ZVLÁŠTNÍ ČÁST

K čl. I

Změna zákona o kybernetické bezpečnosti

1. **K § 1 odst. 2**

V souladu s čl. 48 odst. 3 Legislativních pravidel vlády se do zákona zavádí odkaz na směrnici. Tato úprava je transpoziční k čl. 25 odst. 1 směrnice. Je zapotřebí konstatovat, že termín „zajišťování bezpečnosti sítí a informačních systémů“ je věcně zahrnut v terminu „zajišťování kybernetické bezpečnosti“.

2. **K § 2 písm. c)**

Ustanovení doplňuje a zpřesňuje již existující definici bezpečnosti informací, která s ohledem na definice ve směrnici (čl. 4 odst. 2) zahrnuje i autenticitu informací, resp. údajů.

3. **K § 2 písm. d)**

Navrhovaná úprava ustanovení písmene d) výslovně stanoví, že významný informační systém není totožný s informačním systémem základní služby, jak je dále definován zákonem. Tato úprava odpovídá systematice zákona o kybernetické bezpečnosti, který rozlišuje mezi informačním systémem a komunikačním systémem kritické informační infrastruktury, významným informačním systémem a informačním systémem základní služby (dále také „informační systém ZS“) a spolu s nimi mezi adresáty zákonných povinností, tedy správci a provozovateli informačního systému základní služby a provozovateli základních služeb.

4. **K § 2 písm. f)**

Jedná se o legislativně technickou úpravu vyplývající z potřeby doplnit do § 2 nová písmena h) až m).

5. **K § 2 písm. h) až m)**

Ustanovení transponuje do českého právního řádu čl. 4 směrnice, který definuje pojmy dále ve směrnici používané. Návrh zákona neobsahuje všechny definice ze směrnice, neboť některé z nich bude zapotřebí definovat až v prováděcím právním předpise. Předložený návrh zákona v případě, že některý z definičních termínů je již v českém právním řádu upraven, nevytváří novou definici, ale prostřednictvím poznámky pod čarou odkazuje na již existující pojem.

Jeden z nových významných termínů pro budoucí aplikaci zákona „základní služba“ je v tomto ustanovení definována za použití základních definičních znaků, které tato služba musí splňovat, a vymezení odvětví tak, aby NBÚ mohl následně za použití podrobných kritérií stanovených prováděcím právním předpisem určit provozovatele základní služby. Taxativně stanovená odvětví vychází jak z Přílohy II směrnice, tak i z praktických zkušeností NBÚ. Význam základních služeb je pak vnímán obdobně významu služeb, jež jsou závislé na komunikačních nebo informačních systémech kritické komunikační infrastruktury.

Předkladatel nepovažoval za nutné definovat podstatu služby internetového vyhledávače, neboť má za to, že se jedná o termín běžně používaný. Lze uvést klasické provozovatele služby internetového vyhledávače, jako je například www.seznam.cz nebo www.google.com. Předkladatel však pokládá za

podstatné zdůraznit, že v souladu se směrnicí se za vyhledávač nepovažuje vyhledávání v rámci jedné konkrétní internetové stránky, obvykle nabízené pod ikonkou lupy, či textového odkazu na vyhledávání.

Definice on-line tržiště je ve směrnici odlišná (širší), než jak je tento pojem vymezen v nařízení o řešení spotřebitelských sporů on-line a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (nařízení o řešení spotřebitelských sporů on-line), které v čl. 4 písm. f) definuje internetové tržiště („online marketplace“) jako službu „umožňující spotřebitelům a obchodníkům uzavírat kupní smlouvy nebo smlouvy o poskytování služeb uzavírané on-line, na obchodníkových stránkách“, ačkoliv další definiční znaky pojmu on-line tržiště (obchodník a spotřebitel) jsou totožné, neboť obě směrnice u těchto pojmů odkazují na směrnici 2013/11/EU o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů).

Za službu on-line tržiště pak nelze pokládat on-line služby, jež poskytují srovnání cen konkrétních produktů či služeb různých obchodníků, aby poté uživatele přesměrovaly k nákupu u zvoleného obchodníka (recitál 16 směrnice). V českém internetovém prostoru jde například o stránky www.heureka.cz.

Povinnosti poskytovatelů digitálních služeb, které se do zákona zavádějí touto novelou, se v souladu s čl. 16 odst. 11 směrnice nevztahují na mikropodniky a malé podniky, jak jsou definovány doporučením Komise o definici mikropodniků, malých a středních podniků. Toto negativní vymezení povinností, jež nově dopadají na poskytovatele digitálních služeb, zajišťuje proporcionalitu směrnice.

Ve smyslu přílohy doporučení, na kterou je v poznámce pod čarou odkazováno, je mikropodnikem (někdy je označován jako drobný podnik) podnik, který zaměstnává méně než 10 zaměstnanců a jeho roční obrat nebo bilanční suma roční rozvahy nepřesahuje ročně 2 mil. EUR. Malým podnikem je pak podnik, jenž zaměstnává méně než 50 zaměstnanců a roční obrat nebo bilanční suma roční rozvahy nepřesahuje ročně 10 mil. EUR. Vždy platí, že obě podmínky, jak personální, tak i finanční, musí být splněny kumulativně.

Směrnice ve svém čl. 1 odst. 2 písm. e) stanoví povinnost členských států určit vnitrostátní příslušné orgány pro zajištění řádné implementace směrnice. Předkladatel potřeboval za důležité vymezit věcnou působnost těchto příslušný orgánů jak s ohledem na působnost NBÚ, tak i vzhledem k přeshraniční spolupráci mezi příslušnými orgány, kterou směrnice taktéž upravuje.

6. K § 3 písm. d)

Legislativně technická úprava vyplývající z potřeby doplnit do § 3 nová písmena f) až h).

7. K § 3 písm. f) až h)

Do ustanovení § 3, který určuje subjekty (orgány a osoby), jimž zákon o kybernetické bezpečnosti ukládá povinnosti v oblasti kybernetické bezpečnosti, se na základě směrnice doplňují nové subjekty provozovatelé základních služeb, správci a provozovatelé informačního systému základní služby a poskytovatelé digitálních služeb. V případě, že provozovatelé základních služeb nejsou identičtí se správci nebo provozovateli informačních systémů základních služeb, vztahuje se plnění zákonných povinností především na správce a provozovatele informačních systémů základních služeb, a to

zejména proto, že právě oni mohou reálně zajišťovat bezpečnost informačního systémy základní služby, na nichž poskytování základní služby závisí.

8. K § 3a

V případě poskytovatelů digitálních služeb může, vzhledem k nehmotné povaze těchto služeb, snadno dojít k tomu, že dotčený podnikatel nemusí být usazen (mít sídlo) v rámci Evropské unie. Směrnice takovou situaci řeší stanovením povinnosti poskytovatele ustavit si v rámci Unie svého zástupce. Členský stát Unie, ve kterém je takový zástupce určen, se pak považuje za stát, v němž je poskytovatel digitálních usazen a dopadá na něj tedy regulace příslušného orgánu tohoto členského státu.

Směrnice pojem usazení ve svém recitálu 64 vymezuje takto „*Usazení předpokládá účinný a skutečný výkon činnosti prostřednictvím stálých struktur. Právní forma takových struktur, ať již jde o pobočku, nebo dceřinou společnost s právní subjektivitou, není v tomto ohledu rozhodující. Uvedené kritérium by nemělo záviset na tom, zda se sítě a informační systémy fyzicky nacházejí na daném místě; sama přítomnost a samotné používání takových sítí a systémů nejsou podstatou primárního usazení, a tudíž ani nejsou kritérii pro jeho určení.“.*

Směrnice řeší i stav, kdy je poskytovatel digitálních služeb usazen v jednom členském státu Evropské unie (v našem případě tedy v České republice), ale jeho sítě a informační systémy jsou umístěny v jiném členském státu. V takovém případě se zavádí povinnost NBÚ spolupracovat s příslušným úřadem tohoto dotčeného členského státu pro zjištění reálného stavu zajištění bezpečnosti sítí a informačních systémů a řešení případných nedostatků. Tato spolupráce může zahrnovat například výměnu informací mezi příslušnými orgány nebo vyžádání informací potřebných k posouzení bezpečnosti sítí a informačních systémů poskytovatele digitálních služeb, včetně existující bezpečnostní politiky, a v případě zjištění nedostatků uložení povinnosti jejich nápravy.

Ustaveným zástupcem musí být vždy podnikatel, který je usazený v Evropské unii, neboť v případě, že by tomu tak nebylo, ztrácel by institut ustavení zástupce jakýkoliv reálný smysl. Pro větší právní jistotu se stanoví, že zástupce musí být výslovně (doložitelně) pověřen k jednání jménem poskytovatele digitálních služeb.

9. K § 4 odst. 2

Čl. 14 odst. 1 a 2 směrnice stanoví, že členské státy zajistí, aby provozovatelé základních služeb přijali vhodná a přiměřená technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí sítě a informační systém, které provozovatelé používají pro výkon své činnosti. Tuto povinnost předkladatel transponuje do ustanovení § 4 odst. 2 zákona tím, že rozšiřuje okruh subjektů, na které se vztahuje povinnost zavést a provádět bezpečnostní opatření a vést o nich bezpečnostní dokumentaci. Vzhledem k tomu, že informační systém základní služby nemusí vždy spravovat a provozovat ve smyslu zákona o kybernetické bezpečnosti samotný provozovatel základní služby, adresuje se tato povinnost primárně správcům, potažmo provozovatelům informačnímu systému ZS. Požadavky na bezpečnostní opatření, jež budou v českém právním řádu začleněna do prováděcí vyhlášky, by dle recitálů směrnice měly být stanoveny přiměřeně k rizikům, aby nebyla uvalena nepřiměřená finanční a administrativní zátěž na provozovatele základních služeb, a to s ohledem na nejnovější technický vývoj a se zachováním technologické neutrality.

10. K § 4 odst. 3

V souladu s čl. 16 odst. 1 a 2 směrnice se poskytovateli digitálních služeb ukládá povinnost zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě a informační systémy, které využívají v souvislosti s nabízením svých služeb, tak aby byla zajištěna bezpečnost a kontinuální poskytování digitálních služeb. Na rozdíl od provozovatelů základních služeb nebudou poskytovatelé digitálních služeb „svazováni" konkrétními požadavky ze strany státu a bude především na nich, jak zabezpečí kontinuitu poskytování jejich služeb.

Směrnice tento přístup podporuje v recitálu č. 49 „*Poskytovatelé digitálních služeb by měli zajišťovat míru bezpečnosti přiměřenou míře rizika, jemuž je vystavena bezpečnost jimi poskytovaných digitálních služeb, a to se zřetelem k významu těchto služeb pro fungování jiných podniků v Unii. Míra rizika, jemuž jsou vystaveni provozovatelé základních služeb, mnohdy nezbytných pro zachování klíčových hospodářských a společenských činností, bývá ovšem v praxi vyšší než v případě poskytovatelů digitálních služeb. Bezpečnostní požadavky na poskytovatele digitálních služeb by tudíž měly být méně náročné. Poskytovatelé digitálních služeb by měli mít i nadále možnost přijímat opatření, jež považují za přiměřená z hlediska řízení rizik, kterým je vystavena bezpečnost jejich sítí a informačních systémů.".*

11. K § 4 odst. 4

Navrhovaná úprava reaguje na požadavky z praxe, kdy není zřídkavým jevem, že orgány nebo osoby uvedené v § 3 písm. c) až e) zákona nezahrnou bezpečnostní požadavky pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém do smluvních podmínek při uzavírání smlouvy s dodavatelem služeb. Nemusí tak být zajištěna bezpečnost jmenovaných systémů, což se předkladatel snaží napravit tím, že nově ukládá povinnost pod sankcí tyto požadavky do smluvních podmínek začlenit. Tuto povinnost předkladatel vzhledem k systematice zákona a požadavkům směrnice (čl. 14 odst. 1 a 2) ukládá i správci nebo provozovateli informačního systému ZS.

12. K § 4 odst. 5 a 6

I. Zavádí se nové povinnosti pro vymezené subjekty, a to povinnost mlčenlivosti o připravovaných a přijatých bezpečnostních opatřeních, jež je vyžadována nejen od orgánů a podnikatelů, ale i jejich zaměstnanců. Tato úprava odpovídá obdobné úpravě obsažené v § 97 odst. 8 zákona o elektronických komunikacích, kdy povinnost mlčenlivosti se vztahuje na povinné subjekty a jejich zaměstnance při zřizování rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv, uchovávání a poskytování provozních a lokalizačních údajů a poskytování údajů z databáze účastníků veřejné telefonní služby, tedy při obdobně citlivých činností.

II. Proto, aby byl vždy zajištěn přístup k informacím a datům z informačního systému nebo komunikačního systému kritické informační infrastruktury, významného informačního systému a informačního systému základní služby uloženým v cloudu, zavádí se povinnost správce nebo provozovatele takového systému – orgánu veřejné moci začlenit podmínku dostupnosti dat do jeho smlouvy s poskytovatelem služeb cloud computingu. To plně odpovídá recitálu č. 56, který vysvětluje, že „*Tato směrnice by neměla bránit členským státům v přijetí vnitrostátních opatření ukládajících subjektům veřejného sektoru, aby v rámci zakázek, jež na služby cloud computingu zadávají, zajistily uplatnění zvláštních bezpečnostních požadavků. Veškerá takováto vnitrostátní opatření by se měla vztahovat na dotyčný subjekt veřejného sektoru, a nikoli na poskytovatele služeb cloud computingu.".* Požadavku na vyšší míru zabezpečení přitaká i čl. 1 odst. 6 směrnice, jenž umožňuje členským státům

přijmout opatření s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti, včetně opatření na ochranu informací.

13. K § 4a

Obecně toto ustanovení zakládá povinnosti orgánů nebo osob, které se staly povinnými osobami podle zákona o kybernetické bezpečnosti, a tento fakt má dopad na třetí subjekty, aby tyto subjekty informovaly, tak aby bylo zaručeno, že budou za všech okolností naplňovány požadavky zákona. Způsob informování by měl být ve vlastním zájmu povinných osob prokazatelný.

Povinnost informovat se tedy vztahuje na následující

- orgány a osoby, které se stanou správcem informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury a nejsou provozovateli tohoto systému,
- orgány a osoby, které se stanou správcem nebo provozovatelem informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury, ve vztahu k subjektu zajišťujícímu síť elektronických komunikací, k níž je jejich předmětný informační nebo komunikační systém kritické informační infrastruktury připojen,
- subjekt, který Úřad určí jako provozovatele základní služby a který není zároveň správcem nebo provozovatelem svého informačního systému základní služby.

14. K § 6

Rozšiřuje se vymezení adresátů prováděcího právního předpisu, který stanoví rozsah bezpečnostních opatření, o správce a provozovatele informačního systému základních služeb. Návrh ustanovení reflektuje čl. 14 odst. 1 a 2 směrnice.

15. K § 7 odst. 3

V souladu s čl. 14 odst. 2 směrnice se povinnost detekovat kybernetické bezpečnostní události nově vztahuje i na správce a provozovatele informačního systému základních služeb.

16. K § 8 odst. 1

Toto ustanovení je transpoziční k čl. 14 odst. 3 a 4 směrnice. Dle stávajícího systému zákona o kybernetické bezpečnosti jsou hlášeny všechny kybernetické bezpečnostní incidenty, přičemž náležitosti a způsob hlášení kybernetického bezpečnostního incidentu upravuje prováděcí právní předpis. Nově se stanoví, že v souladu s tímto předpisem incidenty hlásí také správci a provozovatelé informačních systémů základní služby. Jako nadstavbovou informaci poskytne Úřadu provozovatel základní služby informaci o případném závažném dopadu na kontinuitu poskytování základní služby, pokud k takovému dojde, neboť pouze on je schopen posoudit reálné dopady kybernetického bezpečnostního incidentu.

Zároveň návrh tohoto ustanovení reaguje na čl. 33 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

17. K § 8 odst. 2

Tento novelizační bod transponuje čl. 16 odst. 3 a 4 směrnice. Zakládá se povinnost poskytovatelů digitálních služeb bezodkladně ohlásit provozovateli národního CERT kybernetické bezpečnostní incidenty se závažným dopadem na jejich služby. Tato povinnost je zmírněna podmínkou, že poskytovatelé digitálních služeb jsou povinni incident hlásit jen v případě, že mají k dispozici informace, které jim umožní posoudit závažnost dopadu incidentu. Kritéria pro určení závažnosti incidentu bude stanovovat prováděcí právní předpis, který již v současnosti stanoví kritéria incidentů pro ostatní povinné osoby podle tohoto zákona.

18. K § 8 odst. 3

Navrženou úpravou ustanovení § 8 odst. 4 se transponuje čl. 16 odst. 3 směrnice, kdy se za tým CSIRT, jemuž poskytovatel digitálních služeb hlásí kybernetický bezpečnostní incident, určuje národní CERT.

19. K § 8 odst. 4

Navrženou úpravou ustanovení § 8 odst. 5 se transponuje čl. 14 odst. 3 směrnice, kdy se adresátem hlášení kybernetického bezpečnostního incidentu, který nastal u provozovatele základních služeb, určuje NBÚ. Zároveň se text ustanovení legislativně technicky upravuje, neboť legislativní zkratka „Úřad“ byla zavedena již v § 2.

20. K § 8 odst. 6

Toto ustanovení zavádí do českého právního řádu článek 16 odst. 5 směrnice. Navrhovaný odstavec 5 tedy řeší situaci, kdy kybernetickým bezpečnostním incidentem je postižen poskytovatel digitálních služeb, na jehož službách je závislé provozování základních služeb. V tomto případě se ukládá povinnost provozovatele základních služeb informovat o významném dopadu incidentu na kontinuitu poskytování těchto základních služeb NBÚ, neboť právě pouze poskytovatel základní služby je schopen posoudit míru dopadu incidentu.

21. K § 9 odst. 2

Podle současné právní úpravy uchovává Úřad v evidenci incidentů informace o incidentech hlášených povinnými osobami podle zákona o kybernetické bezpečnosti. Vzhledem k tomu, že se nově v § 20 odst. 2 písm. l) rozšiřuje kompetence vládního CERT o přijímání dobrovolných hlášení kybernetických bezpečnostních incidentů, začleňují se informace o těchto hlášeních i do evidence vedené Úřadem podle § 9.

22. K § 11 odst. 3 písm. b) a 4

V souladu s čl. 14 směrnice se rozšiřuje povinnost provádět reaktivní a ochranná opatření i na správce a provozovatele informačního systému základní služby.

23. K § 12 odst. 3

Pokud je z důvodu veřejného zájmu, jímž může být zejména potřeba zvládnutí probíhajícího kybernetického bezpečnostního incidentu, ať již probíhá u provozovatele základních služeb nebo u poskytovatele digitálních služeb, nezbytná informovanost veřejnosti, zavádí se oprávnění NBÚ informovat veřejnost, nebo uložit povinnému subjektu, aby veřejnost informoval sám. NBÚ při rozhodování o zveřejnění informací o kybernetickém bezpečnostním incidentu vezme do úvahy

potřebu zachování rovnováhy mezi zájmem veřejnosti být informovanou o hrozbách a možným poškozením pověsti či obchodních zájmů provozovatelů základních služeb a poskytovatelů digitálních služeb, kteří incidenty ohlašují.

24. K § 13 odst. 4

Legislativně technické zpřesnění povinných subjektů, které odpovídá úpravě § 11 odst. 3.

25. K § 14

Ustanovení bylo nově formulováno tak, aby nemohlo vést ke dvojímu výkladu, a mezi adresáty opatření obecné povahy byli doplněni správci a provozovatelé informačního systému základní služby.

26. K § 16 odst. 2 písm. a)

Zavádí se povinnost poskytovatelů digitálních služeb předávat své kontaktní údaje provozovateli národního CERT. Institut kontaktních údajů slouží například ke komunikaci neformálních informací, závazných individuálních právních aktů vydávaných NBÚ (ochranných a reaktivních opatření). Komunikace prostřednictvím kontaktních údajů má zajistit nikoli jen formální informovanost orgánů a osob, ale i skutečný kontakt pracovišť CERT na konkrétní pracovníky fakticky odpovídající u poskytovatelů digitálních služeb za otázky kybernetické bezpečnosti – prostřednictvím těchto kontaktních údajů tedy bude možno vedle oficiální komunikace řešit též neformální kontakt výkonných pracovníků orgánů a osob s pracovišti CERT, běžnou neformální metodiku, technické konzultace apod.

27. K § 16 odst. 2 písm. b) a odst. 3

Zavádí se povinnost provozovatele základní služby, správců a provozovatelů informačního systému základní služby a poskytovatelů digitální služby předávat pro výkon státní správy a kontroly kontaktní údaje NBÚ a ohlašovat jejich změny, nejedná-li se o údaje, které jsou referenčními údaji vedenými v základních registrech.

28. K § 16 odst. 6

Rozšiřuje se okruh důvodů, za kterých může Úřad požadovat předání informací, jež sbírá provozovatel národního CERT, a to o účely kontroly plnění zákonných povinností podle § 24 zákona.

29. K § 17 odst. 2 písm. a), b), d) a e)

Mezi subjekty, se kterými komunikuje a spolupracuje provozovatel národního CERT, se doplňují poskytovatelé digitálních služeb.

30. K § 17 odst. 2 písm. c)

Mezi subjekty, se kterými spolupracuje provozovatel národního CERT, v tomto případě, u nichž vyhodnocuje kybernetické bezpečnostní incidenty, se doplňují poskytovatelé digitálních služeb. Toto ustanovení je v obráceném gardu k ustanovení, které stanoví povinnost poskytovatelů digitálních služeb hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT.

31. K § 17 odst. 2 písm. g)

Jedná se o jazykovou úpravu ustanovení a výslovného vztažení povinnosti předávání informací na incidenty nahlášené povinnými subjekty.

32. K § 17 odst. 2 písm. h) až l)

Národní CERT (Computer Emergency Response Team) na základě směrnice v tomto ustanovení získává nová kompetence a s nimi související povinnosti. Toto ustanovení je úzce provázáno s § 8, který mimo jiné upravuje hlášení kybernetických bezpečnostních incidentů, které postihly informační systém poskytovatele digitálních služeb. Národní CERT se v tomto ohledu mimo jiné určuje jako jeden z týmů CSIRT (Computer Security Incident Response Team) v České republice; vládní CERT (Národní centrum kybernetické bezpečnosti, jež je součástí NBÚ) je druhým týmem CSIRT ve smyslu směrnice pro incidenty proti bezpečností sítí a informačních systémů určených provozovatelů základních služeb.

33. K § 18 odst. 5

Toto ustanovení reaguje na rozšíření kompetencí provozovatele národního CERT v § 17 a rozšiřuje adekvátně okruh činností, jež provozovatel národního CERT vykonává bezplatně.

34. K § 18 odst. 5

Legislativně technická úprava z důvodu rozšíření kompetencí provozovatele národního CERT. Pro zajištění důsledného naplňování povinností vyplývajících ze směrnice a následně ze zákona o kybernetické bezpečnosti se zakotvuje povinnost národního CERT vynaložit na zajištění výkonu kompetencí adekvátní finanční prostředky.

35. K § 20 písm. a), b), d) a e)

Mezi subjekty, se kterými komunikuje a s nimiž spolupracuje vládní CERT, se doplňují nové povinné subjekty - provozovatelé základních služeb a správci a provozovatelé informačních systémů základních služeb.

36. K § 20 písm. c)

Mezi informační systémy, u nichž vládní CERT vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech, se doplňují informační systémy, na jejichž provozování je závislé poskytování základních služeb.

37. K § 20 písm. i)

Legislativně technická úprava vyplývající z potřeby doplnění nových písmen do tohoto ustanovení.

38. **K § 20 písm. j) a písm. k) až n)**

Vládní CERT na základě směrnice v tomto ustanovení získává nové kompetence a s nimi související povinnosti. Toto ustanovení je úzce provázáno s § 8, který upravuje hlášení kybernetických bezpečnostních incidentů.

Ustanovení upravuje postup vládního CERT v případě, že má nahlášený kybernetický bezpečnostní incident významný dopad na kontinuitu poskytování základních služeb, nebo dopad na poskytování digitálních služeb v jiném členském státu Evropské unie. V takovém případě se v souladu s čl. 14

odst. 5, potažmo čl. 16 odst. 6 směrnice zakotvuje oprávnění vládního CERT informovat o daném incidentu příslušné orgány jiných členských států.

Směrnice předvídá ve svém čl. 20 situaci, kdy subjekt, který nebyl určen jako provozovatel základních služeb a není ani poskytovatelem digitálních služeb, zaregistruje napadení bezpečnosti jeho informačních systémů a má snahu tuto situaci řešit. V tomto případě může tento kybernetický bezpečnostní incident dobrovolně nahlásit vládnímu CERT a ve spolupráci s ním situaci řešit. Vládní CERT v tomto případě hlášení zpracuje, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje přiměřeně, jako když je mu nahlášen kybernetický bezpečnostní incident u provozovatele základních služeb.

39. K § 22 písm. n)

Legislativně technická úprava vyplývající z potřeby doplnění nových písmen do tohoto ustanovení.

40. K § 22 písm. n) a písm. o) až s)

S ohledem na přijetí směrnice a z ní vyplývající nové úkoly pro orgány působící v oblasti kybernetické bezpečnosti rozšiřují se přiměřeně kompetence NBÚ, tak aby tento ústřední orgán státní správy splňoval všechny požadavky směrnice.

Vzhledem k tomu, že správci nebo provozovatelé komunikačních nebo informačních systémů kritické komunikační infrastruktury se na základě § 22a odst. 2 se považují za provozovatele základních služeb, je nutné v souladu se směrnicí pravidelně přezkoumávat aktuálnost jejich určení.

Informačními povinnostmi vůči Evropské komisi a skupině pro spolupráci podle směrnice 2016/xy/EU uvedenými v nově navrhovaném písmenu q) se rozumí tyto povinnosti vyplývajícími ze směrnice:

- povinnost nahlásit působnost týmů CSIRT (čl. 9 odst. 4 směrnice),
- povinnost ve stanoveném termínu a následně každé dva roky předkládat Evropské komisi informace (čl. 5 odst. 7 směrnice), které zahrnují nejméně

a) způsob určení provozovatelů základních služeb,

b) seznam základních služeb určených podle zákona o kybernetické bezpečnosti,

c) počet provozovatelů základních služeb určených v každém odvětví a jejich význam ve vztahu k dotyčnému odvětví,

d) mezní hodnoty, existují-li, pro stanovení příslušné zásobovací úrovně podle počtu uživatelů závislých na dané službě nebo význam konkrétního provozovatele základních služeb.

- povinnost ve stanoveném termínu předložit a poté každý rok předkládat skupině pro spolupráci ustavené v souladu s čl. 11 směrnice souhrnnou zprávu o hlášeních kybernetických bezpečnostních incidentů, jejich počtu, povahy ohlášených kybernetických bezpečnostních incidentů a přijatých opatření (čl. 10 odst. 3 směrnice).

Směrnice ve svém článku 7 ukládá členským státům povinnost zpracovat národní strategii pro bezpečnost sítí a informačních systémů a vymezuje její minimální obsah. Žádá také po členských státech, aby své schválené strategie hlásily Evropské komisi. Předkladatel tuto kompetenci svěřil v § 20 NBÚ s odkazem na požadovaný rozsah strategie podle směrnice.

41. K § 22 odst. 3

Navržené ustanovení naplňuje čl. 15 odst. 4 směrnice, která vyžaduje, aby příslušný úřad při řešení incidentů u provozovatele základních služeb, která poruší ochranu osobních údajů, spolupracoval s orgánem odpovědným za ochranu osobních údajů, v České republice tedy s Úřadem pro ochranu osobních údajů. Podle Strategie pro jednotný digitální trh v Evropě pouze 22 % Evropanů má plnou důvěru ke společnostem, jako jsou vyhledávače, sociální sítě a e-mailové služby a 72 % uživatelů internetu vyjadřuje znepokojení nad tím, že je od nich on-line požadováno příliš mnoho osobních údajů. Zajištění bezpečnosti osobních údajů je tedy nutnou podmínkou rozvoje digitální ekonomiky, a proto předkladatel rozšířil povinnost spolupráce s Úřadem pro ochranu osobních údajů na všechny typy kybernetických bezpečnostních incidentů.

42. K § 22a

I. Navržené ustanovení transponuje čl. 4 bod 4 a čl. 5 odst. 2 a 4 směrnice. Zmocňuje NBÚ k vydání prováděcího právního předpisu (vyhlášky), který stanoví odvětvová a průřezová kritéria, na jejichž základě budou možné určovat formou opatření obecné povahy provozovatele základních služeb a informační systémy základních služeb. Jak vyplývá i z definice informačního systému obsaženého ve směrnici, nemusí být informační systém tvořen pouze jedním zařízením, ale jeho fungování může záviset na vícero propojených (přiřazených) zařízení – technických prostředků, z nichž ne všechny musí nutně provádět automatické zpracování digitálních dat. Přičemž obecně lze konstatovat, že zpracováním dat se v širším kontextu čl. 4 odst. 1 písm. c) myslí jak samotné zpracování, tak i uchovávání, opětovné vyhledávání nebo předávání dat.

II. Systém určování dotčených osob provozovateli základních služeb opatřením obecné povahy odpovídá současnému systému určování správců informačních a komunikačních systémů kritické informační infrastruktury ze soukromé sféry. Vydání opatření obecné povahy zahrnuje podle správního řádu povinnou konzultaci s možností uplatnit odůvodněné námitky ve lhůtě 30 dnů ode dne zveřejnění jeho návrhu. Dotčené subjekty tak mají možnost vyjádřit se k předloženému návrhu a případně oponovat svému určení za provozovatele základních služeb.

III. Základní služby, jak jsou definovány směrnicí a jí nastavenými kritérii, jsou zpravidla služby značného významu a rozsahu v daném členském státě Evropské unie a je tedy více než pravděpodobné, že provozovatelé těchto služeb se nebudou omezovat na působení pouze v jednom členském státě. Tuto situaci směrnice předvídá a zavádí proto povinnost příslušného orgánu (tedy NBÚ) konzultovat určení provozovatele základních služeb s příslušnými orgány dalších členských států, v nichž podnikatel působí. Předkladatel návrhu zákona tuto povinnost konzultace upravuje v odstavci 3 nového § 22a.

IV. Pro zajištění toho, že seznam provozovatelů základních služeb je vždy aktuální a vychází z reálného stavu, ukládá se povinnost Úřadu pravidelně aktuálnost opatření obecné povahy ve dvouletých cyklech ověřovat.

43. K § 23 odst. 1

Vymezuje se rozsah subjektů, u nichž může NBÚ provádět kontrolu, a to rozšířením o nové povinné osoby – provozovatele základní služby, správce a provozovatele informačního systému základní služby.

44. K § 23 odst. 1

V případě poskytovatelů digitálních služeb se zavádí speciální režim kontroly, neboť v souladu s čl. 17 odst. 1 směrnice může být kontrolováno plnění povinností u těchto subjektů pouze v případě, že má příslušný orgán důkazy o tom, že poskytovatel digitálních služeb nesplňuje požadavky stanovené zákonem. Nelze tedy u těchto subjektů vykonávat kontrolu „preventivně".

45. K § 23 odst. 2

Z důvodu nadbytečnosti se vypouští druhý odstavec, jenž pouze rozváděl odstavec první, stanovující rozsah plnění povinností, které může Úřad kontrolovat.

46. K § 24 odst. 2

Mezi informační systémy, jejichž provozování může NBÚ zakázat v případě, že nebyly napraveny zjištěné nedostatky, se zařazují informační systémy, na jejichž provozování je závislé poskytování základní služby, tak aby jejich správci a provozovatelé byli v nejnutnějším případě donuceni nedostatky napravit.

47. K § 25 odst. 2 až 8

I. Do tohoto ustanovení upravujícího přestupky se nově doplňují přestupky, které vyplývají z nesplnění nově upravených transpozičních i jiných povinností v zákoně. Toto ustanovení implementuje do českého právního řádu čl. 21 směrnice.

II. Z důvodu vysoké nebezpečnosti nesplnění povinnosti zavést a provádět bezpečnostní opatření a vést bezpečnostní dokumentaci podle § 4 odst. 2 zákona se přiměřeně zvyšuje maximální výše pokuty u tohoto správního deliktu uvedeného v odst. 3 písm. a) tohoto ustanovení až na 5 mil. Kč, což je částka, která je oproti sankci za nesplnění obdobné povinnosti podnikatelů zajišťujících veřejné sítě elektronických komunikací podle § 98 odst. 1 zákona o elektronických komunikacích čtvrtinová (srov. § 118 odst. 14 písm. h) a odst. 22 zákona o elektronických komunikacích). I při stanovování konkrétní výše pokuty za tento správní delikt platí, že NBÚ přihlédne k závažnosti deliktu, zejména ke způsobu spáchání, následkům a okolnostem spáchání. Není tedy důvod obávat se bezbřehého správního uvážení NBÚ a automatického ukládání pokuty v blízkosti maximální hranice.

III. Dále se rozčleňují výše pokut za spáchané přestupky tak, aby přesněji reflektovaly závažnost jednotlivých přestupků.

48. K § 26 odst. 1

Doplňuje se nový přestupek fyzické osoby vyplývající z nově zavedené povinnosti mlčenlivosti o přijatých bezpečnostních opatření v § 4 odst. 5 zákona.

49. K § 27 odst. 8

Navrhované procesní ustanovení pro dosažení větší právní jistoty poskytovatelů digitálních služeb, již by si ustavili zástupce na území České republiky, stanoví, že i v případě ustavení zástupce na našem území může NBÚ zahájit řízení přímo proti poskytovateli digitálních služeb. Ustanovení naplňuje článek 18 odst. 3 směrnice.

50. K § 28 odst. 2 písm. b)

Legislativně technická úprava vnitřního odkazu v rámci zákona vyplývající z vložení nového odstavce do § 8.

51. K § 28 odst. 2 písm. c)

Jedná se o legislativně technickou úpravu vyvolanou potřebou doplnit do ustanovení nová písmena e) až g).

52. K § 28 odst. 2 písm. e) až g)

Legislativně technicky se upravuje a doplňuje zmocňovací ustanovení, které nově ukládá NBÚ vydat vyhlášku k provedení § 4 odst. 5, § 4 odst. 6 a § 22a odst. 1.

53. K § 30 písm. b)

Legislativně technická úprava vnitřního odkazu v rámci zákona vyplývající z vložení nového odstavce do § 4.

54. K § 31 písm. c)

Legislativně technická úprava vnitřního odkazu v rámci zákona vyplývající z vložení nového odstavce do § 4.

K čl. II

Přechodná ustanovení

1. V souladu s čl. 25 odst. 1 směrnice se stanoví lhůta, ve které má NBÚ povinnost vydat opatření obecné povahy podle § 22a odst. 1. Předpokladem pro splnění této povinnosti je vydání prováděcího právního předpisu, který stanoví kritéria, na jejichž základě budou provozovatelé základních služeb identifikováni.

2. Určení provozovatelé základní služby by měli do 30 dnů od jejich určení nahlásit Úřadu kontaktní údaje a nejpozději do jednoho roku začít plnit ostatní povinnosti podle zákona o kybernetické bezpečnosti.

3. Pro správce a provozovatele informačního systému základní služby se stanoví lhůta pro oznámení kontaktních údajů a přijetí potřebných opatření, tak aby byli schopni zajistit plnění všech zákonných povinností.

4. Poskytovatelům digitálních služeb se stanoví lhůta pro předání kontaktních údajů NBÚ a zahájení plnění povinností podle zákona o kybernetické bezpečnosti.

5. Vzhledem k nově zavedené povinnosti začlenit povinnosti, které se vztahují k bezpečnostním opatřením, do smluvních vztahů stanoví se lhůta, do kdy musí povinné subjekty uvést své smluvní vztahy do souladu se zákonem v případě, že jejich současné znění neodpovídá požadavkům zákona.

K čl. III

Změna zákona o svobodném přístupu k informacím

V současnosti účinná výjimka uvedená v § 11 odst. 4 písm. f) zákona o svobodném přístupu k informacím nenaplňuje požadavky na ochranu citlivých informací, zejména těch, které se vztahují k přijatým bezpečnostním opatřením podle zákona o kybernetické bezpečnosti. Potenciální útočník by tak v současné době mohl požádat podle tohoto zákona správce informačních nebo komunikačních systémů kritické informační infrastruktury nebo správce významných informačních systémů o poskytnutí informací o přijatých bezpečnostních opatřeních, přičemž tento povinný subjekt by byl povinen je poskytnout. Z tohoto důvodu se předkladatel rozhodl, i v souladu s čl. 1 odst. 6 a recitály č. 2 a 8 směrnice pro doplnění výjimky z povinnosti poskytovat informace na základě zákona o svobodném přístupu k informacím o údaje, které se týkají zajišťování kybernetické bezpečnosti a bezpečnosti sítí a informačních systémů podle zákona o kybernetické bezpečnosti.

K čl. IV

Účinnost

Navrhuje se účinnost k prvnímu dni druhého měsíce po publikaci zákona ve Sbírce zákonů tak, aby byla zajištěna dostatečná legisvakance. Tato lhůta naplňuje požadavky čl. 25 odst. 1 směrnice.