SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Připomínky Svazu průmyslu a dopravy České republiky k Návrhu vyhlášky o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu
Č. J.	63/2025
DATUM ZPRACOVÁNÍ	6. 6. 2025
KONTAKTNÍ OSOBA	Kristýna Zábojníková
E-MAIL	kzabojnikova@spcr.cz

Za Svaz průmyslu a dopravy ČR (SPČR) uplatňujeme tyto připomínky:

KONKRÉTNÍ PŘIPOMÍNKY

1. **K řádku 1.7 přílohy vyhlášky – omezení zpracování dat mimo území České republiky**

Navrhujeme vymazání tohoto bodu vyhlášky.

Odůvodnění:

Toto ustanovení jde nad rámec potřebných opatřeních.

Tato připomínka je zásadní.

2. **K řádku 4.3 přílohy vyhlášky – vzdálenost datových center od zdrojů rizik**

Doporučujeme zrušit, nebo stanovit kratší vzdálenost mezi datovými centry.

Odůvodnění:

Vzdálenost 50 km je příliš vysoká a není odůvodněné umísťovat datová centra na takové vzdálenosti od sebe.

Tato připomínka je zásadní.

3. **K řádku 5.5 přílohy vyhlášky – shromažďování provozních údajů o činnostech provedené technickými aktivy**

Navrhujeme odstranit z řádku 5.5 písm. b) přílohy vyhlášky pojem „***~~a technickými aktivy~~***“:

„Provozní údaje se vztahem ke službě cloud computingu se shromažďují zejména o událostech:

[…]

*b) činnosti provedené administrátory[1] **~~a technickými aktivy~~** na straně poskytovatele zejména pokud zaměstnanci nebo externí pracovníci poskytovatele čtou nebo zapisují nešifrovaná zákaznická data nebo*

TELEFON (+420) 731 829 128 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADRESA FREYOVA 948/11, 190 00 PRAHA 9
ZAPSANÝ VE SPOLKOVÉM REJSTŘÍKU, VEDENÉM MĚSTSKÝM SOUDEM V PRAZE ODDÍL L, VLOŽKA 3148.
IČO: 00536211, DIČ: CZ00536211.

specifické provozní údaje zpracovávané ve službě cloud computingu nebo k nim přistupují bez předchozího souhlasu orgánu veřejné správy,“

Odůvodnění:

Předložený návrh vyhlášky doplňuje v řádku 5.5 písm. b) přílohy vyhlášky pojem „technická aktiva“, kterými se rozumí dle § 2 písm. g) vyhlášky „*technické vybavení, komunikační prostředky a programové vybavení služby cloud computingu a objekty, které jsou využívány k poskytování služby cloud computingu a jejichž selhání může mít dopad na službu cloud computingu*“. V důsledku této změny nově platí, že provozní údaje se mají shromažďovat nejen o činnostech provedených administrátory, ale také o činnostech provedených „*technickými aktivy na straně poskytovatel*e“.

Domníváme se, že doplnění pojmu „technická aktiva“ v uvedeném ustanovení přináší významnou právní a praktickou nejistotu ohledně povinnosti shromažďování provozních údajů a způsobu prokázání jejího plnění.

Na rozdíl od činností administrátorů, jejichž přístupy a zásahy do systému je účelné auditovat, logovat a přezkoumávat, činnosti technických aktiv jsou v praxi realizovány standardně automaticky na základě konfigurace systémů, systémových operací a interních procesů cloudové infrastruktury. Technická aktiva, jako jsou servery, úložné systémy, síťová zařízení či virtualizační platformy, standardně zpracovávají zákaznická data v nešifrované podobě při běžných výpočetních operacích. Tyto operace jsou inherentní a nezbytné pro fungování jakékoliv cloudové služby – činnosti provedené technických aktiv probíhají na automatické bázi bez zásahu lidských aktérů a nejedná se o nestandardní situace, které by bylo vůbec technicky účelné logovat a shromažďovat jako provozní údaje.

Z technického hlediska by tento požadavek znamenal nutnost evidovat obrovské množství nízkoúrovňových systémových operací (např. každý přístup procesoru, čtení a zápis na disk, přesuny dat v paměti), které nelze smysluplně sledovat ani zaznamenávat odpovídajícím způsobem. Jako ilustrativní příklad lze uvést běžné automatické zpracování dat v rámci antivirového programu. Takový software průběžně a bez zásahu lidského administrátora skenuje soubory uložené ve službě cloud computingu za účelem detekce škodlivého kódu. Tyto operace probíhají na základě předem nastavených algoritmů a konfigurací systému, nikoli na základě individuálního lidského rozhodnutí. Jenom zaznamenávat každou jednotlivou rutinní antivirovou kontrolu nebo operaci čtení a zápisu při skenování by představovalo generování ohromného množství údajů. V obecné rovině by požadavek shromažďovat provozní údaje o činnostech provedené technickými aktivy představoval nepřiměřenou a prakticky neproveditelnou zátěž.

Důvodová zpráva uvádí, že požadavek na zaznamenávání provozních údajů a jejich náležitostí je obecně zaveden z důvodu, že takové události mohou být klíčové pro vyšetřování útoku nebo bezpečnostního incidentu. Tomuto záměru rozumíme a podporujeme jej, ale domníváme se, že doplnění pojmu „*technická aktiva*“ tento účel neřeší a původní požadavek spíše komplikuje, než přispívá ke zvýšení bezpečnosti. Povinnost nejasné evidence nízkoúrovňových operací z praktického hlediska neposkytne relevantní informace pro účely vyšetřování incidentů, naopak by takový požadavek mohl vést k zahlcení provozních logů nepodstatnými údaji, které by paradoxně mohly zkomplikovat efektivní detekci skutečně závažných incidentů.

Pro úplnost uvádíme, že pojem „*technická aktiva*“ byl doplněn také do řádku 5.5 písm. e) přílohy vyhlášky, kde se stanovuje požadavek na shromažďování údajů o činnostech technických aktiv na straně orgánu veřejné správy. Navrhujeme zvážit, zda z obdobných důvodů, jaké uvádíme výše, není vhodné tento pojem odstranit i z tohoto ustanovení.

Tato připomínka je zásadní.