SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Stanovisko Svazu průmyslu a dopravy ČR k materiálu Návrh vyhlášky o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci
Č. J.	39/2022
DATUM ZPRACOVÁNÍ	9. května 2022
KONTAKTNÍ OSOBA	Ing. Kateřina Kalužová
TELEFON	225 279 202
E-MAIL	kkaluzova@spcr.cz

Svaz průmyslu a dopravy ČR předkládá tyto připomínky k materiálu Návrh vyhlášky o bezpečnostních pravidlech pro využívání služeb cloud computingu orgány veřejné moci. Jedná se o společné připomínky Svaz průmyslu a dopravy ČR, ICT Unie a Hospodářské komory ČR.

OBECNÁ ČÁST

Svaz průmyslu a dopravy ČR (dále jen SPČR) vítá snahu o vytvoření přehledného a jednoduchého seznamu bezpečnostních pravidel pro poskytování služeb cloud computingu. Jednoznačně podporujeme, že při využívání cloudových služeb je nezbytné zajistit důvěrnost, integritu a dostupnost dat. Oceňujeme, že již během projednávání předchozích cloudových vyhlášek se nám v této oblasti podařilo s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) dosáhnout konsensu.

Bohužel se obáváme, že podoba, v jaké byl tento návrh vyhlášky předložen do mezirezortního připomínkového řízení, bude zdrojem extrémní administrativní zátěže nejen pro orgány veřejné moci (dále jen OVM), ale i pro soukromý sektor. Hrozí tak značné zpomalení zavádění pokročilých služeb veřejné správy, které by mohlo mít negativní dopady i na konkurenceschopnost České republiky v mezinárodním srovnání (např. v rámci indexu DESI[1], který dlouhodobě upozorňuje na to, že zavádění digitálních veřejných služeb je v ČR pomalé[2]). To potvrzuje i zpráva NKÚ o digitalizaci, která zdůrazňuje, že digitalizace se zatím nedostatečně projevuje ve zvýšení účinnosti procesů a efektivitě veřejné správy a je jedním z důležitých nástrojů zlepšení fungování státu.

Samotný seznam bezpečnostních pravidel je značně přísnější, než jak je požadováno na základě vyhlášky o kybernetické bezpečnosti (dále jen VKB) pro on-premise řešení i přesto, že kybernetické hrozby jsou v zásadě stejné pro cloud i pro on-premise řešení. Pro využití cloud computingu se uvedeným množstvím detailních kontrolních bodů v podobě pravidel pro OVM popírá smysl průmyslové certifikace rodiny ISO 27000, jejíž plnění je standardně kontrolováno nezávislými auditory.

Očekávali jsme, že v souladu se zmocněním v zákoně o kybernetické bezpečnosti (dále jen ZKB) v § 6, bod e), bude tato vyhláška obsahovat primárně požadavky na OVM, tzn. jakým způsobem mají v jednotlivých bezpečnostních úrovních konfigurovat a využívat cloudové služby, které již prošly zápisem do Katalogu cloud

[1] Meziročně si v roce 2021 ČR o jedno místo pohoršila a skončila mezi 27 členskými státy EU na 18. místě", viz https://www.nku.cz/cz/pro-media/tiskove-zpravy/nku-ve-vyrocni-zprave-hodnoti-fungovani-statu--za-minuly-rok-poukazal-na-radu-nehospodarnych-a-neefektivnich-postupu-statu--systemove-problemy-i-neudr-id12472/

[2] https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

computingu dle pravidel v ZoISVS a především pak vyhlášce č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (CV1). Vycházíme z předpokladu, že veřejná správa smí dle ZoISVS § 6l využívat pouze cloudové služby, které již byly ověřeny dle ex-ante kontrol v CV1, které byly certifikovány a které jsou kontinuálně dokládány jako stále certifikované dle ISO 27000 od příslušných akreditovaných autorit (pro BÚ2 a vyšší). Není nám proto jasný důvod, proč by OVM měly znovu ověřovat detaily opatření, které již byly prověřeny dle CV1 a v rámci mezinárodně certifikovaných standardů ISO (podrobněji viz níže).

Rovněž normativy v oblasti rizik uložení a zpracování zákaznických dat mimo EU by měl být v souladu se stávající evropskou standardizací, zejména se standardem BSI C5, a neměly by jít nad tuto úroveň.

V současné chvíli považujeme za zcela zásadní, aby byly vyjasněny základní principy, kterými by se vyhláška měla řídit. K jednotlivým kritériím pak navrhujeme uspořádání separátního jednání.

ZÁSADNÍ KONCEPČNÍ PŘIPOMÍNKY

1. **Předložený návrh nenaplňuje základní cíle deklarované v "odůvodnění"**, tedy **zavedení jednoduchých a přehledných bezpečnostních pravidel** pro využívání služeb cloud computingu ze strany OVM. Důvodem je zejména duplicita s CV1 a nevyužívání zavedených standardů a certifikací prostřednictvím akreditovaných certifikačních autorit:
    a. Postrádáme odůvodnění, zda a proč je záměrem současného návrhu bezpečnostních pravidel v mnoha případech jít nad rámec zavedených standardů (ISO 27001, ISO 27017, ISO 27018) i nad rámec nedávno zavedených regulací v jiných zemích EU, zejména německé BSI C5. U některých požadavků je nejasné, zda pouze kopírují požadavky těchto standardů nebo zavádějí přísnější nebo odlišný standard. Vzhledem k těmto nejasnostem je návrh bohužel celkově nepřehledný.
2. Jiná navrhovaná pravidla jsou vysloveně duplicitní (nadbytečná) k již vyžadované certifikaci ISO 27000, a pouze opakují kontrolní body, které jsou vyžadovány pro samotné získání této certifikace. **Předložený návrh nezjednoduší ověřování kybernetické bezpečnosti služeb**, které jsou již právně zakotvené formou ex-ante kontroly poskytovatele nabízeného cloud computingu ve vyhlášce CV1. Jejím účelem je zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona a oprostit tak OVM od provádění obecných a opakujících se kontrol bezpečnostních opatření u poskytovatelů. Podrobněji:
    a. Některé z navrhovaných pravidel kopírují stávající kontrolní body z CV1, tedy certifikační kritéria, kterými poskytovatelé musí projít, aby jejich nabídky byly vůbec zařazeny do Katalogu cloud computingu a aby směli tyto služby nabízet veřejné správě. Jsme přesvědčeni, že požadavky na technická řešení kybernetické bezpečnosti na straně poskytovatele, která se neliší pro jednotlivé zákazníky, by z praktických důvodů neměly být předmětem opakované kontroly ze strany zákazníků (v rámci CV2). Naopak by měly být předmětem ex-ante kontroly, primárně v rámci CV1. Přijetí vyhlášky v navržené podobě by způsobilo přenesení významné administrativní a regulatorní zátěže na OVM. Už nyní se jedná o velmi náročný administrativní proces pro samotné poskytovatele cloudových služeb v rámci požadavků CV1, proto považujeme za žádoucí, aby nastavení celého procesu ověřování dle CV2 bylo podrobeno odborné diskuzi na základě jejich dosavadních zkušeností.
    b. V předkládaném návrhu postrádáme zdůraznění skutečného využití nástrojů a funkcí kybernetické bezpečnosti (jako např. vícefaktorová autentizace nebo šifrování dat v úložišti), které dle CV1 musí poskytovatelé nabízet. Není nám však jasný způsob, jak by se kontrolovala

jejich skutečná implementace u OVM. Namísto toho vidíme v návrhu CV2 řadu dalších obecných pravidel pro poskytovatele cloud computingu.

c. Rozsah navrhovaných bezpečnostních pravidel pro OVM jde i nad rámec stávající VKB. Zavádí se tím jistý určitá nerovnost, kdy na provoz systémů v režimu on-premise se uplatňuje pouze VKB, zatímco na provoz systémů využívajících cloud computing se uplatňuje celá řada dalších požadavků. Toto je v rozporu se skutečností, že velká většina kybernetických hrozeb se uplatňuje srovnatelně na systémy využívající cloudové služby, stejně tak jako na systémy v režimu on-premise. Jistý rozdíl je např. v oblasti zpřístupňování zákaznických dat vyšetřujícím orgánům mimo ČR, avšak tento rozdíl je již předmětem podrobné dodatečné regulace v rámci CV1. Není tedy jasné, proč se na systémy využívající cloud computing uplatňují v oblasti technických opatření přísnější pravidla.

3. **Předložený návrh vede k dodatečným nákladům státu na IT řádu miliard korun**. Za značně problematické považujeme, že součástí návrhu vyhlášky není hodnocení dopadů regulace (RIA) - zejména vyhodnocení dodatečných nákladů na straně soukromého sektoru i veřejného sektoru. Konstatování, že vyhláška nebude mít vliv veřejné rozpočty ani podnikatelské prostředí, jak je uvedeno v odůvodnění, považujeme za zcela nedostatečné a nedopovídající realitě.
    a. Požadavky vyplývající z návrhu vyhlášky mají být, na základě zmocnění v § 6 písm. e) ZKB, uplatněna pro všechna OVM, a to včetně místní veřejné správy, na kterou je využívání komerčních cloudových služeb zejména cíleno (sdílené služby SaaS). Navrhovaný seznam pravidel se zdá být nad rámec možností místní veřejné správy a menších úřadů. Nadměrný rozsah pravidel tak může způsobit percepci nesplnitelnosti, a menší OVM mohou na akceptaci CV2 rezignovat s tím, že NÚKIB nebude schopen provádět kontrolu jejího naplnění pro cca 7.000 OVM v ČR. Bylo by účelnější formulovat jednodušší sadu pravidel, která by byla brána jako skutečně splnitelná a zároveň odpovídala požadavkům na adekvátní úroveň zabezpečení.
    b. Jednoduchým příkladem dodatečných nákladů pro celou veřejnou správu je odhad náročnosti posouzení a dokumentace aplikace volitelných kritérií definovaných v příloze 2 vyhlášky. Tyto náklady tvoří jen menší část celkových nákladů na zajištění souladu s navrhovanou vyhláškou. Vycházíme z následujících faktů
        - Náklady na práci zaměstnance úřadu: 562 Kč/hodinu (celkové náklady 90 tis. Kč /měsíc)
        - Rozsah úkonů: povinné vyhodnocení aplikovatelnosti 180 volitelných opatření v 9 aspektech vyhlášky, kde každý úkon vyhotoven za 30 minut =>
        - Celková časová dotace: 810 hodin posouzeni pro jeden typ cloudové služby
        - Celková cena 455 tis. Kč na posouzení jedné cloudové služby
        - Předpoklad použití 5 různých typů cloudových služeb jedním úřadem: 2.276.000,- Kč
        - **Pro 1000 úřadů (z celkového počtu 7000): celkové náklady státu 2.3 mld Kč**
4. **Předložený návrh vytváří obrovskou administrativní zátěž.** Podle předkládaného návrhu by OVM, jen v rámci vyhodnocování nezbytnosti požadavků dle přílohy 2 pro běžný agendový systém zahrnující 15 cloudových služeb, muselo vyhotovit **písemný záznam o posouzení nezbytnosti 24 tisíc dílčích požadavků**[3]. K tomu musí každé OVM naplnění nezbytných pravidel vyhodnotit a zdokumentovat. Dále

[3] Dle § 3 a § 4 návrhu vyhlášky musí OVM pro každé ze 180 volitelných pravidel (viz Příloha 2) a pro každý zamýšlený "typ cloud computingu" provést předepsanou analýzu (dle § 4 odst. (5)) nezbytnosti daného volitelného pravidla a to z 9 různých aspektů (viz body a) až i) tamtéž). O tomto posouzení je třeba vyhotovit písemný záznam a archivovat jej po dobu 10 let. Prakticky to znamená, že pro cloudový agendový systém, které využívá typicky 15 typů cloudových služeb (z katalogu CC), by dané OVM muselo provést 180 x 15 x 9 aspektů = 24.300 úkonů posouzení nezbytnosti.

musí vyhodnotit a zdokumentovat ještě splnění všech povinných pravidel dle přílohy 1. To vytváří administrativní zátěž, která je objektivně nepřiměřená i pro ty největší organizace, natož pak pro menší OVM. Rozdělení bezpečnostních pravidel na část povinnou (viz Příloha 1) a část volitelnou (viz Příloha 2) administrativní zátěž nijak nesnižuje, naopak ji dále zvyšuje z důvodu požadavku na vyhodnocování nezbytnosti volitelných požadavků. Menší úřady mohou rezignovat na volitelnost pravidel dle Přílohy 2 a budou se naopak snažit maximum těchto pravidel smluvně přesunout na poskytovatele, což poskytovateli bude odmítáno jako požadavky nad rámec jejich odpovědnosti ve smluvním vztahu, případně mohou OVM na naplňování požadavků legislativy zcela rezignovat.

Předložený návrh vyhlášky může výrazně zpomalit digitalizaci státní správy. Administrativní zátěž, kterou navrhovaná vyhláška přináší, vytvoří značné bariéry pro digitalizaci státní správy. Cloudová řešení, která by za běžných okolností byla vhodným nástrojem digitalizace, bude velmi administrativně a finančně náročné implementovat. Hrozí tak značné zpomalení digitalizace služeb veřejné správy. Navrhovaná úprava může ohrozit plánovaný časový harmonogram implementace práv občanů na digitální služby a v neposlední řadě i konkurenceschopnost České republiky v mezinárodním srovnání (viz odkazy na str. 1).

Návrhy řešení:

a. Navrhujeme vypustit všechny požadavky, které pouze duplikují mezinárodní standardy (ISO 27001, ISO 27017, ISO 27018). Tyto duplicitní požadavky generují obrovskou administrativní zátěž, ale nijak nezvyšují faktickou úroveň kybernetické bezpečnosti.
b. Pokud navrhovaná vyhláška v některých bodech zamýšlí zavést přísnější požadavky, než vyžadují mezinárodní standardy, navrhujeme tyto formulovat jako výslovné odchylky od mezinárodních standardů a jejich zavedení řádně odůvodnit. Tato přísnější pravidla navrhujeme do maximální možné míry harmonizovat s německým standardem BSI CS, aby nedocházelo k neodůvodněné fragmentaci požadavků v rámci EU.
c. Navrhujeme vypustit všechny požadavky na parametry cloudových služeb, které se odchylují od požadavků v CV 1. Smyslem CV 1 je centralizovaně ověřit způsobilost cloudových služeb pro nasazení ve veřejné správě. Navrhované vyhláška by tedy neměla vyžadovat opětovné ověření splnění těchto požadavků ze strany OVM a měla by se zaměřit pouze na dodatečná opatření na straně OVM.
d. Navrhujeme vypustit všechny požadavky, které již vyplývají ze stávající právní úpravy, zejména VKB. U OVM, které nejsou povinnými subjekty dle ZKB, navrhujeme upřednostnit regulaci formou doporučených minimálních bezpečnostních standardů.

Žádost o prodloužení lhůty konzultace

Vzhledem k velkému množství detailních požadavků, které jsou ve vyhlášce obsaženy, zároveň navrhujeme prodloužit délku připomínkového řízení alespoň o jeden měsíc, aby se všechny dotčené subjekty mohly řádně seznámit se všemi navrhovanými požadavky a mít dostatečný prostor k podání případných připomínek.