SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Připomínky Svazu průmyslu a dopravy České republiky k materiálu Návrh zákona, kterým se mění některé zákony v souvislosti s úpravou vybraných agend v působnosti Digitální a informační agentury
Č. J.	45/2024
DATUM ZPRACOVÁNÍ	9. 5. 2024
KONTAKTNÍ OSOBA	Kateřina Kalužová
TELEFON	225 279 202
E-MAIL	kkaluzova@spcr.cz

KONKRÉTNÍ PŘIPOMÍNKA

1. Změna zákona o zřízení ministerstev a jiných ústředních orgánů

„V § 12 odst. 5 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění zákona č. 71/2006 Sb. a zákona č. 295/2009 Sb., se za slovo „správy“ vkládají slova „dohled nad bezpečností komunikačních a informačních systémů státní správy“. Tuto úpravu navrhujeme z návrhu vypustit.

Odůvodnění:

Nedostatečná specifikace dopadů

Navrhované znění představuje riziko v nejasném ohraničení práv a povinností mezi Ministerstvem vnitra (MV) a Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). Vložení zmínky o „dohledu nad bezpečností komunikačních a informačních systémů státní správy“ není podloženo řádnou dopadovou analýzou. Máme za to, že takto exaktním uvedením kompetence/povinnosti může vést v některých případech k duplikaci činností. Například monitorování/dohled ISVS podléhajících ZoKB, provozovaných v režimu cloudové služby. Současně není jasný souběh „dohledu“ v případě provozování vlastního dohledového centra. Na základě výše uvedeného navrhujeme tuto úpravu týkající se vložení vyjmout.

Potenciální hrozba ovlivnění trhu

Zavedení zmíněného dohledu pouze v gesci MV může mít za následek omezení okruhu jiných potenciálních poskytovatelů dohledové služby. Nepokládáme za vhodné, aby byla takto detailně zanesena v zákoně č. 2/1969 Sb.

Rozsah dohledu nad bezpečností komunikačních a informačních systémů státní správy

Navrhovaný text je příliš obecný. Navrhujeme, aby byl rozsah vloženého dohledu více specifikován, konkrétně, aby nezahrnoval systémy provozované v režimu SeGC, například úpravou ZoKB.

Rozdělení kompetencí mezi NÚKIB A MV

V současné době je NÚKIB tím, kdo provádí kontroly dodržování požadavků zákona o kybernetické bezpečnosti u regulovaných subjektů. Současně s odborem regulace se podílí na přípravě legislativy v oblasti kybernetické bezpečnosti a poskytuje metodickou podporu regulovaným subjektům. Dále na kontrolní činnosti spolupracuje s dalšími kontrolními orgány, jejichž kontrolní činnost má přesah do oblasti kybernetické bezpečnosti. Není zde jasné, jak se bude postupovat v případě, že MV v rámci dohledu odhalí nedostatek nebo porušení v oblasti bezpečnosti komunikačních a informačních systémů státní správy.

V návrhu samotném, ani v důvodové zprávě není uvedeno, zda bude mít MV v rámci dohledu oprávnění aktivního zásahu do služby. Pokud ano, a zásah bude mít za následek nedostupnost služby pro zákazníka, jak se bude řešit porušení SLA, pokuty a pod? Bude se zásah MV považovat za „vyšší moc“?

Sankcionování
NÚKIB je tím, kdo ukládá pokuty za nedodržení ZoKB a VoKB. V žádném z návrhů není definována a blíže popsána spolupráce mezi NÚKIB a MV právě v oblasti dohledu nad bezpečností. Navrhovaná změna přinese řadu nejasností při výkonu praxe obou subjektů. V materiálech chybí definice samotného dohledu a pravomoci v případě ukládání postihů.

Zavadění bezpečnostních opatření
Povinnost subjektů zavádět bezpečnostní opatření vyplývá ze stávajícího ZoKB

Kontrolní subjekty v oblasti kybernetické bezpečnosti
V materiálu není popsáno rozšíření kontrolních subjektů v oblasti kybernetické bezpečnosti na MV.

Zajištění kybernetické bezpečnosti v oblasti CC
Zajištění KYBE v oblasti cloud computingu, zejména pak v oblasti poskytování státní části je upravena v ZoISVS – poskytovatele státního CC pověřuje vláda, registrování všech poskytovatelů služeb a služeb realizuje DIA a tato registrace není možná bez zajištění bezpečnosti komunikačních a informačních systémů. Takže kontrola je tímto realizována.

Kontrolní orgán pro CC služby
Podle § 6i odst. 3) Národní úřad pro kybernetickou a informační bezpečnost kontroluje, zda cloud computing poskytovaný orgánům veřejné správy splňuje požadavky podle § 6n, v případě, že je využíván k provozování informačního systému veřejné správy, který je informačním nebo komunikačním systémem kritické informační infrastruktury, významným informačním systémem nebo informačním systémem základní služby podle právního předpisu upravujícího kybernetickou bezpečnost.

Způsob zajištění koordinace kontrol
Zákon o ISVS neukládá poskytovatelům cloud computingu (ani komerčním poskytovatelům ani poskytovatelům státní části eGovernment cloudu) povinnost spolupracovat při faktické realizaci kybernetické bezpečnosti s MV.
Jakým způsobem mají registrovaní poskytovatelé cloud computingových služeb zahrnout při zajištění kybernetické bezpečností součinnost s MV? Jak mají zmínění poskytovatelé kalkulovat případné dodatečné náklady vynaložených na splnění požadavků MV při umožnění dohledu?

Tato připomínka je zásadní.