Rada
Evropské unie

Brusel 26. listopadu 2021
(OR. en)

14337/21

Interinstitucionální spis:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

POZNÁMKA

Odesílatel:	Generální sekretariát Rady
Příjemce:	Rada
Č. předchozího dokumentu:	9583/2/21, 11724/21
Č. dok. Komise:	14150/20
Předmět:	Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 *– obecný přístup*

I. ÚVOD

1. Dne 16. prosince 2020 přijala Komise návrh směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (dále jen „revidovaná směrnice o bezpečnosti sítí a informací“ nebo „směrnice NIS 2“)[1], jehož účelem bylo nahradit stávající směrnici o bezpečnosti sítí a informačních systémů („směrnice o bezpečnosti sítí a informací“)[2].

[1] Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148.

[2] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Návrh byl jedním z opatření plánovaných ve Strategii kybernetické bezpečnosti EU pro digitální dekádu[3] s cílem zajistit, aby občané a podniky těžili z důvěryhodných digitálních technologií.

2. Cílem návrhu, založeného na článku 114 Smlouvy o fungování EU (dále jen „SFEU“), je dále zlepšit odolnost veřejných a soukromých subjektů, příslušných orgánů a Unie jako celku i jejich schopnosti reagovat na bezpečnostní incidenty.

3. V Evropském parlamentu je výborem příslušným pro návrh Výbor pro průmysl, výzkum a energetiku (ITRE). Výbor ITRE přijal zprávu zpravodaje dne 28. října 2021.

4. Evropský hospodářský a sociální výbor přijal stanovisko dne 28. dubna 2021.

5. Dne 3. února 2021 se Výbor stálých zástupců rozhodl návrh konzultovat s Evropským výborem regionů[4]. Evropský výbor regionů své stanovisko dosud nevydal.

6. Evropský inspektor ochrany údajů přijal stanovisko dne 11. března 2021[5].

7. Ve svých závěrech[6] ze dne 22. března 2021 týkajících se strategie kybernetické bezpečnosti EU pro digitální dekádu vzala Rada na vědomí nový návrh, jenž vychází ze směrnice o bezpečnosti sítí a informací, a znovu potvrdila, že podporuje posilování a harmonizaci vnitrostátních rámců kybernetické bezpečnosti a trvalé spolupráce mezi členskými státy.

8. Evropská rada ve svých závěrech ze zasedání konaného ve dnech 21. a 22. října 2021 vyzvala k dosažení pokroku v práci související s návrhem revidované směrnice o bezpečnosti sítí a informací.

---

3 Dokument 14133/20.
4 Dokument 5573/21.
5 Stanovisko 5/2021 ke strategii kybernetické bezpečnosti EU a směrnici NIS 2.
6 Dokument 6722/21.

II. ČINNOST V RÁMCI PŘÍPRAVNÝCH ORGÁNŮ RADY

9. V Radě návrh posuzuje Horizontální pracovní skupina pro otázky týkající se kybernetiky. Posuzování návrhu bylo zahájeno během portugalského předsednictví dne 19. ledna pečlivým prostudováním návrhu, což členským státům umožnilo předložit jejich otázky a poukázat na jejich hlavní obavy a získat od Komise podrobné vysvětlení změn v revidované směrnici.

10. V průběhu portugalského předsednictví věnovala Horizontální pracovní skupina pro otázky týkající se kybernetiky prezentaci návrhu a jeho prostudování celkem 17 zasedání. Na zasedání Rady pro dopravu, telekomunikace a energetiku dne 4. června 2021 byla předložena zpráva o pokroku v této oblasti.

11. Poté práce pokračovala a zintenzivnila se během slovinského předsednictví s cílem dosáhnout obecného přístupu na zasedání Rady pro dopravu, telekomunikace a energetiku konajícím se dne 3. prosince 2021.Slovinské předsednictví věnovalo revizi návrhu NIS 2 a mnoha dvoustranným jednáním na všech úrovních patnáct zasedání.

12. Horizontální pracovní skupina pro otázky týkající se kybernetiky zaměřila svou práci při redakční úpravě znění návrhu nejprve na vzájemné působení směrnice NIS 2 a odvětvových právních předpisů a na oblast působnosti, zejména pokud jde o veřejnou správu, kořenové servery DNS a ustanovení o vyloučení, a dále mimo jiné na vzájemná hodnocení, pravomoc a vzájemnou pomoc, koordinované odhalování zranitelností, databáze jmen domén a údajů o registraci a na mezinárodní spolupráci.

13. První kompromisní návrh znění navrhované směrnice byl vydán dne 21. září 2021[7] na základě písemných připomínek a pracovních dokumentů obdržených od členských států, jakož i předchozích kompromisních návrhů týkajících se vzájemného působení směrnice NIS 2 a odvětvových právních předpisů a oblasti působnosti směrnice NIS 2.

[7] Dokument 12019/21.

14. Poslední revize[8] kompromisního návrhu předsednictví byla projednána na úrovni pracovní skupiny dne 22. listopadu 2021. Delegace kompromisní znění obecně uvítaly, několik z nich však vzneslo výhrady přezkumu nebo učinilo připomínky k částem kompromisního návrhu. Pro některé části znění byly navrhovány určité technické redakční úpravy.

III. VĚCNÉ ASPEKTY

15. Na základě jednání na úrovni pracovní skupiny byly jako hlavní politické otázky označeny tyto body:

a) Oblast působnosti (článek 2)

Od zahájení jednání o návrhu směrnice NIS 2 bylo hlavní obavou členských států významné zvýšení počtu subjektů, na něž se směrnice vztahuje, a zejména zavedení pravidla velikostního omezení, podle něhož všechny střední a velké subjekty, které působí v odvětvích nebo poskytují druh služeb, na něž se vztahuje směrnice NIS 2, spadají do její oblasti působnosti. Kompromisní návrh sice toto obecné pravidlo zachovává, obsahuje však dodatečná ustanovení k zajištění nezbytné proporcionality, vyšší úrovně řízení rizik a jasných kritérií kritičnosti pro určení subjektů, které spadají do oblasti působnosti směrnice. Kompromisní návrh navíc obsahuje konkrétní ustanovení o upřednostnění používání opatření dohledu na základě přístupu založeného na posouzení rizik.

[8] Dokument ST 12019/5/21 REV 5.

b) Veřejná správa (čl. 2 odst. 2a)

Zahrnutí veřejné správy do oblasti působnosti směrnice NIS 2 bylo velmi diskutovaným tématem, neboť odvětví veřejné správy je odlišnější než jiná odvětví, na něž se směrnice NIS 2 vztahuje. Předsednictví usilovalo o vyvážený přístup, který zohlední specifika vnitrostátních rámců veřejné správy a zajistí členským státům určitou míru flexibility, pokud jde o určování subjektů veřejné správy spadajících do oblasti působnosti směrnice NIS 2. V kompromisním znění se proto směrnice NIS 2 vztahuje na subjekty veřejné správy ústředních vlád, zatímco členské státy mohou rovněž stanovit, že se směrnice vztahuje na subjekty veřejné správy na regionální a místní úrovni.

c) Ustanovení o vyloučení (čl. 2 odst. 3a a 3aa)

Členské státy si přály dále vyjasnit ustanovení o vyloučení v tom smyslu, že se směrnice nevztahuje na subjekty převážně vykonávající činnost v oblasti obrany, národní bezpečnosti, veřejné bezpečnosti nebo prosazování práva nebo na činnosti týkající se národní bezpečnosti nebo obrany. Vyloučeny jsou rovněž soudnictví, parlamenty a centrální banky.

d) Vzájemné působení s odvětvovými právními předpisy

Členské státy zdůraznily potřebu sladění směrnice NIS 2 a odvětvových právních předpisů, zejména nařízení o digitální provozní odolnosti finančního sektoru (DORA) a směrnice o odolnosti kritických subjektů. Směrnice NIS 2, která by měla být základem pro minimální harmonizaci v oblasti kybernetické bezpečnosti, obsahuje zvláštní článek o odvětvových aktech Unie (článek 2b). Pokud jde o vzájemné působení se směrnicí o odolnosti kritických subjektů, kompromisní návrh zajišťuje větší jasnost ohledně přístupu zohledňujícího všechna rizika. Další důležitá doplnění se týkají ujednání o spolupráci mezi příslušnými orgány podle příslušných právních aktů.

e) Vzájemné učení (článek 16)

Až na některé výjimky byly členské státy proti tomu, aby Komise zavedla povinná vzájemná hodnocení. Navrhovaný kompromis zajišťuje, aby nový mechanismus vzájemného učení vycházel ze vzájemné důvěry a byl dobrovolným procesem řízeným členskými státy.

f) Pravomoc a územní působnost (článek 24) a vzájemná pomoc (článek 34)

Členské státy vyjádřily obavy ohledně důsledků rozdílné pravomoci pro subjekty v odvětví IKT, jak navrhla Komise. Kompromisní znění vyjasnilo pravomoc na základě druhu subjektů a posílilo formulaci týkající se vzájemné pomoci.

g) Oznamovací povinnosti (článek 20)

V návaznosti na obavy vyjádřené členskými státy, že by tyto povinnosti příliš zatížily subjekty, na které se vztahuje směrnice NIS 2, a vedly by to k nadměrnému oznamování, bylo povinné oznamování významných kybernetických hrozeb z kompromisního znění vypuštěno.

IV. ZÁVĚR

16. Dne 24. listopadu 2021 dosáhl Výbor stálých zástupců dohody o kompromisním znění uvedeném v příloze a rozhodl o jeho předložení Radě pro dopravu, telekomunikace a energetiku za účelem přijetí obecného přístupu.

17. Rada se proto vyzývá, aby na svém zasedání dne 3. prosince 2021 schválila kompromisní znění předložené předsednictvím a uvedené v příloze a aby přijala obecný přístup.

Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

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

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

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

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

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

s ohledem na stanovisko Výboru regionů[10],

v souladu s řádným legislativním postupem,

[9] Úř. věst. C , , s. .
[10] Úř. věst. C , , s. .

vzhledem k těmto důvodům:

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

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

---

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

12 Článek 11 směrnice (EU) 2016/1148.

13 Článek 12 směrnice (EU) 2016/1148.

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

(4) Právním základem směrnice (EU) 1148/2016 byl článek 114 Smlouvy o fungování Evropské unie (SFEU), jehož cílem je vytvoření a fungování vnitřního trhu posílením opatření ke sbližování vnitrostátních předpisů. Požadavky kybernetické bezpečnosti kladené na subjekty poskytující služby nebo vyvíjející příslušné hospodářské činnosti se mezi členskými státy značně liší co do druhů požadavků, míry jejich podrobnosti a způsobu dohledu. Tyto rozdíly jsou spojeny s dalšími náklady a vytvářejí obtíže pro podniky, které nabízejí přeshraničně zboží nebo služby. Požadavky, jež ukládá jeden členský stát a které se liší od požadavků, jež ukládá jiný členský stát, nebo jsou s nimi dokonce v rozporu, mohou tyto přeshraniční činnosti podstatně ovlivnit.

Dále je pravděpodobné, že možná neoptimální koncepce nebo neoptimální provádění [...] **opatření** v oblasti kybernetické bezpečnosti v jednom členském státě může mít důsledky pro úroveň kybernetické bezpečnosti jiných členských států, zejména vzhledem k intenzivní přeshraniční výměně. Z přezkumu směrnice (EU) 2016/1148 vyplynuly velké rozdíly v jejím provádění členskými státy, a to i ve vztahu k její oblasti působnosti, jejíž vymezení bylo do značné míry ponecháno na uvážení členských států. Směrnice (EU) 2016/1148 rovněž dávala členským státům velmi široký prostor pro uvážení, pokud jde o provedení povinností v oblasti bezpečnosti a hlášení incidentů, které v ní byly stanoveny. Tyto povinnosti byly proto na úrovni členských států provedeny výrazně odlišnými způsoby. K podobným rozdílům v provádění docházelo ve vztahu k ustanovením uvedené směrnice týkajícím se dohledu a vymáhání.

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

(6) [...] (Č)lenské státy **by měly mít možnost** přijmout nezbytná opatření, aby zajistily ochranu svých základních bezpečnostních zájmů, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů [...]. **[...] Směrnice by se neměla vztahovat na určité veřejné či soukromé subjekty, které vyvíjejí činnost v těchto oblastech. Neměla by se vztahovat ani na činnosti subjektů prováděné v těchto oblastech. Dále** není žádný členský stát povinen poskytovat informace, jejichž zpřístupnění by bylo v rozporu se základními zájmy jeho veřejné bezpečnosti. [...] Uplatní se pravidla členských států **nebo** Unie o ochraně utajovaných informací, dohody o zachování důvěrnosti údajů nebo neformální dohody o zachování důvěrnosti, jako je například tzv. „semaforový protokol“ (Traffic Light Protocol)[14].

(6a) Na jakékoli zpracování osobních údajů podle této směrnice se uplatní právo Unie pro ochranu osobních údajů a soukromí. Především není touto směrnicí dotčeno nařízení Evropského parlamentu a Rady (EU) 2016/679 a směrnice Evropského parlamentu a Rady 2002/58/ES, a proto by nemělo mít dopad zejména na úkoly a pravomoci nezávislých orgánů dohledu příslušných pro monitorování souladu s příslušnými unijními právními předpisy pro ochranu údajů.

---

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

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

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

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

(8a) Za účelem zajištění jasného přehledu subjektů spadajících do oblasti působnosti této směrnice by měly mít členské státy možnost stanovit vnitrostátní mechanismy pro vlastní oznamování, jež vyžadují, aby subjekty, na které se vztahuje tato směrnice, nahlásily přinejmenším svůj název, adresu a kontaktní údaje, jakož i odvětví, v němž provozují činnost, nebo druh služby, kterou poskytují, a případně seznam členských států, v nichž daný subjekt poskytuje své služby, příslušným orgánům podle této směrnice nebo subjektům určeným za tímto účelem členskými státy. Členské státy mohou rozhodnout o vhodných mechanismech, pokud na vnitrostátní úrovni existují registry, které umožňují určení subjektů spadajících do oblasti působnosti této směrnice.

(9) Tato směrnice by se [...] měla vztahovat i na **mikrosubjekty nebo** [...] na malé subjekty, které splňují určitá kritéria, jež naznačují klíčovou úlohu pro hospodářství nebo společnosti členských států nebo pro konkrétní odvětví či konkrétní druhy služeb. Členské státy by měly být odpovědné za [...] to, že Komisi předloží [...] **přinejmenším relevantní informace o počtu určených subjektů, odvětví, do kterého náleží, nebo druhu služby, kterou poskytují, a o konkrétních kritériích, na základě kterých byly určeny. Členské státy se mohou rovněž rozhodnout, že Komisi předloží názvy těchto subjektů, je-li to v souladu s vnitrostátními předpisy týkajícími se bezpečnosti.**

(9a) Z oblasti působnosti této směrnice jsou vyloučeny subjekty veřejné správy, které vykonávají činnost v oblasti národní bezpečnosti, obrany, veřejné bezpečnosti, prosazování práva, jakož i soudnictví, parlamenty a centrální banky. Pro účely této směrnice se subjekty s regulační pravomocí nepovažují za subjekty vykonávající činnost v oblasti prosazování práva, a tudíž nejsou z těchto důvodů z oblasti působnosti této směrnice vyloučeny. Kromě toho do oblasti působnosti této směrnice nespadají subjekty veřejné správy na úrovni ústřední státní správy, které jsou zřízeny společně se třetí zemí v souladu s mezinárodní dohodou.

(9aa) Členské státy by měly mít možnost stanovit, že subjekty určené před vstupem této směrnice v platnost jako provozovatelé základních služeb podle směrnice (EU) 2016/1148 mají být považovány za základní subjekty.

(9aaa) Tato směrnice se nevztahuje na diplomatické a konzulární mise členských států v zahraničí a na jejich infrastrukturu v oblasti IKT používanou těmito misemi, pokud se taková infrastruktura nachází v zahraničí nebo je provozována pro uživatele v zahraničí.

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

(11) **[...] Subjekty spadající do oblasti působnosti této směrnice by měly být rozděleny do dvou kategorií: základní a důležité, přičemž by se měla zohlednit úroveň kritičnosti daného odvětví nebo druhu služby, kterou poskytují, jakož i jejich velikost. V této souvislosti by se v případě potřeby měla rovněž náležitě zohlednit veškerá relevantní odvětvová posouzení rizik nebo pokyny příslušných orgánů.** Jak základní, tak důležité subjekty by měly podléhat [...] požadavkům na řízení rizik a oznamovacím povinnostem. Dohledové a sankční režimy by mezi těmito dvěma kategoriemi subjektů měly rozlišovat, aby byla zajištěna spravedlivá vyváženost mezi požadavky a povinnostmi **založenými na posouzení rizik** na jedné straně a správní zátěží vyplývající z dohledu nad dodržováním směrnice na druhé straně.

(12) **Tato směrnice stanoví základ pro opatření v oblasti řízení kybernetických bezpečnostních rizik a oznamovací povinnosti napříč všemi odvětvími, jež spadají do její oblasti působnosti. S cílem zabránit roztříštěnosti ustanovení o kybernetické bezpečnosti v rámci právních aktů Unie, jsou-li v zájmu zajištění vysoké úrovně kybernetické bezpečnosti považována za nezbytná dodatečná odvětvová ustanovení týkající se** opatření v oblasti řízení kybernetických bezpečnostních rizik a **oznamovací povinnosti, měla by Komise posoudit, zda by mohla být taková ustanovení stanovena v prováděcím aktu na základě zmocnění uděleného touto směrnicí. V případě, že by takové akty nebyly pro uvedený účel vhodné, mohly** by k zajištění vysoké úrovně [...] kybernetické bezpečnosti přispět odvětvové právní předpisy při současném plném zohlednění specifik a složitosti [...] **dotčených** odvětví. **V odvětvových právních předpisech je třeba vysvětlit, proč nebyl prováděcí akt na základě zmocnění stanoveného v této směrnici vhodný. Tato odvětvová ustanovení právních aktů Unie by zároveň měla náležitě zohlednit potřebu komplexního a harmonizovaného rámce kybernetické bezpečnosti.** [...] **Tím** nejsou dotčeny stávající prováděcí pravomoci, jež byly Komisi svěřeny v řadě odvětví, včetně odvětví dopravy a energetiky.

(12a) Pokud odvětvový právní akt Unie **obsahuje ustanovení** vyžadující [...], aby základní nebo důležité subjekty přijaly **opatření přinejmenším s rovnocenným účinkem jako povinnosti stanovené v této směrnicí a související** s řízením kybernetických bezpečnostních rizik [...] a **povinnosti** oznamovat **významné** incidenty či významné kybernetické hrozby[...], uplatní se tato odvětvová ustanovení, **včetně ustanovení o dohledu a vymáhání. Při určování rovnocenného účinku povinností stanovených v odvětvových ustanoveních právního aktu Unie by měly být zváženy tyto aspekty: i) opatření v oblasti řízení kybernetických bezpečnostních rizik by měla sestávat z vhodných a přiměřených technických a organizačních opatření pro řízení rizik pro bezpečnost sítí a informačních systémů, jež relevantní subjekty používají při poskytování svých služeb a měla by zahrnovat přinejmenším všechny prvky stanovené v této směrnici; ii) povinnost oznamovat významné incidenty a kybernetické hrozby by měla být přinejmenším rovnocenná povinnostem stanoveným v této směrnici, pokud jde o obsah, formát a lhůty oznamování; iii) způsoby oznamování subjekty a příslušnými orgány odvětvových právních aktů Unie by měly být přinejmenším rovnocenné požadavkům stanoveným v této směrnici, pokud jde o jejich obsah, formát a lhůty, a měly by zohledňovat úlohu týmů CSIRT; iv) požadavky na přeshraniční spolupráci pro příslušné orgány by měly být přinejmenším rovnocenné požadavkům stanoveným v této směrnici. Pokud se odvětvová ustanovení právního aktu Unie nevztahují na všechny subjekty v konkrétním odvětví, jež spadají do oblasti působnosti této směrnice, na subjekty, na něž se uvedená odvětvová ustanovení nevztahují, by se měla nadále použít relevantní ustanovení této směrnice.**

(12aa) Komise **by měla pravidelně přezkoumávat uplatňování požadavku na rovnocenný účinek ve vztahu k odvětvovým ustanovením právních aktů Unie** [...]. **Komise má při přípravě tohoto pravidelného přezkumu konzultovat skupinu pro spolupráci.**

(12aaa) Budoucí odvětvové právní akty Unie by měly řádně zohledňovat definice uvedené v článku 4 této směrnice a rámec pro dohled a vymáhání stanovený v kapitole VI této směrnice.

(12ab) Pokud odvětvová ustanovení právních aktů Unie vyžadují, aby základní nebo důležité subjekty přijaly opatření s přinejmenším rovnocenným účinkem jako oznamovací povinnosti stanovené v této směrnici, je třeba se vyhnout překrývání oznamovacích povinností a zajistit soudržnost a efektivitu řešení oznámení o kybernetických hrozbách nebo incidentech. Za tímto účelem mohou uvedená odvětvová ustanovení členským státům umožnit, aby zavedly společný, automatický a přímý mechanismus pro oznamování významných incidentů a kybernetických hrozeb jak orgánům, jejichž úkoly jsou stanoveny v příslušných odvětvových ustanoveních, tak i příslušným orgánům, případně včetně jednotného kontaktního místa a týmů CSIRT, odpovědným za plnění úkolů v oblasti kybernetické bezpečnosti stanovených v této směrnici, nebo mechanismus, který zajišťuje systematické a okamžité sdílení informací a spolupráci mezi příslušnými orgány a týmy CSIRT, pokud jde o řešení těchto oznámení. Pro účely zjednodušení oznamování a provádění společného, automatického a přímého mechanismu oznamování mohou členské státy v souladu s odvětvovými právními předpisy využívat jedno vstupní místo, které zřídí podle čl. 11 odst. 5a této směrnice. Aby byla zajištěna harmonizace, měly by být oznamovací povinnosti vyplývající z odvětvových právních aktů Unie sladěny s oznamovacími povinnostmi uvedenými v této směrnici. Členské státy mohou v souladu s odvětvovými právními předpisy určit, že oznámení je určeno příslušným orgánům podle této směrnice nebo vnitrostátním týmům CSIRT.

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

(13a) Aby se zabránilo mezerám v povinnostech v oblasti kybernetické bezpečnosti uložených subjektům v odvětví letectví uvedeným v příloze I bodě 2 písm. a) a jejich zdvojování, měly by vnitrostátní orgány určené podle nařízení Evropského parlamentu a Rady (ES) č. 300/2008[16] a (EU) 2018/1139[17] a příslušné orgány podle této směrnice spolupracovat při provádění opatření v oblasti řízení kybernetických bezpečnostních rizik a dohledu nad těmito opatřeními na vnitrostátní úrovni. Soulad určitého subjektu s opatřeními v oblasti řízení kybernetických bezpečnostních rizik podle této směrnice [...] by mohly vnitrostátní orgány určené podle nařízení (ES) č. 300/2008 a (EU) 2018/1139 považovat za vyhovující požadavkům stanoveným v uvedených nařízeních a v relevantních aktech v přenesené pravomoci a prováděcích aktech přijatých podle uvedených nařízení.

---

16 **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).**

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

(14) Vzhledem ke vzájemným vazbám mezi kybernetickou bezpečností a fyzickou bezpečností subjektů by měl být zajištěn soudržný přístup ke směrnici Evropského parlamentu a Rady (EU) XXX/XXX a k této směrnici. Za tímto účelem by členské státy měly zajistit, aby kritické subjekty **[**a rovnocenné subjekty**]** podle směrnice (EU) XXX/XXX byly považovány za základní subjekty podle této směrnice. Členské státy by také měly zajistit, aby jejich strategie kybernetické bezpečnosti stanovily politický rámec pro posílení koordinace mezi příslušným orgánem podle této směrnice a příslušným orgánem podle směrnice (EU) XXX/XXX v souvislosti se sdílením informací o incidentech a kybernetických hrozbách a plněním úkolů v oblasti dohledu. **Příslušné o**[...]rgány podle obou směrnic by měly spolupracovat a vyměňovat si informace, zejména ve vztahu k určení kritických subjektů, kybernetických hrozeb, kybernetických bezpečnostních rizik, incidentů, **jakož i nekybernetických rizik, hrozeb nebo incidentů** dotýkajících se kritických subjektů **[**nebo **subjektů rovnocenných kritickým subjektům],** [...] **včetně** opatření v oblasti kybernetické bezpečnosti a **fyzických opatření** přijatých kritickými subjekty a **výsledků činností v oblasti dohledu prováděných s ohledem na tyto subjekty**. **V zájmu zefektivnění činností v oblasti dohledu mezi příslušnými orgány určenými podle obou směrnic a v zájmu minimalizace administrativní zátěže pro dotčené subjekty by příslušné orgány dále měly usilovat o harmonizaci šablon pro oznamování incidentů a postupů v oblasti dohledu.** [...] **Ve vhodných případech mohou** příslušné orgány podle směrnice (EU) XXX/XXX [...] **požádat** příslušné orgány podle této směrnice, aby [...] vykonávaly své dohledové a vymáhací pravomoci vůči základnímu subjektu, který byl označen jako kritický. [...]

(14a) Subjekty patřící do odvětví digitální infrastruktury jsou v zásadě založeny na sítích a informačních systémech, a proto by povinnosti uložené uvedeným subjektům touto směrnicí měly komplexně řešit fyzickou bezpečnost těchto systémů v rámci jejich povinností v oblasti řízení kybernetických bezpečnostních rizik a oznamování. Jelikož se na tyto záležitosti vztahuje tato směrnice, povinnosti stanovené v kapitolách III až VI směrnice (EU) XXX/XXX [CER] se na tyto subjekty nevztahují.

(15) Podpora a ochrana spolehlivého, odolného a bezpečného systému doménových jmen jsou klíčovým faktorem pro zachování integrity internetu a jsou nezbytné pro jeho nepřetržitý a stabilní provoz, na kterém závisí digitální ekonomika a společnost. Tato směrnice by se proto měla vztahovat na poskytovatele služeb systému doménových jmen (DNS) v celém řetězci **poskytování a** řešení systému doménových jmen, **jež mají význam pro vnitřní trh,** včetně [...] **registrů** internetových domén nejvyšší úrovně (TLD), [...] **subjektů poskytujících služby registrace doménových jmen, provozovatelů** autoritativních jmenných serverů pro doménová jména a **provozovatelů** rekurzivních resolverů. **Pojem „poskytovatel služeb DNS“ by se neměl vztahovat na služby DNS provozované pro vlastní účely dotčeného subjektu a jeho přidružených subjektů. Povinnosti v oblasti kybernetické bezpečnosti vyplývající z této směrnice pro tuto kategorii poskytovatelů jsou omezeny výhradně na opatření v oblasti řízení kybernetických bezpečnostních rizik a oznamování, a proto jimi není dotčena správa globálních DNS komunitou mnoha zúčastněných stran.**

(16) Služby cloud computingu by měly zahrnovat služby, které umožňují správu na vyžádání a široký dálkový přístup k rozšiřitelnému a přizpůsobitelnému úložišti distribuovaných výpočetních zdrojů, které je možno sdílet. Tyto výpočetní zdroje zahrnují zdroje, jako jsou sítě, servery nebo jiná infrastruktura, operační systémy, software, ukládání, aplikace a služby. **Modely služeb cloud computingu zahrnují mimo jiné infrastrukturu jako službu (IaaS), platformu jako službu (PaaS), software jako službu (SaaS) a síť jako službu (NaaA).** Modely zavádění cloud computingu by měly zahrnovat soukromý, komunitní, veřejný a hybridní cloud. Uvedené služby a modely zavádění mají tentýž význam jako podmínky poskytování služeb a modely zavádění definované podle normy ISO/IEC 17788:2014. Schopnost uživatele cloud computingu jednostranně vlastními silami využívat výpočetní potenciál, jako je čas serveru nebo ukládání na síti, bez jakékoli interakce poskytovatele služeb cloud computingu s člověkem, by bylo možné popsat jako správu na vyžádání. Pojem „široký dálkový přístup“ se používá k popsání toho, že cloudová kapacita je poskytována po síti a přístup k ní se uskutečňuje prostřednictvím mechanismu podporujícího použití heterogenních platforem s tenkými nebo tlustými klienty (včetně mobilních telefonů, tabletů, laptopů a pracovních stanic).

Pojem „rozšiřitelný“ poukazuje na skutečnost, že v zájmu pokrytí nerovnoměrné poptávky jsou výpočetní zdroje přidělovány poskytovatelem cloudových služeb flexibilně, bez ohledu na zeměpisnou polohu zdrojů. Pojem „přizpůsobitelné úložiště“ označuje skutečnost, že uvedené výpočetní zdroje jsou poskytovány a uvolňovány na základě poptávky, aby bylo možno urychleně zvyšovat i snižovat dostupné zdroje se zřetelem na zatížení. Pojmem „které je možno sdílet“ se rozumí, že tyto výpočetní zdroje jsou poskytovány vícero uživatelům, kteří k dané službě sdílejí společný přístup, avšak zpracování probíhá pro každého uživatele odděleně, byť je služba poskytována z téhož elektronického zařízení. Pojem „distribuovaný“ označuje ty výpočetní zdroje, které se nacházejí na různých sítově propojených počítačích nebo zařízeních a které mezi sebou komunikují a koordinují prostřednictvím předávání zpráv.

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

(18) Služby, jež nabízejí poskytovatelé služeb datových center, nemusí být vždy poskytovány ve formě služeb cloud computingu. Datová centra tedy ne vždy tvoří součást infrastruktury cloud computingu. Aby bylo možné řídit všechna rizika pro bezpečnost sítí a informačních systémů, měla by se tato směrnice vztahovat také na poskytovatele takových služeb datových center, které nejsou službami cloud computingu. Pro účely této směrnice by pojem „služba datových center“ měl zahrnovat poskytování služby, která zahrnuje struktury nebo skupiny struktur určené pro centralizované úpravy, vzájemné propojení a provozování informačních technologií a síťových zařízení poskytujících služby ukládání, zpracování a přepravu dat spolu se všemi zařízeními a infrastrukturami pro rozvod energie a kontrolu životního prostředí. Pojem „služba datových center“ se nevztahuje na interní, firemní datová centra vlastněná a provozovaná pro vlastní potřebu dotyčného subjektu.

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

---

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

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

(**20a**) **Za účelem dosažení a udržení vysoké úrovně kybernetické bezpečnosti by vnitrostátní strategie kybernetické bezpečnosti požadované touto směrnicí měly sestávat ze soudržných rámců, které zajistí správu v oblasti kybernetické bezpečnosti. Tyto strategie se mohou skládat z jednoho nebo několika dokumentů legislativní nebo nelegislativní povahy.**

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

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

(23) Příslušné orgány nebo týmy CSIRT by měly od subjektů dostávat oznámení o incidentech účinným a účelným způsobem, **mimo jiné s cílem případně usnadnit včasnou reakci na incidenty a poskytnout reakci oznamujícímu subjektu**. Jednotným kontaktním místům by mělo být uloženo, aby zasílala oznámení o incidentech jednotným kontaktním místům jiných dotčených členských států. [...]

(23a) Odvětvové právní akty Unie, které vyžadují opatření v oblasti řízení kybernetických bezpečnostních rizik nebo oznamovací povinnosti s přinejmenším rovnocenným účinkem jako oznamovací povinnosti, které jsou stanoveny v této směrnici, by mohly stanovit, že jejich určené příslušné orgány vykonávají své dohledové a vymáhací pravomoci ve vztahu k těmto opatřením nebo povinnostem za pomoci příslušných orgánů určených v souladu s touto směrnicí. Dotčené příslušné orgány by za tímto účelem mohly uzavřít ujednání o spolupráci. Tato ujednání o spolupráci by mohla mimo jiné stanovit postupy týkající se koordinace činností v oblasti dohledu, včetně postupů šetření a kontrol na místě v souladu s vnitrostátním právem a mechanismu pro výměnu relevantních informací mezi příslušnými orgány o dohledu a vymáhání, včetně přístupu k informacím souvisejícím s kybernetikou, které si vyžádaly příslušné orgány určené v souladu s touto směrnicí.

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

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

(26) S ohledem na význam mezinárodní spolupráce na poli kybernetické bezpečnosti by týmy CSIRT měly mít možnost účastnit se kromě sítě CSIRT zřízené touto směrnicí také dalších sítí pro mezinárodní spolupráci. **Týmy CSIRT a příslušné orgány by si proto mohly za účelem plnění svých úkolů v souladu s nařízením (EU) 2016/679 vyměňovat informace, včetně osobních údajů, s týmy CSIRT třetích zemí nebo jejich orgány. V případě neexistence rozhodnutí o odpovídající ochraně přijatého v souladu s článkem 45 nařízení (EU) 2016/679 nebo vhodných záruk podle článku 46 uvedeného nařízení by výměna osobních údajů, která je považována za nezbytnou pro účely zmírnění významných kybernetických hrozeb a reakce na probíhající významný incident, mohla být považována za důležitý důvod veřejného zájmu ve smyslu čl. 49 odst. 1 písm. d) nařízení (EU) 2016/679.**

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

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

(28) Využití zranitelných míst v sítích a informačních systémech může způsobit vážná narušení a škody, a rychlé určení a náprava těchto zranitelných míst je proto důležitým faktorem při snižování kybernetických bezpečnostních rizik. Subjekty, které takové systémy vyvíjejí **nebo spravují**, by proto měly stanovit vhodné postupy k řešení zranitelných míst, jakmile jsou zjištěna. Jelikož zranitelná místa jsou často zjištěna a ohlášena (jsou zpřístupněny s nimi související informace) třetími stranami (subjekty ohlašujícími incidenty), výrobce nebo poskytovatel produktů nebo služeb IKT by měl rovněž zavést nezbytné postupy pro získávání informací o zranitelných místech od třetích stran. Vodítko pro řešení zranitelných míst a zpřístupňování souvisejících informací v této souvislosti poskytují mezinárodní normy ISO/IEC 30111 a ISO/IEC [...] **29147**. Pokud jde o zpřístupňování informací o zranitelných místech, je obzvláště důležitá koordinace mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů nebo služeb IKT. Koordinované zpřístupňování informací o zranitelných místech specifikuje strukturovaný proces, jehož prostřednictvím jsou zranitelná místa hlášena organizacím takovým způsobem, který organizaci umožní diagnostikovat a odstranit zranitelné místo dříve, než budou podrobné informace o něm sděleny třetím stranám nebo veřejnosti. Koordinované zpřístupňování informací o zranitelných místech by mělo zahrnovat také koordinaci mezi subjektem ohlašujícím incidenty a organizací, pokud jde o načasování odstranění a zveřejnění zranitelných míst.

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

(29) Členské státy by proto měly stanovit příslušnou vnitrostátní politiku a přijmout tak opatření k usnadnění koordinovaného zpřístupňování informací o zranitelných místech. **V rámci své vnitrostátní politiky by členské státy měly usilovat o to, aby se v souladu se svým vnitrostátním právním řádem v co největší míře zabývaly výzvami, jimž čelí výzkumní pracovníci zabývající se zranitelností, včetně jejich možného vystavení trestní odpovědnosti.** [...] Členské státy měly určit tým CSIRT, který převezme úlohu „koordinátora“ a v případě potřeby bude působit jako zprostředkovatel mezi subjekty ohlašujícími incidenty a výrobci nebo poskytovateli produktů nebo služeb IKT. Úkoly koordinátora týmů CSIRT by měly zahrnovat zejména určení a kontaktování dotčených subjektů, podporu subjektů ohlašujících incidenty, dojednávání lhůt pro zpřístupňování informací o zranitelných místech, které se dotýkají mnoha organizací (**koordinované** zpřístupňování informací o zranitelných místech ohrožujících více stran), a řešení těchto zranitelných míst. **Pokud by oznámené** zranitelné místo **mohlo mít případně významný dopad na subjekty** [...] ve více než jednom členském státě, měly by určené týmy CSIRT **ve vhodných případech** spolupracovat v rámci sítě CSIRT.

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

(31) Ačkoli podobné registry nebo databáze zranitelností existují, jsou hostovány a spravovány subjekty, které nejsou usazeny v Unii. Evropský registr zranitelností spravovaný agenturou ENISA by poskytl lepší transparentnost procesu zveřejňování informací předtím, než jsou informace o zranitelném místě oficiálně zpřístupněny, a odolnost v případech narušení nebo přerušení poskytování podobných služeb. S cílem zabránit zdvojení úsilí a v co největší možné míře usilovat o komplementaritu, by agentura ENISA měla zkoumat možnost uzavření strukturovaných dohod o spolupráci s podobnými registry v jurisdikcích třetích zemí. **Agentura ENISA by měla zejména prozkoumat možnost úzké spolupráce s provozovateli systému pro společná zranitelná místa a expozice (Common Vulnerabilities and Exposures, CVE), včetně možnosti stát se stát se jedním z kořenových orgánů pro přidělování čísel CVE“.**

(32) **Skupina pro spolupráci by měla nadále podporovat a usnadňovat strategickou spolupráci a výměnu informací, jakož i posilovat důvěru mezi členskými státy.** Skupina pro spolupráci by měla každé dva roky přijmout pracovní program včetně opatření, které má skupina podniknout ke splnění svých cílů a úkolů. Časový rámec prvního programu, který by byl podle této směrnice přijat, by byl sladěn s časovým rámcem posledního programu přijatého podle směrnice (EU) 2016/1148, aby se zabránilo možnému přerušení práce skupiny.

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

(34) Skupina pro spolupráci by i nadále měla být flexibilním fórem a měla by být schopna reagovat na měnící se a nové priority a výzvy politik, a přitom brát v úvahu dostupnost zdrojů. Měla by organizovat pravidelná společná setkání s relevantními soukromými zúčastněnými stranami z celé Unie za účelem projednání činností prováděných skupinou a shromažďování vstupů týkajících se vznikajících politických výzev. S cílem posílit spolupráci na úrovni Unie by skupina měla zvážit pozvání k účasti na její činnosti pro instituce a agentury Unie zapojené do politiky v oblasti kybernetické bezpečnosti, jako je Evropské centrum pro boj proti kyberkriminalitě (EC3), Agentura Evropské unie pro bezpečnost letectví (EASA) a Agentura Evropské unie pro kosmický program (EUSPA).

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

(35a) Síť CSIRT by měla i nadále přispívat k posilování důvěry a k podpoře rychlé a účinné operativní spolupráce mezi členskými státy. Za účelem posílení operativní spolupráce na úrovni Unie by síť CSIRT měla zvážit možnost, že k účasti na své činnosti přizve instituce a agentury Unie zapojené do politiky kybernetické bezpečnosti, jako je Europol.

(36) [...]

(36a) V zájmu usnadnění účinného provádění ustanovení této směrnice, jako je řešení zranitelných míst, řízení rizik v oblasti kybernetické bezpečnosti, opatření pro oznamování a ujednání o sdílení informací, mohou členské státy spolupracovat se třetími zeměmi a provádět činnosti, které jsou pro tento účel považovány za vhodné, včetně výměny informací o hrozbách, incidentech, zranitelnostech, nástrojích a metodách, taktice, technikách a postupech, připravenosti a cvičeních pro řešení kybernetických krizí, odborné přípravě, budování důvěry a strukturovaných ujednáních o sdílení informací. Tato ujednání o spolupráci by měla být v souladu s právem Unie v oblasti ochrany údajů.

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

(37a) Síť EU-CyCLONe by měla fungovat jako zprostředkující síť mezi technickou a politickou úrovní při rozsáhlých kybernetických bezpečnostních incidentech a krizích. Měla by zlepšit spolupráci na operační úrovni tím, že bude vycházet ze zjištění sítí CSIRT a s využitím vlastních schopnosti vypracovávat analýzy dopadu rozsáhlých incidentů a krizí a bude podporovat rozhodování na politické úrovni. Orgány, instituce a jiné subjekty EU by měly určit příslušný orgán odpovědný za řízení rozsáhlých bezpečnostních incidentů a krizí, který se stane členem sítě EU-CyCLONe.

(38) [...]

(39) [...]

(39a) Povinnost zajistit bezpečnost sítí a informačních systémů mají do značné míry základní a důležité subjekty. Měla by být prosazována a rozvíjena kultura řízení rizik spočívající v posuzování rizik a zavádění bezpečnostních opatření úměrných hrozícím rizikům.

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

(40a) Vzhledem k tomu, že hrozby pro bezpečnost sítí a informačních systémů mohou být různého původu, tato směrnice uplatňuje přístup zohledňující všechna rizika, jenž zahrnuje ochranu sítě a informačních systémů a jejich fyzické prostředí před všemi událostmi, jako je krádež, požár, povodeň, výpadky telekomunikací nebo elektrického proudu, nebo před neoprávněným fyzickým přístupem k informacím a zařízením pro zpracování informací daného subjektu a jejich poškozením a zásahům do nich, jež by mohly narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné. Opatření k řízení rizik by proto měla rovněž řešit fyzickou a environmentální bezpečnost tím, že budou zahrnovat opatření na ochranu sítě a informačních systémů subjektu před selháním systému, lidskou chybou, zlovolným jednáním nebo přírodními jevy v souladu s evropskými nebo mezinárodně uznávanými normami, jako jsou normy obsažené v řadě ISO 27000. V tomto ohledu by se subjekty měly v rámci svých opatření k řízení rizik zabývat rovněž bezpečností lidských zdrojů a zavést vhodné politiky kontroly přístupu. Tato opatření by měla být v souladu se směrnicí XXXX [směrnice CER].

(40b) V případě neexistence příslušných evropských systémů certifikace kybernetické bezpečnosti přijatých v souladu s nařízením (EU) 2019/881 by členské státy mohly ke splnění požadavků na řízení kybernetických bezpečnostních rizik podle této směrnice vyžadovat, aby subjekty používaly certifikované produkty, služby a procesy IKT nebo aby získaly certifikát podle platných vnitrostátních systémů kybernetické bezpečnosti.

(41) Požadavky na řízení kybernetických bezpečnostních rizik by měly být úměrné rizikům, jež dané sí**ti** nebo informační**mu** systém**u** [...] **hrozí**, aby na základní a důležité subjekty nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových opatření a **náklady na jejich provedení**. **Měla by být rovněž náležitě zohledněna velikost subjektu, pravděpodobnost výskytu incidentů a jejich závažnost.**

(41a) V zájmu snížení regulační zátěže by požadavky na provádění opatření k řízení kybernetických bezpečnostních rizik pro střední a malé subjekty nebo mikrosubjekty měly být v zásadě mírnější, ledaže by kritéria kritičnosti nebo vnitrostátní posouzení rizik odůvodňovala přísnější požadavky, a to zejména pokud jde o subjekty, které splňují kritéria týkající se kritičnosti stanovená v této směrnici.

(42) Základní a důležité subjekty by měly zajistit bezpečnost sítí a informačních systémů, které užívají ve svých činnostech. Jedná se především o soukromé sítě a informační systémy, jež jsou buď řízeny jejich interními pracovníky IT, nebo jejichž bezpečnost zajišťuje externí dodavatel. Požadavky týkající se řízení kybernetických bezpečnostních rizik a hlášení podle této směrnice by měly pro příslušné základní a důležité subjekty platit bez ohledu na to, zda správu svých sítí a informačních systémů provádějí interně, nebo s pomocí externího dodavatele.

(42aa) S ohledem na přeshraniční povahu služeb by poskytovatelé služeb DNS, registry TLD a subjekty poskytující služby registrace domén pro TLD, poskytovatelé služeb cloud computingu, poskytovatelé služeb datových center, poskytovatelé sítí pro doručování obsahu, poskytovatelé řízených služeb a poskytovatelé řízených bezpečnostních služeb měli podléhat vyšší míře harmonizace na úrovni Unie. Provádění opatření v oblasti kybernetické bezpečnosti by proto mělo být usnadněno prováděcím aktem.

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

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

(44a) Příslušné vnitrostátní orgány mohou v rámci svých úkolů v oblasti dohledu rovněž využívat služeb kybernetické bezpečnosti, jako jsou bezpečnostní audity a penetrační testování nebo reakce na incidenty. S cílem pomoci subjektům i příslušným vnitrostátním orgánům při výběru kvalifikovaných a důvěryhodných poskytovatelů služeb kybernetické bezpečnosti by Komise s pomocí skupiny pro spolupráci a agentury ENISA měla zvážit možnost požadovat evropské systémy certifikace kybernetické bezpečnosti v souladu s článkem 48 nařízení (EU) 2019/881.

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

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

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

(47) Posouzení rizik dodavatelského řetězce by s ohledem na charakteristické rysy dotčeného odvětví měla zohlednit jak technické, tak případné netechnické faktory včetně faktorů vymezených v doporučení (EU) 2019/534, v koordinovaném posouzení rizik pro bezpečnost sítí 5G v celé EU a v souboru opatření EU pro kybernetickou bezpečnost sítí 5G, na němž se dohodla skupina pro spolupráci. K určení dodavatelských řetězců, které by měly podléhat koordinovanému posouzení rizik, by měla být vzata v úvahu tato kritéria: i) rozsah, v jakém základní a důležité subjekty využívají konkrétní kritické služby, systémy a produkty IKT a jsou na nich závislé; ii) relevantnost konkrétních služeb, systémů nebo produktů IKT pro plnění kritických nebo citlivých funkcí, včetně zpracování osobních údajů; iii) dostupnost alternativních služeb, systémů nebo produktů IKT; iv) odolnost celého dodavatelského řetězce služeb, systémů nebo produktů IKT vůči narušení a v) u vznikajících služeb, systémů nebo produktů IKT jejich budoucí význam pro činnost subjektů.

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

---

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

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

(48a) Bezpečnostní povinnosti stanovené v této směrnici by měly být považovány za doplňkové k požadavkům kladeným na poskytovatele služeb vytvářejících důvěru podle nařízení (EU) č. 910/2014 (nařízení eIDAS). Od poskytovatelů služeb vytvářejících důvěru by mělo být požadováno, aby přijali veškerá vhodná a přiměřená opatření k řízení rizik spojených s jejich službami, a to i ve vztahu k zákazníkům a spoléhajícím se třetím stranám, a aby oznamovali bezpečnostní incidenty podle této směrnice. Tyto povinnosti v oblasti bezpečnosti a hlášení by se rovněž měly týkat fyzické ochrany poskytované služby. I nadále se použije článek 24 nařízení (EU) č. 910/2014.

(48aa) Členské státy mohou orgánům dohledu eIDAS svěřit úlohu příslušných orgánů pro služby vytvářející důvěru s cílem zajistit pokračování stávajících postupů a využít znalostí a zkušeností získaných při uplatňování nařízení eIDAS. Je-li tato úloha přidělena jinému orgánu, měly by příslušné vnitrostátní orgány podle této směrnice úzce a včas spolupracovat formou výměny příslušných informací s cílem zajistit účinný dohled nad poskytovateli služeb vytvářejících důvěru a jejich dodržování požadavků stanovených v této směrnici a nařízení [XXXX/XXXX].

Příslušný vnitrostátní orgán podle této směrnice by měl v příslušných případech neprodleně informovat orgán dohledu podle nařízení eIDAS o všech oznámených významných kybernetických hrozbách nebo incidentech s dopadem na služby vytvářející důvěru, jakož i o jakémkoli nedodržení požadavků podle této směrnice ze strany poskytovatele služeb vytvářejících důvěru. Pro účely hlášení mohou členské státy případně využít jednotného kontaktního místa zřízeného za účelem společného a automatického hlášení incidentů jak orgánu dohledu podle nařízení eIDAS, tak příslušnému orgánu podle této směrnice. Pravidly o povinnostech ohlašování by nemělo být dotčeno nařízení Evropského parlamentu a Rady (EU) 2016/679 a směrnice Evropského parlamentu a Rady 2002/58/ES[24].

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

(49) Pokud je to vhodné a s cílem zabránit zbytečným narušením by stávající vnitrostátní pokyny [...] přijaté k provedení pravidel týkajících se bezpečnostních opatření stanovených v článku 40[...] a 41 směrnice (EU) 2018/1972[...] **měly být zohledňovány v prováděcích opatřeních zavedených členskými státy v souvislosti s touto směrnicí, čímž se využije znalostí a dovedností získaných v rámci směrnice (EU) 2018/1972, pokud jde o opatření k řízení kybernetických bezpečnostních rizik a oznamování incidentů. Agentura ENISA může rovněž pro poskytovatele veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací vypracovat pokyny týkající se požadavků v oblasti bezpečnosti a hlášení s cílem usnadnit harmonizaci a přechod a minimalizovat narušení. Členské státy mohou úlohu příslušných orgánů pro elektronické komunikace svěřit vnitrostátním regulačním orgánům s cílem zajistit pokračování stávajících postupů a využít znalostí a zkušeností získaných v rámci směrnice (EU) 2018/1972.**

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

(51) Vnitřní trh více než kdy předtím spoléhá na fungování internetu. Na službách poskytovaných po internetu jsou závislé služby prakticky všech základních a důležitých subjektů. S cílem zajistit bezproblémové poskytování služeb základních a důležitých subjektů je důležité, aby veřejné sítě elektronických komunikací, jako jsou například internetové páteřní sítě nebo podmořské komunikační kabely, měly zavedena odpovídající opatření v oblasti kybernetické bezpečnosti a hlásily incidenty, které se jich týkají.

(52) V **příslušných** [...] případech by subjekty měly informovat příjemce svých služeb o konkrétních [...] opatřeních, která mohou přijmout, aby snížili riziko, jež jim vyplývá **z významných kybernetických hrozeb**. **Subjekty by měly ve vhodných případech, a zejména v případech, kdy se může naplnit významná kybernetická hrozba, o této hrozbě informovat vedle příslušných orgánů nebo týmů CSIRT také příjemce svých služeb.** Požadavek na informování příjemců o hrozbách by subjekty neměl zbavovat povinnosti přijmout na své vlastní náklady přiměřená a okamžitá opatření s cílem zamezit jakýmkoli kybernetickým hrozbám nebo je odstranit a obnovit běžnou úroveň bezpečnosti služby. Tyto informace o **kybernetických** [...] hrozbách by měly být příjemcům poskytovány zdarma.

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

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

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

(55a) Proaktivní přístup ke kybernetickým hrozbám je zásadní složkou řízení kybernetických rizik, které příslušným orgánům umožní účinně předcházet tomu, aby kybernetické hrozby přerostly do skutečných incidentů, jež mohou způsobit značné hmotné nebo nehmotné ztráty. Za tímto účelem má ohlašování významných kybernetických hrozeb klíčový význam.

(56) Základní a důležité subjekty jsou často v situaci, kdy je konkrétní incident vzhledem k jeho povaze třeba v důsledku oznamovacích povinností uvedených v různých právních nástrojích ohlásit různým orgánům. Takové případy vytvářejí další zátěž a mohou také vést k nejasnostem, pokud jde o formát a postupy takových oznámení. Vzhledem k tomu a za účelem zjednodušení hlášení bezpečnostních incidentů by členské státy [...] **mohly** stanovit *jednotné kontaktní místo* pro všechna hlášení vyžadovaná podle této směrnice i podle jiných právních předpisů Unie, jako je nařízení (EU) 2016/679 a směrnice 2002/58/ES. Agentura ENISA by ve spolupráci se skupinou pro spolupráci měla vypracovat společné šablony hlášení prostřednictvím pokynů, které by zjednodušily a zefektivnily informace uvedené v hlášeních, jež vyžaduje právo Unie, a snížily zátěž pro společnosti.

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

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

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

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

(61) S cílem zajistit dostupnost přesných a úplných údajů o registraci domén by registry internetových domén nejvyšší úrovně (TLD) a subjekty poskytující služby registrace registrace domén TLD (takzvaní registrátoři) měly shromažďovat údaje o registraci domén a zaručovat integritu a dostupnost těchto údajů. **Pokud jde o registrační údaje, měly by subjekty zejména ověřit jméno a e-mailovou adresu držitele registrace.** [...] Registry TLD a subjekty poskytující služby registrace domén TLD by zejména měly stanovit politiky a postupy pro shromažďování a uchovávání přesných a úplných registračních údajů a rovněž zamezit uvádění nesprávných registračních údajů a opravovat je v souladu s pravidly Unie o ochraně osobních údajů.

(62) Registry TLD a subjekty poskytující jim služby registrace domén by měly veřejně zpřístupnit údaje o registraci domén, které nespadají do oblasti působnosti pravidel Unie na ochranu osobních údajů, například údajů, které se týkají právnických osob[25]. Registry internetových domén nejvyšší úrovně a subjekty poskytující služby registrace domén nejvyšší úrovně by také měly v souladu s právem Unie na ochranu osobních údajů umožnit oprávněným žadatelům o přístup zákonný přístup ke konkrétním údajům o registraci domén týkajícím se fyzických osob. Členské státy by měly zajistit, aby registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén bez zbytečného odkladu reagovaly na žádosti [...] o zpřístupnění údajů o registraci domén od **oprávněných žadatelů o přístup, jako jsou příslušné orgány podle unijního nebo vnitrostátního práva v oblasti národní bezpečnosti a trestního soudnictví nebo týmy CSIRT.** Registry internetových domén nejvyšší úrovně a subjekty poskytující jim služby registrace domén by měly stanovit politiky a postupy pro zveřejňování a zpřístupnění registračních údajů, včetně dohod o úrovni služeb k vyřizování žádostí o přístup od oprávněných žadatelů o přístup. Postup poskytování přístupu může také obsahovat užívání rozhraní, portálu nebo jiného technického nástroje k zajištění účinného systému žádostí o registrační údaje a přístupu k těmto údajům. **Členské státy by měly zajistit, aby byl veškerý přístup k údajům (osobním i neosobním) o registraci domén bezplatný. Za** účelem podpory harmonizovaných postupů na vnitřním trhu může Komise přijmout pokyny o takových postupech, aniž jsou dotčeny pravomoci Evropského sboru pro ochranu osobních údajů**, a to v souladu s mezinárodními normami vypracovanými komunitou mnoha zúčastněných stran a jako jejich doplnění.**

---

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

(63) [...]**Z**ákladní a důležité subjekty podle této směrnice by měly podléhat pravomoci členského státu, ve kterém své služby poskytují. **Subjekty uvedené v bodech 1 až 7 a 10 přílohy I, poskytovatelé služeb vytvářejících důvěru a poskytovatelé výměnných uzlů internetu uvedení v bodě 8 přílohy I a v bodech 1 až 5 přílohy II této směrnice by měly podléhat pravomoci členského státu, v němž jsou usazeny.** Poskytuje-li subjekt služby **nebo je-li usazen** ve více než jednom členském státě, měl by podléhat samostatné a souběžné pravomoci každého z těchto členských států. Příslušné orgány těchto členských států by měly spolupracovat, poskytovat si navzájem pomoc a v případě potřeby provádět společné akce v oblasti dohledu. **Pokud se členské státy rozhodnou pravomoc vykonávat, měly by zamezit tomu, aby stejné jednání bylo za porušení povinností stanovených v této směrnici sankcionováno více než jednou.**

(64) S cílem zohlednit přeshraniční povahu služeb a činností poskytovatelů služeb systému doménových jmen (DNS), registrů internetových domén nejvyšší úrovně (TLD)**, subjektů poskytujících služby registrace domén pro TLD,** poskytovatelů sítí pro doručování obsahu, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center a poskytovatelů digitálních služeb by pravomoc nad těmito subjekty měl mít pouze jeden členský stát. Pravomoc by měl mít ten členský stát, v němž má daný subjekt v rámci Unie hlavní místo obchodní činnosti. Kritérium místa obchodní činnosti pro účely této směrnice předpokládá účinný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodujícím faktorem.

To, zda je toto kritérium splněno, by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou hlavního místa obchodní činnosti, a tudíž ani nejsou rozhodujícími kritérii pro jeho určení. Hlavní místo obchodní činnosti by mělo být místo v Unii, kde jsou **převážně** přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. To bude obvykle odpovídat místu, kde se nachází ústřední správa společnosti v Unii. Pokud **místo, kde jsou taková rozhodnutí převážně přijímána, nelze určit nebo** pokud taková rozhodnutí nejsou v Unii přijímána, mělo by se mít za to, že hlavní místo obchodní činnosti je v členském státě, ve kterém má subjekt provozovnu s nejvyšším počtem zaměstnanců v Unii. Pokud jsou služby prováděny skupinou podniků, mělo by se za hlavní místo obchodní činnosti skupiny podniků považovat hlavní místo obchodní činnosti řídícího podniku.

(64a) Pokud je rekurzivní služba DNS poskytována poskytovatelem veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací pouze jako součást služby přístupu k internetu, měl by být daný subjekt považován za subjekt spadající do pravomoci všech členských států, v nichž jsou jeho služby poskytovány.

(64aa) S cílem zajistit jasný přehled poskytovatelů služeb DNS, registrů TLD, subjektů poskytujících služby registrace domén pro TLD, poskytovatelů sítí pro doručování obsahu, poskytovatelů služeb cloud computingu, poskytovatelů služeb datových center a digitálních poskytovatelů poskytujících služby v celé Unii v rámci oblasti působnosti této směrnice by agentura ENISA měla na základě oznámení obdržených členskými státy, případně prostřednictvím jejich vnitrostátních mechanismů pro vlastní oznámení, vytvořit a spravovat registr pro tyto subjekty. V zájmu zajištění přesnosti a úplnosti informací, které by měly být do tohoto registru zahrnuty, by členské státy měly agentuře ENISA předložit informace o těchto subjektech, jež mají ve svých vnitrostátních registrech k dispozici. Agentura ENISA a členské státy by měly přijmout opatření s cílem usnadnit interoperabilitu těchto registrů a současně zajistit ochranu důvěrných nebo utajovaných informací.

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

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

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

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

(69) [...] **V** rozsahu nezbytně nutném a přiměřeném pro účely zajištění bezpečnosti sítí a informací by **zpracování osobních údajů** ze strany **základních a důležitých** subjektů [...] a poskytovatelů bezpečnostních technologií a služeb **mohlo být považováno za nezbytné pro splnění právní povinnosti nebo** [...] by mohlo představovat oprávněný zájem dotčeného správce údajů**[...]** podle nařízení (EU) 2016/679. To by **mohlo** [...] zahrnovat opatření týkající se prevence, odhalování a analýzy incidentů a reakce na incidenty, opatření ke zvyšování povědomí o konkrétních kybernetických hrozbách, výměnu informací v rámci odstraňování a koordinovaného odhalování zranitelných míst a také dobrovolnou výměnu informací o těchto incidentech, kybernetických hrozbách a zranitelných místech, indikátorech narušení, taktice, technikách a postupech, varováních v oblasti kybernetické bezpečnosti a konfiguračních nástrojích. Taková opatření mohou vyžadovat zpracovávání [...] **různých** druhů osobních údajů **jako například**: IP adres, jednotných adres zdroje (URL), doménových jmen a e-mailových adres. **Zpracování osobních údajů příslušnými orgány, jednotnými kontaktními místy pro kybernetickou bezpečnost a týmy CSIRT by mělo být stanoveno ve vnitrostátním právu a považováno za nezbytné pro splnění právní povinnosti nebo pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce údajů, jak je uvedeno v čl. 6 odst. 1 písm. c) nebo e) nařízení (EU) 2016/679.**

(69a) V právních předpisech členských států mohou být v rozsahu nezbytně nutném a přiměřeném pro účely zajištění bezpečnosti sítí a informačních systémů základních a důležitých subjektů stanovena pravidla, která příslušným orgánům, jednotným kontaktním místům pro kybernetickou bezpečnost a týmům CSIRT umožňují zpracovávat zvláštní kategorie osobních údajů v souladu s článkem 9 [...] nařízení (EU) 2016/679, zejména stanovením vhodných a specifických opatření na ochranu základních práv a zájmů fyzických osob, včetně technických omezení opakovaného používání těchto údajů a používání nejmodernějších bezpečnostních opatření a opatření na ochranu soukromí, jako je pseudonymizace, nebo šifrování, pokud anonymizace může významně ovlivnit sledovaný účel.

(70) S cílem posílit pravomoci a činnosti dohledu, které pomáhají zajistit účinný soulad s předpisy, by tato směrnice měla stanovit minimální seznam opatření a prostředků dohledu, jejichž prostřednictvím mohou příslušné orgány uskutečňovat dohled nad základními a důležitými subjekty. Tato směrnice by kromě toho měla zavést rozlišení režimů dohledu mezi základními a důležitými subjekty s cílem zajistit spravedlivou rovnováhu povinností pro oba druhy subjektů a příslušné orgány. Základní subjekty by tak měly podléhat plnohodnotnému režimu dohledu (dohled *ex ante* a *ex post*), zatímco důležité subjekty by měly podléhat mírnému režimu dohledu, pouze dohledu *ex post*. Mírný režim znamená, že důležité subjekty by neměly **mít povinnost** [...] systematicky **dokumentovat** dodržování požadavků na řízení kybernetických bezpečnostních rizik a příslušné orgány by měly provádět reaktivní *ex post* přístup k dohledu, a neměly by tedy obecnou povinnost dohlížet na tyto subjekty. U **důležitých subjektů může být dohled *ex post* zahájen na základě důkazů nebo jakýchkoliv indicií či informací, které byly příslušným orgánům oznámeny a které podle názoru těchto orgánů naznačují možné nesplnění povinností stanovených v této směrnici. Mohlo by se například jednat o takový druh důkazů, indicií nebo informací, jaký příslušným orgánům poskytují jiné orgány, subjekty, občané, sdělovací prostředky nebo jiné zdroje, nebo by se mohlo jednat o veřejně dostupné informace či o důkazy, indicie nebo informace, které mohou vyplynout z jiných činností prováděných příslušnými orgány při plnění jejich úkolů.**

(70a) Pokud jde o výkon dohledu *ex ante*, příslušné orgány by měly mít možnost rozhodnout o stanovení priorit, pokud jde o přiměřené využití opatření a prostředků dohledu, jež mají k dispozici. To znamená, že příslušné orgány mohou o tomto stanovení priorit rozhodnout na základě metodik dohledu, které by se měly řídit přístupem založeným na posouzení rizik. Konkrétně by tyto metodiky mohly zahrnovat kritéria nebo referenční hodnoty pro zařazení základních subjektů do kategorií podle rizika a odpovídající opatření a prostředky dohledu doporučené pro jednotlivé kategorie podle rizika, jako je využití, četnost nebo druh kontrol na místě nebo cílených bezpečnostních auditů či bezpečnostních prověrek, druh informací, jež mají být vyžadovány, a míra podrobnosti těchto informací. Tyto metodiky dohledu mohou být rovněž doplněny o pracovní programy a mohou být pravidelně posuzovány a přezkoumávány, a to i pokud jde o aspekty, jako je přidělování zdrojů a potřeby v této oblasti.

(70aa) Pokud jde o subjekty veřejné správy, měly by být pravomoci dohledu vykonávány v souladu s vnitrostátními rámci a právním řádem. Členské státy by měly mít možnost rozhodnout ve vztahu k těmto subjektům o uložení vhodných, přiměřených a účinných opatření v oblasti dohledu a vymáhání.

(70aaa) Za účelem prokázání souladu s určitými opatřeními k řízení kybernetických bezpečnostních rizik by členské státy mohly vyžadovat, aby základní a důležité subjekty využívaly kvalifikované služby vytvářející důvěru nebo oznámené systémy elektronické identifikace podle nařízení (EU) č. 910/2014.

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

(71a) Ustanovení týkající se odpovědnosti fyzických osob, jež v rámci subjektu nesou určitou odpovědnost za porušení jeho povinnosti zajistit dodržování povinností stanovených v této směrnici, nevyžadují, aby členské státy zajistily trestní stíhání nebo občanskoprávní odpovědnost za škody, jež byly tímto porušením povinností způsobeny třetím stranám.

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

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

(74) Členské státy [...] **mohou** stanovit pravidla týkající se trestních sankcí za porušení vnitrostátních pravidel provádějících tuto směrnici. Uložení trestních sankcí za porušení těchto vnitrostátních pravidel a souvisejících správních sankcí by však nemělo vést k porušení zásady *ne bis in idem*, jak ji vykládá Soudní dvůr.

(75) Nejsou-li správní sankce harmonizovány touto směrnicí nebo v případě potřeby v jiných případech, jako jsou závažná porušení povinností stanovených v této směrnici, měly by členské státy zavést systém, který zajistí uložení účinných, přiměřených a odrazujících sankcí. Povaha těchto trestních nebo správních sankcí by měla být stanovena právem členského státu.

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

(76a) V zájmu zajištění účinného dohledu a vymáhání, zejména v případech s přeshraničním rozměrem, by členské státy, které obdržely žádost o vzájemnou pomoc, měly v rozsahu dané žádosti přijmout ve vztahu k dotčenému subjektu, který na jejich území poskytuje služby nebo jehož síť a informační systém se na jejich území nachází, vhodná opatření v oblasti dohledu a vymáhání.

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

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

(79) Měl by být zaveden **systém** [...] vzájemného [...] **učení**, který **pomůže posílit vzájemnou** důvěru a **čerpat poznatky z osvědčených postupů a zkušeností** a současně umožní [...] **vzájemné výměny** mezi odborníky určenými členskými státy **týkající se** [...] provádění politik kybernetické bezpečnosti[...]. **Při zavádění systému vzájemného učení by měla být věnována zvláštní pozornost tomu, aby se zajistilo, že tento systém nebude pro relevantní orgány členských států představovat zbytečnou nebo nepřiměřenou zátěž. Komise by měla prozkoumat všechny možnosti, jak případně zaručit finanční krytí nákladů, které mohou z pořádání misí vzájemného učení vyplynout. Kromě toho by měl systém vzájemného učení zohledňovat výsledky obdobných mechanismů, jako je systém vzájemného hodnocení sítě CSIRT, vytvářet přidanou hodnotu a zamezit duplikaci činností. Zavedením systému vzájemného učení by neměly být dotčeny vnitrostátní ani unijní právní předpisy o ochraně důvěrných a utajovaných informací. Před zahájením jednotlivých kol vzájemného učení mohou členské státy provést sebehodnocení relevantních aspektů. Na žádost skupiny pro spolupráci může agentura ENISA v případě potřeby poskytnout pokyny týkající se sebehodnocení a relevantních šablon. Členské státy by se mohly rozhodnout, že své příslušné zprávy zveřejní.**

(80) [...]

(81) Za účelem zajištění jednotných podmínek k provedení příslušných ustanovení této směrnice týkajících se procesních opatření nezbytných pro fungování skupiny pro spolupráci, technických prvků opatření k řízení rizik nebo druhu informací, formátu a postupu oznamování incidentů**, kategorií subjektů, od nichž má být vyžadováno používání určitých certifikovaných produktů, služeb a procesů v oblasti IKT,** by Komisi měly být svěřeny prováděcí pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011.[26]

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

[26] 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).

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

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

PŘIJALY TUTO SMĚRNICI:

KAPITOLA I

Obecná ustanovení

Článek 1

Předmět

1. Touto směrnicí se stanoví opatření pro zajištění vysoké společné úrovně kybernetické bezpečnosti v rámci Unie s **cílem zlepšení fungování vnitřního trhu**.

2. Za tímto účelem tato směrnice:

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

   b) stanoví povinnost řízení rizik v oblasti kybernetické bezpečnosti a oznamovací povinnost pro subjekty druhu uvedeného [...] v příloze **I a II** [...];

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

Článek 2

Oblast působnosti

1. Tato směrnice se vztahuje na veřejné a soukromé subjekty druhů **uvedených** [...] v [...] příloh**ách I a II** [...], **které dosahují nebo přesahují stropové hodnoty pro střední podniky** [...] ve smyslu doporučení Komise 2003/361/ES[27]. **Pro účely této směrnice se nepoužije čl. 3 odst. 4 a čl. 6 odst. 2 druhý a třetí pododstavec přílohy uvedeného doporučení.**

2. [...]**B**ez ohledu na [...] velikost **subjektů uvedených v odstavci 1** se tato směrnice rovněž použije, **pokud:** [...]

   a) jsou služby poskytovány jedním z těchto subjektů:

      i) poskytovateli veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací uvedených v bodě 8 přílohy I;

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

      iii) nekvalifikovanými poskytovateli služeb vytvářejících důvěru uvedenými v bodě XX přílohy I;

      iv) registry domén nejvyšší úrovně [...] uvedenými v bodě 8 přílohy I;

   b) [...]

[27] 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).

c) je subjekt v **určitém členském státě** výhradním dodavatelem služeb [...]**, jež mají zásadní význam pro zachování kriticky důležitých společenských nebo hospodářských činností**;

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

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

f) [...];

g) je subjekt označen za kritický podle směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX[28] [směrnice o odolnosti kritických subjektů] **[**nebo za subjekt rovnocenný kritickému subjektu podle článku 7 uvedené směrnice**]**.

2a. **Bez ohledu na velikost se tato směrnice vztahuje rovněž na subjekty veřejné správy ústředních vlád uznané jako takové v členském státě v souladu s vnitrostátními právními předpisy a uvedené v bodě 9 přílohy I. Členské státy mohou stanovit, že se tato směrnice vztahuje rovněž na subjekty veřejné správy na regionální a místní úrovni.**

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

3. [...]

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

3a. (1) Tato směrnice se nevztahuje na:

a) subjekty, na něž se nevztahují právní předpisy Unie, a v každém případě všechny subjekty, které vykonávají činnosti především v oblasti obrany, národní bezpečnosti, veřejné bezpečnosti nebo vymáhání práva bez ohledu na to, který subjekt tyto činnosti vykonává a zda se jedná o veřejný nebo soukromý subjekt, aniž je dotčen odstavec 2;

b) subjekty, které vykonávají činnosti v oblasti justice, parlamenty nebo centrální banky.[...]

(2) Představují-li činnosti subjektů veřejné správy v uvedených oblastech pouze část jejich celkových činností, jsou z oblasti působnosti této směrnice vyloučeny zcela.

3aa. Tato směrnice se nevztahuje na:

i) činnosti subjektů, na něž se nevztahují právní předpisy Unie, a v každém případě všechny činnosti týkající se národní bezpečnosti nebo obrany, bez ohledu na to, který subjekt tyto činnosti vykonává a zda se jedná o veřejný nebo soukromý subjekt;

ii) činnosti subjektů v oblasti justice, parlamentů, centrálních bank a v oblasti veřejné bezpečnosti, včetně subjektů veřejné správy vykonávajících činnosti v oblasti vymáhání práva za účelem prevence, vyšetřování, odhalování nebo stíhání trestných činů nebo výkonu trestních sankcí.

3aaa. Povinnosti stanovené touto směrnicí nezahrnují poskytování informací, jejichž zpřístupnění je v rozporu se zásadními zájmy členských států v oblasti národní bezpečnosti, veřejné bezpečnosti nebo obrany.

3aaaa. Touto směrnicí nejsou dotčeny: právní předpisy Unie v oblasti ochrany osobních údajů, zejména nařízení (EU) 2016/679 a směrnice 2002/58/ES.

3b. Tato směrnice se nepoužije na subjekty, na něž se nevztahuje nařízení Evropského parlamentu a Rady (EU) XXXX/XXXX [nařízení o digitální provozní odolnosti] v souladu s jeho čl. 2 odst. 4.

4. Touto směrnicí nejsou dotčeny [...][29] směrnice Evropského parlamentu a Rady 2011/93/EU[30] a 2013/40/EU[31].

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

---

29 [...]

30 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).

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

Článek 2a

Základní a důležité subjekty

1. Ze subjektů, na něž se vztahuje tato směrnice, se za základní subjekty považují tyto:

i) subjekty druhu uvedeného v příloze I bodech 1 až 8a a 10 této směrnice, které přesahují stropové hodnoty pro střední podniky ve smyslu doporučení Komise 2003/361/ES;

ii) střední podniky uvedené v čl. 2 odst. 2 písm. a) bodě i);

iii) subjekty uvedené v čl. 2 odst. 2 písm. a) bodech ii) a iv) této směrnice, bez ohledu na velikost;

iv) subjekty uvedené v čl. 2 odst. 2 písm. g) a v čl. 2 odst. 2a této směrnice, bez ohledu na velikost;

v) jsou-li zřizovány členskými státy, subjekty, které členské státy před vstupem této směrnice v platnost označily za provozovatele základních služeb v souladu se směrnicí (EU) 2016/1148 nebo vnitrostátními právními předpisy;

vi) subjekty, které přesahují stropové hodnoty pro střední podniky ve smyslu doporučení Komise 2003/361/ES, druhu uvedeného v příloze II, jež členské státy na základě kritérií uvedených v čl. 2 odst. 2 písm. c) až e) označí za zásadní;

vii) střední podniky ve smyslu doporučení Komise 2003/361/ES, jež členské státy na základě kritérií uvedených v čl. 2 odst. 2 písm. c) až e) označí za zásadní;

viii) mikrosubjekty nebo malé subjekty smyslu doporučení Komise 2003/361/ES uvedené v odst. 2 písm. a) bodě i) nebo identifikované podle odst. 2 písm. c) až e) tohoto článku, jež členské státy označí za zásadní na základě vnitrostátního posouzení rizika.

2. Ze subjektů, na něž se vztahuje tato směrnice, se za důležité subjekty považují tyto:

i) subjekty druhu uvedeného v příloze I této směrnice, které se kvalifikují jako střední podniky ve smyslu doporučení Komise 2003/361/ES, a subjekty druhu uvedeného v příloze II, které dosahují nebo přesahují stropové hodnoty pro střední podniky ve smyslu doporučení Komise 2003/361/ES[32];

ii) subjekty uvedené v čl. 2 odst. 2 bodě iii) této směrnice, bez ohledu na velikost;

iii) malé subjekty a mikrosubjekty uvedené v čl. 2 odst. 2 písm. a) bodě i);

iv) malé subjekty a mikrosubjekty, které členské státy na základě čl. 2 odst. 2 písm. c) až e) označí za důležité subjekty.

---

[32] **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).**

Článek 2a

Oznamovací mechanismus

1. **Členské státy mohou zřídit vnitrostátní mechanismus pro oznamování ze strany samotných subjektů, v jehož rámci se ode všech subjektů, na něž se vztahuje tato směrnice, bude vyžadovat, aby příslušným orgánům podle této směrnice nebo subjektům určeným pro tento účel členskými státy oznámily alespoň svůj název, adresu, kontaktní údaje, odvětví, v němž působí nebo druh služeb, které poskytují, a případně seznam členských států, v nichž poskytují služby, na něž se vztahuje tato směrnice.**

2. Členské státy [...] předloží Komisi **ve vztahu k subjektům, které identifikovaly podle čl. 2 odst. 2 písm. b) až e), do [12 měsíců od data provedení této směrnice] alespoň relevantní informace o počtu identifikovaných subjektů, odvětví, do něhož patří nebo druhu služby, kterou poskytují podle příloh, a specifická ustanovení čl. 2 odst. 2, na jejichž základě byly identifikovány.** Členské státy [...] **tyto informace**[...] pravidelně přezkoumávají, a to alespoň každé dva roky od předložení, a v případě potřeby jej aktualizují.

Článek 2b

Právní akty Unie specifické pro jednotlivá odvětví

1. Pokud [...] ustanovení **právních aktů Unie** specifických pro jednotlivá odvětví [...] vyžadují, aby základní nebo důležité subjekty [...] přijaly opatření k řízení rizik v oblasti kybernetické bezpečnosti nebo aby oznamovaly **významné** incidenty či [...] kybernetické hrozby, a pokud je účinek těchto opatření alespoň rovnocenný účinku povinností stanovených v této směrnici, příslušná ustanovení této směrnice, **včetně ustanovení o dohledu a vymáhání v kapitole VI,** se na **uvedené subjekty** neuplatní. **Pokud se právní akty Unie specifické pro jednotlivá odvětví nevztahují na všechny subjekty v konkrétním odvětví, jež náleží do oblasti působnosti této směrnice, na subjekty, na něž se uvedená ustanovení specifická pro jednotlivá odvětví nevztahují, se nadále použijí příslušná ustanovení této směrnice.**

2. Požadavky uvedené v odstavci 1 tohoto článku se považují za rovnocenné povinnostem stanoveným v této směrnici, pokud příslušný akt Unie pro jednotlivé odvětví uděluje příslušným orgánům podle této směrnice nebo určeným týmům CSIRT okamžitý, případně automatický a přímý přístup k oznámením incidentů, a pokud:

a) opatření k řízení kybernetických bezpečnostních rizik jsou fakticky přinejmenším rovnocenná opatřením stanoveným v čl. 18 odst. 1 a 2 této směrnice; nebo

b) požadavky na oznamování významných incidentů jsou fakticky přinejmenším rovnocenné opatřením stanoveným v čl. 20 odst. 1 až 6.

3. Komise pravidelně přezkoumává uplatňování požadavků s rovnocenným účinkem stanovených v odstavcích 1 a 2 tohoto článku ve vztahu k ustanovením právních aktů Unie specifickým pro jednotlivá odvětví. Komise při přípravě těchto pravidelných přezkumů konzultuje skupinu pro spolupráci a agenturu ENISA.

Článek 3

Minimální harmonizace

Aniž jsou dotčeny jejich jiné povinnosti podle právních předpisů Unie, smějí členské státy[...] přijmout nebo zachovat ustanovení zajišťující v **oblastech, na něž se vztahuje tato směrnice,** vyšší úroveň kybernetické bezpečnosti.

Článek 4

Definice

Pro účely této směrnice se rozumí:

1) „sítí a informačním systémem“:

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

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

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

2) „bezpečností sítí a informačních systémů“ schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým **událostem**, které **mohou** narušit**[...]** dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné;

2a) „službami elektronických komunikací“ služby elektronických[...] komunikací ve smyslu čl. 2 bodu 4 směrnice (EU) 2018/1972;

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

4) „národní strategií **kybernetické bezpečnosti**“ [...] soudržný rámec určitého členského státu, jímž se řídí dosažení strategických cílů a priorit v **oblasti** [...] **kybernetické bezpečnosti** [...] v uvedeném členském státě;

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

5a) „rozsáhlým kybernetickým bezpečnostním incidentem“ incident s významným dopadem na nejméně dva členské státy nebo incident, jehož narušení přesahuje schopnost určitého členského státu na něj reagovat.

---

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

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

6a) „rizikem“ možnost ztráty nebo narušení v důsledku incidentu, přičemž toto riziko je vyjádřeno jako kombinace rozsahu takové ztráty nebo takového narušení a pravděpodobnosti vzniku uvedeného incidentu;

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

7a) **„významnou kybernetickou hrozbou“ kybernetická hrozba, u níž lze na základě jejích technických vlastností předpokládat, že má potenciál vážně ovlivnit síť a informační systémy určitého subjektu nebo jeho uživatelů tím, že způsobí značné hmotné nebo nehmotné ztráty;**

8) „zranitelností“ slabá stránka, snížená odolnost nebo chyba prostředku IKT nebo systému [...], která může být využita kybernetickou hrozbou;

8a) „případy, kdy téměř došlo k incidentu“ událost, která mohla potenciálně poškodit síť a informační systémy určitého subjektu nebo jeho uživatelů, bylo však úspěšně zabráněno tomu, aby k tomu došlo;

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

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

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

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

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

14) „poskytovatelem služeb systému doménových jmen (DNS)“ subjekt, který poskytuje rekurzivní nebo autoritativní služby pro překlad doménových jmen **pro** [...] **použití třetími stranami, s výjimkou kořenových jmenných serverů** [...];

---

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

15) „registrem domén nejvyšší úrovně“ subjekt, kterému byla delegována konkrétní TLD a je odpovědný za správu TLD, včetně registrace doménových jmen v rámci TLD a technického provozu TLD, včetně provozu jejích jmenných serverů, vedení jejích databází a distribuce souborů zón TLD mezi jmennými servery, **přičemž jsou vyloučeny situace, kdy registr využívá doménová jména nejvyšší úrovně pouze pro vlastní potřebu**;

15a) „subjekty poskytujícími služby registrace domén pro TLD“ registry názvů TLD, registrátoři TLD a zástupci registrátorů, jako jsou prodejci a poskytovatelé proxy služeb;

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

16a) „službami vytvářejícími důvěru“ služby vytvářející důvěru ve smyslu čl. 3 bodu 16 nařízení (EU) č. 910/2014;

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

16b) „kvalifikovaným poskytovatelem služeb vytvářejících důvěru“ kvalifikovaný poskytovatel služeb vytvářejících důvěru ve smyslu čl. 3 bodu 20 nařízení (EU) č. 910/2014;

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

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

19) „službou cloud computingu“ digitální služba umožňující správu na vyžádání a široký dálkový přístup k rozšiřitelnému a přizpůsobitelnému úložišti [...] výpočetních zdrojů, které je možno sdílet, **včetně těch, které mají několik různých umístění**;

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

---

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

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

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

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

23) „subjektem veřejné správy“ subjekt **takto uznaný v souladu s vnitrostátními právními předpisy v určitém členském státě,** [...] který splňuje tato kritéria:

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

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

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

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

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

25) „základním subjektem“ jakýkoli subjekt druhu [...] **stanoveného v příloze I a označený jako „základní“ v souladu s čl. 2a odst. 1**;

26) „důležitým subjektem“ jakýkoli subjekt druhu [...] **stanoveného v přílohách I a II a označený jako „důležitý“ v souladu s čl. 2a odst. 2**;

26a) „produktem IKT“ produkt IKT ve smyslu čl. 2 bodu 12 nařízení (EU) 2019/881;

(26aa) „službou IKT“ služba IKT ve smyslu čl. 2 bodu 13 nařízení (EU) 2019/881;

26ab) „procesem IKT“ proces IKT ve smyslu čl. 2 bodu 14 nařízení (EU) 2019/881;

26ac) „poskytovatelem spravovaných služeb“ jakýkoli subjekt, který poskytuje služby, jako je síť, aplikace, infrastruktura a bezpečnost, prostřednictvím průběžného a pravidelného řízení, podpory a aktivní správy v prostorách zákazníků, v jejich datovém centru poskytovatele spravovaných služeb (hosting) nebo v datovém centru třetí strany;

26ad) „poskytovatelem spravovaných bezpečnostních služeb“ jakýkoli subjekt, který externě zajišťuje monitorování a správu bezpečnostních zařízení a systémů. Mezi společné služby patří spravovaný firewall, odhalování vniknutí, virtuální soukromá síť, skenování zranitelnosti a antivirové služby.

Rovněž zahrnují využívání vysoce dostupných bezpečnostních operačních středisek (buď z vlastních zařízení, nebo od jiných poskytovatelů datových center) k poskytování služeb 24 hodin denně 7 dní v týdnu, jež jsou navržena tak, aby bylo možné snížit počet pracovníků v oblasti provozní bezpečnosti, které si určitý podnik potřebuje najmout, vyškolit a ponechat, aby si udržel přijatelnou bezpečnostní situaci.

KAPITOLA II

Koordinované regulační rámce kybernetické bezpečnosti

Článek 5

Národní strategie kybernetické bezpečnosti

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

   a) [...] cíle a priority strategie kybernetické bezpečnosti členských států;

   b) správní rámec pro naplnění těchto cílů a priorit, včetně politik uvedených v odstavci 2 a úloh a povinností různých orgánů a subjektů zapojených do provádění strategie [...];

   c) [...] **pokyny** k určení relevantních zařízení a **vyhodnocení** kybernetických rizik v tomto členském státě [...]

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

   e) [...]

f) politický rámec pro lepší koordinaci mezi příslušnými orgány podle této směrnice a směrnice Evropského parlamentu a Rady (EU) XXXX/XXXX[38] [směrnice o odolnosti kritických subjektů] pro účely sdílení informací o **kybernetických bezpečnostních rizicích,** [...] kybernetických hrozbách a **incidentech, stejně jako o nekybernetických rizicích, hrozbách a incidentech** a **případně** pro výkon úkolů v oblasti dohledu;

fa) politický rámec pro koordinaci a spolupráci mezi příslušnými orgány podle této směrnice a příslušnými orgány určenými podle odvětvových právních předpisů.

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

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

b) **politiku** [...] týkající se zařazení a specifikace požadavků na kybernetickou bezpečnost produktů a služeb IKT při zadávání veřejných zakázek**, včetně certifikace kybernetické bezpečnosti**;

c) politiku **pro řízení zranitelností, zahrnující prosazování a usnadňování** [...] **dobrovolného** koordinovaného zveřejňování informací o zranitelnostech ve smyslu čl. 6 **odst. 1**;

d) politiku týkající se udržení celkové dostupnosti, [...] integrity a **důvěrnosti** veřejného jádra otevřeného internetu;

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

---

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

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

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

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

3. Členské státy oznámí své národní strategie kybernetické bezpečnosti Komisi do tří měsíců od jejich přijetí. Členské státy **při tom** mohou z oznámení vyloučit **prvky strategie, které souvisejí s** [...] národní bezpečností.

4. Členské státy posuzují své národní strategie kybernetické bezpečnosti pravidelně a alespoň každých [...] **pět** let podle klíčových ukazatelů výkonnosti a v případě potřeby je změní. Při zpracování národní strategie a klíčových ukazatelů výkonnosti pro posouzení strategie poskytuje členským státům na **jejich** žádost součinnost Agentura Evropské unie pro kybernetickou bezpečnost (ENISA).

Článek 6

Koordinované zveřejňování informací o zranitelnostech a Evropský registr zranitelností

1. Každý členský stát určí jeden ze svých týmů CSIRT podle článku 9 jako koordinátora za účelem koordinovaného zveřejňování informací o zranitelnostech. Tento určený tým CSIRT vystupuje jako důvěryhodný zprostředkovatel, který v případě potřeby usnadňuje interakci mezi oznamujícím subjektem**, vlastníkem potenciální zranitelnosti** a výrobcem nebo poskytovatelem produktů nebo služeb IKT. **Určenému týmu CSIRT může oznámit zranitelnost ve smyslu čl. 4 bodu 8) kterákoli fyzická nebo právnická osoba, a to případně anonymně. Určený tým CSIRT zajistí důsledná opatření v návaznosti na oznámení a utajení totožnosti osoby, která zranitelnost oznamuje.** Pokud **by** oznámená zranitelnost [...] **mohla potenciálně mít významný vliv na subjekty ve více než jednom členském státě**, spolupracuje určený tým CSIRT z každého členského státu **v případě potřeby** s **ostatními určenými týmy CSIRT** v rámci sítě CSIRT.

2. Agentura ENISA v **konzultaci se skupinou pro spolupráci** vytvoří a spravuje Evropský registr zranitelností. Za tímto účelem ENISA zřídí a spravuje informační systémy, politiky a postupy s cílem zejména umožnit důležitým a základním subjektům a jejich dodavatelům sítí a informačních systémů **dobrovolně** zveřejňovat a registrovat **veřejně známé** zranitelnosti v produktech nebo službách IKT a poskytovat přístup k informacím o těchto zranitelnostech uvedeným v registru všem zúčastněným stranám. V registru jsou zejména uvedeny informace popisující zranitelnost, dotčený produkt IKT nebo služby IKT a závažnost této zranitelnosti z hlediska okolností, za nichž může být využita, dostupnost příslušných oprav, a pokud opravy nejsou dostupné, pokyny pro uživatele zranitelných produktů a služeb, jak mohou být rizika vyplývající z odhalených slabých míst zmírněna**, vydané příslušnými vnitrostátními orgány nebo týmy CSIRT**. **Agentura ENISA zajistí, aby Evropský registr zranitelností využíval bezpečnou a odolnou komunikační a informační infrastrukturu.**

Článek 7

Národní rámce krizového řízení kybernetické bezpečnosti

1. Každý členský stát určí jeden nebo více příslušných orgánů odpovědných za řešení rozsáhlých **kybernetických bezpečnostních** incidentů a krizí. Členské státy zajistí, aby příslušné orgány disponovaly odpovídajícími zdroji pro účinné a efektivní plnění svěřených úkolů. **Členské státy zajistí soudržnost se stávajícími rámci pro obecné krizové řízení.**

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

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

   a) cíle vnitrostátních opatření a činností v oblasti připravenosti;

   b) úkoly a odpovědnost příslušných vnitrostátních orgánů;

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

   d) opatření v oblasti připravenosti včetně pravidelného nácviku a školení;

   e) příslušné veřejné a soukromé [...] strany a zapojená infrastruktura;

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

4. Členské státy [...] **uvědomí** Komisi o určení svých příslušných orgánů podle odstavce 1 a předloží **příslušné informace týkající se požadavků podle odstavce 3 tohoto článku ohledně** svých národních plánů reakce na kybernetické bezpečnostní incidenty a krize [...] do tří měsíců od tohoto určení a přijetí těchto plánů. Členské státy mohou [...] vyloučit konkrétní informace, pokud je to [...] nezbytné pro jejich národní bezpečnost**, veřejnou bezpečnost nebo obranu**.

Článek 8

Vnitrostátní příslušné orgány a jednotná kontaktní místa

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

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

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

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

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

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

Článek 9

Bezpečnostní týmy typu CSIRT

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

2. Členské státy zajistí, aby měl každý tým CSIRT odpovídající zdroje pro účinné plnění svých úkolů podle čl. 10 odst. 2. **Týmy CSIRT mohou při plnění těchto úkolů přednostně poskytovat konkrétní služby subjektům, které se řídí přístupem založeným na posouzení rizik.**

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

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

5. Týmy CSIRT se účastní vzájemného [...] **učení** pořádaného v souladu s článkem 16.

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

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

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

Článek 10

Požadavky na týmy CSIRT a jejich úkoly

1. Týmy CSIRT musí splňovat tyto požadavky:

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

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

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

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

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

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

2. Týmy CSIRT mají tyto úkoly:

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

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

c) reakce na incidenty;

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

e) provádění aktivního skenování sítě a informačních systémů [...] [...] za **účelem odhalení zranitelností s potenciálním významným dopadem, a to za předpokladu, že pokud nedal tento subjekt souhlas, nedojde k zásahu do sítě a informačních systémů ani k negativnímu dopadu na jejich fungování**;

f) účast v síti CSIRT a poskytování vzájemné pomoci dalším členům sítě na jejich žádost**, a to v souladu s jejich funkcemi a pravomocemi**;

fa) v případě potřeby působení jako koordinátor za účelem procesu koordinovaného zveřejňování informací o zranitelnostech podle čl. 6 odst. 1, což zahrnuje zejména usnadňování interakce mezi oznamujícími subjekty, vlastníkem potenciální zranitelnosti a výrobcem nebo poskytovatelem produktů IKT nebo služeb IKT v případech, kdy je to nutné, určení a kontaktování dotčených subjektů, podporu oznamujících subjektů, dojednávání harmonogramů zveřejnění a řízení zranitelností, které se dotýkají více organizací (zveřejňování zranitelností ohrožujících více stran).

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

3a. Týmy CSIRT mohou navázat spolupráci s vnitrostátními týmy CSIRT třetích zemí. V rámci této spolupráce si v souladu s právními předpisy Unie o ochraně údajů mohou vyměňovat příslušné informace, včetně osobních údajů.

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

a) postupů řešení incidentů;

b) krizového řízení kybernetické bezpečnosti;

c) koordinovaného zveřejňování informací o zranitelnostech.

Článek 11

Spolupráce na vnitrostátní úrovni

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

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

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

4. V rozsahu nezbytném pro účelné plnění úkolů a povinností stanovených touto směrnicí zajistí členské státy vhodnou spolupráci mezi příslušnými orgány**, týmy CSIRT,** jednotnými kontaktními místy a donucovacími orgány, úřady pro ochranu osobních údajů a příslušnými orgány **určenými** [...] podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]**, příslušnými orgány podle prováděcího nařízení Komise 2019/1583, vnitrostátními regulačními orgány určenými v souladu se směrnicí (EU) 2018/1972, vnitrostátními orgány určenými podle článku 17 nařízení (EU) č. 910/2014,** [...] vnitrostátními finančními orgány určenými v souladu s nařízením Evropského parlamentu a Rady (EU) XXXX/XXXX [nařízení DORA] a **příslušnými orgány určenými v jiných odvětvových právních aktech Unie** v daném členském státě.

5. Členské státy zajistí, aby si jejich příslušné orgány **podle této směrnice a příslušné orgány určené podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]** pravidelně **vyměňovaly** [...] informace [...] o **určení kritických subjektů,** kybernetických bezpečnostních rizicích, kybernetických hrozbách a incidentech**, stejně jako o nekybernetických rizicích, hrozbách a incidentech** postihujících základní subjekty určené jako kritické **[**nebo jako subjekty rovnocenné kritickým subjektům**]** podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů], jakož i o opatřeních [...] přijatých v reakci na tato rizika a incidenty. **Členské státy rovněž zajistí, aby si příslušné informace pravidelně vyměňovaly příslušné orgány podle této směrnice** [...] a **příslušné orgány určené podle nařízení XXXX/XXXX [nařízení DORA], směrnice 2018/1972 a nařízení (EU) č. 910/2014.**

Pokud jde o poskytovatele služeb vytvářejících důvěru a [...] zejména [...] v případech, kdy je dohled podle této směrnice svěřen jinému orgánu než dohledovým orgánům určeným podle nařízení (EU) č. 910/2014, tyto orgány úzce a včas spolupracují formou výměny příslušných informací s cílem zajistit účinný dohled nad poskytovateli služeb vytvářejících důvěru a jejich dodržování požadavků stanovených v této směrnici a nařízení [XXXX/XXXX]**, a tam, kde je to vhodné, příslušný vnitrostátní orgán podle této směrnice neprodleně uvědomí orgán dohledu podle nařízení eIDAS o veškerých oznámených významných kybernetických hrozbách nebo incidentech s dopadem na služby vytvářející důvěru**.

5a. [...] Za účelem zjednodušení hlášení bezpečnostních incidentů členské státy mohou stanovit jednotné vstupní místo pro všechna oznámení vyžadovaná podle této směrnice a případně podle nařízení (EU) 2016/679 a směrnice 2002/58/ES. Členské státy mohou jednotné vstupní místo využívat pro oznámení vyžadovaná v jiných odvětvových právních aktech Unie. Tímto jednotným vstupním místem není dotčeno uplatňování ustanovení nařízení (EU) 2016/679 a směrnice 2002/58/ES, zejména ustanovení týkajících se nezávislých dozorových úřadů.

KAPITOLA III

*Spolupráce v **rámci EU***

Článek 12

Skupina pro spolupráci

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

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

3. Skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA. Činností skupiny pro spolupráci se jako pozorovatel účastní Evropská služba pro vnější činnost. Činností skupiny pro spolupráci se mohou v **souladu s čl. 42 odst. 1 nařízení (EU) XXXX/XXXX [nařízení DORA]** účastnit evropské orgány dohledu [...] a **příslušné orgány určené podle nařízení (EU) XXXX/XXXX [nařízení DORA]**.

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

   Služby sekretariátu zajišťuje Komise.

4. Skupina pro spolupráci má tyto úkoly:

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

   aa) poskytovat doporučení v souvislosti s vypracováváním a prováděním politik v oblasti koordinovaného zveřejňování informací o zranitelnostech podle čl. 5 odst. 2 písm. c) a čl. 6 odst. 1;

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

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

d) vyměňovat si doporučení a spolupracovat s Komisí na návrzích prováděcích aktů Komise [...] přijatých podle této směrnice;

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

ea) vyměňovat si názory na provádění odvětvových právních předpisů s aspekty kybernetické bezpečnosti;

f) projednávat zprávy o vzájemném [...] **učení** podle čl. 16 odst. 7;

g) projednávat [...] **zkušenosti** ze společných dohledových činností v přeshraničních případech podle článku 34;

h) vydávat strategické pokyny síti CSIRT **a síti EU-CyCLONe** ke konkrétním novým problémům;

ha) vyměňovat si názory na politická opatření v návaznosti na rozsáhlé kybernetické bezpečnostní incidenty na základě poznatků získaných sítí CSIRT a sítí EU-CyCLONe;

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

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

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

ka) zavést mechanismus vzájemného učení v souladu s článkem 16 této směrnice.

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

6. Do … [24 měsíců od data vstupu této směrnice v platnost] a poté každé dva roky vypracuje skupina pro spolupráci pracovní program týkající se akcí, jež mají být realizovány za účelem plnění jejích cílů a úkolů. Časový rámec prvního programu přijatého podle této směrnice se sladí s časovým rámcem posledního programu přijatého podle směrnice (EU) 2016/1148.

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

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

Článek 13

Síť CSIRT

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

2. Síť CSIRT tvoří zástupci týmů CSIRT z členských států **určených v souladu s článkem 9** a týmu CERT–EU. Komise se účastní sítě CSIRT jako pozorovatel. Agentura ENISA zajistí služby sekretariátu a aktivně podporuje spolupráci mezi týmy CSIRT.

3. Síť CSIRT má tyto úkoly:

   a) zajišťuje výměnu informací o schopnostech týmů CSIRT;

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

ba) zajišťuje výměnu informací, pokud jde o zveřejňování a doporučení v oblasti kybernetické bezpečnosti;

bb) sdílí technická řešení usnadňující technická řešení incidentů;

bc) vyměňuje si osvědčené postupy, nástroje a procesy, pokud jde o úkoly týmů CSIRT;

c) na žádost [...] **člena** sítě CSIRT potenciálně zasaženého incidentem zajišťuje výměnu informací o tomto incidentu a souvisejících kybernetických hrozbách, rizicích a zranitelnostech;

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

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

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

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

i) kategoriím kybernetických hrozeb a incidentů;

ii) včasným varováním;

iii) vzájemné pomoci;

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

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

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

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

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

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

l) projednává zprávy o vzájemném [...] **učení** podle čl. 16 odst. 7;

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

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

5. Síť CSIRT přijme svůj jednací řád.

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

Článek 14

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

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

2. Síť EU-CyCLONe je tvořena zástupci orgánů členských států pro řízení **kybernetických** krizí určených podle článku 7 [...]. **Komise se účastní činností sítě jako pozorovatel.** Agentura ENISA zajišťuje služby sekretariátu a podporuje bezpečnou výměnu informací a **dále poskytuje nezbytné nástroje na podporu spolupráce mezi členskými státy zajištěním bezpečné výměny informací.**

Tam, kde je to vhodné, může síť EU-CyCLONe přizvat ke spolupráci zástupce příslušných zúčastněných stran.

3. Úkoly sítě EU-CyCLONE jsou:

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

b) rozvíjet společnou informovanost o důležitých událostech [...] v případě rozsáhlých **kybernetických bezpečnostních** incidentů a krizí [...];

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

c) koordinovat **řízení** [...] rozsáhlých kybernetických bezpečnostních incidentů a krizí a podporovat rozhodování na politické úrovni týkající se těchto incidentů a krizí;

d) **na žádost členského státu** projednat **jeho** národní plány reakce na kybernetické bezpečnostní incidenty **a krize** uvedené v čl. 7 odst. **3** [...]**;**[...]

4. Síť EU-CyCLONe přijme svůj jednací řád.

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

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

7. Síť EU-CyCLONe do [24 měsíců od vstupu této směrnice v platnost] předloží Evropskému parlamentu a Radě zprávu, v níž posoudí svou činnost.

Článek 14a

Mezinárodní spolupráce

Unie ve vhodných případech může v souladu s článkem 218 SFEU uzavírat mezinárodní dohody s třetími zeměmi nebo mezinárodními organizacemi, které umožní a zorganizují jejich účast na některých činnostech skupiny pro spolupráci, sítě CSIRT a sítě EU-CyCLONe, a to v souladu s právními předpisy Unie o ochraně údajů.

Článek 15

Zpráva o stavu kybernetické bezpečnosti v Unii

1. Agentura ENISA ve spolupráci s Komisí a **skupinou pro spolupráci** vydává jednou za dva roky zprávu o stavu kybernetické bezpečnosti v Unii. Ve zprávě uvede zejména [...]:

   aa) posouzení kybernetických bezpečnostních rizik na úrovni Unie se zohledněním prostředí hrozeb;

   a) [...] **posouzení** vývoje kapacit v oblasti kybernetické bezpečnosti ve veřejném i soukromém sektoru v celé Unii;

   b) [...]

   c) **agregované posouzení na základě** [...] **kvantitativních a kvalitativních ukazatelů v oblasti** kybernetické bezpečnosti poskytující [...] **přehled o** úrovni vyspělosti kapacit v oblasti kybernetické bezpečnosti**, včetně kapacit v jednotlivých odvětvích**.

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

Článek 16

Vzájemné učení

1. [...] **S cílem posílit vzájemnou důvěru, dosáhnout vysoké společné úrovně kybernetické bezpečnosti a zlepšit kapacity a politiky členských států v oblasti kybernetické bezpečnosti, nutné k účinnému provedení této směrnice, skupina pro spolupráci** [...] s **podporou Komise a** po konzultaci s agenturou ENISA a **případně sítí CSIRT** [...] stanoví nejpozději do [...] **24** měsíců po vstupu této směrnice v platnost metodiku [...] **pro objektivní, nediskriminační a korektní systém** vzájemného [...] **učení, pokud jde o** [...] **provádění této směrnice** ze strany členských států [...]. **Účast na vzájemném učení je dobrovolná.** [...] **Systém spočívá v kolech hodnocení, která** provádějí [...] odborníci na kybernetickou bezpečnost z členských států [...] a která [...] zahrnují **jeden či více následujících aspektů**:

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

   ii) [...] kapacity, včetně dostupných [...] zdrojů, a [...] plnění úkolů příslušných vnitrostátních orgánů **uvedených v článku 8 a týmů CSIRT uvedených v článku 9**;

[...]

i**ii**[...]) [...] **uskutečňování** vzájemné pomoci podle článku 34;

iv) [...] **provádění** rámce sdílení informací podle článku 26 této směrnice [...].

2. **Kritéria, na jejichž základě členské státy určují odborníky, kteří jsou způsobilí k účasti na kolech vzájemného učení, jsou** [...] objektivní, nediskriminační, korektní a transparentní [...] a **jsou obsažena v metodice uvedené v odstavci 1**. Agentura ENISA a Komise [...] **mohou** určit odborníky, kteří se budou **kol vzájemného** [...] **učení** účastnit jako pozorovatelé. [...]

3. [...].

3a. Členské státy mohou před započetím kol vzájemného učení provést sebehodnocení aspektů, jež jsou předmětem konkrétního kola vzájemného učení, a toto sebehodnocení poskytnout určeným odborníkům uvedeným v odstavci 2.

4. Vzájemné [...] **učení** [...] **může** zahrnovat [...] **fyzické** nebo virtuální návštěvy na místě i externí výměny. S ohledem na zásadu dobré spolupráce poskytnou [...] členské státy **účastnící se vzájemného učení** určeným odborníkům [...] informace potřebné k posouzení [...]**, aniž by tím byly dotčeny právní předpisy členských států nebo Unie o ochraně důvěrných či utajovaných informací nebo zabezpečování základních funkcí státu, jako je národní bezpečnost.** Veškeré informace získané v rámci procesu vzájemného [...] **učení** lze použít pouze pro tento účel. Odborníci účastnící se vzájemného [...] **učení** nesmí sdělit žádné citlivé nebo důvěrné informace získané v [...] **této souvislosti** žádným třetím stranám. **Členský stát účastnící se vzájemného učení může vznést námitku vůči určení konkrétních odborníků, a to z řádně opodstatněných důvodů, které sdělí skupině pro spolupráci.**

5. Tytéž aspekty [...]**, které již byly** [...] **předmětem kola** vzájemného [...] **učení**, nejsou v **zúčastněných** členských státech v průběhu [...] **čtyř** let po ukončení **daného** [...] **kola** [...] vzájemného **učení** předmětem dalšího [...] **kola** vzájemného **učení,** [...] **ledaže o to členský stát požádá nebo s tím v návaznosti na návrh skupiny pro spolupráci souhlasí** [...].

6. [...]

7. Odborníci účastnící se **kol** vzájemného [...] **učení** vypracují návrhy zpráv o zjištěních a závěrech [...] **posouzení**. **Členské státy mohou k návrhům svých zpráv uvést připomínky, jež se připojí ke zprávě. Závěrečné** zprávy se předkládají [...] skupině pro spolupráci. **Členské státy mohou rozhodnout o zveřejnění svých zpráv.**

KAPITOLA IV

Řízení kybernetických bezpečnostních rizik a oznamovací povinnosti

ODDÍL I

Řízení a oznamování kybernetických bezpečnostních rizik

Článek 17

Správa a řízení

1. Členské státy zajistí, aby vedoucí orgány základních a důležitých subjektů schválily opatření k řízení rizik v oblasti kybernetické bezpečnosti přijatá těmito subjekty za účelem splnění požadavků článku 18, [...] **dohlížely** nad jejich uplatňováním a **mohly nést** [...] odpovědnost za neplnění povinností subjektů podle tohoto článku.

   Uplatňováním tohoto odstavce nejsou dotčeny vnitrostátní právní předpisy členských států týkající se pravidel odpovědnosti ve veřejných orgánech, ani odpovědnosti úředníků veřejné správy a volených a jmenovaných úředních osob.

2. Členské státy zajistí, aby **členové vedoucího orgánu** [...] **byli povinni** pravidelně absolvova**t** [...] školení, a získali tak dostatečné znalosti a dovednosti, aby mohli posoudit a vyhodnotit kybernetická bezpečnostní rizika a řídicí postupy a jejich dopad na provoz subjektu.

Článek 18

Opatření k řízení rizik v oblasti kybernetické bezpečnosti

1**a. Tato směrnice uplatňuje přístup zohledňující všechna rizika, což zahrnuje ochranu sítě a informačních systémů a jejich fyzické prostředí před všemi událostmi, jež by mohly narušit dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné.**

1. Členské státy zajistí, aby základní a důležité subjekty přijaly vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto subjekty používají pro poskytování svých služeb. S ohledem na nejnovější technický vývoj a **náklady na provádění** musí tato opatření zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika. **Při posuzování proporcionality těchto opatření je třeba řádně zohlednit stupeň vystavení subjektu riziku, jeho velikost a pravděpodobnost vzniku incidentu a jejich závažnost. S ohledem na úroveň a typ rizika, jemuž je společnost vystavena v případě incidentů majících dopad na základní nebo důležité subjekty, mohou být opatření k řízení rizik v oblasti kybernetické bezpečnosti uložená důležitým subjektům méně přísná než opatření uložená základním subjektům.**

2. Opatření uvedená v odstavci 1 zahrnují alespoň:

a) analýzu rizik a politiku bezpečnosti informačních systémů;

b) řešení incidentů (prevence a odhalování incidentů**,** [...] reakce na ně a **zotavení z nich**);

c) řízení kontinuity provozu a krizové řízení;

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

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

f) politiky a postupy [...] za účelem posouzení účelnosti opatření k řízení rizik v oblasti kybernetické bezpečnosti;

g) **politiku pro** používání kryptografie a šifrování;

ga) bezpečnost lidských zdrojů, postupy kontroly přístupu a správa majetku.

3. Členské státy zajistí, aby při zvažování vhodných opatření uvedených v odst. 2 písm. d) subjekty [...] **byly povinny** zohlednit [...] zranitelnosti specifické pro každého **přímého** dodavatele a poskytovatele služeb a celkovou kvalitu produktů a praktik v oblasti kybernetické bezpečnosti svých dodavatelů a poskytovatelů služeb, včetně jejich postupů bezpečného vývoje. **Členské státy rovněž zajistí, aby při zvažování příslušných opatření uvedených v odst. 2 písm. d) měly subjekty povinnost zohlednit výsledky koordinovaného posouzení rizik provedeného v souladu s čl. 19 odst. 1.**

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

5. Komise může přijmout prováděcí akty, aby stanovila technické a metodické specifikace, **jakož i případně odvětvové specifikace** prvků uvedených v odstavci 2 **tohoto článku**. **Komise přijme do [18 měsíců po vstupu v platnost této směrnice] prováděcí akty s cílem stanovit technické a metodické specifikace pro subjekty uvedené v čl. 24 odst. 1 a poskytovatelům služeb vytvářejících důvěru uvedeným v bodě 8 přílohy I. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 37 odst. 2.** Při přípravě **těchto prováděcích** aktů [...] Komise [...] v maximální možné míře **dodržuje** mezinárodní a evropské normy, jakož i příslušné technické specifikace **a vyměňuje si zkušenosti se skupinou pro spolupráci a agenturou ENISA ohledně návrhu prováděcího aktu v souladu s čl. 12 odst. 4 písm. d).**

6. [...]

Článek 19

Koordinované posouzení rizik kritických dodavatelských řetězců v EU

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

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

Článek 20

Oznamovací povinnosti

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

2. [...]

   Ve vhodných případech [...]**základní a důležité** subjekty neprodleně informují příjemce svých služeb, které mohou být ovlivněny významnou kybernetickou hrozbou, o všech krocích nebo nápravných opatřeních, jež příjemci mohou v reakci na danou hrozbu učinit. Ve vhodných případech subjekty příjemce uvědomí také o hrozbě samotné. **Akt** oznámení **sám o sobě** nezakládá u oznamujícího subjektu vyšší míru právní odpovědnosti.

3. Incident se považuje za významný, jestliže:

a) incident dotčenému subjektu způsobil nebo může způsobit **závažné** [...] provozní narušení **služby** nebo finanční ztráty;

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

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

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

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

c) nejpozději do jednoho měsíce od předložení [...]**prvního oznámení** podle písmene a) **závěrečnou** zprávu zahrnující alespoň:

i) podrobný popis incidentu, jeho závažnost a dopad;

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

iii) učiněná a probíhající opatření ke zmírnění následků.

Členské státy zajistí, aby se dotčený subjekt mohl v odůvodněných případech a po dohodě s příslušnými orgány nebo týmem CSIRT odchýlit od lhůt stanovených v písmeni a) a c). **Odchýlení od lhůty stanovené v písmeni c) je možno odůvodnit zejména v případě, že incident stále ještě probíhá.**

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

6. Tam, kde je to vhodné, a zejména pokud se incident podle odstavce 1 týká dvou nebo více členských států, informuje příslušný orgán**,** tým CSIRT **nebo jednotné kontaktní místo**, jimž byl incident oznámen, ostatní dotčené členské státy a agenturu ENISA. **Tato informace zahrnuje alespoň prvky stanovené v odstavci 4 tohoto článku.** Příslušné orgány, týmy CSIRT a jednotná kontaktní místa přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachovávají bezpečnost a obchodní zájmy subjektu, jakož i důvěrnost poskytnutých informací.

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

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

9. Jednotné kontaktní místo předkládá [...] **každých šest měsíců** agentuře ENISA souhrnnou zprávu zahrnující anonymizovaná a agregovaná data o incidentech, závažných kybernetických hrozbách a případech, kdy téměř došlo k incidentu, oznámených podle odstavce 1 [...] a podle článku 27. V zájmu větší srovnatelnosti poskytovaných informací může agentura ENISA vydat technické pokyny k parametrům informací, jež mají být v souhrnné zprávě uvedeny. **Agentura ENISA informuje každých šest měsíců skupinu pro spolupráci a síť týmů CSIRT** o **svých zjištěních v souvislosti s obdrženými oznámeními.**

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

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

Článek 21

Použití evropských systémů certifikace kybernetické bezpečnosti

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

2. Komise může [...] přijmout [...] **prováděcí** akty v přenesené pravomoci upřesňující, které kategorie základních **nebo důležitých** subjektů budou povinny **používat konkrétní certifikované produkty, služby a procesy IKT nebo si** obstarat certifikát [...] podle [...] konkrétních evropských systémů certifikace **přijatých podle článku 49 nařízení (EU) 2019/881.**[...] **Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 37 odst. 2. Při přípravě těchto prováděcích aktů Komise v souladu s článkem 56 nařízení (EU) 2019/881:**

   i) zohlední dopad opatření na výrobce nebo poskytovatele daných produktů, služeb či procesů IKT a na uživatele z hlediska nákladů na tato opatření a společenských nebo hospodářských přínosů plynoucích z očekávaného zvýšení úrovně bezpečnosti pro dotyčné produkty, služby nebo procesy IKT, jakož i alternativní dostupnost na trhu;

   ii) uplatňuje otevřený, transparentní a inkluzivní proces konzultací se všemi relevantními zúčastněnými stranami a s členskými státy;

(i) zohlední prováděcí lhůty, přechodná opatření nebo přechodná období, zejména se zřetelem na možný dopad daných opatření na výrobce nebo poskytovatele produktů, služeb či procesů IKT, či na jejich uživatele, zejména na malé a střední podniky;

(ii) zohlední existenci a provádění příslušných právních předpisů členských států.

3. Komise může požádat agenturu ENISA, aby v případech, kdy není k dispozici žádný vhodný evropský systém certifikace kybernetické bezpečnosti pro účely odstavce 2 **tohoto článku**, vypracovala návrh systému, **nebo aby provedla přezkum stávajícího evropského systému certifikace kybernetické bezpečnosti** podle čl. 48 odst. 2 nařízení (EU) 2019/881.

Článek 22

Standardizace

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

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

Článek 23

Databáze doménových jmen a registračních údajů

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

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

   a) doménové jméno

   b) datum registrace

   c) datum registrace, a to včetně:

      i) pro fyzické osoby – příjmení, jméno a e-mailová adresa;

      ii) pro právnické osoby – jméno a e-mailová adresa.

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

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

5. Členské státy zajistí, aby registry **doménových jmen** TLD a subjekty poskytující služby registrace doménových jmen pro TLD poskytovaly přístup ke konkrétním údajům o registraci doménových jmen na oprávněnou a řádně odůvodněnou žádost oprávněných žadatelů o přístup, a to v souladu s právními předpisy Unie o ochraně osobních údajů. Členské státy zajistí, aby registry **doménových jmen** TLD a subjekty poskytující služby registrace doménových jmen pro TLD neprodleně a **nejpozději do 72 hodin** reagovaly na všechny žádosti o přístup. Členské státy zajistí, aby byly zásady a postupy zveřejňování těchto údajů veřejně dostupné.

Oddíl II

Pravomoc a registrace

Článek 24

Pravomoc a územní působnost

1a. Má se za to, že subjekty podle této směrnice spadají do pravomoci členského státu, ve kterém poskytují své služby. Má se za to, že subjekty uvedené v bodech 1 až 7 a 10 přílohy I, poskytovatelé služeb vytvářejících důvěru a poskytovatelé výměnných uzlů internetu uvedení v bodě 8 přílohy I a v bodech 1 až 5 přílohy II této směrnice spadají do pravomoci členského státu, na jehož území jsou usazeny.

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

2. Pro účely této směrnice se má za to, že hlavním místem obchodní činnosti subjektů uvedených v odstavci 1 v Unii je členský stát, v němž **převážně** přijímají rozhodnutí týkající se opatření k řízení rizik v oblasti kybernetické bezpečnosti. Jestliže **není možno stanovit místo, kde jsou taková rozhodnutí převážně přijímána nebo** tato rozhodnutí nejsou přijímána v žádné provozovně v Unii, má se za to, že hlavní místo obchodní činnosti je v členském státě, kde mají subjekty provozovnu s nejvyšším počtem zaměstnanců v Unii. **Pokud jsou služby poskytovány skupinou podniků, je za hlavní místo obchodní činnosti skupiny podniků považováno hlavní místo obchodní činnosti řídícího podniku.**

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

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

4a. Členské státy, které obdržely žádost o vzájemnou pomoc týkající se subjektů uvedených v odstavci 1, mohou v mezích této žádosti přijmout ohledně dotčeného subjektu, který poskytuje služby nebo jenž má síť nebo informační systém na jejich území, odpovídající opatření pro dohled a prosazování.

Článek 25

Registr pro některé subjekty digitální infrastruktury a digitální poskytovatele

1. [...] **Členské státy zajistí, aby** [...] subjekty **uvedené v čl. 24 odst. 1, které mají hlavní provozovnu na svém území, nebo pokud nejsou usazeny v Unii, které mají svého jmenovaného zástupce v Unii usazeného na svém území, byly povinny** [...] **příslušným orgánům** [...] předložit [nejpozději do 12 měsíců od vstupu této směrnice v platnost] tyto informace:

a) název subjektu;

aa) typ subjektu podle příloh I a II této směrnice;

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

c) aktuální kontaktní údaje, včetně e-mailových adres a telefonních čísel subjektů a **jejich zástupců;**

d) členské státy, v nichž subjekt poskytuje službu.

Tyto informace se předají v případě potřeby prostřednictvím vnitrostátního mechanismu[...] samostatného oznamování uvedeného v článku 2a.

2. **Členské státy zajistí, aby s**[...]ubjekty uvedené v odstavci 1 [...] **rovněž oznámily** všechny změny údajů, které předložily podle odstavce 1, a to neprodleně, nejpozději však do tří měsíců od data, kdy změna začala platit.

3. [...] **Jednotná kontaktní místa členských států** předají **informace uvedené v odstavcích 1 a 2** [...]agentuře [...] **ENISA**. [...]

3a. Na základě informací obdržených podle odstavce 3 tohoto článku agentura ENISA vytvoří a vede rejstřík subjektů uvedených v odstavci 1. Na žádost členských států agentura ENISA umožní přístup do rejstříku odpovídajícím příslušným orgánům, přičemž zajistí případné nezbytné záruky na ochranu důvěrnosti a informací.

4. [...]

KAPITOLA V

Sdílení informací

Článek 26

Ujednání o sdílení informací o kybernetické bezpečnosti

1. [...] Členské státy zajistí, aby základní a důležité subjekty mohly mezi sebou **dobrovolně** sdílet podstatné informace o kybernetické bezpečnosti včetně informací týkajících se kybernetických hrozeb, **případů, kdy téměř došlo k incidentu**, zranitelností, indikátorů narušení, taktiky, technik a postupů, varování při ohrožení kybernetické bezpečnosti a konfiguračních nástrojů, pokud toto sdílení informací:

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

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

2. Členské státy zajistí, aby k výměně informací docházelo v [...] komunitách základních a důležitých subjektů. Tato výměna bude probíhat prostřednictvím ujednání o sdílení informací s ohledem na potenciálně citlivou povahu sdílených informací [...].

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

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

5. [...]Agentura ENISA vznik ujednání o sdílení informací o kybernetické bezpečnosti podle odstavce 2 poskytováním osvědčených postupů a doporučení.

Článek 27

Dobrovolné oznamování podstatných informací

1. Aniž je dotčen článek 20, členské státy zajistí, aby základní a důležité subjekty mohly dobrovolně hlásit příslušným orgánům nebo týmům CSIRT jakékoliv relevantní incidenty, kybernetické hrozby nebo případy, kdy téměř došlo k incidentu.

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

3. Dobrovolná oznámení se zpracují pouze za podmínky, že jejich zpracování nepředstavuje pro dotčené členské státy nepřiměřenou nebo nepatřičnou zátěž.

KAPITOLA VI

Dohled a vymáhání

Článek 28

Obecné aspekty týkající se dohledu a vymáhání

1. Členské státy zajistí, aby příslušné orgány účinně monitorovaly dodržování této směrnice a činily opatření nezbytná k zajištění jejího dodržování, zejména povinností stanovených v článcích 18**,** [...] **a 23**. **Členské státy mohou příslušným orgánům umožnit, aby na základě přístupu založeného na posouzení rizik stanovily priority ohledně dohledu.**

2. Při řešení kybernetických bezpečnostních incidentů příslušné orgány úzce spolupracují s orgány pro ochranu osobních údajů, **příslušnými orgány určenými podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů], orgány dohledu určenými podle nařízení (EU) 910/2014 a jinými příslušnými orgány určenými podle odvětvových právních aktů Unie**. [...]

3. Aniž jsou dotčeny vnitrostátní právní a institucionální rámce, členské státy zajistí, aby příslušné orgány měly při dohledu nad dodržováním této směrnice ze strany subjektů veřejné správy a při prosazování případných sankcí v případě jejího nedodržování odpovídající pravomoci k provedení takových úkolů a měly přitom ve vztahu k subjektům, nad nimiž dohled provádějí, funkční nezávislost. Členské státy mohou rozhodnout o uložení vhodných, přiměřených a účinných opatření pro dohled a vymáhání ve vztahu k těmto subjektům v souladu s vnitrostátními právními rámci a právním řádem.

Článek 29

Dohled a vymáhání u základních subjektů

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

2. Členské státy zajistí, aby se příslušné orgány při výkonu svých dohledových úkolů v souvislosti se základními subjekty **řídily přístupem založeným na posouzení rizik** a měly pravomoc podrobit tyto subjekty **alespoň**:

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

   b) pravidelným **bezpečnostním** auditům;

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

   d) bezpečnostním prověrkám na základě objektivních, nediskriminačních, korektních a transparentních kritérií posouzení rizik**, je-li třeba z technických důvodů, ve spolupráci s dotčeným subjektem**;

   e) požadavkům na informace nezbytné k posouzení opatření v oblasti kybernetické bezpečnosti přijatých subjektem, včetně zadokumentovaných zásad kybernetické bezpečnosti[...];

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

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

2a. Při výkonu svých dohledových úkolů stanovených v odstavci 2 tohoto článku mohou příslušné orgány stanovit metodiky dohledu umožňující určení priorit u takových úkolů na základě přístupu založeného na posouzení rizik.

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

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

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

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

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

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

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

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

g) [...]

h) nařídit těmto subjektům, aby konkrétním způsobem zveřejnily aspekty nedodržování povinností stanovených v této směrnici**, nemá-li takové zveřejnění pro příslušný subjekt za následek poškození**;

i) [...]

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

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

a) pozastavit nebo požádat certifikační nebo schvalovací orgán **nebo soudy podle vnitrostátních právních předpisů** o pozastavení certifikace nebo schválení týkající se všech nebo některých služeb nebo činností poskytovaných základním subjektem;

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

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

Sankce stanovené v tomto odstavci se nevztahují na subjekty veřejné správy, na něž se vztahuje tato směrnice.

6. Členské státy zajistí, aby každá fyzická osoba odpovědná za základní subjekt nebo jednající jako zástupce základního subjektu na základě pravomoci jej zastupovat, oprávnění přijímat rozhodnutí jeho jménem nebo oprávnění vykonávat nad ním kontrolu měla pravomoc zajistit plnění povinností stanovených v této směrnici. Členské státy zajistí, aby tyto fyzické osoby mohly být volány k odpovědnosti za porušení svých úkolů zajistit dodržování povinností stanovených v této směrnici. **Pokud jde o subjekty veřejné správy, nejsou tímto ustanovením dotčeny právní předpisy členských států ohledně odpovědnosti úředníků veřejné správy a zvolených veřejných činitelů a jmenovaných úředníků.**

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

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

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

c) skutečně způsobené škody nebo vzniklé ztráty, případně potenciální škody nebo ztráty, které mohly být způsobeny, pokud je lze určit. Při hodnocení tohoto aspektu je třeba zohlednit mimo jiné skutečné nebo potenciální finanční nebo ekonomické ztráty, účinky na jiné služby, počet postižených nebo potenciálně postižených uživatelů;

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

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

f) dodržování schválených kodexů chování nebo schválených certifikačních mechanismů;

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

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

9. Členské státy zajistí, aby jejich příslušné orgány **podle této směrnice** při výkonu svých pravomocí v oblasti dohledu a vymáhání zaměřených na zajištění dodržování povinností podle této směrnice ze strany základního subjektu určeného podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] za kritický subjekt **[**nebo subjekt, který je rovnocenný kritickému subjektu**]**, informovaly relevantní příslušné orgány v **rámci téhož** [...] členského státu určené podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů]. [...] **P**říslušné orgány podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů] [...] **mohou případně požádat** příslušné orgány **podle této směrnice** [...], aby vykonávaly své **pravomoci v** oblasti dohledu a vymáhání **ve vztahu k** základnímu subjektu spadajícímu do oblasti působnosti této směrnice, který je rovněž označen jako kritický**[**nebo rovnocenný kritickému subjektu **] podle směrnice (EU) XXXX/XXXX [směrnice o odolnosti kritických subjektů].**

10. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice informovaly fórum dohledu podle čl. 29 odst. 1 nařízení (EU) XXXX/XXXX [DORA], když plní své pravomoci v oblasti dohledu a vymáhání zaměřené na zajištění toho, aby základní subjekt označený za kritického poskytovatele služeb IKT z řad třetích stran podle článku 28 nařízení (EU) XXXX/XXXX [DORA] plnil povinnosti podle této směrnice.

10a. Členské státy zajistí, aby jejich příslušné orgány podle této směrnice informovaly relevantní příslušné orgány určené podle nařízení (EU) 910/2014, když plní své pravomoci v oblasti dohledu a vymáhání zaměřené na zajištění toho, aby subjekt označený za poskytovatele služeb vytvářejících důvěru podle nařízení (EU) 910/2014 plnil povinnosti podle této směrnice.

Článek 30

Dohled a vymáhání u důležitých subjektů

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

2. Členské státy zajistí, aby se příslušné orgány při výkonu svých dohledových úkolů v souvislosti s důležitými subjekty **řídily přístupem založeným na posouzení rizik a** měly pravomoc podrobit tyto subjekty **alespoň**:

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

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

   c) bezpečnostním prověrkám na základě objektivních, **nediskriminačních,** korektních a transparentních kritérií posouzení rizik, a **je-li to nezbytné z technických důvodů, ve spolupráci s dotčeným subjektem;**

   d) požadavkům na veškeré informace nezbytné k posouzení opatření v oblasti kybernetické bezpečnosti *ex post* [...];

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

   ea) požadavkům na doklady ohledně provádění politik v oblasti kybernetické bezpečnosti, jako jsou výsledky bezpečnostních auditů provedených kvalifikovaným auditorem a příslušné podpůrné doklady.

2a. Při výkonu svých dohledových úkolů stanovených v odstavci 2 tohoto článku mohou příslušné orgány stanovit metodiky dohledu umožňující určení priorit u takových úkolů na základě přístupu založeného na posouzení rizik.

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

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

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

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

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

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

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

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

g) nařídit těmto subjektům, aby specifikovaným způsobem zveřejnily aspekty neplnění jejich povinností stanovených v této směrnici**, nemá-li takové zveřejnění pro příslušný subjekt za následek poškození**;

h) [...]

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

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

Článek 31

Obecné podmínky ukládání správních pokut základním a důležitým subjektům

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

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

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

4. Členské státy zajistí, aby za porušení povinností stanovených v článku 18 nebo článku 20 **ze strany základních subjektů** byly v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty, jejichž maximální výše bude stanovena na nejméně **4** [...] 000 000 EUR nebo v **případě právnické osoby** [...] 2 % celkového celosvětového ročního obratu podniku, ke kterému patřil základní [...] subjekt v předchozím rozpočtovém roce, podle toho, která částka je vyšší.

4a. Členské státy zajistí, aby za porušení povinností stanovených v článku 18 nebo článku 20 ze strany důležitých podniků byly v souladu s odstavci 2 a 3 tohoto článku uloženy správní pokuty, jejichž maximální výše bude stanovena na nejméně 2 000 000 EUR nebo v případě právnické osoby 1 % celkového celosvětového ročního obratu podniku, ke kterému patřil důležitý subjekt v předchozím rozpočtovém roce, podle toho, která částka je vyšší.

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

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

6a. Neumožňuje-li právo členského státu uložení správních pokut, členské státy zajistí, že se tento článek může uplatňovat tak, aby podnět k uložení pokuty dal příslušný orgán a aby pokuta byla uložena příslušnými vnitrostátními soudy, a současně je třeba zajistit, aby tyto prostředky právní ochrany byly účinné a aby byl jejich účinek rovnocenný správním pokutám, jež ukládají příslušné úřady. Uložené pokuty musí být v každém případě účinné, přiměřené a odrazující. Tyto členské státy oznámí Komisi do […] příslušná ustanovení svých právních předpisů, která přijmou podle tohoto odstavce, a bez prodlení jakékoliv následné novely nebo změny týkající se těchto ustanovení.

Článek 32

Porušení povinností spočívající v porušení zabezpečení osobních údajů

1. Pokud [...] příslušné orgány v **průběhu dohledu nebo vymáhání zjistí** [...], že porušení povinností stanovených v článcích 18 a 20 **této směrnice** základním nebo důležitým subjektem **může mít** [...] za následek porušení zabezpečení osobních údajů ve smyslu čl. 4 odst. 12 nařízení (EU) 2016/679, které musí být oznámeno podle článku 33 uvedeného nařízení, **bez zbytečného prodlení** uvědomí [...] orgány dohledu příslušné podle článků 55 a 56 uvedeného nařízení.

2. Pokud se orgány dohledu příslušné podle článků 55 a 56 nařízení (EU) 2016/679 rozhodnou vykonat své pravomoci podle čl. 58 **odst. 2** písm. i) uvedeného nařízení a uložit správní pokutu, příslušné orgány **uvedené v článku 8 této směrnice** neuloží za [...] porušení článku 31 této směrnice **stejným činem** správní pokutu [...]. Příslušné orgány však mohou uplatnit donucovací opatření nebo sankční pravomoci stanovené v čl. 29 odst. 4 písm. a) až i), čl. 29 odst. 5 a v čl. 30 odst. 4 písm. a) až h) této směrnice.

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

Článek 33

Sankce

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

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

Článek 34

Vzájemná pomoc

1. Pokud základní nebo důležitý subjekt poskytuje služby ve více než jednom členském státě nebo [...] **poskytuje služby** v **jednom nebo více** člensk[...]**ých** stát[...]**ů**, ale jeho sítě a informační systémy se nacházejí v jednom či více jiných členských státech, příslušn[...]**é** orgán**y dotčených** člensk[...]**ých** stát[...]**ů**, [...] podle potřeby spolupracují a jsou si navzájem nápomocny. Tato spolupráce spočívá alespoň v tomto:

a) příslušné orgány uplatňující opatření v oblasti dohledu nebo vymáhání v členském státě konzultují prostřednictvím jednotného kontaktního místa s příslušnými orgány v ostatních dotčených členských státech ohledně přijatých opatřeních v oblasti dohledu a vymáhání a informují je o nich [...];

b) příslušný orgán může požádat jiný příslušný orgán, aby přijal opatření v oblasti dohledu nebo vymáhání [...];

c) po obdržení odůvodněné žádosti jiného příslušného orgánu poskytne příslušný orgán druhému příslušnému orgánu pomoc **úměrnou zdrojům, jež má k dispozici**, aby bylo možné provést opatření v oblasti dohledu nebo vymáhání [...] účelně, efektivně a důsledně. Tato vzájemná pomoc může zahrnovat žádosti o informace a opatření v oblasti dohledu, včetně žádostí o provedení kontrol na místě nebo externího dohledu, případně cílených bezpečnostních auditů. Příslušný orgán, kterému je určena žádost o pomoc, nemůže tuto žádost odmítnout, ledaže se po výměně informací s ostatními dotčenými orgány [...] prokáže, že tento orgán není příslušný k poskytnutí požadované pomoci **nebo nemá nezbytné zdroje** nebo požadovaná pomoc není úměrná prováděným úkolům dohledu příslušného orgánu [...] **nebo se žádost týká informací nebo zahrnuje činnosti, jež jsou v rozporu s národní bezpečností, veřejnou bezpečností nebo obranou daného členského státu**.

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

KAPITOLA VII

Přechodná a závěrečná ustanovení

Článek 35

Přezkum

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

Článek 36

[...]

[...]

[...]

Článek 37

Postup projednávání ve výboru

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

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

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

Článek 38

Provedení ve vnitrostátním právu

1. Členské státy **do**… [[...] **24** měsíců po vstupu této směrnice**]** v platnost přijmou a zveřejní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Neprodleně o nich uvědomí Komisi. Začnou tato opatření uplatňovat ode dne ... [jeden den ode dne uvedeného v prvním pododstavci].

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

Článek 39

Změna nařízení (EU) č. 910/2014

V nařízení (EU) č. 910/2014 se s **účinností od ... [datum provedení této směrnice ve vnitrostátním právu]** zrušuje článek 19**.**

Článek 40

Změna směrnice (EU) 2018/1972

Ve směrnici (EU) 2018/1972 se [...] s **účinností od ... [datum provedení této směrnice ve vnitrostátním právu]** zrušují články 40 a 41**.**

Článek 41

Zrušení

Směrnice (EU) 2016/1148 se zrušuje s účinkem ode dne ... [datum provedení směrnice ve vnitrostátním právu].

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

Článek 42

Vstup v platnost

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

Článek 43

Určení

Tato směrnice je určena členským státům.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda	*předseda* nebo *předsedkyně*

PŘÍLOHA I

ODVĚTVÍ, PODODVĚTVÍ A DRUHY SUBJEKTŮ

Odvětví	Pododvětví	Druh subjektu
1. Energetika	a) elektřina	– elektroenergetické podniky ve smyslu čl. 2 bodu 57 směrnice (EU) 2019/944, které zastávají funkci „dodávky“ ve smyslu čl. 2 bodu 12 uvedené směrnice([39])
		– provozovatelé distribuční soustavy ve smyslu čl. 2 bodu 29 směrnice (EU) 2019/944
		– provozovatelé přenosové soustavy ve smyslu čl. 2 bodu 35 směrnice (EU) 2019/944
		– výrobci ve smyslu čl. 2 bodu 38 směrnice (EU) 2019/944
		— nominovaní organizátoři trhu s elektřinou ve smyslu čl. 2 bodu 8 nařízení (EU) 2019/943 ([40])
		– účastníci trhu s elektřinou ve smyslu čl. 2 bodu 25 nařízení (EU) 2019/943, kteří poskytují služby agregace, odezvy strany poptávky nebo ukládání energie ve smyslu čl. 2 bodů 18, 20 a 59 směrnice (EU) 2019/944
	b) dálkové vytápění	– dálkové vytápění nebo dálkové

[39] 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).

[40] Nařízení Evropského parlamentu a Rady (EU) 2019/943 o vnitřním trhu s elektřinou (Úř. věst. L 158, 14.6.2019, s. 54).

	a chlazení	chlazení ve smyslu čl. 2 bodu 19 směrnice (EU) 2018/2001 o podpoře využívání energie z obnovitelných zdrojů ([41])
	c) ropa	– provozovatelé ropovodů
		– provozovatelé zařízení na těžbu, rafinaci a zpracování ropy a skladovacích a přenosových zařízení
		— ústřední správci zásob ropy ve smyslu čl. 2 písm. f) směrnice Rady 2009/119/ES ([42])
	d) zemní plyn	– dodavatelské podniky ve smyslu čl. 2 bodu 8 směrnice 2009/73/ES ([43])
		– provozovatelé distribuční soustavy ve smyslu čl. 2 bodu 6 směrnice 2009/73/ES
		– provozovatelé přepravní soustavy ve smyslu čl. 2 bodu 4 směrnice 2009/73/ES
		– provozovatelé skladovacího zařízení ve smyslu čl. 2 bodu 10 směrnice 2009/73/ES
		– provozovatelé zařízení LNG ve smyslu čl. 2 bodu 12 směrnice 2009/73/ES

[41] 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).

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

[43] 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).

		– plynárenské podniky ve smyslu čl. 2 bodu 1 směrnice 2009/73/ES
		– provozovatelé zařízení na rafinaci a zpracování zemního plynu
	e) vodík	provozovatelé výroby, skladování a přepravy vodíku
2. Doprava	a) letecká	– letečtí dopravci ve smyslu čl. 3 bodu 4 nařízení (ES) č. 300/2008 ([44]) **využívaní ke komerčním účelům**
		– řídící orgány letiště ve smyslu čl. 2 bodu 2 směrnice 2009/12/ES ([45]), letiště ve smyslu čl. 2 bodu 1 uvedené směrnice, včetně hlavních letišť uvedených v příloze II, části 2 nařízení (EU) č. 1315/2013 ([46]); a subjekty provozující pomocná zařízení v rámci letišť

[44] 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).

[45] 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).

[46] 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).

		– provozovatelé kontroly řízení provozu poskytující služby řízení letového provozu ve smyslu čl. 2 bodu 1 nařízení (ES) č. 549/2004 ([47])
	b) železniční	– provozovatelé infrastruktury ve smyslu čl. 3 bodu 2 směrnice 2012/34/EU ([48])
		– železniční podniky ve smyslu čl. 3 bodu 1 směrnice 2012/34/EU, včetně provozovatelů zařízení služeb ve smyslu čl. 3 bodu 12 směrnice 2012/34/EU
	c) vodní	– společnosti vnitrozemské, námořní a pobřežní osobní a nákladní vodní dopravy, jak jsou vymezeny pro námořní dopravu v příloze I nařízení (ES) č. 725/2004 ([49]), kromě jednotlivých plavidel provozovaných těmito podniky
		– řídící orgány přístavů ve smyslu čl. 3 bodu 1 směrnice 2005/65/ES ([50]), včetně jejich přístavních zařízení ve smyslu čl. 2 bodu 11 nařízení (ES) č. 725/2004; a subjekty provozující díla a zařízení v rámci přístavů

[47] 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).

[48] 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).

[49] 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).

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

		– provozovatelé služeb lodní dopravě ve smyslu čl. 3 písm. o) směrnice 2002/59/ES ([51])
	d) silniční	– silniční orgány ve smyslu čl. 2 bodu 12 nařízení Komise v přenesené pravomoci (EU) 2015/962 ([52]) odpovědné za kontrolu řízení provozu, s **výjimkou veřejných subjektů, pro něž je řízení provozu nebo provozovatelé inteligentních dopravních systémů pouze nepodstatnou součástí jejich obecné činnosti**
		– provozovatelé inteligentních dopravních systémů ve smyslu čl. 4 bodu 1 směrnice 2010/40/EU ([53])
3. Bankovnictví		— Úvěrové instituce ve smyslu čl. 4 bodu 1 nařízení (EU) č. 575/2013 ([54])**, [s výjimkou institucí uvedených v čl. 2 odst. 5 bodě 8 směrnice 2013/36/EU, které jsou vyňaty podle čl. 2 odst. 4 nařízení XX [DORA]]**

[51] Směrnice Evropského parlamentu a Rady 2002/59/ES ze dne 27. června 2002, kterou se stanoví kontrolní a informační systém Společenství pro provoz plavidel a kterou se zrušuje směrnice Rady 93/75/EHS (Úř. věst. L 208, 5.8.2002, s. 10).

[52] Nařízení Komise v přenesené pravomoci (EU) 2015/962 ze dne 18. prosince 2014, kterým se doplňuje směrnice Evropského parlamentu a Rady 2010/40/EU, pokud jde o poskytování informačních služeb o dopravním provozu v reálném čase v celé EU (Úř. věst. L 157, 23.6.2015, s. 21).

[53] 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).

[54] Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 176, 27.6.2013, s. 1).

4. Infrastruktura finančních trhů		– provozovatelé obchodních systémů ve smyslu čl. 4 bodu 24 směrnice 2014/65/EU ([55])
		– ústřední protistrany ve smyslu čl. 2 bodu 1 nařízení (EU) č. 648/2012 ([56])
5. Zdravotnictví		— poskytovatelé zdravotní péče ve smyslu čl. 3 písm. g) směrnice 2011/24/EU ([57])
		— referenční laboratoře EU ve smyslu článku 15 nařízení XXXX/XXXX o vážných přeshraničních zdravotních hrozbách[58]
		— subjekty provádějící výzkum a vývoj týkající se léčivých přípravků ve smyslu čl. 1 bodu 2 směrnice 2001/83/ES ([59]) — subjekty vyrábějící základní farmaceutické výrobky a farmaceutické přípravky ve smyslu sekce C oddílu 21 klasifikace NACE Rev. 2 — subjekty vyrábějící zdravotnické prostředky považované za kritické v případě ohrožení veřejného zdraví (uvedené na „seznamu kritických

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

[56] 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).

[57] 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).

[58] [Nařízení Evropského parlamentu a Rady o vážných přeshraničních zdravotních hrozbách a o zrušení rozhodnutí č. 1082/2013/EU, odkaz bude aktualizován, jakmile bude návrh COM(2020) 727 final přijat]

[59] 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).

		zdravotnických prostředků při mimořádné situaci v oblasti veřejného zdraví“) ve smyslu článku 20 nařízení XXXX[60]
6. Pitná voda		dodavatelé a distributoři vody určené k lidské spotřebě ve smyslu čl. 2 bodu 1 písm. a) směrnice Rady 98/83/ES ([61]), avšak kromě distributorů, pro něž je distribuce vody určené k lidské spotřebě pouze **nepodstatnou** částí jejich obecné činnosti spočívající v distribuci jiných komodit a zboží [...]
7. Odpadní voda		podniky zajišťující odvádění, vypouštění nebo čištění městských odpadních vod, splašků a průmyslových odpadních vod ve smyslu čl. 2 bodů 1 až 3 směrnice Rady 91/271/EHS ([62]), **avšak s vyloučením podniků, pro něž je odvádění, vypouštění nebo čištění městských odpadních vod, splašků a průmyslových odpadních vod pouze nepodstatnou částí jejich obecné činnosti.** [...]
8. Digitální infrastruktura		– poskytovatelé výměnných uzlů internetu
		– poskytovatelé služeb systému doménových jmen (DNS)**, s výjimkou provozovatelů kořenových jmenných serverů**
		— registry internetových domén nejvyšší úrovně (TLD)

[60] [Nařízení Evropského parlamentu a Rady o posílené úloze Evropské agentury pro léčivé přípravky při připravenosti na krize a krizovém řízení v oblasti léčivých přípravků a zdravotnických prostředků, odkaz bude aktualizován, jakmile bude návrh COM(2020) 725 final přijat]

[61] Směrnice Rady 98/83/ES ze dne 3. listopadu 1998 o jakosti vody určené k lidské spotřebě (Úř. věst. L 330, 5.12.1998, s. 32).

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

		– poskytovatelé služeb cloud computingu
		– poskytovatelé služeb datových center
		– poskytovatelé sítí pro doručování obsahu
		– poskytovatelé služeb vytvářejících důvěru ve smyslu čl. 3 bodu 19 nařízení (EU) č. 910/2014 ([63])
		– poskytovatelé veřejných sítí elektronických komunikací ve smyslu čl. 2 bodu 8 směrnice (EU) 2018/1972 ([64]) nebo poskytovatelé služeb elektronických komunikací uvedených v čl. 2 bodu 4 směrnice (EU) 2018/1972, jsou-li jejich služby veřejně dostupné
8.a Řízení služeb IKT (B2B)		— **Poskytovatelé řízených služeb (MSP)** — **Poskytovatelé řízených bezpečnostních služeb (MSSP)**

[63] 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).

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

9. **Subjekty** veřejné správy		— Subjekty veřejné správy ústředních vlád **vymezené členským státem v souladu s vnitrostátním právem** — [...][65][...] — [...]
10. Vesmír		— provozovatelé pozemních infrastruktur vlastněných, spravovaných a provozovaných členskými státy nebo soukromými subjekty a podporujících poskytování služeb využívajících kosmického prostoru, s výjimkou poskytovatelů veřejných sítí elektronických komunikací ve smyslu čl. 2 bodu 8 směrnice (EU) 2018/1972

65 [...]

PŘÍLOHA II

ODVĚTVÍ, PODODVĚTVÍ A DRUHY SUBJEKTŮ

Odvětví	Pododvětví	Druh subjektu
1. Poštovní a kurýrní služby		poskytovatelé poštovních služeb ve smyslu čl. 2 bodu 1[...] směrnice 97/67/ES ([66]) **včetně** [...] poskytovatelů kurýrních služeb
2. Nakládání s odpady		podniky provádějící nakládání s odpady ve smyslu čl. 3 bodu 9 směrnice 2008/98/ES ([67]), avšak s výjimkou podniků, pro které nakládání s odpady nepředstavuje hlavní hospodářskou činnost

[66] 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)**, ve znění směrnice Evropského parlamentu a Rady 2008/6/ES ze dne 20. února 2008, kterou se mění směrnice 97/67/ES s ohledem na úplné dotvoření vnitřního trhu poštovních služeb Společenství (Úř. věst. L 52, 27.2.2008, s. 3)**.

[67] 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).

3. Výroba, produkce a distribuce chemických látek		podniky provádějící výrobu[...] **a** distribuci látek a [...] **směsí** ve smyslu čl. 3 bodů ([...]) 9 a 14 nařízení (ES) č. 1907/2006 ([68]) **a podniky provádějící výrobu předmětů ve smyslu čl. 3 bodu 3 tohoto nařízení z látek a směsí.**
4. Výroba, zpracování a distribuce potravin		potravinářské podniky ve smyslu čl. 3 bodu 2 nařízení (ES) č. 178/2002([69])**, které se podílejí na velkoobchodní distribuci a průmyslové výrobě a zpracování**
5. Výroba	a) výroba zdravotnických prostředků a diagnostických zdravotnických prostředků in vitro	subjekty vyrábějící zdravotnické prostředky ve smyslu čl. 2 bodu 1 nařízení (EU) 2017/745 ([70]) a subjekty vyrábějící diagnostické zdravotnické prostředky in vitro ve smyslu čl. 2 bodu 2 nařízení (EU) 2017/746 ([71]), s výjimkou subjektů vyrábějících zdravotnické prostředky uvedených v příloze 1 bodu 5.
	b) výroba počítačů, elektronických	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu

68 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).

69 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).

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

71 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).

	a optických přístrojů a zařízení	sekce C oddílu 26 klasifikace NACE Rev. 2
	c) výroba elektrických zařízení	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 27 klasifikace NACE Rev. 2
	d) výroba strojů a zařízení j. n.	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 28 klasifikace NACE Rev. 2
	e) výroba motorových vozidel, přívěsů a návěsů	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 29 klasifikace NACE Rev. 2
	f) výroba jiných dopravních prostředků a zařízení	podniky vykonávající kteroukoliv z hospodářských činností ve smyslu sekce C oddílu 30 klasifikace NACE Rev. 2
6. Digitální poskytovatelé		– poskytovatelé on-line tržišť
		– poskytovatelé internetových vyhledávačů
		– poskytovatelé platforem služeb sociálních sítí