mít přeshraniční dopad;

b) bez zbytečného odkladu, nejpozději však do 72 hodin po zjištění významného incidentu, oznámení incidentu, v němž případně aktualizují informace uvedené v písmenu a), předloží prvotní posouzení významného incidentu včetně jeho závažnosti a dopadu a – pokud jsou k dispozici – indikátory kompromitace;

c) na žádost týmu CSIRT nebo případně příslušného orgánu průběžnou zprávu o podstatných aktualizacích stavu;

d) nejpozději do jednoho měsíce od předložení oznámení incidentu podle písmene b) závěrečnou zprávu zahrnující:

   i) podrobný popis incidentu včetně jeho závažnosti a dopadu;

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

   iii) učiněná a probíhající opatření ke zmírnění následků;

   iv) případně přeshraniční dopad incidentu;

e) v případě, že v okamžiku, kdy by měla být předložena závěrečná zpráva podle písmene d), incident stále trvá, členské státy zajistí, aby dotčené subjekty v uvedené lhůtě předložily zprávu o pokroku a následně, nejpozději jeden měsíc po tom, co incident vyřešily, závěrečnou zprávu.

Odchylně od prvního pododstavce písm. b) poskytovatel služby vytvářející důvěru oznámí týmu CSIRT nebo případně příslušnému orgánu významné incidenty, které mají dopad na jím poskytované služby, a to bez zbytečného odkladu, nejpozději však do 24 hodin od okamžiku, kdy se o významném incidentu dozvěděl.

5. Tým CSIRT nebo příslušný orgán poskytnou bez zbytečného odkladu a pokud možno do 24 hodin po obdržení včasného varování podle odst. 4 písm. a) oznamujícímu subjektu své vyjádření, včetně prvotních vyjádření k významnému incidentu, a na žádost subjektu pomoc či podporu při zavádění možných opatření ke zmírnění dopadů. Pokud tým CSIRT není prvotním příjemcem oznámení podle odstavce 1, pomoc či podporu poskytne 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 významný incident povahu trestného činu, tým CSIRT nebo příslušný orgán poskytne také pokyny, jak významný incident oznámit orgánům činným v trestním řízení.

6. Tam, kde je to vhodné, a zejména pokud se významný incident týká dvou nebo více členských států, informuje tým CSIRT, příslušný orgán nebo jednotné kontaktní místo o významném incidentu bez zbytečného odkladu ostatní dotčené členské státy a agenturu ENISA. Takové informace zahrnují druh informací obdržených podle odstavce 4. Tým CSIRT, příslušný orgán nebo jednotné kontaktní místo přitom v souladu s unijním vnitrostátním právem zachovávají bezpečnost a obchodní zájmy subjektu, jakož i důvěrnost poskytnutých informací.

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

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

9. Jednotné kontaktní místo předkládá každé tři měsíce agentuře ENISA souhrnnou zprávu zahrnující anonymizovaná a agregovaná data o významných incidentech, incidentech, kybernetických hrozbách a významných událostech oznámených podle odstavce 1 tohoto článku a podle článku 30. V zájmu větší srovnatelnosti poskytovaných informací může agentura ENISA přijmout technické pokyny k parametrům informací, jež mají být v souhrnné zprávě uvedeny. Agentura ENISA informuje skupinu pro spolupráci a síť CSIRT o svých zjištěních v souvislosti s přijatými oznámeními každých šest měsíců.

10. Týmy CSIRT nebo případně příslušné orgány poskytnou příslušným orgánům podle směrnice (EU) 2022/2557 informace o významných incidentech, incidentech, kybernetických hrozbách a významných událostech oznámených podle odstavce 1 tohoto článku a podle článku 30 subjekty určenými jakožto kritické subjekty podle směrnice (EU) 2022/2557.

11. Komise může přijmout prováděcí akty dále upřesňující druh informací, formát a postup oznámení předkládaných podle odstavce 1 tohoto článku a podle článku 30 a informací poskytnutých podle odstavce 2 tohoto článku.

Do 17. října 2024 přijme Komise, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, jakož i poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí, prováděcí akty dále upřesňující případy, kdy se incident považuje za významný, jak je uvedeno v odstavci 3. Komise může takové prováděcí akty přijmout také ve vztahu k dalším základním a důležitým subjektům.

Komise si v souladu s čl. 14 odst. 4 písm. e) poskytuje se skupinou pro spolupráci vzájemné poradenství a spolupracuje s ní, pokud jde o návrhy prováděcích aktů uvedených v prvním a druhém pododstavci tohoto odstavce.

Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 39 odst. 2.

Článek 24

Použití evropských systémů certifikace kybernetické bezpečnosti

1. K prokázání splnění zvláštních požadavků článku 21 mohou členské státy požadovat, aby základní a důležité subjekty používaly určité produkty IKT, služby IKT a procesy IKT vypracované základním nebo důležitým subjektem nebo získané od třetích stran a certifikované podle evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881. Členské státy kromě toho podporují základní a důležité subjekty, aby využívaly kvalifikované služby vytvářející důvěru.

2. Komisi je v souladu s článkem 38 za účelem doplnění této směrnice svěřena pravomoc přijímat akty v přenesené pravomoci, upřesňující, které kategorie základních a důležitých subjektů budou povinny používat určité certifikované produkty IKT, služby IKT nebo procesy IKT nebo si obstarat certifikát podle evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 49 nařízení (EU) 2019/881. Tyto akty v přenesené pravomoci se přijímají, pokud se zjistí nedostatečná úroveň kybernetické bezpečnosti, a je v nich stanoveno prováděcí období.

Před přijetím těchto aktů v přenesené pravomoci provede Komise posouzení dopadů a povede konzultace v souladu s článkem 56 nařízení (EU) 2019/881.

3. Komise může po konzultaci se skupinou pro spolupráci a Evropskou skupinou pro certifikaci kybernetické bezpečnosti požádat agenturu ENISA, aby v případech, kdy není k dispozici žádný vhodný evropský systém certifikace kybernetické bezpečnosti pro účely odstavce 2, vypracovala návrh systému podle čl. 48 odst. 2 nařízení (EU) 2019/881.

Článek 25

Tvorba norem

1. Členské státy za účelem harmonizovaného provádění čl. 21 odst. 1 a 2 podporují používání evropských a mezinárodních norem a technických 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, a případně po konzultaci s příslušnými zúčastněnými stranami, 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 národních norem, které by umožnily tyto oblasti pokrýt.

KAPITOLA V

PRAVOMOC A REGISTRACE

Článek 26

Pravomoc a územní působnost

1. Má se za to, že subjekty spadající do oblasti působnosti této směrnice podléhají pravomoci členského státu, v němž jsou usazeny, s výjimkou těchto případů:

a) poskytovatelé veřejných sítí elektronických komunikací nebo poskytovatelé veřejně dostupných služeb elektronických komunikací, u nichž se má za to, že podléhají pravomoci členského státu, v němž poskytují své služby;

b) provozovatelé DNS, registry domén nejvyšší úrovně, subjekty poskytující služby registrace jmen domén, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center, poskytovatelé sítí pro doručování obsahu, poskytovatelé řízených služeb, poskytovatelé řízených bezpečnostních služeb, poskytovatelé on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí, u nichž se má za to, že podléhají pravomoci členského státu, ve kterém mají hlavní provozovnu v Unii podle odstavce 2;

c) subjekty veřejné správy, u nichž se má za to, že podléhají pravomoci členského státu, který je zřídil.

2. Pro účely této směrnice se má za to, že hlavní provozovna subjektu podle odst. 1 písm. b) v Unii je umístěna v členském státě, v němž jsou převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. Nelze-li takový členský stát určit, nebo nejsou-li tato rozhodnutí přijímána v Unii, má se za to, že hlavní provozovna je v členském státě, v němž daný subjekt provádí činnosti k zajištění kybernetické bezpečnosti. Nelze-li takový členský stát určit, má se za to, že dotčený subjekt má hlavní provozovnu v členském státě, v němž má provozovnu s nejvyšším počtem zaměstnanců v Unii.

3. Jestliže subjekt uvedený v odst. 1 písm. b) 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 místa usazení zástupce. Neexistuje-li zástupce v Unii určený podle tohoto odstavce, může právní kroky proti subjektu za porušení této směrnice podniknout kterýkoli členský stát, v němž tento subjekt poskytuje služby.

4. Tím, že subjekt uvedený v odst. 1 písm. b) určí svého zástupce, nejsou dotčeny právní kroky, které by mohly být podniknuty proti subjektu samotnému.

5. Členské státy, které obdržely žádost o vzájemnou pomoc týkající se subjektu podle odst. 1 písm. b), mohou v mezích této žádosti přijmout ohledně dotčeného subjektu, který poskytuje služby nebo má síť nebo informační systém na jejich území, odpovídající opatření v oblasti dohledu a vymáhání.

Článek 27

Registr subjektů

1. Agentura ENISA vytvoří a vede registr provozovatelů DNS, registrů domén nejvyšší úrovně, subjektů poskytujících služby registrace jmen domén, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center, poskytovatelů sítí pro doručování obsahu, poskytovatelů řízených služeb, poskytovatelů řízených bezpečnostních služeb, jakož i poskytovatelů on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí na základě informací obdržených od jednotných kontaktních míst podle odstavce 4. Agentura ENISA na žádost umožní přístup do uvedeného rejstříku příslušným orgánům, přičemž v příslušných případech zajistí ochranu důvěrnosti informací.

2. Členské státy vyžadují, aby subjekty uvedené v odstavci 1 do 17. ledna 2025 předložily příslušným orgánům tyto informace:

a) název subjektu;

b) příslušné odvětví, pododvětví a druh subjektu, jak je v příslušných případech uvedeno v příloze I nebo II;

c) adresu hlavní provozovny subjektu a jeho dalších provozoven v Unii nebo, není-li subjekt v Unii usazen, zástupce subjektu určeného podle čl. 26 odst. 3;

d) aktuální kontaktní údaje, včetně e-mailových adres a telefonních čísel subjektu, a případně jeho zástupce určeného podle čl. 26 odst. 3;

e) členské státy, v nichž subjekt poskytuje své služby a

f) IP adresy subjektu.

3. Členské státy zajistí, aby subjekty uvedené v odstavci 1 oznámily příslušnému orgánu všechny změny informací, které předložily podle odstavce 2, a to bezodkladně, nejpozději však do tří měsíců od data změny.

4. Po obdržení informací podle odstavců 2 a 3, s výjimkou informací podle odst. 2 písm. f), jednotné kontaktní místo dotčeného členského státu postoupí bez zbytečného odkladu tyto informace agentuře ENISA.

5. V příslušném případě se informace uvedené v odstavcích 2 a 3 tohoto článku předloží prostřednictvím vnitrostátního mechanismu uvedeného v čl. 3 odst. 4 čtvrtém pododstavci.

Článek 28

Databáze údajů o registraci jmen domén

1. Aby členské státy přispěly k bezpečnosti, stabilitě a odolnosti systému překladu jmen domén, požadují, aby registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén shromažďovaly a uchovávaly přesné a úplné údaje o registraci jmen domén ve vyhrazené databázi, a to s náležitou péčí v souladu s právem Unie v oblasti ochrany údajů, pokud jde o data, jež jsou osobními údaji.

2. Členské státy pro účely odstavce 1 vyžadují, aby databáze údajů o registraci jmen domén obsahovala nezbytné informace umožňující identifikaci a kontaktování držitelů jmen domén a kontaktní místa spravující jména domén v registrech domén nejvyšší úrovně. Tyto informace zahrnují:

a) jméno domény;

b) datum registrace;

c) jméno žadatele o registraci, jeho kontaktní e-mailovou adresu a telefonní číslo;

d) kontaktní e-mailovou adresu a telefonní číslo kontaktního místa spravujícího jméno domény, pokud se liší od kontaktních údajů žadatele o registraci.

3. Členské státy požadují, aby registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén měly zavedeny zásady a postupy, včetně postupů ověřování, zajišťující, aby databáze uvedené v odstavci 1 zahrnovaly přesné a úplné informace. Členské státy požadují, aby byly tyto zásady a postupy veřejně dostupné.

4. Členské státy požadují, aby registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén zveřejňovaly bez zbytečného odkladu po registraci jména domény údaje o registraci jména domény, které nejsou osobními údaji.

5. Členské státy požadují, aby registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén poskytovaly přístup ke konkrétním údajům o registraci jmen domén na oprávněnou a řádně odůvodněnou žádost oprávněných žadatelů o přístup, a to v souladu s právem Unie v oblasti ochrany údajů. Členské státy požadují, aby registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén reagovaly bez zbytečného odkladu, nejpozději však do 72 hodin od obdržení žádosti o přístup. Členské státy požadují, aby byly zásady a postupy zveřejňování těchto údajů veřejně dostupné.

6. Dodržování povinností stanovených v odstavcích 1 až 5 nesmí při shromažďování údajů o registraci jmen domén vést ke zdvojování. Členské státy požadují, aby za tímto účelem registry domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén vzájemně spolupracovaly.

KAPITOLA VI

SDÍLENÍ INFORMACÍ

Článek 29

Ujednání o sdílení informací o kybernetické bezpečnosti

1. Členské státy zajistí, aby subjekty, na které se vztahuje oblast působnosti této směrnice, a případně jiné subjekty nespadající do oblasti působnosti této směrnice mohly mezi sebou dobrovolně sdílet podstatné informace o kybernetické bezpečnosti včetně informací týkajících se kybernetických hrozeb, významných událostí, zranitelností, technik a postupů, indikátorů kompromitace, nepřátelských taktik, informací specifických pro daný subjekt a danou hrozbu, varování při ohrožení kybernetické bezpečnosti a doporučení týkající se konfigurace nástrojů kybernetické bezpečnosti, které slouží k odhalování kybernetických útoků, pokud toto sdílení informací:

a) má za cíl předcházet incidentům, odhalovat je, reagovat na ně, zotavovat se z nich nebo zmírňovat jejich dopad;

b) zvyšuje úroveň kybernetické bezpečnosti, zejména zvyšováním informovanosti o kybernetických hrozbách, omezováním nebo bráněním schopnosti těchto hrozeb šířit se, podporou obranných schopností, nápravou zranitelností a zveřejňováním zranitelností, odhalováním hrozeb, technikami na zamezení šíření hrozeb a předcházení jim, strategií zmírňování nebo fází reakce a obnovy nebo podporou společného výzkumu kybernetických hrozeb ze strany subjektů veřejného a soukromého sektoru.

2. Členské státy zajistí, aby k výměně informací docházelo v komunitách základních a důležitých subjektů a případně jejich dodavatelů nebo poskytovatelů služeb. Tato výměna bude probíhat prostřednictvím ujednání o sdílení informací o kybernetické bezpečnosti s ohledem na potenciálně citlivou povahu sdílených informací.

3. Členské státy usnadní zavedení ujednání o sdílení informací o kybernetické bezpečnosti uvedených v odstavci 2 tohoto článku. Tato ujednání mohou upřesnit provozní prvky, včetně použití vyhrazených platforem IKT a nástrojů automatizace, obsah a podmínky ujednání o sdílení informací. Členské státy podrobně upraví zapojení veřejných orgánů do těchto ujednání, přičemž mohou stanovit podmínky pro informace zpřístupněné příslušnými orgány nebo týmy CSIRT. Členské státy nabídnou podporu při uplatňování těchto ujednání v souladu se svými politikami uvedenými v čl. 7 odst. 2 písm. h).

4. Členské státy zajistí, aby základní a důležité subjekty oznámily příslušným orgánům, že se účastní ujednání o sdílení informací o kybernetické bezpečnosti podle odstavce 2, a to od okamžiku uzavření takových ujednání, nebo v příslušných případech skutečnost, že od nich odstoupily, a to jakmile takové odstoupení nabude účinku.

5. Agentura ENISA podporuje vznik ujednání o sdílení informací o kybernetické bezpečnosti podle odstavce 2 výměnou osvědčených postupů a poskytováním pokynů.

Článek 30

Dobrovolné oznamování relevantních informací

1. Členské státy zajistí, aby vedle oznamovací povinnosti stanovené v článku 23 mohla být oznámení dobrovolně předkládána týmům CSIRT nebo případně příslušným orgánům ze strany:

a) základních a důležitých subjektů, pokud jde o incidenty, kybernetické hrozby a významné události;

b) subjektů, které nejsou uvedeny v písmeni a), bez ohledu na to, zda se na ně vztahuje oblast působnosti této směrnice, pokud jde o významné incidenty, kybernetické hrozby a významné události.

2. Při zpracování oznámení uvedených v odstavci 1 tohoto článku postupují členské státy v souladu s postupem stanoveným v článku 23. Členské státy mohou dát přednost zpracování povinných oznámení před dobrovolnými oznámeními.

V případě potřeby poskytnou týmy CSIRT a případně příslušné orgány jednotným kontaktním místům informace o oznámeních obdržených podle tohoto článku, přičemž zajistí důvěrnost a náležitou ochranu informací, jež poskytl oznamující subjekt. Aniž je dotčena prevence, vyšetřování, odhalování a stíhání trestných činů, nesmí dobrovolné oznámení vést k tomu, že oznamujícímu subjektu budou uloženy další povinnosti, které by neměl, kdyby toto oznámení neučinil.

KAPITOLA VII

DOHLED A VYMÁHÁNÍ

Článek 31

Obecné aspekty týkající se dohledu a vymáhání

1. Členské státy zajistí, aby jejich příslušné orgány účinně dohlížely na dodržování této směrnice a přijímaly opatření nezbytná k zajištění jejího dodržování.

2. Členské státy mohou svým příslušným orgánům umožnit, aby v rámci dohledu vymezily priority u svých činností. Toto vymezení priorit vychází z přístupu založeného na posouzení rizik. Za tímto účelem mohou příslušné orgány při výkonu svých dohledových úkolů stanovených v článcích 32 a 33 stanovit metodiky dohledu, které umožní stanovit priority těchto úkolů na základě přístupu vyplývajícího z posouzení rizik.

3. Při řešení incidentů, v jejichž důsledku došlo k porušení zabezpečení osobních údajů, příslušné orgány úzce spolupracují s dozorovými úřady podle nařízení (EU) 2016/679, aniž jsou dotčeny pravomoci a úkoly dozorových úřadů podle uvedeného nařízení.

4. Aniž jsou dotčeny vnitrostátní právní a institucionální rámce, členské státy zajistí, aby příslušné orgány měly při dohledu nad dodržováním této směrnice ze strany subjektů veřejné správy a při ukládání opatření v oblasti vymáhání za porušení této směrnice odpovídající pravomoci k provedení takových úkolů a měly přitom ve vztahu k subjektům veřejné správy, nad nimiž dohled provádějí, funkční nezávislost. Členské státy mohou rozhodnout o uložení vhodných, přiměřených a účinných opatření v oblasti dohledu a vymáhání ve vztahu k těmto subjektům v souladu s vnitrostátními právními a institucionálními rámci.

Článek 32

Opatření v oblasti dohledu a vymáhání týkající se 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 alespoň:

a) kontrolám na místě i externímu dohledu, včetně namátkových kontrol, které provádí vyškolení odborníci;

b) pravidelným a cíleným bezpečnostním auditům, které provádí nezávislý subjekt nebo příslušný orgán;

c) auditům ad hoc, a to i v případech odůvodněných významným incidentem nebo porušením této směrnice ze strany základního subjektu;

d) bezpečnostním prověrkám na základě objektivních, nediskriminačních, korektních a transparentních kritérií posouzení rizik, které se v případě potřeby provedou ve spolupráci s dotčeným subjektem;

e) požadavkům na informace nezbytné k posouzení opatření k řízení kybernetických bezpečnostních rizik přijatých dotčeným subjektem, včetně zadokumentovaných zásad kybernetické bezpečnosti, jakož i dodržování povinnosti předkládat informace příslušným orgánům podle článku 27;

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

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

Cílené bezpečnostní audity uvedené v prvním pododstavci písm. b) jsou založeny na posouzení rizik, jež provede příslušný orgán nebo auditovaný subjekt, nebo na jiných dostupných informacích týkajících se rizik.

Výsledky cíleného bezpečnostního auditu se zpřístupní příslušnému orgánu. Náklady na takový cílený bezpečnostní audit provedený nezávislým subjektem hradí auditovaný subjekt, s výjimkou řádně odůvodněných případů, kdy příslušný orgán rozhodne jinak.

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

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

a) vydat varování o porušení této směrnice dotčenými subjekty;

b) přijmout závazné pokyny, včetně pokynů týkajících se opatření nezbytných k zabránění incidentu nebo jeho nápravě, lhůt pro provedení těchto opatření a podávání zpráv o jejich provedení, nebo příkaz požadující, aby dotčené subjekty napravily zjištěné nedostatky nebo porušení této směrnice;

c) nařídit dotčeným subjektům, aby ukončily porušování této směrnice, a takového chování se znovu nedopouštěly;

d) nařídit dotčeným subjektům, aby zajistily, že jejich opatření k řízení kybernetických bezpečnostních rizik jsou v souladu s článkem 21, nebo aby plnily oznamovací povinnosti stanovené v článku 23, a to určeným způsobem a ve stanovené lhůtě;

e) nařídit dotčeným subjektům, aby informovaly fyzické nebo právnické osoby, v souvislosti s nimiž poskytují služby nebo vykonávají činnosti, které jsou potenciálně postiženy významnou kybernetickou hrozbou, o povaze této hrozby, jakož i o všech možných ochranných nebo nápravných opatřeních, jež by mohly tyto fyzické nebo právnické osoby učinit v reakci na tuto hrozbu;

f) nařídit dotčeným subjektům, aby v přiměřené lhůtě provedly doporučení vydaná v důsledku bezpečnostního auditu;

g) určit na stanovenou dobu pracovníka pro sledování s přesně vymezenými úkoly, který bude dohlížet na dodržování článků 21 a 23 ze strany dotčených subjektů;

h) nařídit dotčeným subjektům, aby určeným způsobem zveřejnily aspekty týkající se porušení této směrnice;

i) vedle kteréhokoli z opatření uvedených v písmenech a) až h) tohoto odstavce uložit správní pokutu podle článku 34 nebo navrhnout příslušným orgánům nebo soudům v souladu s vnitrostátním právem její uložení.

5. Pokud jsou opatření v oblasti vymáhání přijatá podle odst. 4 písm. a) až d) a f) neúčinná, členské státy zajistí, aby jejich 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 jejich příslušné orgány měly pravomoc:

a) dočasně pozastavit nebo v souladu s vnitrostátním právem požádat certifikační nebo povolovací orgán nebo soud o dočasné pozastavení certifikace nebo povolení týkající se části nebo všech příslušných služeb nebo činností poskytovaných základním subjektem;

b) požadovat, aby příslušné orgány nebo soudy v souladu s vnitrostátním právem uložily dočasný zákaz výkonu řídicích funkcí v základním subjektu jakékoliv fyzické osobě, která má odpovědnost za výkon řídicích funkcí na úrovni výkonného ředitele nebo zákonného zástupce v tomto subjektu.

Dočasná pozastavení nebo zákazy uložené podle tohoto odstavce se použijí pouze do okamžiku, než dotčený subjekt přijme opatření nezbytná k nápravě nedostatků nebo splnění požadavků příslušného orgánu, kvůli nimž byla tato opatření v oblasti vymáhání uplatněna. Uložení takových dočasných pozastavení nebo zákazů podléhá náležitým procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny, včetně práva na účinnou právní ochranu a na spravedlivý proces, presumpce neviny a práva na obhajobu.

Opatření v oblasti vymáhání stanovená v tomto odstavci se nevztahují na subjekty veřejné správy, na něž se vztahuje tato směrnice.

6. Členské státy zajistí, aby každá fyzická osoba jednající za základní subjekt nebo jednající jako právní zástupce základního subjektu na základě oprávnění jej zastupovat, oprávnění přijímat rozhodnutí jeho jménem nebo oprávnění vykonávat nad ním kontrolu měla pravomoc zajistit dodržování této směrnice. Členské státy zajistí, aby byla stanovena odpovědnost těchto fyzických osob za porušení jejich povinností spočívajících v zajištění dodržování této směrnice.

Pokud jde o subjekty veřejné správy, není tímto odstavcem dotčeno vnitrostátní právo o odpovědnosti úředníků veřejné správy a volených veřejných činitelů nebo jmenovaných úředníků.

7. Při přijímání opatření v oblasti vymáhání podle odstavce 4 nebo 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, přičemž následující porušení se vždy považují za závažná:

   i) opakovaná porušení;

   ii) neoznámení nebo nezajištění nápravy významných incidentů;

   iii) nenapravení nedostatků podle závazných pokynů příslušných orgánů;

   iv) maření auditů nebo sledovací činnosti nařízené příslušným orgánem po zjištění porušení;

   v) poskytnutí nepravdivých nebo hrubě nepřesných informací v souvislosti s opatřeními pro řízení rizik v oblasti kybernetické bezpečnosti nebo oznamovacími povinnostmi stanovenými v článcích 21 a 23;

b) dobu trvání porušení;

c) veškerá relevantní porušení, kterých se dotčený subjekt dopustil v minulosti;

d) způsobenou hmotnou nebo nehmotnou újmu, včetně jakékoli finanční nebo ekonomické ztráty, účinků na jiné služby a počtu postižených uživatelů;

e) jakýkoli úmysl nebo nedbalost pachatele porušení;

f) jakákoli opatření přijatá subjektem za účelem zamezení nebo zmírnění hmotné nebo nehmotné újmy;

g) jakékoli dodržování schválených kodexů chování nebo schválených certifikačních mechanismů;

h) úroveň spolupráce odpovědné fyzické nebo právnické osoby s příslušnými orgány.

8. Příslušné orgány svá opatření v oblasti vymáhání podrobně odůvodní. Příslušné orgány před přijetím těchto opatření oznámí dotčeným subjektům svá předběžná zjištění. Rovněž těmto subjektům poskytnou přiměřenou dobu na předložení připomínek, s výjimkou řádně odůvodněných případů, kdy by to bránilo přijetí okamžitých opatření k předcházení incidentům nebo reakci na ně.

9. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice informovaly relevantní příslušné orgány ve stejném členském státě podle směrnice (EU) 2022/2557, když plní své pravomoci v oblasti dohledu a vymáhání zaměřené na zajištění toho, aby subjekt určený jakožto kritický subjekt podle směrnice (EU) 2022/2557 dodržoval tuto směrnici. Příslušné orgány podle směrnice (EU) 2022/2557 mohou případně požádat příslušné orgány podle této směrnice, aby vykonávaly své dohledové a vymáhací pravomoci ve vztahu k subjektu, který je určen jakožto kritický subjekt podle směrnice (EU) 2022/2557.

10. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice spolupracovaly s relevantními příslušnými orgány dotčeného členského státu podle nařízení (EU) 2022/2554. Členské státy zejména zajistí, aby jejich příslušné orgány podle této směrnice informovaly fórum dohledu zřízené podle čl. 32 odst. 1 nařízení (EU) 2022/2554, když plní své pravomoci v oblasti dohledu a vymáhání zaměřené na zajištění toho, aby základní subjekt, který je označen jakožto kritický poskytovatel služeb IKT z řad třetích stran podle článku 31 nařízení (EU) 2022/2554, dodržoval tuto směrnici.

Článek 33

Opatření v oblasti dohledu a vymáhání týkající se důležitých subjektů

1. Jsou-li členským státům předloženy důkazy, indicie nebo informace, které naznačují, že důležitý subjekt údajně nedodržuje tuto směrnici, zejména její články 21 a 23, členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření prostřednictvím dohledových opatření ex post. Členské státy zajistí, aby tato opatření byla 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 s důležitými subjekty pravomoc podrobit tyto subjekty alespoň:

a) kontrolám na místě i externímu dohledu ex post, které provádí vyškolení odborníci;

b) cíleným bezpečnostním auditům, které provádí nezávislý subjekt nebo příslušný orgán;

c) bezpečnostním prověrkám na základě objektivních, nediskriminačních, korektních a transparentních kritérií posouzení rizik, které se v případě potřeby provedou ve spolupráci s dotčeným subjektem;

d) požadavkům na informace nezbytné k posouzení opatření k řízení kybernetických bezpečnostních rizik ex post přijatých dotčeným subjektem, včetně zadokumentovaných zásad kybernetické bezpečnosti, jakož i dodržování povinnosti předkládat informace příslušným orgánům podle článku 28;

e) požadavkům na přístup k údajům, dokumentům a informacím potřebným pro výkon jejich dohledových úkolů;

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

Cílené bezpečnostní audity uvedené v prvním pododstavci písm. b) jsou založeny na posouzení rizik, jež provede příslušný orgán nebo auditovaný subjekt, nebo na jiných dostupných informacích týkajících se rizik.

Výsledky cíleného bezpečnostního auditu se zpřístupní příslušnému orgánu. Náklady na takový cílený bezpečnostní audit provedený nezávislým subjektem hradí auditovaný subjekt, s výjimkou řádně odůvodněných případů, kdy příslušný orgán rozhodne jinak.

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

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

a) vydat varování o porušení této směrnice ze strany dotčených subjektů;

b) přijmout závazné pokyny nebo příkaz požadující, aby dotčené subjekty napravily zjištěné nedostatky nebo porušení této směrnice;

c) nařídit dotčeným subjektům, aby ukončily chování, které porušuje tuto směrnici, a takového chování se znovu nedopouštěly;

d) nařídit dotčeným subjektům, aby zajistily, že jejich opatření k řízení kybernetických bezpečnostních rizik jsou v souladu s článkem 21, nebo aby plnily oznamovací povinnosti stanovené v článku 23, a to určeným způsobem a ve stanovené lhůtě;

e) nařídit dotčeným subjektům, aby informovaly fyzické nebo právnické osoby, v souvislosti s nimiž poskytují služby nebo vykonávají činnosti, které jsou potenciálně postiženy významnou kybernetickou hrozbou, o povaze této hrozby, jakož i o všech možných ochranných nebo nápravných opatřeních, jež by mohly tyto fyzické nebo právnické osoby učinit v reakci na tuto hrozbu;

f) nařídit dotčeným subjektům, aby v přiměřené lhůtě provedly doporučení vydaná v důsledku bezpečnostního auditu;

g) nařídit dotčeným subjektům, aby určeným způsobem zveřejnily aspekty týkající se porušení této směrnice;

h) vedle kteréhokoli z opatření uvedených v písmenech a) až g) tohoto odstavce uložit správní pokutu podle článku 34 nebo navrhnout příslušným orgánům nebo soudům v souladu s vnitrostátním právem její uložení.

5. Ustanovení čl. 32 odst. 6, 7 a 8 se obdobně použijí na opatření v oblasti dohledu a vymáhání stanovená v tomto článku pro důležité subjekty.

6. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice spolupracovaly s relevantními příslušnými orgány dotčeného členského státu podle nařízení (EU) 2022/2554. Členské státy zejména zajistí, aby jejich příslušné orgány podle této směrnice informovaly fórum dohledu zřízené podle čl. 32 odst. 1 nařízení (EU) 2022/2554, když plní své pravomoci v oblasti dohledu a vymáhání zaměřené na zajištění toho, aby důležitý subjekt, který je označen jakožto kritický poskytovatel služeb IKT z řad třetích stran podle článku 31 nařízení (EU) 2022/2554, dodržoval tuto směrnici.

Článek 34

Obecné podmínky ukládání správních pokut základním a důležitým subjektům

1. Členské státy zajistí, aby správní pokuty ukládané základním a důležitým subjektům podle tohoto článku za porušení této směrnice byly účinné, přiměřené a odrazující, přičemž zohlední okolnosti každého jednotlivého případu.

2. Správní pokuty se ukládají spolu s kterýmkoli z opatření uvedených v čl. 32 odst. 4 písm. a) až h), čl. 32 odst. 5 a čl. 33 odst. 4 písm. a) až g).

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. 32 odst. 7.

4. Členské státy zajistí, aby v případě, že základní subjekty poruší článek 21 nebo 23, byly uvedeným subjektům v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty, jejichž maximální výše bude stanovena na nejméně 10 000 000 EUR nebo maximálně na alespoň 2 % celkového celosvětového ročního obratu v předchozím rozpočtovém roce u podniku, ke kterému patří základní subjekt, podle toho, co je vyšší.

5. Členské státy zajistí, aby v případě, že důležité subjekty poruší článek 21 nebo 23, byly uvedeným subjektům v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty, jejichž maximální výše bude stanovena na nejméně 7 000 000 EUR nebo maximálně na alespoň 1,4 % celkového celosvětového ročního obratu v předchozím rozpočtovém roce u podniku, ke kterému patří důležitý subjekt, podle toho, co je vyšší.

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

7. Aniž jsou dotčeny pravomoci příslušných orgánů podle článků 32 a 33, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty subjektům veřejné správy.

8. Neumožňuje-li právo členského státu uložení správních pokut, tento členský stát zajistí, že se tento článek uplatní tak, aby podnět k uložení pokuty dal příslušný orgán a aby pokuta byla uložena příslušnými vnitrostátními soudy, přičemž současně je třeba zajistit, aby tyto prostředky právní nápravy byly účinné a aby byl jejich účinek rovnocenný správním pokutám, jež ukládají příslušné orgány. Uložené pokuty musí být v každém případě účinné, přiměřené a odrazující. Členský stát oznámí Komisi do 17. října 2024 příslušná ustanovení právních předpisů, která přijme podle tohoto odstavce, a bez prodlení jakoukoli následnou novelu nebo změnu týkající se těchto ustanovení.

Článek 35

Porušení obnášející porušení zabezpečení osobních údajů

1. Pokud příslušné orgány v průběhu dohledu nebo vymáhání zjistí, že porušení povinností stanovených v článcích 21 a 23 této směrnice základním nebo důležitým subjektem může obnášet porušení zabezpečení osobních údajů ve smyslu čl. 4 odst. 12 nařízení (EU) 2016/679, které má být oznámeno podle článku 33 uvedeného nařízení, uvědomí bez zbytečného odkladu dozorové úřady podle článku 55 nebo 56 uvedeného nařízení.

2. Pokud dozorové úřady podle článku 55 nebo 56 nařízení (EU) 2016/679 uloží správní pokutu podle čl. 58 odst. 2 písm. i) uvedeného nařízení, příslušné orgány nesmí uložit správní pokutu podle článku 34 této směrnice za porušení uvedené v odstavci 1 tohoto článku za stejné porušení, za něž byla uložena správní pokuta podle čl. 58 odst. 2 písm. i) nařízení (EU) 2016/679. Příslušné orgány však mohou uložit opatření v oblasti vymáhání stanovené v čl. 32 odst. 4 písm. a) až h), čl. 32 odst. 5 a čl. 33 odst. 4 písm. a) až g) této směrnice.

3. Pokud má dozorový úřad příslušný podle nařízení (EU) 2016/679 sídlo v jiném členském státě než příslušný orgán, informuje příslušný orgán dozorový úřad se sídlem ve stejném členském státě o možném porušení zabezpečení údajů podle odstavce 1.

Článek 36

Sankce

Členské státy stanoví sankce za porušení vnitrostátních opatření přijatých podle této směrnice a přijmou veškerá opatření nezbytná k zajištění jejich uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující. Členské státy tyto sankce a opatření oznámí Komisi nejpozději do 17. ledna 2025 a neprodleně jí oznámí všechny jejich následné změny.

Článek 37

Vzájemná pomoc

1. Pokud subjekt poskytuje služby ve více než jednom členském státě, nebo pokud poskytuje služby v jednom nebo více členských státech a jeho sítě a informační systémy se nacházejí v jednom či více jiných členských státech, příslušné orgány dotčených 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 kontaktují prostřednictvím jednotného kontaktního místa příslušné orgány v ostatních dotčených členských státech, konzultují s nimi a informují je ohledně přijatých opatření v oblasti dohledu a vymáhání;

b) příslušný orgán může požádat jiný příslušný orgán, aby učinil opatření v oblasti dohledu nebo vymáhání;

c) po obdržení odůvodněné žádosti jiného příslušného orgánu poskytne příslušný orgán druhému příslušnému orgánu vzájemnou pomoc úměrnou vlastním zdrojům, aby bylo možné provést opatření v oblasti dohledu nebo vymáhání účinně, účelně a důsledně.

Vzájemná pomoc uvedená v prvním pododstavci písm. c) 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 prokáže, že tento orgán není příslušný k poskytnutí požadované pomoci nebo požadovaná pomoc není úměrná úkolům dohledu příslušného orgánu nebo že se žádost týká informací nebo zahrnuje činnosti, které by v případě zveřejnění nebo provedení byly v rozporu se zásadními zájmy v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany daného členského státu. Před zamítnutím takové žádosti konzultuje příslušný orgán ostatní dotčené příslušné orgány a na žádost jednoho z dotčených členských států také Komisi a agenturu ENISA.

2. Je-li to vhodné, mohou se příslušné orgány z různých členských států vzájemně dohodnout, že budou provádět společné činnosti v oblasti dohledu.

KAPITOLA VIII

AKTY V PŘENESENÉ PRAVOMOCI A PROVÁDĚCÍ AKTY

Článek 38

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. 24 odst. 2 je svěřena Komisi na dobu pěti let ode dne 16. ledna 2023.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 24 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. 24 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 39

Postup projednávání ve výboru

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

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

3. Má-li být o stanovisku výboru rozhodnuto písemným postupem, ukončuje se tento postup bez výsledku, pokud o tom ve lhůtě pro vydání stanoviska rozhodne předseda výboru nebo pokud o to požádá člen výboru.

KAPITOLA IX

ZÁVĚREČNÁ USTANOVENÍ

Článek 40

Přezkum

Do 17. října 2027 a poté každých 36 měsíců Komise přezkoumá fungování této směrnice a podá zprávu Evropskému parlamentu a Radě. Ve zprávě se zejména posoudí význam velikosti dotčených subjektů a odvětví, pododvětví a druhy subjektů podle příloh 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. V případě potřeby se ke zprávě přiloží legislativní návrh.

Článek 41

Provedení ve vnitrostátním právu

1. Členské státy do 17. října 2024 přijmou a zveřejní opatření nezbytná pro dosažení souladu s touto směrnicí. Neprodleně o nich uvědomí Komisi.

Použijí tato opatření ode dne 18. října 2024.

2. Opatření uvedená v odst. 1 přijatá 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 42

Změna nařízení (EU) č. 910/2014

Článek 19 nařízení (EU) č. 910/2014 se zrušuje s účinkem ode dne 18. října 2024.

Článek 43

Změna směrnice (EU) 2018/1972

Články 40 a 41 směrnice (EU) 2018/1972 se zrušují s účinkem ode dne 18. října 2024.

Článek 44

Zrušení

Směrnice (EU) 2016/1148 se zrušuje s účinkem ode dne 18. října 2024.

Odkazy na zrušenou směrnici se považují za odkazy na tuto směrnici v souladu se srovnávací tabulkou obsaženou v příloze III.

Článek 45

Vstup v platnost

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

Článek 46

Určení

Tato směrnice je určena členským státům.

Ve Štrasburku dne 14. Prosince 2022.

Za Evropský parlament	*Za Radu*
předsedkyně	*předseda*
R. METSOLA	M. BEK

PŘÍLOHA I

VYSOCE KRITICKÁ ODVĚTVÍ

Odvětví	Pododvětví	Druh subjektu
1. Energetika	a) elektřina	— elektroenergetické podniky ve smyslu čl. 2 bodu 57 směrnice Evropského parlamentu a Rady (EU) 2019/944 ([1]), které zastávají funkci „dodávky“ ve smyslu čl. 2 bodu 12 uvedené směrnice
		— provozovatelé distribuční soustavy ve smyslu čl. 2 bodu 29 směrnice (EU) 2019/944
		— provozovatelé přenosové soustavy ve smyslu čl. 2 bodu 35 směrnice (EU) 2019/944
		— výrobci ve smyslu čl. 2 bodu 38 směrnice (EU) 2019/944
		— nominovaní organizátoři trhu s elektřinou ve smyslu čl. 2 bodu 8 nařízení Evropského parlamentu a Rady (EU) 2019/943 ([2]) — účastníci trhu ve smyslu čl. 2 bodu 25 nařízení (EU) 2019/943, kteří poskytují služby agregace, odezvy strany poptávky nebo ukládání energie ve smyslu čl. 2 bodů 18, 20 a 59 směrnice (EU) 2019/944 — provozovatelé dobíjecích bodů, kteří jsou odpovědní za řízení a provoz dobíjecích bodů, které koncovým uživatelům poskytují službu dobíjení, a to i jménem a na účet poskytovatele služeb mobility
	b) dálkové vytápění a chlazení	— provozovatelé dálkového vytápění nebo dálkového chlazení ve smyslu čl. 2 bodu 19 směrnice Evropského parlamentu a Rady (EU) 2018/2001 ([3])
	c) ropa	— provozovatelé ropovodů
		— provozovatelé zařízení na těžbu, rafinaci a zpracování ropy a skladovacích a přenosových zařízení
		— ústřední správci zásob ve smyslu čl. 2 písm. f) směrnice Rady 2009/119/ES ([4])
	d) zemní plyn	— dodavatelské podniky ve smyslu čl. 2 bodu 8 směrnice Evropského parlamentu a Rady 2009/73/ES ([5])
		— provozovatelé distribuční soustavy ve smyslu čl. 2 bodu 6 směrnice 2009/73/ES
		— provozovatelé přepravní soustavy ve smyslu čl. 2 bodu 4 směrnice 2009/73/ES
		— provozovatelé skladovacího zařízení ve smyslu čl. 2 bodu 10 směrnice 2009/73/ES
		— provozovatelé zařízení LNG ve smyslu čl. 2 bodu 12 směrnice 2009/73/ES
		— plynárenské podniky ve smyslu čl. 2 bodu 1 směrnice 2009/73/ES
		— provozovatelé zařízení na rafinaci a zpracování zemního plynu
	e) vodík	— provozovatelé výroby, skladování a přepravy vodíku

Odvětví	Pododvětví	Druh subjektu
2. Doprava	a) letecká	— letečtí dopravci ve smyslu čl. 3 bodu 4 nařízení (ES) č. 300/2008 využívaní ke komerčním účelům
		— řídící orgány letiště ve smyslu čl. 2 bodu 2 směrnice Evropského parlamentu a Rady 2009/12/ES ([6]), letiště ve smyslu čl. 2 bodu 1 uvedené směrnice, včetně hlavních letišť uvedených v příloze II, části 2 nařízení Evropského parlamentu a Rady (EU) č. 1315/2013 ([7]), a subjekty provozující pomocná zařízení v rámci letišť
		— provozovatelé kontroly řízení provozu poskytující služby řízení letového provozu ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (ES) č. 549/2004 ([8])
	b) železniční	— provozovatelé infrastruktury ve smyslu čl. 3 bodu 2 směrnice Evropského parlamentu a Rady 2012/34/EU ([9])
		— železniční podniky ve smyslu čl. 3 bodu 1 směrnice 2012/34/EU, včetně provozovatelů zařízení služeb ve smyslu čl. 3 bodu 12 uvedené směrnice
	c) vodní	— společnosti vnitrozemské, námořní a pobřežní osobní a nákladní vodní dopravy, jak jsou vymezeny pro námořní dopravu v příloze I nařízení Evropského parlamentu a Rady (ES) č. 725/2004 ([10]), kromě jednotlivých plavidel provozovaných těmito podniky
		— řídící orgány přístavů ve smyslu čl. 3 bodu 1 směrnice Evropského parlamentu a Rady 2005/65/ES ([11]), včetně jejich přístavních zařízení ve smyslu čl. 2 bodu 11 nařízení (ES) č. 725/2004; a subjekty provozující díla a zařízení v rámci přístavů
		— provozovatelé služeb lodní dopravy (VTS) ve smyslu čl. 3 písm. o) směrnice Evropského parlamentu a Rady 2002/59/ES ([12])
	d) silniční	— silniční orgány ve smyslu čl. 2 bodu 12 nařízení Komise v přenesené pravomoci (EU) 2015/962 ([13]) odpovědné za kontrolu řízení provozu, s výjimkou veřejných subjektů, pro něž je řízení provozu nebo provoz inteligentních dopravních systémů nepodstatnou částí jejich obecné činnosti
		— provozovatelé inteligentních dopravních systémů ve smyslu čl. 4 bodu 1 směrnice Evropského parlamentu a Rady 2010/40/EU ([14])
3. Bankovnictví		úvěrové instituce ve smyslu čl. 4 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ([15])
4. Infrastruktura finančních trhů		— provozovatelé obchodních systémů ve smyslu čl. 4 bodu 24 směrnice Evropského parlamentu a Rady 2014/65/EU ([16])
		— ústřední protistrany ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ([17])

Odvětví	Pododvětví	Druh subjektu
5. Zdravotnictví		— poskytovatelé zdravotní péče ve smyslu čl. 3 písm. g) směrnice Evropského parlamentu a Rady 2011/24/EU ([18])
		— referenční laboratoře EU ve smyslu článku 15 nařízení Evropského parlamentu a Rady (EU) 2022/... ([19])
		— subjekty provádějící výzkum a vývoj týkající se léčivých přípravků ve smyslu čl. 1 bodu 2 směrnice Evropského parlamentu a Rady 2001/83/ES ([20]) — subjekty vyrábějící základní farmaceutické výrobky a farmaceutické přípravky ve smyslu sekce C oddílu 21 klasifikace NACE Rev. 2 — subjekty vyrábějící zdravotnické prostředky považované za kriticky důležité v případě mimořádné situace v oblasti veřejného zdraví (uvedené na „seznamu kriticky důležitých zdravotnických prostředků při mimořádné situaci v oblasti veřejného zdraví“) ve smyslu článku 22 nařízení Evropského parlamentu a Rady (EU) 2022/123 ([21])
6. Pitná voda		dodavatelé a distributoři vody určené k lidské spotřebě ve smyslu čl. 2 bodu 1 písm. a) směrnice Evropského parlamentu a Rady (EU) 2020/2184 ([22]), s výjimkou distributorů, pro něž je distribuce vody určené k lidské spotřebě nepodstatnou částí jejich obecné činnosti spočívající v distribuci komodit a zboží
7. Odpadní voda		podniky zajišťující odvádění, vypouštění nebo čištění městských odpadních vod, splašek nebo průmyslových odpadních vod ve smyslu čl. 2 bodů 1, 2 a 3 směrnice Rady 91/271/EHS ([23]), s výjimkou podniků, pro něž je odvádění, vypouštění nebo čištění městských odpadních vod, splašek nebo průmyslových odpadních vod nepodstatnou částí jejich obecné činnosti
8. Digitální infrastruktura		— provozovatelé výměnných uzlů internetu
		— provozovatelé DNS, s výjimkou operátorů kořenových jmenných serverů
		— registry domén nejvyšší úrovně (TLD)
		— poskytovatelé služeb cloud computingu
		— poskytovatelé služeb datových center
		— poskytovatelé sítí pro doručování obsahu
		— poskytovatelé služeb vytvářejících důvěru
		— poskytovatelé veřejných sítí elektronických komunikací
		— poskytovatelé veřejně dostupných služeb elektronických komunikací
9. Řízení služeb IKT (mezi podniky)		— poskytovatelé řízených služeb — poskytovatelé řízených bezpečnostních služeb

Odvětví	Pododvětví	Druh subjektu
10. Veřejná správa		— ústřední subjekty veřejné správy vymezené členským státem v souladu s vnitrostátním právem
		— subjekty regionální veřejné správy vymezené členským státem v souladu s vnitrostátním právem
11. Vesmír		provozovatelé pozemních infrastruktur vlastněných, spravovaných a provozovaných členskými státy nebo soukromými subjekty a podporujících poskytování služeb využívajících kosmického prostoru, s výjimkou poskytovatelů veřejných sítí elektronických komunikací

([1]) Směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU (Úř. věst. L 158, 14.6.2019, s. 125).
([2]) Nařízení Evropského parlamentu a Rady (EU) 2019/943 ze dne 5. června 2019 o vnitřním trhu s elektřinou (Úř. věst. L 158, 14.6.2019, s. 54).
([3]) Směrnice Evropského parlamentu a Rady (EU) 2018/2001 ze dne 11. prosince 2018 o podpoře využívání energie z obnovitelných zdrojů (Úř. věst. L 328, 21.12.2018, s. 82).
([4]) Směrnice Rady 2009/119/ES ze dne 14. září 2009, kterou se členským státům ukládá povinnost udržovat minimální zásoby ropy nebo ropných produktů (Úř. věst. L 265, 9.10.2009, s. 9).
([5]) Směrnice Evropského parlamentu a Rady 2009/73/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh se zemním plynem a o zrušení směrnice 2003/55/ES (Úř. věst. L 211, 14.8.2009, s. 94).
([6]) Směrnice Evropského parlamentu a Rady 2009/12/ES ze dne 11. března 2009 o letištních poplatcích (Úř. věst. L 70, 14.3.2009, s. 11).
([7]) Nařízení Evropského parlamentu a Rady (EU) č. 1315/2013 ze dne 11. prosince 2013 o hlavních směrech Unie pro rozvoj transevropské dopravní sítě a o zrušení rozhodnutí č. 661/2010/EU (Úř. věst. L 348, 20.12.2013, s. 1).
([8]) Nařízení Evropského parlamentu a Rady (ES) č. 549/2004 ze dne 10. března 2004, kterým se stanoví rámec pro vytvoření jednotného evropského nebe (rámcové nařízení) (Úř. věst. L 96, 31.3.2004, s. 1).
([9]) Směrnice Evropského parlamentu a Rady 2012/34/EU ze dne 21. listopadu 2012 o vytvoření jednotného evropského železničního prostoru (Úř. věst. L 343, 14.12.2012, s. 32).
([10]) Nařízení Evropského parlamentu a Rady (ES) č. 725/2004 ze dne 31. března 2004 o zvýšení bezpečnosti lodí a přístavních zařízení (Úř. věst. L 129, 29.4.2004, s. 6).
([11]) Směrnice Evropského parlamentu a Rady 2005/65/ES ze dne 26. října 2005 o zvýšení zabezpečení přístavů (Úř. věst. L 310, 25.11.2005, s. 28).
([12]) Směrnice Evropského parlamentu a Rady 2002/59/ES ze dne 27. června 2002, kterou se stanoví kontrolní a informační systém Společenství pro provoz plavidel a kterou se zrušuje směrnice Rady 93/75/EHS (Úř. věst. L 208, 5.8.2002, s. 10).
([13]) Nařízení Komise v přenesené pravomoci (EU) 2015/962 ze dne 18. prosince 2014, kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU, pokud jde o poskytování informačních služeb o dopravním provozu v reálném čase v celé EU (Úř. věst. L 157, 23.6.2015, s. 21).
([14]) Směrnice Evropského parlamentu a Rady 2010/40/EU ze dne 7. července 2010 o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy (Úř. věst. L 207, 6.8.2010, s. 1).
([15]) Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 176, 27.6.2013, s. 1).
([16]) Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU (Úř. věst. L 173, 12.6.2014, s. 349).
([17]) Nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů (Úř. věst. L 201, 27.7.2012, s. 1).
([18]) Směrnice Evropského parlamentu a Rady 2011/24/EU ze dne 9. března 2011 o uplatňování práv pacientů v přeshraniční zdravotní péči (Úř. věst. L 88, 4.4.2011, s. 45).

([19]) Nařízení Evropského parlamentu a Rady (EU) 2022/2371 ze dne 23. listopadu 2022 o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 1082/2013/EU (Úř. věst. L 314, 6.12.2022, s. 26).

([20]) Směrnice Evropského parlamentu a Rady 2001/83/ES ze dne 6. listopadu 2001 o kodexu Společenství týkajícím se humánních léčivých přípravků (Úř. věst. L 311, 28.11.2001, s. 67).

([21]) Nařízení Evropského parlamentu a Rady (EU) 2022/123 ze dne 25. ledna 2022 o posílené úloze Evropské agentury pro léčivé přípravky při připravenosti na krize a krizovém řízení v oblasti léčivých přípravků a zdravotnických prostředků (Úř. věst. L 20, 31.1.2022, s. 1).

([22]) Směrnice Evropského parlamentu a Rady (EU) 2020/2184 ze dne 16. prosince 2020 o jakosti vody určené k lidské spotřebě (přepracované znění (Úř. věst. L 435, 23.12.2020, s. 1).

([23]) Směrnice Rady 91/271/EHS ze dne 21. května 1991 o čištění městských odpadních vod (Úř. věst. L 135, 30.5.1991, s. 40).

PŘÍLOHA II

DALŠÍ KRITICKÁ ODVĚTVÍ

Odvětví	Pododvětví	Druh subjektu
1. Poštovní a kurýrní služby		poskytovatelé poštovních služeb ve smyslu čl. 2 bodu 1a směrnice 97/67/ES, včetně poskytovatelů kurýrních služeb
2. Nakládání s odpady		podniky provádějící nakládání s odpady ve smyslu čl. 3 bodu 9 směrnice Evropského parlamentu a Rady 2008/98/ES ([1]), avšak s výjimkou podniků, pro které nakládání s odpady nepředstavuje hlavní hospodářskou činnost
3. Výroba, produkce a distribuce chemických látek		podniky provádějící výrobu látek a distribuci látek nebo směsí ve smyslu čl. 3 bodů 9 a 14 nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 ([2]) a podniky provádějící výrobu předmětů ve smyslu čl. 3 bodu 3 uvedeného nařízení z látek či směsí
4. Výroba, zpracování a distribuce potravin		potravinářské podniky ve smyslu čl. 3 bodu 2 nařízení Evropského parlamentu a Rady (ES) č. 178/2002 ([3]), které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním
5. Výroba	a) výroba zdravotnických prostředků a diagnostických zdravotnických prostředků in vitro	subjekty vyrábějící zdravotnické prostředky ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) 2017/745 ([4]) a subjekty vyrábějící diagnostické zdravotnické prostředky in vitro ve smyslu čl. 2 bodu 2 nařízení Evropského parlamentu a Rady (EU) 2017/746 ([5]), s výjimkou subjektů vyrábějících zdravotnické prostředky uvedených v příloze I bodu 5 páté odrážce této směrnice
	b) výroba počítačů, elektronických a optických přístrojů a zařízení	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 26 klasifikace NACE Rev. 2
	c) výroba elektrických zařízení	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 27 klasifikace NACE Rev. 2
	d) výroba strojů a zařízení j. n.	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 28 klasifikace NACE Rev. 2
	e) výroba motorových vozidel, přívěsů a návěsů	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 29 klasifikace NACE Rev. 2
	f) výroba ostatních dopravních prostředků a zařízení	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 30 klasifikace NACE Rev. 2

Odvětví	Pododvětví	Druh subjektu
6. Digitální poskytovatelé		— poskytovatelé on-line tržišť
		— poskytovatelé internetových vyhledávačů
		— poskytovatelé služeb platforem sociálních sítí
7. Výzkum		výzkumné organizace

([1]) Směrnice Evropského parlamentu a Rady 2008/98/ES ze dne 19. listopadu 2008 o odpadech a o zrušení některých směrnic (Úř. věst. L 312, 22.11.2008, s. 3).

([2]) Nařízení Evropského parlamentu a Rady (ES) č. 1907/2006 ze dne 18. prosince 2006 o registraci, hodnocení, povolování a omezování chemických látek (REACH), o zřízení Evropské agentury pro chemické látky, o změně směrnice 1999/45/ES a o zrušení nařízení Rady (EHS) č. 793/93, nařízení Komise (ES) č. 1488/94, směrnice Rady 76/769/EHS a směrnic Komise 91/155/EHS, 93/67/EHS, 93/105/ES a 2000/21/ES (Úř. věst. L 396, 30.12.2006, s. 1).

([3]) Nařízení Evropského parlamentu a Rady (ES) č. 178/2002 ze dne 28. ledna 2002, kterým se stanoví obecné zásady a požadavky potravinového práva, zřizuje se Evropský úřad pro bezpečnost potravin a stanoví postupy týkající se bezpečnosti potravin (Úř. věst. L 31, 1.2.2002, s. 1).

([4]) Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, změně směrnice 2001/83/ES, nařízení (ES) č. 178/2002 a nařízení (ES) č. 1223/2009 a o zrušení směrnic Rady 90/385/EHS a 93/42/EHS (Úř. věst. L 117, 5.5.2017, s. 1).

([5]) Nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích in vitro a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU (Úř. věst. L 117, 5.5.2017, s. 176).

PŘÍLOHA III

SROVNÁVACÍ TABULKA

Směrnice (EU) 2016/1148	Tato směrnice
Čl. 1 odst. 1	Čl. 1 odst. 1
Čl. 1 odst. 2	Čl. 1 odst. 2
Čl. 1 odst. 3	-
Čl. 1 odst. 4	Čl. 2 odst. 12
Čl. 1 odst. 5	Čl. 2 odst. 13
Čl. 1 odst. 6	Čl. 2 odst. 6 a 11
Čl. 1 odst. 7	Článek 4
Článek 2	Čl. 2 odst. 14
Článek 3	Článek 5
Článek 4	Článek 6
Článek 5	-
Článek 6	-
Čl. 7 odst. 1	Čl. 7 odst. 1 a 2
Čl. 7 odst. 2	Čl. 7 odst. 4
Čl. 7 odst. 3	Čl. 7 odst. 3
Čl. 8 odst. 1 až 5	Čl. 8 odst. 1 až 5
Čl. 8 odst. 6	Čl. 13 odst. 4
Čl. 8 odst. 7	Čl. 8 odst. 6
Čl. 9 odst. 1, 2 a 3	Čl. 10 odst. 1, 2 a 3
Čl. 9 odst. 4	Čl. 10 odst. 9
Čl. 9 odst. 5	Čl. 10 odst. 10
Čl. 10 odst. 1, 2 a 3 první pododstavec	Čl. 13 odst. 1, 2 a 3
Čl. 10 odst. 3 druhý pododstavec	Čl. 23 odst. 9
Čl. 11 odst. 1	Čl. 14 odst. 1 a 2
Čl. 11 odst. 2	Čl. 14 odst. 3
Čl. 11 odst. 3	Čl. 14 odst. 4 první pododstavec písm. a) až r) a písm. s) a čl. 14 odst. 7
Čl. 11 odst. 4	Čl. 14 odst. 4 první pododstavec písm. r), a druhý pododstavec
Čl. 11 odst. 5	Čl. 14 odst. 8
Čl. 12 odst. 1 až5	Čl. 15 odst. 1 až 5
Článek 13	Článek 17
Čl. 14 odst. 1 a 2	Čl. 21 odst. 1 až 4
Čl. 14 odst. 3	Čl. 23 odst. 1
Čl. 14 odst. 4	Čl. 23 odst. 3
Čl. 14 odst. 5	Čl. 23 odst. 5, 6 a 8

Směrnice (EU) 2016/1148	Tato směrnice
Čl. 14 odst. 6	Čl. 23 odst. 7
Čl. 14 odst. 7	Čl. 23 odst. 11
Čl. 15 odst. 1	Čl. 31 odst. 1
Čl. 15 odst. 2 první pododstavec, písm. a)	Čl. 32 odst. 2 písm. e)
Čl. 15 odst. 2 první pododstavec, písm. b)	Čl. 32 odst. 2 písm. g)
Čl. 15 odst. 2 druhý pododstavec	Čl. 32 odst. 3
Čl. 15 odst. 3	Čl. 32 odst. 4 písm. b)
Čl. 15 odst. 4	Čl. 31 odst. 3
Čl. 16 odst. 1 a 2	Čl. 21 odst. 1 až 4
Čl. 16 odst. 3	Čl. 23 odst. 1
Čl. 16 odst. 4	Čl. 23 odst. 3
Čl. 16 odst. 5	-
Čl. 16 odst. 6	Čl. 23 odst. 6
Čl. 16 odst. 7	Čl. 23 odst. 7
Čl. 16 odst. 8 a 9	Čl. 21 odst. 5 a čl. 23 odst. 11
Čl. 16 odst. 10	-
Čl. 16 odst. 11	Čl. 2 odst. 1, 2 a 3
Čl. 17 odst. 1	Čl. 33 odst. 1
Čl. 17 odst. 2 písm. a)	Čl. 32 odst. 2 písm. e)
Čl. 17 odst. 2 písm. b)	Čl. 32 odst. 4 písm. b)
Čl. 17 odst. 3	Čl. 37 odst. 1 písm. a) a b)
Čl. 18 odst. 1	Čl. 26 odst. 1 písm. b) a čl. 26 odst. 2
Čl. 18 odst. 2	Čl. 26 odst. 3
Čl. 18 odst. 3	Čl. 26 odst. 4
Článek 19	Článek 25
Článek 20	Článek 30
Článek 21	Článek 36
Čl. 22	Čl. 39
Článek 23	Článek 40
Článek 24	-
Článek 25	Článek 41
Článek 26	Článek 45
Článek 27	Článek 46
Příloha I bod 1	Čl. 11 odst. 1
Příloha I bod 2 písm. a) body i) až iv)	Čl. 11 odst. 2 písm. a) až d)

Směrnice (EU) 2016/1148	Tato směrnice
Příloha I bod 2 písm. a) bod v)	Čl. 11 odst. 2 písm. f)
Příloha I bod 2 písm. b)	Čl. 11 odst. 4
Příloha I bod 2 písm. c) body i) a ii)	Čl. 11 odst. 5 písm. a)
Příloha II	Příloha I
Příloha III body 1 a 2	Příloha II bod 6
Příloha III bod 3	Příloha I bod 8