EVROPSKÁ
KOMISE

V Bruselu dne 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

PŘÍLOHA

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU A RADĚ

Maximální využití směrnice o bezpečnosti sítí a informací – účinné provedení směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

OBSAH

PŘÍLOHA

1. Úvod

Cílem této přílohy je přispět k účinnému uplatňování, provádění a prosazování směrnice (EU) 2016/1148 o bezpečnosti sítí a informačních systémů v Unii[1] (dále jen „směrnice o bezpečnosti sítí a informací“ nebo „směrnice“) a pomoci členským státům zajistit účinné uplatňování práva EU. Konkrétněji má tato příloha tři specifické cíle: a) lépe vnitrostátním orgánům objasnit povinnosti obsažené v uvedené směrnici, které se na ně vztahují, b) zajistit účinné vymáhání povinností, které směrnice ukládá subjektům v oblasti bezpečnostních požadavků a hlášení incidentů, a c) celkově přispět k vytvoření právní jistoty pro všechny příslušné subjekty.

Za tímto účelem příloha obsahuje pokyny k níže uvedeným prvkům, jež jsou klíčové pro dosažení cíle směrnice o bezpečnosti sítí a informací, tj. zajistit v celé EU vysokou společnou úroveň bezpečnosti sítí a informačních systémů, na nichž je postaveno fungování naší společnosti a hospodářství:

- povinnost členských států přijmout národní strategii pro bezpečnost sítí a informačních systémů (bod 2),
- zřízení vnitrostátních příslušných orgánů, jednotných kontaktních míst a skupin pro reakce na počítačové bezpečnostní incidenty (týmů CSIRT) (bod 3),
- bezpečnostní požadavky a požadavky na hlášení incidentů pro provozovatele základních služeb a pro poskytovatele digitálních služeb (bod 4) a
- vztah mezi směrnicí o bezpečnosti sítí a informací a jinými právními předpisy (bod 5).

Při přípravě uvedených pokynů Komise využila informace a analýzy získané během přípravy směrnice, vstupy od Evropské agentury pro bezpečnost sítí a informací (ENISA) a od skupiny pro spolupráci. Zároveň čerpala ze zkušeností členských států. V případě potřeby vzala Komise v potaz hlavní zásady výkladu práva EU: znění, souvislosti a cíle směrnice o bezpečnosti sítí a informací. Vzhledem k tomu, že směrnice ještě nebyla provedena, neexistují dosud žádná rozhodnutí Soudního dvora Evropské unie nebo vnitrostátních soudů. Judikaturu tedy jako vodítko použít nelze.

Shrnutí těchto informací v jediném dokumentu může členským státům dát dobrý přehled o směrnici, který budou moci využít při přípravě svých vnitrostátních právních předpisů. Komise spolu s tím ale zdůrazňuje, že tato příloha není právně závazná a nemá za cíl stanovit nová pravidla. Konečná pravomoc vykládat právo EU přísluší Soudnímu dvoru Evropské unie.

[1] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Směrnice vstoupila v platnost dne 8. srpna 2016.

2. Národní strategie pro bezpečnost sítí a informačních systémů

Podle článku 7 směrnice o bezpečnosti sítí a informací mají členské státy přijmout národní strategii pro bezpečnost sítí a informačních systémů, kterou lze považovat za rovnocennou pojmu „národní strategie kybernetické bezpečnosti“ (NCSS). Smyslem národní strategie je vymezit strategické cíle a vhodná politická a regulační opatření v oblasti kybernetické bezpečnosti. Koncepce národní strategie kybernetické bezpečnosti je zhusta využívána na mezinárodní úrovni i v Evropě, zejména v kontextu spolupráce agentury ENISA s členskými státy na národních strategiích, ze které nedávno vzešla aktualizovaná příručka osvědčených postupů v oblasti národních strategií kybernetické bezpečnosti[2].

V tomto bodě Komise objasňuje, jak směrnice o bezpečnosti sítí a informací zlepšuje připravenost členských států, když po nich požaduje, aby přijaly robustní národní strategie pro bezpečnost sítí a informačních systémů (článek 7). Tento bod je věnován těmto aspektům: a) oblasti působnosti strategie a b) jejímu obsahu a postupu přijetí.

Jak je podrobněji popsáno níže, správné provedení článku 7 směrnice o bezpečnosti sítí a informací je zásadní pro dosažení jejích cílů a vyžaduje, aby byly pro tento účel přiděleny adekvátní finanční i lidské zdroje.

2.1 Oblast působnosti národní strategie

Podle znění článku 7 se povinnost přijmout národní strategii kybernetické bezpečnosti vztahuje pouze na odvětví uvedená v příloze II (energetika, doprava, bankovnictví, finanční trhy, zdravotnictví, dodávky a distribuce pitné vody a digitální infrastruktura) a na služby uvedené v příloze III (on-line tržiště, internetový vyhledávač a služba cloud computingu).

V článku 3 pak směrnice konkrétně uvádí zásadu minimální harmonizace, podle níž mohou členské státy přijímat nebo ponechat v platnosti ustanovení, jejichž cílem je dosáhnout vyšší úrovně bezpečnosti sítí a informačních systémů. Uplatnění této zásady na povinnost přijmout národní strategii kybernetické bezpečnosti umožňuje členským státům do této strategie zahrnout i jiná odvětví a služby než ty, které jsou uvedeny v přílohách II a III směrnice.

Podle názoru Komise a s ohledem na cíl směrnice o bezpečnosti sítí a informačních systémů, jímž je vysoká společná úroveň bezpečnosti sítí a informačních systémů v Unii[3], by bylo vhodné vypracovat národní strategii, která zahrnuje všechny relevantní rozměry společnosti a hospodářství, a ne jen odvětví a digitální služby, na něž se vztahuje příloha II a III směrnice. To je v souladu s osvědčenou mezinárodní praxí (viz pokyn ITU a analýza OECD uvedené níže) i se směrnicí o bezpečnosti sítí a informací.

Jak je vysvětleno níže, je to zejména případ orgánů veřejné správy odpovědných za jiná odvětví a služby než ty, které jsou uvedeny v přílohách II a III směrnice. Veřejné orgány

[2] ENISA, *National Cyber-Security Strategy Good Practice* (Osvědčené postupy v oblasti národních strategií kybernetické bezpečnosti, 2016). K dispozici na adrese: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[3] Viz čl. 1 odst. 1.

mohou zpracovávat citlivé informace, což ospravedlňuje potřebu zahrnout je do národní strategie kybernetické bezpečnosti a plánů řízení, aby nedocházelo k únikům informací a aby byla zajištěna jejich přiměřená ochrana.

2.2 Obsah a postup přijímání národních strategií

Podle článku 7 směrnice o bezpečnosti sítí a informací musí národní strategie kybernetické bezpečnosti zahrnovat alespoň tyto prvky:

i) cíle a priority národní strategie pro bezpečnost sítí a informačních systémů;
ii) správní rámec pro naplnění cílů a priorit vnitrostátní strategie;
iii) stanovení opatření týkajících se připravenosti, reakce a obnovy, včetně spolupráce veřejného a soukromého sektoru;
iv) vymezení příslušných vzdělávacích, informačních a školicích programů;
v) vymezení výzkumných a rozvojových plánů;
vi) plán posouzení rizik pro určení rizik a
vii) seznam subjektů zapojených do provádění strategie.

Ani článek 7, ani příslušný 29. bod odůvodnění nestanoví kritéria pro přijetí národní strategie kybernetické bezpečnosti ani blíže neurčuje její obsah. Z hlediska procesu a dalších prvků souvisejících s obsahem národní strategie považuje Komise níže uvedený přístup za jednu z vhodných metod přijímání národní strategie kybernetické bezpečnosti. Vychází z analýzy zkušeností členských států a třetích zemí při tvorbě jejich vlastních strategií. Dalším zdrojem informací je školicí nástroj k národním strategiím kybernetické bezpečnosti připravený agenturou ENISA ve formě videoklipů a jiných médií, které jsou ke stažení na stránkách agentury[4].

2.3 Proces a otázky k řešení

Proces přípravy a následné přijetí národní strategie je komplexní, obsahuje mnoho aspektů, a má-li být účinný a úspěšný, musí do něj být trvale zapojeni odborníci na kybernetickou bezpečnost a zástupci občanské společnosti a musí být začleněn i do vnitrostátního politického procesu. Nezbytností je podpora ze strany vysokých úředníků veřejné správy – alespoň na úrovni státního tajemníka příslušného ministerstva nebo na rovnocenné úrovni –, ale také politická podpora. Pro úspěšné přijetí národní strategie kybernetické bezpečnosti lze zvážit tento postup v pěti krocích (viz obr. 1):

První krok – **Stanovení hlavních zásad a strategických cílů strategie**

Nejprve by příslušné vnitrostátní orgány měly definovat některé klíčové prvky strategie, a to jaké jsou kýžené výsledky („*cíle a priority*“ v čl. 7 odst. 1 písm. a) směrnice), jak tyto výsledky doplňují vnitrostátní sociální a hospodářskou politiku a zda jsou kompatibilní s pravomocemi a povinnostmi vyplývajícími z členství v Evropské unii. Cíle by měly být konkrétní, měřitelné, dosažitelné, realistické a časově vymezené (SMART). Jeden ilustrativní příklad: „*Zajistíme, aby tato [časově vymezená] strategie byla založena na přesně daném a*

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

komplexním souboru měřitelných údajů, na nichž budeme měřit pokrok směrem k výsledkům, kterých musíme dosáhnout.“[5]

Výše uvedené také zahrnuje politické posouzení toho, zda je na financování realizace strategie možné zajistit významný rozpočet. Současně je nutný i popis zamýšlené oblasti působnosti strategie a jednotlivých kategorií zainteresovaných stran z veřejného i soukromého sektoru, které by měly být zapojeny do přípravy jednotlivých cílů a opatření.

Tento první krok lze splnit prostřednictvím cílených seminářů s vysokými úředníky ministerstev a politiky, které budou moderovat odborníci na kybernetickou bezpečnost s profesionálními komunikačními dovednostmi, kteří dokáží zdůraznit důsledky nulové nebo slabé kybernetické bezpečnosti pro moderní digitální ekonomiku a společnost.

Druhý krok – **Vypracování obsahu strategie**

Strategie by měla obsahovat podpůrná opatření, načasované kroky a klíčové ukazatele výkonnosti pro výsledné hodnocení, dolaďování a zdokonalování po stanoveném prováděcím období. Tato opatření by měla podporovat cíl, priority a výsledky, které byly stanoveny jako hlavní zásady. O potřebě zahrnout podpůrná opatření hovoří čl. 7 odst. 1 písm. c) směrnice o bezpečnosti sítí a informací.

Doporučuje se vytvoření řídící skupiny, které bude předsedat věcně příslušné ministerstvo a která bude řídit přípravný proces a usnadňovat sběr vstupů. V praxi toho lze dosáhnout zřízením řady přípravných skupin příslušných úředníků a odborníků zaměřených na klíčová všeobecná témata – například vyhodnocování rizika, krizové plánování, řešení incidentů, rozvoj dovedností, zvyšování povědomí, výzkumný a průmyslový rozvoj atd. Samostatně by pak každé odvětví (např. energetika, doprava atd.) bylo vyzváno, aby vyhodnotilo dopady svého zapojení, včetně přidělení potřebných zdrojů, a zainteresovalo určené provozovatele základních služeb a poskytovatele klíčových digitálních služeb do stanovování priorit a předkládání návrhů v rámci přípravného procesu. Zapojení odvětvových zainteresovaných stran je nezbytné i s ohledem na potřebu zajistit harmonizované provedení směrnice napříč odvětvími a zároveň zohlednit odvětvová specifika.

Třetí krok – **Budování správního rámce**

Aby byl správní rámec účelný a účinný, měl by být založen na klíčových zainteresovaných stranách, prioritách zjištěných během přípravného procesu a na omezeních a kontextu vnitrostátních správních a politických struktur. Bylo by žádoucí zajistit přímé podávání zpráv na politickou úroveň s tím, že rámec by měl mít rozhodovací pravomoc i pravomoc přidělovat zdroje a měl by mít vstupy od odborníků na kybernetickou bezpečnost i zainteresovaných stran z průmyslových odvětví. Na správní rámec odkazuje čl. 7 odst. 1 písm. b) směrnice o bezpečnosti sítí a informací, který výslovně vyžaduje „*povinnosti vládních orgánů a dalších relevantních subjektů*“.

[5] Výňatek z národní strategie kybernetické bezpečnosti Spojeného království na období 2016–2021, str. 67.

Čtvrtý krok – **Sestavení a revize návrhu strategie**

V této fázi by měl být sestaven a revidován návrh strategie, a to analýzou silných a slabých stránek, příležitostí a hrozeb (tzv. SWOT analýza), díky které bude možné zjistit, zda je nutné revidovat obsah. Po interní revizi by měla následovat konzultace se zúčastněnými stranami. Zároveň bude nutné uspořádat veřejnou konzultaci za účelem přiblížení významu navrhované strategie veřejnosti, získání vstupů ze všech možných zdrojů a zajištění podpory při získávání zdrojů potřebných k provádění strategie.

Pátý krok – **Formální přijetí**

Posledním krokem je formální přijetí na politické úrovni spolu s dostatečným rozpočtem, který odráží skutečnost, že členský stát bere kybernetickou bezpečnost vážně. Pro dosažení cílů směrnice o bezpečnosti sítí a informací Komise členské státy vyzývá, aby při oznamování národní strategie Komisi podle čl. 7 odst. 3 uvedly rovněž informace o rozpočtu. Závazky související s rozpočtem a potřebnými lidskými zdroji jsou naprosto zásadní pro účinné provádění strategie i směrnice. Vzhledem k tomu, že kybernetická bezpečnost je stále poměrně novou a rychle se rozvíjející oblastí veřejné politiky, jsou ve většině případů potřebné nové investice, přestože celková situace veřejných financí si žádá spíše škrty a úspory.

Poradenství k procesu přípravy a k obsahu národních strategií mohou nabídnout různé veřejné i akademické zdroje, např. agentura ENISA[6], Mezinárodní telekomunikační unie (ITU)[7], Organizace pro hospodářskou spolupráci a rozvoj (OECD)[8], Globální fórum kybernetických znalostí (GFCE) či Oxfordská univerzita[9].

[6] ENISA, *National Cyber-Security Strategy Good Practice* (Osvědčené postupy v oblasti národních strategií kybernetické bezpečnosti, 2016). K dispozici na adrese: https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[7] ITU, *National Cybersecurity Strategy Guide* (Příručka k národní strategii kybernetické bezpečnosti, 2011). K dispozici na adrese: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf.
ITU v roce 2017 vydá soubor nástrojů pro vytváření národních strategií kybernetické bezpečnosti (viz prezentace 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* (Tvorba politiky kybernetické bezpečnosti v bodě zlomu: Analýza nové generace národních strategií kybernetické bezpečnosti, 2012). K dispozici na adrese: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[9] Global Cyber Security Capacity Centre a University of Oxford, *Cybersecurity Capacity Maturity Model for Nations (CMM) - Revised Edition* (Model rozvoje schopností (CMM) států v oblasti kybernetické bezpečnosti – revidované znění, 2016). K dispozici na adrese: https://www.thegfce.com/binaries/gfce/documents/publications/2017/02/13/cybersecurity-cmm-for-nations/CMM+revised+edition.pdf

2.4 Konkrétní kroky, které musí členské státy podniknout do lhůty pro provedení směrnice

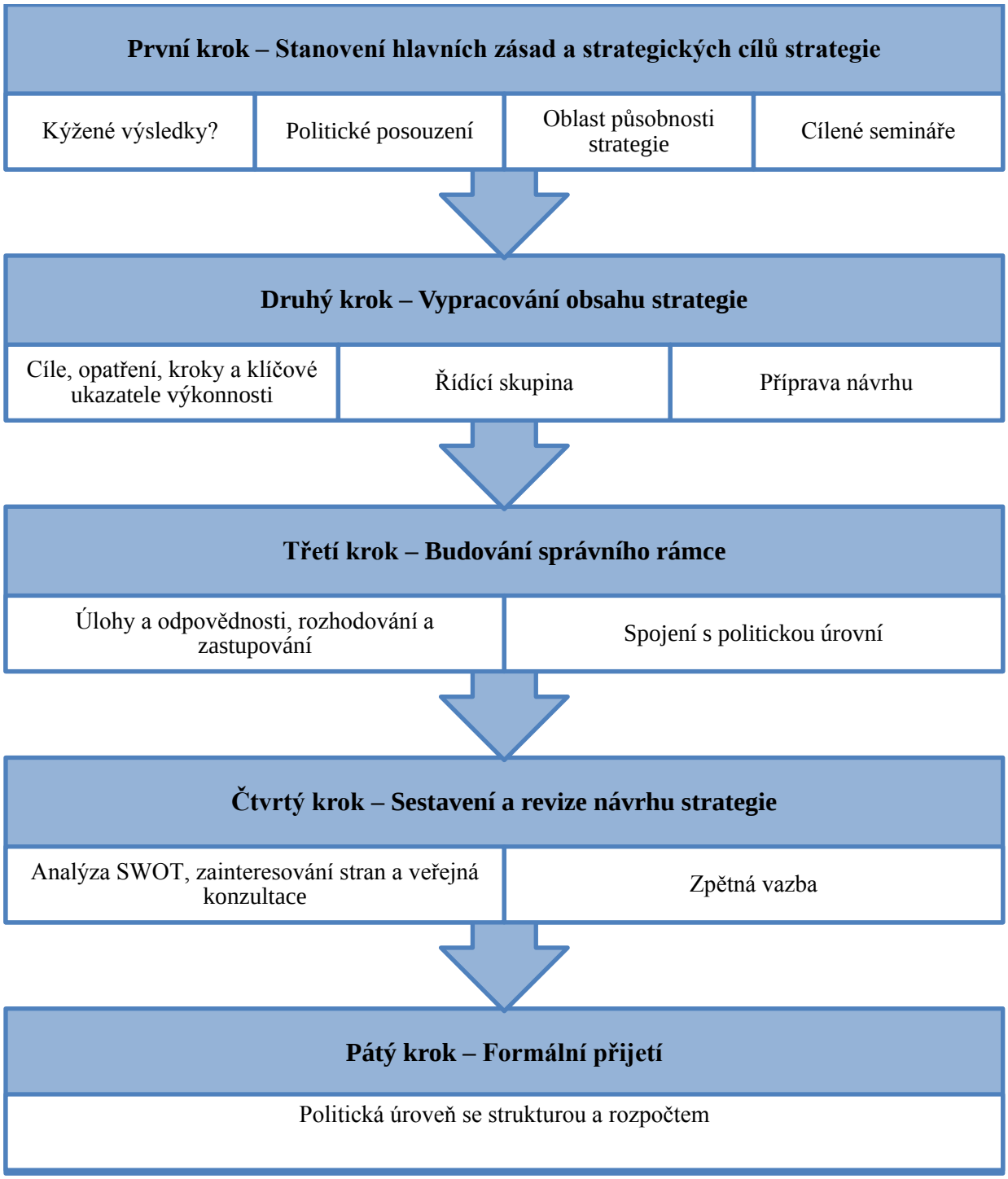
Dokumenty označené jako národní strategie kybernetické bezpečnosti zveřejnily téměř všechny členské státy[10] již před přijetím směrnice. V bodě 6 této přílohy je uveden aktuální seznam národních strategií platných v jednotlivých členských státech[11]. Tyto strategie obvykle zahrnují strategické zásady, pokyny, cíle, a v některých případech i konkrétní opatření ke zmírnění rizik souvisejících s kybernetickou bezpečností.

Vzhledem k tomu, že některé z těchto strategií byly přijaty před přijetím směrnice o bezpečnosti sítí a informací, nemusí nutně obsahovat všechny prvky uvedené v článku 7. Pro správné provedení směrnice ve vnitrostátním právu budou členské státy muset zjistit nedostatky kontrolou, zda jejich národní strategie obsahuje oněch sedm konkrétních požadavků vyjmenovaných v článku 7 směrnice promítnutých do odvětví uvedených v příloze II a služeb uvedených v příloze III směrnice. Zjištěné nedostatky lze pak řešit buď revizí stávajících národních strategií nebo kompletní revizí zásad národní strategie bezpečnosti sítí a informací. Výše uvedené pokyny k postupu přijímání národní strategie kybernetické bezpečnosti platí rovněž pro revizi a aktualizaci stávající národní strategie.

[10] Kromě Řecka, které národní strategii kybernetické bezpečnosti připravuje od roku 2014 (viz https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/view).

[11] Tyto informace čerpají z přehledu národních strategií kybernetické bezpečnosti, který uvádí agentura ENISA na adrese: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

Obrázek 1: Pět kroků k přijetí národní strategie kybernetické bezpečnosti



3. Směrnice o bezpečnosti sítí a informací: vnitrostátní příslušné orgány, jednotná kontaktní místa a skupiny pro reakce na počítačové bezpečnostní incidenty (CSIRT)

V čl. 8 odst. 1 se požaduje, aby členské státy určily jeden nebo více vnitrostátních příslušných orgánů, alespoň pro odvětví podle přílohy II a služby podle přílohy III směrnice, jejichž úkolem je dohlížet na provádění směrnice. Členské státy mohou tuto úlohu svěřit již existujícímu orgánu nebo orgánům.

Tento bod osvětluje, jak směrnice o bezpečnosti sítí a informací zvyšuje připravenost členských států tím, že vyžaduje, aby měly účinné vnitrostátní příslušné orgány a týmy CSIRT. Konkrétněji se v tomto bodu hovoří o povinnosti určit příslušné vnitrostátní orgány a o úloze jednotného kontaktního místa. Pozornost je v něm věnována třem tématům: a) možným řídícím strukturám na vnitrostátní úrovni (např. centralizovaný, decentralizovaný model atd.) a dalším požadavkům, b) úloze jednotného kontaktního místa a c) týmům CSIRT.

3.1 Druhy orgánů

Článek 8 směrnice o bezpečnosti sítí a informací vyžaduje od členských států, aby určily vnitrostátní příslušné orgány v oblasti bezpečnosti sítí a informačních systémů, přičemž výslovně uvádí možnost určit „*jeden nebo více vnitrostátních příslušných orgánů*“. Tuto možnost volby vysvětluje 30. bod odůvodnění směrnice: „*Vzhledem k odlišnostem jednotlivých vnitrostátních správních struktur a s cílem podpořit již existující odvětvová opatření nebo kontrolní a regulační orgány Unie a zamezit zdvojování činností by členské státy měly mít možnost určit více než jeden vnitrostátní příslušný orgán odpovědný za plnění úkolů spojených s bezpečností sítí a informačních systémů provozovatelů základních služeb a poskytovatelů digitálních služeb podle této směrnice.*“

To znamená, že členské státy se mohou rozhodnout, zda určí jeden ústřední orgán, který bude odpovídat za všechna odvětví a služby v oblasti působnosti směrnice, nebo několik takových orgánů, například podle druhu odvětví.

Při rozhodování o nejvhodnějším přístupu mohou členské státy čerpat ze zkušeností s vnitrostátními přístupy použitými v kontextu stávajících právních předpisů o ochraně kritické infrastruktury (OKII). Jak je uvedeno v tabulce 1, v případě ochrany kritické infrastruktury se členské státy při rozdělování kompetencí na vnitrostátní úrovni rozhodovaly mezi centralizovaným, nebo decentralizovaným přístupem. Příklady z jednotlivých států jsou zde uvedeny pouze pro ilustraci a s cílem upozornit členské státy na existující organizační rámce. Komise tedy netvrdí, že model, který jednotlivé země použily pro ochranu kritické informační infrastruktury, by měl být nutně použit také pro účel provedení směrnice o bezpečnosti sítí a informací.

Členské státy se mohou rozhodnout i pro různá hybridní řešení zahrnující prvky jak centralizovaného, tak decentralizovaného přístupu. Při tomto rozhodování lze rovněž zohlednit dřívější vnitrostátní řídicí uspořádání v jednotlivých odvětvích a službách v oblasti působnosti směrnice, nebo mohou nové řešení přijmout dotčené příslušné orgány a příslušné zúčastněné strany, jež jsou provozovateli základních služeb a poskytovateli digitálních služeb. Důležitým faktorem tohoto rozhodování může být také dostatek odborných technických znalostí v oblasti kybernetické bezpečnosti, otázka zdrojů, vztahy mezi zúčastněnými stranami a národní zájmy (např. hospodářský rozvoj, veřejná bezpečnost atd.).

3.2 Zveřejnění a další související hlediska

Podle čl. 8 odst. 7 musí členské státy Komisi oznámit určení vnitrostátních příslušných orgánů a jejich úkolů. Musí tak učinit ve lhůtě pro provedení směrnice ve vnitrostátním právu.

V článcích 15 a 17 směrnice o bezpečnosti sítí a informací je po členských státech požadováno, aby příslušné orgány měly pravomoci a prostředky pro provádění úkolů stanovených v těchto článcích.

Dále musí být zveřejněny konkrétní subjekty, které byly určeny jako příslušné vnitrostátní orgány. Směrnice nestanoví, jak má být toto zveřejnění provedeno. Jelikož cílem tohoto požadavku je vysoká informovanost subjektů, na něž se vztahuje směrnice o bezpečnosti sítí a informací, i široké veřejnosti, a s ohledem na zkušenosti z jiných odvětví (telekomunikace, bankovnictví, léčivé přípravky) lze podle Komise tento požadavek splnit například prostřednictvím dobře propagovaného portálu.

Podle čl. 8 odst. 5 směrnice mají členské stát zajistit, aby tyto orgány disponovaly „odpovídajícími zdroji“ pro plnění směrnicí svěřených úkolů.

Tabulka 1: Vnitrostátní přístupy k ochraně kritické informační infrastruktury (OKII)

Agentura ENISA v roce 2016 zveřejnila studii[12] o různých přístupech členských států k ochraně jejich kritické informační infrastruktury. Uvádí se v ní dva profily řízení OKII v členských státech, které lze použít v souvislosti s prováděním směrnice o bezpečnosti sítí a informací.

Profil 1: Decentralizovaný přístup s několika odvětvovými orgány odpovídajícími za příslušné odvětví a služby uvedené v příloze II a III směrnice

Decentralizovaný přístup se vyznačuje:

i) zásadou subsidiarity,
ii) úzkou spoluprací veřejných subjektů,
iii) odvětvovými právními předpisy.

Zásada subsidiarity

Místo zřízení nebo určení jediného subjektu s celkovou odpovědností se decentralizovaný přístup řídí zásadou subsidiarity. To znamená, že odpovědnost za provádění je v rukou odvětvového orgánu, který nejlépe rozumí danému odvětví a má již se zúčastněnými stranami zavedený vztah. Podle této zásady se rozhodnutí přijímají co nejblíže těm, na něž mají dopad.

Úzká spolupráce veřejných subjektů

S ohledem na rozmanitost veřejných subjektů zapojených do OKII si mnoho členských států zavedlo systémy spolupráce pro koordinaci práce a úsilí jednotlivých orgánů. Tyto systémy spolupráce mohou mít podobu neformálních sítí nebo institucionalizovanějších fór nebo ujednání. Slouží však pouze pro výměnu informací a koordinaci různých veřejných subjektů a nemají nad nimi žádnou pravomoc.

Odvětvové právní předpisy

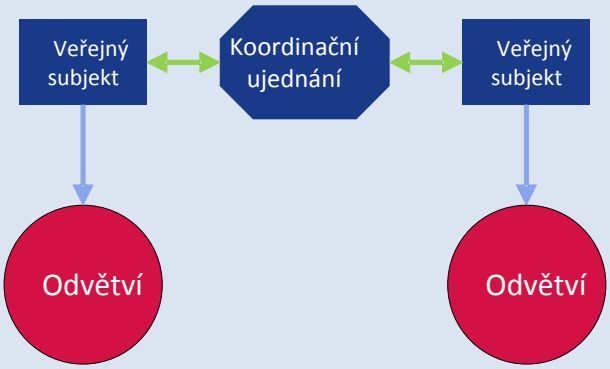
Země, které se rozhodly pro decentralizovaný přístup v nejdůležitějších odvětvích, často oblast OKII legislativně neupravují. Místo toho se právní předpisy přijímají pro konkrétní odvětví, takže se tyto předpisy mezi sebou mohou podstatně lišit. Výhodou tohoto přístupu je harmonizace opatření souvisejících se sítěmi a informačními systémy se stávajícími odvětvovými předpisy, což usnadňuje jejich přijímání daným odvětvím a zvyšuje účinnost vymáhání příslušným orgánem.

Čistě decentralizovaný přístup však skrývá zásadní riziko, že se směrnice nebude napříč různými odvětvími a službami uplatňovat konzistentně. V tomto případě směrnice zavádí jednotná vnitrostátní kontaktní místa, jejichž úkolem je spolupracovat na přeshraničních otázkách; tyto subjekty může dotyčný členský stát rovněž pověřit interní koordinací

[12] ENISA, *Stocktaking, Analysis and Recommendations on the protection of CIIs* (Hodnocení, analýza a doporučení k ochraně kritické informační infrastruktury, 2016). Dostupné na internetových stránkách: https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

a spoluprací mezi několika vnitrostátními příslušnými orgány v souladu s článkem 10 směrnice.

Obrázek 2 – Decentralizovaný přístup



Příklady decentralizovaného přístupu

Dobrým příkladem země s decentralizovaným přístupem k OKII je Švédsko. Tato země využívá tzv. „systémový pohled“, což znamená, že hlavní úkoly v oblasti OKII, jako je identifikace klíčových služeb a kritických infrastruktur, koordinace a podpora provozovatelů, regulační úkoly, jakož i opatření připravenosti na nouzové situace, spadají do odpovědnosti jednotlivých subjektů a obcí. Mezi tyto subjekty patří například švédský úřad pro civilní připravenost (MSB), švédský poštovní a telekomunikační úřad (PTS) a několik švédských subjektů v oblasti obrany, ozbrojených sil a prosazování práva.

V zájmu koordinace činností jednotlivých úřadů a veřejných subjektů zřídila švédská vláda síť pro spolupráci, která zahrnuje orgány „se specifickými společenskými úkoly v oblasti informační bezpečnosti“. Tato skupina pro spolupráci v oblasti informační bezpečnosti (SAMFI) je složena ze zástupců různých orgánů a schází se několikrát do roka, aby projednala otázky národní bezpečnosti informací. SAMFI je činná zejména v politicko-strategických otázkách a věnuje se tématům, jako jsou technické otázky a standardizace, vnitrostátní i mezinárodní vývoj v oblasti informační bezpečnosti či řízení a prevence incidentů v informačních technologiích. (Švédský úřad pro civilní připravenost (MSB) 2015).

Švédsko nepřijalo žádný ústřední zákon o OKII, který by se vztahoval na všechny provozovatele kritické informační infrastruktury (KII) ve všech odvětvích. Přijímání právních předpisů, které stanoví povinnosti společností v jednotlivých odvětvích, naopak přísluší veřejným orgánům. MSB má například právo přijímat předpisy pro vládní orgány v oblasti informační bezpečnosti, zatímco PTS může od provozovatelů vyžadovat přijetí určitých technických nebo organizačních bezpečnostních opatření na základě sekundárního práva.

Dalším příkladem země vykazující vlastnosti tohoto profilu je Irsko. Tato země se řídí „zásadou subsidiarity“, kde je každé ministerstvo odpovědné za identifikaci KII a hodnocení

rizik ve své oblasti. Ani zde nebyly na vnitrostátní úrovni přijaty žádné konkrétní předpisy o ochraně KII. Právní předpisy zůstávají na odvětvové úrovni a týkají se zejména odvětví energetiky a telekomunikací (2015). Dalšími příklady jsou Rakousko, Kypr a Finsko.

Profil 2: Centralizovaný přístup s jedním ústředním orgánem odpovídajícím za všechna odvětví a služby uvedené v příloze II a III směrnice

Centralizovaný přístup se vyznačuje:

i) jedním ústředním orgánem pro všechna odvětví,
ii) komplexními právními předpisy.

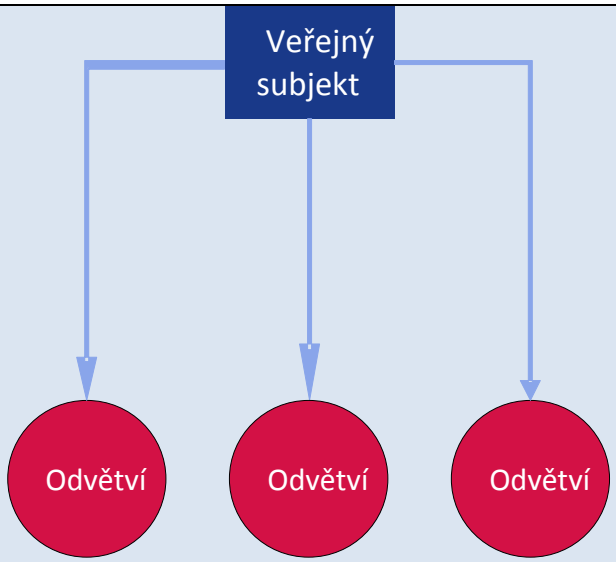
Jeden ústřední orgán pro všechna odvětví

Členské státy, které uplatňují centralizovaný přístup, zřídily orgány s rozsáhlými pravomocemi a odpovědnostmi v několika nebo ve všech klíčových odvětvích nebo rozšířily pravomoci stávajících orgánů. Tyto hlavní orgány pro oblast OKII plní několik úkolů, jako jsou pohotovostní plánování, řízení nouzových situací, regulace či podpora soukromých provozovatelů. V mnoha případech jsou součástí hlavního orgánu pro ochranu kritické informační infrastruktury národní či vládní týmy CSIRT. U ústředního orgánu je s ohledem na celkový nedostatek dovedností v oblasti kybernetické bezpečnosti pravděpodobná vyšší koncentrace příslušné odbornosti než u několika odvětvových orgánů.

Komplexní právní předpisy

Komplexní právní předpisy stanoví povinnosti a požadavky pro všechny provozovatele KII ve všech odvětvích. Může se jednat o nové komplexní právní předpisy nebo o doplnění stávajících odvětvových předpisů. Tento přístup by napomohl jednotnému uplatňování směrnice o bezpečnosti sítí a informací ve všech dotčených odvětvích a službách. Zamezilo by se riziko nedostatků v provádění, které hrozí v případě existence několika orgánů se specifickou působností.

Obrázek 3 – Centralizovaný přístup



Příklady centralizovaného přístupu

Dobrým příkladem členského státu EU s centralizovaným přístupem je Francie. Francouzská Agence Nationale de la Sécurité des Systèmes d'Information (Národní agentura pro bezpečnost informačních systémů, ANSSI) byla v roce 2011 určena za hlavní vnitrostátní orgán obrany informačních systémů. ANSSI má silné postavení v oblasti dohledu nad „provozovateli klíčového významu“: může jim uložit, aby se podřídili bezpečnostním opatřením, a provádět u nich bezpečnostní audity. Kromě toho je hlavním jednotným kontaktním místem pro provozovatele klíčového významu, kteří mají povinnost hlásit agentuře bezpečnostní incidenty.

V případě bezpečnostních incidentů jedná ANSSI jako agentura pro krizové situace v oblasti OKII a rozhoduje o opatřeních, která musí provozovatelé v reakci na krizi přijmout. Vládní opatření jsou koordinována v operačním středisku ANSSI. Detekce hrozeb a reakce na incidenty na operační úrovni je úkolem skupiny CERT-FR, která je součástí ANSSI.

Francie zavedla pro oblast OKII komplexní právní rámec. Předseda vlády v roce 2006 nařídil vypracování seznamu odvětví kritické infrastruktury. Na základě tohoto seznamu, kde bylo identifikováno dvanáct klíčových odvětví, vláda určila zhruba 250 provozovatelů klíčového významu. V roce 2013 vstoupil v platnost zákon o vojenském plánování[13]. Ten ukládá uvedeným provozovatelům různé povinnosti, včetně hlášení incidentů nebo přijímání bezpečnostních opatření. Tyto požadavky se vztahují na všechny provozovatele klíčového významu ve všech odvětvích (francouzský senát, 2013).

[13] La loi de programmation militaire.

3.3 Článek 9 směrnice o bezpečnosti sítí a informací: Bezpečnostní týmy typu CSIRT

Podle článku 9 musí členské státy zřídit jeden nebo více týmů typu CSIRT, které odpovídají za řešení rizik a incidentů v odvětvích uvedených v příloze II a službách uvedených v příloze III směrnice o bezpečnosti sítí a informací. Vzhledem k požadavku na minimální harmonizaci zakotvenému v článku 3 směrnice mohou členské státy využít týmy CSIRT také v dalších odvětvích, na která se tato směrnice nevztahuje, jako je například veřejná správa.

Členské státy se mohou rozhodnout zřídit tým CSIRT v rámci příslušného vnitrostátního orgánu[14].

3.4 Úkoly a požadavky

Úkoly týmů CSIRT podle přílohy I směrnice o bezpečnosti sítí a informací zahrnují:

- monitorování incidentů na vnitrostátní úrovni,
- vydávání včasných varování a upozornění, oznamování a šíření informací o rizicích a incidentech příslušným zúčastněným stranám,
- reakce na incidenty,
- poskytování dynamické analýzy rizik a incidentů a přehledu o situaci a
- účast v síti vnitrostátních týmů CSIRT (dále jen „síť CSIRT“) zřízené podle článku 12.

V čl. 14 odst. 3, 5 a 6 a v čl. 16 odst. 3, 6 a 7 jsou stanoveny další zvláštní úkoly v souvislosti s oznamováním incidentů pro případ, že členský stát rozhodne, že je tým CSIRT může plnit společně s příslušnými vnitrostátními orgány nebo místo nich.

Při provádění této směrnice mohou členské státy rozhodnout o úloze týmů CSIRT v souvislosti s požadavky na oznamování incidentů. Přímé povinné hlášení týmům CSIRT je možnost výhodná z hlediska správní účinnosti, avšak členské státy se mohou rozhodnout i pro přímé hlášení příslušným vnitrostátním orgánům, přičemž týmy CSIRT mají právo na přístup k informacím. Týmy CSIRT se v konečném důsledku soustředí na řešení problémů z hlediska zabránění kybernetickým incidentům, jejich odhalování, reakce na ně a zmírňování jejich dopadu (což platí i pro incidenty, které se nemusí povinně hlásit) společně se zúčastněnými stranami, zatímco dodržování předpisů je spíše věcí příslušných vnitrostátních orgánů.

Podle čl. 9 odst. 3 směrnice členské státy rovněž zajistí, aby jejich týmy CSIRT měly přístup k bezpečné a odolné infrastruktuře IKT.

Podle čl. 9 odst. 4 směrnice členské státy oznámí Komisi rozsah, jakož i hlavní prvky postupu týmů CSIRT při řešení incidentů.

Požadavky na týmy CSIRT zřízené členskými státy jsou uvedeny v příloze I směrnice o bezpečnosti sítí a informací. Tým CSIRT musí zajistit vysokou úroveň dostupnosti svých

[14] Viz čl. 9 odst. 1 poslední věta.

komunikačních služeb. Jeho pracoviště a podpůrné informační systémy se musí nacházet na bezpečném místě a musí být schopny zajistit kontinuitu činnosti. Dále musí mít týmy CSIRT možnost účastnit se mezinárodních sítí pro spolupráci.

3.5 Pomoc s rozvojem týmů CSIRT

Program pro infrastrukturu digitálních služeb (DSI) v oblasti kybernetické bezpečnosti v rámci Nástroje pro propojení Evropy (CEF) může týmům CSIRT jednotlivých členských států významně finančně přispět z prostředků EU při zlepšování jejich schopností a jejich vzájemné spolupráce prostřednictvím mechanismu spolupráce při výměně informací. Tento mechanismus spolupráce, který je vypracováván v rámci projektu SMART 2015/1089, má usnadnit rychlou a účinnou dobrovolnou operativní spolupráci mezi týmy CSIRT členských států, a to zejména na úkolech svěřených síti CSIRT článkem 12 směrnice.

Podrobnosti o příslušných výzvách k předkládání návrhů na budování kapacit týmů CSIRT v členských státech jsou k dispozici na internetových stránkách Výkonné agentury Evropské komise pro inovace a sítě (INEA)[15].

Řídící rada programu DSI v oblasti kybernetické bezpečnosti v rámci CEF je neformální strukturou politického řízení a podpory týmů CSIRT členských států při budování kapacit a zavádění mechanismu dobrovolné spolupráce.

Každý nově ustanovený tým CSIRT nebo tým určený k plnění úkolů uvedených v příloze I směrnice o bezpečnosti sítí a informací může ke zkvalitnění a zefektivnění své práce využít poradenství a odborné znalosti agentury ENISA[16]. V tomto ohledu je třeba poznamenat, že týmy CSIRT členských států by mohly vycházet z některých nedávných výsledků práce této agentury. Konkrétně, jak je uvedeno v bodě 7 této přílohy, agentura vydala několik dokumentů a studií, v nichž byly popsány osvědčené postupy a technická doporučení týkající se hodnocení stupně vývoje týmů CSIRT z hlediska různých jejich schopností a služeb. Kromě toho své pokyny a osvědčené postupy sdílely i sítě CSIRT na světové (FIRST[17]) i evropské úrovni (Trusted Introducer, TI[18]).

3.6 Úloha jednotného kontaktního místa

Podle čl. 8 odst. 3 směrnice o bezpečnosti sítí a informací musí každý členský stát určit vnitrostátní jednotné kontaktní místo, které bude plnit styčnou funkci s cílem zajistit přeshraniční spolupráci s relevantními orgány v jiných členských státech a se skupinou pro spolupráci a sítí CSIRT[19], které zavádí sama směrnice. V 31. bodu odůvodnění a v čl. 8 odst. 4 je vysvětlen účel uvedeného požadavku, tj. usnadnit přeshraniční spolupráci a komunikaci. Ta je zvláště důležitá vzhledem k tomu, že se členské státy mohou rozhodnout, že určí více než jeden vnitrostátní orgán. Jednotné kontaktní místo tak usnadní identifikaci a spolupráci orgánů z různých členských států.

[15] Dostupné na internetových stránkách: https://ec.europa.eu/inea/en/connecting-europe-facility.
[16] Viz čl. 9 odst. 5 směrnice o bezpečnosti sítí a informací.
[17] Fórum týmů pro reakci na bezpečnostní incidenty a pro bezpečnost (https://www.first.org/).
[18] https://www.trusted-introducer.org/
[19] Síť vnitrostátních týmů CSIRT pro operativní spolupráci mezi členskými státy podle článku 12.

Styčná úloha tohoto jednotného kontaktního místa bude pravděpodobně zahrnovat interakci se sekretariáty skupiny pro spolupráci a sítě CSIRT v případech, kdy vnitrostátním jednotným kontaktním místem není ani tým CSIRT, ani člen skupiny pro spolupráci. Členské státy musí kromě toho zajistit, aby bylo jednotné kontaktní místo informováno o oznámeních obdržených od provozovatelů základních služeb a poskytovatelů digitálních služeb.[20]

V čl. 8 odst. 3 směrnice se stanoví, že pokud členský stát zavede centralizovaný přístup, tj. určí pouze jeden příslušný orgán, bude tento orgán zároveň plnit funkci jednotného kontaktního místa. Rozhodne-li se členský stát pro decentralizovaný přístup, může jako jednotné kontaktní místo určit některý z příslušných orgánů. Bez ohledu na zvolený institucionální model, jsou-li příslušný orgán, tým CSIRT a jednotné kontaktní místo samostatnými subjekty, musí členské státy zajistit jejich účinnou spolupráci při plnění povinností stanovených směrnicí.[21]

Jednotné kontaktní místo musí do 9. srpna 2018 a poté každý rok předkládat skupině pro spolupráci souhrnnou zprávu o obdržených oznámeních včetně počtu oznámení a povahy oznámených incidentů a včetně opatření přijatých orgány, jako je informování ostatních dotčených členských států o incidentu či poskytnutí relevantních informací pro řešení incidentu oznamujícímu podniku.[22] Na žádost příslušného orgánu nebo týmu CSIRT musí jednotné kontaktní místo zasílat oznámení provozovatele základních služeb jednotným kontaktním místům ostatních členských států, jichž se incident týká.[23]

Členské státy mají Komisi informovat o určení jednotného kontaktního místa a o jeho úkolech ve lhůtě pro provedení směrnice. Určení jednotného kontaktního místa má být zveřejněno, stejně jako u příslušných vnitrostátních orgánů. Komise zveřejní seznam určených jednotných kontaktních míst.

3.7 Sankce

Článek 21 ponechává členským státům prostor pro rozhodnutí o druhu a povaze platných sankcí, jež však musí být účinné, přiměřené a odrazující. Jinými slovy mohou členské státy v zásadě svobodně rozhodnout o maximální výši sankcí stanovených ve vnitrostátních právních předpisech, ale zvolená částka nebo procento by měly vnitrostátním orgánům umožňovat, aby v každém konkrétním případě uložily účinné, přiměřené a odrazující sankce při zohlednění různých faktorů, jako je závažnost nebo četnost porušení právních předpisů.

4. Subjekty s povinnostmi v oblasti bezpečnostních požadavků a oznamování incidentů

Subjekty s významnou úlohou ve společnosti a v hospodářství, o kterých se hovoří v čl. 4 odst. 4 a 5 směrnice jako o provozovatelích základních služeb a poskytovatelích digitálních služeb, musí přijmout vhodná bezpečnostní opatření a oznamovat závažné incidenty příslušným vnitrostátním orgánům. Důvodem je skutečnost, že dopad bezpečnostních

[20] Viz čl. 10 odst. 3
[21] Viz čl. 10 odst. 1.
[22] Tamtéž.
[23] Viz čl. 14 odst. 5.

incidentů v těchto službách může vážně ovlivnit jejich provoz, což může vést k výraznému narušování ekonomické činnosti a fungování společnosti v širokém měřítku, a narušovat tak důvěru uživatelů a způsobovat značnou újmu hospodářství Unie[24].

V tomto bodě je uveden přehled subjektů spadajících do působnosti příloh II a III směrnice o bezpečnosti sítí a informací, jakož i seznam jejich povinností. Identifikace provozovatelů základních služeb je pokryta vyčerpávajícím způsobem s ohledem na její význam pro harmonizované provádění směrnice o bezpečnosti sítí a informací v celé EU. Tento bod se podrobně věnuje i definici digitální infrastruktury a poskytovatelů digitálních služeb. Zároveň se zabývá možným začleněním dalších odvětví a podrobněji vysvětluje specifický přístup k poskytovatelům digitálních služeb.

4.1 Provozovatelé základních služeb

Směrnice o bezpečnosti sítí a informací výslovně nestanoví, které konkrétní subjekty mají být považovány za provozovatele základních služeb spadající do její oblasti působnosti. Místo toho stanoví kritéria, která mají členské státy použít při určování společností typologicky odpovídajících subjektům uvedeným v příloze II, jež budou považovány za provozovatele základních služeb, a v důsledku toho se na ně budou vztahovat povinnosti stanovené směrnicí.

4.1.1 Typ subjektů uvedených v příloze II směrnice o bezpečnosti sítí a informací

V čl. 4 odst. 4 jsou provozovatelé základních služeb definováni jako veřejné nebo soukromé subjekty, jejichž druh je uveden v příloze II směrnice a jež splňují kritéria stanovená v čl. 5 odst. 2. V příloze II jsou uvedena odvětví, pododvětví a druhy subjektů, u nichž musí členské státy použít postup určování podle čl. 5 odst. 2[25]. Mezi uvedená odvětví patří energetika, doprava, bankovnictví, infrastruktury finančního trhu, zdraví, zásobování vodou a digitální infrastruktura.

U většiny subjektů spadajících do „tradičních“ odvětví obsahují právní předpisy EU zavedené definice, na které příloha II odkazuje. V případě digitální infrastruktury uvedené v bodě 7 přílohy II, včetně výměnných uzlů internetu (IXP), systému doménových jmen (DNS) a registrů internetových domén nejvyšší úrovně (TLD), tomu tak však není. Proto se v zájmu vyjasnění uvedené definice níže podrobně vysvětlují.

1) Výměnný uzel internetu (IXP)

Pojem „výměnný uzel internetu (IXP)“ je definován v čl. 4 odst. 13 a blíže vysvětlen v 18. bodě odůvodnění, přičemž jej lze popsat jako síťové zařízení umožňující propojení více než dvou nezávislých, technicky samostatných systémů, a to primárně pro účely usnadnění výměny dat zasílaných prostřednictvím internetu. Výměnný uzel internetu lze rovněž popsat jako fyzické místo, na němž si více sítí může vzájemně vyměňovat data prostřednictvím

[24] Viz 2. bod odůvodnění.
[25] Postup určování je podrobněji popsán níže v bodě 4.1.6.

síťového přepínače. Hlavním účelem IXP je umožnit sítím přímé propojení prostřednictvím výměnného uzlu, bez potřeby zahrnout jednu nebo více sítí třetích stran. Poskytovatel IXP obvykle neodpovídá za směrování datových toků. Za to jsou odpovědní poskytovatelé sítí. Přímé propojení má mnoho výhod, ale hlavními jsou náklady, latence a šířka pásma. Za datový tok přes výměnný uzel si zpravidla žádná strana neúčtuje poplatek, zatímco za tok k poskytovateli internetových služeb ano. Přímé propojení je často umístěno ve stejném městě jako obě příslušné sítě, a proto údaje nemusí překonávat při přenosu mezi sítěmi velké vzdálenosti, čímž se sníží latence.

Je však třeba poznamenat, že definice IXP nezahrnuje fyzické body, které vzájemně propojují pouze dvě fyzické sítě (tj. poskytovatele sítí jako BASE nebo PROXIMUS). Při provádění směrnice proto členské státy musí rozlišovat mezi provozovateli, kteří usnadňují výměnu souhrnných internetových datových toků mezi více provozovateli sítí, a provozovateli jediné sítě, kteří své sítě fyzicky propojují na základě smlouvy o vzájemném propojení. Ve druhém z uvedených případů poskytovatelé sítí nespadají do definice uvedené v čl. 4 odst. 13. To je vysvětleno v 18. bodě odůvodnění, kde se uvádí, že výměnný uzel internetu neposkytuje přístup k internetu ani nefunguje jako poskytovatel tranzitního připojení nebo tranzitní infrastruktury. Poslední kategorií poskytovatelů jsou podniky poskytující veřejné komunikační sítě nebo služby, na které se vztahují bezpečnostní a ohlašovací povinnosti podle článků 13a a 13b směrnice 2002/21/ES, a které jsou tudíž vyňaty z oblasti působnosti směrnice o bezpečnosti sítí a informací[26].

2) Systém doménových jmen (DNS)

Pojem „systém doménových jmen“ je v čl. 4 odst. 14 definován jako *„hierarchický distribuovaný systém doménových jmen v rámci sítě adresující dotazy na doménová jména“*. Přesněji lze DNS popsat hierarchický distribuovaný systém jmen pro počítače, služby nebo jakékoli jiné zdroje připojené k internetu, který umožňuje kódování doménových jmen do adres IP. Hlavním úkolem tohoto systému je převádět přidělená doménová jména na adresy IP. K uvedenému účelu spravuje DNS svoji databázi a k tomuto typu „převodu“ doménových jmen na operační adresy IP využívá servery doménových jmen a resolver. Ačkoli kódování doménových jmen není jediným úkolem DNS, jedná se o jeho hlavní úlohu. Právní definice v čl. 4 odst. 14 se zaměřuje na hlavní roli systému z hlediska uživatele a nezabývá se techničtějšími podrobnostmi, např. fungováním doménového jmenného prostoru, serverů doménových jmen, resolverů atd. Konečně, v čl. 4 odst. 15 je vyjasněno, kdo má být považován za poskytovatele služeb DNS.

3) Registr internetových domén nejvyšší úrovně (registr TLD)

Registr internetových domén nejvyšší úrovně je v čl. 4 odst. 16 definován jako subjekt, který spravuje a provozuje registraci internetových doménových jmen pod určitou doménou nejvyšší úrovně. Tato správa a řízení doménových jmen zahrnuje kódování jmen TLD do IP adres.

[26] Vztah mezi směrnicí o bezpečnosti sítí a informací a směrnicí 2002/21/ES je podrobněji popsán v bodě 5.2.

Za celosvětovou koordinaci kořenové zóny DNS, přidělování adres internetového protokolu a další zdroje spojené s internetovým protokolem odpovídá Organizace pro přidělování čísel na internetu (IANA). Tento subjekt je zejména odpovědný za přidělování generických domén nejvyšší úrovně (gTLD) jako „.com“ a národních domén nejvyšší úrovně (ccTLD) jako „.be“ provozovatelům (registrům) a za údržbu jejich technických a administrativních údajů. IANA vede celosvětový registr všech přidělených TLD a podílí se na šíření tohoto seznamu mezi uživateli internetu po celém světě, jakož i na zavádění nových TLD.

Významnou úlohou registrů je přidělovat názvy druhé úrovně tzv. držitelům v rámci jejich příslušné TLD. Pokud chtějí, mohou tito držitelé sami přidělovat doménová jména třetí úrovně.Účelem ccTLD je představovat země nebo území na základě normy ISO 3166-1. Generické TLD obvykle nejsou spojeny s určitým zeměpisným vymezením či zemí.

Je třeba poznamenat, že správa registru TLD může zahrnovat poskytování DNS. Například podle pravidel organizace IANA pro delegování musí subjekt, který odpovídá za ccTLD, mimo jiné dohlížet nad doménovými jmény a provozovat DNS dotčené země[27]. Takové okolnosti musejí členské státy v procesu určování provozovatelů základních služeb podle čl. 5 odst. 2 zohlednit.

4.1.2 Určování provozovatelů základních služeb

Podle článku 5 směrnice se od každého členského státu vyžaduje, aby provedl proces určování u všech subjektů odpovídajících druhům uvedeným v příloze II, které mají sídlo na území tohoto členského státu. Jako výsledek tohoto posouzení budou všechny subjekty, které splňují kritéria stanovená v čl. 5 odst. 2, označeny jako provozovatelé základních služeb a budou se na ně vztahovat bezpečnostní a ohlašovací povinnosti podle článku 14.

Provozovatele v každém odvětví a pododvětví mají členské státy určit do 9. listopadu 2018. S cílem pomoci členským státům v tomto procesu skupina pro spolupráci v současné době připravuje pokyny s důležitými informacemi o potřebných krocích a osvědčených postupech při určování provozovatelů základních služeb.

Kromě toho skupina pro spolupráci v souladu s čl. 24 odst. 2 prodiskutuje proces, podstatu a typy vnitrostátních opatření, což umožní určit provozovatele základních služeb v konkrétních odvětvích. Členské státy mohou do 9. listopadu 2018 zaslat své návrhy vnitrostátních opatření, která umožní určit provozovatele základních služeb, k diskusi v rámci skupiny pro spolupráci.

4.1.3 Začlenění dalších odvětví

S ohledem na požadavek na minimální harmonizaci stanovený v článku 3 mohou členské státy přijmout nebo ponechat v platnosti právní předpisy, které zajišťují vyšší míru bezpečnosti sítí a informačních systémů. V tomto ohledu mají členské státy v zásadě volnost při rozšiřování bezpečnostních a oznamovacích povinností podle článku 14 rovněž na subjekty působící v jiných odvětvích a pododvětvích, než která jsou uvedena v příloze II

[27] Informace dostupné na internetové adrese: https://www.icann.org/resources/pages/delegation-2012-02-25-en.

směrnice o bezpečnosti sítí a informací. Některé členské státy se již rozhodly nebo zvažují, že do oblasti působnosti příslušných ustanovení zahrnou nějaká z těchto dalších odvětví:

i) Veřejná správa

Orgány veřejné správy mohou poskytovat základní služby podle přílohy II směrnice, které splňují požadavky uvedené v čl. 5 odst. 2. V takovém případě se na orgány veřejné správy, které tyto služby nabízejí, vztahují příslušné bezpečnostní požadavky a oznamovací povinnosti. Z toho *a contrario* vyplývá, že na orgány veřejné správy poskytující služby, které do uvedené působnosti nespadají, se příslušné povinnosti nevztahují.

Orgány veřejné správy jsou odpovědné za řádné poskytování veřejných služeb orgány státní správy, místními a regionálními orgány, agenturami a dalšími zapojenými podniky. Tyto služby často vyžadují vytvoření a správu osobních a firemních údajů o jednotlivcích a organizacích, které mohou být poskytovány a zpřístupňovány mnoha veřejným subjektům. Obecněji řečeno je vysoká bezpečnost sítí a informačních systémů ve veřejné správě důležitým zájmem celé společnosti a ekonomiky. Komise proto zastává názor, že by bylo rozumné, kdyby členské státy zvážily začlenění veřejné správy do oblasti působnosti vnitrostátních právních předpisů provádějících tuto směrnici, a to nad rámec poskytování základních služeb podle přílohy II a čl. 5 odst. 2.

ii) Odvětví pošt

Odvětví pošt zahrnuje poskytování poštovních služeb, jako je příjem, třídění, přeprava nebo dodávání poštovních zásilek.

iii) Potravinářství

Potravinářství zahrnuje produkci zemědělských a jiných potravinářských výrobků a může zahrnovat základní služby, jako je potravinové zabezpečení a zajištění jakosti a bezpečnosti potravin.

iv) Chemický a atomový průmysl

Chemický a atomový průmysl zahrnuje zejména skladování, výrobu a zpracování chemických a petrochemických produktů nebo jaderného materiálu.

v) Životní prostředí

Environmentální činnosti zahrnují dodávky zboží a služeb nezbytných pro ochranu životního prostředí a řízení zdrojů. Jsou tedy zaměřeny na prevenci, snižování a odstranění znečišťování a ochranu dostupných přírodních zdrojů. V tomto odvětví by základními službami mohly být sledování a kontrola znečištění (např. vzduchu a vody) a meteorologických jevů.

vi) Civilní ochrana

Cílem v odvětví civilní ochrany je prevence, připravenost a reakce v souvislosti s přírodními katastrofami i katastrofami způsobeným člověkem. Mezi služby poskytované za tímto účelem může patřit aktivace čísel tísňového volání a provádění opatření k informování o nouzových situacích, zamezení jejich šíření a jejich řešení.

4.1.4 Pravomoc

Podle čl. 5 odst. 1 musí každý členský stát určit provozovatele základních služeb usazené na jeho území. V ustanovení se blíže neupřesňuje druh zákonného usazení, nicméně 21. bod odůvodnění objasňuje, že takové usazení předpokládá účinný a skutečný výkon činnosti prostřednictvím stálých struktur, přičemž právní forma těchto struktur by neměla být rozhodující. Znamená to, že členský stát může mít pravomoc ve vztahu k provozovateli základních služeb nejen v případech, kdy má provozovatel na jeho území sídlo, ale rovněž tehdy, pokud tam má například pobočku nebo je na jeho území jinak zákonně usazen.

Z toho vyplývá, že určitý subjekt může zároveň podléhat pravomoci více členských států.

4.1.5 Informace předkládané Komisi

Pro účely přezkumu, který musí Komise provést v souladu s čl. 23 odst. 1 směrnice o bezpečnosti sítí a informací, se od členských států vyžaduje, aby Komisi do 9. listopadu 2018 a poté každé dva roky předložily tyto informace:

- vnitrostátní opatření umožňující určení provozovatelů základních služeb,
- seznam základních služeb,
- počet určených provozovatelů základních služeb pro každé odvětví uvedené v příloze II a význam těchto provozovatelů v daném odvětví a
- mezní hodnoty, existují-li, pro stanovení zásobovací úrovně podle počtu uživatelů závislých na dané službě podle čl. 6 odst. 1 písm. a) nebo důležitosti konkrétního subjektu podle čl. 6 odst. 1 písm. f).

Přezkum podle čl. 23 odst. 1, který předchází komplexní revizi směrnice, odráží význam, který spolunormotvůrci přikládají správnému provedení směrnice, pokud jde o určení provozovatelů základních služeb, s cílem předejít roztříštěnosti trhu.

Aby bylo možné provést přezkum co nejlépe, Komise vyzývá členské státy, aby toto téma projednaly ve skupině pro spolupráci a rovněž si vyměnily relevantní zkušenosti. Komise dále členské státy vyzývá, aby jí, kromě veškerých informací, jejichž předložení požaduje směrnice, poskytly – případně důvěrně sdělily – seznamy určených provozovatelů základních služeb, kteří byli nakonec vybráni. Díky těmto seznamům by Komise mohla snadněji a lépe posoudit konzistentnost postupu určování a zároveň by bylo možné porovnat přístupy jednotlivých členských států, čímž by se lépe dosáhlo cílů směrnice.

4.1.6 Jak postupovat při určování provozovatelů základních služeb?

Obrázek 4 znázorňuje šest klíčových otázek, které by si měl vnitrostátní orgán při určování jednotlivých subjektů položit. V následující části každá otázka odpovídá jednomu kroku, který je třeba učinit podle článku 5 ve spojení s článkem 6 a při současném zohlednění použitelnosti čl. 1 odst. 7.

První krok – **Spadá daný subjekt do odvětví/pododvětví uvedeného v příloze II směrnice a odpovídá druhu subjektu v souladu se zmíněnou přílohou?**

Vnitrostátní orgán by měl posoudit, zda subjekt usazený na jeho území spadá do odvětví a pododvětví uvedených v příloze II směrnice. Příloha II obsahuje řadu hospodářských odvětví, která jsou považována za nezbytná pro zajištění řádného fungování vnitřního trhu. Příloha II konkrétně odkazuje na tato odvětví a pododvětví:

- energetika: elektřina, ropa a zemní plyn,
- doprava: letecká, železniční, vodní a silniční,
- bankovnictví: úvěrové instituce,
- infrastruktura finančních trhů: obchodní systémy, ústřední protistrany,
- zdravotnictví: zdravotnická zařízení (včetně nemocnic a soukromých klinik),
- voda: dodávky a rozvody pitné vody,
- digitální infrastruktura výměnné uzly internetu, poskytovatelé služeb systému doménových jmen a registry internetových domén nejvyšší úrovně[28].

Druhý krok – **Použije se *lex specialis*?**

V další fázi musí vnitrostátní orgán posoudit, zda se použije ustanovení o *lex specialis* zakotvené v čl. 1 odst. 7. Toto ustanovení zejména uvádí, že pokud existuje právní akt EU, který od poskytovatelů digitálních služeb nebo provozovatelů základních služeb vyžaduje plnění bezpečnostních požadavků a/nebo požadavků na hlášení incidentů, jež jsou přinejmenším rovnocenné odpovídajícím požadavkům směrnice o bezpečnosti sítí a informací, měly by se uplatnit povinnosti stanovené tímto zvláštním právním aktem. Kromě toho 9. bod odůvodnění objasňuje, že pokud jsou splněny požadavky čl. 1 odst. 7, členské státy by měly použít ustanovení odvětvového právního aktu EU, včetně těch, která se týkají pravomoci. Naopak příslušná ustanovení směrnice o bezpečnosti sítí a informací by se nepoužila. V takovém případě by příslušný orgán neměl v postupu určování podle čl. 5 odst. 2 pokračovat[29].

Třetí krok – **Poskytuje daný provozovatel základní službu ve smyslu směrnice?**

Podle čl. 5 odst. 2 písm. a) musí subjekt, který podléhá určení, poskytovat službu, která je základní z hlediska zachování kritických společenských nebo ekonomických činností. Při tomto posuzování by členské státy měly vzít v úvahu, že jeden subjekt může zároveň poskytovat jak základní, tak i jiné než základní služby. Z toho vyplývá, že bezpečnostní požadavky a požadavky na hlášení incidentů směrnice o bezpečnosti sítí a informací se na určitého provozovatele budou vztahovat pouze v rozsahu, v jakém tento provozovatel poskytuje základní služby.

[28]Tyto subjekty jsou blíže popsány v bodě 4.1.1.

[29] O použitelnosti *lex specialis* pojednává podrobněji bod 5.1.

Podle čl. 5 odst. 3 by měl členský stát vypracovat seznam všech základních služeb, které provozovatelé základních služeb poskytují na jeho území. Tento seznam je nutno předložit Komisi do 9. listopadu 2018 a poté každé dva roky[30].

Čtvrtý krok – **Je daná služba závislá na síti a informačním systému?**

Dále je třeba objasnit, zda tato služba splňuje druhé kritérium uvedené v čl. 5 odst. 2 písm. b), zejména pak zda poskytování takové základní služby závisí na sítích a informačních systémech uvedených v čl. 4 odst. 1.

Pátý krok – **Vedl by bezpečnostní incident k významnému narušení?**

V čl. 5 odst. 2 písm. c) se od vnitrostátního orgánu vyžaduje posouzení toho, zda by incident vedl k významnému narušení poskytování dané služby. V této souvislosti se v čl. 6 odst. 1 uvádí několik okolností působících napříč odvětvími, které je třeba při tomto posouzení zohlednit. V čl. 6 odst. 2 se dále stanoví, že při posuzování by se měly případně zvážit i okolnosti specifické pro jednotlivá odvětví.

Okolnosti působící napříč odvětvími uvedené v čl. 6 odst. 1 jsou tyto:

- počet uživatelů, kteří jsou závislí na službě poskytované daným subjektem,
- závislost dalších odvětví podle přílohy II na službě poskytované daným subjektem,
- možný dopad incidentů, pokud jde o jejich intenzitu a délku trvání, na ekonomické a společenské činnosti nebo na veřejnou bezpečnost,
- podíl daného subjektu na trhu,
- zeměpisný rozsah oblasti, která by mohla být incidentem dotčena,
- důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby, s přihlédnutím k dostupnosti alternativních způsobů zajištění této služby.

Pokud jde o **okolnosti specifické pro jednotlivá odvětví**, několik příkladů, které mohou být pro vnitrostátní orgány užitečným vodítkem, je uvedeno v 28. bodě odůvodnění (viz tabulka č. 4).

Tabulka 4: Příklady okolností působících napříč odvětvími, které by měly být zohledněny při určování významného narušení v případě incidentu

Odvětví	Příklady okolností specifických pro jednotlivá odvětví
Dodavatelé energie	objem výroby elektrické energie na vnitrostátní úrovni nebo podíl na této výrobě
Dodavatelé ropy	objem dodané ropy za den
Letecká doprava (včetně letišť a leteckých přepravců)	poměrný objem dopravy vzhledem k celkovému vnitrostátnímu objemu,

[30] Viz čl. 5 odst. 7 písm. b).

Železniční doprava **Námořní přístavy**	počet cestujících nebo nákladních operací za rok
Bankovnictví nebo infrastruktury finančních trhů	systémový význam na základě celkového majetku, poměrné množství takového majetku vzhledem k HDP
Zdravotnictví	počet pacientů v péči poskytovatele za rok
Výroba, zpracování a dodávky vody	objem dodávek a počet a druh uživatelů (včetně nemocnic, organizací poskytujících veřejné služby nebo fyzických osob), existence alternativních zdrojů vody pro pokrytí téže zeměpisné oblasti

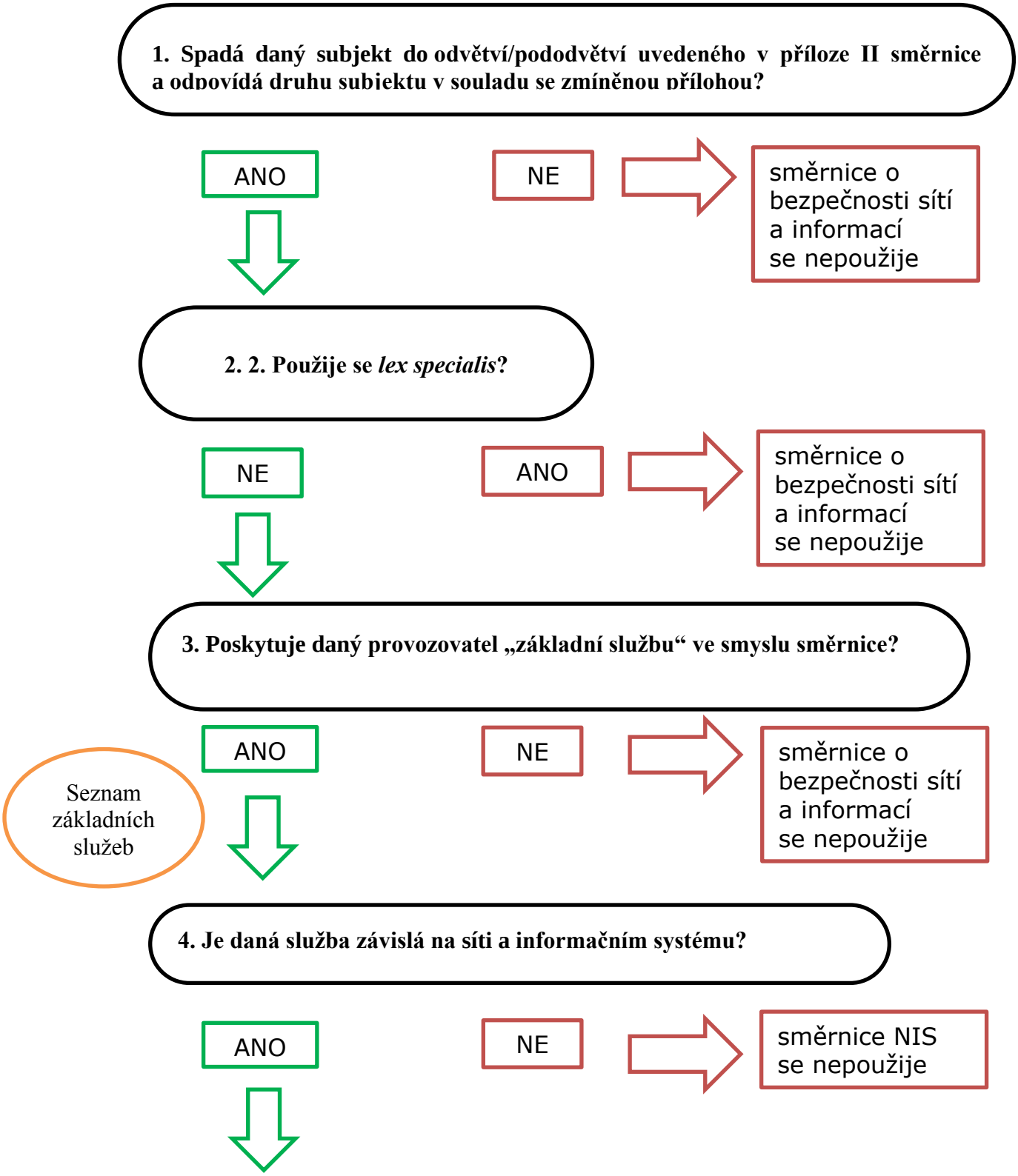
Je třeba upřesnit, že členské státy by při posuzování podle čl. 5 odst. 2 neměly přidávat další kritéria kromě těch, která jsou uvedena ve zmiňovaném ustanovení, neboť by se mohl omezit počet určených provozovatelů základních služeb a mohla by být ohrožena minimální harmonizace na úrovni provozovatelů základních služeb zakotvená v článku 3 směrnice.

Šestý krok – **Poskytuje dotčený provozovatel základní služby v jiných členských státech?**

Šestý krok se týká případů, kdy provozovatel poskytuje základní služby ve dvou či více členských státech. Podle čl. 5 odst. 4 musí dotčené členské státy zahájit konzultace[31], a to před ukončením postupu určování.

[31] Postup konzultací je podrobněji popsán v bodě 4.1.7.

Obrázek 4: Postup určování v šesti krocích



5. Vedl by bezpečnostní incident k významnému narušení?

Okolnosti působící napříč odvětvími (čl. 6 odst. 1)

- **Počet uživatelů**, kteří jsou závislí na daných službách
- **Závislost** dalších zásadních odvětví na dané službě
- Možný dopad incidentů na **ekonomické a společenské činnosti** nebo **na veřejnou bezpečnost**
- Možný **zeměpisný rozsah**
- Důležitost subjektu, pokud jde o udržování dostatečné **úrovně dané služby**

Okolnosti specifické pro jednotlivá odvětví (příklady uvedené v 28. bodě odůvodnění)

- **Energetika**: objem výroby elektrické energie na vnitrostátní úrovni nebo podíl na této výrobě
- **Doprava**: poměrný objem dopravy vzhledem k celkovému vnitrostátnímu objemu a počet operací za rok

ANO

NE

směrnice o bezpečnosti sítí a informací se nepoužije

6. Poskytuje dotčený provozovatel základní služby v jiných členských státech?

ANO

NE

směrnice o bezpečnosti sítí a informací se nepoužije

Povinné konzultace s dotčeným členským státem (státy)

Přijetí vnitrostátních opatření (např. seznam provozovatelů základních služeb, politická a právní opatření).

4.1.7 Postup přeshraničních konzultací

Pokud provozovatel poskytuje základní služby ve dvou či více členských státech, čl. 5 odst. 4 vyžaduje, aby tyto členské státy zahájily vzájemné konzultace, a to před ukončením postupu určování. Ty mají usnadnit hodnocení kritičnosti daného provozovatele z hlediska přeshraničního dopadu.

Kýženým výsledkem konzultací je, aby si zúčastněné vnitrostátní orgány vyměnily své názory a stanoviska a v ideálním případě dospěly v otázce určení daného provozovatele ke stejnému závěru. Směrnice o bezpečnosti sítí a informací však nebrání tomu, aby se závěry členských států, pokud jde o určení či neurčení daného subjektu jako provozovatele základních služeb, lišily. Ve 24. bodě odůvodnění je zmíněna možnost členských států požádat v této souvislosti o součinnost skupinu pro spolupráci.

Komise se domnívá, že by členské státy měly v těchto záležitostech usilovat o konsensus, aby nedošlo k situaci, kdy bude mít jedna společnost v různých členských státech odlišné právní postavení. Odchylky by měly být skutečně výjimečné – například když subjekt, který je v jednom členském státě určený jako provozovatel základních služeb, provádí v jiném členském státě pouze okrajové a nevýznamné činnosti.

4.2 Bezpečnostní požadavky

Podle čl. 14 odst. 1 musí členské státy zajistit, že provozovatelé základních služeb přijmou s ohledem na nejnovější technický vývoj vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, jež tyto organizace používají při poskytování svých služeb. V souladu s čl. 14 odst. 2 musí být přijata vhodná opatření k předcházení incidentům a minimalizaci jejich dopadů.

Zvláštní oblastí činnosti skupiny pro spolupráci je v současné době příprava nezávazných pokynů týkajících se bezpečnostních opatření pro provozovatele základních služeb[32]. Tyto pokyny by měla skupina dokončit v posledním čtvrtletí roku 2017. Komise vybízí členské státy, aby zmiňovaným pokynům vypracovaným skupinou pro spolupráci věnovaly řádnou pozornost, aby se zajistilo, že vnitrostátní předpisy o bezpečnostních požadavcích budou v co největším souladu. Harmonizace těchto požadavků by významným způsobem usnadnila dodržování povinností ze strany provozovatelů základních služeb, kteří často poskytují základní služby ve více než jednom členském státě, jakož i úlohu dohledu příslušných vnitrostátních orgánů a týmů CSIRT.

4.3 Požadavky na hlášení incidentů

Podle čl. 14 odst. 3 musí členské státy zajistit, aby provozovatelé základních služeb hlásili „*incidenty se závažným dopadem na kontinuitu základních služeb*“. To znamená, že by

[32] Pro tyto účely byly rozeslány seznamy mezinárodních norem, osvědčených postupů a metodik posouzení/řízení rizik pro všechna odvětví pokrytá směrnicí o bezpečnosti sítí a informací a byly použity jako vstup pro navrhované bezpečnostní domény a bezpečnostní opatření.

provozovatelé základních služeb neměli hlásit každý menší incident, ale pouze závažné incidenty s dopadem na kontinuitu základních služeb. Podle čl. 4 odst. 7 se incidentem rozumí „*jakákoliv událost, která má reálný negativní dopad na bezpečnost sítí a informačních systémů*“. „*Bezpečnost sítí a informačních systémů*“ je dále v čl. 4 odst. 2 definována jako „*schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné*“. To znamená, že jakákoli událost s negativním dopadem nejen na dostupnost, ale rovněž na autenticitu, integritu nebo důvěrnost dat nebo souvisejících služeb by mohla potenciálně aktivovat ohlašovací povinnost. Kontinuita služby ve smyslu čl. 14 odst. 3 může být skutečně ohrožena nejen v případech, které zasahují fyzickou dostupnost, ale i při jakémkoli jiném bezpečnostním incidentu, který ovlivňuje řádné poskytování uvedené služby[33].

Zvláštní oblastí činnosti skupiny pro spolupráci je v současné době příprava nezávazných pokynů pro hlášení týkajících se okolností, za nichž jsou provozovatelé základních služeb povinni hlásit incidenty v souladu s čl. 14 odst. 7, jakož i formátu a postupu hlášení na vnitrostátní úrovni. Tyto pokyny by měly být dokončeny do posledního čtvrtletí roku 2017.

Rozdílné vnitrostátní požadavky na hlášení incidentů mohou vést k právní nejistotě, složitějším a zdlouhavějším postupům a značným administrativním nákladům pro poskytovatele, kteří působí v přeshraničním styku. Komise proto tuto činnost skupiny pro spolupráci vítá. Stejně jako v případě bezpečnostních požadavků vybízí Komise členské státy, aby zmiňovaným pokynům vypracovaným skupinou pro spolupráci věnovaly řádnou pozornost, aby se zajistilo, že vnitrostátní předpisy o hlášení incidentů budou co nejvíce harmonizovány.

4.4 Směrnice o bezpečnosti sítí a informací, příloha III: Poskytovatelé digitálních služeb

Druhou kategorií subjektů spadajících do oblasti působnosti směrnice o bezpečnosti sítí a informací jsou poskytovatelé digitálních služeb. Považují se za významné hospodářské aktéry, neboť je využívají mnohé podniky při poskytování vlastních služeb a narušení určité digitální služby by mohlo mít dopad na klíčové ekonomické a společenské činnosti.

4.4.1 Kategorie poskytovatelů digitálních služeb

Definice digitálních služeb v čl. 4 odst. 5 odkazuje na právní definici uvedenou v čl. 1 odst. 1 písm. b) směrnice (EU) 2015/1535, jelikož zužuje rozsah druhů služeb uvedených na seznamu v příloze III. V čl. 1 odst. 1 písm. b) směrnice (EU) 2015/1535 jsou služby zejména definovány jako „*každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb*“ a v příloze III směrnice jsou uvedeny tři konkrétní druhy služeb: on-line tržiště, internetový vyhledávač a služba cloud computingu. Na rozdíl od provozovatelů základních služeb zde směrnice od členských států nevyžaduje, aby určily poskytovatele digitálních služeb, na něž by se následně vztahovaly příslušné povinnosti.

[33] Totéž platí pro poskytovatele digitálních služeb.

Příslušné povinnosti vyplývající ze směrnice, konkrétně bezpečnostní požadavky a požadavky na hlášení incidentů stanovené v článku 16, se budou vztahovat na všechny poskytovatele digitálních služeb v její oblasti působnosti.

Následující body dále vysvětlují uvedené tři druhy digitálních služeb, na které se směrnice vztahuje.

1. Poskytovatel služeb on-line tržiště

Prostřednictvím on-line tržiště může velký počet různých podniků provozovat své obchodní činnosti zaměřené na spotřebitele a navazovat mezipodnikové vztahy. On-line tržiště poskytuje společnostem základní infrastrukturu pro obchodování on-line a přes hranice. Poskytovatelé služeb on-line tržiště mají v ekonomice významnou úlohu zejména proto, že malým a středním podnikům poskytují přístup k většímu jednotnému digitální trhu EU. Jejich činnosti mohou zahrnovat i poskytování dálkových počítačových služeb k usnadnění hospodářské činnosti klienta včetně zpracování transakcí a shromažďování informací o kupujících, dodavatelích a produktech nebo usnadnění vyhledávání vhodných produktů, poskytování produktů, transakční odbornosti a vzájemného kontaktu kupujících a prodávajících.

Definice on-line tržiště je obsažena v čl. 4 odst. 17 a podrobněji vysvětlena v 15. bodě odůvodnění. Uvádí se, že se jedná o službu, jejímž prostřednictvím mohou spotřebitelé a obchodníci s konečnou platností uzavírat s obchodníky on-line smlouvy o prodeji nebo o poskytnutí služeb. Za on-line tržiště lze například považovat poskytovatele, jako je *eBay*, který na své platformě umožňuje obchodovat ostatním, kteří zde mohou své produkty a služby zpřístupnit spotřebitelům nebo podnikům on-line. Pod definici on-line tržiště spadají rovněž on-line obchody s aplikacemi zaměřené na distribuci aplikací a softwarových programů, neboť umožňují tvůrcům aplikací prodávat či distribuovat své služby spotřebitelům nebo jiným podnikům. Naopak, na zprostředkovatele služeb třetích stran, jako je *Skyscanner*, nebo služby pro porovnávání cen přesměrovávající uživatele na internetové stránky obchodníka, kde se uzavírá vlastní smlouva o poskytování služeb nebo o produktu, se definice podle čl. 4 odst. 17 nevztahuje.

2. Poskytovatel služeb internetového vyhledávače

Internetový vyhledávač je definován v čl. 4 odst. 18 a podrobněji vysvětlen v 16. bodě odůvodnění. Uvádí se, že se jedná o digitální službu, která uživatelům umožňuje provádět vyhledávání v zásadě na všech internetových stránkách nebo na internetových stránkách v určitém jazyce, a to na základě dotazu na jakékoli téma. Nejsou zahrnuty vyhledávací funkce, které se omezují na vyhledávání v rámci jedné internetové stránky nebo na stránky porovnávající ceny. Například druh vyhledávače, který je k dispozici na stránkách EUR LEX[34], nelze považovat za vyhledávač ve smyslu směrnice, a to vzhledem k tomu, že vyhledávací funkce je omezena pouze na obsah této konkrétní internetové stránky.

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

3. Poskytovatel služeb cloud computingu

V čl. 4 odst. 19 je služba cloud computingu definována jako „digitální služba umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které je možno sdílet“, přičemž v 17. bodě odůvodnění se blíže vysvětluje, co se rozumí pod pojmy výpočetní zdroje, rozšiřitelné a přizpůsobitelné úložiště.

V kostce lze cloud computing popsat jako určitý druh výpočetní služby, který používá společné zdroje pro zpracování údajů na požádání, přičemž sdílené zdroje zahrnují veškeré hardwarové či softwarové prvky (např. sítě, servery či jinou infrastrukturu, úložiště, aplikace a služby), které se na požádání poskytnou uživatelům pro účely zpracování dat. To, že je lze sdílet, znamená, že jde o výpočetní zdroje, kde mnoho uživatelů používá pro zpracování údajů stejnou fyzickou infrastrukturu. Výpočetní zdroj lze definovat jako výpočetní zdroj, který lze sdílet, pokud se soubor zdrojů, které využívá poskytovatel, může kdykoli rozšířit nebo zúžit v závislosti na potřebách uživatelů. Datová centra nebo jednotlivé prvky v rámci datového centra je pak možné připojit nebo odpojit, jestliže celkový objem výpočetní kapacity nebo kapacity úložiště vyžaduje aktualizaci. Koncept přizpůsobitelného úložiště lze popsat jako změny zatížení automatickým přidělováním a odebíráním zdrojů, takže zdroje dostupné v každém okamžiku v maximální možné míře odpovídají aktuální poptávce[35].

V současné době mohou poskytovatelé nabízet tři hlavní typy modelů cloudových služeb:

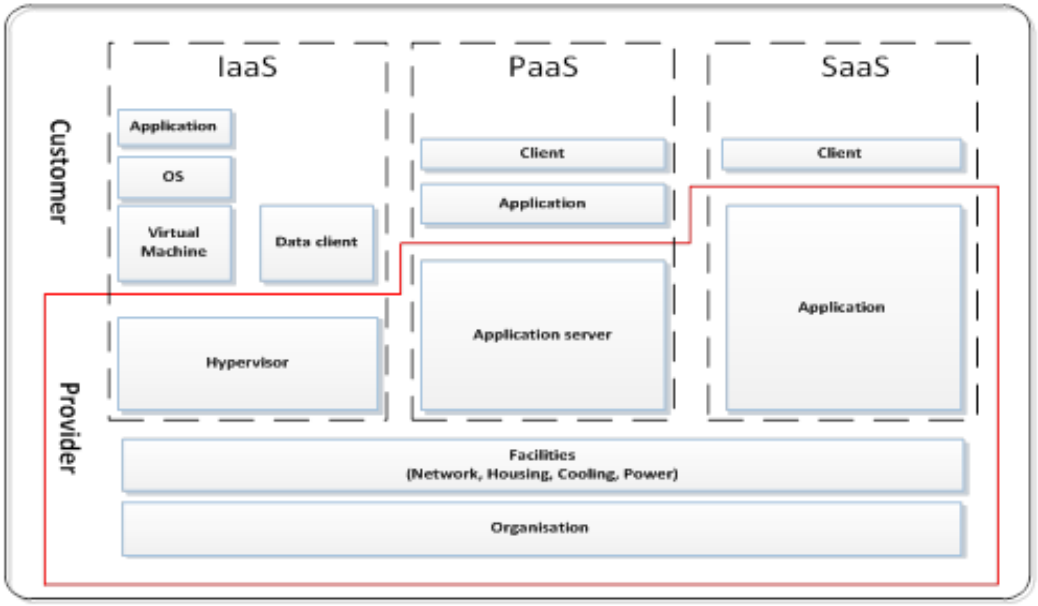
- Infrastruktura jako služba (IaaS): Kategorie cloudové služby, kdy cloudová kapacita poskytovaná zákazníkovi má podobu infrastruktury. Zahrnuje virtuální poskytování výpočetních zdrojů v podobě hardwaru, síťové služby a služby úložiště. Infrastruktura jako služba provozuje servery, úložiště, sítě a operační systémy. Zajišťuje podnikovou infrastrukturu, v níž si podnik může ukládat data a provozovat aplikace nezbytné pro jeho každodenní provoz.

- Platforma jako služba (PaaS): Kategorie cloudové služby, kdy cloudová kapacita poskytovaná zákazníkovi má podobu platformy. Zahrnuje on-line výpočetní platformy, které společnostem umožňují provozovat stávající aplikace nebo vyvinout a vyzkoušet nové.

- Software jako služba (SaaS): Kategorie cloudové služby, kdy cloudová kapacita poskytovaná zákazníkovi má podobu aplikace nebo softwaru nasazovaných přes internet. U tohoto typu cloudových služeb není koncový uživatel nucen kupovat si, instalovat a spravovat software, přičemž dalším výhodou je, že software je přístupný odkudkoliv, kde je internetové připojení.

[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 není), k dispozici na adrese: https://sdqweb.ipd.kit.edu/publications/pdfs/HeKoRe2013-ICAC-Elasticity.pdf. Viz rovněž strany 2–5 dokumentu COM(2012) 529.

Obrázek 5: Modely služeb a prostředky cloud computingu



Agentura ENISA poskytla komplexní pokyny, které se týkají konkrétních témat v oblasti cloud computingu[36], jakož i příručku s úvodem do této problematiky[37].

4.4.2 Bezpečnostní požadavky

Podle čl. 16 odst. 1 musí členské státy zajistit, aby poskytovatelé digitálních služeb přijaly vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systémy, které tyto společnosti využívají při poskytování svých služeb. Tato bezpečnostní opatření by měla zohlednit nejnovější technický vývoj a těchto pět prvků: i) bezpečnost systémů a zařízení; ii) řešení incidentů; iii) řízení kontinuity provozu; iv) monitorování, audity a testování; v) soulad s mezinárodními normami.

V této souvislosti je Komise na základě čl. 16 odst. 8 zmocněna přijímat prováděcí akty, kterými blíže upřesní uvedené prvky a zajistí vysokou úroveň harmonizace, pokud jde o poskytovatele těchto služeb. Očekává se, že Komise přijme příslušný prováděcí akt na podzim roku 2017. Členské státy musí rovněž zajistit, že poskytovatelé digitálních služeb přijmou nezbytná opatření k předcházení incidentům a k minimalizaci jejich dopadu s cílem zajistit kontinuitu svých služeb.

4.4.3 Požadavky na hlášení incidentů

Poskytovatelé digitálních služeb by měli mít povinnost hlásit závažné incidenty příslušným orgánům nebo týmům CSIRT. V souladu s čl. 16 odst. 3 směrnice o bezpečnosti sítí a informací se ohlašovací povinnost pro poskytovatele digitálních služeb aktivuje v případech, kdy má incident významný dopad na poskytování dané služby. Pro určení závažnosti dopadu

[36] K dispozici na adrese: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security
[37] ENISA, *Cloud Security Guide for SMEs* (Průvodce bezpečnosti cloud computingu pro malé a střední podniky, 2015). K dispozici na adrese: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

je v čl. 16 odst. 4 uvedeno pět konkrétních parametrů, které musí poskytovatelé digitálních služeb zohlednit. V této souvislosti je Komise na základě čl. 16 odst. 8 zmocněna přijmout prováděcí akty, v nichž tyto parametry podrobněji popíše. Bližší vymezení těchto parametrů bude součástí prováděcího aktu, kterým se stanoví bezpečnostní prvky zmíněné v bodě 4.4.2 a který se Komise chystá na podzim přijmout.

4.4.4 Regulační přístup založený na rizicích

V článku 17 se stanoví, že poskytovatelé digitálních služeb podléhají dohledu příslušných vnitrostátních orgánů formou následných kontrol. Členské státy musí zajistit, že příslušné orgány přijmou opatření, pokud mají k dispozici důkazy, že poskytovatel digitálních služeb nesplňuje požadavky stanovené v článku 16 směrnice.

Kromě toho je Komise na základě čl. 16 odst. 8 a 9 zmocněna přijímat prováděcí akty v souvislosti s bezpečnostními požadavky a požadavky na hlášení incidentů, což posílí harmonizaci na úrovni poskytovatelů digitálních služeb. Kromě toho se v čl. 16 odst. 10 stanoví, že členské státy nesmějí ukládat poskytovateli digitálních služeb žádné další bezpečnostní požadavky nebo požadavky na hlášení incidentů nad rámec těch, které jsou stanoveny v této směrnici, s výjimkou případů, kdy jsou tato opatření nezbytná k zabezpečení jejich základních státních funkcí – zejména pokud jde o zajištění národní bezpečnosti – a k umožnění vyšetřování, odhalování a stíhání trestných činů.

A konečně, vzhledem k přeshraniční povaze poskytovatelů digitálních služeb směrnice neuplatňuje model souběžné vícenásobné pravomoci, ale přístup vycházející z kritéria primárního usazení společnosti v EU[38]. Tento přístup umožňuje, aby se na poskytovatele digitálních služeb uplatnil jeden soubor pravidel s jedním příslušným orgánem odpovědným za dohled, což je zvláště důležité, neboť mnoho poskytovatelů digitálních služeb nabízí své služby v mnoha členských státech současně. Uplatnění tohoto přístupu minimalizuje zátěž poskytovatelů digitálních služeb spojenou s dodržováním předpisů a zajišťuje řádné fungování jednotného digitálního trhu.

4.4.5 Pravomoc

Jak již bylo uvedeno, podle čl. 18 odst. 1 směrnice o bezpečnosti sítí a informací podléhá poskytovatel digitálních služeb pravomoci členského státu, v němž má svou hlavní provozovnu. Pokud daný poskytovatel digitálních služeb nabízí služby v EU, ale není na jejím území usazen, pak mu čl. 18 odst. 2 ukládá povinnost, aby v Unii určil svého zástupce. V takovém případě podléhá společnost pravomoci členského státu, v němž je usazen její zástupce. Pokud poskytovatel digitálních služeb poskytuje služby v určitém členském státě, ale neurčil v EU svého zástupce, členský stát může v zásadě proti tomuto poskytovateli digitálních služeb přijmout opatření, neboť porušuje povinnosti, které pro něj ze směrnice vyplývají.

[38] Viz zejména článek 18 směrnice.

4.4.6 Osvobození malých poskytovatelů digitálních služeb od bezpečnostních požadavků a požadavků na hlášení incidentů

V čl. 16 odst. 11 se uvádí, že na poskytovatele digitálních služeb, kteří jsou mikropodniky nebo malými podniky ve smyslu doporučení Komise 2003/361/ES39, se nevztahují bezpečnostní požadavky a požadavky na hlášení incidentů podle článku 16. Znamená to tedy, že podniky, které zaměstnávají méně než 50 osob a jejichž roční obrat a/nebo bilanční suma roční rozvahy nepřekračuje 10 milionů EUR, nejsou těmito požadavky vázány. Při určování velikosti subjektu nehraje roli, zda dotčená společnost poskytuje pouze digitální služby ve smyslu směrnice o bezpečnosti sítí a informací, nebo i jiné služby.

5. Vztah mezi směrnicí o bezpečnosti sítí a informací a jinými právními předpisy

Tento bod se zaměřuje na ustanovení o *lex specialis* v čl. 1 odst. 7 směrnice o bezpečnosti sítí a informací a uvádí tři příklady *lex specialis*, které Komise dosud posuzovala a objasňuje bezpečnostní požadavky a požadavky na hlášení incidentů uplatňované pro poskytovatele telekomunikačních služeb a služeb vytvářejících důvěru.

5.1 Směrnice o bezpečnosti sítí a informací, čl. 1 odst. 7: Ustanovení *lex specialis*

V souladu s čl. 1 odst. 7 směrnice o bezpečnosti sítí a informací se ustanovení o bezpečnostních požadavcích a/nebo požadavcích na hlášení ve vztahu k poskytovatelům digitálních služeb nebo provozovatelům základních služeb nepoužijí, pokud existuje odvětvový předpis EU, který stanoví bezpečnostní požadavky a/nebo požadavky na hlášení s účinkem přinejmenším ekvivalentním účinku povinností stanovených uvedenou směrnicí. Členské státy musí čl. 1 odst. 7 zohlednit při celkovém provádění směrnice a informovat Komisi o uplatnění ustanovení *lex specialis*.

Metodika

Při posuzování rovnocennosti odvětvového právního předpisu EU s příslušnými ustanoveními směrnice o bezpečnosti sítí a informací je třeba se zejména zaměřit na otázku, zda bezpečnostní povinnosti daného odvětvového právního předpisu zahrnují opatření, která zajistí bezpečnost sítí a informačních systémů definovanou v čl. 4 odst. 2 směrnice.

Pokud jde o požadavky na hlášení, v čl. 14 odst. 3 a čl. 16 odst. 3 směrnice o bezpečnosti sítí a informací se stanoví, že provozovatelé základních služeb a poskytovatelé digitálních služeb musí příslušným orgánům nebo týmům CSIRT neprodleně ohlásit každý incident s významným/podstatným dopadem na poskytování dané služby. Je třeba věnovat zvláštní pozornost povinnosti provozovatele/poskytovatele digitálních služeb zahrnout do hlášení informace, které příslušnému orgánu nebo týmu CSIRT umožní určit případný přeshraniční dopad daného bezpečnostního incidentu.

[39] Úř. věst. L 24, 20.5.2003, s. 36.

V současné době neexistují pro kategorii poskytovatelů digitálních služeb žádné odvětvové právní předpisy, které by upravovaly bezpečnostní požadavky a požadavky na hlášení incidentů srovnatelné s požadavky článku 16 směrnice o bezpečnosti sítí a informací a které by bylo možné zohlednit při uplatňování čl. 1 odst. 7 uvedené směrnice[40].

Pokud jde o provozovatele základních služeb, bezpečnostní požadavky a/nebo požadavky na hlášení vyplývající z odvětvových právních předpisů EU se v současné době vztahují na finanční sektor, zejména pak na odvětví bankovnictví a infrastruktury finančního trhu, které jsou uvedeny v bodech 3 a 4 přílohy II. Důvodem je skutečnost, že bezpečnost a dobrý stav informačních technologií, sítí a informačních systémů používaných ve finančních institucích je nezbytnou součástí požadavků na krytí operačního rizika, které finančním institucím ukládají právní předpisy EU.

Příklady

i) druhá směrnice o platebních službách

Pokud jde o bankovní odvětví a zejména v souvislosti s poskytováním platebních služeb úvěrovými institucemi definovanými v čl. 4 odst. 1 bodu 1 nařízení (EU) č. 575/2013, takzvaná druhá směrnice o platebních službách[41] stanoví požadavky na bezpečnost a hlášení incidentů, které jsou uvedeny v článcích 95 a 96 zmíněné směrnice.

Konkrétně čl. 95 odst. 1 uvedené směrnice vyžaduje, aby poskytovatelé platebních služeb zavedli příslušná opatření ke zmírnění rizik a kontrolní mechanismy, které umožní řídit operační a bezpečnostní rizika související s platebními službami, které poskytují. Tato opatření by měla zahrnovat stanovení a zachovávání účinných postupů pro řešení incidentů, včetně postupů pro odhalování a klasifikaci závažných operačních a bezpečnostních incidentů. V 95. a 96. bodu odůvodnění druhé směrnice o platebních službách je dále objasněna povaha těchto bezpečnostních opatření. Z uvedených ustanovení vyplývá, že cílem stanovených opatření je řídit bezpečnostní rizika spojená se sítěmi a informačními systémy, které jsou využívány při poskytování platebních služeb. Uvedené bezpečnostní požadavky tedy lze z hlediska účinku považovat za alespoň rovnocenné odpovídajícím ustanovením čl. 14 odst. 1 a 2 směrnice o bezpečnosti sítí a informací.

Pokud jde o požadavky týkající se oznamování, čl. 96 odst. 1 druhé směrnice o platebních službách stanoví povinnost poskytovatelů platebních služeb oznámit příslušnému orgánu bez zbytečného odkladu významné operační nebo bezpečnostní incidenty. Srovnatelně s čl. 14 odst. 5 směrnice o bezpečnosti sítí a informací pak čl. 96 odst. 2 druhé směrnice o platebních službách vyžaduje, aby příslušný orgán informoval příslušné orgány ostatních členských států, pokud je pro ně incident relevantní. Tato povinnost současně předpokládá, že oznámení bezpečnostních incidentů musí obsahovat informace, které těmto orgánům umožní posoudit

[40] Tím není dotčeno ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu podle článku 33 obecného nařízení o ochraně údajů.
[41] Směrnice (EU) 2015/2366, Úř. věst. L 337, 23.12.2015, s. 35.

přeshraniční dopad daného incidentu. V čl. 96 odst. 3 písm. a) druhé směrnice o platebních službách se EBA svěřuje pravomoc vypracovat ve spolupráci s ECB pokyny o přesném obsahu a formátu oznámení.

Lze tedy konstatovat, že podle čl. 1 odst. 7 směrnice o bezpečnosti sítí a informací by se měly použít požadavky týkající se bezpečnosti a oznamování stanovené v článcích 95 a 96 druhé směrnice o platebních službách místo odpovídajících ustanovení článku 14 směrnice o bezpečnosti sítí a informací, pokud jde o poskytování platebních služeb dotčenými úvěrovými institucemi.

ii) nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů

Pokud jde o infrastrukturu finančního trhu, nařízení (EU) č. 648/2012 ve spojení s nařízením Komise v přenesené pravomoci (EU) č. 153/2013 obsahuje ustanovení o bezpečnostních požadavcích na ústřední protistrany, která lze považovat za *lex specialis*. Tyto právní akty zejména stanoví technická a organizační opatření týkající se bezpečnosti sítí a informačních systémů, které mírou podrobnosti dokonce překračují požadavky čl. 14 odst. 1 a 2 směrnice o bezpečnosti sítí a informací, a lze je tedy považovat za splňující požadavky čl. 1 odst. 7 uvedené směrnice, pokud jde o bezpečnostní požadavky.

Ustanovení čl. 26 odst. 1 nařízení (EU) č. 648/2012 konkrétně uvádí, že subjekt by měl mít „*spolehlivé řídicí systémy včetně jasné organizační struktury s dobře vymezenými, transparentními a konzistentními hranicemi odpovědnosti, účinné postupy k zjišťování, řízení, kontrole a oznamování rizik, kterým je nebo by mohla být vystavena, a přiměřené mechanismy vnitřní kontroly včetně řádných administrativních a účetních postupů*.“ Ustanovení čl. 26 odst. 3 vyžaduje, aby organizační struktura zajišťovala nepřetržitý a řádný výkon služeb a činností využíváním vhodných a přiměřených systémů, zdrojů a postupů.

Ustanovení čl. 26 odst. 6 dále objasňuje, že ústřední protistrana musí udržovat „*informační systémy odpovídající složitosti, rozmanitosti a typům vykonávaných služeb a činností tak, aby byly zajištěny vysoké bezpečnostní standardy a neporušenost a důvěrnost uchovávaných informací*.“ Ustanovení čl. 34 odst. 1 dále ukládá povinnost zavést, provádět a udržovat vhodnou politiku pro zachování provozu a plán obnovy činnosti, která by měla zajistit včasné obnovení operací.

Tyto povinnosti jsou dále upřesněny v nařízení Komise v přenesené pravomoci (EU) č. 153/2013 ze dne 19. prosince 2012, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) č. 648/2012, pokud jde o regulační technické normy týkající se požadavků na ústřední protistrany[42]. Zejména jeho článek 4 ukládá ústředním protistranám povinnost vypracovat odpovídající nástroje pro řízení rizik, které by umožnily zvládat všechna příslušná rizika a podávat o nich zprávy, a dále upřesňuje druhy opatření (např.: zavedení spolehlivých informačních systémů a systémů řízení rizika, dostupnost zdrojů, odborností a přístupu ke všem potřebným informacím pro útvar řízení rizik, dostupnost adekvátních interních

[42] Úř. věst. L 52, 23.2.2013, s. 41.

kontrolních mechanismů, jako jsou například řádné správní a účetní postupy, které radě ústřední protistrany pomáhají při monitorování a posuzování adekvátnosti a účinnosti jejích strategií, postupu a systémů řízení rizik).

Kromě toho článek 9 výslovně zmiňuje bezpečnost systémů informačních technologií a stanoví konkrétní technická a organizační opatření související s udržováním spolehlivého rámce pro ochranu informací pro řízení rizik v oblasti bezpečnosti IT. Tato opatření by měla zahrnovat mechanismy a postupy zajišťující dostupnost služeb a ochranu pravosti, celistvosti a důvěrnosti údajů.

iii) směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU[43]

Pokud jde o obchodní systémy, čl. 48 odst. 1 směrnice 2014/65/EU vyžaduje, aby provozovatelé zajistili v případě jakéhokoli selhání jejich obchodních systémů kontinuitu svých služeb. Tato obecná povinnost byla nedávno dále upřesněna a doplněna nařízením Komise v přenesené pravomoci (EU) 2017/584[44] ze dne 14. července 2016, kterým se doplňuje směrnice Evropského parlamentu a Rady 2014/65/EU, pokud jde o regulační technické normy upřesňující organizační požadavky na obchodní systémy[45]. Zejména čl. 23 odst. 1 uvedeného nařízení stanoví, že obchodní systémy zavedou postupy a opatření k zajištění fyzické a elektronické bezpečnosti koncipované tak, aby své systémy chránily před zneužitím nebo neoprávněným přístupem a zajistily integritu údajů. Tato opatření by měla umožnit předcházet riziku útoků na informační systémy nebo toto riziko minimalizovat.

Ustanovení čl. 23 odst. 2 dále vyžaduje, aby tato opatření přijatá provozovateli umožňovala bezodkladně zjistit a řídit rizika týkající se jakéhokoli neoprávněného přístupu, zasahování do systémů, které závažně narušuje nebo přerušuje fungování informačních systémů, a zasahování do údajů, které narušuje dostupnost, integritu nebo pravost údajů. Kromě toho článek 15 uvedeného nařízení ukládá obchodním systémům povinnost mít zavedeny účinné mechanismy kontinuity činnosti k zajištění dostatečné stability systému a k řešení událostí narušujících jejich činnost. Zejména by tato opatření měla provozovateli umožnit obnovit obchodování do dvou nebo přibližně do dvou hodin, a zároveň by měla zajistit, aby se objem údajů, k jejichž ztrátě dojde, blížil nule.

Článek 16 dále uvádí, že určená opatření k řešení a zvládání událostí narušujících činnost by měla být součástí plánu kontinuity činnosti obchodních systémů, a stanoví konkrétní prvky, které musí provozovatel při přijímání plánu kontinuity činnosti zvážit (např. zřízení zvláštního bezpečnostního týmu, provedení posouzení dopadu k určení rizik, které se pravidelně přezkoumává).

Vzhledem k obsahu těchto bezpečnostních opatření je zřejmé, že jsou určena k řízení a řešení rizika souvisejícího s dostupností, pravostí, integritou a důvěrností údajů nebo poskytovaných

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

služeb, a v důsledku toho lze konstatovat, že výše uvedené odvětvové právní předpisy EU obsahují povinnosti v oblasti bezpečnosti, které jsou co do účinku přinejmenším rovnocenné odpovídajícím povinnostem stanoveným v čl. 14 odst. 1 a 2 směrnice o bezpečnosti sítí a informací.

5.2 Směrnice o bezpečnosti sítí a informací, čl. 1 odst. 3: poskytovatelé telekomunikačních služeb a poskytovatelé služeb vytvářejících důvěru

Podle čl. 1 odst. 3 se bezpečnostní požadavky a požadavky na hlášení incidentů stanovené uvedenou směrnicí nevztahují na poskytovatele podléhající požadavkům stanoveným v článcích 13a a 13b směrnice 2002/21/ES. Články 13a a 13b směrnice 2002/21/ES se vztahují na podniky zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací. V důsledku toho musí podnik, pokud jde o zajišťování veřejných komunikačních sítí nebo poskytování veřejně dostupných služeb elektronických komunikací, dodržovat požadavky na bezpečnost a oznamování stanovené ve směrnici 2002/21/ES.

Pokud však týž podnik také poskytuje další služby, jako jsou digitální služby (např. cloud computing nebo on-line tržiště) uvedené v příloze III směrnice o bezpečnosti sítí a informací nebo služby, jako jsou systémy doménových jmen (DNS) nebo výměnné uzly internetu (IXP) podle přílohy II bodu 7 směrnice o bezpečnosti sítí a informací, budou se na podnik vztahovat požadavky na bezpečnost a hlášení stanovené směrnicí o bezpečnosti sítí a informací pro poskytování těchto konkrétních služeb. Je třeba poznamenat, že vzhledem k tomu, že poskytovatelé služeb uvedených v příloze II bodu 7 patří do kategorie provozovatelů základních služeb, jsou členské státy povinny provést proces určení podle čl. 5 odst. 2 a musí určit, kteří jednotliví poskytovatele služeb DNS, IXP nebo registrů internetových domén nejvyšší úrovně (TLD) by měli splňovat požadavky směrnice o bezpečnosti sítí a informací. To znamená, že po takovém posouzení budou mít povinnost splňovat požadavky směrnice o bezpečnosti sítí a informací pouze ti poskytovatelé služeb DNS, IXP nebo TLD, kteří splňují kritéria čl. 5 odst. 2 směrnice o bezpečnosti sítí a informací.

Ustanovení čl. 1 odst. 3 dále uvádí, že bezpečnostní požadavky a požadavky na hlášení incidentů se rovněž nevztahují na poskytovatele služeb vytvářejících důvěru podléhající požadavkům stanoveným v článku 19 nařízení (EU) č. 910/2014.

6. Zveřejněné dokumenty o národních strategiích kybernetické bezpečnosti

	Členský stát	Název strategie a dostupné odkazy
1	Rakousko	*Austrian Cybersecurity Strategy (Rakouská strategie kybernetické bezpečnosti)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf (EN)
2	Belgie	*Securing Cyberspace (Zabezpečení kybernetického prostoru)* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/ncss-be-fr (FR)
3	Bulharsko	*Cyber Resilient Bulgaria 2020 (Kyberneticky bezpečné Bulharsko 2020)* (2016) http://www.cyberbg.eu/ (BG)
4	Chorvatsko	*The national cyber security strategy of the republic of Croatia (Národní strategie kybernetické bezpečnosti Chorvatské republiky)*(2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (EN)
5	Česká republika	*National cyber security strategy of the Czech Republic for the period from 2015 to 2020 (Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020)*(2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf (EN)
6	Kypr	*Cybersecurity Strategy of the Republic of Cyprus (Strategie kybernetické bezpečnosti Kyperské republiky)* (2012) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (EN)
7	Dánsko	*The Danish Cyber and Information Security Strategy (Dánská strategie kybernetické bezpečnosti a bezpečnosti informací)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/DK_NCSS.pdf (EN)
8	Estonsko	*Cyber Security Strategy (Strategie kybernetické bezpečnosti)* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf (EN)
9	Finsko	*Finland´s Cyber security Strategy (Strategie kybernetické bezpečnosti Finska)* (2013)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf (EN)
10	Francie	*French national digital security strategy (Francouzská národní strategie digitální bezpečnosti)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf (EN)
11	Irsko	*National Cyber Security Strategy 2015-2017 (Národní strategie kybernetické bezpečnosti na období 2015–2017)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf (EN)
12	Itálie	*National Strategic Framework for Cyberspace Security (Národní strategický rámec pro bezpečnost kybernetického prostoru)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf (EN)
13	Německo	*Cyber-Sicherheitsstrategie für Deutschland (Strategie kybernetické bezpečnosti pro Německo)* (2016) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/ModerneVerwaltung-OeffentlicherDienst/Informationsgesellschaft/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile (DE)
14	Maďarsko	*National Cyber Security Strategy of Hungary (Národní strategie kybernetické bezpečnosti Maďarska)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf (EN)
15	Lotyšsko	*Cyber Security Strategy of Latvia 2014–2018 (Strategie kybernetické bezpečnosti Lotyšska na období 2014–2018)* (2014) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss (EN)
16	Litva	*The programme for the development of electronic information security (cyber-security) for 2011–2019 (Program pro rozvoj bezpečnosti elektronických informací (kybernetické bezpečnosti) na období 2011–2019)* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf (EN)
17	Lucembursko	*National Cybersecurity Strategy II (Národní strategie kybernetické bezpečnosti II) (2015)* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf (EN)
18	Malta	*National Cyber Security Strategy Green Paper (Národní strategie kybernetické bezpečnosti – zelená kniha)* (2015)

		https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (EN)
19	Nizozemsko	*National Cyber Security Strategy 2 (Národní strategie kybernetické bezpečnosti 2)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf (EN)
20	Polsko	*Cyberspace Protection Policy of the Republic of Poland (Politika ochrany kyberprostoru Polské republiky)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf (EN)
21	Rumunsko	*Strategiei de securitate cibernetică a României (Strategie kybernetické bezpečnosti v Rumunsku)* (2011) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (RO)
22	Portugalsko	*National Cyberspace Security Strategy (Národní strategie bezpečnosti kybernetického prostoru)* (2015) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/portuguese-national-cyber-security-strategy/view (EN)
23	Slovenská republika	*Cyber Security Concept of the Slovak Republic for 2015 – 2020 (Koncepce kybernetické bezpečnosti Slovenské republiky na období 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	*Cyber Security Strategy establishing a system to ensure a high level of cyber security (Strategie kybernetické bezpečnosti, kterou se zřizuje systém pro zajištění vysoké úrovně kybernetické bezpečnosti)* (2016) http://www.uvtp.gov.si/fileadmin/uvtp.gov.si/pageuploads/Cyber_Security_Strategy_Slovenia.pdf (EN)
25	Španělsko	*National Cyber Security Strategy (Národní strategie kybernetické bezpečnosti)* (2013) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf (EN)
26	Švédsko	*The Swedish National Cybersecurity Strategy (Švédská národní strategie kybernetické bezpečnosti)* (2017) http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf (EN)
27	Spojené	*National Cyber Security Strategy (2016-2021) (Národní strategie*

království	*kybernetické bezpečnosti (2016-2021))* (2016) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf (EN)

7. Seznam osvědčených postupů a doporučení vydaných agenturou ENISA

Ohledně reakce na incidenty

- ✓ Strategies for incident response and cyber crisis cooperation (Strategie reakce na incidenty a spolupráce v případě kybernetické krize)[46]

Ohledně řešení incidentů

- ✓ Incident handling automation project (Projekt automatizace řešení incidentů)[47]
- ✓ Good Practice Guide for Incident Management (Příručka osvědčených postupů pro řešení incidentů)[48]

Pro klasifikaci a taxonomii incidentů

- ✓ Overview of existing taxonomies (Přehled stávajících taxonomií)[49]
- ✓ Good practice guide of using taxonomies in incident prevention and detection (Příručka osvědčených postupů pro používání taxonomie v prevenci a odhalování incidentů)[50]

Ohledně vyspělosti CSIRT

- ✓ Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity (Výzvy pro vnitrostátní týmy CSIRT v Evropě v roce 2016: studie o vyspělosti CSIRT)[51]
- ✓ Study on CSIRT Maturity – Evaluation Process (Studie o vyspělosti CSIRT – proces hodnocení)[52]
- ✓ Guidelines for national and governmental CSIRTs on how to assess maturity (Pokyny pro vnitrostátní a vládní týmy CSIRT k hodnocení vyspělosti)[53]

Ohledně budování kapacit CSIRT a odborné přípravě

- ✓ Good Practice Guide on Training Methodologies (Příručka osvědčených postupů týkajících se metodiky odborné přípravy)[54]

Hledání informací o stávajících týmech CSIRT v Evropě – přehled týmů CSIRT podle zemí[55]

---

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

[47] Další informace: https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation

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

[49] Další informace: 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 dispozici 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 dispozici na adrese:https://www.enisa.europa.eu/publications/study-on-csirt-maturity

[52] ENISA, *Study on CSIRT Maturity – Evaluation Process* (2017). K dispozici 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 dispozici na adrese: https://www.enisa.europa.eu/publications/csirt-capabilities

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

[55] Další informace: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map