EURÓPSKA
KOMISIA

V Bruseli 4. 10. 2017
COM(2017) 476 final

ANNEX 1

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 476 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 476 final/2 of 4.10.2017

PRÍLOHA

k

OZNÁMENIU KOMISIE EURÓPSKEMU PARLAMENTU A RADE

Čo najlepšie využívanie sietí a informačných systémov - smerom k účinnej implementácii smernice 2016/1148/EÚ, pokiaľ ide o opatrenia na dosiahnutie vysokej všeobecnej úrovne bezpečnosti sietí a informačných systémov v EÚmeasures for a high common level of security of network and information systems across the Union

OBSAH

PRÍLOHA

1. Úvod

Cieľom tejto prílohy je prispieť k účinnému uplatňovaniu, vykonávaniu a presadzovaniu smernice (EÚ) 2016/1148 o bezpečnosti sietí a informačných systémov v Únii[1] (ďalej len „smernica NIS“ alebo „smernica“) a pomôcť členským štátom zabezpečiť účinné uplatňovanie práva EÚ. Konkrétnejšie má tri špecifické ciele: a) viac vnútroštátnym orgánom objasniť povinnosti uvedené v smernici, ktoré sa na ne vzťahujú; b) zaistiť účinné presadzovanie povinností, ktoré smernica ukladá subjektom v oblasti bezpečnostných požiadaviek a oznamovania incidentov a c) celkovo prispieť k právnej istote pre všetkých relevantných aktérov.

Na tieto účely príloha poskytuje usmernenie k nasledujúcim aspektom kľúčovým pre dosahovanie cieľa smernice NIS, ktorým je zaistiť v EÚ vysokú spoločnú úroveň bezpečnosti sietí a informačných systémov, o ktoré sa opiera fungovanie našej spoločnosti a hospodárstva:

- povinnosť členských štátov prijať národné stratégie v oblasti bezpečnosti sietí a informačných systémov (oddiel 2),
- zriadenie vnútroštátnych príslušných orgánov, jednotných kontaktných miest a jednotiek pre riešenie počítačových bezpečnostných incidentov (oddiel 3),
- požiadavky na bezpečnosť a oznamovanie incidentov, ktoré sa vzťahujú na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb (oddiel 4) a
- vzťah medzi smernicou NIS a inými právnymi predpismi (oddiel 5).

Pri príprave týchto usmernení Komisia využila podnety a analýzy získané v rámci prípravy smernice, vstupy od Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a od skupiny pre spoluprácu. Zároveň využila doterajšie skúsenosti členských štátov. Komisia podľa potreby zohľadnila hlavné zásady výkladu práva EÚ: znenie, kontext a ciele smernice NIS. Keďže smernica ešte nebola transponovaná, zatiaľ neexistujú žiadne rozsudky Súdneho dvora Európskej únie ani vnútroštátnych súdov. Judikatúru teda na usmernenie použiť nemožno.

Zhrnutie všetkých týchto informácií v jednom dokumente môže členským štátom poskytnúť dobrý prehľad o smernici a môžu ich zohľadniť pri príprave svojich vnútroštátnych právnych predpisov. Komisia zároveň zdôrazňuje, že táto príloha nie je záväzná a nemá za cieľ stanovovať nové pravidlá. Právomoc vykladať právo Únie s konečnou platnosťou prináleží Súdnemu dvoru Európskej únie.

[1] 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. Smernica nadobudla účinnosť 8. augusta 2016.

2. Národná stratégia v oblasti bezpečnosti sietí a informačných systémov

Podľa článku 7 smernice NIS majú členské štáty prijať národnú stratégiu v oblasti bezpečnosti sietí a informačných systémov, ktorú možno považovať za rovnocennú pojmu „národná stratégia kybernetickej bezpečnosti“ (NCSS). Zmyslom národnej stratégie je vymedziť strategické ciele a primerané politické a regulačné opatrenia v oblasti kybernetickej bezpečnosti. Koncepcia NCSS sa vo všeobecnosti používa na medzinárodnej scéne i v Európe, najmä v kontexte práce agentúry ENISA s členskými štátmi na národných stratégiách, z ktorej nedávno vzišla aktualizovaná príručka osvedčených postupov v oblasti NCSS[2].

V tomto oddiele Komisia objasňuje, ako smernica NIS zlepšuje pripravenosť členských štátov požiadavkou na robustné národné stratégie v oblasti bezpečnosti sietí a informačných systémov (článok 7). Oddiel je venovaný týmto aspektom: a) rozsah pôsobnosti stratégie a b) jej obsah a postup prijímania.

Ako sa bližšie opisuje ďalej v texte, správna transpozícia článku 7 smernice NIS je pre dosiahnutie jej cieľov kľúčová a vyžaduje si vyčlenenie primeraných finančných a ľudských zdrojov na tento účel.

2.1. Rozsah pôsobnosti národnej stratégie

V zmysle znenia článku 7 sa povinnosť prijať NCSS vzťahuje len na odvetvia uvedené v prílohe II (teda energetika, doprava, bankovníctvo, finančné trhy, zdravotníctvo, dodávka a distribúcia pitnej vody a digitálna infraštruktúra) „a služby uvedené v prílohe III“ (online trhovisko, internetový vyhľadávač a služby cloud computingu).

V článku 3 smernice sa osobitne uvádza zásada minimálnej harmonizácie, podľa ktorej členské štáty môžu prijať alebo zachovať ustanovenia, ktorých cieľom je dosiahnuť vyššiu úroveň bezpečnosti sietí a informačných systémov. Uplatnenie tejto zásady na povinnosť prijať stratégiu NCSS umožňuje členským štátom do tejto stratégie zahrnúť viac odvetví a služieb, než sa uvádza v prílohách II a III k smernici.

Podľa názoru Komisie a vzhľadom na cieľ smernice NIS, ktorým je vysoká spoločná úroveň bezpečnosti sietí a informačných systémov v Únii[3], by bolo vhodné vypracovať národnú stratégiu, ktorá zahŕňa všetky relevantné sféry spoločnosti a hospodárstva, a nielen odvetvia a digitálne služby, na ktoré sa vzťahuje príloha II, resp. III k smernici NIS. Je to v súlade s osvedčenou medzinárodnou praxou (pozri usmernenie ITU a analýzu OECD uvedené ďalej) i so smernicou NIS.

Ako sa vysvetľuje ďalej v texte, platí to najmä v prípade orgánov verejnej správy zodpovedných za iné odvetvia a služby než tie, ktoré sú uvedené v prílohách II a III k

---

[2] ENISA, *National Cyber-Security Strategy Good Practice* (Osvedčené postupy v oblasti národných stratégií kybernetickej bezpečnosti, 2016). K dispozícii na adrese: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[3] Pozri článok 1 ods. 1.

smernici. Verejné orgány môžu spracovávať citlivé informácie, ktoré opodstatňujú potrebu zahrnutia do stratégie NCSS a plánov riadenia, aby sa zabránilo únikom a zaručila primeraná ochrana týchto informácií.

2.2. Obsah a postup prijímania národných stratégií

Podľa článku 7 smernice NIS musí stratégia NCSS zahŕňať aspoň tieto prvky:

i) ciele a priority národnej stratégie v oblasti bezpečnosti sietí a informačných systémov;
ii) rámec riadenia na dosiahnutie cieľov a priorít národnej stratégie;
iii) identifikácia opatrení týkajúcich sa pripravenosti, reakcie a obnovy vrátane spolupráce medzi verejným a súkromným sektorom;
iv) určenie relevantných vzdelávacích programov, programov na zvyšovanie informovanosti a programov odbornej prípravy;
v) určenie plánov výskumu a vývoja;
vi) plán posudzovania rizika na účely identifikácie rizík a
vii) zoznam aktérov zapojených do vykonávania stratégie.

Ani článok 7, ani príslušné odôvodnenie 29 nestanovujú požiadavky na prijatie NCSS ani bližšie nešpecifikujú obsah NCSS. Z hľadiska procesu a dodatočných prvkov spojených s obsahom NCSS Komisia považuje ďalej uvedený postup za jednu z vhodných metód prijímania NCSS. Vychádza z analýzy skúseností členských štátov a tretích krajín pri príprave ich vlastných stratégií. Ďalším zdrojom informácií je školiaci nástroj pre NCSS od agentúry ENISA v podobe videoklipov a médií na stiahnutie na jej stránkach[4].

2.3. Proces a otázky, ktorým treba venovať pozornosť

Proces prípravy a následného prijatia národnej stratégie je komplexný, zahŕňa mnoho aspektov a ak má byť efektívny a úspešný, vyžaduje si neustále zapojenie odborníkov na kybernetickú bezpečnosť, občianskej spoločnosti a vnútroštátnej politickej scény. Nevyhnutnosťou je podpora zo strany vrcholovej administratívy – aspoň na úrovni štátneho tajomníka alebo rovnocennej úrovni gestorského ministerstva, ako aj politický patronát. Na úspešné prijatie NCSS možno zvážiť použitie týchto piatich krokov (pozri obrázok 1):

Prvý krok – **Stanovenie riadiacich zásad a strategických cieľov, ktoré má stratégia dosiahnuť**

Ako prvé by mali vnútroštátne príslušné orgány vymedziť určité kľúčové prvky, ktoré bude stratégia NCSS obsahovať, teda aké sú požadované výsledky (v článku 7 ods. 1 písm. a) smernice sa hovorí o *cieľoch a prioritách*), ako tieto výsledky dopĺňajú vnútroštátne sociálne a hospodárske politiky a či sú zlučiteľné s výsadami a záväzkami vyplývajúcimi z členstva štátu v Európskej únii. Ciele by mali byť konkrétne, merateľné, dosiahnuteľné, realistické a časovo ohraničené (SMART). Ilustračný príklad: „*Zabezpečíme, aby bola táto [časovo*

[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-training-tool.

ohraničená] stratégia založená na dôkladnom a komplexnom súbore ukazovateľov, ktorými možno merať pokrok na ceste k výsledkom, ktoré potrebujeme dosiahnuť.“[5]

Uvedené zahŕňa aj politické vyhodnotenie toho, či možno vykonávanie stratégie zabezpečiť dostatočným rozpočtom. Zároveň je potrebný opis zamýšľanej pôsobnosti stratégie a jednotlivých kategórií zainteresovaných strán z radov verejného i súkromného sektora, ktoré by mali byť zapojené do návrhu jednotlivých cieľov a opatrení.

Tento prvý krok možno dosiahnuť cielenými seminármi s vedúcimi predstaviteľmi ministerstiev a politikmi, ktoré budú moderovať odborníci na kybernetickú bezpečnosť s potrebnými profesionálnymi komunikačnými schopnosťami, aby dokázali vysvetliť dôsledky absentujúceho alebo slabého kybernetického zabezpečenia v modernom digitálnom hospodárstve a spoločnosti.

Druhý krok – **Vypracovanie obsahu stratégie**

Stratégia by mala obsahovať podporné opatrenia, časovo ohraničené kroky a kľúčové ukazovatele výsledkov pre výsledné hodnotenie, dolaďovanie a zdokonaľovanie po stanovenom implementačnom období. Tieto opatrenia by mali podporovať cieľ, priority a výsledky vytýčené ako riadiace zásady. O potrebe uviesť podporné opatrenia hovorí článok 7 ods. 1 písm. c) smernice NIS.

Odporúča sa vytvorenie riadiacej skupiny, ktorej predsedá gestorské ministerstvo a ktorá riadi proces prípravy a uľahčuje zber vstupov. V praxi to možno dosiahnuť zriadením viacerých redakčných skupín relevantných úradníkov a odborníkov zameraných na kľúčové všeobecné témy – napríklad posudzovanie rizika, pohotovostné plánovanie, riadenie incidentov, rozvoj zručností, zvyšovanie povedomia, výskum a priemyselný vývoj atď. Osobitne by sa mali zástupcovia každého odvetvia (napríklad energetika, doprava atď.) prizvať na vyhodnotenie dôsledkov svojho zapojenia vrátane vyčlenenia potrebných zdrojov, pričom určení prevádzkovatelia základných služieb a kľúčoví poskytovatelia digitálnych služieb by mali byť zapojení do stanovovania priorít a predkladania návrhov v procese prípravy. Angažovanie zainteresovaných strán z odvetví je nevyhnutné aj vzhľadom na potrebu zaistiť harmonizované vykonávanie smernice naprieč odvetviami, a pritom zohľadniť sektorové špecifiká.

Tretí krok – **Vytvorenie riadiaceho rámca**

V záujme efektívnosti a účinnosti by mal byť riadiaci rámec postavený na kľúčových zainteresovaných stranách, prioritách identifikovaných v procese návrhu, ako aj na obmedzeniach a kontexte vnútroštátnych administratívnych a politických štruktúr. Je vhodné zabezpečiť priame podávanie správ politickej úrovni, pričom rámec by mal byť schopný rozhodovania, prideľovania zdrojov a získavania vstupov od odborníkov na kybernetickú bezpečnosť i zainteresovaných strán z odvetvia. Článok 7 ods. 1 písm. b) smernice NIS

[5] Úryvok z národnej stratégie kybernetickej bezpečnosti Spojeného kráľovstva na roky 2016 – 2021, s. 67.

riadiaci rámec spomína a osobitne vyžaduje *zodpovednosti vládnych orgánov a ďalších relevantných aktérov*.

Štvrtý krok – **Zostavenie a revízia návrhu stratégie**

V tejto fáze by sa mal zostaviť a revidovať návrh stratégie, a to s použitím analýzy silných a slabých stránok, príležitostí a hrozieb (tzv. SWOT analýza), ktorá by mohla pomôcť určiť, či treba obsah revidovať. Po internej revízii by mali nasledovať konzultácie so zainteresovanými stranami. Zároveň bude nevyhnutné zorganizovať verejnú konzultáciu na priblíženie významu navrhovanej stratégie verejnosti, získanie vstupov zo všetkých možných zdrojov a zaistenie podpory pri získavaní zdrojov potrebných na následnú implementáciu stratégie.

Piaty krok – **Formálne prijatie**

Záverečný krok zahŕňa formálne prijatie na politickej úrovni s postačujúcim rozpočtom, ktorý ukazuje, že daný členský štát berie kybernetickú bezpečnosť vážne. Na dosiahnutie cieľov smernice NIS Komisia členské štáty nabáda, aby pri oznamovaní národnej stratégie Komisii podľa článku 7 ods. 3 uviedli informácie o rozpočte. Záväzky spojené s rozpočtom a potrebnými ľudskými zdrojmi sú absolútne kľúčové pre účinné vykonávanie stratégie i smernice. Keďže kybernetická bezpečnosť je stále pomerne novou a rýchlo sa rozvíjajúcou oblasťou verejnej politiky, vo väčšine prípadov budú potrebné nové investície, aj keď si celková situácia verejných financií vyžaduje škrty a úspory.

Poradenstvo k postupu prípravy a k obsahu národných stratégií môžu ponúknuť rôzne verejné i akademické zdroje, ako napríklad agentúra ENISA[6], Medzinárodná telekomunikačná únia (ITU)[7], OECD[8], Globálne fórum kybernetickej expertízy či Oxfordská univerzita[9].

2.4. Konkrétne kroky, ktoré musia členské štáty podniknúť do transpozičného termínu

Už pred prijatím smernice mali takmer všetky členské štáty[10] publikované dokumenty označené ako NCSS. V oddiele 6 tejto prílohy je uvedený aktuálny zoznam stratégií platných

---

6 ENISA, *National Cyber-Security Strategy Good Practice* (Osvedčené postupy v oblasti národných stratégií kybernetickej bezpečnosti, 2016). K dispozícii na adrese: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

7 ITU, *National Cybersecurity Strategy Guide* (Príručka k národným stratégiám kybernetickej bezpečnosti, 2011). K dispozícii na adrese: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.
ITU zároveň v roku 2017 vydá balík nástrojov na tvorbu národných stratégií kybernetickej bezpečnosti (pozri prezentáciu na adrese: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National%20Strategy%20Toolkit%20introduction.pdf).

8 OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies* (Zlomový bod v tvorbe politiky kybernetickej bezpečnosti: analýza novej generácie národných stratégií kybernetickej bezpečnosti, 2012). K dispozícii na adrese: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

9 Kapacitné centrum globálnej kybernetickej bezpečnosti a Oxfordská univerzita, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* [Model vývoja spôsobilostí (CMM) v oblasti kybernetickej bezpečnosti pre štáty, revidované znenie, 2016]. K dispozícii na adrese: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf.

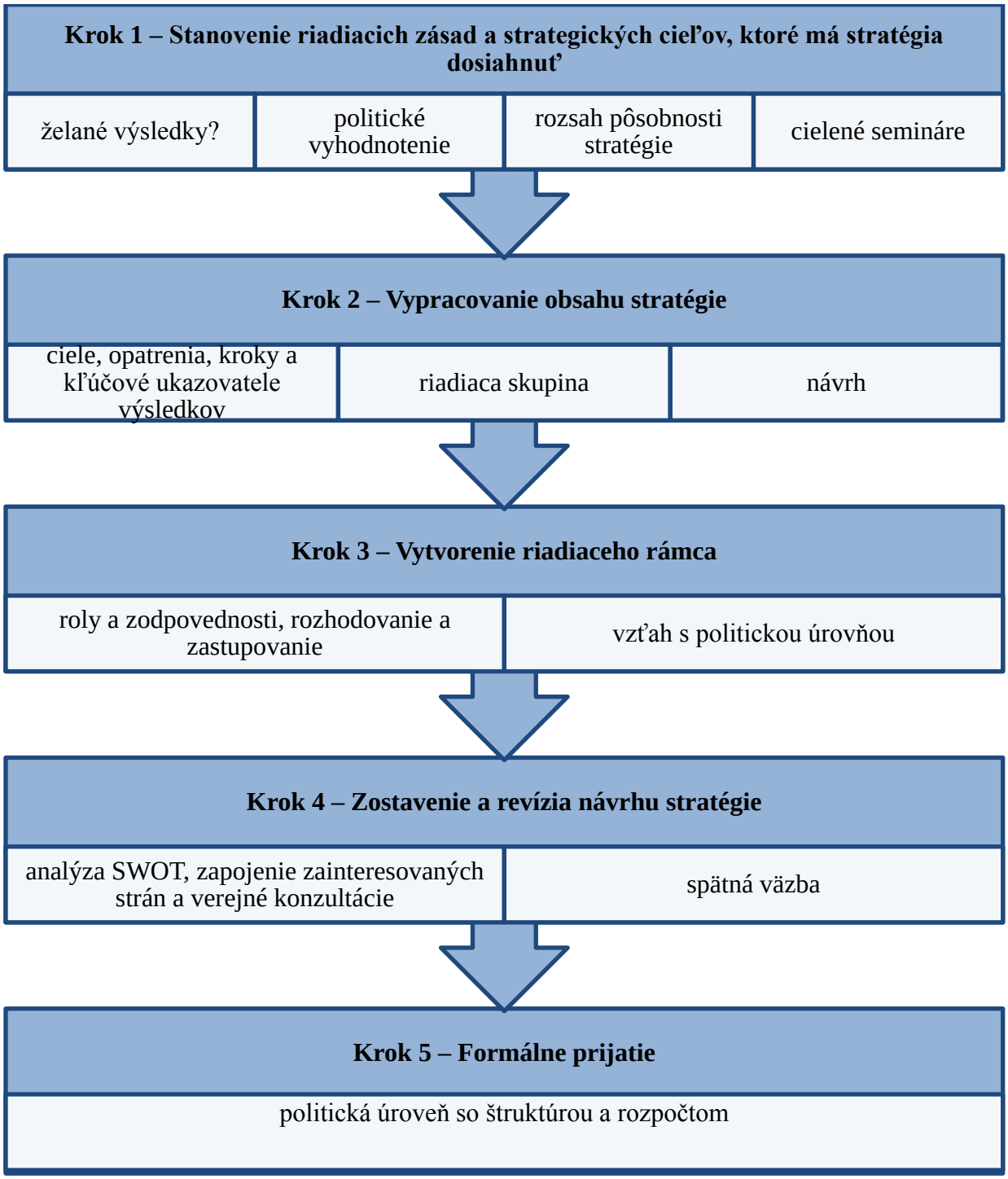
v jednotlivých členských štátoch[11]. Zväčša zahŕňajú strategické zásady, usmernenia, ciele a v niektorých prípadoch aj konkrétne opatrenia na zmiernenie rizík spojených s kybernetickou bezpečnosťou.

Keďže niektoré z týchto stratégií boli prijaté pred prijatím smernice NIS, nemusia nevyhnutne zahŕňať všetky prvky uvedené v článku 7. Na zaistenie správnej transpozície budú členské štáty musieť analyzovať nedostatky zmapovaním obsahu svojich NCSS podľa siedmich osobitných požiadaviek uvedených v článku 7 naprieč rozsahom odvetví uvedených v prílohe II a služieb uvedených v prílohe III k smernici. Zistené nedostatky potom možno riešiť revíziou existujúcich NCSS alebo rozhodnutím celkom nanovo zrevidovať zásady národnej stratégie pre siete a informačné systémy. Uvedené usmernenia o procese prijímania stratégie NCSS platia aj pre revíziu a aktualizáciu existujúcich NCSS.

[10] Okrem Grécka, kde sa národná stratégia kybernetickej bezpečnosti pripravuje od roku 2014 (pozri https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Tieto informácie vychádzajú z prehľadu NCSS, ktorý poskytla agentúra ENISA na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Obrázok 1: Päť krokov k prijatiu NCSS



3. Smernica NIS: vnútroštátne príslušné orgány, jednotné kontaktné miesta a jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT)

V článku 8 ods. 1 sa od členských štátov vyžaduje, aby určili jeden alebo viaceré vnútroštátne príslušné orgány, ktoré sa zaoberajú prinajmenšom odvetviami uvedenými v prílohe II a službami uvedenými v prílohe III k smernici a ktoré majú monitorovať uplatňovanie smernice. Členské štáty môžu touto úlohou poveriť existujúci orgán alebo orgány.

Tento oddiel sa zameriava na to, ako smernica NIS zvyšuje pripravenosť členských štátov tým, že vyžaduje účinné vnútroštátne príslušné orgány a jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT). Konkrétnejšie sa oddiel venuje povinnosti určiť vnútroštátne príslušné orgány vrátane roly jednotného kontaktného miesta. Venuje sa trom témam: a) možné vnútroštátne riadiace štruktúry (napr. centralizovaný vs. decentralizovaný model atď.) a ďalšie požiadavky; b) úloha jednotného kontaktného miesta a c) jednotky pre riešenie počítačových bezpečnostných incidentov.

3.1. Typ orgánov

Článok 8 smernice NIS vyžaduje od členských štátov určenie vnútroštátnych príslušných orgánov v oblasti bezpečnosti sietí a informačných systémov, pričom výslovne uvádza možnosť určiť „*jeden alebo viaceré vnútroštátne príslušné orgány*“. Toto politické rozhodnutie je vysvetlené v odôvodnení 30 smernice: „*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*.“

Znamená to, že členské štáty sa môžu rozhodnúť menovať jeden ústredný orgán, ktorý bude zodpovedať za všetky odvetvia a služby, ktoré pokrýva rozsah pôsobnosti smernice, alebo viacero orgánov, napríklad v závislosti od druhu odvetvia.

Pri rozhodovaní o tom, ktorý prístup zvoliť, môžu členské štáty čerpať zo skúseností s vnútroštátnymi prístupmi uplatnenými v kontexte existujúcej legislatívy o ochrane kritickej infraštruktúry (CIIP). Ako sa opisuje v tabuľke 1, pri CIIP sa členské štáty rozhodovali medzi centralizovaným alebo decentralizovaným prístupom pri prideľovaní kompetencií na vnútroštátnej úrovni. Príklady z jednotlivých štátov sa tu uvádzajú iba na ilustráciu s cieľom ukázať členským štátom existujúce organizačné rámce. Komisia teda netvrdí, že model, ktorý jednotlivé krajiny použili pri CIIP, by mali nevyhnutne použiť aj pri transpozícii smernice NIS.

Členské štáty sa môžu rozhodnúť aj pre rôzne hybridné riešenia zahŕňajúce prvky centralizovaného i decentralizovaného prístupu. Pri tejto voľbe možno vziať do úvahy aj predošlé štruktúry vnútroštátneho riadenia v rôznych odvetviach a službách, ktorých sa smernica týka, alebo ich môžu príslušné orgány a relevantné zainteresované strany identifikované ako prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb určiť nanovo. Významnými faktormi pri tomto rozhodnutí môžu byť aj dostupnosť odbornej expertízy v oblasti kybernetickej bezpečnosti, otázky získavania zdrojov, vzťahy medzi jednotlivými zainteresovanými stranami a národné záujmy (napríklad hospodársky rozvoj, verejná bezpečnosť atď.).

3.2. Publicita a ďalšie relevantné aspekty

V zmysle článku 8 ods. 7 musia členské štáty Komisii oznámiť určenie vnútroštátnych príslušných orgánov a ich úlohy. Treba tak urobiť do termínu na transpozíciu.

V článkoch 15 a 17 smernice NIS sa od členských štátov vyžaduje zabezpečiť, aby príslušné orgány mali osobitné právomoci a prostriedky potrebné na splnenie úloh uvedených v daných článkoch.

Okrem toho treba určenie konkrétnych subjektov za vnútroštátne príslušné orgány zverejniť. Smernica nestanovuje, ako k tomuto zverejneniu pristúpiť. Keďže cieľom tejto požiadavky je silné povedomie aktérov, na ktorých sa smernica NIS vzťahuje, i širokej verejnosti, a vzhľadom na skúsenosti z iných odvetví (telekomunikácie, bankovníctvo, liečivá) to možno podľa Komisie zabezpečiť napríklad dobre spropagovaným portálom.

Článok 8 ods. 5 smernice NIS vyžaduje, aby takéto orgány mali „primerané zdroje“ na výkon úloh, ktoré im smernica ukladá.

Tabuľka 1: Vnútroštátne prístupy k ochrane kritickej informačnej infraštruktúry (CIIP)

Agentúra ENSA v roku 2016 publikovala štúdiu[12] o rôznych prístupoch členských štátov k ochrane kritickej informačnej infraštruktúry. Opisujú sa v nej dva profily riadenia CIIP v členských štátoch, ktoré možno použiť aj v kontexte transpozície smernice NIS.

Profil 1: Decentralizovaný prístup s viacerými odvetvovými orgánmi zodpovedajúcimi za príslušné odvetvia a služby uvedené v prílohe II a III k smernici

Decentralizovaný prístup sa vyznačuje:

i) zásadou subsidiarity;
ii) intenzívnou spoluprácou verejných orgánov;
iii) odvetvovou legislatívou.

Zásada subsidiarity

Miesto zriaďovania alebo určovania jedinej agentúry s prierezovou zodpovednosťou sa decentralizovaný prístup riadi zásadou subsidiarity. Znamená to, že zodpovednosť za vykonávanie má v rukách príslušný odvetvový orgán, ktorý najlepšie rozumie danému odvetviu a už má so zainteresovanými stranami vybudovaný vzťah. Podľa tejto zásady sa rozhodnutia prijímajú čo najbližšie k tým, na ktorých majú dosah.

Intenzívna spolupráca verejných orgánov

Vzhľadom na rôznorodosť verejných orgánov zapojených do CIIP si mnoho členských štátov vytvorilo systémy spolupráce, ktoré slúžia na koordináciu práce a úsilia jednotlivých orgánov. Tieto systémy spolupráce môžu mať podobu neformálnych sietí alebo inštitucionalizovanejších fór či mechanizmov. Slúžia však iba na výmenu informácií a koordináciu jednotlivých verejných orgánov, pričom nad nimi nemajú žiadnu právomoc.

Odvetvová legislatíva

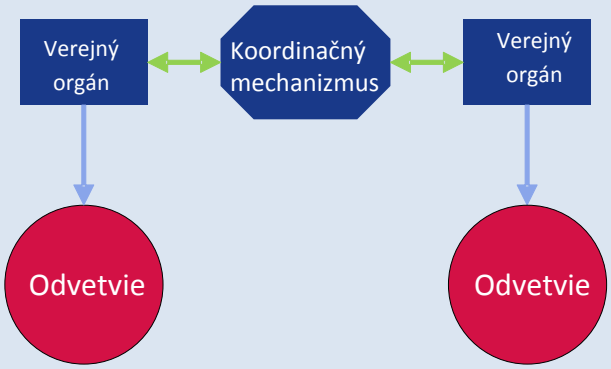
Krajiny, ktoré sa rozhodli pre decentralizovaný prístup v kritických odvetviach, často otázku CIIP centrálne legislatívne neupravujú. Miesto toho zostáva prijímanie zákonov a iných právnych predpisov v právomoci jednotlivých rezortov, takže sa medzi nimi môžu vyskytovať zásadné rozdiely. Výhodou tohto prístupu je zosúladenie opatrení spojených so sieťami a informačnými systémami s existujúcimi odvetvovými predpismi, čo uľahčuje akceptáciu daným odvetvím a zvyšuje účinnosť presadzovania príslušným orgánom.

Puristicky decentralizovaný prístup však zahŕňa podstatné riziko, že uplatňovanie smernice nebude naprieč jednotlivými odvetviami a službami konzistentné. V tomto prípade smernica zavádza jednotné národné kontaktné miesta so styčnou úlohou v cezhraničných otázkach; tieto

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (Hodnotenie, analýza a odporúčania k ochrane kritickej informačnej infraštruktúry, 2016). K dispozícii na adrese: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis.

subjekty by príslušný členský štát mohol zároveň poveriť internou koordináciou a spoluprácou medzi viacerými vnútroštátnymi príslušnými orgánmi v súlade s článkom 10 smernice.

Obrázok 2 – Decentralizovaný prístup



Príklady decentralizovaného prístupu

Dobrým príkladom krajiny s decentralizovaným prístupom k CIIP je Švédsko. Uplatňuje „systémový pohľad“, čo znamená, že hlavné úlohy v oblasti CIIP ako identifikácia kľúčových služieb a kritických infraštruktúr, koordinácia a podpora prevádzkovateľov, regulačné úlohy, ako aj opatrenia núdzovej pripravenosti spadajú do zodpovednosti rôznych orgánov a obcí. Medzi tieto orgány patrí napríklad švédska agentúra pre nepredvídané udalosti v oblasti civilnej ochrany (MSB), švédska poštová a telekomunikačná agentúra (PTS) a viaceré švédske agentúry z rezortu obrany, armády a presadzovania práva.

Na koordináciu činnosti jednotlivých agentúr a verejných subjektov švédska vláda vytvorila sieť spolupráce, ktorá zahŕňa orgány „so špecifickými spoločenskými zodpovednosťami v oblasti informačnej bezpečnosti“. Táto skupina pre spoluprácu v otázkach informačnej bezpečnosti (SAMFI) je zložená zo zástupcov rôznych orgánov a schádza sa niekoľkokrát ročne, aby prediskutovala otázky národnej informačnej bezpečnosti. Práca SAMFI sa venuje najmä politicko-strategickým otázkam a zahŕňa témy ako technické otázky a štandardizácia, vnútroštátne i medzinárodné dianie v oblasti informačnej bezpečnosti, či riadenie a prevencia incidentov v informačných technológiách. [Švédska agentúra pre nepredvídané udalosti v oblasti civilnej ochrany (MSB), 2015].

Švédsko neprijalo o CIIP žiaden ústredný zákon, ktorý by sa vzťahoval na všetkých prevádzkovateľov kritickej informačnej infraštruktúry (CII) vo všetkých odvetviach. Prijímanie legislatívy stanovujúcej povinnosti firiem v konkrétnych sektoroch je zodpovednosťou príslušných verejných orgánov. MSB má napríklad právo prijímať predpisy pre vládne orgány v oblasti informačnej bezpečnosti, zatiaľ čo PTS môže od prevádzkovateľov vyžadovať prijatie určitých technických či organizačných bezpečnostných opatrení na základe sekundárnej legislatívy.

Ďalším príkladom krajiny s podobným profilom je Írsko. Pridržiava sa „doktríny subsidiarity“, kde je každé ministerstvo zodpovedné za identifikáciu CII a posudzovanie rizika vo svojej

oblasti. Ani tu sa na celoštátnej úrovni neprijali žiadne konkrétne predpisy o CIIP. Legislatíva je odvetvová a týka sa najmä energetiky a telekomunikácií (2015). Ďalšími príkladmi sú Rakúsko, Cyprus a Fínsko.

Profil 2: Centralizovaný prístup s jedným ústredným orgánom zodpovedajúcim za všetky odvetvia a služby uvedené v prílohe II a III k smernici

Centralizovaný prístup sa vyznačuje:

i) jedným ústredným orgánom pre všetky odvetvia;
ii) komplexnou legislatívou.

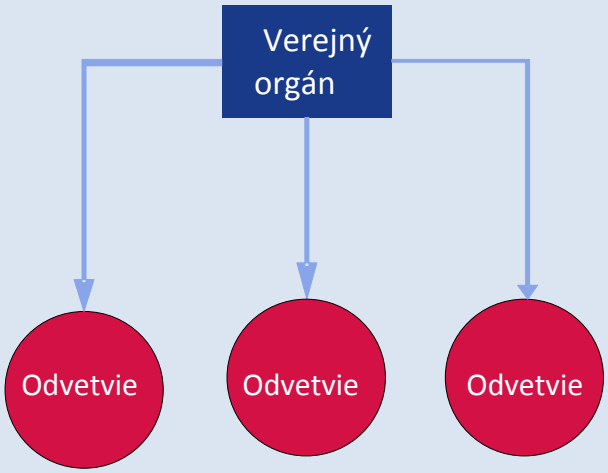
Jeden ústredný orgán pre všetky odvetvia

Členské štáty, ktoré uplatňujú centralizovaný prístup, zriadili orgány so zodpovednosťami a rozsiahlymi právomocami vo viacerých alebo všetkých kľúčových odvetviach, resp. rozšírili právomoci existujúcich orgánov. Tieto hlavné orgány pre oblasť CIIP vykonávajú viaceré úlohy ako pohotovostné plánovanie, riadenie núdzových situácií, regulácia či podpora súkromných prevádzkovateľov. V mnohých prípadoch sú súčasťou hlavného orgánu pre CIIP vnútroštátne alebo vládne jednotky CSIRT. Pri ústrednom orgáne je vzhľadom na celkový nedostatok zručností v oblasti kybernetickej bezpečnosti pravdepodobná vyššia koncentrácia príslušnej expertízy, než pri viacerých odvetvových orgánoch.

Komplexná legislatíva

Komplexná legislatíva stanovuje povinnosti a požiadavky všetkým prevádzkovateľom infraštruktúry CII vo všetkých odvetviach. Môže ísť o nové komplexné zákony alebo doplnenie existujúcej odvetvovej legislatívy. Tento prístup by uľahčil konzistentné uplatňovanie smernice NIS vo všetkých pokrytých odvetviach a službách. Predišlo by sa riziku medzier vo vykonávaní, ktoré hrozia pri viacerých orgánoch so špecifickou pôsobnosťou.

Obrázok 3 – Centralizovaný prístup



Príklady centralizovaného prístupu

Dobrým príkladom členského štátu EÚ s centralizovaným prístupom je Francúzsko. Jeho *Agence Nationale de la Sécurité des Systèmes d'Information* (národná agentúra pre bezpečnosť informačných systémov – ANSSI) bola v roku 2011 vymenovaná za hlavný vnútroštátny orgán obrany informačných systémov. ANSSI má silné postavenie v oblasti dohľadu nad „prevádzkovateľmi kľúčového významu“ (PKV): môže im nariadiť bezpečnostné opatrenia a vykonávať u nich bezpečnostné audity. Okrem toho je hlavným jednotným kontaktným miestom pre PKV, ktorí majú povinnosť nahlasovať agentúre bezpečnostné incidenty.

V prípade bezpečnostných incidentov zodpovedá agentúra ANSSI v oblasti CIIP za nepredvídané udalosti a rozhoduje o opatreniach, ktoré musia prevádzkovatelia v reakcii na krízu prijať. Opatrenia vlády koordinuje operačné centrum ANSSI. Detekcia hrozieb a reakcia na incidenty na operačnej úrovni je zodpovednosťou jednotky CERT-FR, ktorá je súčasťou agentúry.

Francúzsko zaviedlo pre oblasť CIIP komplexný právny rámec. Predseda vlády v roku 2006 nariadil zostavenie zoznamu odvetví s kritickou infraštruktúrou. Na základe tohto zoznamu, kde sa identifikovalo dvanásť kľúčových sektorov, vláda určila zhruba 250 PKV. V roku 2013 vstúpil do platnosti zákon o armádnom plánovaní[13]. Ten ukladá PKV rôzne povinnosti vrátane nahlasovania incidentov či prijímania bezpečnostných opatrení. Požiadavky sa povinne vzťahujú na všetkých PKV vo všetkých odvetviach (francúzsky Senát, 2013).

3.3. Smernica NIS, článok 9: Jednotky pre riešenie počítačových bezpečnostných incidentov (jednotky CSIRT)

V článku 9 sa od členských štátov vyžaduje určenie jednej alebo viacerých jednotiek CSIRT, ktoré zodpovedajú za riešenie rizík a incidentov v odvetviach uvedených v prílohe II k smernici a službách uvedených v prílohe III. Vzhľadom na požiadavku minimálnej harmonizácie zakotvenú v článku 3 smernice môžu členské štáty využiť jednotky CSIRT aj v ďalších odvetviach, na ktoré sa smernica nevzťahuje, ako napríklad verejná správa.

Členské štáty sa môžu rozhodnúť zriadiť jednotku CSIRT v rámci vnútroštátneho príslušného orgánu[14].

3.4. Úlohy a požiadavky

Úlohy určených jednotiek CSIRT stanovené v prílohe I k smernici NIS zahŕňajú:

- monitorovanie incidentov na vnútroštátnej úrovni,

[13] La loi de programmation militaire.
[14] Pozri článok 9 ods. 1 poslednú vetu.

- vydávanie včasného varovania, upozornení, oznamovanie a šírenie informácií o rizikách a incidentoch príslušným zainteresovaným stranám,
- reagovanie na incidenty,
- zabezpečovanie dynamickej analýzy rizík a incidentov a získavanie informácií o situácii a
- účasť na činnosti siete vnútroštátnych jednotiek CSIRT (sieť CSIRT) zriadenej článkom 12.

V článku 14 ods. 3, 5 a 6 a článku 16 ods. 3, 6 a 7 sa stanovujú ďalšie osobitné úlohy v spojení s oznamovaním incidentov, ak členský štát rozhodne, že tieto roly môže jednotka CSIRT plniť spolu s vnútroštátnymi príslušnými orgánmi alebo namiesto nich.

Pri transpozícii smernice môžu členské štáty rozhodnúť o role jednotiek CSIRT v rámci požiadaviek na oznamovanie incidentov. Priame povinné podávanie správ jednotkám CSIRT je možnosť výhodná z hľadiska administratívnej efektívnosti, ale členské štáty sa môžu rozhodnúť aj pre priame podávanie správ vnútroštátnym príslušným orgánom, pričom jednotky CSIRT majú právo na prístup k oznámeným informáciám. Jednotky CSIRT v konečnom dôsledku zaujíma riešenie problémov z hľadiska odrádzania od kybernetických incidentov, ich odhaľovania, reakcie na ne a zmierňovania ich dosahu (čo platí aj pre incidenty, ktoré netreba povinne oznamovať) spolu so zainteresovanými stranami a dodržiavanie predpisov je skôr vecou vnútroštátnych príslušných orgánov.

V zmysle článku 9 ods. 3 smernice musia členské štáty zároveň zabezpečiť, aby takéto jednotky CSIRT mali prístup k bezpečnej a odolnej infraštruktúre IKT.

Článok 9 ods. 4 smernice od členských štátov vyžaduje, aby Komisiu informovali o rozsahu a hlavných prvkoch postupu pri riešení incidentov určenými jednotkami CSIRT.

Požiadavky na jednotky CSIRT určené členskými štátmi sú uvedené v prílohe I k smernici NIS. Jednotky musia zabezpečiť vysokú úroveň dostupnosti svojich komunikačných služieb. Ich pracoviská a podporné informačné systémy musia byť umiestnené na zabezpečených miestach a musia byť schopné zaistiť kontinuitu činnosti. Okrem toho by sa jednotkám CSIRT malo umožniť zapojenie do sietí medzinárodnej spolupráce.

3.5. Pomoc pri vytváraní jednotiek CSIRT

Program kybernetickej bezpečnosti infraštruktúr digitálnych služieb (DSI) v rámci Nástroja na prepájanie Európy (NPE) môže z prostriedkov EÚ výrazne podporiť financovanie na pomoc jednotkám CSIRT členských štátov pri zlepšovaní ich spôsobilostí a pri ich vzájomnej spolupráci na základe mechanizmu spolupráce pri výmene informácií. Tento mechanizmus spolupráce, ktorý sa vyvíja v rámci projektu SMART 2015/1089, má uľahčiť rýchlu a účinnú dobrovoľnú operačnú spoluprácu medzi jednotkami CSIRT členských štátov – najmä na úlohách zverených sieti jednotiek CSIRT článkom 12 smernice.

Podrobnosti o príslušných výzvach na predkladanie návrhov na budovanie kapacít jednotiek CSIRT v členských štátoch sú k dispozícii na webových stránkach Výkonnej agentúry Európskej komisie pre inovácie a siete (INEA)[15].

Riadiaca rada programu kybernetickej bezpečnosti DSI v rámci NPE je neformálnou štruktúrou politického usmerňovania a podpory jednotiek CSIRT členských štátov pri budovaní kapacít a zavádzaní mechanizmu dobrovoľnej spolupráce.

Každá novozriadená jednotka CSIRT alebo jednotka určená na plnenie úloh uvedených v prílohe I k smernici NIS môže na zlepšenie a zefektívnenie práce využiť poradenstvo a expertízu agentúry ENISA[16]. V tomto smere treba podotknúť, že jednotky CSIRT členských štátov by mohli ako referenciu použiť niektoré nedávne výsledky práce agentúry. Konkrétne, ako sa uvádza v oddiele 7 tejto prílohy, agentúra vyprodukovala viacero dokumentov a štúdií, v ktorých sa opisujú osvedčené postupy a technické odporúčania zahŕňajúce posudzovanie stupňa vývoja rôznych spôsobilostí a služieb jednotiek CSIRT. Okrem toho sa o svoje usmernenia a osvedčené postupy podelili aj siete jednotiek CSIRT na svetovej (FIRST[17]) i európskej úrovni (Trusted Introducer, TI[18]).

3.6. Rola jednotného kontaktného miesta

Podľa článku 8 ods. 3 smernice NIS musí každý členský štát určiť národné jednotné kontaktné miesto so styčnou úlohou na zabezpečenie cezhraničnej spolupráce s príslušnými orgánmi iných členských štátov, ako aj so skupinou pre spoluprácu a sieťou CSIRT[19], ktorú zriaďuje samotná smernica. V odôvodnení 31 a článku 8 ods. 4 je vysvetlený účel tejto požiadavky – uľahčiť cezhraničnú spoluprácu a komunikáciu. Tá je mimoriadne potrebná vzhľadom na to, že členské štáty sa môžu rozhodnúť určiť viac než jeden vnútroštátny orgán. Jednotné kontaktné miesto tak uľahčí identifikáciu a spoluprácu orgánov z rôznych členských štátov.

Styčná úloha tohto jednotného kontaktného miesta bude pravdepodobne zahŕňať interakciu so sekretariátmi skupiny pre spoluprácu a siete CSIRT v prípadoch, kde národným jednotným kontaktným miestom nie je ani jednotka CSIRT, ani člen skupiny pre spoluprácu. Okrem toho musia členské štáty zabezpečiť informovanie jednotného kontaktného miesta o prijatých oznámeniach od prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb[20].

V článku 8 ods. 3 smernice sa uvádza, že ak členský štát uplatní centralizovaný prístup a určí iba jeden príslušný orgán, ten zároveň plní funkciu jednotného kontaktného miesta. Ak sa členský štát rozhodne pre decentralizovaný prístup, môže ako jednotné kontaktné miesto určiť niektorý z jednotlivých príslušných orgánov. Bez ohľadu na zvolený inštitucionálny model, ak sú príslušný orgán, jednotka CSIRT a jednotné kontaktné miesto samostatnými subjektmi,

---

15 K dispozícii na adrese: https://ec.europa.eu/inea/en/connecting-europe-facility.

16 Pozri článok 9 ods. 5 smernice NIS.

17 Fórum tímov pre reakciu na bezpečnostné incidenty a pre bezpečnosť (https://www.first.org/).

18 https://www.trusted-introducer.org/.

19 Sieť vnútroštátnych jednotiek CSIRT na účely operačnej spolupráce medzi členskými štátmi podľa článku 12.

20 Pozri článok 10 ods. 3.

členské štáty majú povinnosť zabezpečiť ich účinnú spoluprácu pri plnení povinností stanovených v smernici[21].

Jednotné kontaktné miesto musí do 9. augusta 2018 a potom každý rok predkladať skupine pre spoluprácu súhrnnú správu o prijatých oznámeniach, ktorá obsahuje počet oznámení, charakter oznámených incidentov a opatrenia prijaté orgánmi ako informovanie ostatných dotknutých členských štátov o incidente či poskytnutie relevantných informácií oznamujúcemu podniku na riešenie incidentu[22]. Na žiadosť príslušného orgánu alebo jednotky CSIRT musí jednotné kontaktné miesto postúpiť oznámenia prevádzkovateľov základných služieb jednotným kontaktným miestam ostatných členských štátov, ktorých sa incident dotýka[23].

Členské štáty musia Komisiu o určení jednotného kontaktného miesta a o jeho úlohách informovať do termínu na transpozíciu. Určenie jednotného kontaktného miesta sa má uverejniť rovnako ako pri vnútroštátnych príslušných orgánoch. Komisia uverejní zoznam určených jednotných kontaktných miest.

3.7. Sankcie

Článok 21 poskytuje členským štátom priestor na rozhodnutie o druhu a povahe platných sankcií, ktoré však musia byť účinné, primerané a odrádzajúce. Inými slovami, členské štáty v zásade môžu slobodne rozhodnúť o maximálnej výške sankcií stanovených vo vnútroštátnej legislatíve, no zvolená suma alebo percento by mali vnútroštátnym orgánom umožňovať v každom konkrétnom prípade uložiť účinné, primerané a odrádzajúce sankcie pri zohľadnení rôznych faktorov ako závažnosť alebo frekvencia daného porušenia.

4. Subjekty s povinnosťami z hľadiska bezpečnostných požiadaviek a oznamovania incidentov

Subjekty s významnou úlohou v spoločnosti a hospodárstve, o ktorých sa hovorí v článku 4 ods. 4 a 5 smernice ako o prevádzkovateľoch základných služieb (PZS) a poskytovateľoch digitálnych služieb (PDS) musia prijať vhodné bezpečnostné opatrenia a oznamovať závažné incidenty príslušným vnútroštátnym orgánom. Dôvodom je, že dosah bezpečnostných incidentov v týchto službách môže vážne ohroziť ich prevádzku, čo môže viesť k výraznému narušeniu hospodárskych činností a fungovania spoločnosti ako takej, a tým potenciálne narušiť dôveru používateľa a spôsobiť značné škody hospodárstvu Únie[24].

V tomto oddiele sa uvádza prehľad subjektov, ktoré spadajú do rozsahu pôsobnosti príloh II a III k smernici NIS, ako aj ich povinnosti. Téma identifikácie prevádzkovateľov základných služieb je tiež pokrytá pomerne vyčerpávajúco vzhľadom na jej význam pre harmonizované vykonávanie smernice NIS v EÚ. Oddiel sa intenzívne venuje aj vymedzeniu pojmov

[21] Pozri článok 10 ods. 1.
[22] Tamže.
[23] Pozri článok 14 ods. 5.
[24] Pozri odôvodnenie 2.

digitálna infraštruktúra a poskytovateľ digitálnych služieb. Zároveň poskytuje náhľad na možné zahrnutie ďalších odvetví a bližšie vysvetľuje špecifický prístup k PDS.

4.1. Prevádzkovatelia základných služieb (PZS)

Smernica NIS explicitne nestanovuje, ktoré konkrétne subjekty sa majú považovať za PZS spadajúcich do rozsahu jej pôsobnosti. Miesto toho stanovuje kritériá, ktoré majú členské štáty uplatniť v procese identifikácie na určenie toho, ktoré jednotlivé spoločnosti typologicky zodpovedajúce subjektom uvedeným v prílohe II sa budú považovať za prevádzkovateľov základných služieb, a teda sa na ne budú vzťahovať povinnosti stanovené v smernici.

4.1.1. Typ subjektov uvedených v prílohe II k smernici NIS

V článku 4 ods. 4 sú PZS vymedzení ako verejné alebo súkromné subjekty, ktorých typ sa uvádza v prílohe II k smernici a ktoré spĺňajú kritériá stanovené v článku 5 ods. 2. V prílohe II sa uvádzajú odvetvia, pododvetvia a typ subjektov, pri ktorých musia členské štáty použiť proces identifikácie podľa článku 5 ods. 2[25]. Medzi spomínané odvetvia patrí energetika, doprava, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, zásobovanie vodou a digitálna infraštruktúra.

Pri väčšine subjektov spadajúcich do „tradičných“ odvetví obsahuje legislatíva EÚ ustálené vymedzenia, na ktoré sa príloha II odvoláva. V prípade digitálnej infraštruktúry uvedenej v bode 7 prílohy II vrátane internetových prepojovacích uzlov, systémov názvov domén a registrov domén najvyššej úrovne to tak však nie je. Preto sa tieto pojmy na objasnenie v ďalšej časti podrobne vysvetľujú.

1. Internetový prepojovací uzol (IXP)

Pojem „internetový prepojovací uzol“ je vymedzený v článku 4 ods. 13 a bližšie vysvetlený v odôvodnení 18 a možno ho opísať ako sieťové zariadenie, ktoré umožňuje prepojenie viac než dvoch nezávislých technicky samostatných systémov, pričom sa používa najmä na uľahčenie internetového dátového toku. Internetový prepojovací uzol možno opísať aj ako fyzické miesto, na ktorom si viacero sietí môže vymieňať dátové toky prostredníctvom sieťového prepínača. Hlavným účelom IXP je umožniť sieťam priame vzájomné prepojenie bez potreby jednej alebo viacerých sietí tretích strán. Poskytovateľ IXP zväčša nenesie zodpovednosť za smerovanie dátových tokov. Za to sú zodpovední poskytovatelia sietí. Priame prepojenie má mnoho výhod, no medzi hlavné patria náklady, oneskorenie a šírka pásma. Za dátové toky prúdiace cez prepojovací uzol si zväčša žiadna strana neúčtuje poplatok, zatiaľ čo za toky k poskytovateľovi internetových služieb (ISP) áno. Priame prepojenie je často fyzicky v tom istom meste ako obe príslušné siete, takže údaje nemusia prekonávať pri prenose medzi sieťami veľké vzdialenosti, čo znižuje oneskorenie.

[25] Identifikačný proces je podrobnejšie opísaný ďalej v bode 4.1.6.

Treba však poznamenať, že definícia IXP nezahŕňa fyzické body, ktoré vzájomne spájajú iba dve fyzické siete (t. j. sieťových poskytovateľov ako BASE alebo PROXIMUS). Pri transpozícii smernice preto členské štáty musia rozlišovať medzi prevádzkovateľmi, ktorí sprostredkujú výmenu agregovaných internetových dátových tokov medzi viacerými prevádzkovateľmi sietí, a prevádzkovateľmi s jedinou sieťou, ktorí si siete prepájajú na základe zmluvy o prepojení. V druhom z uvedených prípadov sieťoví poskytovatelia do vymedzenia uvedeného v článku 4 ods. 13 nespadajú. Je to vysvetlené v odôvodnení 18, kde sa uvádza, že IXP neposkytuje prístup do siete, neslúži ako poskytovateľ služieb tranzitu ani ako poskytovateľ príslušnej infraštruktúry. Poslednou kategóriou poskytovateľov sú podniky poskytujúce verejné komunikačné siete a/alebo služby, na ktoré sa vzťahujú bezpečnostné a oznamovacie povinnosti v zmysle článkov 13a a 13b smernice 2002/21/ES a ktoré sú teda z rozsahu pôsobnosti smernice NIS vyňaté[26].

2. Systém názvov domén (DNS)

Pojem „systém názvov domén“ sa v článku 4 ods. 14 vymedzuje ako „*hierarchický distribuovaný systém pomenovaní v sieti, ktorý prekladá vyhľadávanie názvov domén*“. Presnejšie možno systém DNS opísať ako hierarchický distribuovaný systém pomenovaní pre počítače, služby alebo akékoľvek iné zdroje pripojené k internetu, ktorý umožňuje kódovanie názvov domén na IP adresy. Hlavnou úlohou tohto systému je „prekladať“ pridelené názvy domén na IP adresy. DNS má na to vlastnú databázu, pričom na tento „preklad“ názvov domén na funkčné IP adresy používa názvové servery a prekladač. Hoci kódovanie názvov domén nie je jedinou zodpovednosťou systému DNS, ide o jeho hlavnú úlohu. Právna definícia v článku 4 ods. 14 sa zameriava na hlavnú rolu systému z pohľadu používateľa a nezaoberá sa technickejšími podrobnosťami ako fungovanie doménového menného priestoru, názvových serverov, prekladačov atď. Napokon sa v článku 4 ods. 15 objasňuje, kto sa má považovať za poskytovateľa služieb DNS.

3. Register domén najvyššej úrovne (TLD)

Register domén najvyššej úrovne je v článku 4 ods. 16 vymedzený ako subjekt spravujúci a prevádzkujúci registráciu názvov internetových domén v rámci určitej domény najvyššej úrovne. Táto správa a riadenie názvov domén zahŕňa kódovanie názvov TLD na IP adresy.

Za globálnu koordináciu koreňovej zóny DNS, adresy internetového protokolu a ďalšie zdroje spojené s internetovým protokolom zodpovedá Orgán pre prideľovanie čísiel na internete (IANA). Tento orgán je predovšetkým zodpovedný za prideľovanie generických domén najvyššej úrovne (gTLD) ako „.com“ a národných domén najvyššej úrovne (ccTLD) ako „.be“ prevádzkovateľom (registrom), ako aj za údržbu ich technických a administratívnych údajov. IANA spravuje globálny register všetkých pridelených TLD a zohráva rolu pri šírení tohto zoznamu medzi používateľmi internetu po celom svete, ako aj pri zavádzaní nových TLD.

[26] Vzťah medzi smernicou NIS a smernicou 2002/21/ES sa podrobnejšie opisuje v oddiele 5.2.

Významnou úlohou registrov je prideľovať názvy druhej úrovne tzv. držiteľom v ich príslušnej TLD. Ak chcú, môžu títo držitelia sami prideľovať doménové názvy tretej úrovne. Domény ccTLD reprezentujú krajinu alebo územie a vychádzajú z normy ISO 3166-1. Generické TLD zväčša nie sú spojené s určitým zemepisným vymedzením či krajinou.

Treba poznamenať, že prevádzka registra TLD môže zahŕňať poskytovanie DNS. Napríklad podľa pravidiel orgánu IANA pre delegovanie musí určený subjekt zodpovedný za ccTLD okrem iného dohliadať na názvy domén a prevádzkovať DNS príslušnej krajiny[27]. Takéto okolnosti musia členské štáty v procese identifikácie prevádzkovateľov základných služieb podľa článku 5 ods. 2 zohľadniť.

4.1.2. Identifikácia prevádzkovateľov základných služieb

Podľa požiadaviek článku 5 smernice sa od každého členského štátu vyžaduje, aby uskutočnil proces identifikácie všetkých subjektov typov uvedených v prílohe II zákonne usadených na území daného členského štátu. Ako výsledok tohto posúdenia sa všetky subjekty, ktoré spĺňajú kritériá stanovené v článku 5 ods. 2 identifikujú ako PZS a podliehajú bezpečnostným a oznamovacím povinnostiam podľa článku 14.

Prevádzkovateľov v každom odvetví a pododvetví majú členské štáty identifikovať do 9. novembra 2018. S cieľom pomôcť členským štátom v tomto procese skupina pre spoluprácu v súčasnosti pripravuje usmerňovací dokument s relevantnými informáciami o potrebných krokoch a osvedčených postupoch pri identifikácii PZS.

Okrem toho skupina pre spoluprácu v súlade s článkom 24 ods. 2 prerokuje procesný rámec, podstatu a typ vnútroštátnych opatrení, ktoré umožňujú identifikáciu prevádzkovateľov základných služieb v konkrétnych odvetviach. Členské štáty môžu do 9. novembra 2018 predložiť svoje návrhy vnútroštátnych opatrení umožňujúcich identifikáciu prevádzkovateľov základných služieb skupine pre spoluprácu na diskusiu.

4.1.3. Doplnenie ďalších odvetví

Vzhľadom na požiadavku minimálnej harmonizácie stanovenú v článku 3 môžu členské štáty prijať alebo zachovať legislatívu, ktorá zaisťuje vyššiu mieru bezpečnosti sietí a informačných systémov. Z tohto hľadiska majú členské štáty vo všeobecnosti voľnosť pri rozširovaní bezpečnostných a oznamovacích povinností podľa článku 14 aj na subjekty pôsobiace v iných odvetviach a pododvetviach ako tie, ktoré sa uvádzajú v prílohe II k smernici NIS. Rôzne členské štáty sa už rozhodli alebo zvažujú, že do pôsobnosti zahrnú niektoré z týchto dodatočných odvetví:

i) Verejná správa

Orgány verejnej správy môžu poskytovať základné služby podľa prílohy II k smernici, ktoré spĺňajú požiadavky stanovené v článku 5 ods. 2. V takom prípade sa na orgány verejnej správy, ktoré tieto služby ponúkajú, vzťahujú relevantné bezpečnostné požiadavky a oznamovacie povinnosti. Z toho *a contrario* vyplýva, že ak orgány verejnej správy ponúkajú

[27] Informácie k dispozícii na adrese: https://www.icann.org/resources/pages/delegation-2012-02-25-en.

služby, ktoré do uvedeného rozsahu nespadajú, na tieto služby sa príslušné povinnosti nevzťahujú.

Verejné správy sú zodpovedné za riadne poskytovanie verejných služieb orgánmi štátnej správy, regionálnymi a miestnymi samosprávami, agentúrami a súvisiacimi podnikmi. Tieto služby si často vyžadujú vytvorenie a spravovanie údajov o jednotlivcoch a organizáciách, ktoré sa môžu poskytovať a sprístupňovať viacerým verejným subjektom. Všeobecnejšie povedané, vysoká bezpečnosť sietí a informačných systémov vo verejnej správe je dôležitým záujmom celej spoločnosti a hospodárstva. Komisia preto zastáva názor, že by bolo rozumné, ak by členské štáty zvážili zahrnutie verejnej správy do rozsahu pôsobnosti vnútroštátnej legislatívy transponujúcej smernicu nad rámec poskytovania základných služieb v zmysle prílohy II a článku 5 ods. 2.

ii) Sektor pôšt

Poštový sektor zahŕňa poskytovanie poštových služieb ako príjem, triedenie, preprava a distribúcia zásielok.

iii) Potravinárstvo

Potravinárstvo sa týka výroby poľnohospodárskych a iných potravinových výrobkov a môže zahŕňať základné služby ako zaisťovanie potravinovej bezpečnosti, kvality a nezávadnosti potravín.

iv) Chemický a jadrový priemysel

Chemický a jadrový priemysel zahŕňa najmä skladovanie, výrobu a spracovanie chemických a petrochemických produktov či jadrového materiálu.

v) Životné prostredie

Environmentálne činnosti zahŕňajú poskytovanie tovarov a služieb potrebných na ochranu životného prostredia a spravovanie zdrojov. Sú teda zamerané na prevenciu, znižovanie a odstraňovanie znečistenia a ochranu dostupných prírodných zdrojov. V tomto odvetví by základnými službami mohli byť monitorovanie a kontrola znečistenia (napríklad vzduchu a vody) a meteorologických javov.

vi) Civilná ochrana

Cieľom odvetvia civilnej ochrany je prevencia, pripravenosť a reakcia na živelné pohromy i katastrofy spôsobené ľudskou činnosťou. Medzi služby poskytované na tento účel môže patriť aktivácia tiesňových čísel či prijímanie krokov na informovanie o núdzových stavoch, zamedzenie ich šírenia a ich riešenie.

4.1.4. Právomoc

Podľa článku 5 ods. 1 má každý členský štát identifikovať PZS s prevádzkarňou na jeho území. V ustanovení sa bližšie nešpecifikuje typ zákonného usadenia, ale v odôvodnení 21 sa uvádza, že takáto prevádzkareň znamená účinné a skutočné vykonávanie činnosti prostredníctvom stabilných zariadení, takže právna forma týchto zariadení by nemala byť určujúca. Znamená to, že členské štáty môžu mať vo svojej právomoci prevádzkovateľa

základných služieb nielen v prípadoch, keď má na ich území sídlo, ale aj vtedy, keď tam má napríklad pobočku alebo je tam inak zákonne usadený.

Z toho vyplýva, že určitý subjekt môže byť súčasne v pôsobnosti viacerých členských štátov.

4.1.5. Informácie, ktoré sa majú predkladať Komisii

Na účely preskúmania, ktoré musí Komisia vykonať v súlade s článkom 23 ods. 1 smernice NIS, sa od členských štátov žiada, aby jej do 9. novembra 2018 a následne každé dva roky predložili tieto informácie:

- vnútroštátne opatrenia umožňujúce identifikáciu PZS,
- zoznam základných služieb,
- počet identifikovaných PZS v každom z odvetví uvedených v prílohe II a ich významnosť v danom odvetví a
- prípadné prahové hodnoty na určenie úrovne poskytovania podľa počtu používateľov využívajúcich danú službu, ako sa uvádza v článku 6 ods. 1 písm. a), alebo významu konkrétneho subjektu v súlade s článkom 6 ods. 1 písm. f).

Preskúmanie podľa článku 23 ods. 1, ktoré predchádza komplexnej revízii smernice, odráža význam, ktorý spoluzákonodarcovia pripisujú správnej transpozícii smernice z hľadiska identifikácie prevádzkovateľov základných služieb, aby sa nefragmentoval trh.

Aby sa vykonalo čo najlepšie, Komisia nabáda členské štáty, aby o tejto téme v skupine pre spoluprácu diskutovali a vymieňali si relevantné skúsenosti. Komisia zároveň členské štáty nabáda, aby jej okrem všetkých informácií, ktorých zaslanie vyžaduje smernica, poskytli (podľa potreby v dôvernej forme) zoznamy identifikovaných prevádzkovateľov základných služieb, ktorí boli napokon vybraní. Ak by Komisia mala tieto zoznamy k dispozícii, uľahčilo a skvalitnilo by to jej posudzovanie konzistentnosti identifikačného procesu, a zároveň by bolo možné porovnať prístupy jednotlivých členských štátov, čím by sa lepšie dosiahli ciele smernice.

4.1.6. Ako uplatniť identifikačný proces?

Obrázok 4 znázorňuje šesť kľúčových otázok, ktoré by si mal vnútroštátny orgán v identifikačnom procese pri každom subjekte položiť. V nasledujúcej časti každá otázka zodpovedá jednému kroku, ktorý treba vykonať podľa článku 5 v spojení s článkom 6 pri súčasnom zohľadnení pertinentnosti článku 1 ods. 7.

Krok 1 – **Spadá daný subjekt do odvetvia/pododvetvia a zodpovedá typu podľa prílohy II k smernici?**

Vnútroštátny orgán by mal posúdiť, či subjekt s prevádzkarňou na jeho území spadá do odvetví a pododvetví uvedených v prílohe II k smernici. Príloha II zahŕňa viacero hospodárskych odvetví, ktoré sa považujú za nevyhnutné na zaistenie riadneho fungovania vnútorného trhu. Konkrétne hovorí príloha II o týchto odvetviach a pododvetviach:

- energetika: elektrina, ropa a plyn,
- doprava: letecká, železničná, vodná a cestná,
- bankovníctvo: úverové inštitúcie,
- infraštruktúry finančných trhov: obchodné miesta, centrálne protistrany,
- zdravotníctvo: zdravotnícke zariadenia (vrátane nemocníc a súkromných kliník),
- voda: dodávka a distribúcia pitnej vody,
- digitálna infraštruktúra: internetové prepojovacie uzly, poskytovatelia služieb systému názvov domén a registre domén najvyššej úrovne[28].

Krok 2 – **Uplatňuje sa *lex specialis*?**

V ďalšom kroku musí vnútroštátny orgán posúdiť, či sa uplatňujú ustanovenia *lex specialis* podľa článku 1 ods. 7. Konkrétne sa v ňom uvádza, že ak existuje právny akt Únie, ktorý ukladá poskytovateľom digitálnych služieb alebo prevádzkovateľom základných služieb bezpečnostné a/alebo oznamovacie povinnosti aspoň rovnocenné s príslušnými požiadavkami smernice NIS, uplatňujú sa príslušné povinnosti podľa osobitného právneho aktu. Okrem toho sa v odôvodnení 9 objasňuje, že ak je požiadavka článku 1 ods. 7 splnená, členské štáty by mali uplatňovať ustanovenia sektorovej legislatívy EÚ vrátane tých, ktoré sa týkajú právomoci. Z toho *a contrario* vyplýva, že príslušné ustanovenia smernice NIS by sa neuplatnili. V takom prípade by príslušný orgán nemal pokračovať v identifikačnom procese podľa článku 5 ods. 2[29].

Krok 3 – **Poskytuje daný prevádzkovateľ základnú službu v zmysle smernice?**

Podľa článku 5 ods. 2 písm. a) musí skúmaný subjekt poskytovať službu, ktorá má zásadný význam z hľadiska zachovania kľúčových spoločenských a/alebo hospodárskych činností. V tejto otázke by členské štáty mali vziať do úvahy, že jeden subjekt môže súčasne poskytovať základné aj iné služby. Z toho vyplýva, že bezpečnostné a oznamovacie požiadavky smernice NIS sa na určitého prevádzkovateľa budú vzťahovať len z hľadiska základných služieb.

Podľa článku 5 ods. 3 by mal členský štát zostaviť zoznam všetkých základných služieb, ktoré poskytujú PZS na jeho území. Tento zoznam treba predložiť Komisii do 9. novembra 2018 a potom každé dva roky[30].

Krok 4 – **Je služba závislá od siete a informačného systému?**

Ďalej treba objasniť, či táto služba spĺňa druhé kritérium uvedené v článku 5 ods. 2 písm. b), teda či poskytovanie základnej služby závisí od sietí a informačných systémov vymedzených v článku 4 ods. 1.

Krok 5 – **Mal by bezpečnostný incident závažný rušivý vplyv?**

V článku 5 ods. 2 písm. c) sa od vnútroštátneho orgánu vyžaduje posúdenie toho, či by incident mal závažný rušivý vplyv na poskytovanie danej služby. V tejto súvislosti sa v

[28] Tieto subjekty sa bližšie opisujú v bode 4.1.1.
[29] Podrobnosti o uplatniteľnosti *lex specialis* sú uvedené v oddiele 5.1.
[30] Pozri článok 5 ods. 7 písm. b).

článku 6 ods. 1 uvádza viacero medziodvetvových faktorov, ktoré treba pri tomto posudzovaní zohľadniť. Navyše v článku 6 ods. 2 sa stanovuje, že pri posudzovaní by sa mali podľa potreby zohľadniť aj faktory špecifické pre jednotlivé odvetvia.

Medziodvetvové faktory uvedené v článku 6 ods. 1 sú:

- počet používateľov využívajúcich službu, ktorú poskytuje daný subjekt,
- závislosť ostatných odvetví uvedených v prílohe II od služby, ktorú poskytuje daný subjekt,
- vplyv, ktorý by mohli mať incidenty z hľadiska rozsahu a trvania na hospodárske a spoločenské činnosti alebo verejnú bezpečnosť,
- trhový podiel daného subjektu,
- geografické rozšírenie z hľadiska oblasti, ktorú by incident mohol postihnúť,
- význam subjektu z hľadiska zachovania dostatočnej úrovne služby, berúc do úvahy dostupnosť alternatívnych spôsobov poskytovania danej služby.

Pokiaľ ide o **faktory špecifické pre dané odvetvie**, niekoľko príkladov, ktoré by mohli vnútroštátnym orgánom pomôcť, sa uvádza v odôvodnení 28 (pozri tabuľku 4).

Tabuľka 4: Príklady odvetvových faktorov, ktoré by sa mali zohľadniť pri rozhodovaní o závažnom rušivom vplyve v prípade incidentu

Odvetvie	Príklady faktorov špecifických pre dané odvetvie
Dodávatelia energie	objem produkcie elektrickej energie na celoštátnej úrovni alebo podiel na tejto produkcii
Dodávatelia ropy	denný objem dodanej ropy
Letecká doprava (vrátane letísk a leteckých prepravcov) **Železničná doprava** **Námorné prístavy**	podiel na celoštátnej preprave počet cestujúcich alebo operácií nákladnej dopravy za rok
Bankovníctvo alebo infraštruktúry finančných trhov	systémový význam vyplývajúci z celkového objemu aktív pomer celkového objemu aktív k HDP
Zdravotníctvo	počet pacientov, ktorí sú v starostlivosti daného poskytovateľa za rok
Produkcia, spracovanie a dodávka vody	objem produkcie, počet a typ odberateľov (napr. vrátane nemocníc, organizácií poskytujúcich verejné služby alebo jednotlivcov) existencia alternatívnych zdrojov vody na pokrytie potrieb tej istej geografickej oblasti

Treba objasniť, že členské štáty by pri posudzovaní podľa článku 5 ods. 2 nemali pridávať dodatočné kritériá okrem tých, ktoré sú uvedené v danom ustanovení, pretože by sa mohol

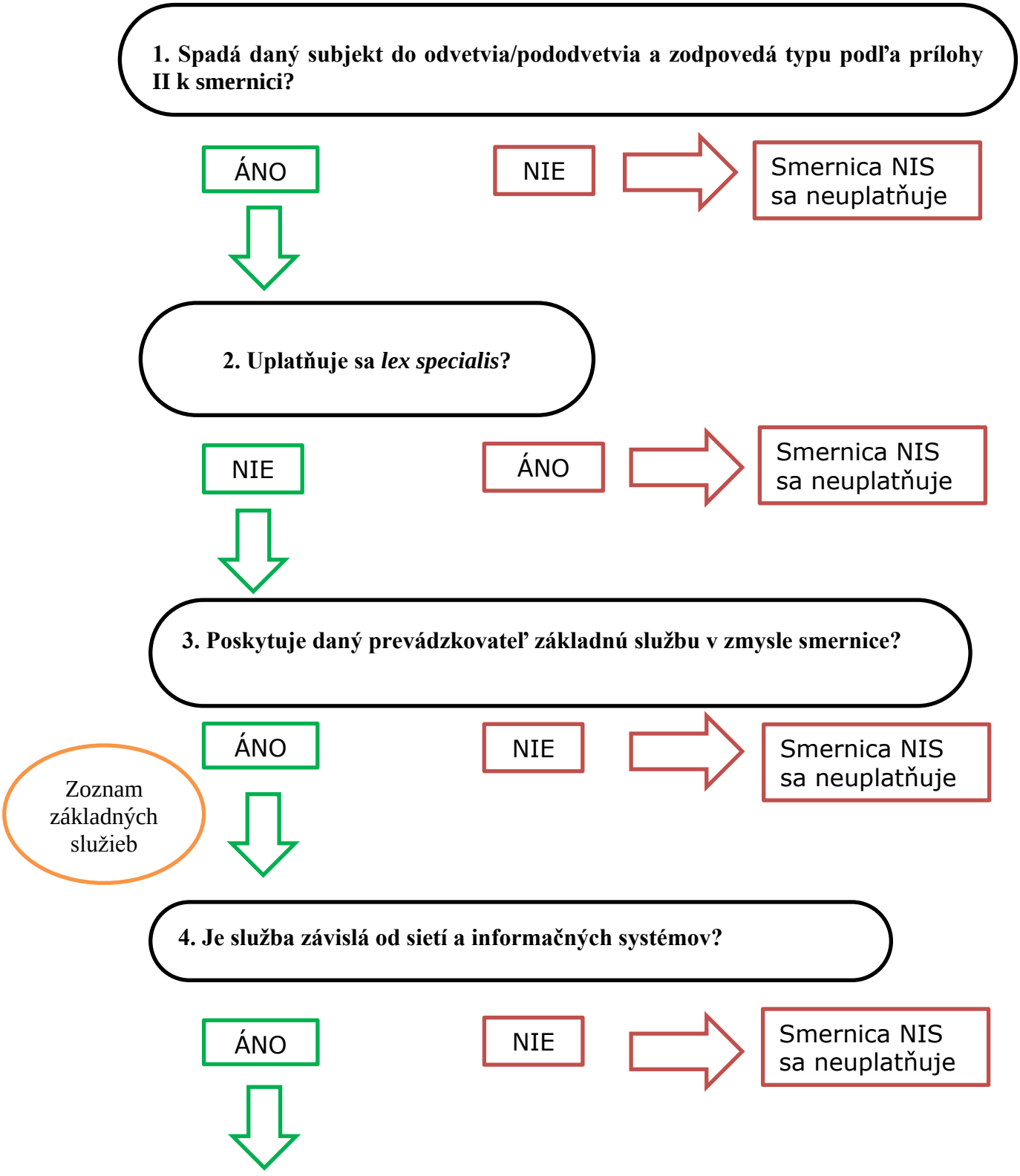
zúžiť počet identifikovaných PZS a ohroziť ich minimálna harmonizácia zakotvená v článku 3 smernice.

Krok 6 **– Poskytuje daný prevádzkovateľ základné služby v iných členských štátoch?**

Krok 6 sa týka prípadov, keď prevádzkovateľ poskytuje svoje základné služby v dvoch alebo viacerých členských štátoch. Článok 5 ods. 4 vyžaduje, aby členské štáty pred ukončením identifikačného procesu začali vzájomné konzultácie[31].

[31] Konzultačný proces je podrobnejšie opísaný v bode 4.1.7.

Obrázok 4: Identifikačný proces v šiestich krokoch



5. Mal by bezpečnostný incident závažný rušivý vplyv?

Medziodvetvové faktory (článok 6 ods. 1)

- **Počet používateľov** využívajúcich službu
- **Závislosť** ostatných základných odvetví od danej služby
- Vplyv prípadných incidentov na **hospodárske a spoločenské činnosti** alebo **verejnú bezpečnosť**
- Možnosť **geografického rozšírenia**
- Význam daného subjektu z hľadiska zachovania dostatočnej **úrovne služby**

Faktory špecifické pre odvetvie (príklady uvedené v odôvodnení 28)

- **Energetika**: objem produkcie elektrickej energie na celoštátnej úrovni alebo podiel na tejto produkcii
- **Doprava**: podiel na celoštátnej preprave a počet operácií za rok
- **Zdravotníctvo**: počet pacientov, ktorí sú

ÁNO

NIE → Smernica NIS sa neuplatňuje

6. Poskytuje daný prevádzkovateľ základné služby v iných členských štátoch?

ÁNO

NIE → Smernica NIS sa neuplatňuje

Povinná konzultácia s dotknutými členskými

Prijatie vnútroštátnych opatrení (napr. zoznam prevádzkovateľov základných služieb, politické a právne opatrenia).

4.1.7. Proces cezhraničnej konzultácie

Ak prevádzkovateľ poskytuje základné služby v dvoch alebo viacerých členských štátoch, článok 5 ods. 4 vyžaduje, aby tieto členské štáty pred uzavretím identifikačného procesu začali vzájomné konzultácie. Tie majú uľahčiť posudzovanie „kľúčovosti“ daného prevádzkovateľa z hľadiska cezhraničného dosahu.

Želaným výsledkom konzultácie je, aby si zapojené vnútroštátne orgány vymenili argumenty a postoje a ideálne dospeli v otázke identifikácie daného prevádzkovateľa k rovnakému záveru. Smernica NIS však nevylučuje možnosť, že sa závery členských štátov v otázke, či je daný subjekt PSZ alebo nie, budú líšiť. V odôvodnení 24 sa spomína možnosť členských štátov požiadať v tejto veci o pomoc skupinu pre spoluprácu.

Podľa názoru Komisie by sa členské štáty mali v týchto veciach usilovať o konsenzus, aby sa predišlo situácii, kde bude mať určitá spoločnosť v rôznych členských štátoch rôzne právne postavenie. Odchýlky by mali byť skutočne výnimočné – napríklad ak vykonáva subjekt určený za PZS v jednom členskom štáte len marginálne a nepodstatné činnosti v inom.

4.2. Bezpečnostné požiadavky

Článok 14 ods. 1 od členských štátov vyžaduje zabezpečiť, aby PZS zohľadňujúc najnovší technický vývoj prijali vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto organizácie využívajú pri poskytovaní svojich služieb. V súlade s článkom 14 ods. 2 musia primerané opatrenia brániť incidentom a minimalizovať ich vplyv.

Osobitnou oblasťou činnosti skupiny pre spoluprácu je v súčasnosti príprava nezáväzných usmernení vo veci bezpečnostných opatrení PZS[32]. Usmerňovací dokument by mala skupina finalizovať v poslednom štvrťroku 2017. Komisia nabáda členské štáty, aby usmerňovaciemu dokumentu skupiny pre spoluprácu venovali riadnu pozornosť, aby boli vnútroštátne ustanovenia o bezpečnostných požiadavkách v čo najväčšom súlade. Harmonizácia týchto požiadaviek by veľmi uľahčila súlad zo strany PZS, ktorí často poskytujú základné služby vo viac než len jednom členskom štáte, ako aj úlohu dohľadu vnútroštátnych príslušných orgánov a jednotiek CSIRT.

4.3. Požiadavky na oznamovanie

V zmysle článku 14 ods. 3 musia členské štáty zabezpečiť, aby PZS oznamovali „*incidenty, ktoré majú závažný vplyv na kontinuitu základných služieb, ktoré poskytujú*“. To znamená, že PZS by nemali oznamovať každý drobný incident, ale iba závažné incidenty s vplyvom na kontinuitu základnej služby. V článku 4 ods. 7 sa incident vymedzuje ako „*každá udalosť, ktorá má skutočne nepriaznivý vplyv na bezpečnosť sietí a informačných systémov*“. Pojem

[32] Na tieto účely sa distribuovali zoznamy medzinárodných noriem, osvedčených postupov a metodík posudzovania/riadenia rizík vo všetkých odvetviach pokrytých smernicou NIS, ktoré sa následne použili ako vstup pre navrhované bezpečnostné okruhy a opatrenia.

„bezpečnosť sietí a informačných systémov“ sa zas vymedzuje v článku 4 ods. 2 ako „*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*“. To znamená, že každá udalosť s nepriaznivým vplyvom nielen na dostupnosť, ale aj pravosť, integritu či dôvernosť údajov alebo súvisiacich služieb, by mohla byť spúšťačom oznamovacej povinnosti. Kontinuita služby v zmysle článku 14 ods. 3 môže byť skutočne ohrozená nielen v prípadoch, ktoré zasahujú fyzickú dostupnosť, ale aj pri akomkoľvek inom bezpečnostnom incidente, ktorý ovplyvňuje riadne poskytovanie danej služby[33].

Osobitnou oblasťou činnosti skupiny pre spoluprácu je v súčasnosti príprava nezáväzných usmernení pre oznamovanie, pokiaľ ide o okolnosti, za ktorých sú prevádzkovatelia základných služieb povinní oznamovať incidenty podľa článku 14 ods. 7, ako aj formát a postupy podávania takýchto oznámení. Tieto usmernenia majú byť dokončené do posledného štvrťroka 2017.

Odlišné vnútroštátne požiadavky na oznamovanie môžu viesť k právnej neistote, zložitejším a nepraktickejším postupom, ako aj výrazným administratívnym nákladom pre cezhraničných poskytovateľov. Komisia preto túto prácu skupiny pre spoluprácu víta. Rovnako, ako v otázke bezpečnostných požiadaviek, Komisia nabáda členské štáty, aby usmerňovaciemu dokumentu skupiny pre spoluprácu venovali riadnu pozornosť, aby boli vnútroštátne ustanovenia o oznamovaní incidentov v čo najväčšom súlade.

4.4. Smernica NIS, príloha III: Poskytovatelia digitálnych služieb

Druhou kategóriou subjektov zahrnutých do rozsahu pôsobnosti smernice NIS sú poskytovatelia digitálnych služieb (PDS). Za významných hospodárskych aktérov sa považujú, lebo ich mnohé podniky využívajú pri poskytovaní vlastných služieb a narušenie danej digitálnej služby by mohlo ovplyvniť kľúčové hospodárske a spoločenské aktivity.

4.4.1. Kategórie PDS

Článok 4 ods. 5, kde sa vymedzujú digitálne služby, sa odvoláva na právnu definíciu v článku 1 ods. 1 písm. b) smernice (EÚ) 2015/1535, pričom rozsah typov služieb obmedzuje na prílohu III. V článku 1 ods. 1 písm. b) smernice (EÚ) 2015/1535 sú tieto služby vymedzené ako „*každá služba, ktorá sa bežne poskytuje za odmenu, na diaľku, elektronickým spôsobom a na základe individuálnej žiadosti príjemcu služieb*“ a v prílohe III k smernici NIS sa uvádzajú tri konkrétne typy služieb: online trhovisko, internetový vyhľadávač a služby cloud computingu. Na rozdiel od prípadu prevádzkovateľov základných služieb tu smernica od členských štátov nevyžaduje identifikáciu poskytovateľov digitálnych služieb, ktorí by následne podliehali príslušným povinnostiam. Príslušné povinnosti vyplývajúce zo smernice – konkrétne bezpečnostné a oznamovacie požiadavky stanovené v článku 16 – sa teda budú vzťahovať na všetkých PDS v jej rozsahu pôsobnosti.

[33] To isté platí aj pre PDS.

V nasledujúcich oddieloch sa bližšie vysvetľujú tri typy digitálnych služieb, ktorých sa smernica týka.

1. Poskytovateľ služby online trhoviska

Online trhovisko umožňuje veľkému počtu rôznych podnikov zapájať sa do obchodných činností so spotrebiteľmi a inými podnikmi. Spoločnostiam poskytuje základnú infraštruktúru na obchodovanie online, a to aj cezhranične. Online trhoviská v hospodárstve zohrávajú významnú úlohu, najmä preto, že pre MSP sprístupňujú širší digitálny jednotný trh EÚ. Činnosti poskytovateľa služby online trhoviska môžu zahŕňať aj poskytovanie diaľkových výpočtových služieb na uľahčenie hospodárskej činnosti klienta vrátane spracovania transakcií a agregácie informácií o kupujúcich, dodávateľoch a produktoch alebo uľahčovanie vyhľadávania vhodných produktov, poskytovanie produktov, transakčnej expertízy a párovania kupujúcich s predávajúcimi.

Pojem online trhovisko sa vymedzuje v článku 4 ods. 17 a bližšie sa objasňuje v odôvodnení 15. Opisuje sa ako služba, ktorá umožňuje spotrebiteľom a obchodníkom uzatvárať s obchodníkmi online kúpne zmluvy alebo zmluvy o službách a je na uzatváranie takýchto zmlúv konečným miestom. Za online trhovisko možno považovať napríklad poskytovateľa ako *eBay*, ktorý umožňuje ostatným obchodovanie na jeho platforme s cieľom online sprístupnia výrobkov a služieb spotrebiteľom alebo firmám. Pod definíciu online trhoviska spadajú aj online obchody na distribúciu aplikácií a softvérových programov, keďže umožňujú vývojárom aplikácií predávať či distribuovať služby spotrebiteľom alebo iným podnikom. Naopak, sprostredkovatelia služieb tretích strán, ako napríklad *Skyscanner* či služby na porovnávanie cien, ktoré presmerúvajú používateľa na webové stránky obchodníka, kde sa napokon zmluva o poskytnutí služby alebo predaji výrobku uzavrie, do vymedzenia podľa článku 4 ods. 17 nespadajú.

2. Poskytovateľ služby internetového vyhľadávača

Internetový vyhľadávač sa vymedzuje v článku 4 ods. 18 a bližšie sa objasňuje v odôvodnení 16. Opisuje sa ako 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 zadaných parametrov. Nezahŕňa funkcie vyhľadávania v rámci jedného webového sídla ani stránky na porovnávanie cien. Napríklad druh vyhľadávača, ktorý je k dispozícii na stránke EUR LEX[34], nemožno považovať za vyhľadávač v zmysle smernice, keďže táto funkcia je obmedzená iba na obsah konkrétneho webového sídla.

3. Poskytovateľ služieb cloud computingu

V článku 4 ods. 19 sa služba cloud computingu vymedzuje ako „digitálna služba, ktorá umožňuje prístup ku škálovateľnému a pružnému súboru počítačových zdrojov, ktoré možno zdieľať“, pričom v odôvodnení 17 sa podrobnejšie vysvetľuje, čo sa myslí pod počítačovými zdrojmi, škálovateľnosťou či pružným súborom.

[34] K dispozícii na adrese: http://eur-lex.europa.eu/homepage.html.

V skratke možno cloud computing opísať ako konkrétny druh výpočtovej služby, ktorý využíva spoločné zdroje na spracovanie údajov na požiadanie, pričom spoločné zdroje zahŕňajú akékoľvek hardvérové či softvérové prvky (napr. siete, servery alebo inú infraštruktúru, úložný priestor, aplikácie a služby), ktoré sa na požiadanie poskytnú používateľom na spracovanie údajov. To, že ich možno zdieľať, znamená, že ide o výpočtové zdroje, pri ktorých mnoho používateľov využíva na spracovanie údajov tú istú fyzickú infraštruktúru. Počítačový zdroj možno považovať za zdieľateľný, ak sa súbor zdrojov, ktoré využíva poskytovateľ, dá kedykoľvek rozšíriť alebo zúžiť v závislosti od potrieb používateľov. Dátové strediská alebo jednotlivé komponenty v rámci dátového strediska sa tak dajú pripájať alebo odpájať, ak si celkové množstvo výpočtovej alebo úložnej kapacity vyžaduje aktualizáciu. Koncept pružného súboru možno opísať ako zmeny zaťaženia automatickým vyčleňovaním a rušením vyčleňovania zdrojov, takže dostupné zdroje v každom časovom okamihu v maximálnej možnej miere zodpovedajú aktuálnemu dopytu[35].

V súčasnosti môžu poskytovatelia ponúkať tri hlavné typy modelov cloudových služieb:

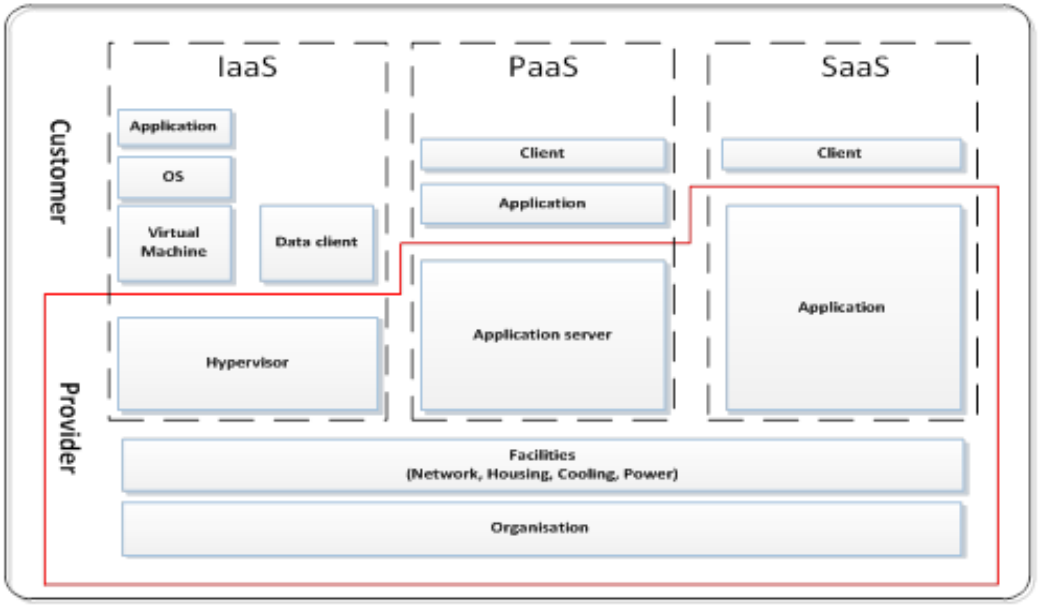
- Infraštruktúra ako služba (IaaS): Kategória cloudovej služby, pri ktorej má cloudová hodnota poskytovaná zákazníkovi podobu infraštruktúry. Zahŕňa virtuálne poskytovanie výpočtových zdrojov v podobe hardvéru, sieťových služieb a úložného priestoru. IaaS prevádzkuje servery, úložiská, siete a operačné systémy. Zabezpečuje podnikovú infraštruktúru, v ktorej si môže firma ukladať údaje a spúšťať aplikácie potrebné na jej každodenné fungovanie.

- Platforma ako služba (PaaS): Kategória cloudovej služby, pri ktorej má cloudová hodnota poskytovaná zákazníkovi podobu platformy. Zahŕňa online výpočtové platformy, ktoré firmám umožňujú spúšťať existujúce aplikácie alebo vyvíjať a testovať nové.

- Softvér ako služba (SaaS): Kategória cloudovej služby, pri ktorej má cloudová hodnota poskytovaná zákazníkovi podobu aplikácie alebo softvéru spúšťaného cez internet. Pri takomto type cloudových služieb si koncový používateľ nemusí kupovať, inštalovať a spravovať softvér, pričom ďalšou výhodou je, že softvér je k dispozícii odkiaľkoľvek, kde je internetové pripojenie.

[35] Nikolas Roman Herbst, Samuel Kounev, Ralf Reussner, Karlsruhe Institute of Technology, *Elasticity in Cloud Computing: What It Is, and What It Is Not* (Elasticita cloud computingu: čím je a čím nie), k dispozícii na adrese: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Pozri aj COM(2012) 529, s. 2 – 5.

Obrázok 5: Modely služieb a zdroje cloud computingu



Agentúra ENISA poskytla komplexné usmernenia ku konkrétnym témam v oblasti cloud computingu[36], ako aj príručku s úvodom do tejto problematiky[37].

4.4.2. Bezpečnostné požiadavky

Článok 16 ods. 1 od členských štátov vyžaduje zabezpečiť, aby PDS prijali vhodné a primerané technické a organizačné opatrenia na riadenie rizík súvisiacich s bezpečnosťou sietí a informačných systémov, ktoré tieto spoločnosti využívajú pri poskytovaní svojich služieb. Uvedené bezpečnostné opatrenia musia zohľadňovať najnovší technický vývoj a týchto päť prvkov: i) bezpečnosť systémov a zariadení; ii) riešenie incidentov; iii) riadenie kontinuity činnosti; iv) monitorovanie, audit a skúšanie; v) súlad s medzinárodnými normami.

V tejto súvislosti je Komisia článkom 16 ods. 8 splnomocnená prijímať vykonávacie akty s cieľom bližšie špecifikovať tieto prvky a zabezpečiť u týchto poskytovateľov služieb vysokú úroveň harmonizácie. Prijatie týchto vykonávacích aktov očakáva Komisia na jeseň 2017. Okrem toho sa od členských štátov vyžaduje zabezpečiť, aby poskytovatelia digitálnych služieb prijali potrebné opatrenia na zabránenie a minimalizovanie vplyvu incidentov s cieľom zabezpečiť kontinuitu týchto služieb.

4.4.3. Požiadavky na oznamovanie

PDS by mali mať povinnosť oznamovať závažné incidenty príslušným orgánom alebo jednotkám CSIRT. V zmysle článku 16 ods. 3 smernice NIS sa notifikačná povinnosť poskytovateľov digitálnych služieb aktivuje v prípadoch, keď má bezpečnostný incident závažný vplyv na poskytovanie danej služby. Na určenie závažnosti vplyvu uvádza článok 16 ods. 4 päť konkrétnych parametrov, ktoré musia poskytovatelia digitálnych služieb zohľadniť.

---

[36] K dispozícii na adrese: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security.

[37] ENISA, *Cloud Security Guide for SMEs* (Príručka k bezpečnosti cloudových služieb pre MSP, 2015). K dispozícii na adrese: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

V tejto súvislosti je Komisia článkom 16 ods. 8 splnomocnená prijímať vykonávacie akty, v ktorých sa tieto parametre opíšu podrobnejšie. Bližšia špecifikácia týchto parametrov bude súčasťou vykonávacieho aktu stanovujúceho bezpečnostné prvky spomínané v bode 4.4.2, ktorý Komisia plánuje prijať na jeseň.

4.4.4. Regulačný prístup založený na riadení rizík

Podľa článku 17 spadajú PDS pod dohľad vnútroštátnych príslušných orgánov formou kontrol *ex post*. Členské štáty musia zabezpečiť konanie príslušných orgánov, ak majú k dispozícii dôkazy, že PDS nespĺňa požiadavky stanovené v článku 16 smernice.

Okrem toho je Komisia v zmysle článku 16 ods. 8 a 9 splnomocnená prijímať vykonávacie akty k bezpečnostným a oznamovacím požiadavkám, ktoré u PDS posilnia úroveň harmonizácie. Navyše v článku 16 ods. 10 sa uvádza, že členské štáty nesmú ukladať PDS žiadne ďalšie bezpečnostné ani oznamovacie požiadavky nad rámec tých, ktoré sú uvedené v smernici, okrem prípadov, keď sú tieto opatrenia potrebné na zabezpečenie ich základných štátnych funkcií, najmä na zaistenie národnej bezpečnosti a umožnenie vyšetrovania, odhaľovania a stíhania trestných činov.

A napokon, vzhľadom na cezhraničnú povahu PDS smernica neuplatňuje model viacerých súbežných právomocí, ale prístup vychádzajúci z kritéria hlavnej prevádzkarne danej spoločnosti v EÚ[38]. Tento prístup umožňuje, aby sa vo vzťahu k PDS uplatnil jeden súbor pravidiel s jedným príslušným orgánom zodpovedným za dohľad, čo je mimoriadne dôležité, keďže mnohí PDS ponúkajú svoje služby v mnohých členských štátoch súčasne. Uplatnenie tohto prístupu minimalizuje zaťaženie PDS pri plnení povinností a zabezpečuje riadne fungovanie digitálneho jednotného trhu.

4.4.5. Právomoc

Ako už bolo uvedené, v zmysle článku 18 ods. 1 smernice NIS podlieha každý PDS právomoci členského štátu, v ktorom má hlavnú prevádzkareň. Ak daný PDS ponúka v EÚ služby, no nie je na jej území usadený, článok 18 ods. 2 mu ukladá povinnosť určiť svojho zástupcu v Únii. V takom prípade podlieha spoločnosť právomoci členského štátu, kde je usadený zástupca. Ak PDS poskytuje v určitom členskom štáte služby, ale nemá v EÚ určeného zástupcu, daný členský štát môže v zásade voči takémuto PDS zakročiť, keďže takýto poskytovateľ porušuje povinnosti, ktoré mu vyplývajú zo smernice.

4.4.6. Oslobodenie drobných poskytovateľov digitálnych služieb od bezpečnostných a oznamovacích požiadaviek

V článku 16 ods. 11 sa uvádza, že poskytovatelia digitálnych služieb, ktorí sú mikropodnikmi alebo malými podnikmi v zmysle odporúčania Komisie 2003/361/ES39 sú vyňatí z uplatňovania bezpečnostných požiadaviek a oznamovania podľa článku 16. To znamená, že dané požiadavky sa nevzťahujú na podniky s menej než 50 zamestnancami a ročným obratom a/alebo celkovou ročnou bilančnou sumou najviac 10 miliónov eur. Pri určovaní veľkosti

[38] Pozri najmä článok 18 smernice.
[39] Ú. v. EÚ L 24, 20.5.2003, s. 36.

subjektu nehrá rolu, či daná spoločnosť poskytuje iba digitálne služby v zmysle smernice NIS alebo aj iné služby.

5. Vzťah medzi smernicou NIS a inými právnymi predpismi

Tento oddiel sa zameriava na ustanovenia smernice NIS o *lex specialis* v článku 1 ods. 7, uvádza tri príklady *lex specialis*, ktoré Komisia doposiaľ posudzovala, a vysvetľuje bezpečnostné a oznamovacie požiadavky platné pre odvetvie telekomunikácií a poskytovateľov dôveryhodných služieb.

5.1. Smernica NIS, článok 1 ods. 7: ustanovenia o *lex specialis*

Podľa článku 1 ods. 7 smernice NIS sa ustanovenia smernice o bezpečnostných a/alebo oznamovacích povinnostiach poskytovateľov digitálnych služieb alebo prevádzkovateľov základných služieb neuplatňujú, ak existuje legislatíva EÚ v konkrétnom odvetví, ktorá zahŕňa bezpečnostné a/alebo oznamovacie požiadavky, ktoré sú účinkom aspoň rovnocenné s príslušnými požiadavkami smernice NIS. Členské štáty musia článok 1 ods. 7 pri celkovej transpozícii smernice zohľadniť a informovať Komisiu o uplatnení ustanovení o *lex specialis*.

Metodika

Pri posudzovaní rovnocennosti sektorovej legislatívy EÚ s príslušnými ustanoveniami smernice NIS sa treba osobitne zamerať na otázku, či bezpečnostné povinnosti v danej sektorovej legislatíve zahŕňajú opatrenia, ktoré zaistia bezpečnosť sietí a informačných systémov vymedzených v článku 4 ods. 2 smernice.

Pokiaľ ide o požiadavky na oznamovanie, v článku 14 ods. 3 a článku 16 ods. 3 smernice NIS sa uvádza, že prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb musia príslušným orgánom alebo jednotkám CSIRT bezodkladne oznámiť každý incident so závažným vplyvom na poskytovanie danej služby. Tu treba venovať osobitnú pozornosť povinnostiam prevádzkovateľa/poskytovateľa digitálnych služieb zahrnúť do oznámenia informácie, ktoré príslušnému orgánu alebo jednotke CSIRT umožnia určiť prípadný cezhraničný vplyv bezpečnostného incidentu.

V súčasnosti neexistujú pre kategóriu poskytovateľov digitálnych služieb odvetvové právne predpisy, ktoré by upravovali bezpečnostné a oznamovacie požiadavky porovnateľne s článkom 16 smernice NIS a ktoré by sa dali zohľadniť pri uplatňovaní jej článku 1 ods. 7[40].

Pokiaľ ide o prevádzkovateľov základných služieb, bezpečnostné a/alebo oznamovacie požiadavky vyplývajúce z odvetvovej legislatívy EÚ momentálne platia vo finančnom sektore, a najmä v odvetviach bankovníctva a infraštruktúr finančných trhov, ktoré sa spomínajú v bodoch 3 a 4 prílohy II. Dôvodom je, že bezpečnosť a dobrý stav informačných

[40] Čo sa nevzťahuje na oznamovanie porušení ochrany osobných údajov dozornému orgánu podľa článku 33 všeobecného nariadenia o ochrane údajov.

technológií, sietí a informačných systémov finančných inštitúcií je nevyhnutnou súčasťou požiadaviek na riadenie operačných rizík, ktoré finančným inštitúciám ukladá legislatíva EÚ.

Príklady

i) Revidovaná smernica o platobných službách

V sektore bankovníctva, a najmä v súvislosti s poskytovaním platobných služieb úverovými inštitúciami vymedzenými v článku 4 ods. 1 nariadenia (EÚ) 575/2013 sa bezpečnostné a oznamovacie požiadavky stanovujú v článkoch 95 a 96 revidovanej smernice o platobných službách (tzv. PSD2)[41].

Konkrétne jej článok 95 ods. 1 vyžaduje, aby poskytovatelia platobných služieb prijali vhodné zmierňujúce opatrenia a kontrolné mechanizmy s cieľom riadiť prevádzkové a bezpečnostné riziká súvisiace s platobnými službami, ktoré poskytujú. Tieto opatrenia by mali zahŕňať zavedenie a zachovávanie účinných postupov riadenia incidentov vrátane postupov na zisťovanie a klasifikáciu závažných prevádzkových a bezpečnostných incidentov. V odôvodneniach 95 a 96 smernice PSD2 sa povaha týchto bezpečnostných opatrení objasňuje bližšie. Z týchto ustanovení je zrejmé, že cieľom predpísaných opatrení je riadenie bezpečnostných rizík spojených so sieťami a informačnými systémami, ktoré sa používajú pri poskytovaní platobných služieb. Tieto bezpečnostné požiadavky teda možno z hľadiska účinku považovať aspoň za rovnocenné zodpovedajúcim ustanoveniam článku 14 ods. 1 a 2 smernice NIS.

Pokiaľ ide o oznamovacie požiadavky, v článku 96 ods. 1 smernice PSD2 sa uvádza povinnosť poskytovateľov platobných služieb bez zbytočného odkladu informovať príslušný orgán o závažných bezpečnostných incidentoch. Okrem toho porovnateľne s článkom 14 ods. 5 smernice NIS vyžaduje článok 96 ods. 2 smernice PSD2, aby príslušný orgán informoval príslušné orgány iných členských štátov, ak je pre ne incident relevantný. Zároveň táto povinnosť znamená, že oznámenia o bezpečnostných incidentoch musia zahŕňať informácie, ktoré daným orgánom umožnia určiť cezhraničný vplyv incidentu. V článku 96 ods. 3 písm. a) smernice PSD2 sa orgánu EBA v spolupráci s ECB v tejto súvislosti ukladá úloha vypracovať usmernenia o presnom obsahu a formáte takýchto oznámení.

Možno preto konštatovať, že podľa článku 1 ods. 7 smernice NIS by sa mali v oblasti poskytovania platobných služieb úverovými inštitúciami miesto zodpovedajúcich ustanovení článku 14 smernice NIS uplatniť tak bezpečnostné, ako aj oznamovacie požiadavky stanovené v článkoch 95 a 96 smernice PSD2.

ii) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov

[41] Smernica (EÚ) 2015/2366, Ú. v. EÚ L 337, 23.12.2015, s. 35.

V oblasti infraštruktúry finančného trhu obsahuje nariadenie (EÚ) 648/2012 v spojení s delegovaným nariadením Komisie (EÚ) 153/2013 ustanovenia o bezpečnostných požiadavkách na centrálne protistrany, ktoré možno považovať za *lex specialis*. Tieto právne akty stanovujú technické a organizačné opatrenia súvisiace s bezpečnosťou sietí a informačných systémov, ktoré mierou podrobnosti dokonca presahujú požiadavky článku 14 ods. 1 a 2 smernice NIS, takže ich možno považovať za vyhovujúce článku 1 ods. 7 smernice NIS z hľadiska bezpečnostných požiadaviek.

Konkrétnejšie sa v článku 26 ods. 1 nariadenia (EÚ) 648/2012 uvádza, že dané subjekty musia mať *„spoľahlivý systém správy, ktorý zahŕňa jasnú organizačnú štruktúru s presne definovanými, transparentnými a konzistentnými líniami zodpovednosti, účinné postupy zisťovania, riadenia, monitorovania a ohlasovania rizík, ktorým je alebo môže byť vystavená, a primerané mechanizmy vnútornej kontroly vrátane spoľahlivých administratívnych a účtovných postupov.“* V článku 26 ods. 3 sa vyžaduje, aby organizačná štruktúra zaisťovala kontinuitu a riadne fungovanie služieb a činností s využitím vhodných a primeraných systémov, zdrojov a postupov.

Navyše sa v článku 26 ods. 6 objasňuje, že centrálna protistrana musí udržiavať „*primerané systémy informačných technológií na zvládnutie zložitosti, rôznorodosti a druhu vykonávaných služieb a činností v záujme zaistenia vysokých noriem bezpečnosti, integrity a dôvernosti uchovávaných informácií*“. Ďalej sa v článku 34 ods. 1 predpisuje zavedenie, vykonávanie a udržiavanie primeranej politiky zabezpečovania kontinuity činnosti a plánu obnovy po havárii, ktorý by mal zaistiť včasnú obnovu činnosti.

Tieto povinnosti sa bližšie špecifikujú v delegovanom nariadení Komisie (EÚ) č. 153/2013 z 19. decembra 2012, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012, pokiaľ ide o regulačné technické normy týkajúce sa požiadaviek na centrálne protistrany[42]. Konkrétne jeho článok 4 ukladá centrálnym protistranám povinnosť vypracovať primerané nástroje na riadenie rizík, ktoré jej umožnia riadiť a ohlasovať všetky príslušné riziká, a bližšie špecifikuje druh daných opatrení (napr. zavedenie spoľahlivých informačných systémov a systémov na kontrolu rizík, dostupnosť potrebných zdrojov, odborných znalostí a prístupu k všetkým informáciám relevantným pre riadenie rizík, primerané mechanizmy vnútornej kontroly ako spoľahlivé administratívne a účtovné postupy na pomoc rade centrálnej protistrany pri monitorovaní a posudzovaní primeranosti a účinnosti jej politík, postupov a systémov riadenia rizík).

Okrem toho sa jeho článok 9 výslovne zameriava na bezpečnosť systémov informačných technológií a stanovuje konkrétne technické a organizačné opatrenia súvisiace s udržiavaním odolného rámca bezpečnosti informácií na riadenie rizika v oblasti bezpečnosti IT. Tieto opatrenia by mali zahŕňať mechanizmy a postupy na zaručenie dostupnosti služieb, ochranu autentickosti, integrity a dôvernosti údajov.

[42] Ú. v. EÚ L 52, 23.2.2013, s. 41.

iii) 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[43]

Pokiaľ ide o obchodné miesta, článok 48 ods. 1 smernice 2014/65/EÚ vyžaduje, aby prevádzkovatelia zabezpečili kontinuitu svojich služieb v prípade akéhokoľvek zlyhania ich systémov obchodovania. Túto všeobecnú povinnosť nedávno bližšie vymedzilo a doplnilo delegované nariadenie Komisie (EÚ) 2017/584[44] zo 14. júla 2016, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/65/EÚ, pokiaľ ide o regulačné technické predpisy bližšie určujúce organizačné požiadavky na obchodné miesta[45]. Konkrétne sa v článku 23 ods. 1 daného nariadenia stanovuje, že obchodné miesta musia mať zavedené postupy a opatrenia týkajúce sa fyzického a elektronického zabezpečenia zamerané na ochranu svojich systémov pred zneužitím alebo neoprávneným prístupom a na zabezpečenie integrity údajov. Tieto opatrenia by mali umožňovať zabránenie alebo minimalizáciu rizík útokov na informačné systémy.

V článku 23 ods. 2 sa ďalej vyžaduje, aby opatrenia prijaté prevádzkovateľmi umožňovali rýchlu identifikáciu a riadenie rizika spojeného s neoprávneným prístupom, narušeniami systému, ktoré závažne komplikujú alebo prerušujú fungovanie informačného systému, a s narušovaním údajov, ktoré zhoršuje dostupnosť, integritu alebo pravosť údajov. Okrem toho článok 15 daného nariadenia ukladá obchodným miestam povinnosť zaviesť účinné opatrenia na zabezpečenie kontinuity činnosti na riešenie rušivých situácií, aby mali ich systémy dostatočnú stabilitu. Tieto opatrenia by najmä mali umožniť prevádzkovateľovi obnoviť obchodovanie do dvoch alebo približne dvoch hodín, a zároveň zabezpečiť takmer nulovú stratu údajov.

V článku 16 sa ďalej uvádza, že identifikované opatrenia na riešenie a riadenie rušivých situácií by mali byť zahrnuté v pláne na zabezpečenie kontinuity činnosti obchodných miest, a poskytuje konkrétne prvky, ktoré má prevádzkovateľ pri prijímaní tohto plánu zvážiť (napr. zriadenie osobitného tímu bezpečnostných operácií alebo posúdenie vplyvu, v ktorom sa určia riziká a ktoré sa pravidelne preskúmava).

Z obsahu týchto bezpečnostných opatrení vyplýva, že sú určené na riadenie a zohľadnenie rizík spojených s dostupnosťou, pravosťou, integritou a dôvernosťou údajov a poskytovaných služieb, takže možno konštatovať, že uvedená odvetvová legislatíva EÚ zahŕňa bezpečnostné povinnosti, ktoré sú účinkom aspoň rovnocenné príslušným povinnostiam uvedeným v článku 14 ods. 1 a 2 smernice NIS.

5.2. Smernica NIS, článok 1 ods. 3: poskytovatelia telekomunikačných a dôveryhodných služieb

Podľa článku 1 ods. 3 sa bezpečnostné a oznamovacie požiadavky smernice nevzťahujú na poskytovateľov, ktorí podliehajú požiadavkám článkov 13a a 13b smernice

[43] Ú. v. EÚ L 173, 12.6.2014, s. 349.
[44] Ú. v. EÚ L 87, 31.3.2017, s. 350.
[45] http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160714-rts-7_en.pdf.

2002/21/ES. Články 13a a 13b smernice 2002/21/ES sa vzťahujú na podniky, ktoré poskytujú verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby. Znamená to, že z hľadiska poskytovania verejných komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb musí daná spoločnosť spĺňať bezpečnostné a oznamovacie požiadavky stanovené v smernici 2002/21/ES.

Ak však daná spoločnosť poskytuje aj iné služby – napríklad digitálne (povedzme cloud computing alebo online trhovisko) uvedené v prílohe III k smernici NIS – alebo služby, ako napríklad prevádzka DNS alebo IXP podľa bodu 7 prílohy II k smernici NIS, podlieha táto spoločnosť z hľadiska poskytovania týchto konkrétnych služieb bezpečnostným a oznamovacím požiadavkám smernice NIS. Treba poznamenať, že poskytovatelia služieb uvedení v bode 7 prílohy II spadajú do kategórie prevádzkovateľov základných služieb, a preto členské štáty musia uskutočniť identifikačný proces podľa článku 5 ods. 2 a identifikovať, ktorí jednotliví poskytovatelia služieb DNS, IXP alebo TLD majú spĺňať požiadavky smernice NIS. Znamená to, že po tomto posúdení budú musieť spĺňať požiadavky smernice NIS iba tí poskytovatelia služieb DNS, IXP alebo TLD, ktorí spĺňajú kritériá článku 5 ods. 2 smernice NIS.

V článku 1 ods. 3 sa ďalej uvádza, že bezpečnostné a oznamovacie požiadavky smernice sa nevzťahujú ani na poskytovateľov dôveryhodných služieb, na ktorých sa vzťahujú podobné požiadavky podľa článku 19 nariadenia (EÚ) č. 910/2014.

6. Uverejnené dokumenty o národných stratégiách kybernetickej bezpečnosti

	Členský štát	Názov stratégie a dostupné odkazy
1	Rakúsko	*Rakúska stratégia kybernetickej bezpečnosti* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgicko	*Zabezpečenie kybernetického priestoru* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulharsko	*Kyberneticky odolné Bulharsko do roku 2020* (2016) http://www.cyberbg.eu/ (BG)
4	Chorvátsko	*Národná stratégia kybernetickej bezpečnosti Chorvátskej republiky* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Česká republika	*Národná stratégia kybernetickej bezpečnosti Českej republiky na roky 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Cyprus	*Stratégia kybernetickej bezpečnosti Cyperskej republiky* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Dánsko	*Dánska stratégia kybernetickej a informačnej bezpečnosti* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estónsko	*Stratégia kybernetickej bezpečnosti* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Fínsko	*Fínska stratégia kybernetickej bezpečnosti* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Francúzsko	*Francúzska národná stratégia digitálnej bezpečnosti* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)

11	Írsko	*Národná stratégia kybernetickej bezpečnosti na roky 2015 – 2017* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Taliansko	*Národný strategický rámec bezpečnosti kybernetického priestoru* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Nemecko	*Stratégia kybernetickej bezpečnosti pre Nemecko* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Maďarsko	*Národná stratégia kybernetickej bezpečnosti Maďarska* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Lotyšsko	*Stratégia kybernetickej bezpečnosti Lotyšska na roky 2014 – 2018* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Litva	*Program vývoja bezpečnosti elektronických informačných systémov (kybernetická bezpečnosť) na roky 2011 – 2019* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Luxembursko	*Národná stratégia kybernetickej bezpečnosti II (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*Národná stratégia kybernetickej bezpečnosti – zelená kniha* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Holandsko	*Národná stratégia kybernetickej bezpečnosti 2* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Poľsko	*Politika Poľskej republiky na ochranu kybernetického priestoru* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Rumunsko	*Stratégia kybernetickej bezpečnosti Rumunska* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf

		(RO)
22	Portugalsko	*Národná stratégia bezpečnosti kybernetického priestoru* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Slovensko	*Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/cyber-security-concept-of-the-slovak-republic-1 (EN)
24	Slovinsko	*Stratégia kybernetickej bezpečnosti, ktorou sa zriaďuje systém na zaistenie vysokej úrovne kybernetickej bezpečnosti* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Španielsko	*Národná stratégia kybernetickej bezpečnosti* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Švédsko	*Švédska národná stratégia kybernetickej bezpečnosti* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Spojené kráľovstvo	*Národná stratégia kybernetickej bezpečnosti (2016 – 2021)* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Zoznam osvedčených postupov a odporúčaní vydaných agentúrou ENISA

Reakcia na incidenty

- ✓ Stratégie reakcie na incidenty a spolupráca v prípade kybernetickej krízy[46]

Riešenie incidentov

- ✓ Projekt automatizácie riešenia incidentov[47]
- ✓ Príručka osvedčených postupov riadenia incidentov[48]

Klasifikácia a taxonómia incidentov

- ✓ Prehľad existujúcich taxonómií[49]
- ✓ Príručka osvedčených postupov používania taxonómií v oblasti prevencie a odhaľovania incidentov[50]

Vývoj jednotiek CSIRT

- ✓ Výzvy európskych vnútroštátnych jednotiek CSIRT v roku 2016: Štúdia stupňa vývoja jednotiek CSIRT[51]
- ✓ Štúdia stupňa vývoja jednotiek CSIRT – proces hodnotenia[52]
- ✓ Usmernenia pre vnútroštátne a vládne jednotky CSIRT pri hodnotení stupňa vývoja[53]

Budovanie kapacít a odborná príprava jednotiek CSIRT

- ✓ Príručka osvedčených postupov v metodikách školenia[54]

Kde nájsť informácie o existujúcich jednotkách CSIRT v Európe – prehľad jednotiek CSIRT podľa krajín[55]

---

46 ENISA, *Strategies for incident response and cyber crisis cooperation* (2016). K dispozícii na adrese:https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation.

47 Viac informácií na adrese: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation.

48 ENISA, *Good Practice Guide for Incident Management* (2010). K dispozícii na adrese:https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.

49 Viac informácií na adrese: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies.

50 ENISA, *A good practice guide of using taxonomies in incident prevention and detection* (2017). K dispozícii na adrese: https://www.enisa.europa.eu/publications/using-taxonomies-in-incident-prevention-detection.

51 ENISA, *Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity* (2017). K dispozícii na adrese:https://www.enisa.europa.eu/publications/study-on-csirt-maturity.

52 ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). K dispozícii na adrese:https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process.

53 ENISA, CSIRT Capabilities. *How to assess maturity? Guidelines for national and governmental CSIRTs* (2016). K dispozícii na adrese: https://www.enisa.europa.eu/publications/csirt-capabilities.

54 ENISA, *Good Practice Guide on Training Methodologies* (2014). K dispozícii na adrese:https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies.

55 Viac informácií na adrese: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.