Úřední věstník L 194

Evropské unie

Svazek 59

České vydání **Právní předpisy** 19. července 2016

Obsah

CS

Akty, jejichž název není vytištěn tučně, se vztahují ke každodennímu řízení záležitostí v zemědělství a obecně platí po omezenou dobu. Názvy všech ostatních aktů jsou vytištěny tučně a předchází jim hvězdička.

I

(Legislativní akty)

SMĚRNICE

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

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 ([1]),

v souladu s řádným legislativním postupem ([2]),

vzhledem k těmto důvodům:

(1) Sítě, informační systémy a informační služby hrají ve společnosti zcela zásadní roli. Jejich spolehlivost a bezpečnost je nezbytná pro ekonomické a společenské činnosti, a především pak pro fungování vnitřního trhu.

(2) Rostoucí rozsah, četnost výskytu a dopad bezpečnostních incidentů představují pro fungování sítí a informačních systémů významnou hrozbu. Uvedené systémy se rovněž mohou stát snadným cílem úmyslných škodlivých akcí za účelem poškození nebo narušení provozu systémů. Tyto incidenty mohou bránit ve výkonu ekonomické činnosti, přivodit významné finanční ztráty, narušit důvěru uživatelů a způsobit značnou újmu hospodářství Unie.

(3) Sítě a informační systémy, především internet, plní zásadní roli při usnadňování přeshraničního pohybu zboží, služeb a osob. Vzhledem k tomuto nadnárodnímu rozměru se může významné narušení uvedených systémů, ať již úmyslné či neúmyslné, dotknout jednotlivých členských států i Unie jako celku, a to bez ohledu na místo, kde k takovému narušení došlo. Bezpečnost sítí a informačních systémů je proto základním předpokladem pro hladké fungování vnitřního trhu.

(4) Na základě značného pokroku, kterého dosáhlo Evropské fórum členských států v podporování diskuzí a výměny osvědčených postupů v oblasti tvorby politik, včetně vypracování zásad evropské spolupráce pro případ kybernetické krize, by měla být ustavena skupina pro spolupráci sestávající ze zástupců členských států, Komise a Agentury Evropské unie pro bezpečnost sítí a informací (ENISA), jež se bude věnovat podpoře a usnadňování

([1]) Úř. věst. C 271, 19.9.2013, s. 133.

([2]) Postoj Evropského parlamentu ze dne 13. března 2014 (dosud nezveřejněný v Úředním věstníku) a postoj Rady v prvním čtení ze dne 17. května 2016 (dosud nezveřejněný v Úředním věstníku). Postoj Evropského parlamentu ze dne 6. července 2016 (dosud nezveřejněný v Úředním věstníku).

strategické spolupráce mezi členskými státy v oblasti bezpečnosti sítí a informačních systémů. Aby byla tato skupina účinná a komplexní, musí mít všechny členské státy minimální schopnosti a strategii zajišťující vysoký stupeň bezpečnosti sítí a informačních systémů na svém území. Kromě toho by se rovněž měly na provozovatele základních služeb a na poskytovatele digitálních služeb vztahovat bezpečnostní požadavky a požadavky na hlášení incidentů, aby byla podpořena kultura řízení rizik a aby bylo zaručeno hlášení nejzávažnějších incidentů.

(5) Stávající schopnosti nejsou pro zajištění vysokého stupně bezpečnosti sítí a informačních systémů v Unii dostačující. Míra připravenosti jednotlivých členských států se velmi liší, což vede v rámci Unie k roztříštěnosti přístupů. Důsledkem toho jsou rozdílné úrovně ochrany spotřebitelů a podniků a zhoršená celková úroveň bezpečnosti sítí a informačních systémů v Unii. Z důvodu neexistence společných požadavků vztahujících se na provozovatele základních služeb a poskytovatele digitálních služeb je pak nemožné vytvořit komplexní a účinný mechanismus spolupráce na úrovni Unie. Pokud jde o stimulaci výzkumu, vývoje a inovací v těchto oblastech, hrají rozhodující úlohu univerzity a výzkumná centra.

(6) Účinná odezva na výzvy, jež bezpečnost sítí a informačních systémů obnáší, proto vyžaduje komplexní přístup na úrovni Unie, jenž bude zahrnovat společné minimální požadavky, pokud jde o budování kapacit a plánování, výměnu informací, spolupráci a společné bezpečnostní požadavky, pokud jde o provozovatele základních služeb a poskytovatele digitálních služeb. Provozovatelům základních služeb a poskytovatelům digitálních služeb však není bráněno v uplatňování bezpečnostních opatření, která jsou přísnější než opatření stanovená touto směrnicí.

(7) Aby byly pokryty všechny relevantní incidenty a rizika, měla by se tato směrnice vztahovat na provozovatele základních služeb i na poskytovatele digitálních služeb. Povinnosti provozovatelů základních služeb a poskytovatelů digitálních služeb by se však neměly vztahovat na podniky zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací ve smyslu směrnice Evropského parlamentu a Rady 2002/21/ES ([1]), na něž se vztahují zvláštní požadavky na bezpečnost a integritu podle uvedené směrnice, ani na poskytovatele služeb vytvářejících důvěru ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([2]), na něž se vztahují bezpečnostní požadavky stanovené v uvedeném nařízení.

(8) Touto směrnicí by neměla být dotčena možnost jednotlivých členských států přijmout nezbytná opatření, aby zajistily ochranu podstatných zájmů své bezpečnosti, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů. Podle článku 346 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“) nemá být žádný členský stát povinen poskytovat údaje, jejichž zpřístupnění podle jeho názoru odporuje podstatným zájmům jeho bezpečnosti. V tomto ohledu jsou relevantní rozhodnutí Rady 2013/488/EU ([3]) a dohody o zachování důvěrnosti údajů nebo neformální dohody o zachování důvěrnosti, jako je například tzv. „semaforový protokol“ (Traffic Light Protocol).

(9) Některá hospodářská odvětví již jsou nebo v budoucnu mohou být regulována odvětvovými právními akty Unie, které zahrnují pravidla upravující bezpečnost sítí a informačních systémů. Kdykoli takové právní akty Unie obsahují ustanovení, jimiž se ukládají požadavky týkající se bezpečnosti sítí a informačních systémů nebo hlášení incidentů, měla by se tato ustanovení použít, pokud jsou tyto požadavky přinejmenším rovnocenné co do účinku povinnostem stanoveným v této směrnici. Členské státy by pak měly uplatňovat ustanovení těchto odvětvových právních aktů Unie včetně ustanovení týkajících se pravomoci členských států a neměly by provádět určování provozovatelů základních služeb, jak je vymezeno touto směrnicí. V tomto ohledu by členské státy měly o uplatnění těchto ustanovení informovat Komisi. Při určování, zda jsou požadavky na bezpečnost sítí a informačních systémů nebo na hlášení incidentů obsažené v odvětvových právních aktech Unie rovnocenné požadavkům obsaženým v této směrnici, by měl být brán zřetel pouze na ustanovení příslušných právních aktů Unie a na jejich uplatňování v členských státech.

(10) V odvětví vodní dopravy se bezpečnostní požadavky na společnosti, plavidla, přístavní zařízení, přístavy a služby pro provoz plavidel podle právních aktů Unie vztahují na všechny operace včetně rádiových a telekomunikačních systémů, počítačových systémů a sítí. Součástí povinných postupů, jimiž je třeba se řídit, je mimo jiné podávání zpráv o všech incidentech, a měly by být tudíž považovány za *lex specialis*, pokud jsou tyto požadavky přinejmenším rovnocenné odpovídajícím ustanovením této směrnice.

([1]) Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice) (Úř. věst. L 108, 24.4.2002, s. 33).

([2]) 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).

([3]) Rozhodnutí Rady 2013/488/EU ze dne 23. září 2013 o bezpečnostních pravidlech na ochranu utajovaných informací EU (Úř. věst. L 274, 15.10.2013, s. 1).

(11) Při určování provozovatelů v oblasti vodní dopravy by členské státy měly zohlednit stávající i budoucí mezinárodní kodexy a pokyny, vypracované především Mezinárodní námořní organizací, a to s cílem zajistit ve vztahu k jednotlivým provozovatelům v námořním odvětví konzistentní přístup.

(12) Regulace a dohled v odvětvích bankovnictví a infrastruktur finančního trhu jsou na úrovni Unie vysoce harmonizovány za využití primárních a sekundárních právních předpisů Unie a díky normám vypracovaným ve spolupráci s evropskými orgány dohledu. V rámci bankovní unie zajišťuje uplatňování těchto požadavků a dohled nad nimi jednotný mechanismus dohledu. V případě členských států, jež nejsou součástí bankovní unie, zajišťují tyto úkoly příslušné vnitrostátní bankovní regulační orgány. V dalších oblastech regulace finančního odvětví zajišťuje vysokou míru soudržnosti a sbližování v postupech dohledu rovněž Evropský systém finančního dohledu. Přímý dohled nad určitými subjekty, jako jsou úvěrové ratingové agentury a registry obchodních údajů vykonává rovněž Evropský orgán pro cenné papíry a trhy.

(13) V odvětvích bankovnictví a infrastruktur finančního trhu je provozní riziko klíčovou součástí obezřetnostní regulace a dohledu. Vztahuje se na všechny operace a zahrnuje i bezpečnosti, integritu a odolnosti sítí a informačních systémů. Požadavky na tyto systémy, které mnohdy přesahují požadavky stanovené touto směrnicí, jsou vymezeny v řadě právních aktů Unie, kam patří: pravidla upravující přístup k činnosti úvěrových institucí a obezřetnostní dohled nad úvěrovými institucemi a investičními podniky a pravidla upravující obezřetnostní požadavky na úvěrové instituce a investiční podniky, v nichž jsou zahrnuty požadavky týkající se operačního rizika; pravidla upravující trhy finančních nástrojů, v nichž jsou zahrnuty požadavky na posouzení rizik pro investiční podniky a regulované trhy; pravidla upravující OTC deriváty, ústřední protistrany a registry obchodních údajů, v nichž jsou zahrnuty požadavky na ústřední protistrany a registry obchodních údajů týkající se provozního rizika; a pravidla upravující zlepšení vypořádání obchodů s cennými papíry v Unii a pravidla upravující centrální depozitáře cenných papírů, v nichž jsou rovněž zahrnuty požadavky týkající se provozního rizika. Kromě toho ve finančním odvětví představují požadavky na hlášení incidentů součást běžných postupů dohledu a mnohdy jsou obsaženy v příručkách, jež jsou dohledu věnovány. Členské státy by tato pravidla a požadavky měly vzít v úvahu při uplatňování *lex specialis*.

(14) Jak konstatovala Evropská centrální banka ve svém stanovisku ze dne 25. července 2014 ([1]), touto směrnicí není dotčen režim Eurosystému pro dohled nad platebními systémy a vypořádacími systémy stanovený unijním právem. Bylo by vhodné, aby si orgány odpovědné za tento dohled vyměňovaly zkušenosti v oblasti bezpečnosti sítí a informačních systémů s orgány příslušnými podle této směrnice. Totéž platí pro členy Evropského systému centrálních bank, kteří nejsou členy eurozóny, kteří vykonávají podobný dohled nad platebními a vypořádacími systémy na základě vnitrostátních právních předpisů.

(15) Prostřednictvím on-line tržiště mohou spotřebitelé a obchodníci s konečnou platností uzavírat s obchodníky on-line smlouvy o prodeji nebo o poskytnutí služeb. Neměly by na něm být nabízeny on-line služby, jež fungují pouze jako služby zprostředkovatelské, směřující ke službám třetích stran, s nimiž lze teprve uzavřít smlouvu. Neměly by na něm být tudíž nabízeny on-line služby, jež poskytují srovnání cen konkrétních produktů či služeb různých obchodníků, aby následně uživatele přesměrovaly k nákupu u zvoleného obchodníka. Výpočetní služby poskytované on-line tržištěm mohou zahrnovat zpracování transakcí, shromažďování údajů nebo sestavování uživatelských profilů. Za druh on-line tržiště se mají považovat obchody s aplikacemi, jež jsou provozovány jako on-line obchody umožňující digitální distribuci aplikací nebo softwarových programů třetích stran.

(16) Internetový vyhledávač umožňuje, aby uživatel prováděl vyhledávání v zásadě na všech internetových stránkách na základě dotazu na jakékoli téma. Rovněž může být případně zaměřen na internetové stránky v konkrétním jazyce. Definice internetového vyhledávače uvedená v této směrnici by se neměla vztahovat na vyhledávací funkce, jež jsou omezeny na obsah konkrétních internetových stránek, a to bez ohledu na to, zda vyhledávací funkci poskytuje externí internetový vyhledávač. Neměla by se vztahovat ani na on-line služby, jež poskytují srovnání cen konkrétních produktů či služeb různých obchodníků, aby poté uživatele přesměrovaly k nákupu u zvoleného obchodníka.

(17) Služby cloud computingu zahrnují širokou škálu činností, jež mohou být poskytovány na základě různých modelů. Pro účely této směrnice se „službami cloud computingu“ rozumí služby umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které je možno sdílet. Tyto výpočetní zdroje zahrnují zdroje jako sítě, servery či jinou infrastrukturu, úložiště, aplikace a služby. 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

([1]) Úř. věst. C 352, 7.10.2014, s. 4.

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.

(18) Funkcí výměnného uzlu internetu (IXP) je propojovat sítě. Výměnný uzel internetu neposkytuje přístup k internetu ani nefunguje jako poskytovatel tranzitního připojení nebo tranzitní infrastruktury. Výměnný uzel internetu rovněž neposkytuje další služby, které nesouvisejí s propojením, což ovšem nebrání provozovateli uzlu, aby takové služby poskytoval. Výměnný uzel internetu existuje za účelem propojení sítí, které jsou z technického a organizačního hlediska oddělené. Pojem „autonomní systém“ se používá k označení technicky soběstačné sítě.

(19) Za určování subjektů, které splňují kritéria definice provozovatele základních služeb, by měly být odpovědné členské státy. V zájmu zajištění konzistentního přístupu by měla být definice provozovatele základních služeb uplatňována ve všech členských státech jednotně. Za tímto účelem upravuje tato směrnice hodnocení subjektů činných v jednotlivých odvětvích a pododvětvích, sestavení seznamu základních služeb, možnost společného seznamu okolností působících napříč odvětvími, díky němuž by bylo možno určit, zda by potenciální incident vedl k významnému narušení, proces konzultací se zapojením relevantních členských států pro případy subjektů poskytujících služby ve více než jednom členském státě a podporu skupiny pro spolupráci při identifikaci. Aby bylo zajištěno, že budou náležitě zohledněny případné změny na trhu, měly by členské státy seznam určených provozovatelů pravidelně podrobovat přezkumu a v případě potřeby jej aktualizovat. Dále by členské státy měly Komisi poskytovat informace nezbytné pro posouzení rozsahu, v němž tato společná metodika umožnila konzistentní uplatňování uvedené definice členskými státy.

(20) V rámci procesu určení provozovatelů základních služeb by členské státy měly posoudit, minimálně pro každé pododvětví uvedené v této směrnici, které služby je nutno považovat za základní z hlediska zachování kritických společenských a ekonomických činností, a zda subjekty uvedené v této směrnici pro jednotlivá odvětví a pododvětví, které tyto služby poskytují, splňují kritéria pro to, aby byly určeny jako provozovatelé. Při posuzování toho, zda určitý subjekt poskytuje službu, která je základní z hlediska zachování kritických společenských nebo ekonomických činností, postačuje ověřit, zda tento subjekt poskytuje některou ze služeb, která je uvedena na seznamu základních služeb. Poté by mělo být prokázáno, že poskytování takové základní služby závisí na sítích a informačních systémech. Při posuzování toho, zda by incident vedl k významnému narušení poskytování dané služby, by pak členské státy měly nakonec vzít zřetel na řadu okolností působících napříč odvětvími, jakož i případně na okolnosti specifické pro jednotlivá odvětví.

(21) Usazení v členském státě předpokládá pro účely určení provozovatelů základních služeb účinný a skutečný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodující.

(22) Subjekty činné v odvětvích a pododvětvích uvedených v této směrnici mohou poskytovat i jiné služby než základní. Například v odvětví letecké dopravy poskytují letiště služby, které může členský stát považovat za základní, jako je údržba vzletových a přistávacích drah, ale rovněž i řadu služeb považovaných za jiné než základní, jako je zajišťování nákupních prostor. Provozovatelé základních služeb by měli podléhat zvláštním bezpečnostním požadavkům pouze ve vztahu k těm službám, jež jsou považovány za základní. Pro účely určení provozovatelů by proto měly členské státy sestavit seznam služeb, které se považují za základní.

(23) Seznam služeb by měl obsahovat veškeré služby poskytované na území příslušného členského státu, které splňují požadavky podle této směrnice. Členské státy by měly mít možnost doplnit do stávajícího seznamu nové služby. Tento seznam služeb by měl sloužit členským státům jako referenční nástroj umožňující identifikovat provozovatele základních služeb. Jeho účelem je identifikovat druhy základních služeb v kterémkoli daném odvětví uvedeném v této směrnici a odlišit je tak od jiných než základních činností, za něž může být odpovědný subjekt činný v kterémkoli z daných odvětví. Seznam služeb, který sestaví každý členský stát, by rovněž sloužil jako další zdroj vstupních informací pro posouzení regulační praxe každého členského státu, a to v zájmu zajištění celkové míry konzistentnosti procesu určování mezi členskými státy.

(24) V případě, že určitý subjekt poskytuje základní služby ve dvou či více členských státech, měly by tyto členské státy při určování zahájit dvoustranné či vícestranné konzultace. Tyto konzultace jim mají pomoci při hodnocení kritičnosti provozovatele z hlediska přeshraničního dopadu a umožnit každému dotčenému členskému státu, aby se vyjádřil k rizikům souvisejícím s poskytovanými službami. Dotčené členské státy by v tomto procesu měly brát vzájemně v potaz svá stanoviska a měly by mít možnost požádat v této souvislosti o součinnost skupinu pro spolupráci.

(25) Výsledkem procesu určování by mělo být přijetí vnitrostátních opatření, jimiž členské státy stanoví, které subjekty podléhají požadavkům na bezpečnost sítí a informačních systémů. Tohoto výsledku by mohlo být dosaženo přijetím úplného seznamu všech provozovatelů základních služeb nebo přijetím vnitrostátních opatření zahrnujících objektivní měřitelná kritéria, jako jsou například objem produkce provozovatele nebo počet uživatelů, umožňující stanovit, které subjekty podléhají požadavkům na bezpečnost sítí a informačních systémů. Vnitrostátní opatření, ať již existující, nebo přijatá na základě této směrnice, by měla zahrnovat veškerá právní a správní opatření a politiky, jež umožňují určení provozovatelů základních služeb podle této směrnice.

(26) Aby bylo možné vyjádřit významnost určených provozovatelů základních služeb ve vztahu k příslušnému odvětví, měly by členské státy brát zřetel na počet a velikost těchto provozovatelů, například z hlediska podílu na trhu nebo objemu produkce či přepravy, aniž by byly povinny sdělovat informace umožňující zjistit, kteří provozovatelé byli určeni.

(27) Aby bylo možné stanovit, zda by případný incident vedl k významnému narušení poskytování základní služby, měly by členské státy brát zřetel na řadu různých okolností, jako například na počet uživatelů, kteří službu využívají pro soukromé nebo profesionální účely. Využití dané služby se může uskutečňovat přímo, nepřímo nebo zprostředkovaně. Při hodnocení dopadu, jejž by z hlediska intenzity a délky trvání mohl případný incident mít na ekonomické a společenské činnosti nebo na veřejnou bezpečnost, by členské státy měly rovněž posoudit dobu, jež pravděpodobně uplyne do okamžiku, než dané narušení kontinuity začne mít negativní účinky.

(28) Aby bylo možné stanovit, zda by případný incident vedl k významnému narušení poskytování základní služby, měly by členské státy brát zřetel nejen na okolnosti působící napříč odvětvími, ale i na okolnosti specifické pro jednotlivá odvětví. Pokud jde o dodavatele energie, mohly by takové okolnosti zahrnovat objem vyrobené energie nebo její podíl na celkovém vnitrostátním objemu; u dodavatelů ropy by mohly zahrnovat objem dodané ropy za den, u letecké dopravy (včetně letišť a leteckých přepravců), železniční dopravy a námořních přístavů by mohly zahrnovat poměrný objem dopravy vzhledem k celkovému vnitrostátnímu objemu a rovněž počet cestujících nebo nákladních operací za rok, u bankovnictví nebo infrastruktur finančního trhu by mohly zahrnovat jejich systémový význam na základě celkového majetku nebo poměrného množství takového majetku vzhledem k HDP, u zdravotnictví by mohly zahrnovat počet pacientů v péči poskytovatele za rok, u výroby, zpracování a dodávek vody by mohly zahrnovat objem dodávek a počet a druh uživatelů (jako například nemocnic, veřejných služeb, organizací nebo fyzických osob), jakož i existenci alternativních zdrojů vody pro pokrytí téže zeměpisné oblasti.

(29) V zájmu dosažení a udržení vysoké úrovně bezpečnosti sítí a informačních systémů by každý členský stát měl mít národní strategii pro bezpečnost sítí a informačních systémů, která by definovala strategické cíle a konkrétní opatření, jež je třeba přijmout.

(30) Vzhledem k odlišnostem jednotlivých vnitrostátních správních struktur a s cílem podpořit již existující odvětvová opatření nebo kontrolní a regulační orgány Unie a zamezit zdvojování činností by členské státy měly mít možnost určit více než jeden vnitrostátní příslušný orgán odpovědný za plnění úkolů spojených s bezpečností sítí a informačních systémů provozovatelů základních služeb a poskytovatelů digitálních služeb podle této směrnice.

(31) Pro usnadnění přeshraniční spolupráce a komunikace a za účelem účinného provedení této směrnice je nezbytné, aniž by tím byla dotčena odvětvová regulační opatření, 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. Příslušné orgány a jednotná kontaktní místa by měly disponovat patřičnými technickými, finančními a lidskými zdroji, aby bylo zajištěno, že budou schopny účinně a efektivně plnit úkoly jim svěřené, a naplnit tak cíle této směrnice. Jelikož cílem této směrnice je zlepšit fungování vnitřního trhu na základě budování důvěry, je třeba, aby orgány členských států mohly účinně spolupracovat s hospodářskými subjekty a aby byly odpovídajícím způsobem strukturovány.

(32) Incidenty by měly být hlášeny příslušným orgánům nebo bezpečnostním týmům typu CSIRT. Jednotným kontaktním místům by hlášení o incidentech přímo zasílána být neměla, neplní-li tato místa současně funkci příslušného orgánu nebo týmu CSIRT. Příslušný orgán nebo tým CSIRT by však měly mít možnost pověřit jednotné kontaktní místo tím, aby hlášení o incidentech postupovalo jednotným kontaktním místům dalších dotčených členských států.

(33) Aby bylo zajištěno, že členským státům i Komisi budou skutečně poskytnuty informace, mělo by jednotné kontaktní místo předkládat souhrnnou zprávu skupině pro spolupráci a tato zpráva by měla být anonymizována, aby byla zachována důvěrnost hlášení a totožnost provozovatelů základních služeb a poskytovatelů digitálních služeb, neboť informace o identitě ohlašujících subjektů nejsou pro účely výměny osvědčených postupů v rámci skupiny pro spolupráci nezbytné. Souhrnná zpráva by měla obsahovat informace o počtu obdržených oznámení a o povaze oznámených incidentů, jako jsou typy narušení bezpečnosti, jejich závažnost nebo délka jejich trvání.

(34) Členské státy by měly být náležitě vybaveny jak technicky, tak organizačně, aby mohly předcházet vzniku incidentů a rizik spojených 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 (Computer Emergency Response Team), které budou splňovat základní požadavky tak, aby byly zaručeny jejich efektivní a kompatibilní schopnosti pro řešení incidentů a rizik a aby byla zajištěna účinná spolupráce na úrovni Unie. Aby měly z uvedených schopností a spolupráce prospěch všechny druhy provozovatelů základních služeb a poskytovatelů digitálních služeb, měly by členské státy zajistit, že každý druh těchto subjektů pokrývá určený tým CSIRT. 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.

(35) Jelikož většinu sítí a informačních systémů provozují soukromé subjekty, je naprosto nezbytná spolupráce mezi veřejným a soukromým sektorem. Provozovatelé základních služeb a poskytovatelé digitálních služeb by měli být motivováni k vytváření svých vlastních neformálních mechanismů spolupráce k zajištění bezpečnosti sítí a informačních systémů. Skupina pro spolupráci by měla mít možnost přizvat ve vhodných případech k jednáním příslušné zúčastněné strany. V zájmu účinné podpory sdílení informací a osvědčených postupů je nezbytné zajistit, aby provozovatelé základních služeb a poskytovatelé digitálních služeb, kteří se na těchto výměnách podílejí, nebyli v důsledku své spolupráce znevýhodněni.

(36) Agentura ENISA by měla členským státům a Komisi pomoci tím, že poskytne odborné znalosti a poradenství a usnadní výměny osvědčených postupů. Především Komise by při uplatňování této směrnice měla agenturu ENISA konzultovat, přičemž členské státy by měly mít možnost tak učinit. V zájmu budování kapacit a znalostí mezi členskými státy by měla skupina pro spolupráci sloužit rovněž jako nástroj pro výměnu osvědčených postupů a projednávání schopností a připravenosti členských států, přičemž na dobrovolném základě by měla být svým členům nápomocna při hodnocení jejich národních strategií pro bezpečnost sítí a informačních systémů, budování kapacit a hodnocení cvičení zaměřených na bezpečnost sítí a informačních systémů.

(37) Při uplatňování této směrnice by členské státy měly mít možnost v náležitých případech využít nebo přizpůsobit stávající organizační struktury či strategie.

(38) Příslušné úkoly skupiny pro spolupráci a agentury ENISA jsou vzájemně provázané a doplňují se. Agentura ENISA by obecně měla být skupině pro spolupráci nápomocna při plnění jejích úkolů na základě cíle agentury ENISA, jenž je stanoven v nařízení Evropského parlamentu a Rady (EU) č. 526/2013 ([1]), podle nějž je agentura zejména nápomocna orgánům, subjektům, úřadům a agenturám Unie a členským státům při provádění politik, které jsou nezbytné k plnění právních a regulačních požadavků na bezpečnost sítí a informačních systémů podle stávajících i budoucích právních aktů Unie. Agentura ENISA by měla především poskytovat podporu v oblastech, jež odpovídají jejím vlastním úkolům uvedeným v nařízení (EU) č. 526/2013, kterými jsou analýza strategií pro bezpečnost sítí a informačních systémů, podpora organizace a pořádání cvičení v Unii zaměřených na bezpečnost sítí a informačních systémů a výměna informací a osvědčených postupů, pokud jde o osvětu a vzdělávání. Agentura ENISA by se také měla podílet na vývoji pokynů pro kritéria pro jednotlivá odvětví, pokud jde o určování významu dopadu incidentů.

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 526/2013 ze dne 21. května 2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004 (Úř. věst. L 165, 18.6.2013, s. 41).

(39) Za účelem podpory vyšší úrovně bezpečnosti sítí a informačních systémů by skupina pro spolupráci měla v příslušných případech spolupracovat s relevantními orgány, subjekty, úřady a agenturami Unie, vyměňovat si s nimi poznatky a osvědčené postupy a poskytovat jim poradenství ohledně aspektů bezpečnosti sítí a informačních systémů, které by mohly mít dopad na jejich činnost, a to při zachování stávajících opatření upravujících výměnu utajovaných informací. Při spolupráci s orgány pro vymáhání práva týkající se aspektů bezpečnosti sítí a informačních systémů, které by mohly mít dopad na jejich činnost, by skupina pro spolupráci měla respektovat stávající informační kanály a zavedené sítě.

(40) Informace o incidentech jsou stále cennější jak pro širokou veřejnost, tak i pro podniky, a to zejména pro malé a střední podniky. V některých případech jsou tyto informace na vnitrostátní úrovni již poskytovány prostřednictvím internetových stránek, v jazyce konkrétní země a se zvláštním zaměřením na incidenty a události vnitrostátního rozměru. Vzhledem k tomu, že podniky v rostoucí míře poskytují své služby přeshraničně a že občané stále častěji využívají on-line služeb, měly by být informace o incidentech poskytovány v souhrnné podobě na úrovni Unie. Sekretariát sítě CSIRT se vybízí, aby spravoval internetové stránky nebo poskytoval hosting zvláštnímu portálu na již existujících internetových stránkách, kde budou široké veřejnosti poskytovány obecné informace o velkých incidentech narušujících bezpečnost sítí a informačních systémů, k nimž došlo v celé Unii, přičemž zvláštní ohled musí být brán na zájmy a potřeby podniků. Týmy CSIRT zapojené do sítě CSIRT se vyzývají, aby na dobrovolném základě poskytovaly informace ke zveřejnění na uvedených internetových stránkách, aniž by uváděly informace důvěrné nebo citlivé povahy.

(41) Pokud se podle unijních a vnitrostátních předpisů o zachovávání důvěrnosti obchodních informací jedná o důvěrné informace, jejich důvěrnost by měla být při provádění činností a plnění cílů stanovených touto směrnicí zajištěna.

(42) Pro testování připravenosti a spolupráce členských států v oblasti bezpečnosti sítí a informačních systémů mají klíčový význam cvičení, během nichž dochází k simulaci scénářů incidentů v reálném čase. Užitečný nástroj pro testování řešení incidentů na úrovni Unie a pro formulaci doporučení v otázce postupného zlepšování této reakce představuje cyklus cvičení CyberEurope koordinovaný agenturou ENISA za účasti členských států. Jelikož v současné době nejsou členské státy povinny plánovat cvičení ani se jich účastnit, vytvoření sítě CSIRT podle této směrnice by členským státům mělo umožnit zapojovat se do cvičení na základě přesného plánování a strategických rozhodnutí. Strategická rozhodnutí týkající se cvičení by měla projednávat skupina pro spolupráci zřízená podle této směrnice, zejména, avšak nikoli výlučně, pokud jde o pravidelnost jejich konání a o sestavování scénářů. Agentura ENISA by v souladu se svým mandátem měla organizaci a konání cvičení na úrovni Unie podporovat, a poskytovat za tímto účelem skupině pro spolupráci a síti CSIRT odborné poznatky a poradenství.

(43) Vzhledem ke globální povaze bezpečnostních problémů postihujících sítě a informační systémy je nutná užší mezinárodní spolupráce zaměřená na zdokonalení bezpečnostních norem a výměny informací a na prosazování společného a komplexního přístupu k otázkám bezpečnosti.

(44) Povinnost zajistit bezpečnost sítí a informačních systémů mají do značné míry provozovatelé základních služeb a poskytovatelé digitálních služeb. Stanovením vhodných regulačních požadavků a pomocí dobrovolných odvětvových postupů by měla být prosazována a rozvíjena kultura řízení rizik spočívající v posuzování rizik a zavádění bezpečnostních opatření úměrných hrozícím rizikům. Pro účinné fungování skupiny pro spolupráci a sítě CSIRT v zájmu zajištění účinné spolupráce všech členských států má zásadní význam rovněž vytvoření důvěryhodných a rovných podmínek.

(45) Tato směrnice se použije pouze na orgány veřejné správy, jež jsou určeny jakožto provozovatelé základních služeb. Za zajištění bezpečnosti sítí a informačních systémů veřejné správy, jež nespadají do oblasti působnosti této směrnice, jsou tak odpovědné členské státy.

(46) Opatření pro řízení rizik zahrnují opatření pro identifikaci veškerých rizik incidentů, předcházení incidentům, jejich odhalování a řešení a snižování jejich dopadu. Bezpečnost sítí a informačních systémů zahrnuje bezpečnost uchovávaných, předávaných a zpracovávaných údajů.

(47) Příslušné orgány by měly být oprávněny přijímat na vnitrostátní úrovni pokyny ohledně okolností, za nichž jsou provozovatelé základních služeb povinni hlásit incidenty.

(48) Řada podniků v Unii spoléhá při poskytování vlastních služeb na poskytovatele digitálních služeb ve smyslu této směrnice. Protože některé digitální služby by mohly být pro své uživatele, včetně provozovatelů základních služeb, významným zdrojem a protože tito uživatelé nemusejí mít vždy k dispozici dostupnou alternativu, měla by se tato směrnice vztahovat rovněž na poskytovatele uvedených služeb. Bezpečnost, kontinuita a spolehlivost druhů digitálních služeb uvedených v této směrnici mají zásadní význam pro bezproblémové fungování mnoha podniků. Narušení takové digitální služby by mohlo bránit v poskytování jiných služeb, jež jsou na ní závislé, a mohlo by tak mít dopad na klíčové ekonomické a společenské činnosti v Unii. Tyto digitální služby tudíž mohou mít zásadní význam pro bezproblémové fungování podniků, jež jsou na nich závislé, a kromě toho i pro účast takových podniků na vnitřním trhu a přeshraničním obchodu v celé Unii. Poskytovateli digitálních služeb, na které se vztahuje tato směrnice, jsou ti poskytovatelé, u nichž se má za to, že nabízejí digitální služby, na kterých je rostoucí měrou závislé velké množství podniků v Unii.

(49) Poskytovatelé digitálních služeb by měli zajišťovat míru bezpečnosti přiměřenou míře rizika, jemuž je vystavena bezpečnost jimi poskytovaných digitálních služeb, a to se zřetelem k významu těchto služeb pro fungování jiných podniků v Unii. Míra rizika, jemuž jsou vystaveni provozovatelé základních služeb, mnohdy nezbytných pro zachování klíčových hospodářských a společenských činností, bývá ovšem v praxi vyšší než v případě poskytovatelů digitálních služeb. Bezpečnostní požadavky na poskytovatele digitálních služeb by tudíž měly být méně náročné. Poskytovatelé digitálních služeb by měli mít i nadále možnost přijímat opatření, jež považují za přiměřená z hlediska řízení rizik, kterým je vystavena bezpečnost jejich sítí a informačních systémů. Vzhledem ke své přeshraniční povaze by měli poskytovatelé digitálních služeb podléhat harmonizovanějšímu přístupu na úrovni Unie. Vymezení a provádění takovýchto opatření by mělo být usnadněno prostřednictvím prováděcích aktů.

(50) Přestože výrobci hardwaru a vývojáři softwaru nejsou provozovateli základních služeb ani poskytovateli digitálních služeb, přispívají svými produkty k bezpečnosti sítí a informačních systémů. Plní tudíž významnou úlohu tím, že provozovatelům základních služeb a poskytovatelům digitálních služeb umožňují zabezpečit jejich sítě a informační systémy. Na tyto hardwarové a softwarové produkty se již vztahují stávající pravidla o odpovědnosti za výrobky.

(51) Technická a organizační opatření ukládaná provozovatelům základních služeb a poskytovatelům digitálních služeb by neměla vyžadovat, aby byl konkrétní komerční produkt v oblasti informační a komunikační technologie navržen, vyvinut nebo vyroben určitým konkrétním způsobem.

(52) Provozovatelé základních služeb a poskytovatelé digitálních služeb by měli zajišťovat bezpečnost sítí a informačních systémů, které používají. Jedná se především o soukromé sítě a informační systémy, jež jsou buď spravovány jejich interními pracovníky IT, nebo jejichž bezpečnost zajišťuje externí dodavatel. Požadavky týkající se bezpečnosti a hlášení by měly pro provozovatele základních služeb a poskytovatele digitálních služeb platit bez ohledu na to, zda své sítě a informační systémy spravují interně, nebo s pomocí externího dodavatele.

(53) Uvedené požadavky by měly být úměrné rizikům, jež daná síť nebo informační systém obnáší, aby na provozovatele základních služeb a poskytovatele digitálních služeb nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na nejnovější technický vývoj takových opatření. V případě poskytovatelů digitálních služeb by se tyto požadavky neměly vztahovat na mikropodniky a malé podniky.

(54) Pokud služeb nabízených ze strany poskytovatelů digitálních služeb využívají orgány veřejné správy členských států, zejména pokud jde o služby cloud computingu, mohou se tyto orgány rozhodnout, že budou od poskytovatelů dotyčných služeb vyžadovat dodatečná bezpečnostní opatření nad rámec obvyklé nabídky poskytovatelů digitálních služeb, která je v souladu s požadavky této směrnice. Měly by mít možnost tak učinit formou smluvních závazků.

(55) Definice on-line tržišť, internetových vyhledávačů a služeb cloud computingu uvedené v této směrnici jsou určeny pro konkrétní účel této směrnice a nejsou jimi dotčeny jiné nástroje.

(56) Tato směrnice by neměla bránit členským státům v přijetí vnitrostátních opatření ukládajících subjektům veřejného sektoru, aby v rámci zakázek, jež na služby cloud computingu zadávají, zajistily uplatnění zvláštních bezpečnostních požadavků. Veškerá takováto vnitrostátní opatření by se měla vztahovat na dotyčný subjekt veřejného sektoru, a nikoli na poskytovatele služeb cloud computingu.

(57) Se zřetelem k zásadním rozdílům mezi provozovateli základních služeb, zejména z hlediska jejich přímého napojení na fyzickou infrastrukturu, a poskytovateli digitálních služeb, zejména z hlediska jejich přeshraniční povahy, by tato směrnice měla ve vztahu k uvedeným dvěma skupinám subjektů uplatňovat diferencovaný přístup, pokud jde o míru harmonizace. V případě provozovatelů základních služeb by členské státy měly mít možnost určit příslušné provozovatele a ukládat přísnější požadavky, než jsou požadavky stanovené touto směrnicí. Členské státy by neměly určovat poskytovatele digitálních služeb, neboť tato směrnice by se měla použít na všechny poskytovatele digitálních služeb v oblasti její působnosti. Kromě toho by tato směrnice a prováděcí akty přijaté v souvislosti s ní měly pro poskytovatele digitálních služeb zajišťovat vysokou míru harmonizace, co se týče bezpečnostních požadavků a požadavků na hlášení incidentů. S poskytovateli digitálních služeb v celé Unii by mělo být zacházeno jednotným způsobem a přiměřeně k jejich povaze a míře rizika, kterému by mohli čelit.

(58) Tato směrnice by neměla členským státům bránit, aby ukládaly bezpečnostní požadavky a požadavky na hlášení incidentů subjektům, které nejsou poskytovateli digitálních služeb spadajícími do oblasti působnosti této směrnice, aniž by však byly dotčeny povinnosti členských států vyplývající z práva Unie.

(59) Příslušné orgány by měly věnovat náležitou pozornost zachování neformálních a důvěryhodných informačních kanálů pro sdílení informací. Zveřejňování incidentů ohlášených příslušným orgánům by mělo zachovávat patřičnou rovnováhu mezi zájmem veřejnosti být informovanou o hrozbách a možným poškozením pověsti či obchodních zájmů provozovatelů základních služeb a poskytovatelů digitálních služeb, kteří incidenty ohlašují. Při zavádění povinnosti hlášení incidentů by příslušné orgány a týmy CSIRT měly věnovat zvláštní pozornost skutečnosti, že informace o zranitelnosti produktu musí až do přijetí vhodných bezpečnostních řešení zůstat přísně důvěrné.

(60) Poskytovatelé digitálních služeb by měli podléhat mírné a reaktivní následné kontrole, odůvodněné povahou jejich služeb a činností. Dotčený příslušný orgán by měl tudíž jednat pouze v případě, že má k dispozici důkazy, například přímo od poskytovatele digitálních služeb, od jiného příslušného orgánu, včetně příslušných orgánů jiného členského státu, nebo od uživatele dané služby, které potvrzují, že některý poskytovatel digitálních služeb nesplňuje požadavky této směrnice, a to zejména poté, co již došlo k incidentu. Příslušný orgán by proto neměl mít obecnou povinnost vykonávat nad poskytovateli digitálních služeb kontrolu.

(61) Příslušné orgány by měly mít k dispozici potřebné prostředky k plnění svých povinností, včetně pravomoci mít přístup k informacím nezbytným pro posouzení míry bezpečnosti sítí a informačních systémů.

(62) K incidentům může docházet v důsledku trestné činnosti, jejíž předcházení, vyšetřování a stíhání je podporováno prostřednictvím koordinace a spolupráce mezi provozovateli základních služeb, poskytovateli digitálních služeb, příslušnými orgány a orgány pro vymáhání práva. Existuje-li podezření, že určitý incident souvisí se závažnou trestnou činností podle unijního nebo vnitrostátního práva, měly by členské státy motivovat provozovatele základních služeb a poskytovatele digitálních služeb, aby incidenty s podezřením na trestní povahu ohlašovali z vlastní iniciativy orgánům pro vymáhání práva. V určitých případech je žádoucí, aby koordinaci mezi příslušnými orgány a orgány pro vymáhání práva různých členských států zprostředkovávaly Evropské centrum pro boj proti kyberkriminalitě (EC3) a agentura ENISA.

(63) V důsledku incidentů je v mnoha případech ohrožena ochrana osobních údajů. V tomto ohledu by příslušné orgány a orgány pro ochranu osobních údajů měly spolupracovat a vyměňovat si informace o všech významných skutečnostech, aby řešily jakékoli porušení ochrany osobních údajů, k němuž v důsledku incidentů dochází.

(64) Pravomoc nad poskytovateli digitálních služeb by měl mít ten členský stát, v němž je daný poskytovatel v rámci Unie primárně usazen, což v zásadě odpovídá místu, kde se v Unii nachází jeho sídlo. Usazení předpokládá účinný a skutečný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodující. Uvedené kritérium

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 primárního usazení, a tudíž ani nejsou kritérii pro jeho určení.

(65) Nabízí-li poskytovatel digitálních služeb usazený mimo Unii služby v rámci Unie, měl by ustanovit svého zástupce. Aby bylo možno určit, zda takový poskytovatel digitálních služeb nabízí služby v rámci Unie, mělo by být ověřeno, zda má dotyčný poskytovatel digitálních služeb zjevně v úmyslu nabízet služby osobám v jednom nebo více členských státech. Pouhá dostupnost internetových stránek poskytovatele digitálních služeb 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 poskytovatel digitálních služeb 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 poskytovatel digitálních služeb má v úmyslu nabízet služby v rámci Unie. Zástupce by měl jednat jménem poskytovatele digitálních služeb a příslušné orgány nebo týmy CSIRT by měly být oprávněny zástupce kontaktovat. Zástupce by měl být výslovně písemně pověřen poskytovatelem digitálních služeb, aby mohl jednat jeho jménem v otázkách jeho povinností podle této směrnice, včetně hlášení incidentů.

(66) Standardizace bezpečnostních požadavků vychází z potřeb trhu. Za účelem zajištění jednotného konzistentního uplatňování bezpečnostních norem by členské státy měly podporovat dodržování určitých norem či soulad s nimi, aby byla zaručena vysoká míra bezpečnosti sítí a informačních systémů na úrovni Unie. Členským státům by měla být prostřednictvím poradenství a pokynů nápomocna agentura ENISA. V tomto ohledu by mohlo být vhodné vypracovat návrhy harmonizovaných norem, což by mělo být provedeno v souladu s nařízením Evropského parlamentu a Rady (EU) č. 1025/2012 ([1]).

(67) Také subjekty mimo oblast působnosti této směrnice mohou zaznamenat incidenty se závažným dopadem na služby, které poskytují. Pro případ, že tyto subjekty budou mít za to, že je ve veřejném zájmu ohlásit takové incidenty, měly by mít možnost dobrovolně tak učinit. Tato hlášení by měly příslušné orgány nebo týmy CSIRT zpracovat za podmínky, že jejich zpracování nebude pro dotčené členské státy představovat nepřiměřenou nebo nepatřičnou zátěž.

(68) Za účelem zajištění jednotných podmínek k provedení této směrnice by měly být Komisi svěřeny prováděcí pravomoci, pokud jde o stanovení procesních opatření nezbytných pro fungování skupiny pro spolupráci a o vymezení požadavků na poskytovatele digitálních služeb, co se týče bezpečnostních požadavků a požadavků na hlášení incidentů. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ([2]). Při přijímání prováděcích aktů upravujících procedurální opatření nezbytná pro fungování skupiny pro spolupráci by Komise měla brát maximální ohled na stanovisko agentury ENISA.

(69) Při přijímání prováděcích aktů ohledně bezpečnostních požadavků na poskytovatele digitálních služeb by Komise měla brát maximální ohled na stanovisko agentury ENISA a měla by konzultovat zúčastněné strany. Navíc by měla brát v úvahu následující příklady: pokud jde o bezpečnost systémů, budov a zařízení: fyzická a environmentální bezpečnost, bezpečnost dodávek, kontrola přístupu k sítím a informačním systémům, integrita sítí a informačních systémů; pokud jde o řešení incidentů: postupy řešení incidentů, schopnosti pro odhalování incidentů, hlášení incidentů a komunikace ohledně incidentů; pokud jde o řízení kontinuity provozu: strategie a krizové plány pro zajištění kontinuity činnosti, schopnosti pro obnovení provozu po mimořádné události; a pokud jde o monitorování, audit a testování: politiky monitorování a pořizování záznamů, procvičování krizových plánů, testování sítí a informačních systémů, posuzování bezpečnosti a sledování souladu s předpisy.

(70) Při provádění této směrnice by Komise měla vhodným způsobem úzce spolupracovat s příslušnými odvětvovými výbory a orgány zřízenými na úrovni Unie v oblastech, na něž se tato směrnice vztahuje.

([1]) 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).

([2]) 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).

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

(72) V rámci sdílení informací o rizicích a incidentech prostřednictvím skupiny pro spolupráci a sítě CSIRT a v rámci plnění povinnosti hlásit incidenty vnitrostátním příslušným orgánům nebo týmům CSIRT může vyvstat potřeba zpracovávat osobní údaje. Takové zpracování osobních údajů by mělo být prováděno v souladu se směrnicí Evropského parlamentu a Rady 95/46/ES ([1]) a nařízením Evropského parlamentu a Rady (ES) č. 45/2001 ([2]). Při uplatňování této směrnice by se podle okolností mělo použít nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ([3]).

(73) V souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 byl konzultován evropský inspektor ochrany údajů, který vydal své stanovisko dne 14. června 2013 ([4]).

(74) Jelikož cíle této směrnice, totiž dosažení vysoké společné úrovně bezpečnosti sítí a informačních systémů 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.

(75) 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 a oblast působnosti

1. Touto směrnicí se stanoví opatření pro dosažení vysoké společné úrovně bezpečnosti sítí a informačních systémů v rámci Unie s cílem zlepšení fungování vnitřního trhu.

2. Za tímto účelem tato směrnice:

a) ukládá všem členským státům povinnost přijmout národní strategii pro bezpečnost sítí a informačních systémů;

b) ustavuje skupinu pro spolupráci, jejímž účelem je podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy a budovat vzájemnou důvěru;

c) ustavuje síť bezpečnostních týmů typu CSIRT (dále jen „síť CSIRT“), jejímž účelem je přispívat k budování důvěry mezi členskými státy a podporovat rychlou a účinnou operativní spolupráci;

([1]) Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, s. 31).
([2]) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).
([3]) Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (Úř. věst. L 145, 31.5.2001, s. 43).
([4]) Úř. věst. C 32, 4.2.2014, s. 19.

d) zavádí bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb;

e) ukládá členským státům povinnost určit vnitrostátní příslušné orgány, jednotná kontaktní místa a týmy CSIRT, jejichž úkoly budou souviset s bezpečností sítí a informačních systémů.

3. Bezpečnostní požadavky a požadavky na hlášení incidentů stanovené touto směrnicí se nevztahují na podniky podléhající požadavkům stanoveným v článcích 13a a 13b směrnice 2002/21/ES ani na poskytovatele služeb vytvářejících důvěru podléhající požadavkům stanoveným v článku 19 nařízení (EU) č. 910/2014.

4. Touto směrnicí nejsou dotčeny směrnice Rady 2008/114/ES ([1]) a směrnice Evropského parlamentu a Rady 2011/93/EU ([2]) a 2013/40/EU ([3]).

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

6. Touto směrnicí nejsou dotčena opatření, jež členské státy přijímají s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, zejména pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti.

7. Pokud odvětvový právní akt Unie vyžaduje, aby provozovatelé základních služeb nebo poskytovatelé digitálních služeb zajistili bezpečnost svých sítí a informačních systémů nebo aby hlásili incidenty, použijí se požadavky tohoto odvětvového právního aktu Unie, pokud jsou tyto požadavky co do účinku přinejmenším rovnocenné povinnostem stanoveným v této směrnici.

Článek 2

Zpracování osobních údajů

1. Zpracování osobních údajů podle této směrnice se provádí v souladu se směrnicí 95/46/ES.

2. Zpracování osobních údajů, které provádějí orgány a instituce Unie podle této směrnice, se provádí v souladu s nařízením (ES) č. 45/2001.

Článek 3

Minimální harmonizace

Aniž je dotčen čl. 16 odst. 10 a aniž jsou dotčeny povinnosti členských států podle práva Unie, mohou členské státy přijímat nebo ponechat v platnosti ustanovení, jejichž cílem je dosáhnout vyšší úrovně bezpečnosti sítí a informačních systémů.

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

([2]) 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).

([3]) 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 4

Definice

Pro účely této směrnice se rozumí:

1) „sítí a informačním systémem“:

   a) síť elektronických komunikací ve smyslu čl. 2 odst. a) směrnice 2002/21/ES;

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

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

2) „bezpečností sítí a informačních systémů“ schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné;

3) „národní strategií pro bezpečnost sítí a informačních systémů“ rámec vymezující strategické cíle a priority v oblasti bezpečnosti sítí a informačních systémů na vnitrostátní úrovni;

4) „provozovatelem základních služeb“ veřejný nebo soukromý subjekt, jehož druh je uveden v příloze II a jenž splňuje kritéria stanovené v čl. 5 odst. 2;

5) „digitální službou“ služba ve smyslu čl. 1 odst. 1 písm. b) směrnice Evropského parlamentu a Rady (EU) 2015/1535 ([1]), jejíž druh je uveden v příloze III;

6) „poskytovatelem digitálních služeb“ jakákoli právnická osoba poskytující digitální službu;

7) „incidentem“ jakákoliv událost, která má reálný negativní dopad na bezpečnost sítí a informačních systémů;

8) „řešením incidentu“ veškeré postupy, které pomáhají incident odhalit, analyzovat, zamezit jeho šíření a reagovat na něj;

9) „rizikem“ jakákoli v přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů;

10) „zástupcem“ fyzická či právnická osoba usazená v Unii, výslovně pověřená, aby jednala jménem poskytovatele digitálních služeb, jenž v Unii usazen není, přičemž vnitrostátní příslušný orgán nebo tým CSIRT může se zástupcem jednat namísto daného poskytovatele digitálních služeb, pokud jde o povinnosti poskytovatele digitálních služeb vyplývající z této směrnice;

11) „normou“ norma ve smyslu čl. 2 bodu 1 nařízení (EU) č. 1025/2012;

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

13) „výměnným uzlem internetu (IXP)“ síťové zařízení umožňující propojení více než dvou nezávislých 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;

14) „systémem doménových jmen (DNS)“ hierarchický distribuovaný systém doménových jmen v rámci sítě adresující dotazy na doménová jména;

([1]) 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).

15) „poskytovatelem služeb DNS“ subjekt poskytující na internetu služby DNS;

16) „registrem internetových domén nejvyšší úrovně“ subjekt, který spravuje a provozuje registraci internetových doménových jmen pod určitou doménou nejvyšší úrovně;

17) „on-line tržištěm“ digitální služba, která spotřebitelům ve smyslu čl. 4 odst. 1 písm. a) směrnice Evropského parlamentu a Rady 2013/11/EU ([1]) a obchodníkům ve smyslu čl. 4 odst. 1 písm. b) uvedené směrnice, umožňuje uzavírat s obchodníky on-line smlouvy o prodeji a o poskytnutí služeb, a to prostřednictvím internetových stránek on-line tržiště nebo prostřednictvím internetových stránek obchodníka, jež využívají výpočetních služeb poskytovaných on-line tržištěm;

18) „internetovým vyhledávačem“ digitální služba, která uživatelům umožňuje provádět vyhledávání v zásadě na všech internetových stránkách nebo na internetových stránkách v určitém jazyce, a to na základě dotazu na jakékoli téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem;

19) „službou cloud computingu“ digitální služba umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které je možno sdílet.

Článek 5

Určování provozovatelů základních služeb

1. Do 9. listopadu 2018 členské státy v každém odvětví a pododvětví uvedeném v příloze II určí provozovatele základních služeb usazené na jejich území.

2. Kritéria pro určení provozovatele základních služeb podle čl. 4 bodu 4 jsou tato:

a) subjekt poskytuje službu, která je základní z hlediska zachování kritických společenských nebo ekonomických činností;

b) poskytování dotyčné služby je závislé na sítích a informačních systémech a

c) incident by vedl k významnému narušení poskytování této služby.

3. Pro účely odstavce 1 sestaví každý členský stát seznam služeb uvedených v odst. 2 písm. a).

4. V případě, že jeden subjekt poskytuje službu uvedenou v odst. 2 písm. a) ve dvou či více členských státech, zahájí tyto členské státy pro účely odstavce 1 vzájemné konzultace. Tyto konzultace proběhnou před přijetím rozhodnutí o určení provozovatele základní služby.

5. Seznam určených provozovatelů základních služeb členské státy pravidelně, a to alespoň každé dva roky ode dne 9. května 2018, přezkoumávají a v případě potřeby jej aktualizují.

6. Úlohou skupiny pro spolupráci je v souladu s úkoly uvedenými v článku 11 podporovat členské státy, aby v rámci procesu určování provozovatelů základních služeb uplatňovaly konzistentní přístup.

7. Pro účely přezkumu uvedeného v článku 23 členské státy do 9. listopadu 2018 a poté každé dva roky předkládají Komisi informace, jež Komise potřebuje k hodnocení provádění této směrnice, zejména z hlediska konzistentnosti přístupů členských států v otázce určování provozovatelů základních služeb. Tyto informace zahrnují alespoň:

a) vnitrostátní opatření umožňující určení provozovatelů základních služeb;

([1]) Směrnice Evropského parlamentu a Rady 2013/11/EU ze dne 21. května 2013 o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů) (Úř. věst. L 165, 18.6.2013, s.63).

b) seznam služeb uvedený v odstavci 3;

c) počet provozovatelů základních služeb určených v každém odvětví podle přílohy II a jejich význam ve vztahu k dotyčnému odvětví;

d) mezní hodnoty, existují-li, pro stanovení příslušné zásobovací úrovně podle počtu uživatelů závislých na dané službě podle čl. 6 odst. 1 písm. a) nebo významu konkrétního provozovatele základních služeb podle čl. 6 odst. 1 písm. f).

V zájmu větší srovnatelnosti poskytovaných informací může Komise s maximálním ohledem na stanovisko agentury ENISA přijmout patřičné technické pokyny upravující parametry informací uvedených v tomto odstavci.

Článek 6

Významné narušení

1. Při určování významnosti narušení podle čl. 5 odst. 2 písm. c) členské státy zváží alespoň tyto okolnosti působící napříč odvětvími:

a) počet uživatelů, kteří jsou závislí na službě poskytované daným subjektem;

b) závislost dalších odvětví podle přílohy II na službě poskytované daným subjektem;

c) možný dopad incidentů, pokud jde o jejich intenzitu a délku trvání, na ekonomické a společenské činnosti nebo na veřejnou bezpečnost;

d) podíl daného subjektu na trhu;

e) zeměpisný rozsah oblasti, která by mohla být incidentem dotčena;

f) důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.

2. Při posuzování toho, zda by incident vedl k významnému narušení, členské státy případně zváží rovněž okolnosti specifické pro jednotlivá odvětví.

KAPITOLA II

NÁRODNÍ RÁMCE PRO BEZPEČNOST SÍTÍ A INFORMAČNÍCH SYSTÉMŮ

Článek 7

Národní strategie pro bezpečnost sítí a informačních systémů

1. Každý členský stát přijme národní strategii pro bezpečnost sítí a informačních systémů, ve které vymezí strategické cíle a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně bezpečnosti sítí a informačních systémů a udržovat ji a která pokrývá alespoň odvětví uvedená v příloze II a služby uvedené v příloze III. Předmětem národní strategie pro bezpečnost sítí a informačních systémů jsou především následující cíle a opatření:

a) cíle a priority národní strategie pro bezpečnost sítí a informačních systémů;

b) správní rámec pro naplnění cílů a priorit vnitrostátní strategie pro bezpečnost sítí a informačních systémů, včetně úlohy a povinností vládních orgánů a dalších relevantních subjektů;

c) stanovení opatření týkajících se připravenosti, reakce a obnovy, včetně spolupráce veřejného a soukromého sektoru;

d) vymezení vzdělávacích, informačních a školicích programů souvisejících s vnitrostátní strategií pro bezpečnost sítí a informačních systémů;

e) vymezení výzkumných a rozvojových plánů souvisejících s národní strategií pro bezpečnost sítí a informačních systémů;

f) plán posouzení rizik pro určení rizik;

g) seznam různých subjektů zapojených do provádění národní strategie pro bezpečnost sítí a informačních systémů.

2. Členské státy si mohou při vypracovávání národních strategií pro bezpečnost sítí a informačních systémů vyžádat pomoc agentury ENISA.

3. Členské státy oznámí své národní strategie pro bezpečnost sítí a informačních systémů Komisi do tří měsíců od jejich přijetí. Členské státy mohou z oznámení vyloučit prvky strategie, které souvisejí s národní bezpečností.

Článek 8

Vnitrostátní příslušné orgány a jednotné kontaktní místo

1. Každý členský stát určí jeden nebo více vnitrostátních příslušných orgánů v oblasti bezpečnosti sítí a informačních systémů (dále jen „příslušný orgán“) alespoň pro odvětví podle přílohy II a služby podle přílohy III. Členské státy mohou tuto úlohu svěřit již existujícímu orgánu nebo orgánům.

2. Příslušné orgány dohlížejí na provádění této směrnice na vnitrostátní úrovni.

3. Každý členský stát určí vnitrostátní jednotné kontaktní místo pro oblast bezpečnosti sítí a informačních systémů (dále jen „jednotné kontaktní místo“). Členské státy mohou tuto úlohu svěřit již existujícímu orgánu. Určí-li členský stát pouze jeden příslušný orgán, je tento orgán rovněž jednotným kontaktním místem.

4. Jednotné kontaktní místo plní styčnou funkci s cílem zajistit přeshraniční spolupráci orgánů členských států s relevantními orgány v jiných členských státech a se skupinou pro spolupráci uvedenou v článku 11 a sítí CSIRT uvedenou v článku 12.

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

6. Příslušné orgány a jednotné kontaktní místo v náležitých případech a v souladu s vnitrostátními právními předpisy konzultují vnitrostátní příslušné orgány pro vymáhání práva a vnitrostátní orgány pro ochranu osobních údajů a spolupracují s nimi.

7. Každý členský stát Komisi neprodleně oznámí určení příslušného orgánu a jednotného kontaktního místa, jejich úkoly a jakékoliv změny, které se jich týkají. Každý členský stát zveřejní určení příslušného orgánu a jednotného kontaktního místa. 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 (Computer Security Incident Response Team; dále jen „tým CSIRT"), které pokrývají alespoň odvětví uvedená v příloze II a služby uvedené v příloze III, které jsou odpovědné za zvládání rizik a řešení incidentů podle řádně vymezených postupů a splňují požadavky uvedené v příloze I bodě 1. Tým CSIRT může být zřízen v rámci příslušného orgánu.

2. Členské státy zajistí, aby týmy CSIRT měly odpovídající zdroje pro účinné plnění jejich úkolů podle přílohy I bodu 2.

Členské státy zajistí, aby jejich týmy CSIRT v rámci sítě CSIRT uvedené v článku 12 účelně, účinně a spolehlivě spolupracovaly.

3. Členské státy zajistí, aby jejich týmy CSIRT měly přístup k odpovídající, bezpečné a odolné komunikační a informační infrastruktuře na vnitrostátní úrovni.

4. Členské státy oznámí Komisi oblast působnosti svých týmů CSIRT, jakož i hlavní prvky jejich postupu při řešení incidentů.

5. Členské státy si mohou při budování týmů CSIRT vyžádat pomoc agentury ENISA.

Článek 10

Spolupráce na vnitrostátní úrovni

1. Pokud existují odděleně, příslušný orgán, jednotné kontaktní místo a týmy CSIRT téhož členského státu vzájemně spolupracují při plnění povinností stanovených touto směrnicí.

2. Členské státy zajistí, aby příslušné orgány nebo týmy CSIRT obdržely hlášení o incidentech podaná podle této směrnice. Pokud členský stát rozhodne, že týmy CSIRT nemají hlášení přijímat, bude týmům CSIRT v rozsahu nezbytném pro plnění jejich úkolů povolen přístup k údajům o incidentech hlášených provozovateli základních služeb podle čl. 14 odst. 3 a 5 nebo poskytovateli digitálních služeb podle čl. 16 odst. 3 a 6.

3. Členské státy zajistí, aby příslušné orgány nebo týmy CSIRT informovaly jednotná kontaktní místa o hlášeních incidentů podaných podle této směrnice.

Do dne 9. srpna 2018 a poté každý rok předloží jednotné kontaktní místo skupině pro spolupráci souhrnnou zprávu o obdržených hlášeních včetně jejich počtu a povahy ohlášených incidentů, jakož i přijatých opatření ve smyslu čl. 14 odst. 3 a 5 a čl. 16 odst. 3 a 6.

KAPITOLA III

SPOLUPRÁCE

Článek 11

Skupina pro spolupráci

1. S cílem podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy a budovat důvěru a v zájmu dosažení vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii se zřizuje skupina pro spolupráci.

Skupina pro spolupráci vykonává své úkoly na základě dvouletých pracovních programů, jak je uvedeno v odst. 3 druhém pododstavci.

2. Skupina pro spolupráci je tvořena zástupci členských států, Komise a agentury ENISA.

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

Služby sekretariátu zajistí Komise.

3. Skupina pro spolupráci má tyto úkoly:

a) poskytuje strategické vedení pro činnosti sítě CSIRT zřízené podle článku 12;

b) zajišťuje výměnu osvědčených postupů, pokud jde o výměnu informací souvisejících s hlášením incidentů podle čl. 14 odst. 3 a 5 a čl. 16 odst. 3 a 6;

c) zajišťuje výměnu osvědčených postupů mezi členskými státy a ve spolupráci s agenturou ENISA napomáhá členským státům při budování kapacit v oblasti zajišťování bezpečnosti sítí a informačních systémů;

d) jedná o schopnostech a připravenosti členských států a na dobrovolném základě hodnotí národní strategie pro bezpečnost sítí a informačních systémů a účinnost týmů CSIRT a identifikuje osvědčené postupy;

e) zajišťuje výměnu informací a osvědčených postupů v oblasti zvyšování osvěty a odborné přípravy;

f) zajišťuje výměnu informací a osvědčených postupů v oblasti výzkumu a vývoje, pokud jde o oblast bezpečnosti sítí a informačních systémů;

g) v náležitých případech zajišťuje výměnu zkušeností v záležitostech týkajících se bezpečnosti sítí a informačních systémů s příslušnými orgány, subjekty, úřady a agenturami Unie;

h) jedná o normách a specifikacích uvedených v článku 19 se zástupci příslušných evropských normalizačních organizací;

i) shromažďuje informace o osvědčených postupech, pokud jde o rizika a incidenty;

j) každoročně posuzuje souhrnné zprávy uvedené v čl. 10 odst. 3. druhém pododstavci;

k) jedná o práci vykonané ve vztahu k cvičením, vzdělávacím programům a odborné přípravě v oblasti bezpečnosti sítí a informačních systémů, včetně práce prováděné agenturou ENISA;

l) s pomocí agentury ENISA zajišťuje výměnu osvědčených postupů pro určování provozovatelů základních služeb členskými státy, a to rovněž ve vztahu k přeshraničním vazbám, souvisejících s riziky a incidenty;

m) jedná o způsobech hlášení incidentů podle článků 14 a 16.

Do dne 9. února 2018 a poté každé dva roky stanoví skupina pro spolupráci pracovní program zahrnující opatření, která mají být přijata pro účely plnění jejích cílů a úkolů a která odpovídají cílům této směrnice.

4. Pro účely přezkumu podle článku 23 vypracuje skupina pro spolupráci do dne 9. srpna 2018 a poté každých osmnáct měsíců zprávu, v níž posoudí zkušenosti získané při strategické spolupráci vyvíjené podle tohoto článku.

5. Komise přijme prováděcí akty, kterými stanoví procesní pravidla nezbytná pro fungování skupiny pro spolupráci. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 22 odst. 2.

Komise předloží výboru uvedenému v čl. 22 odst. 1 první návrh prováděcího aktu podle prvního pododstavce do 9. února 2017.

Článek 12

Síť CSIRT

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

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

3. Síť CSIRT má tyto úkoly:

a) zajišťuje výměnu informací o službách, činnostech a schopnostech pro spolupráci nabízených týmy CSIRT;

b) na žádost zástupce týmu CSIRT z členského státu potenciálně zasaženého incidentem zajišťuje výměnu jiných než obchodně citlivých informací týkajících se takového incidentu a souvisejících rizik a jednání o nich; tým CSIRT z členského státu však může odmítnout účastnit se tohoto jednání, pokud by tím mohlo být ohroženo vyšetřování daného incidentu;

c) zajišťuje výměnu a dobrovolné zpřístupnění jiných než důvěrných informací o jednotlivých incidentech;

d) na žádost zástupce týmu CSIRT z některého členského státu jedná a pokud možno určuje koordinovanou reakci na incident, který byl zjištěn v oblasti spadající do pravomoci tohoto členského státu;

e) poskytuje členským státům podporu při řešení přeshraničních incidentů na základě jejich dobrovolné vzájemné pomoci;

f) projednává, hledá a vymezuje další formy operativní spolupráce, a to mimo jiné ve vztahu:

   i) ke kategoriím rizik a incidentů,

   ii) k včasným varováním,

   iii) k vzájemné pomoci,

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

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

h) jedná o poznatcích získaných ze cvičení týkajících se bezpečnosti sítí a informačních systémů, včetně cvičení pořádaných agenturou ENISA;

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

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

4. Pro účely přezkumu podle článku 23 vypracuje síť CSIRT do 9. srpna 2018 a poté každých osmnáct měsíců zprávu, v níž posoudí zkušenosti získané při operativní spolupráci vyvíjené podle tohoto článku a uvede závěry a doporučení. Tato zpráva bude rovněž předložena skupině pro spolupráci.

5. Síť CSIRT přijme svůj jednací řád.

Článek 13

Mezinárodní spolupráce

Unie může v souladu s článkem 218 Smlouvy o fungování EU uzavírat mezinárodní dohody se třetími zeměmi nebo mezinárodními organizacemi s cílem umožnit a upravit jejich účast na některých činnostech skupiny pro spolupráci. Takové dohody zohledňují nutnost zajistit patřičnou ochranu údajů.

KAPITOLA IV

BEZPEČNOST SÍTÍ A INFORMAČNÍCH SYSTÉMŮ PROVOZOVATELŮ ZÁKLADNÍCH SLUŽEB

Článek 14

Bezpečnostní požadavky a hlášení incidentů

1. Členské státy zajistí, aby jejich provozovatelé základních služeb přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež provozovatelé používají pro výkon své činnosti. S ohledem na nejnovější technický vývoj tato opatření musí zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika.

2. Členské státy zajistí, aby provozovatelé základních služeb přijali vhodná opatření k předcházení incidentům ovlivňujícím bezpečnost sítí a informačních systémů používaných pro poskytování těchto základních služeb a k minimalizaci jejich dopadu, aby byla zajištěna kontinuita těchto služeb.

3. Členské státy zajistí, aby provozovatelé základních služeb hlásili příslušnému orgánu nebo týmu CSIRT bez zbytečného prodlení incidenty se závažným dopadem na kontinuitu základních služeb, které poskytují. Hlášení zahrnuje informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit případný přeshraniční dopad daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti.

4. Při posuzování významnosti dopadu incidentu se zohlední zejména tyto parametry:

a) počet uživatelů postižených narušením základní služby;

b) délka trvání incidentu;

c) zeměpisný rozsah oblasti dotčené incidentem.

5. Na základě informací, které provozovatel základních služeb poskytl v hlášení, informuje příslušný orgán nebo tým CSIRT další dotčený členský stát nebo dotčené členské státy, pokud má incident významný dopad na kontinuitu základních služeb v tomto členském státě nebo členských státech. Příslušný orgán nebo tým CSIRT přitom v souladu s právem Unie nebo vnitrostátními právními předpisy, které jsou v souladu s právem Unie, zachová bezpečnost a obchodní zájmy provozovatele základních služeb, jakož i důvěrnost informací poskytnutých v jeho hlášení.

Pokud to okolnosti dovolují, příslušný orgán nebo tým CSIRT poskytne ohlašujícímu provozovateli základních služeb relevantní informace týkající se následných opatření přijatých na základě jeho hlášení, například informace, které by mohly podpořit účinné řešení incidentu.

Na žádost příslušného orgánu nebo týmu CSIRT postoupí jednotné kontaktní místo hlášení uvedená v prvním pododstavci jednotným kontaktním místům dalších dotčených členských států.

6. Pokud je pro zamezení incidentu nebo zvládání probíhajícího incidentu nezbytná informovanost veřejnosti, může příslušný orgán nebo tým CSIRT po konzultaci ohlašujícího provozovatele základních služeb informovat o jednotlivých incidentech veřejnost.

7. Příslušné orgány jednající společně v rámci skupiny pro spolupráci mohou vypracovat a přijmout pokyny týkající se okolností, za nichž jsou provozovatelé základních služeb povinni hlásit incidenty, včetně parametrů pro určení významnosti dopadu daného incidentu, jak je uvedeno v odstavci 4.

Článek 15

Provádění a vymáhání

1. Členské státy zajistí, aby příslušné orgány měly všechny nezbytné pravomoci a prostředky pro posouzení toho, zda provozovatelé základních služeb dodržují své povinnosti podle článku 14, a s tím souvisejících důsledků pro bezpečnost sítí a informačních systémů.

2. Členské státy zajistí, aby příslušné orgány měly pravomoci a prostředky nezbytné k tomu, aby mohly od provozovatelů základních služeb požadovat poskytnutí:

a) informací nezbytných pro posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky;

b) dokladů o účinném provádění bezpečnostních politik, jako jsou výsledky bezpečnostního auditu provedeného příslušným orgánem nebo kvalifikovaným auditorem, a v případě kvalifikovaného auditora, aby mohlo být požadováno předložení těchto výsledků včetně podpůrných dokladů příslušnému orgánu.

Pokud příslušný orgán žádá o poskytnutí těchto informací nebo dokladů, uvede účel své žádosti a upřesní informace, které jsou požadovány.

3. V návaznosti na posouzení poskytnutých informací nebo výsledků bezpečnostních auditů uvedených v odstavci 2 může příslušný orgán vydat provozovatelům základních služeb závazné pokyny k nápravě zjištěných nedostatků.

4. Při řešení incidentů, v jejichž důsledku došlo k porušení ochrany osobních údajů, příslušný orgán úzce spolupracuje s orgány pro ochranu osobních údajů.

KAPITOLA V

BEZPEČNOST SÍTÍ A INFORMAČNÍCH SYSTÉMŮ POSKYTOVATELŮ DIGITÁLNÍCH SLUŽEB

Článek 16

Bezpečnostní požadavky a hlášení incidentů

1. Členské státy zajistí, aby poskytovatelé digitálních služeb určili a přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž jsou vystaveny sítě a informační systémy, které využívají v souvislosti s nabízením služeb uvedených v příloze III v rámci Unie. S ohledem na nejnovější technický vývoj tato opatření musí zajišťovat úroveň bezpečnosti sítí a informačních systémů odpovídající existující míře rizika, přičemž zohledňují:

a) bezpečnost systémů a zařízení;

b) řešení incidentů;

c) řízení kontinuity provozu;

d) monitorování, audity a testování;

e) soulad s mezinárodními normami.

2. Členské státy zajistí, aby poskytovatelé digitálních služeb přijali opatření k předcházení incidentům ovlivňujícím bezpečnost jejich sítí a informačních systémů a k minimalizaci dopadu těchto incidentů na služby uvedené v příloze III, které jsou nabízeny v rámci Unie, aby byla zajištěna kontinuita těchto služeb.

3. Členské státy zajistí, aby poskytovatelé digitálních služeb bez zbytečného odkladu hlásili příslušnému orgánu nebo týmu CSIRT incidenty, které mají významný dopad na poskytování služby uvedené v příloze III, kterou nabízejí v rámci Unie. Hlášení musí obsahovat takové informace, které příslušnému orgánu nebo týmu CSIRT umožní posoudit významnost případného přeshraničního dopadu daného incidentu. Ohlášení nezakládá u oznamující strany vyšší míru právní odpovědnosti.

4. Při posuzování toho, zda je dopad incidentu významný, se zohlední zejména tyto parametry:

a) počet uživatelů postižených incidentem, zejména těch uživatelů, kteří na službu spoléhají při poskytování vlastních služeb;

b) délka trvání incidentu;

c) zeměpisný rozsah oblasti dotčené incidentem;

d) rozsah, v jakém bylo narušeno fungování služby;

e) rozsah dopadu na společenské a ekonomické činnosti.

Ohlášení incidentu je povinné, pouze pokud má poskytovatel digitální služby přístup k informacím, které jsou nezbytné k posouzení dopadu incidentu na základě parametrů uvedených v prvním pododstavci.

5. Pokud provozovatel základních služeb spoléhá na vnějšího poskytovatele digitálních služeb při poskytování služby, která je základní z hlediska zachování kritických společenských a ekonomických činností, ohlásí provozovatel základních služeb jakýkoli významný dopad na kontinuitu těchto základních služeb způsobený incidentem, jímž byl poskytovatel digitálních služeb postižen.

6. Tam, kde je to vhodné, a zejména pokud se incident podle odstavce 3 týká dvou nebo více členských států, informuje příslušný orgán nebo tým CSIRT, jimž byl incident ohlášen, ostatní dotčené členské státy. 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 poskytovatele digitálních služeb, jakož i důvěrnost poskytnutých informací.

7. V případě, že informovanost veřejnosti je nezbytná pro předejití incidentu nebo ke zvládání probíhajícího incidentu, nebo pokud je zveřejnění incidentu ve veřejném zájmu z jiných důvodů, může příslušný orgán nebo tým CSIRT, jimž byl incident ohlášen, popřípadě příslušný orgán nebo tým CSIRT jiných dotčených členských států po konzultaci dotčeného poskytovatele digitálních služeb informovat o jednotlivých incidentech veřejnost nebo nařídit poskytovateli digitálních služeb, aby tak učinil.

8. Komise přijme prováděcí akty, kterými blíže upřesní prvky uvedené v odstavci 1 a parametry uvedené v odstavci 4 tohoto článku. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 22 odst. 2 do 9. srpna 2017.

9. Komise může přijmout prováděcí akty, kterými stanoví formáty a postupy týkající se požadavků na hlášení incidentů. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 22 odst. 2.

10. Aniž je dotčen čl. 1 odst. 6, členské státy neuloží poskytovatelům digitálních služeb žádné další bezpečnostní požadavky či požadavky na hlášení incidentů.

11. Kapitola V se nevztahuje na mikropodniky a malé podniky ve smyslu doporučení Komise 2003/361/ES ([1]).

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

Článek 17

Provádění a vymáhání

1. Členské státy zajistí, aby příslušné orgány v případě potřeby přijaly opatření v rámci následné kontroly, mají-li důkazy o tom, že poskytovatel digitálních služeb nesplňuje požadavky stanovené v článku 16. Takové důkazy mohou být předloženy příslušným orgánem jiného členského státu, v němž je služba poskytována.

2. Pro účely odstavce 1 musí mít příslušné orgány nezbytné pravomoci a prostředky, aby mohly od poskytovatelů digitálních služeb požadovat:

a) poskytnutí informací potřebných k posouzení bezpečnosti jejich sítí a informačních systémů, včetně existující bezpečnostní politiky;

b) nápravu případného neplnění požadavků stanovených v článku 16.

3. Pokud je poskytovatel digitálních služeb primárně usazen nebo má zástupce v jednom členském státě, ale jeho sítě a informační systémy se nacházejí v jednom či více jiných členských státech, příslušný orgán členského státu, v němž je poskytovatel primárně usazen nebo v němž má svého zástupce, a příslušné orgány těchto jiných členských států podle potřeby spolupracují a jsou si navzájem nápomocny. Taková pomoc a spolupráce může zahrnovat výměny informací mezi dotčenými příslušnými orgány a žádosti o přijetí kontrolních opatření podle odstavce 2.

Článek 18

Pravomoc a územní působnost

1. Pro účely této směrnice se má za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je primárně usazen. Má-li poskytovatel digitálních služeb v některém členském státě své sídlo, má se za to, že je v tomto členském státě rovněž primárně usazen.

2. Poskytovatel digitálních služeb, který není v Unii usazen, ale nabízí v Unii služby uvedené v příloze III, určí svého zástupce v Unii. Tento zástupce musí být usazen v jednom ze členských států, v němž jsou služby nabízeny. Má se za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je zástupce usazen.

3. Určí-li poskytovatel digitálních služeb svého zástupce, není tím dotčena možnost zahájit právní řízení proti samotnému poskytovateli digitálních služeb.

KAPITOLA VI

STANDARDIZACE A DOBROVOLNÉ HLÁŠENÍ

Článek 19

Standardizace

1. Členské státy za účelem harmonizovaného provádění čl. 14 odst. 1 a 2 a čl. 16 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 20

Dobrovolné hlášení incidentů

1. Aniž je dotčen článek 3, mohou subjekty, které nebyly určeny jako provozovatelé základních služeb a které nejsou poskytovateli digitálních služeb, dobrovolně hlásit incidenty se závažným dopadem na kontinuitu služeb, které poskytují.

2. Při zpracování hlášení postupují členské státy postupem stanoveným v článku 14. Členské státy mohou dát přednost zpracování povinných hlášení před dobrovolnými hlášeními. Dobrovolná hlášení se zpracují pouze za podmínky, že jejich zpracování nepředstavuje pro dotčené členské státy nepřiměřenou nebo nepatřičnou zátěž.

Na základě dobrovolného ohlášení nesmí být oznamujícímu subjektu uložena žádná povinnost, která by mu nebyla uložena, kdyby toto ohlášení neučinil.

KAPITOLA VII

ZÁVĚREČNÁ USTANOVENÍ

Článek 21

Sankce

Členské státy stanoví sankce za porušení vnitrostátních právních předpisů přijatých podle této směrnice a přijmou veškerá opatření nezbytná k zajištění jejich uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující. Členské státy oznámí takto stanovené sankce a daná opatření Komisi do dne 9. května 2018 a neprodleně jí oznámí všechny následné změny, jež se těchto ustanovení a opatření týkají.

Článek 22

Postup projednávání ve výboru

1. Komisi je nápomocen Výbor pro bezpečnost sítí a informačních systémů. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

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

Článek 23

Přezkum

1. Komise do 9. května 2019 předloží Evropskému parlamentu a Radě zprávu, v níž vyhodnotí, zda jsou přístupy členských států, pokud jde o proces určování provozovatelů základních služeb, konzistentní.

2. Komise pravidelně přezkoumává fungování této směrnice a podává zprávu Evropskému parlamentu a Radě. Za tímto účelem a s cílem dále rozvíjet strategickou a operativní spolupráci Komise zohlední zprávy skupiny pro spolupráci a sítě CSIRT, pokud jde o zkušenosti získané na strategické a operativní úrovni. Ve svém přezkumu Komise rovněž zhodnotí seznamy obsažené v přílohách II a III a konzistentnost ve vztahu k procesu určování provozovatelů základních služeb a služeb v odvětvích uvedených v příloze II. První zprávu předloží do dne 9. května 2021.

Článek 24

Přechodná opatření

1. Aniž je dotčen článek 25, a s cílem poskytnout členským států další možnosti pro vhodnou spolupráci v období provádění začne skupina pro spolupráci plnit své úkoly podle čl. 11 odst. 3 a síť CSIRT podle čl. 12 odst. 3 nejpozději dne 9. února 2017.

2. V období od 9. února 2017 do 9. listopadu 2018 a za účelem podpory členských států při zaujímání konzistentního přístupu v procesu určování provozovatelů základních služeb, jedná skupina pro spolupráci o pokroku, podstatě a druhu vnitrostátních opatření, která umožní určit provozovatele základních služeb v konkrétním odvětví v souladu s kritérii stanovenými v článcích 5 a 6. Skupina pro spolupráci rovněž na žádost kteréhokoli členského státu projedná jeho návrhy konkrétních vnitrostátních opatření umožňující určit provozovatele základních služeb v konkrétním odvětví v souladu s kritérii stanovenými v článcích 5 a 6.

3. Do dne 9. února 2017 a pro účely tohoto článku členské státy zajistí náležité zastoupení ve skupině pro spolupráci a v síti CSIRT.

Článek 25

Provedení ve vnitrostátním právu

1. Členské státy do 9. května 2018 přijmou a zveřejní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí. Znění těchto předpisů neprodleně sdělí Komisi.

Použijí tyto předpisy ode dne 10. května 2018.

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.

2. Členské státy sdělí Komisi znění hlavních ustanovení vnitrostátních právních předpisů, které přijmou v oblasti působnosti této směrnice.

Článek 26

Vstup v platnost

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

Článek 27

Určení

Tato směrnice je určena členským státům.

Ve Štrasburku dne 6. července 2016.

Za Evropský parlament	*Za Radu*
předseda	*předseda*
M. SCHULZ	I. KORČOK

PŘÍLOHA I

ÚKOLY A POŽADAVKY NA BEZPEČNOSTNÍ TÝMY TYPU CSIRT

Úkoly a požadavky na týmy CSIRT jsou přiměřeně a jasně vymezeny a jsou podpořeny vnitrostátními pravidly a právními předpisy. Zahrnují tyto povinnosti a úkoly:

1) Požadavky na týmy CSIRT

   a) Týmy CSIRT zajistí, aby v jejich komunikačních službách nebyla žádná kritická místa (tzv. single points of failure), a tyto služby tak byly široce dostupné, a disponují několika způsoby, jimiž budou kontaktovat ostatní a jimiž bude možné kontaktovat je, a to kdykoli. Komunikační kanály musí být navíc jasně specifikované a spolupracujícím partnerům a subjektům spadajícím do působnosti týmů dobře známé.

   b) Pracoviště týmů CSIRT a jejich podpůrné informační systémy se nacházejí na bezpečném místě.

   c) Kontinuita činnosti:

      i) týmy CSIRT jsou vybaveny vhodnými systémy řízení a směrování požadavků, které usnadní předávání,

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

      iii) týmy CSIRT musí pracovat s infrastrukturou, jejíž kontinuita je zaručena. Za tímto účelem musí být k dispozici záložní systémy a pracoviště,

   d) týmy CSIRT musí mít možnost účastnit se mezinárodních sítí pro spolupráci, pokud chtějí být jejich součástí.

2) Úkoly týmů CSIRT

   a) Úkoly týmů CSIRT zahrnují alespoň:

      i) monitorování incidentů na vnitrostátní úrovni,

      ii) vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám,

      iii) reakce na incidenty,

      iv) poskytování dynamické analýzy rizik a incidentů a přehledu o situaci,

      v) účast v síti CSIRT.

   b) Týmy CSIRT naváží spolupráci se soukromým sektorem.

   c) V zájmu usnadnění spolupráce týmy CSIRT prosazují přijetí a používání společných či standardních postupů v oblasti:

      i) řešení incidentů a rizik,

      ii) klasifikace incidentů, rizik a informací.

PŘÍLOHA II

DRUHY SUBJEKTŮ PRO ÚČELY ČL. 4 BODU 4

Odvětví	Pododvětví	Druh subjektu
1. Energetika	a) elektřina	— elektroenergetické podniky ve smyslu čl. 2 bodu 35 směrnice Evropského parlamentu a Rady 2009/72/ES ([1]), které zastávají funkci „dodávky“ ve smyslu čl. 2 bodu 19 uvedené směrnice
		— provozovatelé distribuční soustavy ve smyslu čl. 2 bodu 6 směrnice 2009/72/ES
		— provozovatelé přenosové soustavy ve smyslu čl. 2 bodu 4 směrnice 2009/72/ES
	b) ropa	— provozovatelé ropovodů
		— provozovatelé zařízení na těžbu, rafinaci a zpracování ropy a skladovacích a přenosových zařízení
	c) zemní plyn	— dodavatelské podniky ve smyslu čl. 2 bodu 8 směrnice Evropského parlamentu a Rady 2009/73/ES ([2])
		— provozovatelé distribuční soustavy ve smyslu čl. 2 bodu 6 směrnice 2009/73/ES
		— provozovatelé přepravní soustavy ve smyslu čl. 2 bodu 4 směrnice 2009/73/ES
		— provozovatelé skladovacího zařízení ve smyslu čl. 2 bodu 10 směrnice 2009/73/ES
		— provozovatelé zařízení LNG ve smyslu čl. 2 bodu 12 směrnice 2009/73/ES
		— plynárenské podniky ve smyslu čl. 2 bodu 1 směrnice 2009/73/ES
		— provozovatelé zařízení na rafinaci a zpracování zemního plynu
2. Doprava	a) letecká doprava	— letečtí dopravci ve smyslu čl. 3 bodu 4 nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ([3])
		— řídící orgány letiště ve smyslu čl. 2 bodu 2 směrnice Evropského parlamentu a Rady 2009/12/ES ([4]), letiště ve smyslu čl. 2 bodu 1 uvedené směrnice, včetně hlavních letišť uvedených v příloze II, části 2 nařízení Evropského parlamentu a Rady (EU) č. 1315/2013 ([5]); a subjekty provozující pomocná zařízení v rámci letišť

Odvětví	Pododvětví	Druh subjektu
		— provozovatelé kontroly řízení provozu poskytující služby řízení letového provozu ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (ES) č. 549/2004 ([6])
	b) železniční doprava	— provozovatelé infrastruktury ve smyslu čl. 3 bodu 2 směrnice Evropského parlamentu a Rady 2012/34/EU ([7])
		— 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 doprava	— společnosti vnitrozemské, námořní a pobřežní osobní a nákladní vodní dopravy, jak jsou vymezeny pro námořní dopravu v příloze I nařízení Evropského parlamentu a Rady (ES) č. 725/2004 ([8]), kromě jednotlivých plavidel provozovaných těmito podniky
		— řídící orgány přístavů ve smyslu čl. 3 bodu 1 směrnice Evropského parlamentu a Rady 2005/65/ES ([9]), včetně jejich přístavních zařízení ve smyslu čl. 2 bodu 11 nařízení (ES) č. 725/2004; a subjekty provozující díla a zařízení v rámci přístavů
		— provozovatelé služeb lodní dopravě ve smyslu čl. 3 písm. o) směrnice Evropského parlamentu a Rady 2002/59/ES ([10])
	d) silniční doprava	— silniční orgány ve smyslu čl. 2 bodu 12 nařízení Komise v přenesené pravomoci (EU) 2015/962 ([11]) odpovědné za kontrolu řízení provozu
		— provozovatelé inteligentních dopravních systémů ve smyslu čl. 4 bodu 1 směrnice Evropského parlamentu a Rady 2010/40/EU ([12])
3. Bankovnictví		úvěrové instituce ve smyslu čl. 4 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ([13])
4. Infrastruktura finančních trhů		— provozovatelé obchodních systémů ve smyslu čl. 4 bodu 24 směrnice Evropského parlamentu a Rady 2014/65/EU ([14])
		— ústřední protistrany ve smyslu čl. 2 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ([15])
5. Zdravotnictví	zdravotnická zařízení (včetně nemocnic a soukromých klinik)	poskytovatelé zdravotní péče ve smyslu čl. 3 písm. g) směrnice Evropského parlamentu a Rady 2011/24/EU ([16])

Odvětví	Pododvětví	Druh subjektu
6. Dodávky a rozvody pitné vody		dodavatelé a distributoři „vody určené k lidské spotřebě“ ve smyslu čl. 2 bodu 1 písm. a) směrnice Rady 98/83/ES ([17]), avšak kromě distributorů, pro něž je distribuce vody určené k lidské spotřebě pouze částí jejich obecné činnosti spočívající v distribuci komodit a zboží, která není považována za základní službu
7. Digitální infrastruktura		— výměnné uzly internetu (IXP)
		— poskytovatelé služeb systému doménových jmen (DNS)
		— registry internetových domén nejvyšší úrovně (TLD)

([1]) Směrnice Evropského parlamentu a Rady 2009/72/ES ze dne 13. července 2009 o společných pravidlech pro vnitřní trh s elektřinou a o zrušení směrnice 2003/54/ES (Úř. věst. L 211, 14.8.2009, s. 55).
([2]) 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).
([3]) 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).
([4]) 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).
([5]) 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).
([6]) 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).
([7]) 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).
([8]) 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).
([9]) 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.
([10]) 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).
([11]) 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).
([12]) 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).
([13]) 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).
([14]) 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)
([15]) 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).
([16]) 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).
([17]) 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).

PŘÍLOHA III

DRUHY DIGITÁLNÍCH SLUŽEB PRO ÚČELY ČL. 4 BODU 5.

1. On-line tržiště
2. Internetový vyhledávač
3. Služba cloud computingu

ISSN 1977-0626 (elektronické vydání)
ISSN 1725-5074 (papírové vydání)

Úřad pro publikace Evropské unie
2985 Lucemburk
LUCEMBURSKO

CS