SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Připomínky k materiálu Ministerstva vnitra ČR – návrh zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
Č. J.	GŘ/83/SHP/2016
DATUM ZPRACOVÁNÍ	11. 8. 2016
KONTAKTNÍ OSOBA	Mgr. Tereza Šamanová
TELEFON	225 279 603
E-MAIL	tsamanova@spcr.cz

OBECNÉ ZÁSADNÍ PŘIPOMÍNKY

1. Připomínka obecného charakteru:

Důvodem předložení materiálu je transpozice Směrnice Evropského parlamentu a Rady 2016/1148/EU ze dne 6. července 2016 o opatřeních k zajištění vysoké úrovně bezpečnosti sítí a informačních systému v unii (dále jen „směrnice NIS“). Přestože požadavek přijetí nové právní úpravy vyplývá z práva EU, je třeba i v tomto případě při provádění transpozice norem sekundárního práva zohlednit jejich dopady na jednotlivé subjekty, zejména poskytovatele základních služeb. **Tyto dopady nejsou v obecné části důvodové zprávy dostatečně kvantifikovány a řádně posouzeny**. Zejména není **obecná část důvodové zprávy obsahující dopady na podnikatelské subjekty ani RIA zpracována dostatečně**, protože k předkládanému materiálu chybí jakákoliv hlubší analýza finančních dopadů na nezbytné implementační výdaje ICT systémů v dotčených odvětvích včetně alespoň obecné kvantifikace těchto výdajů. To se týká jak v obecné rovině, tak i jednotlivých zasažených odvětví, např. v případě regulovaných činností dle zákona č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů, v platném znění.

Předložení materiálu do meziresortního připomínkového řízení navíc přichází ve velmi krátké době po zveřejnění směrnice NIS v Úředním věstníku EU (19. července 2016, L 194), přestože transpoziční lhůta stanovená v čl. 25 směrnice končí až dne 9. května 2018.

Směrnice NIS také např. požaduje jednotné uplatňování definice základních služeb v členských státech (viz. bod 19 preambule směrnice) a k zajištění konzistentního přístupu pak v článku 11 odst. 3 to uvádí jako jeden z úkolů „skupiny pro spolupráci“. Podle článku 24 má být ale tato skupina ustavena nejpozději k 9. únoru 2017, přičemž je na tento proces stanoveno období od 9. 2. 2016 do 9. 11. 2018, takže nevidíme důvod pro zrychlený způsob implementace směrnice, který byl v ČR zvolen.

Navíc byla na úrovni EU ustanovena skupina ENISA, která by měla podporovat spolupráci a harmonizovaný přístup k zajišťování kybernetické bezpečnosti v členských státech. Tato skupina vypracovává bezpečnostní požadavky a požadavky na hlášení incidentů, aby byla podpořena kultura

řízení rizik a aby bylo zaručeno hlášení nejzávažnějších incidentů, které by se rovněž měly nyní nově na provozovatele základních služeb a na poskytovatele digitálních služeb vztahovat.

Přidání konceptu základní služby definované směrnicí ke stávajícímu vymezení kritické infrastruktury dané současným zákonem může do značné míry zvýšit počet ekonomických subjektů, na něž bude mít nový zákon dopad. Stane se tak zejména tehdy, nebudou-li sladěna kritéria materiality pro definování provozovatele základní služby a stávající kritické infrastruktury.

To, že sladěna v současné době nejsou, dokumentuje materiál „Teze vyhlášky o určování poskytovatelů základních služeb“ v oblasti dopadových kritérií. Např. dopadové kritérium „omezení základní služby postihující více než 50 tis. osob“ v oblasti bankovnictví způsobí, že poskytovatelem základní služby se stanou prakticky všechny banky v ČR (prakticky všechny mají více než 50 tis. klientů). V oblasti bankovnictví je dnes totiž za kritickou službu, která je podporována prvky kritické informační infrastruktury, vnímán hotovostní i bezhotovostní platební styk, tedy služba, kterou poskytují všechny banky pro prakticky všechny své klienty. Oproti současnému stavu, kdy zákon definoval kritickými pouze 3 banky, by šlo o řádově vyšší dopad.

Bez znalosti návazné regulace, zejména pak zmíněných dopadových kritérií, která budou stanovena prováděcím právním předpisem k zákonu o kybernetické bezpečnosti (vyhláškou), pak nelze odhadnout, jak předkládaný materiál ovlivní podnikatelské prostředí, zejména pak, jaké budou náklady na jeho implementaci.

Vzhledem k tomu, že

- návrh neobsahuje výše uvedené zohlednění všech dopadů na dotčené subjekty a nenaplňuje standardy hodnocení dopadů regulace,
- nepočítá se zohledněním výstupů práce ENISA do této transpoziční novely,
- u řady novelizovaných ustanovení (např. § 4, § 22a) byla ze strany předkladatele materiálu svěřena podrobnější a přitom zásadní právní úprava prováděcímu právnímu předpisu (např. čl. I body 12. a 42.), jehož alespoň základní znění nebylo spolu s materiálem předloženo,
- oblast kybernetické bezpečnosti je v českém právním řádu upravena i celou řadou dalších předpisů (např. zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, v platném znění - ZoEK a zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, v platném znění - ZoKŘ), které však nejsou navrhovanou novelizací měněny, což předkladatel spolehlivě neodůvodňuje a neuvádí vztah navrhované novelizace a transpozice směrnice k již existující úpravě,

považujeme v tomto okamžiku předložení materiálu do meziresortního připomínkového řízení za předčasné.

Z výše uvedených důvodů navrhujeme přerušit projednávání předloženého návrhu, a to i s ohledem na to, že ČR již základní legislativu pro tuto oblast má a na transpozici je stanoveno období 21 měsíců. Není tedy vhodné o transpozici směrnice NIS překotně aktivovat jen jeden předpis z existujícího zákonného rámce a znepřehlednit a znehodnotit tím funkční systém legislativy pro oblast kybernetické bezpečnosti. Naopak navrhujeme časový prostor využít k vyladění a vyjasnění případných duplicit a překryvů

(například v termínech, postupech, numerických kritériích a koncepci). Jako příklad uvádíme: současná legislativa předpokládá elektronickou komunikaci jako typickou součást procesů zpracování informací a definuje kromě informačního systému též komunikační systém, NIS však vzájemnou komunikaci informačních systémů základních služeb exaktně neřeší.

Z uvedených důvodů se domníváme, že by bylo vhodné legislativní proces pozdržet a zejména průvodní dokumenty k materiálu doplnit o spolehlivé vyhodnocení jeho dopadů a současně s ním zahájit legislativní proces k prováděcím předpisům, jejichž prostřednictvím bude možné získat bližší informace o zákonodárcem zamýšlené implementaci materiálu.

KONKRÉTNÍ ZÁSADNÍ PŘIPOMÍNKY

1. Připomínka k čl. I, novelizace § 2 (Vymezení pojmů):

Navrhujeme text doplnit o definici pojmu „kybernetická bezpečnost".

Odůvodnění: Pojem kybernetická bezpečnost není definován, přitom jde o zcela zásadní pojem, který se v textu zákona často opakuje.

2. Připomínka k čl. I, novelizace § 2 (Vymezení pojmů):

Navrhujeme text doplnit o definici pojmu „provozovatel informačního systému", analogicky s existující definicí správce informačního systému.

Odůvodnění:

Díky absenci definice není například jasné:

- zdali je totéž j), g) „provozovatel základní služby" a f) „provozovatel informačního systému základní služby"
- dále nejasné též § 4a (1) ….Orgány a osoby, které se staly správcem informačního nebo komunikačního systému kritické informační infrastruktury nebo správcem významného informačního systému, a nejsou provozovatelem tohoto systému….

3. Připomínka k čl. I, bod 5, novelizace § 2 (Vymezení pojmů), písm. h), bod 9.:

Ustanovení se vzájemně vylučuje s § 2 písm. d), je třeba tento nesoulad odstranit.

Odůvodnění: Užití veřejné správy v rámci základní služby vylučuje užití „významných systémů" dle § 2 písm. d).

4. Připomínka k čl. I, bod 5, novelizace § 2 (Vymezení pojmů), písm. k):

V písm. k) digitální službou informační společnosti, která spočívá v poskytování služby:

Odůvodnění: Z navrhovaného znění zákona není zřejmé, jaký je vztah digitálních služeb vyjmenovaných ve směrnici NIS k budoucím službám podle nařízení eIDAS. Navrhujeme explicitně zakotvit, že poskytovatelé služeb vytvářejících důvěru nespadají do působnosti zákona a že nejde nad rámec směrnice.

5. Připomínka k čl. I, bod 5, novelizace § 2 (Vymezení pojmů), písm. k), bod 1:

Navrhujeme doplnit jednoznačnou definici termínu „on-line tržiště".

Odůvodnění: Pojem „on-line tržiště“ je sice definován ve směrnici NIS, není však obsažen v navrhované novele zákona o kybernetické bezpečnosti, což může způsobit nejasnosti při výkladu tohoto pojmu. Navrhujeme proto definici doplnit v souladu se zněním směrnice. Analogicky je třeba odkázat i na definice „internetových vyhledávačů“ a „služeb cloud computingu“ dle směrnice.

6. Připomínka k čl. I, bod 9, novelizace § 4 (Bezpečnostní opatření), odst. 2:

Navrhujeme text ustanovení upravit takto:

(2) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět bezpečnostní opatření zabraňující vzniku kybernetických bezpečnostních událostí v rámci informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, významného informačního systému a informačního systému základní služby a vést o nich bezpečnostní dokumentaci.

Odůvodnění: Pro osoby správce a provozovatele informačního systému základní služby §3 písm. f) zákon v přechodných ustanoveních, viz §§ 29-31 nestanoví dobu zavedení bezpečnostní opatření.

7. Připomínka k čl. I, bod 11, novelizace § 4, odst. 4:

Navrhujeme větu první nahradit větou: *„Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou.“*.

Odůvodnění:

- Nejedná se o odstavec 4, ale o odstavec 3
- Vzhledem k oslabení zákona, kdy je vypuštěna formulace “*Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži*” by zohlednění požadavků pro veřejné zadavatele mělo být promítnuto v novele zákona o zadávání veřejných zakázek, aby se konkretizoval dopad naznačené povinnosti do zadávacího řízení a zadávací dokumentace, nikoli jen do smlouvy. Mohlo by být zneužito pro hosp. soutěže

8. Připomínka k čl. I, bod 12, novelizace § 4, odst. 5:

Navrhujeme z materiálu vypustit povinnost mlčenlivosti subjektů a jejich zaměstnanců, která jde nad rámec transpozice.

Odůvodnění: Nesouhlasíme s navrženým ustanovením odstavce 5, kterým by orgány a osoby uvedené v § 3 písm. c) až f) a jejich zaměstnanci byli povinni zachovávat mlčenlivost o připravovaných a přijatých bezpečnostních opatřeních.
Povinnost mlčenlivosti představuje v návrhu novely zákona o kybernetické bezpečnosti jako doplněk nad rámec transpozice Směrnice NIS.
Z důvodové zprávy je patrno, že důvodem pro legislativní zakotvení mlčenlivosti je údajné „značné bezpečnostní riziko úniku citlivých informací“. Je zmíněna snaha zabránit vyzrazení „citlivých údajů“ týkajících se zabezpečení sítí a informačních systémů a obava, že únik „citlivých informací“ by ohrozil provádění bezpečnostních opatření. V odůvodnění novelizace však zcela chybí kvalitativní i kvantitativní data k tomuto „bezpečnostnímu riziku“, v kolika případech skutečně došlo k úmyslnému či neúmyslnému vyzrazení těchto údajů právě zaměstnanci dané společnosti, jaké množství, jakého

typu a v jaké úrovni detailu uniklá data byla, zda to reálně ohrozilo realizaci bezpečnostních opatření a jaká je velikost tohoto rizika v porovnání s ostatními kanály úniku dat (dodavatelé, státní správa, externí útočníci) a ostatními riziky obecně.

Alternativní návrh – Většina dotčených subjektů má interně definovaný systém klasifikace informací. Na řadu energetických subjektů navíc dopadá zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zákon o krizovém řízení, které nakládání s klasifikovanými informacemi řeší (např. informace na stupni "vyhrazeno", „zvláštní skutečnosti") a dále také zákon č. 224/2015 Sb., o prevenci závažných havárií.

S ohledem na výše uvedené lze konstatovat, že pro účinnou ochranu klasifikovaných skutečností lze minimálně v odvětví energetiky využít existující legislativu. Případně lze do zákona o kybernetické bezpečnosti zavést povinnost dotčených subjektů informace a informační aktiva analyzovat, klasifikovat a náležitě chránit a dále povinnost interně klasifikovat informace o opatřeních na nejvyšší stupeň. Informace by pak byly chráněny během transferu, během uložení i během použití a daná problematika by byla podchycena koncepčně a odborně.

9. Připomínka k čl. I, bod 12, novelizace § 4, odst. 6:

Navrhujeme ve větě první slovní spojení *v reálném čase* vypustit a nahradit slovním spojením *bez zbytečného odkladu.*

Odůvodnění: Není jasné, co se myslí pojmem „v reálném čase", navíc je v textu použito časové vymezení „bez zbytečného odkladu" ve vztahu k poskytnutí informací, navrhujeme jej použít také ve věci umožnění kontroly.

10. Připomínka k čl. I, bod 12, novelizace § 4, odst. 6:

Navrhujeme ustanovení doplnit následovně:

(6) Orgány a osoby uvedené v § 3 písm. c) až f), které jsou orgánem veřejné moci, jsou povinny si ve smlouvě, kterou uzavírají s poskytovatelem služeb cloud computingu, zejména zajistit, že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává, a možnost kontroly uchovávaných informací a dat v reálném čase. Náležitosti smlouvy stanoví prováděcí právní předpis. Poskytovatel služeb není povinen zpřístupnit data spojená s technickým zajištěním provozu cloudových služeb zákazníků.

Odůvodnění: Je třeba vyjasnit, že zákazníkovi budou poskytnuta pouze data, která zákazník poskytl poskytovateli služby a s nimi spojené údaje spojené s provozem služby (zabezpečení, zálohování, monitoring atp.). Poskytoval služeb nemá povinnost zpřístupňovat data spojená s technickým zajištěním provozu cloudových služeb zákazníků (např. nastavením routerů, switchů, napájení a chlazení datacentra atp.), zde se jedná o obchodní modely ne o bezpečnost.

11. Připomínka k čl. I, body 16 - 20, novelizace § 8 (Hlášení kybernetického bezpečnostního incidentu):

Je třeba doplnit do přechodných ustanovení zákona okamžik vzniku povinností stanovených v § 8 pro osoby správce a provozovatele informačního systému základní služby.

Odůvodnění: zákon ve svých přechodných ustanoveních (§ 29 - § 31) nestanoví dobu vzniku povinností stanovených v § 8, což komplikuje implementaci § 8.

12. Připomínka k čl. I, bod 17, novelizace § 8:

V souvislosti s novým odst. 2 § 8 navrhujeme dále do § 7 do odstavce (2) vložit definici významného dopadu na poskytování služeb provozovatelem digitální služby s odkazem na parametry, které vyplynou z práce ENISA.

Odůvodnění: Jde o zajištění právní jistoty pro poskytovatele digitálních služeb vymezit, který incident má významný dopad na poskytování služeb tak, aby organizace byly schopny dostát povinnostem ukládaným v § 8 (2). V§ 8 odst. (5) je sice uvedeno, že prováděcí předpis stanoví typy a kategorie kybernetických incidentů a náležitosti a způsoby jejich hlášení, definice kybernetického incidentu, který má významný dopad na poskytování služby, by však měla být obsažena v zákoně. Navíc je tato definice důležitá pro harmonizovaný postup napříč členskými státy EU, který byl jedním z cílů směrnice. 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnostních sítí a informačních systémů v Unii. Článek 14 odst. 7 této směrnice uvádí, že „státy mohou vypracovat a přijmout pokyny týkající se okolností, za nichž jsou provozovatelé základních služeb povinni hlásit incident, **včetně parametrů pro určení významnosti dopadu daného incidentu**." Česká republika se na práci ENISA podílí, považujeme tedy za nezbytné, aby výsledky této práce byly reflektovány v této zákonné normě i jejích prováděcích předpisech.

13. Připomínka k čl. I, bod 22, novelizace § 11, odst. 3, písm. b):

Navrhujeme text ustanovení upravit takto:

(3) Reaktivní opatření jsou povinny provádět

a) orgány a osoby uvedené v § 3 písm. a) a b) za stavu kybernetického nebezpečí nebo za nouzového stavu[4)] vyhlášeného na základě žádosti podle § 21 odst. 6 a

b) orgány a osoby uvedené v ~~§ 3~~ písm. ~~c) až e)~~ § 3 písm. c) až f).

Odůvodnění: Reaktivní opatření pro soukromoprávní subjekty §3 písm. c), d), f) by mělo mít pouze formu doporučení, neboť Úřad nedokáže kvalifikovaně posoudit dopad opatření na každý jednotlivý systém. Existuje riziko, že vlivem plošného rozhodnutí dojde k omezení dostupnosti systémů a tedy i ekonomickým škodám.

Riziko: Pokud stát nařídí provést opatření musí být i nutně odpovědný za případně vzniklou škodu.

14. Připomínka k čl. I, bod 23, novelizace § 12:

Navrhujeme z textu vypustit slovní spojení *„z důvodu veřejného zájmu oprávněn"* a *„nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám"* a text odstavce (3) upravit následovně:

Pokud je pro zamezení incidentu nebo pro zvládání probíhajícího incidentu nezbytné informovat veřejnost, může Úřad po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat.

Odůvodnění: Právo Úřadu informovat o kybernetickém incidentu veřejnost je v návrhu stanoveno příliš obecně a široce pomocí sousloví „ve veřejném zájmu" a jde tak nad rámec směrnice. Čl. 14 směrnice jasně stanoví, že povinnost informovat veřejnost nastává pouze v případě, že je to nutné pro zamezení incidentu zamezit nebo jeho zvládnutí. Také považujeme za zbytečnou byrokratickou zátěž ukládat

povinnost informovat veřejnost také poskytovateli základních služeb, navíc tato povinnost jde opět nad rámec směrnice.

Navrhovaná formulace „*nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám*“ navíc může způsobit kolizi ustanovení s povinností mlčenlivosti stanovenou v § 4 odst. 5, a to zejména u soukromoprávních subjektů.

15. Připomínka k čl. I, návrh novelizace § 13. odst. 2:

Navrhujeme vypustit odst. 2 a následující odstavce přečíslovat.

Odůvodnění: V případě soukromých subjektů by mohla okamžitá realizace opatření zbytečně způsobit škodu, konkrétní systém u těchto subjektů může být přitom zabezpečen jiným způsobem.

Existuje riziko, že „plošným“ rozhodnutím může dojít k omezení dostupnosti některých systémů, u nichž dopad rozhodnutí není nutný, a následně pak dojít i ke vzniku škody.

16. V rámci řízení o rozkladu lze situaci vyjasnit a vzniku škody předejít

17. Připomínka k čl. I, novelizace § 15a, odst.1:

Navrhujeme text upravit takto:

§ 15a

(1) Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na návrh správce informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby nebo významného informačního systému rozhodnutím uložit provozovateli tohoto systému povinnost předat správci data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému; návrh musí obsahovat odůvodnění požadavku, podrobný popis předchozího jednání mezi provozovatelem a správcem tohoto systému a možné následky, pokud nedojde k předání požadovaných dat, provozních údajů a informací.

Odůvodnění: Informační systémy základní služby lze z hlediska jejich významu a možných dopadů v případě jejich nefunkčnosti položit na roveň systémům kritické informační infrastruktury a nelze předpokládat, že správce a provozovatel těchto systémů bude vždy totožný. Sice platí, že „subjekty naplňující kritéria a definice pro provozovatele základní služby i kritické infastruktury, kteří budou zároveň důležití pro fungování státu jako takového a budou naplňovat kritéria podle nařízení vlády č. 432/2010 Sb., budou regulováni jakožto kritická informační infrastruktura“, nicméně neplatí to vždy obráceně, že provozovatele základní služby lze považovat za orgán nebo osobu uvedenou v § 3 písm. c) a d). Proto se domnívám, že je třeba v § 15a, odst. 1 explicitně uvést i informační systém základní služby.

18. Připomínka k čl. I, body 26 - 27, novelizace § 16:

Navrhujeme text ustanovení změnit takto:

(2) Kontaktní údaje a jejich změny oznamují

a) orgány a osoby uvedené v ~~§ 3 písm. a) a b)~~ § 3 písm. a), b) a h) provozovateli národního CERT a

b) orgány a osoby uvedené v ~~§ 3 písm. c) až e)~~ § 3 písm. c) až g) Úřadu.

Odůvodnění: U osob §3 písm. f) až h) není v rámci přechodných ustanovení (§§ 29-31) stanovena lhůta pro oznámení kontaktních údajů.

19. Připomínka k čl. I, bod 32, novelizace § 17, odst. 2, písm. j):

V souvislosti s novým zněním písm. j) v odst. 2 § 17 navrhujeme do dokumentu vložit definici významného dopadu na poskytování služeb provozovatelem digitální služby s odkazem na parametry, které vyplynou z práce ENISA.

Odůvodnění: Ad připomínka č. 13.

20. Připomínka k čl. I, bod 40, novelizace § 22, písm. p):

Navrhujeme blíže upřesnit záměr zákonodárce a zejména proces, na jehož základě má dojít k určení konkrétního informačního systému základní služby.

Odůvodnění: Ustanovení je neurčité a není zcela zřejmý záměr zákonodárce – zejm. není jasný proces, na jehož základě dojde k určení konkrétního informačního systému základní služby, tj. zda např. Úřad osloví vybrané subjekty a ty mu jsou povinny poskytnout požadované informace. Pokud ano, nejsou jasné podmínky tohoto procesu, tj. v jakém formátu, v jaké lhůtě a jakým způsobem má dojít k předání informací.

21. Připomínka k čl. I, bod 47, novelizace § 25 odst. 2 až 8 (Správní delikty):

Navrhujeme přehodnotit výši navrhovaných pokut za správní delikty.

Odůvodnění: Oproti původní úpravě jednotlivých skutkových podstat správních deliktů obsažených v § 25 došlo k významnému navýšení peněžitých sankcí za správní delikty. Ve zvláštní části důvodové zprávy k bodu 47. je sice uvedeno, že výše sankcí je oproti ZoEK čtvrtinová, avšak při zohlednění dopadu dosud nevyčíslitelných nezbytných nákladů na implementaci ICT systémů poskytovatelů základních služeb novým povinnostem je tato výše nepřiměřená.

V textu zvláštní části důvodové zprávy je navíc u tohoto novelizačního bodu chybně uváděno, že se jedná o přestupky, přičemž jde o správní delikty postihující výhradně právnické osoby.

22. Připomínka k čl. I, bod 47, novelizace § 25 odst. 5:

Navrhujeme z výčtu přestupců vyjmout osoby specifikované v § 3 písm. f).

Odůvodnění: Orgán nebo osoba uvedená v § 3 písm. f) se nemůže dopustit přestupku, neboť není stanovena příslušná lhůta pro zavedení opatření a začátek platnosti.

23. Připomínka k čl. I, návrh novelizace § 29 - § 31:

Navrhujeme doplnit též odklad plnění povinností stanovených v § 8 odst. 1 pro osoby uvedené v § 3 písm. f), a to až o 2 roky.

Odůvodnění: Pro osoby správce a provozovatele informačního systému základní služby chybí odkladná lhůta pro zahájení plnění povinnosti hlásit kybernetické bezpečnostní incidenty. Navrhuje se až dvouletá lhůta, protože se nejedná o kritickou infrastrukturu.

DOPORUČUJÍCÍ PŘIPOMÍNKY

1. Připomínka k § 11:

Domníváme se, že v ustanovení zcela chybí část preventivních a detekčních bezpečnostních opatření. Detekční bezpečnostní opatření jsou zmiňována např. v § 5 a § 8 a je zde tak nekonzistence v textaci.