EVROPSKÁ UNIE

EVROPSKÝ PARLAMENT,R

ADA

Brusel, 17. listopadu 2022
(OR. en)

2020/0359(COD) **PE-CONS 32/22**

CYBER 239
TELECOM 295
CSC 290
CSCI 97
DATAPROTECT 202
JAI 946
MI 510
CODEC 991

LEGISLATIVNÍ AKTY A JINÉ NÁSTROJE

Předmět:	SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v celé Unii, kterým se mění nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a zrušuje směrnice (EU) 2016/1148 (směrnice NIS 2).

SMĚRNICE (EU) 2022/...
EVROPSKÉHO PARLAMENTU A RADY

...

o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v celé Unii, kterým se mění nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a zrušuje 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 předání návrhu legislativního aktu vnitrostátním parlamentům, s

ohledem na stanovisko Evropské centrální banky1,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru2, po

konzultaci s Výborem regionů,

v souladu s řádným legislativním postupem3,

---

1 C 233, 16.6.2022, s. 22.
2 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 .....

vzhledem k tomu, že:

(1) Cílem směrnice Evropského parlamentu a Rady (EU) 2016/11481 bylo vybudovat schopnosti kybernetické bezpečnosti v celé Unii, zmírnit hrozby pro síťové a informační systémy používané k poskytování základních služeb v klíčových odvětvích a zajistit kontinuitu těchto služeb v případě incidentů, a přispět tak k bezpečnosti Unie a k účinnému fungování její ekonomiky a společnosti.

(2) Od vstupu směrnice (EU) 2016/1148 v platnost bylo dosaženo významného pokroku při zvyšování úrovně kybernetické odolnosti Unie. Přezkum uvedené směrnice ukázal, že posloužila jako katalyzátor institucionálního a regulačního přístupu ke kybernetické bezpečnosti v Unii a připravila půdu pro významnou změnu myšlení. Uvedená směrnice zajistila dokončení vnitrostátních rámců bezpečnosti sítí a informačních systémů tím, že stanovila vnitrostátní strategie bezpečnosti sítí a informačních systémů a vytvořila vnitrostátní kapacity a zavedla regulační opatření, která se vztahují na základní infrastruktury a subjekty určené jednotlivými členskými státy.
Směrnice (EU) 2016/1148 rovněž přispěla ke spolupráci na úrovni Unie prostřednictvím zřízení skupiny pro spolupráci a sítě národních týmů pro reakci na počítačové bezpečnostní incidenty. Bez ohledu na tyto úspěchy se přezkum
Směrnice (EU) 2016/1148 odhalila vnitřní nedostatky, které jí brání účinně řešit současné a vznikající výzvy v oblasti kybernetické bezpečnosti.

[1] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních pro vysokou společnou úroveň bezpečnosti sítí a informačních systémů v celé Unii (Úř. věst. L 194, 19.7.2016, s. 1).

(3) S rychlou digitální transformací a propojením společnosti, včetně přeshraniční výměny, se síťové a informační systémy staly ústředním prvkem každodenního života. Tento vývoj vedl k rozšíření prostředí kybernetických hrozeb a přinesl nové výzvy, které vyžadují přizpůsobené, koordinované a inovativní reakce ve všech členských státech. Počet, rozsah, sofistikovanost, četnost a dopad incidentů se zvyšuje a představuje velkou hrozbu pro fungování síťových a informačních systémů. V důsledku toho mohou incidenty bránit výkonu hospodářských činností na vnitřním trhu, způsobovat finanční ztráty, podkopávat důvěru uživatelů a způsobovat velké škody hospodářství a společnosti Unie. Připravenost a účinnost kybernetické bezpečnosti jsou proto nyní pro řádné fungování vnitřního trhu zásadnější než kdy dříve. Kybernetická bezpečnost je navíc klíčovým faktorem, který umožňuje mnoha kritickým odvětvím úspěšně přijmout digitální transformaci a plně využít hospodářských, sociálních a udržitelných přínosů digitalizace.

(4) Právním základem směrnice (EU) 2016/1148 byl článek 114 Smlouvy o fungování Evropské unie (SFEU), jehož cílem je vytvoření a fungování vnitřního trhu posílením opatření pro sbližování vnitrostátních předpisů. Požadavky na kybernetickou bezpečnost kladené na subjekty poskytující služby nebo vykonávající hospodářsky významné činnosti se v jednotlivých členských státech značně liší, pokud jde o typ požadavku, míru jeho podrobnosti a způsob dohledu. Tyto rozdíly s sebou nesou dodatečné náklady a způsobují potíže subjektům, které nabízejí zboží nebo služby přes hranice. Požadavky uložené jedním členským státem, které se liší od požadavků uložených jiným členským státem, nebo jsou s nimi dokonce v rozporu, mohou tyto přeshraniční činnosti podstatně ovlivnit. Kromě toho je pravděpodobné, že možnost nevhodného návrhu nebo provádění požadavků na kybernetickou bezpečnost v jednom členském státě bude mít dopady na úroveň kybernetické bezpečnosti ostatních členských států, zejména vzhledem k intenzitě přeshraniční výměny. Přezkum směrnice (EU) 2016/1148 ukázal velké rozdíly v jejím provádění členskými státy, a to i pokud jde o její oblast působnosti, jejíž vymezení bylo do značné míry ponecháno na uvážení členských států. Směrnice (EU) 2016/1148 rovněž ponechávala členským státům velmi široký prostor pro uvážení, pokud jde o provádění v ní stanovených povinností v oblasti bezpečnosti a hlášení incidentů. Tyto povinnosti byly proto na vnitrostátní úrovni prováděny značně odlišnými způsoby. K podobným rozdílům dochází i při provádění ustanovení směrnice (EU) 2016/1148 o dohledu a prosazování.

(5) Všechny tyto rozdíly vedou k roztříštěnosti vnitřního trhu a mohou mít negativní dopad na jeho fungování, zejména na přeshraniční poskytování služeb a úroveň kybernetické odolnosti v důsledku uplatňování různých opatření. V konečném důsledku by tyto rozdíly mohly vést k vyšší zranitelnosti některých členských států vůči kybernetickým hrozbám s možnými vedlejšími účinky v celé Unii. Cílem této směrnice je odstranit tyto velké rozdíly mezi členskými státy, zejména stanovením minimálních pravidel týkajících se fungování koordinovaného regulačního rámce, stanovením mechanismů účinné spolupráce mezi odpovědnými orgány v jednotlivých členských státech, aktualizací seznamu odvětví a činností, na které se vztahují povinnosti v oblasti kybernetické bezpečnosti, a stanovením účinných opravných prostředků a donucovacích opatření, které jsou klíčové pro účinné prosazování těchto povinností. 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 hospodářství, aby bylo zajištěno komplexní pokrytí odvětví a služeb, které mají zásadní význam pro klíčové společenské a hospodářské činnosti na vnitřním trhu. Cílem této směrnice je zejména překonat nedostatky rozlišování mezi provozovateli základních služeb a poskytovateli digitálních služeb, které se ukázalo jako zastaralé, neboť neodráží význam odvětví nebo služeb pro společenské a hospodářské činnosti na vnitřním trhu.

(7) Podle směrnice (EU) 2016/1148 byly členské státy odpovědné za určení subjektů, které splňují kritéria pro to, aby mohly být považovány za provozovatele základních služeb. Aby se odstranily velké rozdíly mezi členskými státy v tomto ohledu a zajistila právní jistota, pokud jde o opatření k řízení rizik v oblasti kybernetické bezpečnosti a oznamovací povinnosti pro všechny příslušné subjekty, mělo by být stanoveno jednotné kritérium, které určí subjekty spadající do oblasti působnosti této směrnice. Toto kritérium by mělo spočívat v uplatnění pravidla velikostního limitu, podle něhož by do oblasti působnosti této směrnice spadaly všechny subjekty, které se kvalifikují jako střední podniky podle článku 2 přílohy doporučení Komise 2003/361/ES1 nebo které překračují stropy pro střední podniky stanovené v odstavci 1 uvedeného článku a které působí v odvětvích a poskytují druhy služeb nebo vykonávají činnosti, na něž se vztahuje tato směrnice. Členské státy by měly rovněž stanovit pro některé malé podniky a mikropodniky, jak jsou definovány v čl. 2 odst. 2
a 3 uvedené přílohy, které splňují zvláštní kritéria, jež ukazují na klíčovou úlohu pro společnost, hospodářství nebo pro určitá odvětví či druhy služeb, které spadají do oblasti působnosti této směrnice.

1 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).

(8) Vyloučení subjektů veřejné správy z oblasti působnosti této směrnice by se mělo vztahovat na subjekty, jejichž činnosti jsou převážně vykonávány v oblasti národní bezpečnosti, veřejné bezpečnosti, obrany nebo prosazování práva, včetně prevence, vyšetřování, odhalování a stíhání trestných činů. Subjekty veřejné správy, jejichž činnosti s těmito oblastmi souvisejí pouze okrajově, by však z oblasti působnosti této směrnice vyloučeny být neměly. Pro účely této směrnice se má za to, že subjekty s regulačními pravomocemi nevykonávají činnosti v oblasti vymáhání práva, a proto nejsou z tohoto důvodu z oblasti působnosti této směrnice vyloučeny. Z oblasti působnosti této směrnice jsou vyloučeny subjekty veřejné správy, které jsou společně zřízeny se třetí zemí v souladu s mezinárodní dohodou. Tato směrnice se nevztahuje na diplomatické a konzulární mise členských států ve třetích zemích ani na jejich síťové a informační systémy, pokud jsou tyto systémy umístěny v prostorách mise nebo jsou provozovány pro uživatele ve třetí zemi.

(9) Členské státy by měly mít možnost přijmout nezbytná opatření k zajištění ochrany základních zájmů národní bezpečnosti, k ochraně veřejného pořádku a veřejné bezpečnosti a k umožnění prevence, vyšetřování, odhalování a stíhání trestných činů. Za tímto účelem by členské státy měly mít možnost vyjmout určité subjekty, které vykonávají činnosti v oblasti národní bezpečnosti, veřejné bezpečnosti, obrany nebo vymáhání práva, včetně prevence, vyšetřování, odhalování a stíhání trestných činů, z určitých povinností stanovených v této směrnici, pokud jde o tyto činnosti. Pokud subjekt poskytuje služby výhradně subjektu veřejné správy, který je vyloučen z oblasti působnosti této směrnice, měly by mít členské státy možnost vyjmout tento subjekt z některých povinností stanovených v této směrnici, pokud jde o tyto služby. Kromě toho by žádný členský stát neměl být povinen poskytovat informace, jejichž zveřejnění by bylo v rozporu se základními zájmy jeho národní bezpečnosti, veřejné bezpečnosti nebo obrany. V této souvislosti by měla být zohledněna pravidla Unie nebo vnitrostátní pravidla pro ochranu utajovaných informací, dohody o zachování mlčenlivosti a neformální dohody o zachování mlčenlivosti, jako je například protokol "semafor". Protokol "semafor" je třeba chápat jako prostředek pro poskytování informací o případných omezeních s ohledem na další šíření informací. Používá se téměř ve všech týmech pro reakci na počítačové bezpečnostní incidenty (CSIRT) a v některých střediscích pro analýzu a sdílení informací.

(10) Ačkoli se tato směrnice vztahuje na subjekty, které vykonávají činnosti v oblasti výroby elektřiny z jaderných elektráren, některé z těchto činností mohou souviset s národní bezpečností. V takovém případě by měl mít členský stát možnost vykonávat svou odpovědnost za ochranu národní bezpečnosti s ohledem na tyto činnosti, včetně činností v rámci jaderného hodnotového řetězce, v souladu se Smlouvami.

(11) Některé subjekty vykonávají činnosti v oblasti 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. 910/20141 , by měli spadat do oblasti působnosti této směrnice, aby byla zajištěna stejná úroveň bezpečnostních požadavků a dohledu, jaká byla dříve stanovena v uvedeném nařízení ve vztahu k poskytovatelům služeb vytvářejících důvěru. V souladu s vyloučením některých specifických služeb z působnosti nařízení (EU) č. 910/2014 by se tato směrnice neměla vztahovat na poskytování služeb vytvářejících důvěru, které jsou využívány výhradně v rámci uzavřených systémů vyplývajících z vnitrostátního práva nebo z dohod mezi vymezeným okruhem účastníků.

1 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 definovaní ve směrnici Evropského parlamentu a Rady 97/67/ES1 , včetně poskytovatelů kurýrních služeb, by měli podléhat této směrnici, pokud poskytují alespoň jeden z kroků poštovního dodacího řetězce, zejména vybírání, třídění, přepravu nebo distribuci poštovních zásilek, včetně služeb vyzvedávání, přičemž se zohlední míra jejich závislosti na síťových a informačních systémech. Přepravní služby, které nejsou poskytovány ve spojení s jedním z těchto kroků, by měly být z oblasti působnosti poštovních služeb vyloučeny.

(13) Vzhledem k zesílení a zvýšené sofistikovanosti kybernetických hrozeb by členské státy měly usilovat o zajištění toho, aby subjekty, které jsou vyloučeny z oblasti působnosti této směrnice, dosáhly vysoké úrovně kybernetické bezpečnosti, a podporovat provádění rovnocenných opatření pro řízení rizik v oblasti kybernetické bezpečnosti, která odrážejí citlivou povahu těchto subjektů.

1 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).

(14) Na jakékoli zpracování osobních údajů podle této směrnice se vztahuje právo Unie v oblasti ochrany údajů a právo Unie v oblasti ochrany soukromí. Touto směrnicí není dotčeno zejména nařízení Evropského parlamentu a Rady (EU) 2016/6791 a směrnice Evropského parlamentu a Rady 2002/58/ES2. Tato směrnice by proto neměly být dotčeny mimo jiné úkoly a pravomoci orgánů příslušných k monitorování dodržování platného práva Unie v oblasti ochrany údajů a práva Unie v oblasti ochrany soukromí.

(15) Subjekty, které spadají do oblasti působnosti této směrnice pro účely dodržování opatření k řízení rizik v oblasti kybernetické bezpečnosti a ohlašovacích povinností, by měly být rozděleny do dvou kategorií, a to na zásadní a významné subjekty, což odráží míru jejich zásadního významu z hlediska jejich odvětví nebo druhu služeb, které poskytují, jakož i jejich velikost. V tomto ohledu by měla být náležitě zohledněna veškerá relevantní odvětvová posouzení rizik nebo případné pokyny příslušných orgánů. Režimy dohledu a vymáhání pro tyto dvě kategorie subjektů by měly být diferencovány, aby byla zajištěna spravedlivá rovnováha mezi požadavky a povinnostmi založenými na riziku na jedné straně a administrativní zátěží vyplývající z dohledu nad dodržováním předpisů na straně druhé.

---

1 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).

2 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).

(16) Aby se předešlo tomu, že subjekty, které mají partnerské podniky nebo které jsou propojenými podniky, budou považovány za základní nebo významné subjekty v případech, kdy by to bylo nepřiměřené, mohou členské státy při uplatňování čl. 6 odst. 2 přílohy doporučení 2003/361/ES zohlednit míru nezávislosti subjektu ve vztahu k jeho partnerským nebo propojeným podnikům. Členské státy mohou zejména zohlednit skutečnost, že subjekt je nezávislý na svých partnerských nebo propojených podnicích, pokud jde o síť a informační systémy, které tento subjekt používá při poskytování svých služeb, a pokud jde o služby, které subjekt poskytuje. Na tomto základě mohou členské státy případně usoudit, že takový subjekt nelze považovat za střední podnik podle článku 2 přílohy doporučení 2003/361/ES nebo že nepřekračuje stropy pro střední podnik stanovené v odstavci 1 uvedeného článku, pokud by po zohlednění míry nezávislosti tohoto subjektu nebyl tento subjekt považován za střední podnik nebo by nepřekročil tyto stropy, pokud by byly zohledněny pouze jeho vlastní údaje. Tím nejsou dotčeny povinnosti partnerských a propojených podniků, které spadají do oblasti působnosti této směrnice, stanovené v této směrnici.

(17) Členské státy by měly mít možnost rozhodnout, že subjekty, které byly před vstupem této směrnice v platnost označeny jako provozovatelé základních služeb v souladu s Směrnice (EU) 2016/1148 se považují za základní subjekty.

(18) Aby byl zajištěn jasný přehled o subjektech, které spadají do oblasti působnosti této směrnice, měly by členské státy vytvořit seznam základních a důležitých subjektů a subjektů poskytujících služby registrace doménových jmen. Za tímto účelem by členské státy měly požadovat, aby subjekty předkládaly příslušným orgánům alespoň následující informace, a to název, adresu a aktuální kontaktní údaje, včetně e-mailových adres, IP rozsahů a telefonních čísel subjektu, a případně příslušné odvětví a pododvětví uvedené v přílohách, jakož i případně seznam členských států, v nichž poskytují služby spadající do oblasti působnosti této směrnice. Za tímto účelem Komise za pomoci Agentury Evropské unie pro kybernetické bezpečnosti (ENISA), by měla bez zbytečného odkladu poskytnout pokyny a šablony týkající se povinnosti předkládat informace. Aby se usnadnilo sestavování a aktualizace seznamu základních a významných subjektů, jakož i subjektů poskytujících služby registrace doménových jmen, měly by mít členské státy možnost zavést vnitrostátní mechanismy, aby se subjekty mohly registrovat samy. Pokud na vnitrostátní úrovni existují registry, mohou členské státy rozhodnout o vhodných mechanismech, které umožní identifikaci subjektů spadajících do oblasti působnosti této směrnice.

(19) Členské státy by měly být odpovědné za to, že Komisi předloží alespoň počet základních a významných subjektů pro každé odvětví a pododvětví uvedené v přílohách, jakož i příslušné informace o počtu určených subjektů a ustanovení z těch, která jsou stanovena v této směrnici, na jejichž základě byly určeny, a o druhu služby, kterou poskytují. Členské státy se vyzývají, aby si s Komisí vyměňovaly informace o základních a významných subjektech a v případě rozsáhlého kybernetického bezpečnostního incidentu i příslušné informace, jako je název dotčeného subjektu.

(20) Komise by měla ve spolupráci se skupinou pro spolupráci a po konzultaci s příslušnými zúčastněnými stranami poskytnout pokyny k provádění kritérií použitelných na mikropodniky a malé podniky pro posouzení, zda spadají do oblasti působnosti této směrnice. Komise by rovněž měla zajistit, aby byly mikropodnikům a malým podnikům, které spadají do oblasti působnosti této směrnice, poskytnuty příslušné pokyny. Komise by měla s pomocí členských států poskytnout mikropodnikům a malým podnikům v tomto ohledu informace.

(21) Komise by mohla poskytnout pokyny, které by členským státům pomohly při provádění ustanovení této směrnice o oblasti působnosti a při posuzování přiměřenosti opatření, která mají být přijata podle této směrnice, zejména pokud jde o subjekty se složitými obchodními modely nebo provozními prostředími, kdy subjekt může současně splňovat kritéria přiřazená jak základním, tak významným subjektům nebo může současně vykonávat činnosti, z nichž některé spadají do oblasti působnosti a některé jsou z ní vyloučeny.
této směrnice.

(22) Tato směrnice stanoví základní pravidla pro opatření k řízení rizik v oblasti kybernetické bezpečnosti a povinnosti podávání zpráv v odvětvích, která spadají do její působnosti. Aby se předešlo roztříštěnosti ustanovení právních aktů Unie týkajících se kybernetické bezpečnosti, měla by Komise v případech, kdy se má za to, že k zajištění vysoké úrovně kybernetické bezpečnosti v celé Unii jsou nezbytné další odvětvové právní akty Unie týkající se opatření k řízení rizik v oblasti kybernetické bezpečnosti a oznamovacích povinností, posoudit, zda by taková další ustanovení mohla být stanovena v prováděcím aktu podle této směrnice. Pokud by takový prováděcí akt nebyl pro tento účel vhodný, mohly by k zajištění vysoké úrovně kybernetické bezpečnosti v celé Unii přispět odvětvové právní akty Unie, které by plně zohledňovaly specifika a složitost dotčených odvětví. Za tímto účelem tato směrnice nevylučuje přijetí dalších odvětvových právních aktů Unie, které se budou zabývat kybernetickou bezpečností.
opatření k řízení rizik a povinnosti podávat zprávy, které náležitě zohledňují potřebu komplexního a konzistentního rámce kybernetické bezpečnosti. Touto směrnicí nejsou dotčeny stávající prováděcí pravomoci, které byly Komisi svěřeny v řadě odvětví, včetně dopravy a energetiky.

(23) Pokud odvětvový právní akt Unie obsahuje ustanovení, která vyžadují, aby základní nebo významné subjekty přijaly opatření k řízení rizik v oblasti kybernetické bezpečnosti nebo aby oznamovaly významné incidenty, a pokud jsou tyto požadavky svým účinkem přinejmenším rovnocenné povinnostem stanoveným v této směrnici, měla by se na tyto subjekty vztahovat tato ustanovení, včetně ustanovení o dohledu a prosazování. Pokud se odvětvový právní akt Unie nevztahuje na všechny subjekty v určitém odvětví spadajícím do oblasti působnosti této směrnice, měla by se příslušná ustanovení této směrnice nadále vztahovat na subjekty, na které se tento akt nevztahuje.

(24) Pokud ustanovení odvětvového právního aktu Unie vyžadují, aby zásadní nebo důležité subjekty plnily ohlašovací povinnosti, které jsou svým účinkem přinejmenším rovnocenné ohlašovacím povinnostem stanoveným v této směrnici, měla by být zajištěna konzistentnost a účinnost zpracování oznámení o událostech. Za tímto účelem by ustanovení týkající se oznámení incidentů v odvětvovém právním aktu Unie měla poskytovat týmům CSIRT, příslušným orgánům nebo jednotným kontaktním místům pro kybernetickou bezpečnost (dále jen "jednotná kontaktní místa") podle této směrnice okamžitý přístup k oznámením incidentů podaným v souladu s odvětvovým právním aktem Unie. Tento okamžitý přístup lze zajistit zejména tehdy, pokud jsou oznámení o incidentech bez zbytečného odkladu předávána CSIRT, příslušnému orgánu nebo jednotnému kontaktnímu místu podle této směrnice. Členské státy by měly případně zavést mechanismus automatického a přímého hlášení, který zajistí systematické a okamžité sdílení informací s CSIRT, příslušnými orgány nebo jednotnými kontaktními místy, pokud jde o vyřizování takových oznámení o incidentech. Pro účely zjednodušení hlášení a zavedení mechanismu automatického a přímého hlášení by členské státy mohly v souladu s odvětvovým právním aktem Unie využívat jediné vstupní místo.

(25) Odvětvové právní akty Unie, které stanoví opatření pro řízení rizik v oblasti kybernetické bezpečnosti nebo oznamovací povinnosti, které jsou svým účinkem přinejmenším rovnocenné opatřením stanoveným v této směrnici, by mohly stanovit, že příslušné orgány podle těchto aktů vykonávají své pravomoci v oblasti dohledu a prosazování práva ve vztahu k těmto opatřením nebo povinnostem s pomocí příslušných orgánů podle této směrnice. Dotčené příslušné orgány by za tímto účelem mohly uzavřít dohody o spolupráci. Tato ujednání o spolupráci by mohla mimo jiné stanovit postupy týkající se koordinace činností v oblasti dohledu, včetně postupů vyšetřování a kontrol na místě v souladu s vnitrostátním právem, a mechanismus výměny relevantních informací o dohledu a prosazování mezi příslušnými orgány, včetně přístupu k informacím souvisejícím s kybernetickým prostředím, které si příslušné orgány vyžádají podle této směrnice.

(26) Pokud odvětvové právní akty Unie vyžadují nebo motivují subjekty k oznamování významných kybernetických hrozeb, měly by členské státy rovněž podporovat sdílení významných kybernetických hrozeb s CSIRT, příslušnými orgány nebo jednotnými kontaktními místy podle této směrnice, aby se zajistila vyšší úroveň informovanosti těchto subjektů o kybernetických hrozbách a aby mohly účinně a včas reagovat, pokud se významné kybernetické hrozby naplní.

(27) Budoucí odvětvové právní akty Unie by měly náležitě zohlednit definice a rámec dohledu a prosazování stanovený v této směrnici.

(28) Nařízení Evropského parlamentu a Rady (EU) .../...1+ by mělo být považováno za odvětvový právní akt Unie ve vztahu k této směrnici, pokud jde o finanční subjekty. Namísto ustanovení této směrnice by se měla použít ustanovení nařízení (EU) .../...++ **týkající** se řízení rizik v oblasti informačních a komunikačních technologií (IKT), řízení incidentů souvisejících s IKT, a zejména hlášení závažných incidentů souvisejících s IKT, jakož i ustanovení o testování digitální provozní odolnosti, dohodách o sdílení informací a rizicích souvisejících s IKT pro třetí strany. Členské státy by proto neměly uplatňovat ustanovení této směrnice týkající se povinností v oblasti řízení rizik v oblasti kybernetické bezpečnosti a podávání zpráv a dohledu a vymáhání práva na finanční subjekty, na které se vztahuje Nařízení (EU) .../... ++. Současně je důležité udržovat pevný vztah a výměnu informací s finančním sektorem podle této směrnice. Za tímto účelem bylo přijato nařízení (EU) .../... ++ umožňuje evropským orgánům dohledu (ESA) a příslušným orgánům podle uvedeného nařízení účastnit se činností skupiny pro spolupráci, vyměňovat si informace a spolupracovat s jednotnými kontaktními místy, jakož i s CSIRT a příslušnými orgány podle této směrnice. Příslušné orgány podle nařízení (EU) .../... ++ by rovněž měly předávat podrobnosti o závažných incidentech souvisejících s IKT a případně o významných kybernetických hrozbách týmům CSIRT, příslušným orgánům nebo jednotným kontaktním místům podle této směrnice. Toho lze dosáhnout tím, že se zajistí okamžitý přístup k oznámením o incidentech a jejich předávání buď přímo, nebo prostřednictvím jednotného kontaktního místa. Kromě toho by členské státy měly i nadále zahrnovat finanční sektor do svých strategií kybernetické bezpečnosti a CSIRT mohou do své činnosti zahrnout i finanční sektor.

---

1 Nařízení Evropského parlamentu a Rady (EU) .../... ze dne ... o provozní digitální 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 (Úř. věst. L ...., ... , s.).

\+ Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)) a do poznámky pod čarou vložte číslo, datum a odkaz na Úřední věstník uvedeného nařízení.

++ Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

(29) Aby se předešlo mezerám mezi povinnostmi v oblasti kybernetické bezpečnosti uloženými subjektům v odvětví letectví nebo jejich zdvojování, měly by vnitrostátní orgány podle nařízení Evropského parlamentu a Rady (ES) č. 300/20081 a (EU) 2018/11392 a příslušné orgány podle této směrnice spolupracovat v souvislosti s prováděním opatření pro řízení rizik v oblasti kybernetické bezpečnosti a dohledem nad dodržováním těchto opatření na vnitrostátní úrovni. Splnění bezpečnostních požadavků stanovených v nařízeních (ES) č. 300/2008 a (EU) 2018/1139 a v příslušných aktech v přenesené pravomoci a prováděcích aktech přijatých podle těchto nařízení by mohly příslušné orgány podle této směrnice považovat za splnění odpovídajících požadavků stanovených v této směrnici.

1 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).

2 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 a o změně 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 o zrušení nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 (Úř. věst.8.2018, p. 1).

(30) Vzhledem k provázanosti kybernetické bezpečnosti a fyzické bezpečnosti subjektů by měl být zajištěn soudržný přístup mezi směrnicí Evropského parlamentu a Rady (EU) .../...1+ a touto směrnicí. Za tímto účelem by měly subjekty označené jako kritické subjekty podle směrnice (EU) .../... [++] by měly být považovány za zásadní subjekty podle této směrnice. Kromě toho by každý členský stát měl zajistit, aby jeho vnitrostátní strategie kybernetické bezpečnosti stanovila politický rámec pro posílenou koordinaci v rámci daného členského státu mezi jeho příslušnými orgány podle této směrnice a orgány podle směrnice (EU) .../.....[++] v souvislosti se sdílením informací o rizicích, kybernetických hrozbách a incidentech, jakož i o nekybernetických rizicích, hrozbách a incidentech a o výkonu úkolů v oblasti dohledu. Příslušné orgány podle této směrnice a orgány podle směrnice (EU) .../.....[++] by měly bez zbytečného odkladu spolupracovat a vyměňovat si informace, zejména pokud jde o identifikaci kritických subjektů, rizik, kybernetických hrozeb a incidentů, jakož i pokud jde o nekybernetická rizika, hrozby a incidenty ovlivňující kritické subjekty, včetně kybernetických bezpečnostních a fyzických opatření přijatých kritickými subjekty, jakož i výsledků činností dohledu prováděných ve vztahu k těmto subjektům.

---

1 Směrnice Evropského parlamentu a Rady (EU) .../... ze dne ... o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (Úř. věst. L ...., ... , s) .

+ Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)) a do poznámky pod čarou vložte číslo, datum a odkaz na Úř. věst. této směrnice.
51/22 (2020/0365(COD)).

++ Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS.

51/22 (2020/0365(COD)).

Kromě toho, aby se zefektivnily činnosti dohledu mezi příslušnými orgány podle této směrnice a orgány podle směrnice (EU) .../... [+] a s cílem minimalizovat administrativní zátěž pro dotčené subjekty by tyto příslušné orgány měly usilovat o harmonizaci šablon pro oznamování událostí a postupů dohledu. V případě potřeby by příslušné orgány podle směrnice (EU) .../... [+], by měly mít možnost požádat příslušné orgány podle této směrnice, aby vykonávaly své pravomoci v oblasti dohledu a prosazování práva ve vztahu k subjektu, který je označen za kritický subjekt podle směrnice (EU) .../.... [+]. Příslušné orgány podle této směrnice a orgány podle směrnice (EU) .../. [+] by měly za tímto účelem, pokud možno v reálném čase, spolupracovat a vyměňovat si informace.

(31) Subjekty patřící do odvětví digitální infrastruktury jsou v podstatě založeny na síťových a informačních systémech, a proto by se povinnosti uložené těmto subjektům podle této směrnice měly komplexně zabývat fyzickou bezpečností těchto systémů jako součástí jejich opatření pro řízení rizik v oblasti kybernetické bezpečnosti a povinností podávat zprávy. Vzhledem k tomu, že se na tyto záležitosti vztahuje tato směrnice, povinnosti stanovené v kapitolách III, IV a VI směrnice (EU) .../.... [+] **se na** tyto subjekty nevztahují.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS. 51/22 (2020/0365(COD)).

(32) Udržování a ochrana spolehlivého, odolného a bezpečného systému názvů domén (DNS) jsou klíčovými faktory pro zachování integrity internetu a jsou nezbytné pro jeho nepřetržitý a stabilní provoz, na němž závisí digitální ekonomika a společnost. Tato směrnice by se proto měla vztahovat na registry názvů domén nejvyšší úrovně (TLD) a poskytovatele služeb DNS, kterými je třeba rozumět subjekty poskytující veřejně dostupné služby rekurzivního rozlišení doménových jmen pro koncové uživatele internetu nebo autoritativní služby rozlišení doménových jmen 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 vzdálený přístup ke škálovatelnému a pružnému fondu sdílených výpočetních zdrojů, a to i v případech, kdy jsou tyto zdroje rozděleny na více míst. 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 (NaaS).
Modely nasazení cloud computingu by měly zahrnovat soukromý, komunitní, veřejný a hybridní cloud. Služby cloud computingu a modely nasazení mají stejný význam jako definované pojmy služby a modely nasazení
podle normy ISO/IEC 17788:2014. Schopnost uživatele cloud computingu jednostranně si sám poskytovat výpočetní kapacity, jako je například čas na serveru nebo síťové úložiště, bez jakékoli lidské interakce ze strany poskytovatele služeb cloud computingu, lze označit jako správu na vyžádání.

Termín "široký vzdálený přístup" se používá k popisu toho, že cloudové funkce jsou poskytovány prostřednictvím sítě a přístupné prostřednictvím mechanismů podporujících používání různorodých tenkých nebo tlustých klientských platforem, včetně mobilních telefonů, tabletů, notebooků a pracovních stanic. Termín "škálovatelný" označuje výpočetní zdroje, které jsou flexibilně přidělovány poskytovatelem cloudových služeb bez ohledu na geografickou polohu zdrojů, aby bylo možné zvládat výkyvy v poptávce. Termínem "elastický fond" se označují výpočetní zdroje, které jsou poskytovány a uvolňovány podle poptávky s cílem rychle zvyšovat a snižovat dostupné zdroje v závislosti na pracovním zatížení. Termín "sdílený" se používá k popisu výpočetních zdrojů, které jsou poskytovány více uživatelům, kteří sdílejí společný přístup ke službě, ale zpracování probíhá pro každého uživatele zvlášť, ačkoli je služba poskytována ze stejného elektronického zařízení. Termín "distribuovaný" se používá k popisu výpočetních prostředků, které jsou umístěny na různých počítačích nebo zařízeních v síti a které mezi sebou komunikují a koordinují se prostřednictvím předávání zpráv.

(34) Vzhledem k nástupu inovativních technologií a nových obchodních modelů se očekává, že se na interním trhu objeví nové modely služeb a nasazení cloud computingu, které budou reagovat na vyvíjející se potřeby zákazníků. V této souvislosti mohou být služby cloud computingu poskytovány ve vysoce distribuované formě, a to i blíže místu, kde jsou data generována nebo shromažďována, čímž se přechází od tradičního modelu k vysoce distribuovanému modelu
(edge computing).

(35) Služby nabízené poskytovateli služeb datových center nemusí být vždy poskytovány formou služby cloud computingu. Datová centra proto nemusí vždy představovat součást infrastruktury cloud computingu. V zájmu řízení všech rizik, která představují pro bezpečnost sítí a informačních systémů, by se proto tato směrnice měla vztahovat na poskytovatele služeb datových center, které nejsou službami cloud computingu. Pro účely této směrnice,
pojem "služba datového centra" by měl zahrnovat poskytování služby, která zahrnuje struktury nebo skupiny struktur určené k centralizovanému umístění, propojení a provozu zařízení informačních technologií (IT) a síťových zařízení poskytujících služby ukládání, zpracování a přenosu dat spolu se všemi zařízeními a infrastrukturami pro rozvod energie a kontrolu prostředí. Pojem "služba datového centra" by se neměl vztahovat na vnitropodniková datová centra, která vlastní a provozuje dotčený subjekt pro své vlastní účely.

(36) Výzkumné činnosti hrají klíčovou roli při vývoji nových produktů a procesů. Mnoho z těchto činností provádějí subjekty, které výsledky svého výzkumu sdílejí, šíří nebo využívají pro komerční účely. Tyto subjekty proto mohou být důležitými účastníky hodnotových řetězců, což činí bezpečnost jejich sítí a informačních systémů nedílnou součástí celkové kybernetické bezpečnosti vnitřního trhu. Výzkumnými organizacemi by se měly rozumět subjekty, které podstatnou část své činnosti zaměřují na provádění aplikovaného výzkumu nebo experimentálního vývoje ve smyslu Frascati Organizace pro hospodářskou spolupráci a rozvoj (OECD).
Příručka 2015: Pokyny pro shromažďování a vykazování údajů o výzkumu a experimentálním vývoji s cílem využít jejich výsledky pro komerční účely, jako je výroba nebo vývoj výrobku či procesu, poskytování služby nebo jejich uvádění na trh.

(37) Rostoucí vzájemná závislost je důsledkem stále více přeshraniční a vzájemně závislé sítě poskytování služeb využívající klíčové infrastruktury v celé Unii v odvětvích, jako je energetika, doprava, digitální infrastruktura, pitná a odpadní voda, zdravotnictví, některé aspekty veřejné správy, jakož i vesmír, pokud jde o poskytování některých služeb závislých na pozemních infrastrukturách, které vlastní, spravují a provozují buď členské státy, nebo soukromé subjekty, a nevztahuje se tedy na infrastruktury vlastněné, spravované nebo provozované Unií nebo jejím jménem v rámci jejího vesmírného programu. Tyto vzájemné závislosti znamenají, že jakékoli narušení, i když se zpočátku týká pouze jednoho subjektu nebo jednoho odvětví, může mít kaskádové účinky v širším měřítku a může mít za následek dalekosáhlé a dlouhodobé negativní dopady na poskytování služeb na celém vnitřním trhu. Intenzivnější kybernetické útoky během pandemie COVID-19 ukázaly zranitelnost stále více vzájemně závislých společností tváří v tvář
rizika s nízkou pravděpodobností.

(38) Vzhledem k rozdílům ve vnitrostátních strukturách řízení a v zájmu ochrany již existujících odvětvových opatření nebo orgánů dohledu a regulace Unie by členské státy měly mít možnost určit nebo zřídit jeden nebo více příslušných orgánů odpovědných za kybernetickou bezpečnost a za úkoly dohledu podle této směrnice.

(39) Aby se usnadnila přeshraniční spolupráce a komunikace mezi orgány a umožnilo se účinné provádění této směrnice, je nezbytné, aby každý členský stát určil jediné kontaktní místo odpovědné za koordinaci otázek týkajících se bezpečnosti sítí a informačních systémů a přeshraniční spolupráce na úrovni Unie.

(40) Jednotná kontaktní místa by měla zajistit účinnou přeshraniční spolupráci s příslušnými orgány ostatních členských států a případně s Komisí.
a ENISA. Jednotná kontaktní místa by proto měla mít za úkol předávat oznámení o významných incidentech s přeshraničním dopadem jednotným kontaktním místům ostatních dotčených členských států na žádost CSIRT nebo příslušného orgánu. Na vnitrostátní úrovni by jednotná kontaktní místa měla umožňovat hladký průběh meziodvětvová spolupráce s dalšími příslušnými orgány. Jednotná kontaktní místa by rovněž mohla být adresáty příslušných informací o incidentech týkajících se finančních subjektů od příslušných orgánů podle nařízení (EU) .../.....[+], které by měly být schopny případně předávat CSIRT nebo příslušným orgánům podle této směrnice.

[+] Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

(41) Členské státy by měly být dostatečně vybaveny, a to jak z hlediska technických, tak organizačních schopností, aby mohly předcházet incidentům a rizikům, odhalovat je, reagovat na ně a zmírňovat je. Členské státy by proto měly zřídit nebo určit jeden či více CSIRT podle této směrnice a zajistit, aby měly odpovídající zdroje a technické schopnosti.
CSIRT by měly splňovat požadavky stanovené v této směrnici, aby byly zaručeny účinné a slučitelné schopnosti řešit incidenty a rizika a aby byla zajištěna účinná spolupráce na úrovni Unie. Členské státy by měly mít možnost určit stávající týmy pro reakci na počítačové hrozby (CERT) jako CSIRT. V zájmu posílení vztahu důvěry mezi subjekty a týmy CSIRT, pokud je tým CSIRT součástí příslušného orgánu, by členské státy měly mít možnost zvážit funkční oddělení operativních úkolů zajišťovaných týmy CSIRT, zejména pokud jde o sdílení informací a pomoc poskytovanou subjektům, od dozorových činností příslušných orgánů.

(42) Úkolem CSIRT je řešení incidentů. To zahrnuje zpracování velkých objemů někdy citlivých dat. Členské státy by měly zajistit, aby týmy CSIRT měly k dispozici infrastrukturu pro sdílení a zpracování informací, jakož i dobře vybavený personál, který zajistí důvěrnost a důvěryhodnost jejich činnosti. Týmy CSIRT by v tomto ohledu mohly rovněž přijmout kodexy chování.

(43) Pokud jde o osobní údaje, týmy CSIRT by měly být schopny v souladu s nařízením (EU) 2016/679 na žádost zásadního nebo významného subjektu provádět proaktivní skenování sítě a informačních systémů používaných pro poskytování služeb tohoto subjektu. Členské státy by měly případně usilovat o zajištění stejné úrovně technických schopností všech odvětvových CSIRT. Členské státy by měly mít možnost požádat agenturu ENISA o pomoc při vytváření svých CSIRT.

(44) Týmy CSIRT by měly mít možnost na žádost zásadního nebo důležitého subjektu monitorovat jeho aktiva na internetu, a to jak v jeho prostorách, tak mimo ně, aby bylo možné identifikovat, pochopit a řídit celková organizační rizika subjektu, pokud jde o nově zjištěná ohrožení dodavatelského řetězce nebo kritické zranitelnosti. Subjekt by měl být vyzván, aby týmu CSIRT sdělil, zda provozuje rozhraní pro privilegovanou správu, neboť by to mohlo ovlivnit rychlost přijetí zmírňujících opatření.

(45) Vzhledem k významu mezinárodní spolupráce v oblasti kybernetické bezpečnosti by měly mít týmy CSIRT možnost účastnit se kromě sítě CSIRT zřízené touto směrnicí také sítí mezinárodní spolupráce. Za účelem plnění svých úkolů by proto týmy CSIRT a příslušné orgány měly mít možnost vyměňovat si informace, včetně osobních údajů, s národními týmy pro řešení počítačových bezpečnostních incidentů nebo příslušnými orgány třetích zemí za předpokladu, že jsou splněny podmínky podle práva Unie v oblasti ochrany údajů pro předávání osobních údajů do třetích zemí, mimo jiné podmínky článku 49 Nařízení (EU) 2016/679, jsou splněny.

(46) Pro splnění cílů této směrnice a umožnění příslušným orgánům a skupinám CSIRT plnit úkoly stanovené touto směrnicí je nezbytné zajistit odpovídající zdroje. Členské státy mohou na vnitrostátní úrovni zavést mechanismus financování k pokrytí nezbytných výdajů v souvislosti s plněním úkolů veřejných subjektů odpovědných za kybernetickou bezpečnost v 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 nadále přispívat k posilování důvěry a důvěryhodnosti a podporovat rychlou a účinnou operativní spolupráci mezi členskými státy. V zájmu posílení operativní spolupráce na úrovni Unie by síť CSIRT měla zvážit přizvání orgánů a agentur Unie zapojených do politiky kybernetické bezpečnosti, jako je Europol, k účasti na své práci.

(48) Za účelem dosažení a udržení vysoké úrovně kybernetické bezpečnosti by vnitrostátní strategie kybernetické bezpečnosti požadované podle této směrnice měly sestávat z ucelených rámců, které stanoví strategické cíle a priority v oblasti kybernetické bezpečnosti a řízení k jejich dosažení. Tyto strategie se mohou skládat z jednoho nebo více legislativních či nelegislativních nástrojů.

(49) Zásady kybernetické hygieny představují základ pro ochranu infrastruktury sítí a informačních systémů, zabezpečení hardwaru, softwaru a online aplikací a obchodních údajů nebo údajů koncových uživatelů, na které se subjekty spoléhají. Zásady kybernetické hygieny zahrnující společný základní soubor postupů, včetně aktualizací softwaru a hardwaru, změn hesel, správy nových instalací, omezení přístupových účtů na úrovni správce a zálohování dat, umožňují vytvořit proaktivní rámec připravenosti a celkové bezpečnosti a zabezpečení v případě incidentů nebo kybernetických hrozeb. Agentura ENISA by měla sledovat a analyzovat politiky kybernetické hygieny členských států.

(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 využívána ke kybernetickým útokům. Mělo by být vyvinuto úsilí o zvýšení celkového povědomí o rizicích spojených s těmito zařízeními, přičemž hodnocení na úrovni Unie by mohlo pomoci zajistit společné chápání těchto rizik v rámci vnitřního trhu.

(51) Členské státy by měly podporovat využívání veškerých inovativních technologií, včetně umělé inteligence, jejichž použití by mohlo zlepšit odhalování kybernetických útoků a jejich prevenci, což by umožnilo efektivnější přesměrování zdrojů na kybernetické útoky. Členské státy by proto měly ve svých vnitrostátních strategiích kybernetické bezpečnosti podporovat činnosti v oblasti výzkumu a vývoje s cílem usnadnit využívání takových technologií, zejména těch, které se týkají automatizovaných nebo poloautomatizovaných nástrojů v oblasti kybernetické bezpečnosti, a případně sdílení údajů potřebných pro školení uživatelů takových technologií a pro jejich zdokonalování. Používání jakýchkoli inovativních technologií, včetně umělé inteligence, by mělo být v souladu s právem Unie v oblasti ochrany údajů, včetně zásad ochrany údajů, kterými jsou přesnost, minimalizace údajů, spravedlnost a transparentnost, a zabezpečení údajů, jako je nejmodernější šifrování. Měly by se plně využívat požadavky na záměrnou a standardní ochranu údajů stanovené v nařízení (EU) 2016/679.

(52) Nástroje a aplikace kybernetické bezpečnosti s otevřeným zdrojovým kódem mohou přispět k vyšší míře otevřenosti a mohou mít pozitivní dopad na účinnost průmyslových inovací. Otevřené standardy usnadňují interoperabilitu mezi bezpečnostními nástroji, což prospívá bezpečnosti průmyslových subjektů. Open-source nástroje a aplikace kybernetické bezpečnosti mohou využívat širší vývojářskou komunitu, což umožňuje diverzifikaci dodavatelů. Otevřený zdrojový kód může vést k transparentnějšímu procesu ověřování nástrojů souvisejících s kybernetickou bezpečností a komunitou řízený proces odhalování zranitelností. Členské státy by proto měly mít možnost podporovat používání softwaru s otevřeným zdrojovým kódem a otevřených standardů tím, že budou prosazovat politiky týkající se používání otevřených dat a otevřeného zdrojového kódu jako součásti bezpečnosti prostřednictvím transparentnosti. Politiky podporující zavádění a udržitelné využívání nástrojů kybernetické bezpečnosti s otevřeným zdrojovým kódem mají zvláštní význam pro malé a střední podniky, které se potýkají se značnými náklady na jejich zavedení, jež by mohly být minimalizovány snížením potřeby specifických aplikací nebo nástrojů.

(53) Veřejné služby jsou ve městech stále častěji připojovány k digitálním sítím za účelem zlepšení městských dopravních sítí, modernizace zařízení pro zásobování vodou a likvidaci odpadu a zvýšení účinnosti osvětlení a vytápění budov. Tyto digitalizované veřejné služby jsou zranitelné vůči kybernetickým útokům a v případě úspěšného kybernetického útoku hrozí, že kvůli svému propojení poškodí občany ve velkém měřítku. Členské státy by měly v rámci své národní strategie kybernetické bezpečnosti vypracovat politiku, která se bude zabývat rozvojem takových propojených nebo inteligentních měst a jejich možnými dopady na společnost.

(54) V posledních letech se Unie potýká s exponenciálním nárůstem útoků ransomwaru, při nichž malware zašifruje data a systémy a za jejich uvolnění požaduje výkupné. Rostoucí četnost a závažnost útoků ransomwaru může být způsobena několika faktory, jako jsou různé vzory útoků, zločinecké obchodní modely kolem "ransomwaru jako služby" a kryptoměn, požadavky na výkupné a nárůst útoků na dodavatelský řetězec. Členské státy by měly v rámci své vnitrostátní strategie kybernetické bezpečnosti vypracovat politiku, která by se zabývala nárůstem útoků ransomwaru.

(55) Partnerství veřejného a soukromého sektoru (PPP) v oblasti kybernetické bezpečnosti může poskytnout vhodný rámec pro výměnu znalostí, sdílení osvědčených postupů a vytvoření společné úrovně porozumění mezi zúčastněnými stranami. Členské státy by měly podporovat politiky podporující vytváření partnerství veřejného a soukromého sektoru zaměřených na kybernetickou bezpečnost. Tyto politiky by měly mimo jiné objasnit rozsah a zúčastněné strany, model řízení, dostupné možnosti financování a interakci mezi zúčastněnými stranami s ohledem na partnerství veřejného a soukromého sektoru. Partnerství veřejného a soukromého sektoru mohou využít odborných znalostí subjektů ze soukromého sektoru, aby pomohly příslušným orgánům při rozvoji nejmodernějších služeb a procesů, včetně výměny informací, včasného varování, cvičení v oblasti kybernetických hrozeb a incidentů, krizového řízení a plánování odolnosti.

(56) Členské státy by se ve svých vnitrostátních strategiích kybernetické bezpečnosti měly zabývat specifickými potřebami malých a středních podniků v oblasti kybernetické bezpečnosti. Malé a střední podniky představují v celé Unii velké procento průmyslového a obchodního trhu a často mají problém přizpůsobit se novým obchodním postupům v propojenějším světě a digitálnímu prostředí, kdy zaměstnanci pracují z domova a obchody se stále častěji uskutečňují online. Některé malé a střední podniky se potýkají se specifickými problémy v oblasti kybernetické bezpečnosti, jako je nízké kybernetické povědomí, nedostatek
vzdálené zabezpečení IT, vysoké náklady na řešení kybernetické bezpečnosti a zvýšená úroveň hrozeb, jako je ransomware, pro které by měli dostat pokyny a pomoc. Malé a střední podniky se stále častěji stávají terčem útoků na dodavatelský řetězec, protože mají méně důsledná opatření pro řízení rizik v oblasti kybernetické bezpečnosti a řízení útoků a mají omezené bezpečnostní zdroje. Takové útoky na dodavatelský řetězec mají dopad nejen na malé a střední podniky a jejich provoz izolovaně, ale mohou mít i kaskádový efekt na větší útoky na subjekty, kterým poskytovaly dodávky. Členské státy by měly prostřednictvím svých vnitrostátních strategií kybernetické bezpečnosti pomáhat malým a středním podnikům řešit problémy, kterým čelí jejich dodavatelské řetězce.
Členské státy by měly mít kontaktní místo pro malé a střední podniky na celostátní nebo regionální úrovni, které by malým a středním podnikům buď poskytovalo poradenství a pomoc, nebo by je nasměrovalo na příslušné orgány, které by jim poskytly poradenství a pomoc v otázkách souvisejících s kybernetickou bezpečností. Členské státy se rovněž vyzývají, aby mikropodnikům a malým podnikům, které nemají tyto možnosti, nabízely služby, jako je konfigurace webových stránek a umožnění přihlašování.

(57) Členské státy by měly v rámci svých vnitrostátních strategií kybernetické bezpečnosti přijmout politiky na podporu aktivní kybernetické ochrany jako součásti širší obranné strategie. Aktivní kybernetická ochrana představuje spíše než reaktivní reakci prevenci, detekci, monitorování, analýzu a zmírňování narušení bezpečnosti sítě aktivním způsobem v kombinaci s využitím schopností nasazených v síti oběti i mimo ni. To by mohlo zahrnovat nabídku bezplatných služeb nebo nástrojů ze strany členských států určitým subjektům, včetně samoobslužných kontrol, detekčních nástrojů a služeb pro odstraňování útoků. Schopnost rychle a automaticky sdílet a chápat informace a analýzy hrozeb, upozornění na kybernetickou aktivitu a reakční opatření je zásadní pro umožnění jednoty úsilí při úspěšném předcházení, odhalování, řešení a blokování útoků na síťové a informační systémy. Aktivní kybernetická ochrana je založena na defenzivní strategii, která vylučuje ofenzivní opatření.

(58) Vzhledem k tomu, že zneužití zranitelných míst v síťových a informačních systémech může způsobit značné narušení a škody, je rychlá identifikace a náprava těchto zranitelných míst důležitým faktorem pro snížení rizika. Subjekty, které vyvíjejí nebo spravují síťové a informační systémy, by proto měly zavést vhodné postupy pro řešení zranitelností v případě jejich odhalení. Vzhledem k tomu, že zranitelnosti jsou často objevovány a zveřejňovány třetími stranami, měl by výrobce nebo poskytovatel produktů nebo služeb informačních a komunikačních technologií rovněž zavést nezbytné postupy pro přijímání informací o zranitelnostech od třetích stran. V tomto ohledu poskytují mezinárodní normy ISO/IEC 30111 a ISO/IEC 29147 pokyny pro nakládání se zranitelnostmi a jejich zveřejňování. Posílení koordinace mezi fyzickými a právnickými osobami podávajícími hlášení a výrobci nebo poskytovateli produktů nebo služeb IKT je obzvláště důležité pro účely usnadnění dobrovolného rámce zveřejňování zranitelností. Koordinované zveřejňování zranitelností specifikuje strukturovaný proces, jehož prostřednictvím jsou zranitelnosti hlášeny výrobci nebo poskytovateli potenciálně zranitelných produktů ICT nebo služeb ICT způsobem, který mu umožňuje diagnostikovat a odstranit zranitelnost předtím, než jsou podrobné informace o zranitelnosti zveřejněny třetím stranám nebo veřejnosti. Koordinované zveřejňování zranitelností by mělo zahrnovat také koordinaci mezi ohlašující fyzickou nebo právnickou osobou a výrobcem nebo poskytovatelem potenciálně zranitelných produktů ICT nebo služeb ICT, pokud jde o načasování nápravy a zveřejnění zranitelností.

(59) Komise, agentura ENISA a členské státy by měly i nadále podporovat sladění s mezinárodními normami a stávajícími osvědčenými postupy v odvětví v oblasti řízení rizik kybernetické bezpečnosti, například v oblasti 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 vytvořením příslušné vnitrostátní politiky. V rámci své vnitrostátní politiky by členské státy měly usilovat o to, aby v souladu s vnitrostátními právními předpisy v co největší míře řešily problémy, kterým čelí výzkumníci v oblasti zranitelností, včetně jejich možného vystavení trestní odpovědnosti. Vzhledem k tomu, že fyzické a právnické osoby provádějící výzkum zranitelností by mohly být v některých členských státech vystaveny trestní a občanskoprávní odpovědnosti, doporučuje se členským státům, aby přijaly pokyny, pokud jde o nestíhání výzkumníků v oblasti informační bezpečnosti a osvobození od občanskoprávní odpovědnosti za jejich činnost.

(61) Členské státy by měly určit jeden ze svých CSIRT jako koordinátora, který bude v případě potřeby působit jako důvěryhodný prostředník mezi fyzickými nebo právnickými osobami podávajícími hlášení a výrobci nebo poskytovateli produktů nebo služeb IKT, které mohou být zranitelností dotčeny. Úkoly CSIRT určeného jako koordinátor by měly zahrnovat identifikaci a kontaktování dotčených subjektů, pomoc fyzickým nebo právnickým osobám, které zranitelnost ohlašují, vyjednávání o termínech zveřejnění a správu zranitelností, které se týkají více subjektů (koordinované zveřejnění zranitelností více subjekty). Pokud by nahlášená zranitelnost mohla mít významný dopad na subjekty ve více než jednom členském státě, měly by CSIRT určené jako koordinátoři případně spolupracovat v rámci sítě CSIRT.

(62) Přístup ke správným a včasným informacím o zranitelnostech produktů a služeb IKT přispívá k lepšímu řízení rizik kybernetické bezpečnosti. Zdroje veřejně dostupných informací o zranitelnostech jsou důležitým nástrojem pro subjekty a uživatele jejich služeb, ale také pro příslušné orgány a CSIRT. Z tohoto důvodu by agentura ENISA měla zřídit evropskou databázi zranitelností, v níž by subjekty, bez ohledu na to, zda spadají do oblasti působnosti této směrnice, a jejich dodavatelé síťových a informačních systémů, jakož i příslušné orgány a CSIRT mohly dobrovolně zveřejňovat a registrovat veřejně známé zranitelnosti, aby uživatelé mohli přijmout vhodná zmírňující opatření. Cílem této databáze je řešit jedinečné problémy, které představují rizika pro subjekty Unie. Agentura ENISA by dále měla stanovit vhodný postup týkající se procesu zveřejňování, aby subjekty měly čas přijmout zmírňující opatření, pokud jde o jejich zranitelnosti, a využívat nejmodernější opatření pro řízení rizik v oblasti kybernetické bezpečnosti, jakož i strojově čitelné soubory údajů a odpovídající rozhraní. Podporovat kulturu odhalení zranitelností by nemělo mít pro oznamující fyzickou nebo právnickou osobu žádné škodlivé účinky.

(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 zajistila lepší transparentnost, pokud jde o proces zveřejňování před zveřejněním zranitelnosti, a odolnost v případě narušení nebo přerušení poskytování podobných služeb. Aby se v co největší míře zabránilo zdvojování úsilí a usilovalo se o doplňkovost, měla by agentura ENISA prozkoumat možnost uzavření strukturovaných dohod o spolupráci s podobnými registry nebo databázemi, které spadají pod jurisdikci třetích zemí. Agentura ENISA by měla zejména prozkoumat možnost úzké spolupráce s provozovateli systému CVE (Common Vulnerabilities and Exposures).

(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 vypracovat pracovní program. Pracovní program by měl zahrnovat opatření, která má skupina pro spolupráci přijmout k provádění svých cílů a úkolů. Časový rámec pro vypracování prvního pracovního programu podle této směrnice by měl být sladěn s časovým rámcem posledního pracovního programu vypracovaného podle směrnice (EU) 2016/1148, aby se předešlo případným narušením činnosti skupiny pro spolupráci.

(65) Skupina pro spolupráci by měla při vypracovávání pokynů důsledně mapovat vnitrostátní řešení a zkušenosti, posuzovat dopad výstupů skupiny pro spolupráci na vnitrostátní přístupy, diskutovat o problémech při provádění a formulovat konkrétní doporučení, zejména pokud jde o usnadnění sladění provádění této směrnice v členských státech, které je třeba řešit lepším prováděním stávajících pravidel. Skupina pro spolupráci by rovněž mohla zmapovat vnitrostátní řešení s cílem podpořit kompatibilitu řešení kybernetické bezpečnosti uplatňovaných v jednotlivých konkrétních odvětvích v celé Unii. To se týká zejména odvětví, která mají mezinárodní nebo přeshraniční povahu.

(66) Skupina pro spolupráci by měla zůstat flexibilním fórem a měla by být schopna reagovat na měnící se a nové politické priority a výzvy a zároveň zohledňovat dostupnost zdrojů. Mohla by pořádat pravidelná společná setkání s příslušnými soukromými zúčastněnými stranami z celé Unie, na nichž by se projednávaly činnosti prováděné skupinou pro spolupráci a shromažďovaly údaje a podněty týkající se nových politických výzev. Kromě toho by skupina pro spolupráci měla provádět pravidelné hodnocení aktuálního stavu kybernetických hrozeb nebo incidentů, jako je ransomware. V zájmu posílení spolupráce na úrovni Unie by skupina pro spolupráci měla zvážit přizvání příslušných orgánů, institucí, úřadů a agentur Unie zapojených do politiky kybernetické bezpečnosti, jako je Evropský parlament, Europol, Evropský sbor pro ochranu údajů, Agentura Evropské unie pro bezpečnost letectví zřízená nařízením (EU) 2018/1139 a Agentura Evropské unie pro vesmírný program zřízená nařízením Evropského parlamentu a Rady (EU) 2021/6961 , k účasti na své práci.

(67) Příslušné orgány a týmy CSIRT by měly mít možnost účastnit se výměnných programů pro úředníky z jiných členských států, a to ve zvláštním rámci a případně s výhradou požadované bezpečnostní prověrky úředníků účastnících se těchto výměnných programů, aby se zlepšila spolupráce a posílila důvěra mezi členskými státy. Příslušné orgány by měly přijmout nezbytná opatření, aby úředníci z jiných členských států mohli hrát účinnou úlohu v činnostech hostitelského příslušného orgánu nebo hostitelského CSIRT.

[1] Nařízení Evropského parlamentu a Rady (EU) 2021/696 ze dne 28. dubna 2021, kterým se zřizuje kosmický program Unie a 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).

(68) Členské státy by měly přispět k vytvoření rámce EU pro reakci na kybernetické krize, jak je stanoveno v doporučení Komise (EU) 2017/15841, prostřednictvím stávajících sítí spolupráce, zejména sítě evropských styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), sítě CSIRT a skupiny pro spolupráci. EU-CyCLONe a síť CSIRT by měly spolupracovat na základě procedurálních ujednání, která upřesňují podrobnosti této spolupráce a zabraňují zdvojování úkolů. Jednací řád sítě EU-CyCLONe by měl dále upřesňovat ujednání, na jejichž základě by tato síť měla fungovat, včetně rolí sítě, prostředků spolupráce, interakcí s dalšími příslušnými aktéry a šablon pro sdílení informací, jakož i prostředků komunikace. Pokud jde o řešení krizí na úrovni Unie, měly by příslušné strany vycházet z ujednání EU o integrovaném řešení politických krizí podle prováděcího rozhodnutí Rady (EU) 2018/19932 (ujednání IPCR). Komise by za tímto účelem měla využívat proces meziodvětvové koordinace krizí na vysoké úrovni ARGUS. Pokud krize zahrnuje důležitý vnější rozměr nebo rozměr společné bezpečnostní a obranné politiky, měl by být aktivován mechanismus reakce na krize Evropské služby pro vnější činnost.

1 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).

2 Prováděcí rozhodnutí Rady (EU) 2018/1993 ze dne 11. prosince 2018 o integrovaných opatřeních EU pro řešení politických krizí (Úř. věst. L 320, 17.12.2018, s. 28).

(69) V souladu s přílohou doporučení (EU) 2017/1584 by se rozsáhlým kybernetickým bezpečnostním incidentem měl rozumět incident, který způsobí narušení v míře, jež přesahuje schopnost členského státu na něj reagovat, nebo který má významný dopad na nejméně dva členské státy. V závislosti na příčině a dopadu mohou rozsáhlé kybernetické bezpečnostní incidenty eskalovat a přerůst v plnohodnotné krize, které neumožňují řádné fungování vnitřního trhu nebo představují vážné riziko pro veřejnou bezpečnost a bezpečnost subjektů nebo občanů v několika členských státech nebo v Unii jako celku. Vzhledem k tomu, že
rozsáhlý rozsah a ve většině případů přeshraniční povaha těchto událostí by členské státy a příslušné orgány, instituce a jiné subjekty Unie měly spolupracovat na technické, operativní a politické úrovni, aby řádně koordinovaly reakci v celé Unii.

(70) Rozsáhlé kybernetické bezpečnostní incidenty a krize na úrovni Unie vyžadují koordinovaný postup, aby byla zajištěna rychlá a účinná reakce, a to z důvodu vysoké míry vzájemné závislosti mezi odvětvími a členskými státy. Dostupnost síťových a informačních systémů odolných vůči kybernetickým hrozbám a dostupnost, důvěrnost a integrita údajů jsou zásadní pro bezpečnost Unie a ochranu jejích občanů, podniků a institucí před incidenty a kybernetickými hrozbami, jakož i pro posílení důvěry jednotlivců a organizací ve schopnost Unie podporovat a chránit globální, otevřený, svobodný, stabilní a bezpečný kyberprostor založený na lidských právech, základních svobodách, demokracii a právním státě.

(71) EU-CyCLONe by měl fungovat jako prostředník mezi technickou a politickou úrovní při rozsáhlých kybernetických bezpečnostních incidentech a krizích a měl by posílit spolupráci na operativní úrovni a podporovat rozhodování na politické úrovni. Ve spolupráci s Komisí a s ohledem na její pravomoci v oblasti krizového řízení by měl EU-CyCLONe vycházet z poznatků sítě CSIRT a využívat své vlastní kapacity k vytváření analýz dopadů rozsáhlých kybernetických bezpečnostních incidentů a krizí.

(72) Kybernetické útoky jsou přeshraniční povahy a závažný incident může narušit a poškodit kritické informační infrastruktury, na nichž 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/EU1 odpovědná za opatření obecné připravenosti, včetně řízení koordinačního centra pro reakci na mimořádné události a společného komunikačního a informačního systému pro mimořádné události, udržování a dalšího rozvoje situačního povědomí a analytických schopností a vytvoření a řízení schopnosti mobilizovat a vysílat týmy odborníků v případě žádosti o pomoc ze strany členského státu nebo třetí země. Komise rovněž odpovídá za poskytování analytických zpráv pro opatření IPCR podle prováděcího rozhodnutí (EU) 2018/1993, a to i v souvislosti se situačním povědomím a připraveností v oblasti kybernetické bezpečnosti, jakož i za situační povědomí a reakci na krize v oblasti zemědělství, nepříznivých povětrnostních podmínek, mapování a předpovědí konfliktů, systémů včasného varování pro přírodní katastrofy, mimořádných zdravotních situací, dozoru nad infekčními chorobami, zdraví rostlin, chemických událostí, bezpečnosti potravin a krmiv, zdraví zvířat, migrace, cel, jaderných a radiačních mimořádných událostí a energetiky.

1 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).

(73) Unie může případně uzavírat mezinárodní dohody v souladu s článkem 218 Smlouvy o fungování EU se třetími zeměmi nebo mezinárodními organizacemi, které umožňují a organizují jejich účast na konkrétních činnostech skupiny pro spolupráci, sítě CSIRT a EU-CyCLONe. Tyto dohody by měly zajistit zájmy Unie a odpovídající ochranu údajů. To by nemělo bránit právu členských států spolupracovat se třetími zeměmi v oblasti řízení zranitelností a řízení rizik kybernetické bezpečnosti, usnadňovat podávání zpráv a obecné sdílení informací v souladu s právem Unie.

(74) Za účelem usnadnění účinného provádění této směrnice, mimo jiné pokud jde o řízení zranitelností, opatření k řízení rizik v oblasti kybernetické bezpečnosti, povinnosti podávání zpráv a ujednání o sdílení informací v oblasti kybernetické bezpečnosti, mohou členské státy spolupracovat se třetími zeměmi a provádět činnosti, které jsou za tímto účelem považovány za vhodné, včetně výměny informací o kybernetických hrozbách, incidentech, zranitelnostech, nástrojích a metodách, taktikách, technikách a postupech, připravenosti a cvičeních v oblasti krizového řízení kybernetické bezpečnosti, odborné přípravy, budování důvěry a strukturovaných dohody o sdílení informací.

(75) Mělo by být zavedeno vzájemné hodnocení, které pomůže poučit se ze společných zkušeností, posílit vzájemnou důvěru a dosáhnout vysoké společné úrovně kybernetické bezpečnosti. Vzájemná hodnocení mohou vést k cenným poznatkům a doporučením posilujícím celkové schopnosti v oblasti kybernetické bezpečnosti, vytvořit další funkční cestu pro sdílení osvědčených postupů mezi členskými státy a přispět ke zvýšení úrovně vyspělosti členských států v oblasti kybernetické bezpečnosti. Kromě toho by vzájemné hodnocení mělo zohledňovat výsledky podobných mechanismy, jako je systém vzájemného hodnocení sítě CSIRT, a měly by přinášet přidanou hodnotu a zamezit duplicitě. Prováděním vzájemných hodnocení by neměly být dotčeny právní předpisy Unie ani vnitrostátní právní předpisy o ochraně důvěrných nebo utajovaných informací.

(76) Skupina pro spolupráci by měla vytvořit metodiku sebehodnocení pro členské státy, jejímž cílem bude zahrnout faktory, jako je úroveň provádění opatření pro řízení rizik v oblasti kybernetické bezpečnosti a povinnosti podávat zprávy, úroveň schopností a účinnost plnění úkolů příslušných orgánů, operační schopnosti CSIRT, úroveň provádění vzájemné pomoci, úroveň provádění ujednání o sdílení informací v oblasti kybernetické bezpečnosti nebo specifické otázky přeshraniční nebo meziodvětvové povahy. Členské státy by měly být vybízeny k tomu, aby pravidelně prováděly sebehodnocení a aby výsledky sebehodnocení předkládaly a projednávaly s ostatními členskými státy. sebehodnocení v rámci skupiny pro spolupráci.

(77) Odpovědnost za zajištění bezpečnosti sítě a informačního systému leží do značné míry na základních a důležitých subjektech. Měla by být podporována a rozvíjena kultura řízení rizik zahrnující hodnocení rizik a zavádění opatření pro řízení rizik kybernetické bezpečnosti odpovídajících rizikům, kterým čelí.

(78) Opatření pro řízení rizik v oblasti kybernetické bezpečnosti by měla zohledňovat míru závislosti základního nebo významného subjektu na síťových a informačních systémech a zahrnovat opatření pro identifikaci rizik incidentů, prevenci, detekci, reakci na incidenty a zotavení z nich a zmírnění jejich dopadu. Bezpečnost sítí a informačních systémů by měla zahrnovat bezpečnost uložených, přenášených a zpracovávaných údajů. Opatření pro řízení rizik v oblasti kybernetické bezpečnosti by měla zajistit systémovou analýzu s přihlédnutím k lidskému faktoru, aby byl k dispozici úplný obraz o bezpečnosti sítě a informačního systému.

(79) Vzhledem k tomu, že hrozby pro bezpečnost síťových a informačních systémů mohou mít různý původ, měla by opatření pro řízení rizik v oblasti kybernetické bezpečnosti vycházet z přístupu založeného na všech rizicích, jehož cílem je chránit síťové a informační systémy a fyzické prostředí těchto systémů před událostmi, jako je krádež, požár, povodeň, výpadek telekomunikací nebo napájení nebo neoprávněný fyzický přístup a poškození a narušení základního nebo důležitá zařízení subjektu pro zpracování informací a informací, která by mohla ohrozit dostupnost, pravost, integritu nebo důvěrnost uložených, přenášených nebo zpracovávaných dat nebo služeb nabízených síťovými a informačními systémy nebo přístupných jejich prostřednictvím. Opatření pro řízení rizik kybernetické bezpečnosti by se proto měla zabývat také fyzickou bezpečností a bezpečností prostředí síťových a informačních systémů tím, že budou zahrnovat opatření na ochranu těchto systémů před selháním systému, lidskou chybou, škodlivými činy nebo přírodními jevy, a to 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 pro řízení rizik v oblasti kybernetické bezpečnosti zabývat také bezpečností lidských zdrojů a mít zavedeny vhodné politiky řízení přístupu. Tato opatření by měla být v souladu se směrnicí (EU) .../... [+].

+ Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

(80) Za účelem prokázání souladu s opatřeními pro řízení rizik v oblasti kybernetické bezpečnosti a při neexistenci vhodných evropských systémů certifikace kybernetické bezpečnosti přijatých v souladu s nařízením Evropského parlamentu a Rady (EU) 2019/8811 by členské státy měly po konzultaci se skupinou pro spolupráci a Evropskou skupinou pro certifikaci kybernetické bezpečnosti podporovat používání příslušných evropských a mezinárodních norem zásadními a důležitými subjekty nebo mohou vyžadovat, aby subjekty používaly certifikované produkty IKT, služby IKT a procesy IKT.

(81) Aby se předešlo nepřiměřené finanční a administrativní zátěži pro základní a důležité subjekty, měla by být opatření k řízení rizik v oblasti kybernetické bezpečnosti přiměřená rizikům, která představují pro danou síť a informační systém, s přihlédnutím k nejnovějšímu stavu těchto opatření a případně k příslušným evropským a mezinárodním normám, jakož i k nákladům na jejich provedení.

1 Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA (Agentuře Evropské unie pro kybernetickou bezpečnost) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení tohoto

nařízení
Nařízení (EU) č. 526/2013 (akt o kybernetické bezpečnosti) (Úř. věst. L 151, 7.6.2019, s. 15).

(82) Opatření k řízení rizik v oblasti kybernetické bezpečnosti by měla být přiměřená míře vystavení zásadního nebo významného subjektu rizikům a společenskému a hospodářskému dopadu, který by incident měl. Při stanovování opatření k řízení rizik v oblasti kybernetické bezpečnosti přizpůsobených základním a významným subjektům by měla být náležitě zohledněna rozdílná míra vystavení základních a významných subjektů rizikům, jako je kritičnost subjektu, rizika, včetně společenských rizik, kterým je subjekt vystaven, velikost subjektu a pravděpodobnost výskytu incidentů a jejich závažnost, včetně jejich společenského a hospodářského dopadu.

(83) Podstatné a důležité subjekty by měly zajistit bezpečnost sítě a informačních systémů, které používají při své činnosti. Tyto systémy jsou především soukromé sítě a informační systémy, které spravují interní IT pracovníci základních a významných subjektů nebo jejichž zabezpečení bylo zadáno externím dodavatelům. Opatření pro řízení rizik v oblasti kybernetické bezpečnosti a oznamovací povinnosti stanovené v této směrnici by se měly vztahovat na příslušné základní a významné subjekty bez ohledu na to, zda tyto subjekty udržují své sítě a informační systémy interně, nebo jejich údržbu zajišťují externě.

(84) S ohledem na jejich přeshraniční povahu by poskytovatelé služeb DNS, registry názvů 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, on-line vyhledávačů a platforem služeb sociálních sítí a poskytovatelé služeb vytvářejících důvěru měli podléhat vysokému stupni harmonizace na úrovni Unie. Provádění opatření k řízení rizik v oblasti kybernetické bezpečnosti ve vztahu k těmto subjektům by proto měl usnadnit prováděcí akt.

(85) Řešení rizik vyplývajících z dodavatelského řetězce subjektu a jeho vztahů s dodavateli, jako jsou poskytovatelé služeb ukládání a zpracování dat nebo poskytovatelé řízených bezpečnostních služeb a vydavatelé softwaru, je obzvláště důležité vzhledem k častým incidentům, kdy se subjekty staly oběťmi kybernetických útoků a kdy škodlivý Pachatelé byli schopni narušit bezpečnost sítě a informačních systémů subjektu zneužitím zranitelností, které se týkaly produktů a služeb třetích stran. Podstatné a důležité subjekty by proto měly posuzovat a zohledňovat celkovou kvalitu a odolnost produktů a služeb, v nich zakotvená opatření pro řízení rizik kybernetické bezpečnosti a postupy kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje. Zásadní a významné subjekty by měly být zejména vybízeny k tomu, aby do smluvních ujednání se svými přímými dodavateli a poskytovateli služeb začlenily opatření k řízení kybernetických rizik. Tyto subjekty by mohly zvážit rizika plynoucí z dalších úrovní dodavatelů a poskytovatelů služeb.

(86) Mezi poskytovateli služeb hrají zvláště důležitou roli poskytovatelé řízených bezpečnostních služeb v oblastech, jako je reakce na incidenty, penetrační testování, bezpečnostní audity a poradenství, kteří pomáhají subjektům v jejich úsilí o prevenci, odhalování, reakci na incidenty nebo zotavení z nich. Poskytovatelé řízených bezpečnostních služeb se však také sami stávají terčem kybernetických útoků a vzhledem ke své úzké integraci do provozu subjektů představují zvláštní riziko. Podstatné a důležité subjekty by proto měly při výběru poskytovatele řízených bezpečnostních služeb postupovat se zvýšenou pečlivostí.

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

(88) Podstatné a důležité subjekty by se měly zabývat také riziky plynoucími z jejich interakcí a vztahů s ostatními zúčastněnými stranami v rámci širšího ekosystému, a to i s ohledem na boj proti průmyslové špionáži a ochranu obchodních tajemství. Tyto subjekty by měly zejména přijmout vhodná opatření, aby zajistily, 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 k informacím a jejich šíření obecně a zejména o ochranu duševního vlastnictví. Podobně by vzhledem k významu a hodnotě údajů pro činnosti základních a důležitých subjektů měly tyto subjekty, pokud se spoléhají na služby transformace a analýzy údajů od třetích stran, přijmout veškerá vhodná opatření pro řízení rizik v oblasti kybernetické bezpečnosti.

(89) Zásadní a důležité subjekty by měly přijmout celou řadu základních postupů kybernetické hygieny, jako jsou zásady nulové důvěryhodnosti, aktualizace softwaru, konfigurace zařízení, segmentace sítě, správa identit a přístupu nebo informovanost uživatelů, organizovat školení pro své zaměstnance a zvyšovat povědomí o kybernetických hrozbách, phishingu nebo technikách sociálního inženýrství. Dále by tyto subjekty měly vyhodnotit své vlastní schopnosti v oblasti kybernetické bezpečnosti a případně usilovat o integraci technologií zvyšujících kybernetickou bezpečnost, jako je umělá inteligence nebo systémy strojového učení, aby zvýšily své schopnosti a bezpečnost síťových a informačních systémů.

(90) S cílem dále řešit klíčová rizika dodavatelského řetězce a pomoci základním a důležitým subjektům působícím v odvětvích, na něž se vztahuje tato směrnice, vhodně řídit rizika spojená s dodavatelským řetězcem a dodavateli by skupina pro spolupráci ve spolupráci s Komisí a agenturou ENISA a případně po konzultaci s příslušnými zúčastněnými stranami, včetně subjektů z odvětví, měla provádět koordinovaná posouzení bezpečnostních rizik kritických dodavatelských řetězců, jak byla provedena v případě sítí 5G podle doporučení Komise (EU) 2019/5341, s cílem určit podle odvětví kritické služby IKT, systémy IKT nebo produkty IKT, příslušné hrozby a zranitelná místa. Taková koordinovaná posouzení bezpečnostních rizik by měla identifikovat opatření, plány na zmírnění a osvědčené postupy pro boj proti kritickým závislostem, potenciálním jediným bodům selhání, hrozbám, zranitelnostem a dalším rizikům spojeným s dodavatelským řetězcem a měla by zkoumat způsoby, jak dále podporovat jejich širší přijetí zásadními a důležitými subjekty. Potenciální netechnické rizikové faktory, jako je nepatřičný vliv třetí země na dodavatele a poskytovatele služeb, zejména v případě alternativních modelů řízení, zahrnují skryté zranitelnosti nebo zadní vrátka a potenciální systémové narušení dodávek, zejména v případě technologického uzamčení nebo závislosti na poskytovateli.

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

(91) Koordinované posuzování bezpečnostních rizik kritických dodavatelských řetězců by mělo s ohledem na vlastnosti daného odvětví zohledňovat jak technické, tak případně i jiné aspekty,
netechnických faktorů, včetně faktorů definovaných v doporučení (EU) 2019/534, v koordinovaném posouzení rizik kybernetické bezpečnosti sítí 5G a v souboru nástrojů EU pro kybernetickou bezpečnost 5G, na němž se dohodla skupina pro spolupráci. Pro určení dodavatelských řetězců, které by měly být předmětem koordinovaného posouzení bezpečnostních rizik, by měla být zohledněna následující kritéria: (i) rozsah, v jakém zásadní a důležité subjekty využívají konkrétní kritické služby IKT, systémy IKT nebo produkty IKT a spoléhají se na ně; ii) význam konkrétních kritických 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 v průběhu jejich životního cyklu vůči rušivým událostem a v) v případě nově vznikajících služeb IKT, systémů IKT nebo produktů IKT jejich potenciální budoucí význam pro činnost subjektů. Kromě toho by měl být kladen zvláštní důraz na služby ICT, systémy ICT nebo produkty ICT, které podléhají zvláštním požadavkům vyplývajícím ze třetích zemí.

(92) S cílem zefektivnit povinnosti uložené poskytovatelům veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací a poskytovatelům služeb vytvářejících důvěru, které se týkají bezpečnosti jejich sítí a informačních systémů, a umožnit těmto subjektům a příslušným orgánům v rámci Směrnice Evropského parlamentu a Rady (EU) 2018/19721 a nařízení (EU) č. 910/2014, resp. aby mohly využívat právního rámce stanoveného touto směrnicí, včetně určení CSIRT odpovědného za řešení incidentů, účasti dotčených příslušných orgánů na činnosti skupiny pro spolupráci a sítě CSIRT, měly by tyto subjekty spadat do oblasti působnosti této směrnice. Odpovídající ustanovení stanovená v nařízení (EU) č. 910/2014 a směrnici (EU) 2018/1972 týkající se uložení bezpečnostních a oznamovacích požadavků na tyto typy subjektů by proto měla být zrušena. Pravidly týkajícími se oznamovací povinnosti stanovenými v této směrnici by neměla být dotčena Nařízení (EU) 2016/679 a směrnice 2002/58/ES.

[1] Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterým se zavádí evropský kodex elektronických komunikací (Úř. věst. L 321, 17.12.2018, s. 36).

(93) Povinnosti v oblasti 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. Poskytovatelé důvěryhodných služeb by měli být povinni přijmout veškerá vhodná a přiměřená opatření k řízení rizik, která představují jejich služby, a to i ve vztahu ke klientům a spoléhajícím se třetím stranám, a hlásit incidenty podle této směrnice. Tyto povinnosti v oblasti kybernetické bezpečnosti a hlášení by se měly týkat rovněž fyzické ochrany poskytovaných služeb. Požadavky na kvalifikované poskytovatele služeb vytvářejících důvěru stanovené v článku 24 nařízení (EU) č. 910/2014 platí i nadále.

(94) Členské státy mohou svěřit úlohu příslušných orgánů pro svěřenské služby orgánům dohledu podle nařízení (EU) č. 910/2014, aby zajistily pokračování stávajících postupů a navázaly na znalosti a zkušenosti získané při uplatňování uvedeného nařízení. V takovém případě by příslušné orgány podle této směrnice měly s těmito orgány dohledu úzce a včas spolupracovat prostřednictvím výměny relevantních informací, aby byl zajištěn účinný dohled a soulad poskytovatelů služeb vytvářejících důvěru s požadavky stanovenými v této směrnici a ve
Nařízení (EU) č. 910/2014. V příslušných případech by CSIRT nebo příslušný orgán podle této směrnice měl neprodleně informovat orgán dohledu podle
nařízení (EU) č. 910/2014 o jakékoli oznámené významné kybernetické hrozbě nebo incidentu, který má vliv na služby vytvářející důvěru, a o jakémkoli porušení této směrnice poskytovatelem služeb vytvářejících důvěru. Pro účely hlášení mohou členské státy případně využít jednotné vstupní místo zřízené za účelem dosažení společného a automatického hlášení incidentů jak orgánu dohledu podle nařízení (EU) č. 910/2014, tak CSIRT nebo příslušnému orgánu podle této směrnice.

(95) Ve vhodných případech a s cílem zabránit zbytečnému narušení by se při provádění této směrnice měly zohlednit stávající vnitrostátní pokyny přijaté pro provedení pravidel týkajících se bezpečnostních opatření stanovených v článcích 40 a 41 směrnice (EU) 2018/1972, a navázat tak na znalosti a dovednosti, které již byly získány podle směrnice (EU) 2018/1972 v oblasti bezpečnostních opatření a oznamování incidentů. Agentura ENISA může rovněž vypracovat pokyny týkající se bezpečnostních požadavků a oznamovacích povinností pro poskytovatele veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací, aby se usnadnila harmonizace a přechod a minimalizovalo narušení. Členské státy mohou svěřit úlohu příslušných orgánů pro elektronické komunikace vnitrostátním regulačním orgánům v rámci

Směrnice (EU) 2018/1972 s cílem zajistit pokračování stávajících postupů a navázat na znalosti a zkušenosti získané v důsledku provádění směrnice (EU) 2018/1972.

tuto směrnici.

(96) Vzhledem k rostoucímu významu mezilidských komunikačních služeb nezávislých na čísle, jak jsou definovány ve směrnici (EU) 2018/1972, je nutné zajistit, aby tyto služby s ohledem na jejich specifickou povahu a hospodářský význam rovněž podléhaly příslušným bezpečnostním požadavkům. Vzhledem k tomu, že se povrch útoků stále rozšiřuje,
na čísle nezávislé služby mezilidské komunikace, jako jsou služby zasílání zpráv, se stávají rozšířenými vektory útoku. Zlomyslní pachatelé využívají platformy ke komunikaci a lákají oběti k otevření napadených webových stránek, čímž zvyšují pravděpodobnost incidentů zahrnujících zneužití osobních údajů, a tím i bezpečnost síťových a informačních systémů. Poskytovatelé mezilidských komunikačních služeb nezávislých na číslech by měli zajistit úroveň zabezpečení sítí a informačních systémů odpovídající rizikům, která s tím souvisejí. Vzhledem k tomu, že poskytovatelé
interpersonální komunikační služby nezávislé na čísle obvykle nevykonávají skutečnou kontrolu nad přenosem signálů po sítích, lze míru rizik, která pro tyto služby představují, považovat v některých ohledech za nižší než u tradičních služeb elektronických komunikací. Totéž platí pro interpersonální komunikační služby ve smyslu směrnice (EU) 2018/1972, které využívají čísla a které nevykonávají skutečnou kontrolu nad přenosem signálů.

(97) Vnitřní trh je na fungování internetu závislý více než kdy jindy. Služby téměř všech základních a důležitých subjektů jsou závislé na službách poskytovaných prostřednictvím internetu. V zájmu zajištění bezproblémového poskytování služeb poskytovaných základními a důležitými subjekty je důležité, aby všichni poskytovatelé veřejných sítí elektronických komunikací měli zavedena vhodná opatření pro řízení rizik v oblasti kybernetické bezpečnosti a aby v souvislosti s nimi hlásili významné incidenty. Členské státy by měly zajistit, aby byla zachována bezpečnost veřejných sítí elektronických komunikací a aby byly jejich důležité bezpečnostní zájmy chráněny před sabotáží a špionáží. Vzhledem k tomu, že mezinárodní konektivita posiluje a urychluje konkurenceschopnou digitalizaci Unie a jejího hospodářství, měly by být incidenty, které mají vliv na podmořské komunikační kabely, hlášeny na CSIRT nebo případně příslušný orgán. Vnitrostátní strategie kybernetické bezpečnosti by měla případně zohlednit kybernetickou bezpečnost podmořských komunikačních kabelů a zahrnovat zmapování potenciálních rizik kybernetické bezpečnosti a opatření k jejich zmírnění s cílem zajistit co nejvyšší úroveň 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 koncového šifrování, jakož i bezpečnostních koncepcí zaměřených na data, jako je kartografie, segmentace, označování, politika přístupu a řízení přístupu a automatizované rozhodování o přístupu. V případě potřeby by mělo být používání šifrování, zejména end-to-end šifrování, pro poskytovatele veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací povinné v souladu se zásadami standardní bezpečnosti a ochrany soukromí a ochrany soukromí již od návrhu pro účely této směrnice. Používání koncového šifrování by mělo být sladěno s pravomocemi členských států zajistit ochranu jejich základních bezpečnostních zájmů a veřejné bezpečnosti a umožnit prevenci, vyšetřování, odhalování a stíhání trestných činů v souladu s právem Unie. To by však nemělo oslabit end-to-end šifrování, které je klíčovou technologií pro účinnou ochranu dat a soukromí a bezpečnost komunikace.

(99) V zájmu zajištění bezpečnosti veřejných sítí elektronických komunikací a veřejně dostupných služeb elektronických komunikací a zabránění jejich zneužití a manipulaci s nimi by se mělo podporovat používání standardů bezpečného směrování, aby se zajistila integrita a robustnost směrovacích funkcí v celém ekosystému poskytovatelů služeb přístupu k internetu.

(100) V zájmu ochrany funkčnosti a integrity internetu a podpory bezpečnosti a odolnosti DNS by příslušné zúčastněné strany, včetně subjektů soukromého sektoru Unie, poskytovatelů veřejně dostupných služeb elektronických komunikací, zejména poskytovatelů služeb přístupu k internetu, a poskytovatelů internetových vyhledávačů měly být vybízeny k přijetí strategie diverzifikace řešení DNS. Členské státy by dále měly podporovat vývoj a používání veřejné a bezpečné evropské služby DNS resolveru.

(101) Tato směrnice stanoví vícestupňový přístup k hlášení závažných incidentů, aby byla zajištěna správná rovnováha mezi rychlým hlášením, které pomáhá zmírnit potenciální šíření závažných incidentů a umožňuje zásadním a důležitým subjektům vyhledat pomoc, na jedné straně a hloubkovým hlášením, které z jednotlivých incidentů vyvozuje cenné poznatky a postupem času zvyšuje kybernetickou odolnost jednotlivých subjektů i celých odvětví, na straně druhé. V tomto ohledu by tato směrnice měla zahrnovat hlášení incidentů, které by na základě prvotního posouzení provedeného dotčeným subjektem mohly způsobit vážné narušení provozu služeb nebo finanční ztrátu tohoto subjektu nebo ovlivnit jiné fyzické či právnické osoby tím, že způsobí značnou materiální či nemateriální škodu. Toto počáteční posouzení by mělo mimo jiné zohlednit postiženou síť a informační systémy, zejména jejich význam při poskytování služeb daného subjektu, závažnost a technické charakteristiky kybernetické hrozby a případné základní zranitelnosti, které jsou zneužívány, jakož i zkušenosti daného subjektu s podobnými incidenty. Ukazatele, jako je rozsah, v jakém je ovlivněno fungování služby, doba trvání incidentu nebo počet postižených příjemců služeb, by mohly hrát důležitou roli při určování, zda je narušení provozu služby závažné.

(102) Pokud se zásadní nebo důležité subjekty dozvědí o závažné události, měly by být povinny podat včasné varování bez zbytečného odkladu a v každém případě do 24 hodin. Po tomto včasném varování by mělo následovat oznámení o incidentu. Dotčené subjekty by měly podat oznámení o incidentu bez zbytečného odkladu a v každém případě do 72 hodin od okamžiku, kdy se o významném incidentu dozvěděly, a to zejména s cílem aktualizovat informace předložené v rámci včasného varování a uvést prvotní posouzení významného incidentu, včetně jeho závažnosti a dopadu, jakož i ukazatele ohrožení, jsou-li k dispozici. Závěrečná zpráva by měla být předložena nejpozději do jednoho měsíce od oznámení incidentu. Včasné varování by mělo obsahovat pouze informace nezbytné k tomu, aby se CSIRT, případně příslušný orgán, dozvěděl o významném incidentu a aby mohl dotčený subjekt v případě potřeby požádat o pomoc. Toto včasné varování by případně mělo uvádět, zda existuje podezření, že významný incident byl způsoben protiprávním nebo zákeřným jednáním, a zda je pravděpodobné, že bude mít přeshraniční dopad. Členské státy by měly zajistit, aby povinnost předložit toto včasné varování nebo následné oznámení incidentu neodváděla zdroje oznamujícího subjektu od činností souvisejících s řešením incidentů, které by měly být upřednostněny, aby se předešlo tomu, že povinnost hlásit incidenty buď odvede zdroje od řešení závažných incidentů, nebo jinak ohrozí úsilí subjektu v tomto ohledu. V případě probíhajícího incidentu v době podání závěrečné zprávy by členské státy měly zajistit, aby dotčené subjekty v této době předložily zprávu o pokroku a závěrečnou zprávu do jednoho měsíce od vyřešení významného incidentu.

(103) Zásadní a důležité subjekty by měly případně bez zbytečného odkladu informovat příjemce svých služeb o opatřeních nebo nápravných opatřeních, která mohou přijmout ke zmírnění rizik vyplývajících z významné kybernetické hrozby. Tyto subjekty by měly, je-li to vhodné a zejména v případech, kdy je pravděpodobné, že se významná kybernetická hrozba naplní, informovat své příjemce služeb také o hrozbě samotné. Požadavek informovat tyto příjemce o významných kybernetických hrozbách by měl být splněn na základě maximálního úsilí, ale neměl by tyto subjekty zbavovat povinnosti přijmout na vlastní náklady vhodná a okamžitá opatření k prevenci nebo nápravě takových hrozeb a k obnovení běžné úrovně bezpečnosti služby. Poskytování těchto informací o významných kybernetických hrozbách příjemcům služeb by mělo být bezplatné a mělo by být vypracováno ve snadno srozumitelném jazyce.

(104) Poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací by měli zavést bezpečnost již ve fázi návrhu a ve výchozím nastavení a informovat příjemce svých služeb o významných kybernetických hrozbách a o opatřeních, která mohou přijmout na ochranu bezpečnosti svých zařízení a komunikace, například používáním konkrétních typů softwaru nebo šifrovacích technologií.

(105) Proaktivní přístup ke kybernetickým hrozbám je důležitou součástí řízení rizik kybernetické bezpečnosti, která by měla příslušným orgánům umožnit účinně předcházet tomu, aby se kybernetické hrozby proměnily v incidenty, které mohou způsobit značné materiální nebo nemajetková újma. Za tímto účelem má klíčový význam oznamování kybernetických hrozeb. Za tímto účelem jsou subjekty vyzývány k dobrovolnému oznamování kybernetických hrozeb.

(106) V zájmu zjednodušení oznamování informací požadovaných podle této směrnice a snížení administrativní zátěže subjektů by členské státy měly poskytnout technické prostředky, jako je jednotné vstupní místo, automatizované systémy, online formuláře, uživatelsky přívětivá rozhraní, šablony, specializované platformy, které by subjekty mohly využívat k předkládání příslušných informací, jež mají být oznamovány, bez ohledu na to, zda spadají do oblasti působnosti této směrnice. Financování Unie na podporu provádění této směrnice, zejména v rámci programu Digitální Evropa zřízeného nařízením Evropského parlamentu a Rady (EU) 2021/6941 , by mohlo zahrnovat podporu jednotných kontaktních míst. Subjekty se navíc často dostávají do situace, kdy je třeba určitý incident vzhledem k jeho vlastnostem hlásit různým orgánům v důsledku oznamovacích povinností obsažených v různých právních nástrojích. Takové případy vytvářejí další administrativní zátěž a mohly by také vést k nejasnostem ohledně formátu a postupů těchto oznámení. Pokud je zřízeno jediné vstupní místo, členské státy se vyzývají, aby toto jediné vstupní místo využívaly také pro oznámení bezpečnostních incidentů vyžadovaná podle jiných právních předpisů Unie, jako je nařízení (EU) 2016/679 a směrnice 2002/58/ES. Použitím takového jednotného kontaktního místa pro hlášení 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.
Nařízení (EU) 2016/679 a směrnice 2002/58/ES, zejména ty, které se týkají nezávislosti orgánů v nich uvedených. Agentura ENISA by měla ve spolupráci se skupinou pro spolupráci vypracovat společné vzory oznámení prostřednictvím pokynů, aby se zjednodušily a zefektivnily informace, které mají být podle práva Unie oznamovány, a snížila se administrativní zátěž oznamujících subjektů.

1 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).

(107) Pokud existuje podezření, že incident souvisí se závažnou trestnou činností podle práva Unie nebo vnitrostátního práva, měly by členské státy vybízet zásadní a důležité subjekty, aby na základě platných pravidel trestního řízení v souladu s právem Unie oznámily incidenty, u nichž existuje podezření na závažnou trestnou činnost, příslušným donucovacím orgánům. Aniž jsou dotčena pravidla ochrany osobních údajů vztahující se na Europol, je žádoucí, aby koordinaci mezi příslušnými orgány a donucovacími orgány různých členských států případně usnadňovalo Evropské centrum pro boj proti kyberkriminalitě (EC3) a agentura ENISA.

(108) Osobní údaje jsou v mnoha případech ohroženy v důsledku incidentů. 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 Směrnice 2002/58/ES.

(109) Udržování přesných a úplných databází údajů o registraci doménových jmen (údajů WHOIS) a poskytování zákonného přístupu k těmto údajům má zásadní význam pro zajištění bezpečnosti, stability a odolnosti systému DNS, což následně přispívá k vysoké společné úrovni kybernetické bezpečnosti v celé Unii. Za tímto konkrétním účelem by se od registrů názvů TLD a subjektů poskytujících služby registrace názvů domén mělo vyžadovat, aby zpracovávaly 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 doménových jmen pro jiné účely, například na základě smluvních ujednání nebo právních požadavků stanovených v jiných právních předpisech Unie nebo vnitrostátních právních předpisech. Cílem této povinnosti je dosáhnout úplného a přesného souboru registračních údajů a neměla by vést k vícenásobnému shromažďování stejných údajů. Registry názvů domén nejvyšší úrovně a subjekty poskytující služby registrace názvů domén by měly vzájemně spolupracovat, aby nedocházelo k duplicitě tohoto úkolu.

(110) Dostupnost a včasná dostupnost údajů o registraci doménových jmen pro oprávněné žadatele o přístup je zásadní pro prevenci a boj proti zneužívání DNS a pro prevenci a odhalování incidentů a reakci na ně. Oprávněnými žadateli o přístup se rozumí každá fyzická nebo právnická osoba, která podá žádost podle práva Unie nebo vnitrostátního práva. Mohou mezi ně patřit orgány, které jsou příslušné podle této směrnice, a orgány, které jsou podle práva Unie nebo vnitrostátního práva příslušné pro prevenci, vyšetřování, odhalování nebo stíhání trestných činů, a CERT nebo CSIRT. Od registrů názvů domén nejvyšší úrovně a subjektů poskytujících služby registrace názvů domén by se mělo vyžadovat, aby oprávněným žadatelům o přístup v souladu s právem Unie a vnitrostátním právem umožnily zákonný přístup ke konkrétním údajům o registraci názvů domén, které jsou nezbytné pro účely žádosti o přístup. K žádosti oprávněných žadatelů o přístup by mělo být přiloženo odůvodnění umožňující posoudit nezbytnost přístupu k údajům.

(111) Aby byla zajištěna dostupnost přesných a úplných údajů o registraci doménových jmen. údajů, měly by registry názvů TLD a subjekty poskytující služby registrace názvů domén shromažďovat a zaručovat integritu a dostupnost údajů o registraci názvů domén. Registry názvů TLD a subjekty poskytující služby registrace názvů domén by měly zejména zavést zásady a postupy pro shromažďování a uchovávání přesných a úplných údajů o registraci názvů domén, jakož i pro prevenci a opravu nepřesných údajů o registraci v souladu s právem Unie v oblasti ochrany údajů. Tyto zásady a postupy by měly v co největší míře zohledňovat standardy vypracované vícestrannými řídícími strukturami na mezinárodní úrovni. Registry názvů TLD a subjekty poskytující služby registrace názvů domén by měly přijmout a provádět přiměřené postupy pro ověřování údajů o registraci názvů domén. Tyto postupy by měly odrážet osvědčené postupy používané v odvětví a v co největší míře pokrok dosažený v oblasti elektronické identifikace. Příklady ověřovacích postupů mohou zahrnovat kontroly ex ante prováděné v době registrace a kontroly ex post prováděné po registraci. Registry jmen domén nejvyšší úrovně a subjekty poskytující služby registrace jmen domén by měly zejména ověřovat alespoň jeden kontaktní prostředek žadatele o registraci.

(112) Registry názvů TLD a subjekty poskytující služby registrace názvů domén by měly být povinny zveřejňovat údaje o registraci názvů domén, které nespadají do oblasti působnosti práva Unie v oblasti ochrany údajů, jako jsou údaje týkající se právnických osob, v souladu s preambulí nařízení (EU) 2016/679. V případě právnických osob by měly registry názvů domén nejvyšší úrovně a subjekty poskytující služby registrace doménových jmen zveřejnit alespoň jméno registrátora a kontaktní telefonní číslo. Zveřejněna by měla být rovněž kontaktní e-mailová adresa, pokud neobsahuje žádné osobní údaje, jako například v případě e-mailových aliasů nebo funkčních účtů. Registry názvů domén nejvyšší úrovně a subjekty poskytující služby registrace názvů domén by rovněž měly oprávněným žadatelům o přístup umožnit zákonný přístup ke konkrétním údajům o registraci názvů domén týkajících se fyzických osob, a to v souladu s právem Unie v oblasti ochrany údajů. Členské státy by měly vyžadovat, aby registry názvů TLD a subjekty poskytující služby registrace názvů domén bez zbytečného odkladu reagovaly na žádosti oprávněných žadatelů o přístup o zpřístupnění údajů o registraci názvů domén. Registry názvů domén nejvyšší úrovně a subjekty poskytující služby registrace názvů domén by měly stanovit zásady a postupy pro zveřejňování a zpřístupňování registračních údajů, včetně dohod o úrovni služeb pro vyřizování žádostí o přístup od oprávněných žadatelů o přístup. Tyto zásady a postupy by měly v co největší míře zohledňovat veškeré pokyny a standardy vypracované řídícími strukturami více zúčastněných stran na mezinárodní úrovni. Postup přístupu by mohl zahrnovat použití rozhraní, portálu nebo jiného technického nástroje, který by poskytoval účinný systém pro podávání žádostí o registrační údaje a přístup k nim. S cílem podpořit harmonizované postupy na celém vnitřním trhu může Komise, aniž jsou dotčeny pravomoci Evropského sboru pro ochranu osobních údajů, poskytnout pokyny týkající se těchto postupů, které v co největší míře zohlední normy vypracované vícestrannými řídícími strukturami na mezinárodní úrovni. Členské státy by měly zajistit, aby všechny typy přístupu k osobním a neosobním údajům o registraci doménových jmen byly bezplatné.

(113) Subjekty, které spadají do oblasti působnosti této směrnice, by měly být považovány za subjekty spadající do jurisdikce členského státu, v němž jsou usazeny. Poskytovatelé veřejných sítí elektronických komunikací nebo poskytovatelé veřejně dostupných služeb elektronických komunikací by však měli být považováni za spadající do jurisdikce členského státu, v němž poskytují své služby. Poskytovatelé služeb DNS, registry jmen domén nejvyšší úrovně, subjekty poskytující služby registrace jmen domén, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center, poskytovatelé sítí pro doručování obsahu, poskytovatelé spravovaných služeb, poskytovatelé spravovaných bezpečnostních služeb, jakož i poskytovatelé on-line tržišť, on-line vyhledávačů a platforem služeb sociálních sítí by měli být považováni za subjekty spadající do jurisdikce členského státu, v němž mají hlavní provozovnu v Unii. Subjekty veřejné správy by měly spadat do pravomoci členského státu, který je zřídil. Pokud subjekt poskytuje služby nebo je usazen ve více než jednom členském státě, měl by spadat do samostatné a souběžné pravomoci každého z těchto členských států. Příslušné orgány těchto členských států by měly spolupracovat, poskytovat si vzájemnou pomoc a případně provádět společná opatření v oblasti dohledu. Pokud členské státy vykonávají svou pravomoc, neměly by v souladu se zásadou *ne bis in idem ukládat* donucovací opatření nebo sankce za stejné jednání vícekrát.

(114) S cílem zohlednit přeshraniční povahu služeb a činností poskytovatelů služeb DNS, registrů názvů domén nejvyšší úrovně, subjektů poskytujících služby registrace názvů domén, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center, poskytovatelů sítí pro doručování obsahu, poskytovatelů spravovaných služeb, poskytovatelů spravovaných bezpečnostních služeb, jakož i poskytovatelů on-line tržišť, on-line vyhledávačů a platforem služeb sociálních sítí by měl mít nad těmito subjekty pravomoc pouze jeden členský stát. Příslušnost by měla být přidělena členskému státu, v němž má dotčený subjekt hlavní provozovnu v Unii. Kritérium usazení pro účely této směrnice znamená skutečný výkon činnosti prostřednictvím stabilních ujednání. Právní forma těchto uspořádání, ať již prostřednictvím pobočky nebo dceřiné společnosti s právní subjektivitou, není v tomto ohledu rozhodující. Splnění tohoto kritéria by nemělo záviset na tom, zda se síť a informační systémy fyzicky nacházejí na daném místě; přítomnost a používání takových systémů samy o sobě nepředstavují takovou hlavní provozovnu, a nejsou proto rozhodujícím kritériem pro určení hlavní provozovny. Za hlavní provozovnu by měla být považována provozovna v členském státě, v němž jsou v Unii přijímána převážně rozhodnutí týkající se opatření k řízení rizik v oblasti kybernetické bezpečnosti. To bude obvykle odpovídat místu
ústřední správy subjektů v Unii. Nelze-li takový členský stát určit nebo nejsou-li taková rozhodnutí v Unii přijímána, mělo by se za hlavní provozovnu považovat sídlo v členském státě, v němž jsou prováděny operace v oblasti kybernetické bezpečnosti. Pokud takový členský stát nelze určit, mělo by se za hlavní provozovnu považovat místo v členském státě, kde má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud služby poskytuje skupina podniků, měla by se za hlavní provozovnu skupiny podniků považovat hlavní provozovna ovládajícího podniku.

(115) Pokud je veřejně dostupná rekurzivní služba DNS poskytována poskytovatelem veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací pouze jako součást služby přístupu k internetu, mělo by se mít za to, že tento subjekt spadá do jurisdikce všech členských států, v nichž jsou jeho služby poskytovány.

(116) Pokud poskytovatel služeb DNS, registr názvů TLD, subjekt poskytující služby registrace názvů domén, poskytovatel služeb cloud computingu, poskytovatel služeb datového centra, poskytovatel sítě pro doručování obsahu, poskytovatel spravovaných služeb, poskytovatel spravovaných bezpečnostních služeb nebo poskytovatel online tržiště, online vyhledávače nebo platformy pro služby sociálních sítí, který není usazen v Unii, nabízí služby v Unii, měl by určit svého zástupce v Unii. Za účelem určení, zda takový subjekt nabízí služby v Unii, by mělo být zjištěno, zda subjekt plánuje nabízet služby osobám v jednom nebo více členských státech. Pouhá dostupnost internetových stránek subjektu nebo zprostředkovatele v Unii nebo e-mailové adresy či jiných kontaktních údajů nebo použití jazyka obecně používaného ve třetí zemi, v níž je subjekt usazen, by neměly být považovány za dostatečné pro zjištění takového záměru. Avšak faktory, jako je používání jazyka nebo měny obecně používané v jednom nebo více členských státech s možností objednání služeb v tomto jazyce nebo uvedení zákazníků či uživatelů, kteří se nacházejí v Unii, by mohly vést k tomu, že subjekt plánuje nabízet služby v Unii. Zástupce by měl jednat jménem subjektu a příslušné orgány nebo CSIRT by měly mít možnost se na zástupce obrátit. Zástupce by měl být výslovně určen písemným pověřením subjektu, aby jednal jeho jménem, pokud jde o jeho povinnosti stanovené v této směrnici, včetně hlášení incidentů.

(117) V zájmu zajištění jasného přehledu o poskytovatelích služeb DNS, registrech názvů TLD, subjektech poskytujících služby registrace názvů domén, poskytovatelích služeb cloud computingu, poskytovatelích služeb datových center, poskytovatelích sítí pro doručování obsahu, poskytovatelích spravovaných služeb, poskytovatelích spravovaných bezpečnostních služeb, jakož i poskytovatelích on-line tržišť, on-line vyhledávačů a platforem služeb sociálních sítí, kteří poskytují služby v celé Unii, jež spadají do oblasti působnosti této směrnice, by agentura ENISA měla vytvořit a vést registr těchto subjektů na základě informací obdržených členskými státy, případně prostřednictvím vnitrostátních mechanismů zřízených pro registraci subjektů.
Jednotná kontaktní místa by měla agentuře ENISA předávat informace a jejich případné změny. S cílem zajistit přesnost a úplnost informací, které mají být do tohoto registru zahrnuty, mohou členské státy agentuře ENISA předložit informace o těchto subjektech, které jsou k dispozici v jakýchkoli vnitrostátních registrech. Agentura ENISA a členské státy by měly přijmout opatření k usnadnění interoperability těchto registrů a zároveň zajistit ochranu důvěrných nebo utajovaných informací. Agentura ENISA by měla zavést vhodné protokoly o klasifikaci a správě informací, aby zajistila bezpečnost a důvěrnost zveřejněných informací a omezila přístup k těmto informacím, jejich uchovávání a přenos pouze na určené uživatele.

(118) Pokud jsou podle této směrnice vyměňovány, oznamovány nebo jinak sdíleny informace, které jsou utajované v souladu s právem Unie nebo vnitrostátním právem, měla by se použít odpovídající pravidla pro nakládání s utajovanými informacemi. Agentura ENISA by navíc měla mít k dispozici infrastrukturu, postupy a pravidla pro nakládání s citlivými a utajovanými informacemi v souladu s platnými bezpečnostními pravidly pro ochranu utajovaných informací EU.

(119) Vzhledem k tomu, že kybernetické hrozby jsou stále složitější a sofistikovanější, závisí dobré odhalení těchto hrozeb a opatření na jejich prevenci do značné míry na pravidelném sdílení informací o hrozbách a zranitelnostech mezi subjekty. Sdílení informací přispívá k
lepší informovanost o kybernetických hrozbách, což zvyšuje schopnost subjektů předcházet tomu, aby se tyto hrozby proměnily v incidenty, a umožňuje subjektům lépe zvládat následky incidentů a účinněji se z nich zotavovat. Vzhledem k absenci pokynů na úrovni Unie se zdá, že sdílení těchto informací brání různé faktory, zejména nejistota ohledně slučitelnosti s pravidly hospodářské soutěže a odpovědnosti.

(120) Členské státy by měly subjekty podporovat a pomáhat jim, aby společně využívaly své individuální znalosti a praktické zkušenosti na strategické, taktické a operativní úrovni s cílem posílit své schopnosti odpovídajícím způsobem předcházet incidentům, odhalovat je, reagovat na ně nebo se z nich zotavovat či zmírňovat jejich dopad. Je proto nezbytné umožnit, aby na úrovni Unie vznikla dobrovolná ujednání o sdílení informací v oblasti kybernetické bezpečnosti. Za tímto účelem by členské státy měly aktivně pomáhat subjektům, jako jsou subjekty poskytující služby a výzkum v oblasti kybernetické bezpečnosti, jakož i příslušným subjektům, které nespadají do oblasti působnosti této směrnice, a podporovat je v účasti na takových ujednáních o sdílení informací v oblasti kybernetické bezpečnosti. Tato ujednání by měla být uzavřena v souladu s pravidly Unie v oblasti hospodářské soutěže a s právem Unie v oblasti ochrany údajů.

(121) Zpracování osobních údajů v rozsahu nezbytném a přiměřeném pro účely zajištění bezpečnosti sítě a informačních systémů základními a důležitými subjekty by mohlo být považováno za zákonné na základě toho, že takové zpracování splňuje právní povinnost, která se na správce vztahuje, 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, které sledují zásadní a významné subjekty, jakož i poskytovatelé bezpečnostních technologií a služeb jednající 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 související s prevencí, odhalováním, identifikací, omezováním, analýzou a reakcí na incidenty, opatření ke zvyšování povědomí v souvislosti s konkrétními kybernetickými hrozbami, výměna informací v souvislosti s odstraňováním zranitelností a koordinovaným zveřejňováním zranitelností, dobrovolná výměna informací o těchto incidentech, a kybernetických hrozeb a zranitelností, indikátorů kompromitace, taktik, technik a postupů, kybernetických bezpečnostních výstrah a konfiguračních nástrojů by mohlo vyžadovat zpracování určitých kategorií osobních údajů, jako jsou IP adresy, jednotné lokátory zdrojů (URL), názvy domén, e-mailové adresy a, pokud odhalují osobní údaje, časová razítka. Zpracování osobních údajů příslušnými orgány, jednotnými kontaktními místy a týmy CSIRT by mohlo představovat právní povinnost nebo by mohlo být považováno za nezbytné pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci svěřené správci podle čl. 6 odst. 1 písm. c) nebo e) a čl. 6 odst. 3 nařízení (EU) 2016/679 nebo pro sledování oprávněného zájmu zásadních a významných subjektů, jak je uvedeno v čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679.

Vnitrostátní právo by dále mohlo stanovit pravidla, která by příslušným orgánům, jednotným kontaktním místům a CSIRT umožnila v rozsahu, který je nezbytný a přiměřený pro účely zajištění bezpečnosti sítí a informačních systémů základních a důležitých subjektů, 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 použití nejmodernějších bezpečnostních opatření a opatření na ochranu soukromí, jako je pseudonymizace nebo šifrování, pokud by anonymizace mohla významně ovlivnit sledovaný účel.

(122) V zájmu posílení pravomocí a opatření v oblasti dohledu, které pomáhají zajistit účinné dodržování předpisů, by tato směrnice měla stanovit minimální seznam opatření a prostředků dohledu, jejichž prostřednictvím mohou příslušné orgány vykonávat dohled nad základními a významnými subjekty. Kromě toho by tato směrnice měla stanovit rozlišení režimu dohledu mezi základními a významnými subjekty s cílem zajistit spravedlivou rovnováhu povinností těchto subjektů a příslušných orgánů. Podstatné subjekty by proto měly podléhat komplexnímu režimu dohledu *ex ante* a *ex post,* zatímco významné subjekty by měly podléhat mírnému režimu dohledu pouze *ex post.* Důležité subjekty by proto neměly mít povinnost systematicky dokumentovat dodržování opatření k řízení kybernetických rizik, zatímco příslušné orgány by měly uplatňovat reaktivní přístup k dohledu *ex post,* a neměly by tedy mít obecnou povinnost vykonávat dohled nad těmito subjekty. Následný dohled nad významnými subjekty může být zahájen na základě důkazů, indicií nebo informací, o nichž byly příslušné orgány informovány a které podle těchto orgánů naznačují možné porušení této směrnice. Takové důkazy, indicie nebo informace mohou být například toho druhu, že je příslušným orgánům poskytly jiné orgány, subjekty, občané, média nebo jiné zdroje či veřejně dostupné informace, nebo mohou vyplynout z jiných činností, které příslušné orgány provádějí při plnění svých úkolů.

(123) Plnění úkolů dohledu příslušnými orgány by nemělo zbytečně bránit podnikatelským aktivitám dotčeného subjektu. Pokud příslušné orgány vykonávají své úkoly v oblasti dohledu ve vztahu k základním subjektům, včetně provádění kontrol na místě a dohledu mimo místo, vyšetřování porušení této směrnice a provádění bezpečnostních auditů nebo bezpečnostních prověrek, měly by minimalizovat dopad na obchodní činnosti dotčeného subjektu.

(124) Při výkonu dohledu ex ante by příslušné orgány měly mít možnost rozhodnout o prioritách použití opatření a prostředků dohledu, které mají k dispozici, a to přiměřeným způsobem. To znamená, že příslušné orgány mohou rozhodovat o tomto stanovení priorit na základě metodik dohledu, které by měly vycházet z přístupu založeného na riziku. Konkrétně by tyto metodiky mohly zahrnovat kritéria nebo referenční hodnoty pro klasifikaci základních subjektů do rizikových kategorií a odpovídající opatření a prostředky dohledu doporučené pro jednotlivé rizikové kategorie, jako je použití, četnost nebo druhy kontrol na místě, cílené bezpečnostní audity nebo bezpečnostní skenování, druh požadovaných informací a úroveň podrobnosti těchto informací. Tyto metodiky dohledu by mohly být rovněž doprovázeny pracovními programy a pravidelně posuzovány a revidovány, včetně aspektů, jako je přidělování a potřeby zdrojů. Ve vztahu k subjektům veřejné správy by měly být dozorové pravomoci vykonávány v souladu s vnitrostátními právními a institucionálními rámci.

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

(126) V řádně odůvodněných případech, kdy si je vědom významné kybernetické hrozby nebo bezprostředního rizika, by měl být příslušný orgán schopen přijmout okamžitá rozhodnutí o prosazování práva s cílem zabránit incidentu nebo na něj reagovat.

(127) Aby bylo prosazování účinné, měl by být stanoven minimální seznam donucovacích pravomocí, které lze uplatnit v případě porušení opatření k řízení rizik v oblasti kybernetické bezpečnosti a oznamovacích povinností stanovených v této směrnici, čímž se vytvoří jasný a konzistentní rámec pro toto prosazování v celé Unii. Náležitý ohled by měl být brán na povahu, závažnost a dobu trvání porušení této směrnice, způsobenou hmotnou nebo nehmotnou škodu , zda bylo porušení úmyslné nebo z nedbalosti, opatření přijatá k zabránění nebo zmírnění hmotné nebo nehmotné škody, míru odpovědnosti nebo případná předchozí porušení, míru spolupráce s příslušným orgánem a jakékoli další přitěžující nebo polehčující okolnosti. Donucovací opatření, včetně správních pokut, by měla být přiměřená a jejich uložení by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listinou základních práv Evropské unie (dále jen "Listina"), včetně práva na účinnou právní ochranu a spravedlivý proces, presumpce neviny a práva na obhajobu.

(128) Tato směrnice nevyžaduje, aby členské státy stanovily trestní nebo občanskoprávní odpovědnost fyzických osob odpovědných za zajištění souladu subjektu s touto směrnicí za škodu, která vznikla třetím osobám v důsledku porušení této směrnice.

(129) Aby bylo zajištěno účinné vymáhání povinností stanovených v této směrnici, měl by mít každý příslušný orgán pravomoc ukládat správní pokuty nebo o jejich uložení požádat.

(130) Pokud je správní pokuta uložena zásadnímu nebo významnému subjektu, který je podnikem, měl by se pro tyto účely podnikem rozumět podnik v souladu s články 101 a 102 SFEU. Pokud je správní pokuta uložena osobě, která není podnikem, měl by příslušný orgán při zvažování přiměřené výše pokuty přihlédnout k obecné úrovni příjmů v členském státě, jakož i k hospodářské situaci dané osoby. Mělo by být na členských státech, aby určily, zda a v jakém rozsahu by měly orgány veřejné moci podléhat správním pokutám. Uložením správní pokuty není dotčeno uplatňování jiných pravomocí příslušných orgánů ani jiných sankcí stanovených ve vnitrostátních předpisech provádějících tuto směrnici.

(131) Členské státy by měly mít možnost stanovit pravidla pro trestní sankce za porušení vnitrostátních předpisů provádějících tuto směrnici. Ukládání trestních sankcí za porušení těchto vnitrostátních předpisů a souvisejících správních sankcí by však nemělo vést k porušení zásady *ne bis in idem, jak ji* vykládá Soudní dvůr Evropské unie.

(132) Pokud tato směrnice neharmonizuje správní sankce nebo pokud je to nezbytné v jiných případech, například v případě závažného porušení této směrnice, měly by členské státy zavést systém, který stanoví účinné, přiměřené a odrazující sankce. Povahu těchto sankcí a to, zda jsou trestní nebo správní, by mělo stanovit vnitrostátní právo.

(133) V zájmu dalšího posílení účinnosti a odrazujícího účinku donucovacích opatření použitelných v případě porušení této směrnice by příslušné orgány měly být oprávněny dočasně pozastavit nebo požádat o dočasné pozastavení osvědčení nebo povolení týkající se části nebo všech příslušných služeb poskytovaných nebo činností vykonávaných základním subjektem a požádat o uložení dočasného zákazu výkonu řídících funkcí jakékoli fyzické osobě vykonávající řídící funkce na úrovni výkonného ředitele nebo právního zástupce. Vzhledem k tomu, že
jejich závažnosti a dopadu na činnost subjektů a v konečném důsledku na uživatele, by se taková dočasná pozastavení nebo zákazy měly uplatňovat pouze přiměřeně závažnosti porušení a s přihlédnutím k okolnostem každého jednotlivého případu, včetně toho, zda bylo porušení úmyslné nebo z nedbalosti, a k veškerým opatřením přijatým k zabránění nebo zmírnění hmotné nebo nehmotné škody. Taková dočasná pozastavení nebo zákazy by měly být uplatňovány pouze jako poslední možnost, a to až poté, co byla vyčerpána ostatní příslušná donucovací opatření stanovená v této směrnici, a pouze do doby, než dotčený subjekt přijme nezbytná opatření k nápravě nedostatků nebo splní požadavky příslušného orgánu, pro které byla taková dočasná pozastavení nebo zákazy uplatněny. Uložení takových dočasných pozastavení nebo zákazů by mělo podléhat vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny , včetně práva na účinnou právní ochranu a spravedlivý proces, presumpce neviny a práva na obhajobu.

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

(135) V zájmu zajištění účinného dohledu a prosazování práva, zejména v situaci s přeshraničním rozměrem, by měl členský stát, který obdržel žádost o vzájemnou pomoc, přijmout v mezích této žádosti vhodná opatření v oblasti dohledu a prosazování práva ve vztahu k subjektu, který je předmětem této žádosti a který poskytuje služby nebo má síť a informační systém na území tohoto členského státu.

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

(137) Cílem této směrnice by mělo být zajištění vysoké úrovně odpovědnosti za opatření k řízení rizik v oblasti kybernetické bezpečnosti a povinnosti podávat zprávy na úrovni základních a významných subjektů. Proto by řídicí orgány základních a významných subjektů měly schvalovat opatření k řízení rizik v oblasti kybernetické bezpečnosti a dohlížet na jejich provádění.

(138) V zájmu zajištění vysoké společné úrovně kybernetické bezpečnosti v celé Unii na základě této směrnice by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování EU, pokud jde o doplnění této směrnice stanovením toho, které kategorie základních a významných subjektů mají být povinny používat určité certifikované produkty IKT, služby IKT a procesy IKT nebo získat certifikát v rámci evropského systému certifikace kybernetické bezpečnosti. Je obzvláště důležité, aby Komise během přípravných prací 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 předpisů1. Zejména v zájmu zajištění rovné účasti na přípravě aktů v přenesené pravomoci dostávají Evropský parlament a Rada veškeré dokumenty ve stejnou dobu jako odborníci členských států a jejich odborníci mají systematicky přístup na zasedání odborných skupin Komise, které se zabývají přípravou aktů v přenesené pravomoci.

1 L 123, 12.5.2016, s. 1.

(139) Za účelem zajištění jednotných podmínek pro provádění této směrnice by měly být Komisi svěřeny prováděcí pravomoci ke stanovení procesních opatření nezbytných pro fungování skupiny pro spolupráci a technických a metodických, jakož i odvětvových požadavků týkajících se kybernetické bezpečnosti.
opatření k řízení rizik a dále upřesnit druh informací, formát a postup při oznamování incidentů, kybernetických hrozeb a téměř chybných hlášení a sdělení o významných kybernetických hrozbách, jakož i případy, kdy se incident považuje za významný. Tyto pravomoci by měly být vykonávány v souladu s
Nařízení Evropského parlamentu a Rady (EU) č. 182/20111.

1 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).

(140) Komise by měla tuto směrnici po konzultaci se zúčastněnými stranami pravidelně přezkoumávat, zejména s cílem určit, zda je vhodné navrhnout změny s ohledem na změny společenských, politických, technologických nebo tržních podmínek. V rámci těchto přezkumů by Komise měla posoudit význam velikosti dotčených subjektů a odvětví, pododvětví a typů subjektů uvedených v přílohách této směrnice pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností.
Komise by měla mimo jiné posoudit, zda poskytovatelé spadající do oblasti působnosti této směrnice, kteří jsou označeni jako velmi velké online platformy ve smyslu článku 33 nařízení (EU) .../.....Evropského parlamentu a Rady1+ , by mohli být označeny za základní subjekty podle této směrnice.

---

1 Nařízení Evropského parlamentu a Rady (EU) .../... ze dne..... o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (akt o digitálních službách) (Úř. věst. L ...., ... , s. .).

\+ Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 30/22 (2020/0361(COD)) a do poznámky pod čarou vložte číslo, datum a odkaz na Úřední věstník uvedeného nařízení.

(141) Tato směrnice vytváří nové úkoly pro agenturu ENISA, čímž posiluje její úlohu, a mohla by také vést k tomu, že agentura ENISA bude muset plnit své stávající úkoly podle

Nařízení (EU) 2019/881 na vyšší úroveň než dříve. Aby bylo zajištěno, že agentura ENISA bude mít k dispozici potřebné finanční a lidské zdroje k plnění stávajících a nových úkolů, jakož i k plnění případné vyšší úrovně plnění těchto úkolů vyplývající z její posílené úlohy, měl by být odpovídajícím způsobem navýšen její rozpočet. Kromě toho by agentura ENISA měla mít v zájmu zajištění účinného využívání zdrojů větší flexibilitu, pokud jde o způsob, jakým může interně rozdělovat zdroje za účelem účinného plnění svých úkolů a naplňování očekávání.

(142) Jelikož cíle této směrnice, totiž dosažení vysoké společné úrovně kybernetické bezpečnosti v celé Unii, nemůže být uspokojivě dosaženo na úrovni členských států, ale spíše jej může být z důvodu účinků opatření 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 respektuje základní práva a dodržuje zásady uznané Listinou , zejména právo na respektování soukromého života a komunikace, ochranu osobních údajů, svobodu podnikání, vlastnické právo, 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) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/17251 a vydal stanovisko dne 11. března 20212,

PŘIJALY TUTO SMĚRNICI:

---

1 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).

2 C 183, 11.5.2021, s. 3.

Kapitola I

Obecná ustanovení

Článek 1

Předmět úpravy

1. Tato směrnice stanoví opatření, jejichž cílem je dosáhnout vysoké společné úrovně kybernetické bezpečnosti v celé Unii s cílem zlepšit fungování vnitřního trhu.

2. Za tímto účelem tato směrnice stanoví:

   (a) povinnosti, které vyžadují, aby členské státy přijaly vnitrostátní strategie kybernetické bezpečnosti a určily nebo zřídily příslušné orgány, orgány pro řešení kybernetických krizí, jednotná kontaktní místa pro kybernetickou bezpečnost a týmy pro řešení počítačových bezpečnostních incidentů (CSIRT);

   (b) opatření k řízení rizik v oblasti kybernetické bezpečnosti a povinnosti podávání zpráv pro subjekty typu uvedeného v příloze I nebo II, jakož i pro subjekty označené za kritické subjekty podle směrnice (EU) .../... [+];

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

   (d) povinnosti členských států v oblasti dohledu a vymáhání práva.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

Článek 2

Oblast

působnosti

1. Tato směrnice se vztahuje na veřejné nebo soukromé subjekty typu uvedeného v příloze I nebo II, které se kvalifikují jako střední podniky podle článku 2 přílohy doporučení 2003/361/ES nebo překračují stropy pro střední podniky stanovené v odstavci 1 uvedeného článku a které poskytují své služby nebo vykonávají své činnosti v Unii.

   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 typu uvedeného v příloze I nebo II, pokud:

   (a) služby poskytuje:

      (i) poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací;

      (ii) důvěryhodnost poskytovatelů služeb;

      (iii) registry doménových jmen nejvyšší úrovně a poskytovatelé služeb systému doménových jmen;

(b) subjekt je v členském státě jediným poskytovatelem služby, která je nezbytná pro zachování kritických společenských nebo hospodářských činností;

(c) narušení služby poskytované subjektem by mohlo mít významný dopad na veřejnou bezpečnost, veřejnou bezpečnost nebo veřejné zdraví;

(d) narušení služby poskytované subjektem by mohlo vyvolat významné systémové riziko, zejména v odvětvích, kde by takové narušení mohlo mít přeshraniční dopad;

(e) subjekt je kritický z důvodu svého specifického významu na národní nebo regionální úrovni pro dané odvětví nebo druh služby nebo pro jiná vzájemně závislá odvětví v členském státě;

(f) subjekt je subjektem veřejné správy:

(i) ústřední vlády, jak je definována členským státem v souladu s vnitrostátními právními předpisy, nebo

(ii) na regionální úrovni vymezené členským státem v souladu s vnitrostátními právními předpisy, které na základě posouzení rizik poskytují služby, jejichž narušení by mohlo mít významný dopad na kritické společenské nebo hospodářské činnosti.

3. Tato směrnice se bez ohledu na jejich velikost vztahuje na subjekty, které jsou podle směrnice (EU) .../... označeny jako kritické subjekty. [+].

4. Tato směrnice se vztahuje na subjekty poskytující služby registrace doménových jmen bez ohledu na jejich velikost.

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

   (a) subjekty veřejné správy na místní úrovni;

   (b) vzdělávací instituce, zejména tam, kde provádějí kritické výzkumné činnosti.

6. Touto směrnicí není dotčena odpovědnost členských států za ochranu národní bezpečnosti a jejich pravomoc chránit další základní funkce státu, včetně zajištění územní celistvosti státu a udržování veřejného pořádku.

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

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

8. Členské státy mohou z povinností stanovených v článku 21 nebo 23 ve vztahu k těmto činnostem nebo službám vyjmout určité subjekty, které vykonávají činnosti v oblasti národní bezpečnosti, veřejné bezpečnosti, obrany nebo vymáhání práva, včetně prevence, vyšetřování, odhalování a stíhání trestných činů, nebo které poskytují služby výhradně subjektům veřejné správy uvedeným v odstavci 7 tohoto článku. V takových případech se opatření v oblasti dohledu a prosazování uvedená v kapitole VII ve vztahu k těmto konkrétním činnostem nebo službám nepoužijí. Pokud subjekty vykonávají činnosti nebo poskytují služby výhradně typu uvedeného v tomto odstavci, mohou členské státy rozhodnout, že tyto subjekty rovněž osvobodí od povinností stanovených v článcích 3 a 27.

9. Odstavce 7 a 8 se nepoužijí, pokud subjekt působí jako poskytovatel svěřenských služeb.

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

11. Povinnosti stanovené v této směrnici neznamenají poskytnutí informací, jejichž zveřejnění by bylo v rozporu se základními zájmy národní bezpečnosti, veřejné bezpečnosti nebo obrany členských států.

[+] Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

12. Tato směrnice se použije, aniž je dotčeno nařízení (EU) 2016/679, směrnice 2002/58/ES, směrnice Evropského parlamentu a Rady 2011/93/EU1 a 2013/40/EU2 a směrnice (EU) .../.....+.

13. Aniž je dotčen článek 346 Smlouvy o fungování EU, informace, které jsou důvěrné podle pravidel Unie nebo vnitrostátních pravidel, jako jsou pravidla o obchodním tajemství, se vyměňují s Komisí a dalšími příslušnými orgány v souladu s touto směrnicí, pouze pokud je tato výměna nezbytná pro uplatňování této směrnice. Výměna informací se omezí na informace, které jsou relevantní a přiměřené účelu této výměny. Při výměně informací se zachovává důvěrnost těchto informací a chrání se bezpečnostní a obchodní zájmy dotčených subjektů.

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

---

1 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).

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

\+ Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

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 o ochraně údajů a právem Unie o ochraně soukromí, zejména se směrnicí 2002/58/ES.

Článek 3

Základní a důležité subjekty

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

(a) subjekty typu uvedeného v příloze I, které překračují stropy pro střední podniky stanovené v čl. 2 odst. 1 přílohy doporučení 2003/361/ES;

(b) kvalifikované poskytovatele důvěryhodných služeb a registry doménových jmen nejvyšší úrovně, jakož i poskytovatele služeb DNS bez ohledu na jejich velikost;

(c) poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací, kteří se kvalifikují jako střední podniky podle článku 2 přílohy doporučení 2003/361/ES;

(d) subjekty veřejné správy uvedené v čl. 2 odst. 2 písm. f) bodě i);

(e) všechny ostatní subjekty typu uvedeného v příloze I nebo II, které členský stát označí za základní subjekty podle čl. 2 odst. 2 písm. b) až e);

(f) subjekty označené jako kritické subjekty podle směrnice (EU) .../... [+] uvedené v čl. 2 odst. 3 této směrnice;

(g) pokud tak členský stát stanoví, subjekty, které tento členský stát identifikoval před ... [datum vstupu této směrnice v platnost] jako provozovatele základních služeb v souladu se směrnicí (EU) 2016/1148 nebo vnitrostátními právními předpisy.

2. Pro účely této směrnice se za významné subjekty považují subjekty typu uvedeného v příloze I nebo II, které se nekvalifikují jako významné subjekty podle odstavce 1 tohoto článku. To zahrnuje subjekty, které členské státy označily za důležité subjekty podle čl. 2 odst. 2 písm. b) až e).

3. Podle ... [27 měsíců ode dne vstupu této směrnice v platnost] vytvoří členské státy seznam základních a důležitých subjektů a subjektů poskytujících služby registrace doménových jmen. Členské státy tento seznam pravidelně přezkoumávají a případně aktualizují, a to nejméně každé dva roky.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22

(2020/0365(COD)).

4. Pro účely sestavení seznamu uvedeného v odstavci 3 členské státy vyžadují, aby subjekty uvedené v tomto odstavci předložily příslušným orgánům alespoň tyto informace:

(a) název subjektu;

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

(c) případně příslušné odvětví a pododvětví uvedené v příloze 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 veškeré změny údajů předložených podle prvního pododstavce tohoto odstavce neprodleně a v každém případě do dvou týdnů ode dne změny.

Komise s pomocí Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) bez zbytečného odkladu poskytne pokyny a vzory týkající se povinností stanovených v tomto odstavci.

Členské státy mohou zavést vnitrostátní mechanismy pro registraci subjektů.

5. Podle ... [27 měsíců ode dne vstupu této směrnice v platnost] a poté každé dva roky oznámí příslušné orgány:

(a) Komisi a Skupině pro spolupráci počet základních a významných subjektů uvedených v seznamu podle odstavce 3 pro každé odvětví a pododvětví uvedené v příloze I nebo II a

(b) Komisi příslušné informace o počtu základních a významných subjektů určených podle čl. 2 odst. 2 písm. b) až e), o odvětví a pododvětví uvedeném v příloze I nebo II, do kterého patří, o druhu služby, kterou poskytují, a o ustanovení z těch, která jsou uvedena v čl. 2 odst. 2 písm. b) až e), na jejichž základě byly určeny.

6. Dokud ... [27 měsíců ode dne vstupu této směrnice v platnost] a na žádost Komise mohou členské státy oznámit Komisi názvy podstatných a důležitých subjektů uvedených v odst. 5 písm. b).

Článek 4

Odvětvové právní akty Unie

1. Pokud odvětvové právní předpisy Unie vyžadují, aby zásadní nebo významné subjekty přijaly opatření k řízení rizik v oblasti kybernetické bezpečnosti nebo aby oznamovaly významné incidenty, a pokud jsou tyto požadavky svým účinkem přinejmenším rovnocenné povinnostem stanoveným v této směrnici, příslušná ustanovení této směrnice, včetně ustanovení o dohledu a prosazování stanovených v kapitole VII, se na tyto subjekty nevztahují. V případě, že
se odvětvové právní akty Unie nevztahují na všechny subjekty v určitém odvětví, které spadají do oblasti působnosti této směrnice, se příslušná ustanovení této směrnice nadále vztahují na subjekty, na které se tyto odvětvové právní akty Unie nevztahují.

2. Požadavky uvedené v odstavci 1 tohoto článku se považují za rovnocenné s povinnostmi stanovenými v této směrnici, pokud:

   (a) opatření k řízení rizik v oblasti kybernetické bezpečnosti jsou svým účinkem přinejmenším rovnocenná opatřením stanoveným v čl. 21 odst. 1 a 2; nebo

   (b) odvětvový právní akt Unie zajišťuje okamžitý, případně automatický a přímý přístup k oznámením o událostech ze strany CSIRT, příslušných orgánů nebo jednotných kontaktních míst podle této směrnice a kde jsou požadavky na oznamování závažných událostí přinejmenším rovnocenné požadavkům stanoveným v čl. 23 odst. 1 až 6 této směrnice.

3. Komise prostřednictvím ... [šest měsíců ode dne vstupu této směrnice v platnost] poskytne pokyny objasňující uplatňování odstavců 1 a 2. Komise tyto pokyny pravidelně přezkoumává. Při přípravě těchto pokynů Komise zohlední veškeré připomínky skupiny pro spolupráci a agentury ENISA.

Článek 5

Minimální harmonizace

Tato směrnice nebrání členským státům v přijetí nebo zachování ustanovení zajišťujících vyšší úroveň kybernetické bezpečnosti, pokud jsou tato ustanovení v souladu s povinnostmi členských států stanovenými v právu Unie.

Článek 6

Definice

Pro účely této směrnice platí následující definice:

(1) "síťovým a informačním systémem" se rozumí:

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

(b) jakékoliv zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí podle programu automatické zpracování digitálních dat, nebo

(c) digitální údaje uchovávané, zpracovávané, vyhledávané nebo přenášené prvky uvedenými v písmenech a) a b) pro účely jejich provozu, používání, ochrany a údržby;

(2) "bezpečností síťových a informačních systémů" se rozumí schopnost síťových a informačních systémů odolat na dané úrovni spolehlivosti jakékoli události, která by mohla ohrozit dostupnost, pravost, integritu nebo důvěrnost uložených, přenášených nebo zpracovávaných údajů nebo služeb nabízených těmito síťovými a informačními systémy nebo přístupných jejich prostřednictvím;

(3) "kybernetickou bezpečností" kybernetická bezpečnost ve smyslu definice v čl. 2 bodě 1 nařízení (EU)
2019/881;

(4) "národní strategií kybernetické bezpečnosti" se rozumí ucelený rámec členského státu, který stanoví strategické cíle a priority v oblasti kybernetické bezpečnosti a řízení k jejich dosažení v daném členském státě;

(5) "skoronehodou" se rozumí událost, která mohla ohrozit dostupnost, pravost, integritu nebo důvěrnost uložených, přenášených nebo zpracovávaných údajů nebo služeb nabízených síťovými a informačními systémy nebo přístupných jejich prostřednictvím, ale které se podařilo zabránit nebo která se neuskutečnila;

(6) "incidentem" se rozumí událost, která ohrožuje dostupnost, pravost, integritu nebo důvěrnost uložených, přenášených nebo zpracovávaných údajů nebo služeb nabízených síťovými a informačními systémy nebo přístupných jejich prostřednictvím;

(7) "rozsáhlým kybernetickým bezpečnostním incidentem" incident, který způsobí narušení v míře, jež přesahuje schopnost členského státu na něj reagovat, nebo který má významný dopad na nejméně dva členské státy;

(8) "řešením incidentů" se rozumí veškeré činnosti a postupy zaměřené na prevenci, odhalování, analýzu,
a zvládnout nebo reagovat na incident a zotavit se z něj;

(9) "rizikem" se rozumí možnost ztráty nebo narušení způsobené událostí a vyjadřuje se jako kombinace velikosti takové ztráty nebo narušení a pravděpodobnosti výskytu události;

(10) "kybernetickou hrozbou" se rozumí kybernetická hrozba podle definice v čl. 2 bodě 8 nařízení (EU) 2019/881;

(11) "významnou kybernetickou hrozbou" se rozumí kybernetická hrozba, u níž lze na základě jejích technických charakteristik předpokládat, že může mít závažný dopad na síť a informační systémy subjektu nebo na uživatele jeho služeb tím, že způsobí značnou materiální nebo nemateriální škodu;

(12) "produktem IKT" se rozumí produkt IKT definovaný v čl. 2 bodě 12 nařízení (ES) č. 1266/2009.
Nařízení (EU) 2019/881;

(13) "službou ICT" se rozumí služba ICT definovaná v čl. 2 bodě 13 nařízení (EU) 2019/881;

(14) "procesem IKT" se rozumí proces IKT definovaný v čl. 2 bodě 14 nařízení (ES) č. 1266/2006.
Nařízení (EU) 2019/881;

(15) "zranitelností" se rozumí slabost, náchylnost nebo vada produktů nebo služeb IKT. které mohou být zneužity kybernetickou hrozbou;

(16) "normou" se rozumí norma definovaná v čl. 2 bodě 1 nařízení (EU) 2016/679. Evropského parlamentu a Rady č. 1025/20121;

(17) "technickou specifikací" technická specifikace podle definice v čl. 2 bodě 4 nařízení (EU) č. 1025/2012;

(18) "internetovým výměnným bodem" se rozumí síťové zařízení, které umožňuje propojení více než dvou nezávislých sítí (autonomních systémů), především za účelem usnadnění výměny internetového provozu, které zajišťuje propojení pouze pro autonomní systémy a které nevyžaduje, aby internetový provoz procházející mezi jakoukoli dvojicí zúčastněných autonomních systémů procházel jakýmkoli třetím autonomním systémem, ani tento provoz nemění nebo jinak neruší;

[1] Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, o 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 o zrušení rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

(19) "systémem doménových jmen" nebo "DNS" se rozumí hierarchický distribuovaný systém pojmenování, který umožňuje identifikaci internetových služeb a zdrojů a umožňuje koncovým uživatelským zařízením využívat služby směrování a připojení k internetu k dosažení těchto služeb a zdrojů;

(20) "poskytovatelem služeb DNS" se rozumí subjekt, který poskytuje:

(a) veřejně dostupné služby rekurzivního překladu doménových jmen pro koncové uživatele internetu nebo

(b) autoritativní služby pro překlad názvů domén pro použití třetími stranami, s výjimkou kořenových jmenných serverů;

(21) "registrem názvů domén nejvyšší úrovně" nebo "registrem názvů TLD" se rozumí subjekt, kterému byla svěřena určitá TLD a který je odpovědný za správu TLD, včetně registrace doménových jmen pod TLD a technického provozu TLD, včetně provozu jeho jmenných serverů, údržby jeho databází a distribuce zónových souborů TLD mezi jmennými servery, bez ohledu na to, zda některou z těchto operací provádí sám subjekt nebo je zadána externě, avšak s výjimkou situací, kdy registr používá názvy TLD pouze pro vlastní potřebu;

(22) "subjektem poskytujícím služby registrace doménových jmen" se rozumí registrátor nebo zástupce jednající

jménem registrátorů, jako je poskytovatel služeb registrace soukromí nebo zmocnění nebo prodejce;

(23) "digitální službou" se rozumí služba definovaná v čl. 1 odst. 1 písm. b) nařízení (ES) č. 1308/2009.

Směrnice Evropského parlamentu a Rady (EU) 2015/15351;

(24) "službou vytvářející důvěru" služba vytvářející důvěru ve smyslu

definice v čl. 3 bodě 16 nařízení (EU) č. 910/2014;

(25) "poskytovatelem služeb vytvářejících důvěru" poskytovatel služeb vytvářejících důvěru podle definice v čl. 3 bodě 19 nařízení (ES) č. 1083/2006.

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 služeb vytvářejících důvěru" kvalifikovaný poskytovatel služeb vytvářejících důvěru, jak je definován v článku 3.

Čl. 3 bod 20 nařízení (EU) č. 910/2014;

(28) "on-line tržištěm" se rozumí on-line tržiště podle definice v čl. 2 písm. n) směrnice

Evropského parlamentu a Rady 2005/29/ES2;

---

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

2 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 (ES) č. 2006/2004.

Evropského parlamentu a Rady ("směrnice o nekalých obchodních praktikách") (Úř. věst. L 149, 11.6.2005, s. 22).

(29) "online vyhledávačem" se rozumí online vyhledávač podle definice v čl. 2 bodě 5 nařízení Evropského parlamentu a Rady (EU) 2019/11501;

(30) "službou cloud computingu" se rozumí digitální služba, která umožňuje správu na vyžádání a široký vzdálený přístup ke škálovatelnému a pružnému fondu sdílených výpočetních zdrojů, včetně případů, kdy jsou tyto zdroje rozděleny na více míst;

(31) "službou datového centra" se rozumí služba, která zahrnuje struktury nebo skupiny struktur určené k centralizovanému umístění, propojení a provozu zařízení IT a síťových zařízení poskytujících služby ukládání, zpracování a přenosu dat spolu se všemi zařízeními a infrastrukturami pro rozvod energie a kontrolu prostředí;

(32) "sítí pro doručování obsahu" se rozumí síť geograficky rozmístěných serverů pro zajištění vysoké dostupnosti, přístupnosti nebo rychlého doručování digitálního obsahu a služeb uživatelům internetu jménem poskytovatelů obsahu a služeb;

(33) "platformou pro služby sociálních sítí" se rozumí platforma, která koncovým uživatelům umožňuje vzájemné propojení, sdílení, objevování a komunikaci na různých zařízeních, zejména prostřednictvím chatů, příspěvků, videí a doporučení;

[1] 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).

(34) "zástupcem" fyzická nebo právnická osoba usazená v Unii, která je výslovně určena k jednání jménem poskytovatele služeb DNS, registru názvů TLD, subjektu poskytujícího služby registrace názvů domén, poskytovatele služeb cloud computingu, poskytovatele služeb datového centra, poskytovatele sítě pro doručování obsahu, poskytovatele spravovaných služeb, poskytovatele řízených bezpečnostních služeb nebo poskytovatele online tržiště, online vyhledávače nebo platformy služeb sociálních sítí, který není usazen v Unii, na které se může obracet příslušný orgán nebo CSIRT namísto samotného subjektu, pokud jde o povinnosti tohoto subjektu podle této směrnice;

(35) "subjektem veřejné správy" subjekt, který je za takový uznán v členském státě v souladu s vnitrostátním právem, s výjimkou soudnictví, parlamentů nebo centrálních bank, a který splňuje následující kritéria:

(a) je zřízena za účelem uspokojování potřeb v obecném zájmu a nemá průmyslový nebo obchodní charakter;

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

(c) je z větší části financován státem, regionálními orgány nebo jinými veřejnoprávními subjekty, podléhá řídícímu dohledu těchto orgánů nebo subjektů nebo má správní, řídící nebo dozorčí radu, jejíž více než polovinu členů jmenuje stát, regionální orgány nebo jiné veřejnoprávní subjekty;

(d) má pravomoc adresovat fyzickým nebo právnickým osobám správní nebo regulační rozhodnutí, která se dotýkají jejich práv při přeshraničním pohybu osob, zboží, služeb nebo kapitálu;

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

(37) "službou elektronických komunikací" se rozumí služba elektronických komunikací jako definované v čl. 2 bodě 4 směrnice (EU) 2018/1972;

(38) "subjektem" fyzická nebo právnická osoba, která byla vytvořena a uznána jako taková podle vnitrostátního práva místa svého usazení a která může jednat pod svým vlastním jménem, vykonávat práva a podléhat povinnostem;

(39) "poskytovatelem řízených služeb" se rozumí subjekt, který poskytuje služby související s instalací, správou, provozem nebo údržbou produktů IKT, sítí, infrastruktury, aplikací nebo jiných síťových a informačních systémů, a to prostřednictvím asistence nebo aktivní správy prováděné buď v prostorách zákazníka, nebo na dálku;

(40) "poskytovatelem řízených bezpečnostních služeb" se rozumí poskytovatel řízených služeb, který provádí činnosti související s řízením rizik kybernetické bezpečnosti nebo poskytuje pomoc při těchto činnostech;

(41) "výzkumnou organizací" subjekt, jehož hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj za účelem využití výsledků tohoto výzkumu ke komerčním účelům, ale který 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 stanoví strategické cíle, zdroje potřebné k dosažení těchto cílů a vhodná politická a regulační opatření s cílem dosáhnout a udržet vysokou úroveň kybernetické bezpečnosti. Vnitrostátní strategie kybernetické bezpečnosti zahrnuje:

   (a) cíle a priority strategie kybernetické bezpečnosti členského státu zahrnující zejména odvětví uvedená v přílohách I a II;

   (b) rámec řízení pro dosažení cílů a priorit uvedených v bodě 2. (a) tohoto odstavce, včetně zásad uvedených v odstavci 2;

   (c) rámec řízení, který vyjasňuje úlohy a odpovědnosti příslušných zúčastněných stran na vnitrostátní úrovni a který je základem spolupráce a koordinace na vnitrostátní úrovni mezi příslušnými orgány, jednotnými kontaktními místy a CSIRT podle této směrnice, jakož i koordinace a spolupráce mezi těmito subjekty a příslušnými orgány podle odvětvových právních aktů Unie;

(d) mechanismus pro identifikaci příslušných aktiv a posouzení rizik v daném členském státě;

(e) určení opatření zajišťujících připravenost na mimořádné události, reakci na ně a obnovu po nich, včetně spolupráce mezi veřejným a soukromým sektorem;

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

(g) politický rámec pro posílenou koordinaci mezi příslušnými orgány podle této směrnice a příslušnými orgány podle směrnice (EU) .../... [+] za účelem sdílení informací o rizicích, kybernetických hrozbách a incidentech, jakož i o nekybernetických rizicích, hrozbách a incidentech a případně o výkonu úkolů v oblasti dohledu;

(h) plán, včetně nezbytných opatření, na zvýšení obecné úrovně povědomí občanů o kybernetické bezpečnosti.

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

(a) řešení kybernetické bezpečnosti v dodavatelském řetězci produktů a služeb IKT, které subjekty využívají pro poskytování svých služeb;

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

(b) o zahrnutí a specifikaci požadavků souvisejících s kybernetickou bezpečností produktů a služeb IKT do veřejných zakázek, včetně požadavků na certifikaci kybernetické bezpečnosti, šifrování a používání kybernetických bezpečnostních produktů s otevřeným zdrojovým kódem;

(c) řízení zranitelností, včetně podpory a usnadnění koordinovaného zveřejňování zranitelností podle čl. 12 odst. 1;

(d) související s udržením obecné dostupnosti, integrity a důvěrnosti veřejného jádra otevřeného internetu, včetně případné kybernetické bezpečnosti podmořských komunikačních kabelů;

(e) podpora vývoje a integrace příslušných pokročilých technologií s cílem zavést nejmodernější opatření pro řízení rizik v oblasti kybernetické bezpečnosti;

(f) podpora a rozvoj vzdělávání a odborné přípravy v oblasti kybernetické bezpečnosti, dovedností v oblasti kybernetické bezpečnosti, zvyšování povědomí a iniciativ v oblasti výzkumu a vývoje, jakož i pokyny týkající se správných postupů a kontrol v oblasti kybernetické hygieny, které jsou určeny občanům, zúčastněným stranám a subjektům;

(g) podpora akademických a výzkumných institucí při vývoji, zdokonalování a propagaci zavádění nástrojů kybernetické bezpečnosti a bezpečné síťové infrastruktury;

(h) včetně příslušných postupů a vhodných nástrojů pro sdílení informací na podporu dobrovolného sdílení informací o kybernetické bezpečnosti mezi subjekty v souladu s právem Unie;

(i) posílení kybernetické odolnosti a základní úrovně kybernetické hygieny malých a středních podniků, zejména těch, které jsou vyloučeny z oblasti působnosti této směrnice, a to poskytováním snadno dostupných pokynů a pomoci pro jejich specifické potřeby;

(j) podpora aktivní kybernetické ochrany.

3. Členské státy oznámí své vnitrostátní 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 nejméně jednou za pět let vyhodnocují své vnitrostátní strategie kybernetické bezpečnosti na základě klíčových ukazatelů výkonnosti a v případě potřeby je aktualizují. 2. Agentura ENISA je členským státům na jejich žádost nápomocna při vypracovávání nebo aktualizaci vnitrostátní strategie kybernetické bezpečnosti a klíčových ukazatelů výkonnosti pro hodnocení této strategie, aby ji sladila s požadavky a povinnostmi stanovenými v této směrnici.

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 za úkoly dohledu uvedené v kapitole VII (příslušné orgány).

2. Příslušné orgány uvedené v odstavci 1 sledují provádění této směrnice na vnitrostátní úrovni.

3. Každý členský stát určí nebo zřídí jediné kontaktní místo. Pokud členský stát určí nebo zřídí pouze jeden příslušný orgán podle odstavce 1, je tento příslušný orgán rovněž jediným kontaktním místem pro tento členský stát.

4. Každé jednotné kontaktní místo vykonává styčnou funkci pro zajištění přeshraniční spolupráce orgánů svého členského státu s příslušnými orgány jiných členských států a případně s Komisí a agenturou ENISA, jakož i pro zajištění meziodvětvové spolupráce s ostatními příslušnými orgány v rámci svého členského státu.

5. Členské státy zajistí, aby jejich příslušné orgány a jednotná kontaktní místa měly dostatečné zdroje k účinnému a účelnému plnění úkolů, které jim byly svěřeny, a tím i k plnění cílů této směrnice.

6. Každý členský stát bez zbytečného odkladu oznámí Komisi totožnost příslušného orgánu uvedeného v odstavci 1 a jednotného kontaktního místa uvedeného v odstavci 3, úkoly těchto orgánů a jakékoli jejich následné změny. Každý členský stát zveřejní totožnost svého příslušného orgánu.
Komise zveřejní seznam jednotných kontaktních míst.

Článek 9

Národní rámce pro řešení kybernetických krizí

1. Každý členský stát určí nebo zřídí jeden nebo více příslušných orgánů odpovědných za řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí (orgány pro řešení kybernetických krizí). Členské státy zajistí, aby tyto orgány měly dostatečné zdroje k účinnému a efektivnímu plnění úkolů, které jim byly svěřeny. Členské státy zajistí soulad se stávajícími rámci pro obecné vnitrostátní krizové řízení.

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

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

4. Každý členský stát přijme vnitrostátní plán reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize, v němž stanoví cíle a opatření pro zvládání rozsáhlých kybernetických bezpečnostních incidentů a krizí. Tento plán stanoví zejména:

   (a) cíle národních opatření a činností v oblasti připravenosti;

(b) úkoly a povinnosti orgánů příslušných k řešení kybernetických krizí;

(c) postupy pro řešení kybernetických krizí, včetně jejich začlenění do obecného vnitrostátního rámce pro řešení krizí a kanálů pro výměnu informací;

(d) opatření národní připravenosti, včetně cvičení a školení;

(e) příslušné veřejné a soukromé zúčastněné strany a zapojenou infrastrukturu;

(f) vnitrostátní postupy a ujednání mezi příslušnými vnitrostátními orgány a subjekty s cílem zajistit účinnou účast členského státu na koordinovaném řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí na úrovni Unie a jeho podporu.

5. Do tří měsíců od určení nebo zřízení orgánu příslušného k řešení kybernetických krizí podle odstavce 1 oznámí každý členský stát Komisi totožnost svého orgánu a veškeré jeho následné změny. 3. Členské státy předloží Komisi a evropské síti styčných organizací pro řešení kybernetických krizí
(EU-CyCLONe) příslušné informace týkající se požadavků odstavce 4 o svých vnitrostátních plánech reakce na rozsáhlé kybernetické bezpečnostní incidenty a krize do tří měsíců od přijetí těchto plánů. Členské státy mohou informace vyloučit, pokud je to nezbytné pro jejich národní bezpečnost a v takovém rozsahu, v jakém je to nezbytné.

Článek 10

Týmy pro reakci na počítačové bezpečnostní incidenty (CSIRT)

1. Každý členský stát určí nebo zřídí jeden nebo více CSIRT. CSIRT mohou být určeny nebo zřízeny v rámci příslušného orgánu. Týmy CSIRT musí splňovat požadavky stanovené v čl. 11 odst. 1, musí pokrývat alespoň odvětví, pododvětví a typy subjektů uvedené v přílohách I a II a musí být odpovědné za řešení incidentů v souladu s přesně definovaným postupem.

2. Členské státy zajistí, aby každý CSIRT měl dostatečné zdroje k účinnému plnění svých úkolů, jak je stanoveno v čl. 11 odst. 3.

3. Členské státy zajistí, aby každý CSIRT měl k dispozici vhodnou, bezpečnou a odolnou komunikační a informační infrastrukturu, jejímž prostřednictvím si může vyměňovat informace se základními a důležitými subjekty a dalšími příslušnými zúčastněnými stranami. Za tímto účelem členské státy zajistí, aby každý CSIRT přispíval k zavádění nástrojů pro bezpečnou výměnu informací.

4. CSIRT spolupracují a případně si vyměňují příslušné informace v souladu s článkem 29 s odvětvovými nebo meziodvětvovými společenstvími zásadních a významných subjektů.

5. CSIRT se účastní vzájemných hodnocení organizovaných v souladu s článkem 19.

6. Členské státy zajistí účinnou, efektivní a bezpečnou spolupráci svých CSIRT v síti CSIRT.

7. CSIRT mohou navázat spolupráci s národními týmy pro reakci na počítačové bezpečnostní incidenty třetích zemí. V rámci těchto vztahů spolupráce členské státy usnadňují účinnou, efektivní a bezpečnou výměnu informací s národními týmy třetích zemí pro reakci na počítačové bezpečnostní incidenty za použití příslušných protokolů pro sdílení informací, včetně protokolu "semafor". Týmy CSIRT si mohou s národními týmy třetích zemí pro reakci na počítačové bezpečnostní incidenty vyměňovat příslušné informace, včetně osobních údajů v souladu s právem Unie v oblasti ochrany údajů.

8. CSIRT mohou spolupracovat s národními týmy pro řešení počítačových bezpečnostních incidentů třetích zemí nebo s rovnocennými orgány třetích zemí, zejména za účelem poskytování pomoci v oblasti kybernetické bezpečnosti.

9. Každý členský stát bez zbytečného odkladu oznámí Komisi totožnost CSIRT uvedeného v odstavci 1 tohoto článku a CSIRT určeného jako koordinátor podle čl. 12 odst. 1, jejich příslušné úkoly ve vztahu k základním a důležitým subjektům a veškeré jejich následné změny.

10. Členské státy mohou požádat agenturu ENISA o pomoc při vytváření svých CSIRT.

Článek 11

Požadavky, technické schopnosti a úkoly CSIRT

1. CSIRT musí splňovat následující požadavky:

(a) týmy CSIRT zajistí vysokou úroveň dostupnosti svých komunikačních kanálů tím, že se vyhnou jediným bodům selhání, a mají k dispozici několik způsobů, jak být kdykoli kontaktován a jak kontaktovat ostatní; jasně specifikují komunikační kanály a informují o nich složky a spolupracující partnery;

(b) prostory CSIRT a podpůrné informační systémy se nacházejí na adrese zabezpečené stránky;

(c) týmy CSIRT musí být vybaveny vhodným systémem pro správu a směrování žádostí, zejména pro usnadnění účinného a efektivního předávání;

(d) CSIRT zajistí důvěrnost a důvěryhodnost svých operací;

(e) týmy CSIRT musí mít dostatečný počet zaměstnanců, aby byla zajištěna nepřetržitá dostupnost jejich služeb, a musí zajistit, aby jejich zaměstnanci byli náležitě vyškoleni;

(f) CSIRT jsou vybaveny redundantními systémy a záložními pracovními prostory, aby byla zajištěna kontinuita jejich služeb.

CSIRT se mohou účastnit mezinárodních sítí spolupráce.

2. Členské státy zajistí, aby jejich CSIRT společně disponovaly technickými možnostmi nezbytnými k plnění úkolů uvedených v odstavci 3. Členské státy zajistí, aby jejich CSIRT byly přiděleny dostatečné zdroje k zajištění odpovídajícího počtu zaměstnanců, aby CSIRT mohly rozvíjet své technické schopnosti.

3. Úkoly CSIRT jsou následující:

(a) sledování a analýza kybernetických hrozeb, zranitelností a incidentů na vnitrostátní úrovni a na požádání poskytování pomoci dotčeným základním a důležitým subjektům, pokud jde o sledování jejich sítí a informačních systémů v reálném čase nebo téměř v reálném čase;

(b) poskytování včasných varování, výstrah, oznámení a šíření informací o kybernetických hrozbách, zranitelnostech a incidentech zásadním a důležitým dotčeným subjektům, jakož i příslušným orgánům a dalším relevantním zúčastněným stranám, pokud možno téměř v reálném čase;

(c) reakce na incidenty a případné poskytování pomoci dotčeným základním a důležitým subjektům;

(d) shromažďování a analýza forenzních dat a poskytování dynamické analýzy rizik a incidentů a povědomí o situaci v oblasti kybernetické bezpečnosti;

(e) na žádost zásadního nebo důležitého subjektu proaktivní skenování sítě a informačních systémů dotčeného subjektu s cílem odhalit zranitelnosti s potenciálním významným dopadem;

(f) účast v síti CSIRT a poskytování vzájemné pomoci v souladu s jejich schopnostmi a kompetencemi ostatním členům sítě CSIRT na jejich žádost;

(g) případně působí jako koordinátor pro účely koordinovaného odhalování zranitelnosti podle čl. 12 odst. 1;

(h) přispívat k zavádění nástrojů pro bezpečné sdílení informací podle čl. 10 odst. 3.

CSIRT mohou provádět proaktivní nerušivé skenování veřejně přístupných sítí a informačních systémů základních a důležitých subjektů. Toto skenování se provádí s cílem odhalit zranitelné nebo nezabezpečené síťové a informační systémy a informovat o tom dotčené subjekty. Toto prověřování nesmí mít žádný negativní dopad na fungování služeb těchto subjektů.

Při provádění úkolů uvedených v prvním pododstavci mohou týmy CSIRT stanovit priority jednotlivých úkolů na základě přístupu založeného na riziku.

4. CSIRT naváže spolupráci s příslušnými zúčastněnými stranami v soukromém sektoru za účelem dosažení cílů této směrnice.

5. Za účelem usnadnění spolupráce uvedené v odstavci 4 podporují CSIRT přijetí a používání společných nebo standardizovaných postupů, klasifikačních schémat a taxonomií v souvislosti s:

(a) postupy pro řešení incidentů;

(b) krizové řízení a

(c) koordinované zveřejnění zranitelnosti podle čl. 12 odst. 1.

Článek 12

Koordinované zveřejňování zranitelností a evropská databáze zranitelností

1. Každý členský stát určí jeden ze svých CSIRT jako koordinátora pro účely koordinovaného odhalování zranitelností. CSIRT určený jako koordinátor působí jako důvěryhodný prostředník, který v případě potřeby na žádost jedné ze stran usnadňuje interakci mezi fyzickou nebo právnickou osobou, která zranitelnost ohlásila, a výrobcem nebo poskytovatelem potenciálně zranitelných produktů nebo služeb IKT. Úkoly CSIRT určeného jako koordinátor zahrnují:

(a) identifikace a kontaktování dotčených subjektů;

(b) pomoc fyzickým nebo právnickým osobám, které ohlásily zranitelnost, a

(c) vyjednávání časových harmonogramů zveřejnění a správa zranitelností, které se týkají více subjektů.

Členské státy zajistí, aby fyzické nebo právnické osoby mohly anonymně nahlásit zranitelnost, pokud o to požádají, týmu CSIRT určenému jako koordinátor. CSIRT určený jako koordinátor zajistí, aby byla v souvislosti s nahlášenou zranitelností provedena důsledná následná opatření, a zajistí anonymitu fyzické nebo právnické osoby, která zranitelnost nahlásila. Pokud by nahlášená zranitelnost mohla mít významný dopad na subjekty ve více než jednom členském státě, CSIRT určený jako koordinátor každého dotčeného členského státu případně spolupracuje s ostatními CSIRT určenými jako koordinátoři v rámci sítě CSIRT.

2. Agentura ENISA po konzultaci se skupinou pro spolupráci vytvoří a udržuje evropskou databázi zranitelností. Za tímto účelem agentura ENISA zřídí a udržuje vhodné informační systémy, politiky a postupy a přijme nezbytná technická a organizační opatření k zajištění bezpečnosti a integrity evropské databáze zranitelností, zejména s cílem umožnit subjektům, bez ohledu na to, zda spadají do oblasti působnosti této směrnice, a jejich dodavatelům síťových a informačních systémů dobrovolně zveřejňovat a registrovat veřejně známé zranitelnosti produktů nebo služeb IKT. Všem zúčastněným stranám bude umožněn přístup k informacím o zranitelnostech obsažených v evropské databázi zranitelností. Tato databáze obsahuje:

(a) informace popisující zranitelnost;

(b) postižené produkty nebo služby ICT a závažnost zranitelnosti z hlediska okolností, za nichž může být zneužita;

(c) dostupnost příslušných záplat a v případě, že záplaty nejsou k dispozici, pokyny příslušných orgánů nebo CSIRT určené uživatelům zranitelných produktů a služeb IKT, jak lze rizika vyplývající z odhalených zranitelností zmírnit.

Článek 13

Spolupráce na vnitrostátní úrovni

1. Pokud jsou příslušné orgány, jednotné kontaktní místo a CSIRT téhož členského státu oddělené, spolupracují při plnění povinností stanovených v této směrnici.

2. Členské státy zajistí, aby jejich týmy CSIRT nebo případně jejich příslušné orgány dostávaly oznámení o významných incidentech podle článku 23 a o incidentech, kybernetických hrozbách a téměř nehodách podle článku 30.

3. Členské státy zajistí, aby jejich týmy CSIRT nebo případně jejich příslušné orgány informovaly svá jednotná kontaktní místa o oznámeních incidentů, kybernetických hrozeb a skoronehod podaných podle této směrnice.

4. Aby bylo zajištěno účinné plnění úkolů a povinností příslušných orgánů, jednotných kontaktních míst a CSIRT, zajistí členské státy v co největším rozsahu vhodnou spolupráci mezi těmito subjekty a donucovacími orgány, orgány pro ochranu údajů, vnitrostátními orgány podle nařízení (ES) č. 300/2008 a (EU) 2018/1139, orgány dozoru podle nařízení (EU) č. 910/2014, příslušnými orgány podle nařízení (EU) .../.... [+], vnitrostátní regulační orgány podle směrnice (EU) 2018/1972, příslušné orgány podle směrnice (EU) .../.... [++, **jakož**] i příslušné orgány podle jiných odvětvových právních aktů Unie v daném členském státě.

[+] Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

[++] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

5. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice a jejich příslušné orgány podle směrnice (EU) .../... [+] spolupracovaly a pravidelně si vyměňovaly informace týkající se identifikace kritických subjektů, rizik, kybernetických hrozeb a incidentů, jakož i nekybernetických rizik, hrozeb a incidentů, které mají vliv na subjekty identifikované jako kritické subjekty podle směrnice (EU) .../. ...[+], a o opatřeních přijatých v reakci na tato rizika, hrozby a incidenty. Členské státy rovněž zajistí, aby jejich příslušné orgány podle této směrnice a jejich příslušné orgány podle nařízení (EU) č. 910/2014, nařízení (EU) .../.....[++] a směrnice (EU) 2018/1972 pravidelně vyměňovaly příslušné informace, a to i s ohledem na příslušné incidenty a kybernetické hrozby.

6. Členské státy zjednoduší podávání zpráv technickými prostředky pro oznámení uvedená v článcích 23 a 30.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

[++] Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS. 41/22 (2020/0266(COD)).

Kapitola III

Spolupráce na úrovni Unie a na mezinárodní úrovni

Článek 14 Skupina pro spolupráci

1. S cílem podpořit a usnadnit strategickou spolupráci a výměnu informací mezi členskými státy a posílit důvěru se zřizuje skupina pro spolupráci.

2. Skupina pro spolupráci plní své úkoly na základě dvouletých pracovních programů uvedených v odstavci 7.

3. Skupina pro spolupráci se skládá ze zástupců členských států, Komise a agentury ENISA. Evropská služba pro vnější činnost se účastní činnosti skupiny pro spolupráci jako pozorovatel. Evropské orgány dohledu (ESA) a příslušné orgány podle nařízení (EU) .../.....[+] se mohou účastnit činností skupiny pro spolupráci v souladu s čl. 47 odst. 1 uvedeného nařízení.

[+] Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS. 41/22 (2020/0266(COD)).

Skupina pro spolupráci může v případě potřeby přizvat k účasti na své práci Evropský parlament a zástupce příslušných zúčastněných stran.

Sekretariát zajišťuje Komise.

4. Skupina pro spolupráci má tyto úkoly:

(a) poskytovat příslušným orgánům pokyny týkající se provedení a provádění této směrnice;

(b) poskytovat pokyny příslušným orgánům v souvislosti s vypracováním a prováděním politik koordinovaného zveřejňování informací o zranitelnosti, jak je uvedeno v čl. 7 odst. 2 písm. c);

(c) vyměňovat si osvědčené postupy a informace v souvislosti s prováděním této směrnice, a to i pokud jde o kybernetické hrozby, incidenty, zranitelná místa, skoronehody, iniciativy na zvyšování povědomí, odbornou přípravu, cvičení a dovednosti, budování kapacit, normy a technické specifikace, jakož i určení základních a důležitých subjektů podle čl. 2 odst. 2 písm. b) až e);

(d) vyměňovat si s Komisí rady a spolupracovat s ní na nových politických iniciativách v oblasti kybernetické bezpečnosti a na celkové konzistenci požadavků na kybernetickou bezpečnost v jednotlivých odvětvích;

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

(f) vyměňovat si osvědčené postupy a informace s příslušnými orgány, institucemi a agenturami Unie;

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

(h) v případě potřeby projednat zprávy o vzájemném hodnocení uvedeném v čl. 19 odst. 9 a vypracovat závěry a doporučení;

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

(j) projednávat případy vzájemné pomoci, včetně zkušeností a výsledků přeshraničních společných akcí v oblasti dohledu podle článku 37;

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

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

(m) výměna názorů na politiku následných opatření po rozsáhlých kybernetických bezpečnostních incidentech a krizích na základě zkušeností získaných v rámci sítě CSIRT a EU-CyCLONe;

(n) přispět ke schopnostem v oblasti kybernetické bezpečnosti v celé Unii tím, že usnadní výměnu vnitrostátních úředníků prostřednictvím programu budování kapacit, do něhož se zapojí pracovníci příslušných orgánů nebo CSIRT;

(o) pořádat pravidelná společná setkání s příslušnými soukromými zúčastněnými stranami z celé Unie, na nichž se projednávají činnosti prováděné skupinou pro spolupráci a shromažďují se podněty k novým politickým výzvám;

(p) projednat práci, která byla vykonána v souvislosti s cvičeními v oblasti kybernetické bezpečnosti, včetně práce agentury ENISA;

(q) stanovit metodiku a organizační aspekty vzájemných hodnocení uvedených v čl. 19 odst. 1, jakož i metodiku sebehodnocení pro členské státy v souladu s čl. 19 odst. 5, a to za pomoci Komise a agentury ENISA, a ve spolupráci s Komisí a agenturou ENISA vypracovat kodexy chování, které budou základem pracovních metod určených odborníků na kybernetickou bezpečnost v souladu s čl. 19 odst. 6;

(r) vypracovávat zprávy pro účely přezkumu uvedeného v článku 40 o zkušenostech získaných na strategické úrovni a ze vzájemných hodnocení;

(s) pravidelně projednávat a provádět hodnocení aktuálního stavu kybernetických hrozeb nebo incidentů, jako je ransomware.

Skupina pro spolupráci předkládá zprávy uvedené v prvním pododstavci písm. r) Komisi, Evropskému parlamentu a Radě.

5. Členské státy zajistí účinnou, efektivní a bezpečnou spolupráci svých zástupců ve skupině pro spolupráci.

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

7. Do 1. února 2024 a poté každé dva roky skupina pro spolupráci vypracuje pracovní program týkající se opatření, která mají být přijata k provádění jejích cílů a úkolů.

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

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

   Komise si vyměňuje rady a spolupracuje se skupinou pro spolupráci na návrzích prováděcích aktů uvedených v prvním pododstavci tohoto odstavce v souladu s odst. 4 písm. e).

9. Skupina pro spolupráci se pravidelně a v každém případě alespoň jednou ročně setkává se skupinou pro odolnost kritických subjektů zřízenou podle směrnice (EU)... /.....[+] na podporu a usnadnění strategické spolupráce a výměny informací.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

Článek 15 Síť

CSIRT

1. S cílem přispět k rozvoji důvěry a důvěryhodnosti a podpořit rychlou a účinnou operativní spolupráci mezi členskými státy se zřizuje síť národních CSIRT.

2. Síť CSIRT tvoří zástupci CSIRT určených nebo zřízených podle článku 10 a tým pro reakci na počítačové hrozby pro orgány, instituce a agentury Unie (CERT-EU). Komise se účastní sítě CSIRT jako pozorovatel. Agentura ENISA zajišťuje sekretariát a aktivně pomáhá při spolupráci mezi CSIRT.

3. Síť CSIRT má tyto úkoly:

   (a) vyměňovat si informace o schopnostech CSIRT;

   (b) usnadnit sdílení, přenos a výměnu technologií a příslušných opatření, politik, nástrojů, postupů, osvědčených postupů a rámců mezi CSIRT;

   (c) vyměňovat si relevantní informace o incidentech, skoronehodách, kybernetických hrozbách, rizicích a zranitelnostech;

   (d) vyměňovat si informace o publikacích a doporučeních týkajících se kybernetické bezpečnosti;

(e) zajistit interoperabilitu s ohledem na specifikace a protokoly pro sdílení informací;

(f) na žádost člena sítě CSIRT, který je potenciálně dotčen incidentem, vyměňovat a projednávat informace týkající se tohoto incidentu a souvisejících kybernetických hrozeb, rizik a zranitelností;

(g) na žádost člena sítě CSIRT projednat a případně provést koordinovanou reakci na incident, který byl zjištěn v rámci jurisdikce tohoto členského státu;

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

(i) spolupracovat, vyměňovat si osvědčené postupy a poskytovat pomoc CSIRT určeným jako koordinátoři podle čl. 12 odst. 1, pokud jde o řízení koordinovaného odhalování zranitelností, které by mohly mít významný dopad na subjekty ve více než jednom členském státě;

(j) projednat a určit další formy operativní spolupráce, mimo jiné v souvislosti s:

(i) kategorie kybernetických hrozeb a incidentů;

(ii) včasné varování;

(iii) vzájemná pomoc;

(iv) zásady a opatření pro koordinaci reakce na přeshraniční rizika a události;

(v) příspěvek k vnitrostátnímu plánu reakce na kybernetické bezpečnostní incidenty a krize velkého rozsahu uvedenému v čl. 9 odst. 4 na žádost členského státu;

(k) informovat skupinu pro spolupráci o její činnosti a o dalších formách operativní spolupráce projednávaných podle písmene j) a v případě potřeby si v tomto ohledu vyžádat pokyny;

(l) zhodnotit cvičení v oblasti kybernetické bezpečnosti, včetně cvičení organizovaných agenturou ENISA;

(m) na žádost jednotlivého CSIRT projednat schopnosti a připravenost tohoto CSIRT;

(n) spolupracovat a vyměňovat si informace s bezpečnostními operačními středisky (SOC) na regionální a unijní úrovni s cílem zlepšit společné situační povědomí o incidentech a kybernetických hrozbách v celé Unii;

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

(p) poskytnout pokyny s cílem usnadnit sbližování operačních postupů, pokud jde o uplatňování ustanovení tohoto článku týkajících se operativní spolupráce.

4. Do ... 24 měsíců ode dne vstupu této směrnice v platnost a poté každé dva roky provede síť CSIRT pro účely přezkumu uvedeného v odstavci ....
článek 40, posoudí pokrok dosažený v oblasti operativní spolupráce a přijme zprávu. Zpráva obsahuje zejména závěry a doporučení na základě výsledků vzájemných hodnocení uvedených v článku 19, která jsou prováděna ve vztahu k národním CSIRT. Tato zpráva se předkládá skupině pro spolupráci.

5. Síť CSIRT přijme svůj jednací řád.

6. Síť CSIRT a EU-CyCLONe se dohodnou na procesních opatřeních a spolupracují na jejich základě.

Článek 16

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

1. EU-CyCLONe je zřízena na podporu koordinovaného řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí na operativní úrovni a na zajištění pravidelné výměny příslušných informací mezi členskými státy a orgány, institucemi a agenturami Unie.

2. EU-CyCLONe se skládá ze zástupců orgánů členských států pro řešení kybernetických krizí a v případech, kdy potenciální nebo probíhající rozsáhlý kybernetický bezpečnostní incident má nebo může mít významný dopad na služby a činnosti spadající do oblasti působnosti této směrnice, také z Komise. V ostatních případech se Komise účastní činností EU-CyCLONe jako pozorovatel.

Agentura ENISA zajišťuje sekretariát EU-CyCLONe a podporuje bezpečnou výměnu informací a poskytuje nezbytné nástroje na podporu spolupráce mezi členskými státy, které zajišťují bezpečnou výměnu informací.

V případě potřeby může EU-CyCLONe přizvat zástupce příslušných zúčastněných stran, aby se účastnili jeho práce jako pozorovatelé.

3. EU-CyCLONe má tyto úkoly:

(a) zvýšit úroveň připravenosti na zvládání rozsáhlých kybernetických bezpečnostních incidentů a krizí;

(b) vytvořit sdílené situační povědomí o rozsáhlých kybernetických bezpečnostních incidentech a krizích;

(c) posoudit důsledky a dopady příslušných rozsáhlých kybernetických bezpečnostních incidentů a krizí a navrhnout možná opatření ke zmírnění jejich následků;

(d) koordinovat řízení rozsáhlých kybernetických bezpečnostních incidentů a krizí a podporovat rozhodování na politické úrovni v souvislosti s těmito incidenty a krizemi;

(e) na žádost dotčeného členského státu projednat vnitrostátní plány reakce na kybernetické bezpečnostní incidenty a krize velkého rozsahu uvedené v čl. 9 odst. 4.

4. EU-CyCLONe přijme svůj jednací řád.

5. EU-CyCLONe podává skupině pro spolupráci pravidelné zprávy o zvládání rozsáhlých kybernetických bezpečnostních incidentů a krizí, jakož i o trendech, se zaměřením zejména na jejich dopad na zásadní a důležité subjekty.

6. EU-CyCLONe spolupracuje se sítí CSIRT na základě dohodnutých procesních opatření stanovených v čl. 15 odst. 6.

7. Podle ... [18 měsíců ode dne vstupu této směrnice v platnost] a poté každých 18 měsíců předloží EU-CyCLONe Evropskému parlamentu a Radě zprávu hodnotící jeho práci.

Článek 17

Mezinárodní spolupráce

Unie může v případě potřeby uzavírat mezinárodní dohody v souladu s čl. 3 odst. 1 písm. a) a b). Článek 218 SFEU, se třetími zeměmi nebo mezinárodními organizacemi, umožňující a organizující jejich účast na konkrétních činnostech skupiny pro spolupráci, sítě CSIRT.
a 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 přijme ve spolupráci s Komisí a skupinou pro spolupráci každé dva roky zprávu o stavu kybernetické bezpečnosti v Unii a předloží ji Evropskému parlamentu. Zpráva se mimo jiné zpřístupní ve strojově čitelných údajích a obsahuje následující údaje:

   (a) posouzení rizik kybernetické bezpečnosti na úrovni Unie s přihlédnutím ke stavu kybernetických hrozeb;

   (b) posouzení rozvoje schopností v oblasti kybernetické bezpečnosti ve veřejném a 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) souhrnné hodnocení výsledků vzájemných hodnocení podle článku 19;

(e) souhrnné posouzení úrovně vyspělosti schopností a zdrojů kybernetické bezpečnosti v celé Unii, včetně těch na odvětvové úrovni, jakož i míry sladění vnitrostátních strategií kybernetické bezpečnosti členských států.

2. Zpráva obsahuje konkrétní politická doporučení s cílem řešit nedostatky a zvýšit úroveň kybernetické bezpečnosti v celé Unii a shrnutí zjištění za dané období z technických situačních zpráv o kybernetické bezpečnosti EU týkajících se incidentů a kybernetických hrozeb, které vypracovala agentura ENISA v souladu s čl. 7 odst. 6 nařízení (EU) 2019/881.

3. Agentura ENISA ve spolupráci s Komisí, skupinou pro spolupráci a sítí CSIRT vypracuje metodiku souhrnného hodnocení uvedeného v odst. 1 písm. e), včetně příslušných proměnných, jako jsou kvantitativní a kvalitativní ukazatele.

Článek 19

Vzájemné

hodnocení

1. Skupina pro spolupráci do ... [24 měsíců ode dne vstupu této směrnice v platnost] s pomocí Komise a agentury ENISA a případně sítě CSIRT stanoví metodiku a organizační aspekty vzájemných hodnocení s cílem poučit se ze společných zkušeností, posílit vzájemnou důvěru, dosáhnout vysoké společné úrovně kybernetické bezpečnosti, jakož i posílit schopnosti členských států v oblasti kybernetické bezpečnosti a politiky nezbytné k provádění této směrnice. Účast na vzájemných hodnoceních je dobrovolná. Vzájemná hodnocení provádějí odborníci na kybernetickou bezpečnost. Odborníci na kybernetickou bezpečnost jsou jmenováni nejméně dvěma členskými státy, odlišnými od členského státu, který je předmětem přezkumu.

   Vzájemné hodnocení se týká alespoň jednoho z následujících bodů:

   (a) úroveň provádění opatření pro řízení rizik v oblasti kybernetické bezpečnosti a povinnosti podávat zprávy stanovené v článcích 21 a 23;

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

(c) operační schopnosti CSIRT;

(d) úroveň provádění vzájemné pomoci podle článku 37;

(e) úroveň provádění ujednání o sdílení informací v oblasti kybernetické bezpečnosti uvedených v článku 29;

(f) specifické otázky přeshraniční nebo meziodvětvové povahy.

2. Metodika uvedená v odstavci 1 zahrnuje objektivní, nediskriminační, spravedlivá a transparentní kritéria, na jejichž základě členské státy určí odborníky na kybernetickou bezpečnost způsobilé k provádění vzájemných hodnocení. Komise a agentura ENISA se vzájemných hodnocení účastní jako pozorovatelé.

3. Členské státy mohou pro účely vzájemného hodnocení určit konkrétní otázky uvedené v odst. 1 písm. f).

4. Před zahájením vzájemného hodnocení podle odstavce 1 oznámí členské státy zúčastněným členským státům jeho rozsah, včetně konkrétních problémů zjištěných podle odstavce 3.

5. Před zahájením vzájemného hodnocení mohou členské státy provést. sebehodnocení přezkoumávaných aspektů a poskytnout toto sebehodnocení určeným odborníkům na kybernetickou bezpečnost. Skupina pro spolupráci s pomocí Komise a agentury ENISA stanoví metodiku pro sebehodnocení členských států.

6. Vzájemné hodnocení zahrnuje fyzické nebo virtuální návštěvy na místě a výměnu informací mimo místo. V souladu se zásadou řádné spolupráce poskytne členský stát, který je předmětem vzájemného hodnocení, určeným odborníkům na kybernetickou bezpečnost informace nezbytné pro posouzení, aniž je dotčeno právo Unie nebo vnitrostátní právo týkající se ochrany důvěrných nebo utajovaných informací a ochrany základních funkcí státu, jako je národní bezpečnost. 3. Skupina pro spolupráci ve spolupráci s Komisí a agenturou ENISA vypracuje vhodné kodexy chování, které budou základem pracovních metod určených odborníků na kybernetickou bezpečnost. Veškeré informace získané v rámci vzájemného hodnocení se použijí výhradně k tomuto účelu. Odborníci na kybernetickou bezpečnost, kteří se účastní vzájemného hodnocení, nesdělí žádné citlivé nebo důvěrné informace získané v průběhu tohoto vzájemného hodnocení třetím stranám.

7. Jakmile je jednou provedeno vzájemné hodnocení, nesmí být tytéž aspekty přezkoumávané v členském státě předmětem dalšího vzájemného hodnocení v tomto členském státě po dobu dvou let od ukončení vzájemného hodnocení, pokud členský stát nepožádá o něco jiného nebo pokud se na návrh skupiny pro spolupráci nedohodne jinak.

8. Členské státy zajistí, aby jakékoli riziko střetu zájmů týkající se určených odborníků na kybernetickou bezpečnost bylo před zahájením vzájemného hodnocení oznámeno ostatním členským státům, skupině pro spolupráci, Komisi a agentuře ENISA. Členský stát, na který se vztahuje vzájemné hodnocení, může vznést námitky proti jmenování konkrétních odborníků na kybernetickou bezpečnost na základě řádně odůvodněných důvodů, které sdělí jmenujícímu členskému státu.

9. Odborníci na kybernetickou bezpečnost, kteří se účastní vzájemných hodnocení, vypracují zprávy o zjištěních a závěrech vzájemných hodnocení. Členské státy, jichž se vzájemné hodnocení týká, mohou k návrhům zpráv, které se jich týkají, předložit připomínky, které se ke zprávám připojí. Zprávy obsahují doporučení umožňující zlepšení aspektů, jichž se vzájemné hodnocení týká. Zprávy se předkládají skupině pro spolupráci a případně síti CSIRT. Členský stát, který je předmětem vzájemného hodnocení, se může rozhodnout, že svou zprávu nebo její redigovanou verzi zveřejní.

Kapitola IV

Opatření pro řízení rizik v oblasti kybernetické bezpečnosti a povinnosti podávání zpráv

Článek 20

Správa a řízení

1. Členské státy zajistí, aby řídicí orgány základních a významných subjektů schvalovaly opatření k řízení rizik v oblasti kybernetické bezpečnosti přijatá těmito subjekty za účelem dosažení souladu s článkem 21, dohlížely na jejich provádění a mohly nést odpovědnost za porušení uvedeného článku ze strany těchto subjektů.

   Použitím tohoto odstavce není dotčeno vnitrostátní právo, pokud jde o pravidla odpovědnosti použitelná na veřejné instituce, jakož i odpovědnost státních zaměstnanců a volených nebo jmenovaných úředníků.

2. Členské státy zajistí, aby členové řídících orgánů základních a významných subjektů byli povinni absolvovat školení, a podpoří základní a významné subjekty, aby podobné školení pravidelně nabízely svým zaměstnancům, aby získali dostatečné znalosti a dovednosti, které jim umožní identifikovat rizika a posoudit postupy řízení kybernetických rizik a jejich dopad na služby poskytované subjektem.

Článek 21

Opatření pro řízení rizik v oblasti kybernetické bezpečnosti

1. Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická, provozní a organizační opatření k řízení rizik, která představují pro bezpečnost síťových a informačních systémů, jež tyto subjekty používají pro své operace nebo poskytování svých služeb, a k předcházení nebo minimalizaci dopadu incidentů na příjemce jejich služeb a na jiné služby.

   S přihlédnutím k nejnovějším poznatkům a případně k příslušným evropským a mezinárodním normám, jakož i k nákladům na provedení, zajistí opatření uvedená v prvním pododstavci úroveň bezpečnosti sítí a informačních systémů odpovídající rizikům, která představují. Při posuzování přiměřenosti těchto opatření se náležitě zohlední míra vystavení subjektu rizikům, velikost subjektu a pravděpodobnost výskytu incidentů a jejich závažnost, včetně jejich společenského a hospodářského dopadu.

2. Opatření uvedená v odstavci 1 jsou založena na přístupu zohledňujícím všechna rizika, jehož cílem je chránit síťové a informační systémy a fyzické prostředí těchto systémů před incidenty, a zahrnují alespoň tyto prvky:

   (a) zásady analýzy rizik a bezpečnosti informačních systémů;

   (b) řešení incidentů;

(c) kontinuitu podnikání, jako je správa zálohování a zotavení po havárii, a krizové řízení;

(d) bezpečnost dodavatelského řetězce, včetně bezpečnostních aspektů týkajících se vztahů mezi jednotlivými subjekty a jejich přímými dodavateli nebo poskytovateli služeb;

(e) bezpečnost při pořizování, vývoji a údržbě sítí a informačních systémů, včetně řešení a odhalování zranitelností;

(f) zásady a postupy pro hodnocení účinnosti opatření pro řízení rizik v oblasti kybernetické bezpečnosti;

(g) základní postupy kybernetické hygieny a školení o kybernetické bezpečnosti;

(h) zásady a postupy týkající se používání kryptografie a případně šifrování;

(i) zabezpečení lidských zdrojů, zásady řízení přístupu a správu majetku;

(j) používání vícefaktorového ověřování nebo řešení průběžného ověřování, zabezpečené hlasové, video a textové komunikace a případně zabezpečených systémů nouzové komunikace v rámci subjektu.

3. Členské státy zajistí, aby subjekty při zvažování, která opatření uvedená v odst. 2 písm. d) tohoto článku jsou vhodná, zohlednily zranitelnost specifickou pro každého přímého dodavatele a poskytovatele služeb a celkovou kvalitu produktů a postupy kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje. Členské státy rovněž zajistí, aby při zvažování, která opatření uvedená v tomto písmenu jsou vhodná, subjekty zohlednily výsledky koordinovaných posouzení rizik kritických dodavatelských řetězců provedených v souladu s čl. 22 odst. 1.

4. Členské státy zajistí, aby subjekt, který zjistí, že nesplňuje opatření stanovená v odstavci 2, přijal bez zbytečného odkladu všechna nezbytná, vhodná a přiměřená nápravná opatření.

5. Podle ... [21 měsíců ode dne vstupu této směrnice v platnost] přijme Komise prováděcí akty, kterými stanoví technické a metodické požadavky na opatření uvedená v odstavci 2, pokud jde o poskytovatele služeb DNS, registry názvů domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele spravovaných služeb, poskytovatele spravovaných bezpečnostních služeb, poskytovatele on-line tržišť, on-line vyhledávačů a platforem služeb sociálních sítí a poskytovatele služeb vytvářejících důvěru.

Komise může přijmout prováděcí akty, kterými stanoví technické a metodické požadavky, jakož i odvětvové požadavky na opatření uvedená v odstavci 2, pokud jde o jiné zásadní a důležité subjekty než subjekty uvedené v prvním pododstavci tohoto odstavce.

Při přípravě prováděcích aktů uvedených v prvním a druhém pododstavci tohoto odstavce se Komise v co největší míře řídí evropskými a mezinárodními normami a příslušnými technickými specifikacemi. Komise si vyměňuje rady a spolupracuje se skupinou pro spolupráci a agenturou ENISA na návrzích prováděcích aktů v souladu s čl. 14 odst. 4 písm. e).

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

Článek 22

Koordinované posuzování bezpečnostních rizik kritických dodavatelských řetězců na úrovni Unie.

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

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

Článek 23

Ohlašovací povinnosti

1. Každý členský stát zajistí, aby základní a důležité subjekty bez zbytečného odkladu oznámily svému CSIRT nebo případně 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). 3. Dotčené subjekty případně bez zbytečného odkladu oznámí příjemcům svých služeb významné incidenty, které mohou mít nepříznivý vliv na poskytování těchto služeb. Každý členský stát zajistí, aby tyto subjekty hlásily mimo jiné veškeré informace, které CSIRT nebo případně příslušnému orgánu umožní určit případný přeshraniční dopad incidentu. Samotný akt oznámení nezakládá zvýšenou odpovědnost oznamujícího subjektu.

Pokud dotčené subjekty oznámí příslušnému orgánu závažnou událost podle prvního pododstavce, členský stát zajistí, aby tento příslušný orgán oznámení po obdržení předal CSIRT.

V případě přeshraniční nebo meziodvětvové závažné události členské státy zajistí, aby jejich jednotná kontaktní místa včas obdržela příslušné informace oznámené v souladu s odstavcem 4.

2. Členské státy případně zajistí, aby zásadní a důležité subjekty bez zbytečného odkladu sdělily příjemcům svých služeb, kteří jsou potenciálně zasaženi významnou kybernetickou hrozbou, veškerá opatření nebo nápravná opatření, která mohou tito příjemci v reakci na tuto hrozbu přijmout. V případě potřeby tyto subjekty tyto příjemce informují také o samotné významné kybernetické hrozbě.

3. Událost se považuje za významnou, pokud:

(a) způsobila nebo může způsobit vážné narušení provozu služeb nebo finanční ztrátu dotyčnému subjektu;

(b) ovlivnilo nebo může ovlivnit jiné fyzické nebo právnické osoby tím, že způsobí značnou majetkovou nebo nemajetkovou újmu.

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

(a) bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o závažném incidentu dozví, včasné varování, v němž případně uvede, zda je podezření, že závažný incident byl způsoben protiprávním nebo zlovolným jednáním, nebo zda by mohl mít přeshraniční dopad;

(b) bez zbytečného odkladu a v každém případě do 72 hodin od okamžiku, kdy se o závažném incidentu dozvěděl, oznámení o incidentu, v němž případně aktualizuje informace uvedené v písmenu a) a uvede počáteční hodnocení závažného incidentu, včetně jeho závažnosti a dopadu, jakož i ukazatele ohrožení, jsou-li k dispozici;

(c) na žádost CSIRT nebo případně příslušného orgánu průběžnou zprávu o aktualizaci příslušného stavu;

(d) závěrečnou zprávu nejpozději do jednoho měsíce od podání oznámení o události podle písmene b), která obsahuje:

(i) podrobný popis incidentu, včetně jeho závažnosti a dopadu;

(ii) typ hrozby nebo hlavní příčinu, která pravděpodobně incident vyvolala;

(iii) uplatňovaná a průběžná zmírňující opatření;

(iv) případně přeshraniční dopad incidentu;

(e) v případě probíhajícího incidentu v době předložení závěrečné zprávy uvedené v písmenu d) členské státy zajistí, aby dotčené subjekty v této době předložily zprávu o pokroku a závěrečnou zprávu do jednoho měsíce od vyřešení incidentu.

Odchylně od prvního pododstavce písm. b) poskytovatel služeb vytvářejících důvěru oznámí významné incidenty, které mají dopad na poskytování jeho služeb vytvářejících důvěru, CSIRT nebo případně příslušnému orgánu bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy se o významném incidentu dozvěděl.

5. CSIRT nebo příslušný orgán poskytne oznamujícímu subjektu bez zbytečného odkladu a pokud možno do 24 hodin od obdržení včasného varování uvedeného v odst. 4 písm. a) odpověď, včetně prvotní zpětné vazby k závažnému incidentu, a na žádost subjektu pokyny nebo operativní poradenství ohledně provádění možných opatření ke zmírnění následků. Pokud CSIRT není prvotním příjemcem oznámení uvedeného v odstavci 1, poskytne pokyny příslušný orgán ve spolupráci s CSIRT. Pokud o to dotčený subjekt požádá, poskytne CSIRT další technickou podporu. Pokud existuje podezření, že významný incident má trestněprávní povahu, poskytne CSIRT nebo příslušný orgán rovněž pokyny k ohlášení významného incidentu orgánům činným v trestním řízení.

6. V případě potřeby, a zejména pokud se závažný incident týká dvou nebo více členských států, informuje CSIRT, příslušný orgán nebo jednotné kontaktní místo o závažném incidentu bez zbytečného odkladu ostatní dotčené členské státy a agenturu ENISA. Tyto informace zahrnují druh informací obdržených v souladu s odstavcem 4. CSIRT, příslušný orgán nebo jednotné kontaktní místo přitom v souladu s právem Unie nebo vnitrostátním právem zachovávají bezpečnostní a obchodní zájmy subjektu, jakož i důvěrnost poskytnutých informací.

7. Pokud je informovanost veřejnosti nezbytná k prevenci závažného incidentu nebo k řešení probíhajícího závažného incidentu nebo pokud je zveřejnění závažného incidentu jinak ve veřejném zájmu, může CSIRT členského státu nebo případně jeho příslušný orgán a případně CSIRT nebo příslušné orgány ostatních dotčených členských států po konzultaci s dotčeným subjektem informovat veřejnost o závažném incidentu nebo požadovat, aby tak učinil subjekt.

8. Na žádost CSIRT nebo příslušného orgánu předá jednotné kontaktní místo oznámení přijatá podle odstavce 1 jednotným kontaktním místům ostatních dotčených členských států.

9. 2. Jednotné kontaktní místo předkládá agentuře ENISA každé tři měsíce souhrnnou zprávu, včetně anonymizovaných a agregovaných údajů o významných incidentech, událostech, kybernetických hrozbách a skoronehodách oznámených v souladu s odstavcem 1 tohoto článku a s článkem 30. S cílem přispět k poskytování srovnatelných informací může agentura ENISA přijmout technické pokyny týkající se parametrů informací, které mají být do souhrnné zprávy zahrnuty. 3. Agentura ENISA informuje skupinu pro spolupráci a síť CSIRT o svých zjištěních týkajících se přijatých oznámení každých šest měsíců.

10. CSIRT nebo případně příslušné orgány poskytnou příslušným orgánům podle směrnice (EU)..../.....[+] informace o významných incidentech, mimořádných událostech, kybernetických hrozbách a skoronehodách oznámených v souladu s odstavcem 1 tohoto článku a s článkem 30 subjekty, které byly identifikovány jako kritické subjekty podle směrnice (EU) .../....[+].

11. Komise může přijmout prováděcí akty, kterými dále upřesní druh informací, formát a postup oznámení předkládaného podle odstavce 1 tohoto článku a článku 30 a sdělení předkládaného podle odstavce 2 tohoto článku.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22

(2020/0365(COD)).

Podle ... [21 měsíců ode dne vstupu této směrnice v platnost] přijme Komise s ohledem na poskytovatele služeb DNS, registry názvů TLD, 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, on-line vyhledávačů a platforem služeb sociálních sítí prováděcí akty, kterými dále upřesní případy, kdy se incident považuje za významný, jak je uvedeno v odstavci 3. Komise může přijmout takové prováděcí akty s ohledem na další zásadní a důležité subjekty.

Komise si vyměňuje rady a spolupracuje se skupinou pro spolupráci na návrzích prováděcích aktů uvedených v prvním a druhém pododstavci tohoto odstavce v souladu s čl. 14 odst. 4 písm. e).

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

Článek 24

Využívání evropských systémů certifikace kybernetické bezpečnosti

1. Za účelem prokázání souladu s konkrétními požadavky článku 21 mohou členské státy požadovat, aby základní a významné subjekty používaly konkrétní produkty IKT, služby IKT a procesy IKT vyvinuté základním nebo významným subjektem nebo pořízené od třetích stran, které jsou certifikovány v rámci evropských systémů certifikace kybernetické bezpečnosti přijatých podle článku 49 nařízení (EU) 2019/881. Členské státy dále podporují, aby základní a významné subjekty využívaly kvalifikované služby vytvářející důvěru.

2. Komise je zmocněna přijímat akty v přenesené pravomoci v souladu s článkem 38, kterými doplní tuto směrnici tím, že stanoví, které kategorie základních a významných subjektů musí používat určité certifikované produkty IKT, služby IKT a procesy IKT nebo získat certifikát v rámci evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 49 nařízení (EU) 2019/881. Tyto akty v přenesené pravomoci se přijímají v případech, kdy byla zjištěna nedostatečná úroveň kybernetické bezpečnosti, a zahrnují prováděcí období.

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

3. 3. Pokud není k dispozici žádný vhodný evropský systém certifikace kybernetické bezpečnosti pro účely odstavce 2 tohoto článku, může Komise po konzultaci se skupinou pro spolupráci a Evropskou skupinou pro certifikaci kybernetické bezpečnosti požádat agenturu ENISA, aby připravila kandidátský systém podle čl. 48 odst. 2 nařízení (EU) 2019/881.

Článek 25

Standardizace

1. Za účelem podpory jednotného provádění čl. 21 odst. 1 a 2 členské státy podporují používání evropských a mezinárodních norem a technických specifikací týkajících se bezpečnosti sítí a informačních systémů, aniž by ukládaly nebo diskriminovaly používání určitého typu technologie.

2. Agentura ENISA ve spolupráci s členskými státy a případně po konzultaci s příslušnými zúčastněnými stranami vypracuje rady a pokyny týkající se technických oblastí, které je třeba zvážit v souvislosti s odstavcem 1, jakož i již existujících norem, včetně vnitrostátních norem, které by umožnily tyto oblasti zahrnout.

Kapitola V

Příslušnost a registrace

Článek 26

Příslušnost a teritorialita

1. Subjekty, které spadají do oblasti působnosti této směrnice, se považují za subjekty spadající do pravomoci členského státu, v němž jsou usazeny, s výjimkou případů, kdy:

   (a) poskytovatelé veřejných sítí elektronických komunikací nebo poskytovatelé veřejně dostupných služeb elektronických komunikací, kteří spadají do pravomoci členského státu, v němž poskytují své služby;

   (b) poskytovatelé služeb DNS, registry názvů TLD, subjekty poskytující služby registrace názvů domén, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center, poskytovatelé sítí pro doručování obsahu, poskytovatelé spravovaných služeb, poskytovatelé spravovaných bezpečnostních služeb, jakož i poskytovatelé on-line tržišť, on-line vyhledávačů nebo platforem služeb sociálních sítí, u nichž se má za to, že spadají do pravomoci členského státu, v němž mají hlavní provozovnu v Unii podle odstavce 2;

(c) subjekty veřejné správy, které se považují za spadající do pravomoci členského státu, který je zřídil.

2. Pro účely této směrnice se má za to, že subjekt uvedený v odst. 1 písm. b) má hlavní provozovnu v Unii v členském státě, v němž jsou převážně přijímána rozhodnutí týkající se opatření k řízení rizik v oblasti kybernetické bezpečnosti. Nelze-li takový členský stát určit nebo nejsou-li taková rozhodnutí v Unii přijímána, má se za to, že hlavní provozovna se nachází v členském státě, v němž jsou prováděny operace v oblasti kybernetické bezpečnosti. Pokud takový členský stát nelze určit, má se za to, že hlavní provozovna se nachází v členském státě, v němž má dotčený subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii.

3. Pokud subjekt uvedený v odst. 1 písm. b) není usazen v Unii, ale nabízí služby v Unii, určí v Unii svého zástupce. Zástupce musí být usazen v jednom z členských států, kde jsou služby nabízeny. Má se za to, že takový subjekt spadá pod jurisdikci členského státu, v němž je zástupce usazen. Není-li v Unii určen zástupce podle tohoto odstavce, může kterýkoli členský stát, v němž subjekt poskytuje služby, podat proti subjektu žalobu pro porušení této směrnice.

4. Určením zástupce subjektem uvedeným v odst. 1 písm. b) nejsou dotčeny právní kroky, které by mohly být zahájeny proti samotnému subjektu.

5. Členské státy, které obdržely žádost o vzájemnou pomoc ve vztahu k subjektu uvedenému v odst. 1 písm. b), mohou v mezích této žádosti přijmout vhodná opatření v oblasti dohledu a prosazování práva ve vztahu k dotyčnému subjektu, který poskytuje služby nebo který má síť a informační systém na jejich území.

Článek 27 Registr subjektů

1. Agentura ENISA vytvoří a vede registr poskytovatelů služeb DNS, registrů názvů domén nejvyšší úrovně, subjektů poskytujících služby registrace názvů domén, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center, poskytovatelů sítí pro doručování obsahu, poskytovatelů spravovaných služeb, poskytovatelů spravovaných bezpečnostních služeb, jakož i poskytovatelů on-line tržišť, on-line vyhledávačů a platforem služeb sociálních sítí, a to na základě informací obdržených od jednotných kontaktních míst v souladu s odstavcem 4. Agentura ENISA na požádání umožní příslušným orgánům přístup do tohoto registru, přičemž v příslušných případech zajistí ochranu důvěrnosti informací.

2. 2. Členské státy vyžadují, aby subjekty uvedené v odstavci 1 předložily příslušným orgánům do ... [24 měsíců ode dne vstupu této směrnice v platnost]:

(a) název subjektu;

(b) případně příslušné odvětví, pododvětví a typ subjektu uvedený v příloze I nebo II;

(c) adresu hlavní provozovny subjektu a jeho dalších právních provozoven v Unii, nebo pokud není usazen v Unii, adresu jeho zástupce 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 služby, a

(f) rozsahy IP subjektu.

3. Členské státy zajistí, aby subjekty uvedené v odstavci 1 oznámily příslušnému orgánu veškeré změny informací, které předložily podle odstavce 2, a to neprodleně a v každém případě do tří měsíců ode dne změny.

4. Po obdržení informací uvedených v odstavcích 2 a 3, s výjimkou informací uvedených v odst. 2 písm. f), je jednotné kontaktní místo dotčeného členského státu bez zbytečného odkladu předá agentuře ENISA.

5. Informace uvedené v odstavcích 2 a 3 tohoto článku se případně předkládají prostřednictvím vnitrostátního mechanismu uvedeného v čl. 3 odst. 4 čtvrtém pododstavci.

Článek 28

Databáze údajů o registraci doménových jmen

1. Za účelem přispění k bezpečnosti, stabilitě a odolnosti DNS členské státy vyžadují, aby registry názvů TLD a subjekty poskytující služby registrace názvů domén shromažďovaly a uchovávaly přesné a úplné údaje o registraci názvů domén ve vyhrazené databázi s náležitou péčí v souladu s právem Unie v oblasti ochrany údajů, pokud jde o údaje, které jsou osobními údaji.

2. Pro účely odstavce 1 členské státy vyžadují, aby databáze údajů o registraci jmen domén obsahovala informace nezbytné k identifikaci a kontaktování držitelů jmen domén a kontaktních míst spravujících jména domén v rámci TLD. Tyto informace zahrnují:

   (a) název domény;

(b) datum registrace;

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

(d) kontaktní e-mailovou adresu a telefonní číslo kontaktní osoby, která spravuje název domény, pokud se liší od adresy a telefonu registrátora.

3. Členské státy vyžadují, aby registry názvů TLD a subjekty poskytující služby registrace názvů domén zavedly zásady a postupy, včetně postupů ověřování, které zajistí, aby databáze uvedené v odstavci 1 obsahovaly přesné a úplné informace. Členské státy vyžadují, aby tyto zásady a postupy byly veřejně přístupné.

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

5. Členské státy vyžadují, aby registry názvů TLD a subjekty poskytující služby registrace názvů domén poskytovaly přístup ke konkrétním údajům o registraci názvů domén na základě zákonných a řádně odůvodněných žádostí oprávněných žadatelů o přístup v souladu s právem Unie v oblasti ochrany údajů. Členské státy vyžadují, aby registry názvů domén nejvyšší úrovně a subjekty poskytující služby registrace názvů domén odpovídaly bez zbytečného odkladu a v každém případě do 72 hodin od obdržení žádosti o přístup. Členské státy vyžadují, aby byly politiky a postupy týkající se zpřístupňování těchto údajů zveřejněny.

6. Splnění povinností stanovených v odstavcích 1 až 5 nesmí vést k duplicitě shromažďování údajů o registraci doménových jmen. Za tímto účelem členské státy vyžadují, aby registry názvů TLD a subjekty poskytující služby registrace názvů domén vzájemně spolupracovaly.

Kapitola VI Sdílení informací

Článek 29

Ujednání o sdílení informací v oblasti kybernetické bezpečnosti

1. 1. Členské státy zajistí, aby si subjekty spadající do oblasti působnosti této směrnice a případně další subjekty, které nespadají do oblasti působnosti této směrnice, mohly mezi sebou dobrovolně vyměňovat relevantní informace o kybernetické bezpečnosti, včetně informací týkajících se kybernetických hrozeb, skoronehod, zranitelností, technik a postupů, indikátorů kompromitace, taktik protivníka, informací specifických pro aktéry hrozeb, výstrah v oblasti kybernetické bezpečnosti a doporučení týkajících se konfigurace nástrojů kybernetické bezpečnosti pro odhalování kybernetických útoků, pokud k takovému sdílení informací dochází:

   (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 povědomí o kybernetických hrozbách, omezováním nebo ztěžováním šíření těchto hrozeb, podporou řady obranných schopností, odstraňováním a zveřejňováním zranitelností, odhalováním hrozeb, technikami jejich omezování a prevence, strategiemi zmírňování nebo fázemi reakce a obnovy nebo podporou společného výzkumu kybernetických hrozeb mezi veřejnými a soukromými subjekty.

2. Členské státy zajistí, aby výměna informací probíhala v rámci společenství základních a významných subjektů a případně jejich dodavatelů nebo poskytovatelů služeb. Tato výměna se provádí prostřednictvím dohod o sdílení informací v oblasti kybernetické bezpečnosti s ohledem na potenciálně citlivou povahu sdílených informací.

3. Členské státy usnadní vytvoření ujednání o sdílení informací v oblasti kybernetické bezpečnosti uvedených v odstavci 2 tohoto článku. Tato ujednání mohou specifikovat provozní prvky, včetně používání specializovaných platforem IKT a automatizačních nástrojů, obsahu a podmínek ujednání o sdílení informací. Při stanovení podrobností zapojení orgánů veřejné moci do těchto ujednání mohou členské státy stanovit podmínky pro informace zpřístupňované příslušnými orgány nebo CSIRT. Členské státy nabídnou pomoc při uplatňování těchto ujednání v souladu se svými politikami uvedenými v čl. 7 odst. 2 písm. h).

4. 3. Členské státy zajistí, aby zásadní a důležité subjekty oznámily příslušným orgánům svou účast v ujednáních o sdílení informací v oblasti kybernetické bezpečnosti uvedených v odstavci 2 při uzavření těchto ujednání nebo případně při odstoupení od těchto ujednání, jakmile toto odstoupení nabude účinnosti.

5. 3. Agentura ENISA poskytuje pomoc při vytváření ujednání o sdílení informací v oblasti kybernetické bezpečnosti uvedených v odstavci 2 prostřednictvím výměny osvědčených postupů a poskytováním pokynů.

Článek 30

Dobrovolné oznamování relevantních informací

1. Členské státy zajistí, aby kromě oznamovací povinnosti stanovené v článku 23 mohla být oznámení podávána CSIRT nebo případně příslušným orgánům dobrovolně:

(a) zásadní a důležité subjekty, pokud jde o incidenty, kybernetické hrozby a skoronehody;

(b) subjekty jiné než uvedené v písmenu a), bez ohledu na to, zda spadají do oblasti působnosti této směrnice, pokud jde o závažné incidenty, kybernetické hrozby a skoronehody.

2. Členské státy zpracovávají oznámení uvedená v odstavci 1 tohoto článku postupem podle článku 23. Členské státy mohou upřednostnit zpracování povinných oznámení před dobrovolnými oznámeními.

V případě potřeby poskytnou týmy CSIRT a případně příslušné orgány jednotným kontaktním místům informace o oznámeních přijatých podle tohoto článku, přičemž zajistí důvěrnost a odpovídající ochranu informací poskytnutých oznamujícím subjektem. Aniž je dotčeno předcházení trestným činům, jejich vyšetřování, odhalování a stíhání, dobrovolné oznamování nesmí mít za následek uložení jakýchkoli dalších povinností oznamujícímu subjektu, které by se na něj nevztahovaly, pokud by oznámení nepodal.

Kapitola VII Dozor a prosazování

Článek 31

Obecné aspekty týkající se dohledu a prosazování

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

2. Členské státy mohou svým příslušným orgánům povolit, aby stanovily priority úkolů v oblasti dohledu. Toto stanovení priorit musí být založeno na přístupu založeném na riziku. Za tímto účelem mohou příslušné orgány při výkonu svých úkolů v oblasti dohledu stanovených v článcích 32 a 33 stanovit metodiky dohledu, které umožní stanovit priority těchto úkolů na základě přístupu založeného na riziku.

3. Příslušné orgány při řešení incidentů vedoucích k porušení zabezpečení osobních údajů 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 při dohledu nad dodržováním této směrnice subjekty veřejné správy a při ukládání donucovacích opatření v případě porušení této směrnice měly příslušné orgány odpovídající pravomoci k provádění těchto úkolů s provozní nezávislostí na dohlížených subjektech veřejné správy. Členské státy mohou rozhodnout o uložení vhodných, přiměřených a účinných opatření v oblasti dohledu a prosazování ve vztahu k těmto subjektům v souladu s vnitrostátními právními a institucionálními rámci.

Článek 32

Dozor a donucovací opatření ve vztahu k základním subjektům

1. Členské státy zajistí, aby opatření v oblasti dohledu nebo vymáhání uložená základním subjektům v souvislosti s povinnostmi stanovenými v této směrnici byla účinná, přiměřená a odrazující s přihlédnutím k okolnostem každého jednotlivého případu.

2. Členské státy zajistí, aby příslušné orgány měly při výkonu svých úkolů v oblasti dohledu ve vztahu k základním subjektům pravomoc podrobit tyto subjekty alespoň:

   (a) kontroly na místě a dohled mimo místo, včetně namátkových kontrol prováděných vyškolenými odborníky;

   (b) pravidelné a cílené bezpečnostní audity prováděné nezávislým subjektem nebo příslušným orgánem;

   (c) ad hoc audity, a to i v případech, kdy je to odůvodněno závažnou událostí nebo porušením této směrnice ze strany základního subjektu;

(d) bezpečnostní prověrky založené na objektivních, nediskriminačních, spravedlivých a transparentních kritériích hodnocení rizik, v případě potřeby ve spolupráci s dotčeným subjektem;

(e) žádosti o informace nezbytné k posouzení opatření k řízení rizik v oblasti kybernetické bezpečnosti přijatých dotčeným subjektem, včetně zdokumentovaných politik kybernetické bezpečnosti, jakož i splnění povinnosti předložit informace příslušným orgánům podle článku 27;

(f) žádosti o přístup k údajům, dokumentům a informacím, které jsou nezbytné k plnění jejich úkolů v oblasti dohledu;

(g) žádosti o důkazy o provádění politik kybernetické bezpečnosti, jako jsou výsledky bezpečnostních auditů provedených kvalifikovaným auditorem a příslušné podklady.

Cílené bezpečnostní audity uvedené v prvním pododstavci písm. b) vycházejí z posouzení rizik provedeného příslušným orgánem nebo auditovaným subjektem nebo z jiných dostupných informací 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) nebo g) příslušné orgány uvedou účel žádosti a specifikují požadované informace.

4. Členské státy zajistí, aby jejich příslušné orgány měly při výkonu svých donucovacích pravomocí ve vztahu k základním subjektům alespoň pravomoc:

(a) vydávat varování před porušením této směrnice dotčenými subjekty;

(b) přijmout závazné pokyny, včetně opatření nezbytných k prevenci nebo nápravě události, jakož i lhůty pro provedení těchto opatření a pro podávání zpráv o jejich provádění, nebo příkaz, kterým se dotčeným subjektům uloží povinnost odstranit zjištěné nedostatky nebo porušení této směrnice;

(c) nařídit dotčeným subjektům, aby ukončily jednání, které je v rozporu s touto směrnicí, a aby se zdržely jeho opakování;

(d) nařídit dotčeným subjektům, aby zajistily, že jejich opatření pro řízení rizik v oblasti kybernetické bezpečnosti jsou v souladu s článkem 21, nebo aby splnily oznamovací povinnosti stanovené v článku 23, a to stanoveným způsobem a ve stanovené lhůtě;

(e) nařídit dotčeným subjektům, aby informovaly fyzické nebo právnické osoby, jimž poskytují služby nebo vykonávají činnosti, které jsou potenciálně ovlivněny významnou kybernetickou hrozbou, o povaze této hrozby, jakož i o případných ochranných nebo nápravných opatřeních, která mohou tyto fyzické nebo právnické osoby v reakci na tuto hrozbu přijmout;

(f) nařídit dotčeným subjektům, aby v přiměřené lhůtě provedly doporučení vyplývající z bezpečnostního auditu;

(g) jmenovat kontrolora s přesně vymezenými úkoly, který bude po stanovenou dobu dohlížet na dodržování článků 21 a 23 ze strany dotčených subjektů;

(h) nařídit dotčeným subjektům, aby určitým způsobem zveřejnily aspekty porušení této směrnice;

(i) uložit nebo požádat příslušné orgány, soudy nebo tribunály o uložení správní pokuty podle článku 34 vedle opatření uvedených v písmenech a) až h) tohoto odstavce v souladu s vnitrostátním právem.

5. Pokud jsou donucovací opatření přijatá podle odst. 4 písm. a) až d) a f) neúčinná, členské státy zajistí, aby jejich příslušné orgány měly pravomoc stanovit lhůtu, v níž je základní subjekt vyzván, aby přijal nezbytná opatření k nápravě nedostatků nebo splnil požadavky těchto orgánů. Pokud požadované opatření není ve stanovené lhůtě přijato, členské státy zajistí, aby příslušné orgány měly pravomoc:

(a) dočasně pozastavit certifikační nebo autorizační orgán nebo soud či tribunál v souladu s vnitrostátními právními předpisy, nebo požádat o dočasné pozastavení certifikace nebo autorizace týkající se části nebo všech příslušných služeb poskytovaných nebo činností vykonávaných základním subjektem;

(b) požadovat, aby příslušné orgány, soudy nebo tribunály v souladu s vnitrostátními právními předpisy dočasně zakázaly jakékoli fyzické osobě, která je odpovědná za výkon řídících funkcí na úrovni výkonného ředitele nebo právního zástupce v základním subjektu, vykonávat řídící funkce v tomto subjektu.

Dočasná pozastavení nebo zákazy uložené podle tohoto odstavce se uplatňují pouze do doby, než dotyčný subjekt přijme nezbytná opatření k nápravě nedostatků nebo splní požadavky příslušného orgánu, pro který byla tato donucovací opatření uplatněna. Uložení takových dočasných pozastavení nebo zákazů podléhá vhodným procesním zárukám v souladu s obecnými zásadami práva Unie a Listiny, včetně práva na účinnou právní ochranu a spravedlivý proces, presumpce neviny a práva na obhajobu.

Donucovací opatření stanovená v tomto odstavci se nevztahují na subjekty veřejné správy, na které se vztahuje tato směrnice.

6. Členské státy zajistí, aby každá fyzická osoba odpovědná za základní subjekt nebo jednající jako jeho právní zástupce na základě oprávnění jej zastupovat, oprávnění přijímat rozhodnutí jeho jménem nebo oprávnění vykonávat nad ním kontrolu měla pravomoc zajistit jeho soulad s touto směrnicí. Členské státy zajistí, aby bylo možné tyto fyzické osoby činit odpovědnými za porušení jejich povinností zajistit soulad s touto směrnicí.

Pokud jde o subjekty veřejné správy, není tímto odstavcem dotčeno vnitrostátní právo, pokud jde o odpovědnost státních zaměstnanců a volených nebo jmenovaných úředníků.

7. Při přijímání jakýchkoli donucovacích opatření uvedených v odstavci 4 nebo 5 musí příslušné orgány dodržovat právo na obhajobu a přihlížet k okolnostem každého jednotlivého případu a minimálně řádně zohlednit:

(a) závažnost porušení a důležitost porušených ustanovení, přičemž závažným porušením je mimo jiné v každém případě:

(i) opakovaná porušení;

(ii) neoznámení nebo nenapravení závažných incidentů;

(iii) neodstranění nedostatků na základě závazných pokynů příslušných orgánů;

(iv) bránění auditům nebo monitorovacím činnostem nařízeným příslušným orgánem po zjištění porušení předpisů;

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

(b) dobu trvání protiprávního jednání;

(c) veškerá relevantní předchozí porušení ze strany dotčeného subjektu;

(d) jakoukoli způsobenou hmotnou nebo nehmotnou škodu, včetně jakékoli finanční nebo hospodářské ztráty, dopadů na jiné služby a počtu dotčených uživatelů;

(e) úmysl nebo nedbalost pachatele porušení;

(f) veškerá opatření, která subjekt přijal k prevenci nebo zmírnění hmotné nebo nehmotné újmy;

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

(h) úroveň spolupráce odpovědných fyzických nebo právnických osob s příslušnými orgány.

8. Příslušné orgány podrobně odůvodní svá donucovací opatření. Před přijetím těchto opatření příslušné orgány oznámí dotčeným subjektům svá předběžná zjištění. Rovněž poskytnou těmto subjektům přiměřenou lhůtu k podání připomínek, s výjimkou řádně odůvodněných případů, kdy by jinak byla znemožněna okamžitá opatření k předcházení incidentům nebo reakce na ně.

9. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice informovaly relevantní příslušné orgány v témže členském státě podle směrnice (EU) .../.....[+] při výkonu svých dozorových a donucovacích pravomocí, jejichž cílem je zajistit soulad subjektu, který byl identifikován jako kritický subjekt podle směrnice (EU) ... /.. , s právními předpisy. [+] s touto směrnicí. V případě potřeby příslušné orgány podle směrnice (EU) .../... [+] mohou požádat příslušné orgány podle této směrnice, aby vykonávaly své pravomoci v oblasti dohledu a prosazování práva ve vztahu k subjektu, který je označen za kritický subjekt podle směrnice (EU) .../... [+].

10. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice spolupracovaly s příslušnými orgány dotčeného členského státu podle nařízení (EU) .../.... [++]. Členské státy zejména zajistí, aby jejich příslušné orgány podle této směrnice informovaly fórum pro dohled zřízené podle čl. 32 odst. 1 nařízení (EU) .../.... [++] při výkonu svých dozorových a donucovacích pravomocí zaměřených na zajištění souladu zásadního subjektu, který je určen jako kritický poskytovatel služeb..... IKT třetí strany podle článku 31 nařízení (EU) .../. ..... [++] s touto směrnicí.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

[++] Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 41/22

(2020/0266(COD)).

Článek 33

Opatření v oblasti dohledu a prosazování práva ve vztahu k významným subjektům

1. Pokud jsou poskytnuty důkazy, indicie nebo informace o tom, že důležitý subjekt údajně nedodržuje tuto směrnici, zejména její články 21 a 23, členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření v oblasti dohledu *ex post*. Členské státy zajistí, aby tato opatření byla účinná, přiměřená a odrazující s ohledem na okolnosti každého jednotlivého případu.

2. Členské státy zajistí, aby příslušné orgány měly při výkonu svých úkolů v oblasti dohledu ve vztahu k významným subjektům pravomoc podrobit tyto subjekty alespoň:

   (a) kontroly na místě a *následný* dohled mimo místo prováděný vyškolenými odborníky;

   (b) cílené bezpečnostní audity prováděné nezávislým subjektem nebo příslušným orgánem;

(c) bezpečnostní prověrky založené na objektivních, nediskriminačních, spravedlivých a transparentních kritériích hodnocení rizik, v případě potřeby ve spolupráci s dotčeným subjektem;

(d) žádosti o informace nezbytné k *následnému* posouzení kybernetické bezpečnosti. opatření k řízení rizik přijatá dotčeným subjektem, včetně zdokumentovaných politik kybernetické bezpečnosti, jakož i plnění povinnosti předkládat informace příslušným orgánům podle článku 27;

(e) žádosti o přístup k údajům, dokumentům a informacím, které jsou nezbytné pro plnění jejich úkolů v oblasti dohledu;

(f) žádosti o důkazy o provádění politik kybernetické bezpečnosti, jako jsou výsledky bezpečnostních auditů provedených kvalifikovaným auditorem a příslušné podklady.

Cílené bezpečnostní audity uvedené v prvním pododstavci písm. b) vycházejí z posouzení rizik provedeného příslušným orgánem nebo auditovaným subjektem nebo z jiných dostupných informací 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) příslušné orgány uvedou účel žádosti a specifikují požadované informace.

4. Členské státy zajistí, aby příslušné orgány měly při výkonu svých donucovacích pravomocí ve vztahu k významným subjektům alespoň pravomoc:

(a) vydávat varování před porušením této směrnice dotčenými subjekty;

(b) přijmout závazné pokyny nebo příkaz, kterým se dotčeným subjektům uloží povinnost odstranit zjištěné nedostatky nebo porušení této směrnice;

(c) nařídit dotčeným subjektům, aby ukončily jednání, které je v rozporu s touto směrnicí, a aby se zdržely jeho opakování;

(d) nařídit dotčeným subjektům, aby zajistily, že jejich opatření pro řízení rizik v oblasti kybernetické bezpečnosti jsou v souladu s článkem 21, nebo aby splnily oznamovací povinnosti stanovené v článku 23, a to stanoveným způsobem a ve stanovené lhůtě;

(e) nařídit dotčeným subjektům, aby informovaly fyzické nebo právnické osoby, jimž poskytují služby nebo vykonávají činnosti, které jsou potenciálně ovlivněny významnou kybernetickou hrozbou, o povaze této hrozby, jakož i o případných ochranných nebo nápravných opatřeních, která mohou tyto fyzické nebo právnické osoby v reakci na tuto hrozbu přijmout;

(f) nařídit dotčeným subjektům, aby v přiměřené lhůtě provedly doporučení vyplývající z bezpečnostního auditu;

(g) nařídit dotčeným subjektům, aby určitým způsobem zveřejnily aspekty porušení této směrnice;

(h) uložit nebo požádat příslušné orgány, soudy nebo tribunály o uložení správní pokuty podle článku 34 vedle opatření uvedených v písmenech a) až g) tohoto odstavce v souladu s vnitrostátním právem.

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

6. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice spolupracovaly s příslušnými orgány dotčeného členského státu podle nařízení (EU) .../.... [+]. Členské státy zejména zajistí, aby jejich příslušné orgány podle této směrnice informovaly fórum pro dohled zřízené podle čl. 32 odst. 1 nařízení (EU) .../.... [+] při výkonu svých dozorových a donucovacích pravomocí zaměřených na zajištění souladu důležitého subjektu, který je označen za poskytovatele kritických služeb IKT třetí strany podle článku 31 nařízení (EU) .../..... [+] s touto směrnicí.

[+] Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

Článek 34

Obecné podmínky pro ukládání správních pokut zásadním a významným subjektům

1. Členské státy zajistí, aby správní pokuty ukládané základním a významným subjektům podle tohoto článku za porušení této směrnice byly účinné, přiměřené a odrazující s přihlédnutím k okolnostem každého jednotlivého případu.

2. Správní pokuty se ukládají vedle 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 o její výši v každém jednotlivém případě se náležitě zohlední alespoň prvky stanovené v čl. 32 odst. 7.

4. Členské státy zajistí, aby v případě porušení článku 21 nebo 23 byly základním subjektům v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty v maximální výši nejméně 10 000 000 EUR nebo v maximální výši nejméně 2 % celkového celosvětového ročního obratu podniku, ke kterému základní subjekt patří, za předchozí účetní období, podle toho, která částka je vyšší.

5. Členské státy zajistí, aby v případě porušení článku 21 nebo 23 byly významným subjektům v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty v maximální výši nejméně 7 000 000 EUR nebo v maximální výši nejméně 1,4 % celkového celosvětového ročního obratu podniku, k němuž významný subjekt patří, podle toho, která částka je vyšší.

6. Členské státy mohou stanovit pravomoc ukládat penále s cílem přimět základní nebo významný subjekt, aby přestal porušovat tuto směrnici v souladu s předchozím rozhodnutím příslušného orgánu.

7. Aniž jsou dotčeny pravomoci příslušných orgánů podle článků 32 a 33, může každý členský stát stanovit pravidla, zda a v jakém rozsahu lze ukládat správní pokuty subjektům veřejné správy.

8. Pokud právní systém členského státu nestanoví správní pokuty, zajistí tento členský stát, aby byl tento článek uplatňován tak, že pokutu zahajuje příslušný orgán a ukládají ji příslušné vnitrostátní soudy, přičemž zajistí, aby tyto opravné prostředky byly účinné a měly rovnocenný účinek jako správní pokuty ukládané příslušnými orgány. V každém případě musí být uložené pokuty účinné, přiměřené a odrazující. Členský stát oznámí Komisi ustanovení právních předpisů, které přijme podle tohoto odstavce, do .....[21 měsíců ode dne vstupu této směrnice v platnost] a neprodleně všechny následné pozměňovací zákony nebo změny, které se jich týkají.

Článek 35

Porušení, která vedou k narušení bezpečnosti osobních údajů

1. Pokud se příslušné orgány v průběhu dohledu nebo vymáhání práva dozvědí, že porušení povinností stanovených v článcích 21 a 23 této směrnice ze strany zásadního nebo významného subjektu může mít za následek porušení zabezpečení osobních údajů ve smyslu čl. 4 bodu 12 nařízení (EU) 2016/679, které má být oznámeno podle článku 33 uvedeného nařízení, bez zbytečného odkladu informují orgány dozoru uvedené v článku 55 nebo 56 uvedeného nařízení.

2. Pokud dozorové úřady uvedené v článku 55 nebo 56 nařízení (EU) 2016/679 uloží správní pokutu podle čl. 58 odst. 2 písm. i) uvedeného nařízení, příslušné orgány neuloží správní pokutu podle článku 34 této směrnice za porušení uvedené v odstavci 1 tohoto článku, které vyplývá ze stejného jednání, které bylo předmětem správní pokuty podle čl. 58 odst. 2 písm. i) nařízení (EU) 2016/679. Příslušné orgány však mohou uložit donucovací opatření stanovená 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 je dozorový úřad příslušný podle nařízení (EU) 2016/679 usazen v jiném členském státě než příslušný orgán, informuje příslušný orgán dozorový úřad usazený v jeho členském státě o možném porušení ochrany údajů uvedeném v odstavci 1.

Článek 36

Sankce

Členské státy stanoví pravidla pro sankce za porušení vnitrostátních opatření přijatých podle této směrnice a přijmou veškerá opatření nezbytná k zajištění jejich provádění. Stanovené sankce musí být účinné, přiměřené a odrazující. Členské státy do 30 dnů od tohoto oznámení stanoví, že se sankce ukládají v souladu s čl. 3 odst. 2. [24 měsíců ode dne vstupu této směrnice v platnost] oznámí Komisi tato pravidla a tato opatření a neprodleně jí oznámí veškeré následné změny, které se jich týkají.

Článek 37

Vzájemná pomoc

1. Pokud subjekt poskytuje služby ve více než jednom členském státě nebo poskytuje služby v jednom či více členských státech a jeho síť a informační systémy se nacházejí v jednom či více jiných členských státech, příslušné orgány dotčených členských států v případě potřeby spolupracují a vzájemně si pomáhají. Tato spolupráce zahrnuje alespoň to, že:

   (a) příslušné orgány, které uplatňují opatření v oblasti dohledu nebo vymáhání práva v členském státě, informují prostřednictvím jednotného kontaktního místa příslušné orgány v ostatních dotčených členských státech a konzultují s nimi přijatá opatření v oblasti dohledu a vymáhání práva;

(b) příslušný orgán může požádat jiný příslušný orgán, aby přijal opatření v oblasti dohledu nebo vynucování;

(c) příslušný orgán po obdržení odůvodněné žádosti od jiného příslušného orgánu poskytne druhému příslušnému orgánu vzájemnou pomoc přiměřenou jeho vlastním zdrojům, aby mohla být opatření v oblasti dohledu nebo prosazování prováděna účinně, efektivně a konzistentně.

Vzájemná pomoc uvedená v prvním pododstavci písm. c) může zahrnovat žádosti o informace a opatření dohledu, včetně žádostí o provedení inspekcí na místě nebo dohledu mimo místo či cílených bezpečnostních auditů. Příslušný orgán, jemuž je žádost o pomoc adresována, tuto žádost neodmítne, pokud se neprokáže, že nemá pravomoc požadovanou pomoc poskytnout, že požadovaná pomoc není přiměřená úkolům příslušného orgánu v oblasti dohledu nebo že se žádost týká informací nebo zahrnuje činnosti, jejichž zveřejnění nebo provedení by bylo v rozporu se základními zájmy národní bezpečnosti, veřejné bezpečnosti nebo obrany členského státu. Před odmítnutím takové žádosti příslušný orgán konzultuje ostatní dotčené příslušné orgány a na žádost jednoho z dotčených členských států také Komisi a agenturu ENISA,

2. Příslušné orgány různých členských států mohou v případě potřeby a po vzájemné dohodě provádět společné dohledové akce.

Kapitola VIII Akty v přenesené pravomoci a prováděcí akty

Článek 38 Výkon přenesení pravomocí

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 od ... [datum vstupu této směrnice v platnost].

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 24 odst. 2 kdykoli zrušit. Rozhodnutím o odvolání se ukončuje přenesení pravomoci uvedené v tomto rozhodnutí. Rozhodnutí nabývá účinku dnem následujícím po jeho zveřejnění v *Úředním věstníku Evropské unie* nebo k pozdějšímu datu, které je v něm uvedeno. Rozhodnutí nemá vliv na platnost již platných aktů v přenesené pravomoci.

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

5. Jakmile Komise přijme akt v přenesené pravomoci, oznámí jej současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle čl. 24 odst. 2 vstoupí v platnost, pouze 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. Tato lhůta se z podnětu Evropského parlamentu nebo Rady prodlouží o dva měsíce.

Článek 39

Postup 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 stanovisko výboru získáno písemným postupem, je tento postup ukončen bez výsledku, pokud o tom ve lhůtě pro vydání stanoviska rozhodne předseda výboru nebo o to požádá některý z členů výboru.

Kapitola IX
Závěrečná ustanovení

Článek 40

Recenze

Podle ... [57 měsíců ode dne vstupu této směrnice v platnost] a poté každých 36 měsíců Komise přezkoumá fungování této směrnice a podá zprávu Evropskému parlamentu a Radě. Zpráva zejména posoudí význam velikosti dotčených subjektů a odvětví, pododvětví a typů subjektů uvedených v přílohách I a II pro fungování hospodářství a společnosti v souvislosti s kybernetickou bezpečností. Za tímto účelem a s cílem dále rozvíjet strategickou a operativní spolupráci Komise zohlední zprávy skupiny pro spolupráci a sítě CSIRT o zkušenostech získaných na strategické a operativní úrovni. Ke zprávě se v případě potřeby přiloží legislativní návrh.

Článek 41

Transpozice

1. Do ... 21 měsíců ode dne vstupu této směrnice v platnost členské státy přijmou a zveřejní opatření nezbytná pro dosažení souladu s touto směrnicí. Neprodleně o nich uvědomí Komisi.

   Tato opatření uplatňují od ... [jeden den po dni uvedeném v prvním pododstavci]. pododstavec].

2. Tato opatření přijatá členskými státy musí obsahovat odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsoby odkazu stanoví členské státy.

Článek 42

Změna nařízení (EU) č. 910/2014

V nařízení (EU) č. 910/2014 se článek 19 zrušuje s účinkem od ... [datum stanovené v čl. 41 odst. 1 druhém pododstavci].

Článek 43

Změna směrnice (EU) 2018/1972

Ve směrnici (EU) 2018/1972 se články 40 a 41 zrušují s účinkem od ... [datum stanovené v čl. 41 odst. 1 druhém pododstavci].

Článek 44

Zrušení

Směrnice (EU) 2016/1148 se zrušuje s účinkem od ... [datum stanovené v čl. 41 odst. 1 druhém pododstavci].

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

Článek 45

Vstup v platnost

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

Úřední věstník Evropské unie.

Článek 46 Adresáti

Tato směrnice je určena členským státům. V ...,

Za Evropský *parlamentza Radu*

PrezidentPrezident

PŘÍLOHA I

ODVĚTVÍ S VYSOKOU KRITIČNOSTÍ

Sektor	Podsektor	Typ subjektu
1. Energie	(a) Elektřina	-Elektrárenské podniky ve smyslu čl. 2 bodu 57 směrnice Evropského parlamentu a Rady (EU) 2019/9441 , které vykonávají funkci "dodávky" ve smyslu čl. 2 bodu 12 uvedené směrnice.
		-Provozovatelé distribučních soustav podle definice v čl. 2 bodu 29 směrnice (EU) 2019/944.
		-Provozovatelé přenosových soustav podle definice v čl. 2 bodu 35 směrnice (EU) 2019/944.
		-výrobci podle definice v čl. 2 bodě 38 směrnice (EU) 2019/944
		-Jmenovaní operátoři trhu s elektřinou, jak jsou definováni v čl. 2 bodě 8 nařízení Evropského parlamentu a Rady (EU) 2019/9432.

[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).

Sektor	Podsektor	Typ subjektu
		– Účastníci trhu definovaní v čl. 2 bodě 25 nařízení (EU) 2019/943, kteří poskytují služby agregace, odezvy na straně poptávky nebo skladování energie definované v čl. 2 bodě 18, (20) a (59) směrnice (EU) 2019/944 – Provozovatelé dobíjecího místa, kteří jsou odpovědní za správu a provoz dobíjecího místa, které poskytuje službu dobíjení koncovým uživatelům, a to i jménem a na účet poskytovatele služeb mobility.
	(b) Dálkové vytápění a chlazení	-Provozovatelé dálkového vytápění nebo dálkového chlazení podle definice v čl. 2 bodu 19 směrnice Evropského parlamentu a Rady (EU) 2018/20011.
	(c) Olej	-Provozovatelé ropovodů pro přepravu ropy
		-Provozovatelé zařízení na těžbu, rafinaci a zpracování ropy, skladování a přepravu.
		-Centrální akciové společnosti podle definice v čl. 2 písm. f) směrnice Rady 2009/119/ES2.

[1] 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).

[2] Směrnice Rady 2009/119/ES ze dne 14. září 2009, kterou se členským státům ukládá povinnost udržovat minimální zásoby ropy a/nebo ropných produktů (Úř. věst. L 265, 9.10.2009, s. 9).

Sektor	Podsektor	Typ subjektu
	(d) Plyn	-dodavatelské podniky ve smyslu čl. 2 bodu 8 směrnice Evropského parlamentu a Rady (EU) 2009/73/ES1.
		-Provozovatelé distribučních soustav podle definice v čl. 2 bodě 6 směrnice 2009/73/ES.
		-Provozovatelé přenosových soustav podle definice v čl. 2 bodě 4 směrnice 2009/73/ES.
		-provozovatelé skladovacích systémů podle definice v čl. 2 bodě 10 směrnice 2009/73/ES
		-provozovatelé plynárenských soustav podle definice v čl. 2 bodě 12 směrnice 2009/73/ES
		-plynárenské podniky podle definice v čl. 2 bodě 1 směrnice 2009/73/ES.
		-provozovatelé zařízení na rafinaci a úpravu zemního plynu
	(e) Vodík	-Provozovatelé výroby, skladování a přenosu vodíku

[1] 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).

Sektor		Podsektor		Typ subjektu
2.	Přeprava	(a)	Vzduch	-letečtí dopravci definovaní v čl. 3 bodě 4 nařízení (ES) č. 300/2008, kteří se používají pro obchodní účely.
				-řídící orgány letišť ve smyslu čl. 2 bodu 2 směrnice Evropského parlamentu a Rady 2009/12/ES1, letiště ve smyslu čl. 2 bodu 1 uvedené směrnice, včetně hlavních letišť uvedených v oddíle 2 přílohy II nařízení Evropského parlamentu a Rady (EU) č. 1315/20132, a subjekty provozující pomocná zařízení na letištích.
				-Provozovatelé řízení letového provozu poskytující služby řízení letového provozu (ATC) podle definice v čl. 2 bodě 1 nařízení Evropského parlamentu a Rady (ES) č. 549/20043.

1 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).

2 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).

3 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).

Sektor	Podsektor	Typ subjektu
	(b) Železnice	-správci infrastruktury ve smyslu čl. 3 bodu 2 směrnice Evropského parlamentu a Rady 2012/34/EU1.
		-Železniční podniky podle definice v čl. 3 bodě 1 směrnice 2012/34/EU, včetně provozovatelů servisních zařízení podle definice v čl. 3 bodě 12 uvedené směrnice.
	(c) Voda	-společnosti vnitrozemské , námořní a pobřežní osobní a nákladní vodní dopravy, jak jsou definovány pro námořní dopravu v příloze I nařízení Evropského parlamentu a Rady (ES) č. 725/20042 , s výjimkou jednotlivých plavidel provozovaných těmito společnostmi.
		-Řídící orgány přístavů, jak jsou definovány v čl. 3 bodě 1 směrnice Evropského parlamentu a Rady 2005/65/ES3 , včetně jejich přístavních zařízení, jak jsou definována v čl. 2 bodě 11 nařízení (ES) č. 725/2004, a subjekty provozující stavby a zařízení v přístavech.
		-Provozovatelé služeb lodní dopravy (VTS), jak jsou definováni v čl. 3 písm. o) směrnice Evropského parlamentu a Rady 2002/59/ES4.

[1] 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).

[2] 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).

[3] Směrnice Evropského parlamentu a Rady 2005/65/ES ze dne 26. října 2005 o zvýšení bezpečnosti přístavů (Úř. věst. L 310, 25.11.2005, s. 28).

[4] 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 zrušuje směrnice Rady 93/75/EHS (Úř. věst. L 208, 5.8.2002, s. 10).

Sektor	Podsektor	Typ subjektu
	(d) Silnice	-Silniční orgány definované v čl. 2 bodu 12 nařízení Komise v přenesené pravomoci (EU) 2015/9621 odpovědné za řízení dopravy, s výjimkou veřejných subjektů, pro které řízení dopravy nebo provozování inteligentních dopravních systémů není podstatnou součástí jejich obecné činnosti.
		-Provozovatelé inteligentních dopravních systémů podle definice v čl. 4 bodě 1 směrnice Evropského parlamentu a Rady 2010/40/EU2.
3. Bankovnictví		Úvěrové instituce ve smyslu čl. 4 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 575/20133.
4. Infrastruktury finančního trhu		-provozovatelé obchodních systémů ve smyslu čl. 4 bodu 24 směrnice Evropského parlamentu a Rady 2014/65/EU4.
		-Centrální protistrany (CCP), jak jsou definovány v čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 648/20125.

[1] 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 dopravních informačních služeb v reálném čase v celé EU (Úř. věst. L 157, 23.6.2015, s. 21).

[2] 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).

[3] 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).

[4] Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnice 2002/92/ES a směrnice 2011/61/EU (Úř. věst. L 173, 12.6.2014, s. 349).

[5] 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).

Sektor		Podsektor	Typ subjektu
5.	Zdraví		-Poskytovatelé zdravotní péče ve smyslu čl. 3 písm. g) směrnice Evropského parlamentu a Rady 2011/24/EU1.
			-referenční laboratoře EU uvedené v článku 15 nařízení Evropského parlamentu a Rady (EU) .../...2+
			– Subjekty provádějící výzkum a vývoj léčivých přípravků podle definice v čl. 1 bodě 2 směrnice Evropského parlamentu a Rady 2001/83/ES3. – Subjekty vyrábějící základní farmaceutické výrobky a farmaceutické přípravky uvedené v sekci C oddílu 21 klasifikace NACE Rev. 2 – Subjekty vyrábějící zdravotnické prostředky, které jsou považovány za kritické během mimořádné situace v oblasti veřejného zdraví (seznam kritických prostředků v oblasti veřejného zdraví) ve smyslu článku 22 nařízení Evropského parlamentu a Rady (EU) 2022/1234.

1 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).

2 Nařízení Evropského parlamentu a Rady (EU) .../... ze dne ... o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 1082/2013/EU (Úř. věst. L ...., ... ,s.).

+ Úř. věst.: vložte prosím do textu číslo nařízení obsaženého v dokumentu PE-CONS 40/22 (2020/0322(COD)) a do poznámky pod čarou vložte číslo, datum a odkaz na toto nařízení v Úředním věstníku.

3 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).

4 Nařízení Evropského parlamentu a Rady (EU) 2022/123 ze dne 25. ledna 2022 o posílení úlohy Evropské agentury pro léčivé přípravky v oblasti připravenosti na krize a jejich řešení (Úř. věst. L 20, 31.1.2022, s. 1).

Sektor		Podsektor	Typ subjektu
6.	Pitná voda		Dodavatelé a distributoři vody určené k lidské spotřebě podle definice v čl. 2 odst. 1 písm. a) směrnice Evropského parlamentu a Rady (EU) 2020/21841 , s výjimkou distributorů, pro které je distribuce vody určené k lidské spotřebě nepodstatnou součástí jejich obecné činnosti spočívající v distribuci jiných komodit a zboží.
7.	Odpadní voda		Podniky, které odvádějí, zneškodňují nebo čistí městské odpadní vody, odpadní vody z domácností nebo průmyslové odpadní vody, jak jsou definovány v čl. 2 bodech 1, 2 a 3 směrnice Rady 91/271/EHS2 , s výjimkou podniků, pro které odvádění, zneškodňování nebo čištění městských odpadních vod, odpadních vod z domácností nebo průmyslových odpadních vod není podstatnou součástí jejich obecné činnosti.

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

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

Sektor	Podsektor	Typ subjektu
8. Digitální infrastruktura		-Poskytovatelé internetových výměnných bodů
		-Poskytovatelé služeb DNS, s výjimkou provozovatelů kořenových jmenných serverů.
		-Registry názvů TLD
		-Poskytovatelé služeb cloud computingu
		-Poskytovatelé služeb datových center
		-Poskytovatelé sítí pro doručování obsahu
		-Důvěřujte poskytovatelům služeb
		-Poskytovatelé veřejných sítí elektronických komunikací
		-poskytovatelé veřejně dostupných služeb elektronických komunikací
9.Řízení služeb ICT (business-to-business)		– Poskytovatelé spravovaných služeb – Poskytovatelé spravovaných bezpečnostních služeb

Sektor	Podsektor	Typ subjektu
10. Veřejná správa		-subjekty veřejné správy ústředních vlád, jak jsou definovány členským státem v souladu s vnitrostátními právními předpisy.
		-subjekty veřejné správy na regionální úrovni, jak je definuje členský stát v souladu s vnitrostátními právními předpisy.
11. Prostor		Provozovatelé pozemní infrastruktury, kterou vlastní, spravují a provozují členské státy nebo soukromé subjekty a která podporuje poskytování kosmických služeb, s výjimkou poskytovatelů veřejných sítí elektronických komunikací.

PŘÍLOHA II

Ostatní kritická odvětví

Sektor		Podsektor	Typ 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 podle definice v čl. 3 bodě 9 směrnice Evropského parlamentu a Rady 2008/98/ES1 , s výjimkou podniků, pro které nakládání s odpady není hlavní hospodářskou činností.
3.	Výroba, produkce a distribuce chemických látek		Podniky provádějící výrobu látek a distribuci látek nebo směsí podle čl. 3 bodů 9 a 14 nařízení Evropského parlamentu a Rady (ES) č. 1907/20062 a podniky provádějící výrobu předmětů z látek nebo směsí podle čl. 3 bodu 3 uvedeného nařízení.

[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, 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).

Sektor		Podsektor		Typ subjektu
4.	Výroba, zpracování a distribuce potravin			Potravinářské podniky ve smyslu čl. 3 bodu 2 nařízení Evropského parlamentu a Rady (ES) č. 178/20021 , 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 podle definice v čl. 2 bodě 1 nařízení Evropského parlamentu a Rady (EU) 2017/7452 a subjekty vyrábějící diagnostické zdravotnické prostředky *in vitro* podle definice v čl. 2 bodě 2 nařízení Evropského parlamentu a Rady (EU) 2017/7463 s výjimkou subjektů vyrábějících zdravotnické prostředky uvedené v příloze I bodě 5 páté odrážce této směrnice.
		(b)	Výroba počítačů, elektronických a optických výrobků	Podniky, které vykonávají některou z ekonomických činností uvedených v oddílu C oddílu 26 klasifikace NACE Rev. 2.

[1] 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).

[2] Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, kterým se mění 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).

[3] 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).

Sektor	Podsektor	Typ subjektu
	(c)Výroba elektrických zařízení	Podniky, které vykonávají některou z ekonomických činností uvedených v oddílu C oddílu 27 klasifikace NACE Rev. 2.
	(d)Výroba strojů a zařízení j. n.	Podniky, které vykonávají některou z ekonomických činností uvedených v oddílu C oddílu 28 klasifikace NACE Rev. 2.
	(e) Výroba motorových vozidel, přívěsů a návěsů	Podniky, které vykonávají některou z ekonomických činností uvedených v oddílu C oddílu 29 klasifikace NACE Rev. 2.
	(f)Výroba ostatních dopravních prostředků	Podniky, které vykonávají některou z ekonomických činností uvedených v oddílu C oddílu 30 klasifikace NACE Rev. 2.
6. Poskytovatelé digitálních služeb		-Poskytovatelé online tržišť
		-Poskytovatelé online vyhledávačů
		-Poskytovatelé platforem pro služby sociálních sítí
7. Výzkum		Výzkumné organizace

PŘÍLOHA III

KORELAČNÍ
TABULKA

Směrnice (EU) 2016/1148	Tato směrnice
Článek 1 odst. 1	Článek 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

Směrnice (EU) 2016/1148	Tato směrnice
Čl. 9 odst. 4	Čl. 10 odst. 9
Čl. 9 odst. 5	Článek 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 b) (q) a (s) a odstavec (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 až 5	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
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)

Směrnice (EU) 2016/1148	Tato směrnice
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 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
Článek 22	Článek 39
Článek 23	Článek 40
Článek 24	-

Směrnice (EU) 2016/1148	Tato směrnice
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)
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) podbod 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