I

(Legislatívne akty)

SMERNICE

SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/1148

zo 6. júla 2016

o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru ([1]),

konajúc v súlade s riadnym legislatívnym postupom ([2]),

keďže:

(1) Siete a informačné systémy a služby zohrávajú v spoločnosti kľúčovú úlohu. Ich spoľahlivosť a bezpečnosť sú nevyhnutné pre hospodárske a spoločenské činnosti, a najmä pre fungovanie vnútorného trhu.

(2) Rozsah, frekvencia a vplyv bezpečnostných incidentov sa zvyšujú a predstavujú významnú hrozbu pre fungovanie sietí a informačných systémov. Tieto systémy sa tiež môžu stať cieľom úmyselného škodlivého konania, účelom ktorého je poškodiť alebo prerušiť fungovanie týchto systémov. Takéto incidenty môžu zabraňovať realizácii ekonomických aktivít, spôsobovať značné finančné straty, narúšať dôveru používateľa a spôsobovať značné škody hospodárstvu Únie.

(3) Siete a informačné systémy, a predovšetkým internet zohrávajú zásadnú úlohu pri uľahčovaní cezhraničného pohybu tovaru, služieb a osôb. Z dôvodu tohto nadnárodného charakteru môžu mať zásadné narušenia týchto systémov, či už úmyselné, alebo nie, a bez ohľadu na to, kde k nim dôjde, dôsledky pre jednotlivé členské štáty aj Úniu ako celok. Bezpečnosť sietí a informačných systémov je preto základným predpokladom hladkého fungovania vnútorného trhu.

(4) Na základe značného pokroku, ktorý sa dosiahol v rámci Európskeho fóra členských štátov pri podpore diskusií a výmen týkajúcich sa osvedčených postupov vrátane formulácie zásad pre európsku spoluprácu pri kybernetickej kríze, by sa mala zriadiť skupina pre spoluprácu zložená zo zástupcov členských štátov, Komisie a Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ďalej len „agentúra ENISA“) na účely podpory a uľahčenia

([1]) Ú. v. EÚ C 271, 19.9.2013, s. 133.

([2]) Pozícia Európskeho parlamentu z 13. marca 2014 (zatiaľ neuverejnená v úradnom vestníku) a pozícia Rady v prvom čítaní zo 17. mája 2016 (zatiaľ neuverejnená v úradnom vestníku). Pozícia Európskeho parlamentu zo 6. júla 2016 (zatiaľ neuverejnená v úradnom vestníku).

strategickej spolupráce medzi členskými štátmi v oblasti bezpečnosti sietí a informačných systémov. Aby bola práca tejto skupiny efektívna a inkluzívna, všetky členské štáty musia disponovať minimálnymi spôsobilosťami a stratégiou, ktoré by na ich území zaistili vysokú úroveň bezpečnosti sietí a informačných systémov. Okrem toho by sa na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb mali uplatňovať bezpečnostné a oznamovacie požiadavky s cieľom podporovať kultúru riadenia rizika a zaistiť oznamovanie najzávažnejších incidentov.

(5) Existujúce spôsobilosti nie sú na zaručenie vysokej úrovne bezpečnosti sietí a informačných systémov v Únii postačujúce. V členských štátoch je rôzna úroveň pripravenosti, čo vedie k fragmentácii prístupov v Únii. To má za následok rozdielnu úroveň ochrany spotrebiteľov a podnikov a narúša celkovú úroveň bezpečnosti sietí a informačných systémov v rámci Únie. Neexistencia spoločných požiadaviek na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb zase znemožňuje, aby sa na úrovni Únie vytvoril globálny a účinný mechanizmus spolupráce. Univerzity a výskumné centrá zohrávajú rozhodujúcu úlohu pri podnecovaní výskumu, vývoja a inovácií v týchto oblastiach.

(6) Účinné reagovanie na výzvy, pokiaľ ide o bezpečnosť sietí a informačných systémov, si preto vyžaduje komplexný prístup na úrovni Únie, ktorý by sa vzťahoval na spoločné minimálne požiadavky na budovanie kapacít a plánovanie, výmenu informácií, spoluprácu a spoločné bezpečnostné požiadavky pre prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb. Prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb sa však nebráni uplatňovať prísnejšie bezpečnostné opatrenia, než sú opatrenia stanovené v tejto smernici.

(7) Táto smernica by sa v záujme obsiahnutia všetkých relevantných incidentov a rizík mala uplatňovať tak na prevádzkovateľov základných služieb, ako aj poskytovateľov digitálnych služieb. Povinnosti vzťahujúce sa na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb by sa však nemali uplatňovať na podniky poskytujúce verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby v zmysle smernice Európskeho parlamentu a Rady 2002/21/ES ([1]), ktoré podliehajú osobitným požiadavkám týkajúcim sa bezpečnosti a integrity stanoveným v uvedenej smernici, ani by sa nemali uplatňovať na poskytovateľov dôveryhodných služieb v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 ([2]), ktorí podliehajú bezpečnostným požiadavkám stanoveným v uvedenom nariadení.

(8) Touto smernicou by nemala byť dotknutá možnosť každého členského štátu prijať potrebné opatrenia na zaručenie ochrany základných záujmov vlastnej bezpečnosti, chrániť verejný poriadok a verejnú bezpečnosť a umožniť vyšetrovanie a odhaľovanie trestných činov, ako aj stíhanie ich páchateľov. V súlade s článkom 346 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“) nie je žiadny členský štát povinný poskytovať informácie, ktorých sprístupnenie podľa neho odporuje základným záujmom jeho bezpečnosti. V tejto súvislosti je relevantné rozhodnutie Rady 2013/488/EÚ ([3]) a dohody o zachovaní mlčanlivosti alebo neformálne dohody o zachovaní mlčanlivosti, ako je napr. tzv. semaforový protokol (Traffic Light Protocol – TLP).

(9) Určité odvetvia hospodárstva sú už regulované alebo môžu byť v budúcnosti regulované právnymi aktmi Únie, ktoré sú špecifické pre jednotlivé odvetvia a zahŕňajú predpisy týkajúce sa bezpečnosti sietí a informačných systémov. Vždy keď tieto právne akty Únie obsahujú ustanovenia, ktorými sa ukladajú požiadavky týkajúce sa bezpečnosti sietí a informačných systémov alebo oznamovania incidentov, mali by sa uvedené ustanovenia uplatňovať, ak obsahujú požiadavky, ktorých účinok je aspoň rovnocenný s účinkom povinností obsiahnutých v tejto smernici. Členské štáty by potom mali uplatňovať ustanovenia takýchto právnych aktov Únie špecifických pre jednotlivé odvetvia vrátane ustanovení, ktoré sa týkajú právomoci, a nemali by vykonávať proces identifikácie prevádzkovateľov základných služieb v zmysle tejto smernice. V tejto súvislosti by členské štáty mali poskytnúť Komisii informácie o uplatňovaní takýchto ustanovení *lex specialis*. Pri určovaní, či sú požiadavky na bezpečnosť sietí a informačných systémov a oznamovanie incidentov obsiahnuté v právnych aktoch Únie špecifických pre jednotlivé odvetvia rovnocenné s požiadavkami stanovenými v tejto smernici, by sa mali zohľadňovať iba ustanovenia príslušných právnych aktov Únie a ich uplatňovanie v členských štátoch.

(10) V odvetví vodnej dopravy sa bezpečnostné požiadavky pre spoločnosti, lode, prístavné zariadenia, prístavy a plavebno-prevádzkové služby podľa právnych aktov Únie vzťahujú na všetky operácie vrátane rádiových a telekomunikačných systémov, počítačových systémov a sietí. Časť povinných postupov, ktoré sa majú dodržiavať, zahŕňa oznamovanie všetkých incidentov, a preto by sa mala považovať za *lex specialis*, pokiaľ sú tieto požiadavky aspoň rovnocenné s príslušnými ustanoveniami tejto smernice.

([1]) Smernica Európskeho parlamentu a Rady 2002/21/ES zo 7. marca 2002 o spoločnom regulačnom rámci pre elektronické komunikačné siete a služby (rámcová smernica) (Ú. v. ES L 108, 24.4.2002, s. 33).

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES (Ú. v. EÚ L 257, 28.8.2014, s. 73).

([3]) Rozhodnutie Rady 2013/488/EÚ z 23. septembra 2013 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 274, 15.10.2013, s. 1).

(11) Pri identifikácii prevádzkovateľov v odvetví vodnej dopravy by členské štáty mali zohľadniť súčasné a budúce medzinárodné kódexy a usmernenia, najmä Medzinárodnej námornej organizácie, s cieľom poskytovať jednotlivým prevádzkovateľom námornej dopravy ucelený prístup.

(12) Regulácia a dohľad v odvetviach bankovníctva a infraštruktúr finančných trhov sú na úrovni Únie vo veľkej miere harmonizované, a to prostredníctvom primárneho a sekundárneho práva Únie a noriem vypracovaných spoločne s európskymi orgánmi dohľadu. V bankovej únii zabezpečuje uplatňovanie uvedených požiadaviek a dohľad nad nimi jednotný mechanizmus dohľadu. V prípade členských štátov, ktoré nie sú súčasťou bankovej únie, sa to zabezpečuje prostredníctvom príslušných bankových regulačných orgánov členských štátov. Vysoký stupeň štandardizácie a zbližovania postupov v oblasti dohľadu zabezpečuje v iných oblastiach regulácie finančného odvetvi aj európsky systém finančného dohľadu. Európsky orgán pre cenné papiere a trhy taktiež vykonáva pre niektoré subjekty, najmä ratingové agentúry a archívy obchodných údajov, funkciu priameho dohľadu.

(13) Operačné riziko je kľúčovou časťou prudenciálnej regulácie a dohľadu v odvetviach bankovníctva a infraštruktúr finančných trhov. Vzťahuje sa na všetky operácie vrátane bezpečnosti, integrity a odolnosti sietí a informačných systémov. Požiadavky v súvislosti s uvedenými systémami, ktoré sú často prísnejšie ako požiadavky stanovené v tejto smernici, sú stanovené vo viacerých právnych aktoch Únie vrátane: pravidiel týkajúcich sa prístupu k činnosti úverových inštitúcií a prudenciálneho dohľadu nad úverovými inštitúciami a investičnými spoločnosťami a pravidiel týkajúcich sa prudenciálnych požiadaviek na úverové inštitúcie a investičné spoločnosti, medzi ktoré patria požiadavky týkajúce sa operačného rizika; pravidiel týkajúcich sa trhov s finančnými nástrojmi, medzi ktoré patria požiadavky týkajúce sa posudzovania rizika pre investičné spoločnosti a regulované trhy; pravidiel týkajúcich sa OTC derivátov, centrálnych protistrán a archívov obchodných údajov, medzi ktoré patria požiadavky týkajúce sa operačného rizika pre centrálne protistrany a archívy obchodných údajov; a pravidiel týkajúcich sa zlepšenia vyrovnania transakcií s cennými papiermi v Únii a centrálnych depozitárov cenných papierov, medzi ktoré patria požiadavky týkajúce sa operačného rizika. Navyše sú požiadavky na oznamovanie incidentov súčasťou bežných postupov dohľadu vo finančnom odvetví a sú často zahrnuté do príručiek týkajúcich sa dohľadu. Členské štáty by mali zvážiť uvedené pravidlá a požiadavky pri uplatňovaní *lex specialis*.

(14) Ako poznamenala Európska centrálna banka vo svojom stanovisku z 25. júla 2014 ([1]), táto smernica nemá vplyv na režim Eurosystému pre dohľad nad platobnými a zúčtovacími systémami podľa práva Únie. Bolo by vhodné, aby si podľa tejto smernice orgány zodpovedné za takýto dohľad vymieňali skúsenosti v otázkach týkajúcich sa bezpečnosti sietí a informačných systémov s príslušnými orgánmi. To isté platí pre členov Európskeho systému centrálnych bánk, ktorí nepatria do eurozóny a ktorí vykonávajú takýto dohľad nad platobnými a zúčtovacími systémami na základe vnútroštátnych zákonov a iných právnych predpisov.

(15) Online trhovisko umožňuje spotrebiteľom a obchodníkom uzatvárať s obchodníkmi online kúpne zmluvy alebo zmluvy o službách a je na uzatváranie takýchto zmlúv konečným miestom. Nemalo by pokrývať online služby, ktoré len sprostredkúvajú služby tretích strán, prostredníctvom ktorých možno zmluvu naozaj uzavrieť. Nemalo by preto pokrývať online služby, ktoré porovnávajú ceny určitých výrobkov alebo služieb od rozličných obchodníkov a následne presmerujú používateľa na uprednostňovaného obchodníka tak, aby si kúpil jeho výrobok. Počítačové služby poskytované prostredníctvom online trhoviska môžu zahŕňať spracúvanie transakcií, zosumarizovanie údajov alebo profilovanie používateľov. Obchody s aplikáciami, ktoré fungujú ako online obchody umožňujúce digitálnu distribúciu aplikácií alebo softvérových programov od tretích strán, sa majú považovať za druh online trhoviska.

(16) Internetový vyhľadávač umožňuje používateľovi vyhľadávanie v zásade všetkých webových sídiel na základe dopytu na akúkoľvek tému. Alternatívne môže byť zameraný na internetové stránky v určitom jazyku. Vymedzenie internetového vyhľadávača stanovené v tejto smernici by sa nemalo vzťahovať na vyhľadávacie funkcie, ktoré sú obmedzené na obsah určitého webového sídla, bez ohľadu na to, či funkciu vyhľadávania poskytuje externý vyhľadávač. Nemalo by taktiež pokrývať online služby, ktoré porovnávajú ceny určitých výrobkov alebo služieb od rozličných obchodníkov a následne presmerujú používateľa na uprednostňovaného obchodníka, aby si kúpil jeho výrobok.

(17) Služby cloud computingu zahŕňajú širokú škálu činností, ktoré sa môžu realizovať podľa rôznych modelov. Na účely tejto smernice pojem „služby cloud computingu“ zahŕňa služby, ktoré umožňujú prístup k škálovateľnému a pružnému súboru zdieľateľných počítačových zdrojov. Uvedené počítačové zdroje zahŕňajú zdroje, ako sú napríklad siete, servery alebo iná infraštruktúra, úložiská, aplikácie a služby. Pojem „škálovateľné“ odkazuje na počítačové zdroje, ktoré pružne prideľuje poskytovateľ cloudových služieb bez ohľadu na zemepisnú polohu zdrojov s cieľom zvládať výkyvy v dopyte. Pojem „pružný súbor“ sa používa na označenie tých počítačových

([1]) Ú. v. EÚ C 352, 7.10.2014, s. 4.

zdrojov, ktoré sa poskytujú a uvoľňujú na základe dopytu s cieľom rýchlo zvýšiť a znížiť dostupné zdroje v závislosti od záťaže. Pojem „zdieľateľný“ sa používa na označenie tých počítačových zdrojov, ktoré sa poskytujú viacerým používateľom, ktorí zdieľajú spoločný prístup k službe, ale spracúvanie sa vykonáva oddelene pre každého používateľa, hoci sa služba poskytuje z toho istého elektronického zariadenia.

(18) Funkciou internetového prepojovacieho uzla (internet exchange point – ďalej len „IXP“) je prepájať siete. IXP neposkytuje prístup do siete ani neslúži ako poskytovateľ služieb tranzitu ani ako poskytovateľ infraštruktúry pre služby tranzitu. Cez IXP sa neposkytujú ani iné služby, ktoré nesúvisia s prepojením, hoci to prevádzkovateľovi IXP nebráni poskytovať nesúvisiace služby. Cez IXP sa prepájajú siete, ktoré sú technicky a organizačne oddelené. Na opísanie technicky samostatnej siete sa používa pojem „autonómny systém“.

(19) Členské štáty by mali byť zodpovedné za určenie subjektov, ktoré spĺňajú kritériá vymedzenia pojmu „prevádzkovateľ základných služieb“. V záujme zaistenia konzistentného prístupu by sa vymedzenie pojmu „prevádzkovateľ základných služieb“ malo jednotne uplatňovať vo všetkých členských štátoch. Na tento účel sa v smernici stanovuje posúdenie subjektov pôsobiacich v konkrétnych odvetviach a pododvetviach, vytvorenie zoznamu základných služieb, zohľadnenie spoločného zoznamu medziodvetvových faktorov na určenie toho, či by potenciálny incident mal závažný rušivý vplyv, konzultačný proces medzi príslušnými členskými štátmi v prípade subjektov poskytujúcich služby vo viac ako jednom členskom štáte a podporu skupiny pre spoluprácu pri procese identifikácie. S cieľom zabezpečiť, aby boli prípadné zmeny na trhu presne zaznamenané, by členské štáty mali pravidelne kontrolovať a v prípade potreby aktualizovať zoznam identifikovaných prevádzkovateľov. Napokon by členské štáty mali Komisii predložiť informácie potrebné na posúdenie miery, do akej táto spoločná metodika umožnila konzistentné uplatňovanie vymedzenia pojmu zo strany členských štátov.

(20) V rámci procesu identifikácie prevádzkovateľov základných služieb by členské štáty mali posudzovať, aspoň pre každé pododvetvie uvedené v tejto smernici, ktoré služby sa musia považovať za základné pre zachovanie rozhodujúcich spoločenských a hospodárskych činností a či subjekty, ktoré sú uvedené v odvetviach a pododvetviach uvedených v tejto smernici a ktoré poskytujú tieto služby, spĺňajú kritériá na identifikáciu prevádzkovateľov. Pri posudzovaní toho, či subjekt poskytuje služby, ktoré sú pre zachovanie rozhodujúcich spoločenských alebo hospodárskych činností zásadné, stačí preskúmať, či uvedený subjekt poskytuje službu, ktorá je zahrnutá do zoznamu základných služieb. Okrem toho by sa malo preukázať, že poskytovanie základnej služby závisí od sietí a informačných systémov. Napokon by členské štáty pri posudzovaní toho, či by incident mal závažný rušivý vplyv na poskytovanie služby, mali zohľadniť viacero medziodvetvových faktorov a podľa potreby aj faktory špecifické pre určité odvetvie.

(21) Na účely identifikácie prevádzkovateľov základných služieb si naplnenie pojmu prevádzkareň v členskom štáte vyžaduje účinné a skutočné vykonávanie činnosti prostredníctvom stabilných zariadení. Právna forma takýchto zariadení, či už ide o pobočku, alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom.

(22) Je pravdepodobné, že subjekty pôsobiace v odvetviach a pododvetviach uvedených v tejto smernici poskytujú základné aj druhotné služby. Napríklad v odvetví leteckej dopravy letiská poskytujú služby, ktoré by členské štáty mohli považovať za základné, ako napríklad riadenie vzletových a pristávacích dráh, ale aj viaceré služby, ktoré by bolo možné považovať za druhotné, ako napríklad poskytovanie nákupných zón. Prevádzkovatelia základných služieb by mali podliehať osobitným bezpečnostným požiadavkám iba vo vzťahu k tým službám, ktoré sa považujú za základné. Na účely identifikácie prevádzkovateľov by preto členské štáty mali vytvoriť zoznam služieb, ktoré sa považujú za základné.

(23) Zoznam služieb by mal obsahovať všetky služby poskytované na území daného členského štátu, ktoré spĺňajú požiadavky tejto smernice. Členské štáty by mali mať možnosť doplniť existujúci zoznam zahrnutím nových služieb. Zoznam služieb by mal pre členské štáty slúžiť ako referenčný bod umožňujúci identifikáciu prevádzkovateľov základných služieb. Jeho účelom je určiť typy základných služieb v ktoromkoľvek danom odvetví uvedenom v tejto smernici, čím sa odlíšia od druhotných činnosti, za ktoré by subjekt pôsobiaci v ktoromkoľvek z daných odvetví mohol byť zodpovedný. Zoznam služieb, ktorý zavedie každý členský štát, by slúžil ako ďalší vstup pri posudzovaní regulačnej praxe každého členského štátu s cieľom zabezpečiť celkovú jednotnosť procesu identifikácie medzi členskými štátmi.

(24) V prípade, že subjekt poskytuje základnú službu v dvoch alebo vo viacerých členských štátoch, tieto členské štáty by sa mali na účely procesu identifikácie zapojiť do vzájomnej dvojstrannej alebo viacstrannej diskusie. Tento konzultačný proces im má pomôcť posúdiť kritickú povahu prevádzkovateľa, pokiaľ ide o cezhraničný vplyv, pričom každému dotknutému členskému štátu umožňuje vyjadriť svoje stanovisko k rizikám spojeným s poskytovanými službami. Dotknuté členské štáty by v tomto procese mali navzájom zohľadňovať svoje názory a mali by mať v tejto súvislosti možnosť požiadať o pomoc skupinu pre spoluprácu.

(25) V dôsledku procesu identifikácie by členské štáty mali prijať vnútroštátne opatrenia, ktorými sa určia subjekty, ktoré podliehajú povinnostiam v oblasti bezpečnosti sietí a informačných systémov. To by sa mohlo dosiahnuť prijatím zoznamu všetkých prevádzkovateľov základných služieb alebo prijatím vnútroštátnych opatrení vrátane objektívnych kvantifikovateľných kritérií, ako napríklad výkon prevádzkovateľa alebo počet používateľov, ktoré umožnia určiť, ktoré subjekty podliehajú povinnostiam týkajúcim sa bezpečnosti sietí a informačných systémov. Vnútroštátne opatrenia, či už existujúce, alebo prijaté v súvislosti s touto smernicou, by mali zahŕňať všetky právne opatrenia, administratívne opatrenia a politiky, ktoré umožňujú identifikáciu prevádzkovateľov základných služieb podľa tejto smernice.

(26) S cieľom poskytnúť vo vzťahu k dotknutému odvetviu informáciu o význame identifikovaných prevádzkovateľov základných služieb by členské štáty mali brať do úvahy počet a veľkosť uvedených prevádzkovateľov napríklad z hľadiska trhového podielu alebo produkovaného alebo prenášaného objemu, a to bez toho, aby boli povinné poskytnúť informácie, ktoré by identifikovaných prevádzkovateľov odhalili.

(27) S cieľom určiť, či by incident mal závažný rušivý vplyv na poskytovanie základnej služby, by členské štáty mali zohľadňovať viacero rôznych faktorov, ako napríklad počet používateľov využívajúcich túto službu na súkromné alebo profesionálne účely. Táto služba sa môže využívať priamo, nepriamo alebo sprostredkovane. Pri posudzovaní dôsledkov, ktoré by incident mohol mať, pokiaľ ide o ich mieru a trvanie, pre hospodárske a spoločenské činnosti alebo verejnú bezpečnosť, by členské štáty mali tiež vyhodnotiť pravdepodobnú dĺžku obdobia, ktoré uplynie, kým by spôsobená diskontinuita začala mať negatívny vplyv.

(28) Popri medziodvetvových faktoroch by sa mali zohľadniť aj faktory špecifické pre jednotlivé odvetvia s cieľom určiť, či by incident mal závažný rušivý vplyv na poskytovanie základnej služby. Pokiaľ ide o dodávateľov energie, medzi takéto faktory by mohol patriť objem produkcie elektrickej energie na celoštátnej úrovni alebo podiel na tejto produkcii; v prípade dodávateľov ropy objem za deň; v prípade leteckej dopravy vrátane letísk a leteckých prepravcov, železničnej dopravy a námorných prístavov podiel na celoštátnej preprave a počet cestujúcich alebo operácií nákladnej dopravy za rok; v prípade infraštruktúry bankového alebo finančného trhu jej systémový význam vyplývajúci z celkového objemu aktív alebo pomeru tohto celkového objemu aktív k HDP; v prípade zdravotníctva počet pacientov, ktorí sú v starostlivosti daného poskytovateľa za rok; v prípade produkcie, spracovania a dodávania vody objem produkcie, počet a typ odberateľov, ako napríklad nemocníc, organizácií poskytujúcich verejné služby alebo jednotlivcov a existencia alternatívnych zdrojov vody na pokrytie potrieb tej istej geografickej oblasti.

(29) S cieľom dosiahnuť a udržiavať vysokú úroveň bezpečnosti sietí a informačných systémov by každý členský štát mal mať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov, v ktorej by boli vymedzené strategické ciele a konkrétne opatrenia, ktoré sa majú v rámci tejto politiky vykonať.

(30) Vzhľadom na rozdiely vo vnútroštátnych štruktúrach riadenia a s cieľom chrániť už existujúce odvetvové dohody alebo orgány dohľadu a regulačné orgány Únie a zamedziť zdvojeniu by členské štáty mali mať možnosť určiť viac než jeden vnútroštátny príslušný orgán zodpovedný za vykonávanie úloh súvisiacich s bezpečnosťou sietí a informačných systémov prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb podľa tejto smernice.

(31) V záujme uľahčenia cezhraničnej spolupráce a komunikácie a s cieľom umožniť účinné vykonávanie tejto smernice je potrebné, aby každý členský štát bez toho, aby boli dotknuté odvetvové regulačné dohody, určil národné jednotné kontaktné miesto zodpovedné za koordináciu záležitostí týkajúcich sa bezpečnosti sietí a informačných systémov a cezhraničnú spoluprácu na úrovni Únie. Príslušné orgány a jednotné kontaktné miesta by mali mať k dispozícii primerané technické, finančné a ľudské zdroje, aby mohli efektívnym a účinným spôsobom vykonávať úlohy, ktoré sú im pridelené, a tak dosahovať ciele tejto smernice. Keďže táto smernica je zameraná na zlepšenia fungovania vnútorného trhu vybudovaním dôvery, je potrebné, aby orgány členských štátov boli schopné účinne spolupracovať s hospodárskymi subjektmi a aby boli zodpovedajúcim spôsobom štruktúrované.

(32) Oznámenia o incidentoch by sa mali posielať príslušným orgánom alebo jednotkám pre riešenie počítačových bezpečnostných incidentov (computer security incident response team – ďalej len „CSIRT“). Jednotným kontaktným miestam by sa oznámenia o incidentoch priamo posielať nemali, pokiaľ tiež nekonajú ako príslušný orgán alebo jednotka CSIRT. Príslušný orgán alebo jednotka CSIRT by však mali mať možnosť jednotnému kontaktnému miestu nariadiť, aby oznámenia o incidentoch postúpilo jednotným kontaktným miestam ostatných dotknutých členských štátov.

(33) S cieľom zabezpečiť účinné poskytovanie informácií členským štátom a Komisii by jednotné kontaktné miesto malo skupine pre spoluprácu predkladať súhrnnú správu, ktorá by mala byť anonymizovaná v záujme zachovania dôverného charakteru oznámení a utajenia totožnosti prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, keďže informácie o totožnosti oznamujúcich subjektov sa na účely výmeny najlepších postupov v rámci skupiny pre spoluprácu nevyžadujú. Súhrnná správa by mala obsahovať informácie o počte prijatých oznámení, ako aj údaje o povahe oznamovaných incidentov, ako je druh porušenia bezpečnosti, jeho závažnosť alebo dĺžka jeho trvania.

(34) Členské štáty by mali mať primerané vybavenie, pokiaľ ide o technické a organizačné spôsobilosti, aby mohli predchádzať incidentom a rizikám v oblasti sietí a informačných systémov, odhaľovať ich, reagovať na ne a zmierňovať ich. Členské štáty by preto mali zabezpečiť, aby mali dobre fungujúce jednotky CSIRT, známe aj ako jednotky reakcie na núdzové počítačové situácie (computer emergency response teams – ďalej len „jednotky CERT“), ktoré budú dodržiavať základné požiadavky s cieľom zaručiť účinné a zlučiteľné spôsobilosti na riešenie incidentov a rizík a zabezpečiť účinnú spoluprácu na úrovni Únie. Aby mohli mať z takýchto spôsobilostí a spolupráce úžitok všetky typy prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, členské štáty by mali zabezpečiť, aby určená jednotka CSIRT pokrývala všetky tieto typy. Vzhľadom na význam medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti by sa malo jednotkám CSIRT umožniť, aby sa okrem siete jednotiek CSIRT zriadenej podľa tejto smernice mohli stať súčasťou sietí medzinárodnej spolupráce.

(35) Keďže väčšinu sietí a informačných systémov prevádzkujú súkromní operátori, spolupráca medzi verejným a súkromným sektorom je nevyhnutná. Prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb by sa mali nabádať, aby sa v záujme zaistenia bezpečnosti sietí a informačných systémov usilovali o vytvorenie vlastných neformálnych mechanizmov spolupráce. Skupina pre spoluprácu by mala mať možnosť pozývať v prípade potreby relevantné zainteresované strany do diskusie. V záujme účinnej podpory výmeny informácií a najlepších postupov má zásadný význam zaistenie toho, aby prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb, ktorí sa na týchto výmenách podieľajú, neboli z dôvodu svojej spolupráce znevýhodnení.

(36) Agentúra ENISA by mala členským štátom a Komisii pomáhať poskytovaním odborných znalostí a poradenstva a uľahčovaním výmeny najlepších postupov. Najmä pri uplatňovaní tejto smernice by sa Komisia mala radiť s agentúrou ENISA a členské štáty by mali mať takú možnosť konzultácie s agentúrou ENISA. Na účely budovania kapacít a rozvoja vedomosti medzi členskými štátmi by skupina pre spoluprácu mala slúžiť aj ako nástroj na výmenu najlepších postupov, diskusiu o spôsobilostiach a pripravenosti členských štátov a dobrovoľnú pomoc svojim členom pri hodnotení národných stratégií v oblasti bezpečnosti sietí a informačných systémov, budovaní kapacít a hodnotení cvičení v oblasti bezpečnosti sietí a informačných systémov.

(37) Ak je to vhodné, členské štáty by mali mať pri uplatňovaní tejto smernice možnosť využiť alebo upraviť existujúce organizačné štruktúry alebo stratégie.

(38) Úlohy skupiny pre spoluprácu a agentúry ENISA sú vzájomne závislé a navzájom sa dopĺňajú. Agentúra ENISA by vo všeobecnosti mala pomáhať skupine pre spoluprácu pri plnení jej úloh v súlade s cieľom agentúry ENISA stanoveným v nariadení Európskeho parlamentu a Rady (EÚ) č. 526/2013 ([1]), a to najmä pomáhať inštitúciám, orgánom, úradom a agentúram Únie a členským štátom vykonávať politiky potrebné na splnenie právnych a regulačných požiadaviek v oblasti bezpečnosti sietí a informačných systémov stanovených v platných a budúcich právnych aktoch Únie. Agentúra ENISA by mala predovšetkým poskytovať pomoc v tých oblastiach, ktoré zodpovedajú jej vlastným úlohám, ako sa stanovuje v nariadení (EÚ) č. 526/2013, a to najmä pri analýze stratégií v oblasti bezpečnosti sietí a informačných systémov, podpore pri organizácii a realizácii cvičení v oblasti bezpečnosti sietí a informačných systémov v Únii a výmene informácií a najlepších postupov týkajúcich sa informovanosti a odbornej prípravy. Agentúra ENISA by tiež mala byť zapojená do vypracúvania usmernení ku kritériám špecifickým pre jednotlivé odvetvia na určenie významnosti vplyvu incidentu.

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 526/2013 z 21. mája 2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a o zrušení nariadenia (ES) č. 460/2004 (Ú. v. EÚ L 165, 18.6.2013, s. 41).

(39) S cieľom presadzovať pokročilú bezpečnosť sietí a informačných systémov by skupina pre spoluprácu mala v prípade potreby spolupracovať s relevantnými inštitúciami, orgánmi, úradmi a agentúrami Únie, vymieňať si know-how a najlepšie postupy a poskytovať poradenstvo o bezpečnostných aspektoch sietí a informačných systémov, ktoré by mohli mať vplyv na ich prácu, rešpektujúc pritom existujúce dojednania týkajúce sa výmeny dôverných informácií. Pri spolupráci s orgánmi presadzovania práva v otázkach bezpečnosti sietí a informačných systémov, ktoré by mohli mať vplyv na ich prácu, by skupina pre spoluprácu mala rešpektovať existujúce informačné kanály a zavedené siete.

(40) Informácie o incidentoch majú pre širokú verejnosť a podniky, najmä malé a stredné podniky, čoraz väčšiu hodnotu. V niektorých prípadoch sa tieto informácie už poskytujú prostredníctvom webových sídiel na vnútroštátnej úrovni, v jazyku danej krajiny a so zameraním najmä na incidenty a udalosti, ktoré majú vnútroštátny rozmer. Vzhľadom na to, že podniky čoraz väčšmi vykonávajú cezhraničnú činnosť a občania využívajú online služby, informácie o incidentoch by sa mali poskytovať v súhrnnej podobe na úrovni Únie. Sekretariát siete jednotiek CSIRT sa nabáda, aby viedol webové sídlo alebo poskytoval hosting osobitnej webovej stránke na existujúcom webovom sídle, kde by sa širokej verejnosti sprístupňovali všeobecné informácie o závažných incidentoch, ktoré sa vyskytli v Únii, pričom osobitný ohľad sa musí brať na záujmy a potreby podnikov. Jednotky CSIRT, ktoré sú súčasťou siete jednotiek CSIRT, sa nabádajú, aby dobrovoľne poskytovali informácie, ktoré by sa na uvedenom webovom sídle mali uverejňovať, pričom by to nemalo zahŕňať dôverné ani citlivé informácie.

(41) Ak sa informácie považujú v súlade s pravidlami Únie a vnútroštátnymi pravidlami o obchodnom tajomstve za dôverné, dôvernosť týchto informácií by sa pri výkone činností a plnení cieľov stanovených v tejto smernici mala zaručiť.

(42) Cvičenia, ktoré simulujú priebeh incidentov v reálnom čase, sú pre testovanie pripravenosti a spolupráce členských štátov v oblasti bezpečnosti sietí a informačných systémov kľúčové. Cyklus cvičení CyberEurope, ktorý koordinuje agentúra ENISA a na ktorom sa zúčastňujú členské štáty, je užitočný nástroj na testovanie a zostavovanie odporúčaní týkajúcich sa toho, ako by sa malo postupne zlepšovať riešenie incidentov na úrovni Únie. Vzhľadom na to, že v súčasnosti členské štáty nie sú povinné plánovať cvičenia ani zúčastňovať sa na nich, vytvorenie siete jednotiek CSIRT podľa tejto smernice by malo členským štátom umožniť zúčastňovať sa na cvičeniach na základe presného plánovania a strategickej voľby. Skupina pre spoluprácu zriadená podľa tejto smernice by mala prediskutovať strategické rozhodnutia týkajúce sa cvičení, najmä, nie však výlučne, pokiaľ ide o pravidelnosť cvičení a tvorbu scenárov incidentov. Agentúra ENISA by v súlade so svojím mandátom mala podporovať organizáciu a realizáciu cvičení v celej Únii, a to poskytovaním svojich odborných znalostí a poradenstva skupine pre spoluprácu a sieti jednotiek CSIRT.

(43) Vzhľadom na globálny charakter bezpečnostných problémov ovplyvňujúcich siete a informačné systémy je potrebná užšia medzinárodná spolupráca s cieľom zlepšiť bezpečnostné normy a výmenu informácií a presadzovať spoločný globálny prístup k bezpečnostným otázkam.

(44) Zodpovednosť za zaistenie bezpečnosti sietí a informačných systémov nesú vo veľkej miere prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb. Kultúra riadenia rizika vrátane hodnotenia rizika a vykonávania bezpečnostných opatrení, ktoré sú primerané existujúcim rizikám, by sa mala podporovať a rozvíjať prostredníctvom vhodných regulačných požiadaviek a dobrovoľných postupov v danom odvetví. Vytvorenie hodnoverných rovnakých podmienok pre všetkých je tiež kľúčové pre účinné fungovanie skupiny pre spoluprácu a siete jednotiek CSIRT v záujme zabezpečenia účinnej spolupráce všetkých členských štátov.

(45) Táto smernica sa uplatňuje iba na tie orgány verejnej správy, ktoré sú identifikované ako prevádzkovatelia základných služieb. Zodpovednosť za zaistenie bezpečnosti sietí a informačných systémov orgánov verejnej správy, ktoré nepatria do rozsahu pôsobnosti tejto smernice, nesú preto členské štáty.

(46) Opatrenia na riadenie rizika zahŕňajú opatrenia na identifikáciu rizika incidentov, opatrenia na predchádzanie incidentom a ich odhaľovanie a zvládanie, ako aj opatrenia na zmiernenie ich vplyvu. Bezpečnosť sietí a informačných systémov zahŕňa bezpečnosť uchovávaných, prenášaných a spracúvaných údajov.

(47) Príslušné orgány by mali mať naďalej možnosť prijímať vnútroštátne usmernenia týkajúce sa okolností, za akých sa od prevádzkovateľov základných služieb vyžaduje, aby oznamovali incidenty.

(48) Mnohé podniky v Únii závisia pri poskytovaní svojich služieb od poskytovateľov digitálnych služieb. Keďže určité digitálne služby by mohli byť pre ich používateľov vrátane prevádzkovateľov základných služieb dôležitým zdrojom a užívatelia ako takí by nemuseli mať vždy k dispozícii alternatívy, táto smernica by sa mala vzťahovať aj na poskytovateľov takýchto služieb. Bezpečnosť, kontinuita a spoľahlivosť typov digitálnych služieb uvedených v tejto smernici majú pre hladké fungovanie mnohých podnikov zásadný význam. Narušenie takejto digitálnej služby by mohlo brániť poskytovaniu iných služieb, ktoré od nej závisia, a mohlo by tak mať vplyv na kľúčové hospodárske a spoločenské činnosti v Únii. Takéto digitálne služby by preto mohli mať zásadný význam pre hladké fungovanie podnikov, ktoré od nich závisia, a okrem toho pre účasť týchto podnikov na vnútornom trhu a cezhraničnom obchode v rámci Únie. Poskytovateľmi digitálnych služieb, na ktorých sa vzťahuje táto smernica, sú tí poskytovatelia, ktorí sú považovaní za ponúkajúcich digitálne služby, od ktorých čoraz viac závisia mnohé podniky v Únii.

(49) Poskytovatelia digitálnych služieb by mali zabezpečiť úroveň bezpečnosti primeranú stupňu rizika ohrozujúceho bezpečnosť digitálnych služieb, ktoré poskytujú, vzhľadom na význam ich služieb pre fungovanie ostatných podnikov v Únii. V praxi prevádzkovatelia základných služieb, ktoré sú často základné pre zachovanie rozhodujúcich spoločenských a hospodárskych činností, čelia vyššiemu stupňu rizika ako poskytovatelia digitálnych služieb. Bezpečnostné požiadavky na poskytovateľov digitálnych služieb by preto mali byť menej prísne. Poskytovatelia digitálnych služieb by mali mať naďalej právo slobodne prijímať opatrenia, ktoré považujú za vhodné na riadenie rizík v oblasti bezpečnosti ich sietí a informačných systémov. Z dôvodu ich cezhraničného charakteru by poskytovatelia digitálnych služieb mali podliehať harmonizovanejšiemu prístupu na úrovni Únie. Špecifikáciu a vykonávanie takýchto opatrení by mali uľahčiť vykonávacie akty.

(50) Hoci výrobcovia hardvéru a vývojári softvéru nie sú prevádzkovateľmi základných služieb ani poskytovateľmi digitálnych služieb, ich produkty zlepšujú bezpečnosť sietí a informačných systémov. Zohrávajú teda dôležitú úlohu, pretože prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb umožňujú zabezpečiť ich siete a informačné systémy. Na takéto hardvérové a softvérové produkty sa už vzťahujú existujúce pravidlá o zodpovednosti za výrobok.

(51) V technických a organizačných opatreniach uložených prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb by sa nemalo vyžadovať, aby bol určitý komerčný produkt informačnej a komunikačnej technológie navrhnutý, vyvinutý alebo vyrobený určitým spôsobom.

(52) Prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb by mali zaistiť bezpečnosť sietí a informačných systémov, ktoré používajú. Ide predovšetkým o súkromné siete a informačné systémy, ktoré spravujú ich interní pracovníci IT alebo ktorých bezpečnosť zaisťujú externí dodávatelia. Požiadavky týkajúce sa bezpečnosti a oznamovania by sa mali vzťahovať na relevantných prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb bez ohľadu na to, či údržbu svojich sietí a informačných systémov vykonávajú interne, alebo prostredníctvom externého dodávateľa.

(53) S cieľom vyhnúť sa neprimeranému finančnému a administratívnemu zaťaženiu prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb by požiadavky mali byť primerané riziku, ktorým čelí daná sieť a daný informačný systém, berúc pritom do úvahy najnovší vývin v oblasti takýchto opatrení. V prípade poskytovateľov digitálnych služieb by sa uvedené požiadavky nemali týkať mikropodnikov a malých podnikov.

(54) V prípade, že orgány verejnej správy členských štátov využívajú služby ponúkané poskytovateľmi digitálnych služieb, najmä služby v oblasti cloud computingu, mohli by sa tieto orgány rozhodnúť, že budú od poskytovateľov takýchto služieb požadovať dodatočné bezpečnostné opatrenia nad rámec toho, čo poskytovatelia digitálnych služieb bežne ponúkajú v súlade s požiadavkami tejto smernice. Mali by mať možnosť tak urobiť prostredníctvom zmluvných záväzkov.

(55) Pojmy online trhovisko, online vyhľadávač a služby cloud computingu v tejto smernici sú vymedzené na osobitný účel tejto smernice a nie sú tým dotknuté nijaké iné nástroje.

(56) Táto smernica by nemala členským štátom brániť v prijímaní vnútroštátnych opatrení, ktorými sa od subjektov verejného sektora požaduje splnenie osobitných bezpečnostných požiadaviek v prípade, že si zmluvne objednajú služby cloud computingu. Takéto vnútroštátne opatrenia by sa mali uplatňovať na dotknutý subjekt verejného sektora, a nie na poskytovateľa služieb cloud computingu.

(57) Vzhľadom na fundamentálne rozdiely medzi prevádzkovateľmi základných služieb, najmä na ich priame spojenie s fyzickou infraštruktúrou, a poskytovateľmi digitálnych služieb, najmä na ich cezhraničný charakter, by sa v tejto smernici mal zaujať diferencovaný prístup, pokiaľ ide o úroveň harmonizácie vo vzťahu k týmto dvom skupinám subjektov. Pokiaľ ide o prevádzkovateľov základných služieb, členské štáty by mali byť schopné identifikovať príslušných prevádzkovateľov a ukladať prísnejšie požiadavky než požiadavky stanovené v tejto smernici. Členské štáty by nemali identifikovať poskytovateľov digitálnych služieb, keďže rozsah pôsobnosti tejto smernice by sa mal vzťahovať na všetkých poskytovateľov digitálnych služieb. Touto smernicou a vykonávacími aktmi prijatými na jej základe by sa okrem toho mala pre poskytovateľov digitálnych služieb zabezpečiť vysoká úroveň harmonizácie s ohľadom na bezpečnostné a oznamovacie požiadavky. To by malo umožňovať rovnaké zaobchádzanie s poskytovateľmi digitálnych služieb v celej Únii, a to spôsobom primeraným ich povahe a stupňu rizika, ktorému by mohli čeliť.

(58) Touto smernicou by sa nemalo členským štátom brániť v tom, aby ukladali bezpečnostné a oznamovacie požiadavky subjektom, ktoré nie sú poskytovateľmi digitálnych služieb patriacimi do rozsahu pôsobnosti tejto smernice, bez toho, aby boli dotknuté povinnosti členských štátov podľa práva Únie.

(59) Príslušné orgány by mali venovať náležitú pozornosť zachovaniu neformálnych a dôveryhodných kanálov na zdieľanie informácií. Pri uverejňovaní incidentov oznámených príslušným orgánom by sa mala náležitým spôsobom udržiavať rovnováha medzi záujmom verejnosti mať informácie o hrozbách a možným poškodením dobrej povesti a obchodných záujmov prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, ktorí incidenty oznámia. Pri vykonávaní oznamovacej povinnosti by príslušné orgány a jednotky CSIRT mali venovať osobitnú pozornosť potrebe, aby sa pred vydaním vhodných bezpečnostných opráv zachovali informácie o zraniteľných stránkach produktu v prísnej tajnosti.

(60) Na poskytovateľov digitálnych služieb by sa mali vzťahovať mierne a reaktívne následné činnosti dohľadu, odôvodnené povahou ich služieb a operácií. Dotknutý príslušný orgán by mal preto prijať opatrenia iba v prípade, ak sa mu poskytol dôkaz, napríklad zo strany samotného poskytovateľa digitálnych služieb, iného príslušného orgánu vrátane príslušného orgánu iného členského štátu alebo používateľa služieb, že poskytovateľ digitálnych služieb nespĺňa požiadavky tejto smernice, najmä po výskyte incidentu. Príslušný orgán by preto nemal mať všeobecnú povinnosť dohľadu nad poskytovateľmi digitálnych služieb.

(61) Príslušné orgány by mali mať prostriedky potrebné na plnenie svojich povinností vrátane právomocí získať dostatočné informácie na účely posúdenia úrovne bezpečnosti sietí a informačných systémov.

(62) Incidenty môžu byť výsledkom trestnej činnosti, ktorej prevenciu, vyšetrovanie a stíhanie podporuje koordinácia a spolupráca medzi prevádzkovateľmi základných služieb, poskytovateľmi digitálnych služieb, príslušnými orgánmi a orgánmi presadzovania práva. Ak existuje podozrenie, že incident súvisí so závažnou trestnou činnosťou podľa práva Únie alebo vnútroštátneho práva, členské štáty by mali nabádať prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, aby príslušným orgánom presadzovania práva oznamovali incidenty, pri ktorých existuje podozrenie o ich súvise so závažnou trestnou činnosťou. Tam, kde je to vhodné, je potrebné zabezpečiť, aby koordináciu medzi príslušnými orgánmi a orgánmi presadzovania práva rôznych členských štátov uľahčovalo Európske centrum boja proti počítačovej kriminalite (EC3) a agentúra ENISA.

(63) V dôsledku incidentov je v mnohých prípadoch porušená ochrana osobných údajov. V tejto súvislosti by príslušné orgány a orgány na ochranu údajov mali navzájom spolupracovať a vymieňať si informácie o všetkých súvisiacich otázkach s cieľom riešiť akékoľvek prípady porušenia ochrany osobných údajov v dôsledku incidentov.

(64) Právomoc vzťahujúca sa na poskytovateľov digitálnych služieb by sa mala udeliť členskému štátu, v ktorom má dotknutý poskytovateľ digitálnych služieb svoju hlavnú prevádzkareň v Únii, čo v zásade zodpovedá miestu, kde má poskytovateľ v Únii svoje sídlo. Pod prevádzkarňou sa rozumie miesto, kde dochádza k účinnému a skutočnému výkonu činnosti prostredníctvom stabilných zariadení. Právna forma takýchto zariadení, či už ide o pobočku, alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom. Toto

kritérium by nemalo závisieť od toho, či sa siete a informačné systémy fyzicky nachádzajú na danom mieste; samotná prítomnosť a používanie takýchto sietí a systémov nepredstavuje hlavnú prevádzkareň, a preto nejde o kritérium na jej určenie.

(65) Keď poskytovateľ digitálnych služieb, ktorý nie je usadený v Únii, ponúka služby v Únii, mal by určiť svojho zástupcu. Aby bolo možné určiť, či takýto poskytovateľ digitálnych služieb ponúka služby v Únii, malo by sa zistiť, či je zrejmé, že daný poskytovateľ digitálnych služieb plánuje ponúkať služby osobám v jednom alebo vo viacerých členských štátoch. Samotná dostupnosť webového sídla poskytovateľa digitálnych služieb alebo jeho sprostredkovateľa v Únii alebo e-mailovej adresy a iných kontaktných údajov alebo použitie jazyka, ktorý sa všeobecne používa v tretej krajine, v ktorej je poskytovateľ digitálnych služieb usadený, nepostačuje na potvrdenie takého úmyslu. Na základe faktorov, ako je používanie jazyka alebo meny bežne používaných v jednom alebo vo viacerých členských štátoch s možnosťou objednania služieb v tomto druhom jazyku alebo spomenutie zákazníkov alebo používateľov, ktorí sa nachádzajú v Únii, môže byť však zjavné, že poskytovateľ digitálnych služieb plánuje ponúkať služby v Únii. Zástupca by mal konať v mene poskytovateľa digitálnych služieb a príslušné orgány alebo jednotky CSIRT by mali mať možnosť obrátiť sa na zástupcu. Poskytovateľ digitálnych služieb by mal výslovne určiť zástupcu prostredníctvom písomného mandátu oprávneného konať v mene daného poskytovateľa digitálnych služieb v súvislosti s povinnosťami prevádzkovateľa podľa tejto smernice vrátane oznamovania incidentov.

(66) Normalizácia bezpečnostných požiadaviek je proces poháňaný trhom. V záujme zaistenia zbližujúceho sa uplatňovania bezpečnostných noriem by členské štáty mali podporovať plnenie určených noriem alebo súlad s nimi s cieľom zabezpečiť vysoký stupeň bezpečnosti sietí a informačných systémov na úrovni Únie. Agentúra ENISA by mala pomáhať členským štátom prostredníctvom poradenstva a usmernení. Na tento účel by mohlo byť užitočné navrhnúť harmonizované normy, čo by sa malo uskutočniť v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 1025/2012 ([1]).

(67) Subjekty, ktoré nepatria do rozsahu pôsobnosti tejto smernice, môžu byť vystavené incidentom, ktoré majú významný vplyv na služby, ktoré poskytujú. Ak sa tieto subjekty domnievajú, že je vo verejnom záujme oznámiť, že k takýmto incidentom došlo, mali by mať možnosť dobrovoľne ich oznamovať. Takéto oznámenia by mal príslušný orgán alebo jednotka CSIRT spracovať, ak to nepredstavuje neprimerané ani nenáležité zaťaženie dotknutých členských štátov.

(68) S cieľom zabezpečiť jednotné podmienky vykonávania tejto smernice by sa na Komisiu mali preniesť vykonávacie právomoci, pokiaľ ide o stanovenie procesných opatrení potrebných na fungovanie skupiny pre spoluprácu a o stanovenie bezpečnostných a oznamovacích požiadaviek uplatniteľných na poskytovateľov digitálnych služieb. Uvedené právomoci by sa mali vykonávať v súlade s nariadením Európskeho parlamentu a Rady (EÚ) č. 182/2011 ([2]). Pri prijímaní vykonávacích aktov týkajúcich sa procesných opatrení potrebných na fungovanie skupiny pre spoluprácu by Komisia mala v čo najväčšej miere zohľadniť stanovisko agentúry ENISA.

(69) Pri prijímaní vykonávacích aktov týkajúcich sa bezpečnostných požiadaviek na poskytovateľov digitálnych služieb by Komisia mala v čo najväčšej miere zohľadniť stanovisko agentúry ENISA a mala by sa radiť so zainteresovanými stranami. Komisia sa okrem toho nabáda, aby zohľadnila tieto príklady: pokiaľ ide o bezpečnosť systémov a zariadení: fyzickú a environmentálnu bezpečnosť, bezpečnosť dodávok, kontrolu prístupu k sieťam a informačným systémom a ich integritu; pokiaľ ide o riešenie incidentov: postupy riešenia incidentov, nástroj na odhaľovanie incidentov, oznamovanie incidentov a súvisiacu komunikáciu; pokiaľ ide o riadenie kontinuity činností: stratégiu kontinuity služieb a plánovanie pre nepredvídané udalosti, spôsobilosti obnovy po núdzovej udalosti; a pokiaľ ide o monitorovanie, audit a testovanie: politiky týkajúce sa monitorovania a vedenia záznamov, cvičné plány pre nepredvídané udalosti, testovanie sietí a informačných systémov, hodnotenie bezpečnosti a monitorovanie dodržiavania požiadaviek.

(70) Pri vykonávaní tejto smernice by Komisia mala podľa potreby spolupracovať s relevantnými odvetvovými výbormi a orgánmi zriadenými na úrovni Únie v oblastiach, na ktoré sa táto smernica vzťahuje.

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho 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 ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES (Ú. v. EÚ L 316, 14.11.2012, s. 12).

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 182/2011 zo 16. februára 2011, ktorým sa ustanovujú pravidlá a všeobecné zásady mechanizmu, na základe ktorého členské štáty kontrolujú vykonávanie vykonávacích právomocí Komisie (Ú. v. EÚ L 55, 28.2.2011, s. 13).

(71) Komisia by mala túto smernicu pravidelne preskúmavať a radiť sa pritom so zainteresovanými subjektmi najmä s cieľom určiť, či je potrebné zmeniť ju na základe zmien spoločenských, politických, technologických a trhových podmienok.

(72) Zdieľanie informácií o rizikách a incidentoch v rámci skupiny pre spoluprácu a siete jednotiek CSIRT a dodržiavanie požiadaviek oznamovať incidenty vnútroštátnym príslušným orgánom alebo jednotkám CSIRT by si mohlo vyžadovať spracúvanie osobných údajov. Takéto spracúvanie by malo byť v súlade so smernicou Európskeho parlamentu a Rady 95/46/ES ([1]) a nariadením Európskeho parlamentu a Rady (ES) č. 45/2001 ([2]). Pri uplatňovaní tejto smernice by sa malo podľa potreby uplatňovať nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 ([3]).

(73) S európskym dozorným úradníkom pre ochranu údajov sa konzultovalo v súlade s článkom 28 ods. 2 nariadenia (ES) č. 45/2001 a 14. júna 2013 európsky dozorný úradník pre ochranu údajov vydal stanovisko ([4]).

(74) Keďže cieľ tejto smernice, a to dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii, nie je možné uspokojivo dosiahnuť na úrovni samotných členských štátov, ale z dôvodu účinku tohto opatrenia ho možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku táto smernica neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa.

(75) V tejto smernici sa dodržiavajú základné práva a zásady uznané Chartou základných práv Európskej únie, najmä právo na rešpektovanie súkromného života a komunikácie, ochrana osobných údajov, sloboda podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy pred súdom a právo na vypočutie. Táto smernica by sa mala vykonávať v súlade s uvedenými právami a zásadami,

PRIJALI TÚTO SMERNICU:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

1. Touto smernicou sa stanovujú opatrenia na dosiahnutie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v rámci Únie s cieľom zlepšiť fungovanie vnútorného trhu.

2. Na tento účel sa v tejto smernici:

a) stanovujú pre všetky členské štáty povinnosti prijať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov;

b) vytvára skupina pre spoluprácu s cieľom podporiť a uľahčiť strategickú spoluprácu a výmenu informácií medzi členskými štátmi a rozvíjať vzájomnú dôveru medzi nimi;

c) vytvára sieť jednotiek pre riešenie počítačových bezpečnostných incidentov (computer security incident response teams network – ďalej len „sieť jednotiek CSIRT“) s cieľom prispievať k rozvoju dôvery medzi členskými štátmi a podporovať rýchlu a účinnú operačnú spoluprácu;

([1]) Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (Ú. v. ES L 281, 23.11.1995, s. 31).
([2]) Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1).
([3]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (Ú. v. ES L 145, 31.5.2001, s. 43).
([4]) Ú. v. EÚ C 32, 4.2.2014, s. 19.

d) stanovujú bezpečnostné a oznamovacie požiadavky pre prevádzkovateľov základných služieb a pre poskytovateľov digitálnych služieb;

e) stanovujú povinnosti členských štátov určiť príslušné vnútroštátne orgány, národné jednotné kontaktné miesta a jednotky CSIRT s úlohami súvisiacimi s bezpečnosťou sietí a informačných systémov.

3. Bezpečnostné a oznamovacie požiadavky stanovené v tejto smernici sa nevzťahujú na podniky, ktoré podliehajú požiadavkám článkov 13a a 13b smernice 2002/21/ES, ani na poskytovateľov dôveryhodných služieb, na ktorých sa vzťahujú požiadavky článku 19 nariadenia (EÚ) č. 910/2014.

4. Uplatňovaním tejto smernice nie je dotknutá smernica Rady 2008/114/ES ([1]) a smernice Európskeho parlamentu a Rady 2011/93/EÚ ([2]) a 2013/40/EÚ ([3]).

5. Bez toho, aby bol dotknutý článok 346 ZFEÚ, informácie, ktoré sú dôverné podľa predpisov Únie a vnútroštátnych predpisov, ako napríklad predpisov o obchodnom tajomstve, sa vymieňajú s Komisiou a inými príslušnými orgánmi len v prípade, ak je takáto výmena potrebná na účely uplatňovania tejto smernice. Vymieňané informácie sa obmedzujú na tie, ktoré sú relevantné a primerané účelu takejto výmeny. Pri takejto výmene informácií sa zachováva dôvernosť týchto informácií a chránia sa bezpečnostné a obchodné záujmy prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb.

6. Touto smernicou nie sú dotknuté opatrenia prijímané členskými štátmi na zabezpečenie ich základných štátnych funkcií, najmä na zabezpečenie národnej bezpečnosti vrátane opatrení na ochranu informácií, ktorých sprístupnenie členské štáty považujú za odporujúce základným záujmom ich bezpečnosti, a na udržanie verejného poriadku, najmä na účely umožnenia vyšetrovania, odhaľovania a stíhania trestných činov.

7. Ak sa podľa právneho aktu Únie špecifického pre určité odvetvie vyžaduje, aby prevádzkovatelia základných služieb alebo poskytovatelia digitálnych služieb buď zaisťovali bezpečnosť ich sietí a informačných systémov, alebo aby oznamovali incidenty, uplatňujú sa ustanovenia tohto právneho aktu Únie špecifického pre určité odvetvie pod podmienkou, že tieto požiadavky majú aspoň rovnocenný účinok ako povinnosti stanovené v tejto smernici.

Článok 2

Spracúvanie osobných údajov

1. Spracúvanie osobných údajov podľa tejto smernice sa vykonáva v súlade so smernicou 95/46/ES.

2. Spracúvanie osobných údajov inštitúciami a orgánmi Únie podľa tejto smernice sa vykonáva v súlade s nariadením (ES) č. 45/2001.

Článok 3

Minimálna harmonizácia

Bez toho, aby bol dotknutý článok 16 ods. 10 a povinnosti členských štátov podľa práva Únie, členské štáty môžu prijať alebo zachovať ustanovenia, ktorých cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov.

([1]) Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23.12.2008, s. 75).

([2]) Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV (Ú. v. EÚ L 335, 17.12.2011, s. 1).

([3]) Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV (Ú. v. EÚ L 218, 14.8.2013, s. 8).

Článok 4

Vymedzenie pojmov

Na účely tejto smernice sa uplatňuje toto vymedzenie pojmov:

1. „sieť a informačný systém“ je:

   a) elektronická komunikačná sieť v zmysle článku 2 písm. a) smernice 2002/21/ES;

   b) každé zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú na základe programu automatické spracúvanie digitálnych údajov, alebo

   c) digitálne údaje, ktoré sa ukladajú, spracúvajú, získavajú alebo prenášajú prostredníctvom prvkov uvedených v písmenách a) a b) na účely ich prevádzkovania, používania, ochrany a udržiavania;

2. „bezpečnosť sietí a informačných systémov“ je schopnosť sietí a informačných systémov odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov;

3. „národná stratégia v oblasti bezpečnosti sietí a informačných systémov“ je rámec, v ktorom sa stanovujú strategické ciele a priority v oblasti bezpečnosti sietí a informačných systémov na vnútroštátnej úrovni;

4. „prevádzkovateľ základných služieb“ je verejný alebo súkromný subjekt, ktorého typ sa uvádza v prílohe II, spĺňajúci kritériá stanovené v článku 5 ods. 2;

5. „digitálna služba“ je služba v zmysle článku 1 ods. 1 písm. b) smernice Európskeho parlamentu a Rady (EÚ) 2015/1535 ([1]), ktorej druh sa uvádza v prílohe III;

6. „poskytovateľ digitálnych služieb“ je každá právnická osoba, ktorá poskytuje digitálnu službu;

7. „incident“ je každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov;

8. „riešenie incidentov“ sú všetky postupy na podporu odhaľovania, analýzy a obmedzenia následkov incidentu a reakcie naň;

9. „riziko“ je každá primerane rozpoznateľná okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na bezpečnosť sietí a informačných systémov;

10. „zástupca“ je akákoľvek fyzická alebo právnická osoba usadená v Únii, ktorá je výslovne poverená konať v mene poskytovateľa digitálnej služby, ktorý nie je usadený v Únii, na ktorú sa môže vnútroštátny príslušný orgán alebo jednotka CSIRT obrátiť namiesto poskytovateľa digitálnych služieb, pokiaľ ide o povinnosti uvedeného poskytovateľa digitálnych služieb podľa tejto smernice;

11. „norma“ je norma v zmysle článku 2 bodu 1 nariadenia (EÚ) č. 1025/2012;

12. „špecifikácia“ je technická špecifikácia v zmysle článku 2 bodu 4 nariadenia (EÚ) č. 1025/2012;

13. „internetový prepojovací uzol (IXP)“ je sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých autonómnych systémov najmä na účely uľahčenia internetového dátového toku; IXP prepojuje len autonómne systémy; pri IXP nemusí internetový dátový tok medzi ktoroukoľvek dvojicou zúčastnených autonómnych systémov prechádzať cez žiadny tretí autonómny systém, pričom tento dátový tok sa nijako nemení ani sa doň nijako nezasahuje;

14. „systém názvov domén (DNS)“ je hierarchický distribuovaný systém pomenovaní v sieti, ktorý prekladá vyhľadávanie názvov domén;

([1]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/1535 z 9. septembra 2015, ktorou sa stanovuje postup pri poskytovaní informácií v oblasti technických predpisov a pravidiel vzťahujúcich sa na služby informačnej spoločnosti (Ú. v. EÚ L 241, 17.9.2015, s. 1).

15. „poskytovateľ služieb DNS“ je subjekt, ktorý poskytuje na internete služby DNS;

16. „register domén najvyššej úrovne“ je subjekt, ktorý spravuje a prevádzkuje registráciu názvov internetových domén v rámci určitej domény najvyššej úrovne (TLD);

17. „online trhovisko“ je digitálna služba, ktorá umožňuje spotrebiteľom a/alebo obchodníkom v zmysle článku 4 ods. 1 písm. a) a b) smernice Európskeho parlamentu a Rady 2013/11/EÚ ([1]) uzavierať online kúpne zmluvy alebo zmluvy o službách s obchodníkmi buď na webovom sídle online trhoviska, alebo na webovom sídle obchodníka, ktoré využíva počítačové služby poskytované online trhoviskom;

18. „internetový vyhľadávač“ je digitálna služba, ktorá umožňuje používateľom vyhľadávať v zásade na všetkých webových sídlach alebo na webových sídlach v konkrétnom jazyku informácie o akejkoľvek téme na základe kľúčového slova, vety alebo iných zadaných údajov, pričom jeho výsledkom sú linky, prostredníctvom ktorých možno nájsť informácie súvisiace s požadovaným obsahom;

19. „služba v oblasti cloud computingu“ je digitálna služba, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať.

Článok 5

Identifikácia prevádzkovateľov základných služieb

1. Členské štáty do 9. novembra 2018 určia pre každé odvetvie a pododvetvie uvedené v prílohe II prevádzkovateľov základných služieb s prevádzkarňou na ich území.

2. Kritériá na identifikáciu prevádzkovateľov základných služieb uvedených v článku 4 bode 4 sú tieto:

a) subjekt poskytuje službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností;

b) poskytovanie tejto služby je závislé od sietí a informačných systémov a

c) incident by mal závažný rušivý vplyv na poskytovanie uvedenej služby.

3. Na účely odseku 1 každý členský štát zostaví zoznam služieb uvedených v odseku 2 písm. a).

4. Na účely odseku 1, ak subjekt poskytuje službu uvedenú v odseku 2 písm. a) v dvoch alebo vo viacerých členských štátoch, tieto členské štáty začnú vzájomné konzultácie. Tieto konzultácie sa uskutočnia pred tým, ako sa rozhodne o identifikácii.

5. Členské štáty pravidelne a aspoň každé dva roky od 9. mája 2018 preskúmavajú a v prípade potreby aktualizujú zoznam identifikovaných prevádzkovateľov základných služieb.

6. Úlohou skupiny pre spoluprácu je v súlade s úlohami uvedenými v článku 11 podporovať členské štáty, aby v procese identifikácie prevádzkovateľov základných služieb postupovali jednotne.

7. Na účely preskúmania uvedeného v článku 23 a do 9. novembra 2018 a potom každé dva roky členské štáty predložia Komisii informácie, ktoré potrebuje na to, aby mohla posúdiť vykonávanie tejto smernice, najmä jednotnosť postupov členských štátov pri identifikácii prevádzkovateľov základných služieb. Tieto informácie zahŕňajú aspoň:

a) vnútroštátne opatrenia umožňujúce identifikáciu prevádzkovateľov základných služieb;

([1]) Smernica Európskeho parlamentu a Rady 2013/11/EÚ z 21. mája 2013 o alternatívnom riešení spotrebiteľských sporov, ktorou sa mení nariadenie (ES) č. 2006/2004 a smernica 2009/22/ES (smernica o alternatívnom riešení spotrebiteľských sporov) (Ú. v. EÚ L 165, 18.6.2013, s. 63).

b) zoznam služieb uvedený v odseku 3;

c) počet prevádzkovateľov základných služieb určených pre každé z odvetví uvedených v prílohe II a ich význam pre dané odvetvie;

d) prípadné prahové hodnoty na určenie príslušnej úrovne poskytovania podľa počtu používateľov využívajúcich túto službu, ako sa uvádza v článku 6 ods. 1 písm. a), alebo významu konkrétneho prevádzkovateľa základných služieb, ako sa uvádza v článku 6 ods. 1 písm. f).

S cieľom prispieť k poskytovaniu porovnateľných informácií môže Komisia, zohľadňujúc v čo najväčšej miere stanovisko agentúry ENISA, prijať vhodné technické usmernenia týkajúce sa parametrov informácií uvedených v tomto odseku.

Článok 6

Závažný rušivý vplyv

1. Pri určovaní závažnosti rušivého vplyvu uvedeného v článku 5 ods. 2 písm. c) členské štáty zohľadňujú aspoň tieto medziodvetvové faktory:

a) počet používateľov využívajúcich službu, ktorú poskytuje daný subjekt;

b) závislosť ostatných odvetví uvedených v prílohe II od služby, ktorú poskytuje daný subjekt;

c) vplyvu, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti alebo verejnú bezpečnosť;

d) trhový podiel daného subjektu;

e) geografické rozšírenie z hľadiska oblasti, ktorú by incident mohol postihnúť;

f) význam subjektu z hľadiska zachovania dostatočnej úrovne služby, berúc do úvahy dostupnosť alternatívnych spôsobov poskytovania danej služby.

2. Pri určovaní toho, či by mal incident závažný rušivý vplyv, členské štáty zohľadňujú podľa potreby aj faktory špecifické pre jednotlivé odvetvia.

KAPITOLA II

VNÚTROŠTÁTNE RÁMCE V OBLASTI BEZPEČNOSTI SIETÍ A INFORMAČNÝCH SYSTÉMOV

Článok 7

Národná stratégia v oblasti bezpečnosti sietí a informačných systémov

1. Každý členský štát prijme národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov, v ktorej sa vymedzia strategické ciele a vhodné politické a regulačné opatrenia na dosiahnutie a udržanie vysokej úrovne bezpečnosti sietí a informačných systémov a ktorá sa vzťahuje aspoň na odvetvia uvedené v prílohe II a služby uvedené v prílohe III. Národná stratégia v oblasti bezpečnosti sietí a informačných systémov sa venuje najmä týmto otázkam:

a) ciele a priority národnej stratégie v oblasti bezpečnosti sietí a informačných systémov;

b) rámec riadenia na dosiahnutie cieľov a priorít národnej stratégie v oblasti bezpečnosti sietí a informačných systémov vrátane úloh a zodpovedností vládnych orgánov a ďalších relevantných aktérov;

c) identifikácia opatrení týkajúcich sa pripravenosti, reakcie a obnovy vrátane spolupráce medzi verejným a súkromným sektorom;

d) určenie vzdelávacích programov, programov na zvyšovanie informovanosti a programov odbornej prípravy súvisiacich s národnou stratégiou v oblasti bezpečnosti sietí a informačných systémov;

e) určenie plánov výskumu a vývoja súvisiacich s národnou stratégiou v oblasti bezpečnosti sietí a informačných systémov;

f) plán posudzovania rizika na účely identifikácie rizík;

g) zoznam rôznych aktérov zapojených do vykonávania národnej stratégie v oblasti bezpečnosti sietí a informačných systémov.

2. Členské štáty môžu pri vypracúvaní národných stratégií v oblasti bezpečnosti sietí a informačných systémov požiadať o pomoc agentúru ENISA.

3. Členské štáty oznámia Komisii svoje národné stratégie v oblasti bezpečnosti sietí a informačných systémov do troch mesiacov od ich prijatia. Členské štáty môžu pritom vylúčiť prvky stratégie, ktoré sa týkajú národnej bezpečnosti.

Článok 8

Vnútroštátne príslušné orgány a národné jednotné kontaktné miesto

1. Každý členský štát určí jeden alebo viaceré vnútroštátne príslušné orgány pre bezpečnosť sietí a informačných systémov (ďalej len „príslušný orgán“), ktoré sa zaoberajú prinajmenšom odvetviami uvedenými v prílohe II a službami uvedenými v prílohe III. Členské štáty môžu touto úlohou poveriť existujúci orgán alebo orgány.

2. Príslušné orgány monitorujú uplatňovanie tejto smernice na vnútroštátnej úrovni.

3. Každý členský štát určí národné jednotné kontaktné miesto pre bezpečnosť sietí a informačných systémov (ďalej len „jednotné kontaktné miesto“). Členské štáty môžu touto úlohou poveriť existujúci orgán. Ak členský štát určí iba jeden príslušný orgán, tento príslušný orgán je aj jednotným kontaktným miestom.

4. Jednotné kontaktné miesto vykonáva styčnú úlohu, aby zabezpečilo cezhraničnú spoluprácu orgánov členských štátov s príslušnými orgánmi v iných členských štátoch, so skupinou pre spoluprácu uvedenou v článku 11 a sieťou jednotiek CSIRT uvedenou v článku 12.

5. Členské štáty zabezpečia, aby príslušné orgány a jednotné kontaktné miesta mali primerané zdroje na účinné a efektívne vykonávanie zverených úloh, a teda na plnenie cieľov tejto smernice. Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu určených zástupcov v rámci skupiny pre spoluprácu.

6. Príslušné orgány a jednotné kontaktné miesto vždy, keď je to vhodné, a v súlade s vnútroštátnym právom konzultujú a spolupracujú s príslušnými vnútroštátnymi orgánmi presadzovania práva a vnútroštátnymi orgánmi pre ochranu údajov.

7. Každý členský štát bezodkladne oznámi Komisii určenie príslušného orgánu a jednotného kontaktného miesta, ich úlohy a akékoľvek následné zmeny. Každý členský štát zverejní určenie príslušného orgánu a jednotného kontaktného miesta. Komisia uverejní zoznam určených jednotných kontaktných miest.

Článok 9

Jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT)

1. Každý členský štát určí jednu alebo viac jednotiek CSIRT, ktoré spĺňajú požiadavky stanovené v bode 1 prílohy I, pokrývajú aspoň odvetvia uvedené v prílohe II a služby uvedené v prílohe III a ktoré zodpovedajú za riešenie rizík a incidentov podľa presne stanoveného postupu. Jednotku CSIRT možno zriadiť v rámci príslušného orgánu.

2. Členské štáty zabezpečia, aby jednotky CSIRT mali primerané zdroje na účinné plnenie svojich úloh stanovených v bode 2 prílohy I.

Členské štáty zabezpečia účinnú, efektívnu a bezpečnú spoluprácu svojich jednotiek CSIRT v rámci siete jednotiek CSIRT uvedenej v článku 12.

3. Členské štáty zabezpečia, aby ich jednotky CSIRT mali prístup k primeranej, bezpečnej a odolnej komunikačnej a informačnej infraštruktúre na vnútroštátnej úrovni.

4. Členské štáty informujú Komisiu o rozsahu a hlavných prvkoch postupu pri riešení incidentov zo strany ich jednotiek CSIRT.

5. Členské štáty môžu pri tvorbe vnútroštátnych jednotiek CSIRT požiadať o pomoc agentúru ENISA.

Článok 10

Spolupráca na vnútroštátnej úrovni

1. Ak príslušný orgán, jednotné kontaktné miesto a jednotka CSIRT jedného členského štátu sú samostatnými subjektmi, pri plnení povinností stanovených v tejto smernici spolupracujú.

2. Členské štáty zabezpečia, aby ich príslušné orgány alebo jednotky CSIRT dostávali oznámenia o incidentoch predložené podľa tejto smernice. Ak členský štát rozhodne, že jednotka CSIRT nebude dostávať oznámenia, jednotke CSIRT sa v rozsahu potrebnom na plnenie jej úloh poskytne prístup k údajom o incidentoch, ktoré oznámili prevádzkovatelia základných služieb podľa článku 14 ods. 3 a 5 alebo poskytovatelia digitálnych služieb podľa článku 16 ods. 3 a 6.

3. Členské štáty zabezpečia, aby príslušné orgány alebo jednotky CSIRT informovali jednotné kontaktné miesta o oznámeniach o incidentoch predložených podľa tejto smernice.

Do 9. augusta 2018 a potom každý rok jednotné kontaktné miesto predkladá skupine pre spoluprácu súhrnnú správu o prijatých oznámeniach, ktorá obsahuje aj počet oznámení a charakter oznámených incidentov a opatrenia prijaté v súlade s článkom 14 ods. 3 a 5 a článkom 16 ods. 3 a 6.

KAPITOLA III

SPOLUPRÁCA

Článok 11

Skupina pre spoluprácu

1. S cieľom podporiť a uľahčiť strategickú spoluprácu a výmenu informácií medzi členskými štátmi a rozvíjať dôveru a dosiahnuť vysokú spoločnú úroveň bezpečnosti sietí a informačných systémov v Únii sa týmto zriaďuje skupina pre spoluprácu.

Skupina pre spoluprácu si plní svoje úlohy na základe dvojročných pracovných programov uvedených v odseku 3 druhom pododseku.

2. Skupina pre spoluprácu sa skladá zo zástupcov členských štátov, Komisie a agentúry ENISA.

Vo vhodných prípadoch môže skupina pre spoluprácu pozvať na účasť na svojej práci zástupcov príslušných zainteresovaných strán.

Sekretariát zabezpečuje Komisia.

3. Skupina pre spoluprácu plní tieto úlohy:

a) poskytovanie strategického usmernenia pre činnosť siete jednotiek CSIRT zriadenej podľa článku 12;

b) vymieňanie si najlepších postupov v oblasti výmeny informácií týkajúcich sa oznamovania incidentov podľa článku 14 ods. 3 a 5 a článku 16 ods. 3 a 6;

c) vymieňanie si najlepších postupov medzi členskými štátmi a v spolupráci s agentúrou ENISA, pomáhanie členským štátom pri budovaní kapacít na zaistenie bezpečnosti sietí a informačných systémov;

d) diskutovanie o spôsobilostiach a pripravenosti členských štátov a na dobrovoľnom základe hodnotenie národných stratégií v oblasti bezpečnosti sietí a informačných systémov a účinnosti jednotiek CSIRT, ako aj identifikovanie najlepších postupov;

e) vymieňanie si informácií a najlepších postupov v oblasti zvyšovania informovanosti a odbornej prípravy;

f) vymieňanie si informácií a najlepších postupov v oblasti výskumu a vývoja bezpečnosti sietí a informačných systémov;

g) vo vhodných prípadoch vymieňanie si skúsenosti v otázkach bezpečnosti sietí a informačných systémov s príslušnými inštitúciami, orgánmi, úradmi a agentúrami Únie;

h) diskutovanie o normách a špecifikáciách uvedených v článku 19 so zástupcami príslušných európskych organizácií pre normalizáciu;

i) zbieranie informácií o najlepších postupoch v súvislosti s rizikami a incidentmi;

j) každoročné skúmanie súhrnných správ uvedených v článku 10 ods. 3 druhom pododseku;

k) diskutovanie o práci vykonanej v súvislosti s cvičeniami v oblasti bezpečnosti sietí a informačných systémov, vzdelávacími programami a odbornou prípravou vrátane práce vykonanej agentúrou ENISA;

l) s pomocou agentúry ENISA vymieňanie si najlepších postupov, pokiaľ ide o identifikáciu prevádzkovateľov základných služieb zo strany členských štátov aj pokiaľ ide o cezhraničnú závislosť v súvislosti s rizikami a incidentmi;

m) diskutovanie o spôsoboch informovania o oznámených incidentoch podľa článkov 14 a 16.

Do 9. februára 2018 a potom každé dva roky skupina pre spoluprácu zostaví pracovný program týkajúci sa činností, ktoré sa majú uskutočniť v rámci plnenia jej cieľov a úloh, ktoré sú v súlade s cieľmi tejto smernice.

4. Na účely preskúmania uvedeného v článku 23 a do 9. augusta 2018 a potom každý rok a pol skupina pre spoluprácu pripraví správu, v ktorej posúdi skúsenosti získané v rámci strategickej spolupráce vykonávanej podľa tohto článku.

5. Komisia prijme vykonávacie akty stanovujúce procesné opatrenia potrebné na fungovanie skupiny pre spoluprácu. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 22 ods. 2.

Na účely prvého pododseku Komisia predloží prvý návrh vykonávacieho aktu výboru uvedenému v článku 22 ods. 1 do 9. februára 2017.

Článok 12

Sieť jednotiek CSIRT

1. S cieľom prispieť k rozvoju dôvery medzi členskými štátmi a podporiť rýchlu a účinnú operačnú spoluprácu sa zriaďuje sieť vnútroštátnych jednotiek CSIRT.

2. Sieť jednotiek CSIRT sa skladá zo zástupcov jednotiek CSIRT členských štátov a jednotky CERT-EU. Komisia sa zúčastňuje na práci siete jednotiek CSIRT ako pozorovateľ. Agentúra ENISA zabezpečuje sekretariát a aktívne podporuje spoluprácu medzi jednotkami CSIRT.

3. Sieť jednotiek CSIRT plní tieto úlohy:

a) vymieňanie si informácií o službách, operáciách a spôsobilostiach spolupráce jednotiek CSIRT;

b) na žiadosť zástupcu jednotky CSIRT z členského štátu, ktorý je potenciálne postihnutý incidentom, vymieňanie si a prerokúvanie informácií, ktoré nie sú citlivé z obchodného hľadiska a týkajú sa daného incidentu a súvisiacich rizík; avšak ktorákoľvek jednotka CSIRT členského štátu môže odmietnuť prispieť k tejto diskusii, ak hrozí riziko ovplyvnenia vyšetrovania daného incidentu;

c) na dobrovoľnom základe vymieňanie si a sprístupňovanie informácií o jednotlivých incidentoch, ktoré nie sú dôverné;

d) na žiadosť zástupcu jednotky CSIRT členského štátu prediskutovanie a pokiaľ možno identifikovanie koordinovanej reakcie na incident, ktorý bol identifikovaný v jurisdikcii tohto členského štátu;

e) poskytovanie podpory členským štátom pri riešení cezhraničných incidentov na základe ich dobrovoľnej vzájomnej pomoci;

f) diskutovanie o ďalších formách operačnej spolupráce, preskúmavanie a identifikovanie ich, a to aj v súvislosti:

   i) s kategóriami rizík a incidentov;

   ii) so včasnými varovaniami;

   iii) so vzájomnou pomocou;

   iv) so zásadami a spôsobmi koordinácie, keď členské štáty reagujú na cezhraničné riziká a incidenty;

g) informovanie skupiny pre spoluprácu o svojej činnosti a o ďalších formách operačnej spolupráce, o ktorých sa diskutuje podľa písmena f), a požadovanie usmernení v tomto ohľade;

h) diskutovanie o ponaučeniach z cvičení v oblasti bezpečnosti sietí a informačných systémov vrátane tých, ktoré organizuje agentúra ENISA;

i) na žiadosť určitej jednotky CSIRT diskutovanie o spôsobilostiach a pripravenosti tejto jednotky CSIRT;

j) vydávanie usmernení s cieľom uľahčiť konvergenciu operačných postupov so zreteľom na uplatňovanie ustanovení tohto článku, pokiaľ ide o operačnú spoluprácu.

4. Na účely preskúmania uvedeného v článku 23 a do 9. augusta 2018 a potom každý rok a pol sieť jednotiek CSIRT vypracuje správu, v ktorej posúdi skúsenosti získané v rámci operačnej spolupráce vykonávanej podľa tohto článku, pričom uvedie aj závery a odporúčania. Táto správa sa tiež predloží skupine pre spoluprácu.

5. Sieť jednotiek CSIRT si stanoví vlastný rokovací poriadok.

Článok 13

Medzinárodná spolupráca

Únia môže uzatvárať medzinárodné dohody v súlade s článkom 218 ZFEÚ s tretími krajinami alebo medzinárodnými organizáciami, ktorými môže povoľovať a organizovať ich účasť na niektorých činnostiach skupiny pre spoluprácu. V takýchto dohodách sa zohľadňuje potreba zabezpečiť primeranú ochranu údajov.

KAPITOLA IV

BEZPEČNOSŤ SIETÍ A INFORMAČNÝCH SYSTÉMOV PREVÁDZKOVATEĽOV ZÁKLADNÝCH SLUŽIEB

Článok 14

Bezpečnostné požiadavky a oznamovanie incidentov

1. Členské štáty zabezpečia, aby prevádzkovatelia základných služieb prijali vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré využívajú vo svojej prevádzke. S ohľadom na najnovší technický vývoj tieto opatrenia zabezpečujú takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika.

2. Členské štáty zabezpečia, aby prevádzkovatelia základných služieb prijali primerané opatrenia na zabránenie a minimalizovanie vplyvu incidentov, ktoré ovplyvňujú bezpečnosť sietí a informačných systémov používaných na poskytovanie týchto základných služieb, s cieľom zabezpečiť ich kontinuitu.

3. Členské štáty zabezpečia, aby prevádzkovatelia základných služieb bez zbytočného odkladu oznamovali príslušnému orgánu alebo jednotke CSIRT incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú. Oznámenia obsahujú informácie umožňujúce príslušnému orgánu alebo jednotke CSIRT určiť prípadný cezhraničný vplyv incidentu. Oznámenie nemá pre oznamujúcu stranu za následok vyššiu zodpovednosť.

4. S cieľom určiť závažnosť vplyvu incidentu sa zohľadnia najmä tieto parametre:

a) počet používateľov postihnutých narušením základnej služby;

b) dĺžka trvania incidentu;

c) geografické rozšírenie z hľadiska oblasti, ktorú incident postihol.

5. Na základe informácií, ktoré poskytol prevádzkovateľ základných služieb v oznámení, príslušný orgán alebo jednotka CSIRT informuje ostatné postihnuté členské štáty, ak má incident závažný vplyv na kontinuitu základných služieb v týchto členských štátoch. Príslušný orgán alebo jednotka CSIRT pritom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, chráni bezpečnosť a obchodné záujmy prevádzkovateľa základných služieb, ako aj dôvernosť informácií poskytnutých v jeho oznámení.

Pokiaľ to okolnosti umožňujú, príslušný orgán alebo jednotka CSIRT poskytnú oznamujúcemu prevádzkovateľovi základných služieb relevantné informácie týkajúce sa následných opatrení prijatých na základe jeho oznámenia, ako sú napríklad informácie, ktoré by mohli podporiť účinné riešenie incidentu.

Na žiadosť príslušného orgánu alebo jednotky CSIRT jednotné kontaktné miesto postúpi oznámenia uvedené v prvom pododseku jednotným kontaktným miestam ostatných postihnutých členských štátov.

6. Po porade s oznamujúcim prevádzkovateľom základných služieb môže príslušný orgán alebo jednotka CSIRT informovať o jednotlivých incidentoch verejnosť, ak je informovanosť verejnosti potrebná na zabránenie incidentu alebo na riešenie prebiehajúceho incidentu.

7. Príslušné orgány konajúce spoločne v rámci skupiny pre spoluprácu môžu vypracovať a prijať usmernenia týkajúce sa okolností, za akých sú prevádzkovatelia základných služieb povinní oznamovať incidenty, ako aj parametrov na určenie závažnosti vplyvu incidentu, ako sa uvádza v odseku 4.

Článok 15

Vykonávanie a presadzovanie

1. Členské štáty zabezpečia, aby príslušné orgány mali právomoci a prostriedky potrebné na posúdenie toho, či prevádzkovatelia základných služieb dodržiavajú svoje povinnosti podľa článku 14, a s tým súvisiacich dôsledkov pre bezpečnosť sietí a informačných systémov.

2. Členské štáty zabezpečia, aby príslušné orgány mali právomoci a prostriedky potrebné na to, aby mohli od prevádzkovateľov základných služieb požadovať, aby poskytovali:

a) informácie potrebné na posúdenie bezpečnosti svojich sietí a informačných systémov vrátane zdokumentovaných bezpečnostných politík;

b) dôkazy o účinnom vykonávaní bezpečnostných politík, ako sú výsledky bezpečnostného auditu, ktorý vykoná príslušný orgán alebo kvalifikovaný audítor, pričom v prípade, že ho vykoná kvalifikovaný audítor, sa výsledky spolu s podkladovými dôkazmi poskytnú príslušnému orgánu.

Pri požadovaní takýchto informácií alebo dôkazov príslušný orgán uvedie účel žiadosti a aké informácie sa požadujú.

3. Po posúdení informácií alebo výsledkov bezpečnostných auditov uvedených v odseku 2 môže príslušný orgán vydať prevádzkovateľom základných služieb záväzné pokyny na nápravu zistených nedostatkov.

4. Príslušný orgán pri riešení incidentov, ktoré majú za následok porušenie ochrany osobných údajov, úzko spolupracuje s orgánmi na ochranu údajov.

KAPITOLA V

BEZPEČNOSŤ SIETÍ A INFORMAČNÝCH SYSTÉMOV POSKYTOVATEĽOV DIGITÁLNYCH SLUŽIEB

Článok 16

Bezpečnostné požiadavky a oznamovanie incidentov

1. Členské štáty zabezpečia, aby poskytovatelia digitálnych služieb identifikovali riziká súvisiace s bezpečnosťou sietí a informačných systémov, ktoré používajú v kontexte poskytovania služieb uvedených v prílohe III v rámci Únie, a aby prijali vhodné a primerané technické a organizačné opatrenia na riadenie týchto rizík. S ohľadom na najnovší technický vývoj musia tieto opatrenia zabezpečiť takú úroveň bezpečnosti sietí a informačných systémov, ktorá zodpovedá miere daného rizika, a zohľadniť tieto prvky:

a) bezpečnosť systémov a zariadení;

b) riešenie incidentov;

c) riadenie kontinuity činnosti;

d) monitorovanie, audit a skúšanie;

e) súlad s medzinárodnými normami.

2. Členské štáty zabezpečia, aby poskytovatelia digitálnych služieb prijali opatrenia na zabránenie a minimalizovanie vplyvu incidentov ovplyvňujúcich bezpečnosť ich sietí a informačných systémov na služby uvedené v prílohe III, ktoré sa poskytujú v rámci Únie, s cieľom zabezpečiť kontinuitu týchto služieb.

3. Členské štáty zabezpečia, aby poskytovatelia digitálnych služieb bezodkladne oznámili príslušnému orgánu alebo jednotke CSIRT každý incident, ktorý má závažný vplyv na poskytovanie služby uvedenej v prílohe III, ktorú poskytujú v rámci Únie. Oznámenia obsahujú informácie, ktoré umožnia príslušnému orgánu alebo jednotke CSIRT určiť závažnosť prípadného cezhraničného vplyvu. Oznámenie nesmie mať pre oznamujúcu stranu za následok vyššiu zodpovednosť.

4. Pri určovaní, či je vplyv incidentu závažný, sa zohľadňujú najmä tieto parametre:

a) počet používateľov postihnutých incidentom, najmä používateľov využívajúcich danú službu na účely poskytovania vlastných služieb;

b) dĺžka trvania incidentu;

c) geografické rozšírenie z hľadiska oblasti, ktorú incident postihol;

d) stupeň narušenia fungovania služby;

e) rozsah vplyvu na hospodárske a spoločenské činnosti.

Povinnosť oznámiť incident sa uplatňuje len v prípade, ak má poskytovateľ digitálnych služieb prístup k informáciám, ktoré sú potrebné na posúdenie dosahu incidentu na základe parametrov uvedených v prvom pododseku.

5. Ak prevádzkovateľ základných služieb využíva tretiu stranu, ktorou je poskytovateľ digitálnych služieb, na poskytovanie služby, ktorá je základná pre zachovanie rozhodujúcich spoločenských a hospodárskych činností, uvedený prevádzkovateľ oznamuje každý závažný vplyv na kontinuitu základných služieb, ktorý je dôsledkom incidentu, ktorý postihol poskytovateľa digitálnych služieb.

6. Ak je to vhodné, a najmä ak sa incident uvedený v odseku 3 týka dvoch alebo viacerých členských štátov, príslušný orgán alebo jednotka CSIRT informuje ostatné dotknuté členské štáty. Príslušné orgány, jednotky CSIRT a jednotné kontaktné miesta pritom v súlade s právom Únie alebo vnútroštátnymi právnymi predpismi, ktoré sú v súlade s právom Únie, chránia bezpečnosť a obchodné záujmy poskytovateľa digitálnych služieb, ako aj dôvernosť poskytnutých informácií.

7. Po porade s dotknutým poskytovateľom digitálnych služieb môže príslušný orgán alebo jednotka CSIRT a prípadne orgány alebo jednotky CSIRT ďalších dotknutých členských štátov informovať verejnosť o jednotlivých incidentoch alebo požiadať o to poskytovateľa digitálnych služieb, ak je informovanosť verejnosti potrebná na zabránenie incidentu alebo riešenie prebiehajúceho incidentu alebo ak je zverejnenie incidentu vo verejnom záujme z iného dôvodu.

8. Komisia prijme vykonávacie akty s cieľom bližšie špecifikovať prvky uvedené v odseku 1 a parametre uvedené v odseku 4 tohto článku. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 22 ods. 2 do 9. augusta 2017.

9. Komisia môže prijať vykonávacie akty stanovujúce formáty a postupy uplatniteľné na oznamovacie požiadavky. Uvedené vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 22 ods. 2.

10. Bez toho, aby bol dotknutý článok 1 ods. 6, členské štáty nesmú ukladať poskytovateľom digitálnych služieb žiadne ďalšie bezpečnostné ani oznamovacie požiadavky.

11. Kapitola V sa nevzťahuje na mikropodniky a malé podniky, ako sú vymedzené v odporúčaní Komisie 2003/361/ES ([1]).

([1]) Odporúčanie Komisie 2003/361/ES zo 6. mája 2003 o vymedzení pojmov mikro, malé a stredné podniky (Ú. v. EÚ L 124, 20.5.2003, s. 36).

Článok 17

Vykonávanie a presadzovanie

1. Členské štáty zabezpečia, aby príslušné orgány konali podľa potreby prostredníctvom následných opatrení dohľadu, ak majú k dispozícii dôkazy, že poskytovateľ digitálnych služieb nespĺňa požiadavky stanovené v článku 16. Takéto dôkazy môže predložiť príslušný orgán iného členského štátu, v ktorom sa služba poskytuje.

2. Na účely odseku 1 musia mať príslušné orgány potrebné právomoci a prostriedky na to, aby od poskytovateľov digitálnych služieb požadovali:

a) poskytovanie informácií potrebných na posúdenie bezpečnosti ich sietí a informačných systémov vrátane zdokumentovaných bezpečnostných politík;

b) napravenie akéhokoľvek nesplnenia požiadaviek stanovených v článku 16.

3. Ak sa hlavná prevádzkareň alebo zástupca poskytovateľa digitálnych služieb nachádza v členskom štáte, ale jeho siete a informačné systémy sú umiestnené v jednom alebo vo viacerých iných členských štátoch, príslušný orgán členského štátu, v ktorom sa nachádza hlavná prevádzkareň alebo zástupca, a príslušné orgány týchto iných členských štátov spolupracujú a v prípade potreby si navzájom pomáhajú. Takáto pomoc a spolupráca môže zahŕňať výmenu informácií medzi dotknutými príslušnými orgánmi a žiadosti o prijatie opatrení dohľadu uvedených v odseku 2.

Článok 18

Právomoc a teritorialita

1. Na účely tejto smernice sa má za to, že poskytovateľ digitálnych služieb podlieha právomoci členského štátu, v ktorom má hlavnú prevádzkareň. V prípade poskytovateľa digitálnych služieb sa má za to, že hlavnú prevádzkareň má v tom členskom štáte, v ktorom sa nachádza jeho sídlo.

2. Poskytovateľ digitálnych služieb, ktorý nie je usadený v Únii, ale ponúka v nej služby uvedené v prílohe III, určí svojho zástupcu v Únii. Zástupca musí byť usadený v jednom z členských štátov, v ktorých ponúka služby. Má sa za to, že poskytovateľ digitálnych služieb podlieha právomoci toho členského štátu, v ktorom je usadený jeho zástupca.

3. Určením zástupcu poskytovateľa digitálnych služieb nie sú dotknuté právne kroky, ktoré by mohli byť podniknuté proti samotnému poskytovateľovi digitálnych služieb.

KAPITOLA VI

NORMALIZÁCIA A DOBROVOĽNÉ OZNAMOVANIE

Článok 19

Normalizácia

1. Členské štáty v záujme presadzovania zbližujúceho sa vykonávania článku 14 ods. 1 a 2 a článku 16 ods. 1 a 2 a bez toho, aby ukladali povinnosť využívať určitý typ technológie alebo diskriminovali v prospech takéhoto využívania, podporujú využívanie európskych alebo medzinárodne uznávaných noriem a špecifikácií, ktoré sú relevantné pre bezpečnosť sietí a informačných systémov.

2. Agentúra ENISA v spolupráci s členskými štátmi vypracúva odporúčania a usmernenia týkajúce sa technických oblastí, ktoré sa majú zvážiť v súvislosti s odsekom 1, ako aj odporúčania a usmernenia týkajúce sa už existujúcich noriem vrátane vnútroštátnych noriem členských štátov, ktoré by sa mohli vzťahovať na uvedené oblasti.

Článok 20

Dobrovoľné oznamovanie

1. Bez toho, aby bol dotknutý článok 3, subjekty, ktoré neboli určené ako prevádzkovatelia základných služieb a nie sú poskytovateľmi digitálnych služieb, môžu na dobrovoľnom základe oznamovať incidenty, ktoré majú závažný vplyv na kontinuitu služieb, ktoré poskytujú.

2. Pri spracúvaní oznámení členské štáty konajú v súlade s postupom stanoveným v článku 14. Členské štáty môžu uprednostniť spracúvanie povinných oznámení pred dobrovoľnými oznámeniami. Dobrovoľné oznámenia sa spracúvajú len vtedy, ak takéto spracovanie nepredstavuje neprimerané alebo nenáležité zaťaženie dotknutých členských štátov.

V dôsledku dobrovoľného oznámenia nevznikajú oznamujúcemu subjektu žiadne povinnosti, ktoré by sa naň neboli vzťahovali, ak by oznámenie nepodal.

KAPITOLA VII

ZÁVEREČNÉ USTANOVENIA

Článok 21

Sankcie

Členské štáty stanovia pravidlá ukladania sankcií za porušenie vnútroštátnych predpisov prijatých podľa tejto smernice a prijmú všetky opatrenia potrebné na zabezpečenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty do 9. mája 2018 informujú Komisiu o týchto pravidlách a opatreniach a bezodkladne jej oznámia akékoľvek následné zmeny, ktoré na ne majú vplyv.

Článok 22

Postup výboru

1. Komisii pomáha Výbor pre bezpečnosť sietí a informačných systémov. Uvedený výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 nariadenia (EÚ) č. 182/2011.

Článok 23

Preskúmanie

1. Komisia do 9. mája 2019 predloží Európskemu parlamentu a Rade správu, v ktorej posúdi jednotnosť prístupu členských štátov pri identifikácii prevádzkovateľov základných služieb.

2. Komisia pravidelne skúma fungovanie tejto smernice a podáva o tom správu Európskemu parlamentu a Rade. Na tento účel a s cieľom ďalej napredovať v strategickej a operačnej spolupráci Komisia zohľadní správy skupiny pre spoluprácu a siete jednotiek CSIRT o skúsenostiach získaných na strategickej a operačnej úrovni. Vo svojom preskúmaní Komisia posúdi aj zoznamy uvedené v prílohách II a III a jednotnosť pri identifikácii prevádzkovateľov základných služieb a služieb v odvetviach uvedených v prílohe II. Prvá správa sa predloží do 9. mája 2021.

Článok 24

Prechodné opatrenia

1. Bez toho, aby bol dotknutý článok 25, a s cieľom poskytnúť členským štátom ďalšie možnosti pre vhodnú spoluprácu počas obdobia transpozície začne skupina pre spoluprácu a sieť jednotiek CSIRT vykonávať úlohy stanovené v článku 11 ods. 3 a článku 12 ods. 3 do 9. februára 2017.

2. V období od 9. februára 2017 do 9. novembra 2018 a s cieľom podporiť členské štáty, aby zaujímali jednotný prístup k procesu identifikácie prevádzkovateľov základných služieb, skupina pre spoluprácu prerokuje procesný rámec, podstatu a typ vnútroštátnych opatrení, ktoré umožnia identifikáciu prevádzkovateľov základných služieb v konkrétnom odvetví v súlade s kritériami stanovenými v článkoch 5 a 6. Skupina pre spoluprácu na žiadosť členského štátu tiež prerokuje konkrétne návrhy vnútroštátnych opatrení daného členského štátu, ktoré umožňujú identifikáciu prevádzkovateľov základných služieb v konkrétnom odvetví, v súlade s kritériami stanovenými v článkoch 5 a 6.

3. Členské štáty do 9. februára 2017 a na účely tohto článku zabezpečia svoje primerané zastúpenie v skupine pre spoluprácu a sieti jednotiek CSIRT.

Článok 25

Transpozícia

1. Členské štáty prijmú a uverejnia do 9. mája 2018 zákony, iné právne predpisy a správne opatrenia potrebné na dosiahnutie súladu s touto smernicou. Bezodkladne o tom informujú Komisiu.

Tieto opatrenia uplatňujú od 10 mája 2018.

Členské štáty uvedú priamo v prijatých opatreniach alebo pri ich úradnom uverejnení odkaz na túto smernicu. Podrobnosti o odkaze upravia členské štáty.

2. Členské štáty oznámia Komisii znenie hlavných ustanovení vnútroštátnych právnych predpisov, ktoré prijmú v oblasti pôsobnosti tejto smernice.

Článok 26

Nadobudnutie účinnosti

Táto smernica nadobúda účinnosť dvadsiatym dňom po jej uverejnení v *Úradnom vestníku Európskej únie*.

Článok 27

Adresáti

Táto smernica je určená členským štátom.

V Štrasburgu 6. júla 2016

Za Európsky parlament	*Za Radu*
predseda	*predseda*
M. SCHULZ	I. KORČOK

PRÍLOHA I

POŽIADAVKY TÝKAJÚCE SA JEDNOTIEK PRE RIEŠENIE POČÍTAČOVÝCH BEZPEČNOSTNÝCH INCIDENTOV (JEDNOTKY CSIRT) A ICH ÚLOHY

Požiadavky na jednotky CSIRT a ich úlohy musia byť primerane a jasne vymedzené a podporované vnútroštátnymi politikami a/alebo právnymi prepismi. Zahŕňajú:

1. požiadavky na jednotky CSIRT

   a) Jednotky CSIRT zabezpečujú vysokú úroveň dostupnosti svojich komunikačných služieb, a to tak, že predchádzajú tomu, že zlyhajú ako celok, ak zlyhá ich ľubovoľný jediný bod, a majú k dispozícii niekoľko spôsobov, ktorými ich možno kontaktovať a ktorými môžu oni kedykoľvek kontaktovať iných. Okrem toho sú komunikačné kanály jasne vymedzené a zainteresované strany a spolupracujúci partneri sú o nich dobre informovaní.

   b) Pracoviská jednotiek CSIRT a podporné informačné systémy sú umiestnené na zabezpečených miestach.

   c) Zabezpečenie kontinuity činnosti:

      i) Jednotky CSIRT majú zavedený vhodný systém riadenia a zasielania žiadostí v záujme jednoduchšieho odovzdávania.

      ii) Jednotky CSIRT sú primerane personálne vybavené, aby sa zabezpečila stála dostupnosť ich služieb.

      iii) Jednotky CSIRT využívajú infraštruktúru, ktorej kontinuita je zabezpečená. Na tento účel sú k dispozícii záložné systémy a záložný pracovný priestor.

   d) Jednotky CSIRT musia mať možnosť zapojiť sa do sietí medzinárodnej spolupráce, pokiaľ majú v úmysle byť ich súčasťou.

2. Úlohy jednotiek CSIRT

   a) Úlohy jednotiek CSIRT zahŕňajú prinajmenšom:

      i) monitorovanie incidentov na vnútroštátnej úrovni;

      ii) vydávanie včasného varovania, upozornení, oznamovanie a šírenie informácií o rizikách a incidentoch príslušným zainteresovaným stranám;

      iii) reagovanie na incidenty;

      iv) zabezpečovanie dynamickej analýzy rizík a incidentov a získavanie informácií o situácii;

      v) účasť na činnosti siete jednotiek CSIRT.

   b) Jednotky CSIRT nadviažu spoluprácu so súkromným sektorom.

   c) V záujme uľahčenia spolupráce jednotky CSIRT podporujú prijímanie a využívanie spoločnej alebo normalizovanej praxe v oblasti:

      i) postupov na riešenie incidentov a rizík;

      ii) systémov klasifikácie incidentov, rizík a informácií.

PRÍLOHA II

TYPY SUBJEKTOV NA ÚČELY ČLÁNKU 4 BODU 4

Odvetvie	Pododvetvie	Typ subjektu
1. Energetika	a) Elektrická energia	— elektroenergetické podniky, ako sa vymedzujú v článku 2 bode 35 smernice Európskeho parlamentu a Rady 2009/72/ES ([1]), ktoré vykonávajú funkciu „dodávky“ podľa vymedzenia v článku 2 bode 19 uvedenej smernice
		— prevádzkovatelia distribučnej sústavy, ako sa vymedzujú v článku 2 bode 6 smernice 2009/72/ES
		— prevádzkovatelia prenosovej sústavy, ako sa vymedzujú v článku 2 bode 4 smernice 2009/72/ES
	b) Ropa	— prevádzkovatelia ropovodov
		— prevádzkovatelia zariadení na ťažbu, rafinovanie a spracovanie ropy, jej skladovanie a prepravu
	c) Plyn	— dodávateľské podniky, ako sa vymedzujú v článku 2 bode 8 smernice Európskeho parlamentu a Rady 2009/73/ES ([2])
		— prevádzkovatelia distribučnej siete, ako sa vymedzujú v článku 2 bode 6 smernice 2009/73/ES
		— prevádzkovatelia prepravnej siete, ako sa vymedzujú v článku 2 bode 4 smernice 2009/73/ES
		— prevádzkovatelia zásobníkov, ako sa vymedzujú v článku 2 bode 10 smernice 2009/73/ES
		— prevádzkovatelia zariadení LNG, ako sa vymedzujú v článku 2 bode 12 smernice 2009/73/ES
		— plynárenské podniky, ako sa vymedzujú v článku 2 bode 1 smernice 2009/73/ES
		— prevádzkovatelia zariadení na rafinovanie a spracovanie zemného plynu
2. Doprava	a) Letecká doprava	— leteckí dopravcovia, ako sa vymedzujú v článku 3 bode 4 nariadenia Európskeho parlamentu a Rady (ES) č. 300/2008 ([3])
		— riadiace orgány letiska, ako sa vymedzujú v článku 2 bode 2 smernice Európskeho parlamentu a Rady 2009/12/ES ([4]), letiská, ako sa vymedzujú v článku 2 bode 1 uvedenej smernice vrátane hlavných letísk uvedených v oddiele 2 prílohy II k nariadeniu Európskeho parlamentu a Rady (EÚ) č. 1315/2013 ([5]), a subjekty prevádzkujúce pomocné zariadenia nachádzajúce sa na letiskách

Odvetvie	Pododvetvie	Typ subjektu
		— prevádzkovatelia poskytujúci služby riadenia letovej prevádzky (ATC), ako sa vymedzujú v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (ES) č. 549/2004 ([6])
	b) Železničná doprava	— manažéri infraštruktúry, ako sa vymedzujú v článku 3 bode 2 smernice Európskeho parlamentu a Rady 2012/34/EÚ ([7])
		— železničné podniky, ako sa vymedzujú v článku 3 bode 1 smernice 2012/34/EÚ, vrátane prevádzkovateľov servisných zariadení, ako sa vymedzujú v článku 3 bode 12 smernice 2012/34/EÚ
	c) Vodná doprava	— spoločnosti prevádzkujúce vnútrozemskú, námornú a pobrežnú osobnú a nákladnú vodnú dopravu, ako sa vymedzujú pre námornú dopravu v prílohe I k nariadeniu Európskeho parlamentu a Rady (ES) č. 725/2004 ([8]), bez jednotlivých plavidiel, ktoré tieto spoločnosti prevádzkujú
		— riadiace orgány prístavu, ako sa vymedzujú v článku 3 bode 1 smernice Európskeho parlamentu a Rady 2005/65/ES ([9]), vrátane ich prístavných zariadení, ako sa vymedzujú v článku 2 bode 11 nariadenia (ES) č. 725/2004, a subjekty prevádzkujúce činnosti a zariadenia v rámci prístavu
		— prevádzkovatelia plavebno-prevádzkových služieb, ako sa vymedzujú v článku 3 písm. o) smernice Európskeho parlamentu a Rady 2002/59/ES ([10])
	d) Cestná doprava	— cestné orgány zodpovedné za kontrolu riadenia cestnej premávky, ako sa vymedzujú v článku 2 bode 12 delegovaného nariadenia Komisie (EÚ) 2015/962 ([11])
		— prevádzkovatelia inteligentných dopravných systémov, ako sa vymedzujú v článku 4 bode 1 smernice Európskeho parlamentu a Rady 2010/40/EÚ ([12])
3. Bankovníctvo		úverové inštitúcie, ako sa vymedzujú v článku 4 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013 ([13])
4. Infraštruktúry finančných trhov		— prevádzkovatelia obchodných miest, ako sa vymedzujú v článku 4 bode 24 smernice Európskeho parlamentu a Rady 2014/65/EÚ ([14])
		— centrálne protistrany, ako sa vymedzujú v článku 2 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 648/2012 ([15])
5. Zdravotníctvo	Zdravotnícke zariadenia (vrátane nemocníc a súkromných kliník)	poskytovatelia zdravotnej starostlivosti, ako sa vymedzujú v článku 3 písm. g) smernice Európskeho parlamentu a Rady 2011/24/EÚ ([16])

Odvetvie	Pododvetvie	Typ subjektu
6. Dodávka a distribúcia pitnej vody		dodávatelia a distribútori vody určenej na ľudskú spotrebu, ako sa vymedzujú v článku 2 ods. 1 písm. a) smernice Rady 98/83/ES ([17]), s výnimkou distribútorov, u ktorých je distribúcia vody na ľudskú spotrebu iba časťou ich celkovej činnosti v oblasti distribúcie iných komodít a tovaru, ktorá sa nepovažuje za základnú službu
7. Digitálna infraštruktúra		— internetové prepojovacie uzly (IXP)
		— poskytovatelia služieb DNS
		— registre domén najvyššej úrovne (TLD)

([1]) Smernica Európskeho parlamentu a Rady 2009/72/ES z 13. júla 2009 o spoločných pravidlách pre vnútorný trh s elektrinou, ktorou sa zrušuje smernica 2003/54/ES (Ú. v. EÚ L 211, 14.8.2009, s. 55).
([2]) Smernica Európskeho parlamentu a Rady 2009/73/ES z 13. júla 2009 o spoločných pravidlách pre vnútorný trh so zemným plynom, ktorou sa zrušuje smernica 2003/55/ES (Ú. v. EÚ L 211, 14.8.2009, s. 94).
([3]) Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002 (Ú. v. EÚ L 97, 9.4.2008, s. 72).
([4]) Smernica Európskeho parlamentu a Rady 2009/12/ES z 11. marca 2009 o letiskových poplatkoch (Ú. v. EÚ L 70, 14.3.2009, s. 11).
([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1315/2013 z 11. decembra 2013 o usmerneniach Únie pre rozvoj transeurópskej dopravnej siete a o zrušení rozhodnutia č. 661/2010/EÚ (Ú. v. EÚ L 348, 20.12.2013, s. 1).
([6]) Nariadenie Európskeho parlamentu a Rady (ES) č. 549/2004 z 10. marca 2004, ktorým sa stanovuje rámec na vytvorenie jednotného európskeho neba (rámcové nariadenie) (Ú. v. EÚ L 96, 31.3.2004, s. 1).
([7]) Smernica Európskeho parlamentu a Rady 2012/34/EÚ z 21. novembra 2012, ktorou sa zriaďuje jednotný európsky železničný priestor (Ú. v. EÚ L 343, 14.12.2012, s. 32).
([8]) Nariadenie Európskeho parlamentu a Rady (ES) č. 725/2004 z 31. marca 2004 o zvýšení bezpečnosti lodí a prístavných zariadení (Ú. v. EÚ L 129, 29.4.2004, s. 6).
([9]) Smernica Európskeho parlamentu a Rady 2005/65/ES z 26. októbra 2005 o zvýšení bezpečnosti prístavov (Ú. v. EÚ L 310, 25.11.2005, s. 28).
([10]) Smernica Európskeho parlamentu a Rady 2002/59/ES z 27. júna 2002, ktorou sa zriaďuje monitorovací a informačný systém Spoločenstva pre lodnú dopravu a ktorou sa zrušuje smernica Rady 93/75/EHS (Ú. v. ES L 208, 5.8.2002, s. 10).
([11]) Delegované nariadenie Komisie (EÚ) 2015/962 z 18. decembra 2014, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2010/40/EÚ, pokiaľ ide o poskytovanie informačných služieb o doprave v reálnom čase v celej EÚ (Ú. v. EÚ L 157, 23.6.2015, s. 21).
([12]) Smernica Európskeho parlamentu a Rady 2010/40/EÚ zo 7. júla 2010 o rámci na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy (Ú. v. EÚ L 207, 6.8.2010, s. 1).
([13]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).
([14]) Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ (Ú. v. EÚ L 173, 12.6.2014, s. 349).
([15]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012, s. 1).
([16]) Smernica Európskeho parlamentu a Rady 2011/24/EÚ z 9. marca 2011 o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti (Ú. v. EÚ L 88, 4.4.2011, s. 45).
([17]) Smernica Rady 98/83/ES z 3. novembra 1998 o kvalite vody určenej na ľudskú spotrebu (Ú. v. ES L 330, 5.12.1998, s. 32).

PRÍLOHA III

DRUHY DIGITÁLNYCH SLUŽIEB NA ÚČELY ČLÁNKU 4 BODU 5

1. Online trhovisko
2. Internetový vyhľadávač
3. Služby cloud computingu