SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Stanovisko Svazu průmyslu a dopravy ČR k materiálu Návrh vyhlášky o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.
Č. J.	33/2021
DATUM ZPRACOVÁNÍ	5. května 2021
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 úrovních pro využívání cloud computingu orgány veřejné moci. Jedná se o společné připomínky Svaz průmyslu a dopravy ČR, ICT Unie a Hospodářské komory ČR.

OBECNÉ ZÁSADNÍ PŘIPOMÍNKY

PŘIPOMÍNKA Č. 1

Domníváme se, že předkladatel neposkytl dostatečně jasné a určité vysvětlení některých kritérií uvedených v návrhu vyhlášky (a to ani v rámci důvodové zprávy k jejímu návrhu), které blíže rozebíráme dále v rámci konkrétních připomínek.
Navrhujeme vyjasnit vztah předkládaného materiálu se zákonem č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen „**ZoISVS**“), respektive ZoISVS ve znění sněmovního tisku 756, který je v současné době v legislativním procesu v Poslanecké sněmovně (dále jen „**DEPO ZoISVS**“). Podle § 2 odst. w) DEPO ZoISVS platí, že bezpečnostní úrovní cloud computingu se rozumí *„bezpečnostní úroveň pro využívání cloud computingu orgány veřejné moci podle právního předpisu upravujícího kybernetickou bezpečnost“*; tj. platí, bezpečnostní úroveň má být stanovena podle § 6 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „**ZKB**“). Z předkládaného návrhu ani jeho důvodové zprávy však není zcela jasné, že navrhovaný materiál stanovuje bezpečnostní úrovně pro účely katalogu cloud computingu ve smyslu DEPO ZoISVS, nikoliv pouze § 6 písm. e) ZKB . Navrhujeme proto vyjasnit, že bezpečnostní úrovně vymezené v předkládaném materiálu zároveň slouží jako bezpečnostní úrovně ve smyslu § 6 písm. e) ZKB rovněž pro účely katalogu cloud computingu ve smyslu ZoISVS, resp. DEPO ZoISVS.

KONKRÉTNÍ ZÁSADNÍ PŘIPOMÍNKY

PŘIPOMÍNKA Č. 1

Ke kritériím pro stanovení dopadu kybernetického bezpečnostního incidentu

V odst. 2 přílohy č. 1 materiálu navrhujeme následující úpravu:
„(2) Při zjišťování nejhoršího možného dopadu kybernetického bezpečnostního incidentu zohlední orgán veřejné moci ~~zejména~~ možné narušení dostupnosti, důvěrnosti a integrity poptávaného cloud computingu a povahu informačního nebo komunikačního systému, který je poptávaným cloud computingem, jako celku. V případě, že je poptávaným cloud computingem pouze určitá část informačního nebo komunikačního systému, zohlední také vztah této části k bezpečnostní úrovni informačního nebo komunikačního systému jako celku.“

Odůvodnění:

Domníváme se, že hodnotící kritéria pro zařazení poptávaného cloudu computingu do dané bezpečnostní úrovně je nezbytné stanovit taxativním způsobem. Pro zařazování do bezpečnostní úrovně tedy orgány

veřejné moci musí hodnotit dopady kybernetického bezpečnostního incidentu na standardní bezpečnostní triádu – dostupnost, důvěrnost a integritu poptávaného cloud computingu. Orgány veřejné moci by v rámci kategorizace poptávaného cloud computingu do bezpečnostní úrovně neměly zvažovat jiné aspekty.
Zároveň platí, že se hodnotí nejhorší možné dopady kybernetického bezpečnostního incidentu. Definice kybernetického incidentu přitom sama v sobě již zahrnuje požadavky na zajištění dostupnosti, důvěrnosti a integrity; proto není třeba ji dále rozvíjet:

- **kybernetický bezpečnostní** incident je definován v § 7 odst. 2 ZKB jako *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“*
- **kybernetická událost** je definována v § 7 odst. 1 ZKB jako *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.“*
- **bezpečnost informací** je definována v ustanovení § 2 písm. c) ZKB jako *„zajištění důvěrnosti, integrity a dostupnosti informací a dat“.*

PŘIPOMÍNKA Č. 2

K bezpečnostní úrovni „4. Kritická“

Návrh: V tabulce specifikující oblasti dopadu v bezpečnostní úrovni „4. Kritická“ navrhujeme následující úpravy:

OBLAST DOPADU	**KRITÉRIUM PRO URČENÍ BEZPEČNOSTNÍ ÚROVNĚ „4. KRITICKÁ“**
Bezpečnost a zdraví osob	Může vést ke zranění více než 2 500 osob nebo přímému ohrožení nebo ztrátě života více než 250 osob.
Ochrana osobních údajů	Může vést k porušení povinností spojených se zpracováním osobních údajů, které je nezbytné pro plnění úkolu a výkon veřejné moci za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech, nebo k zajišťování obranných a bezpečnostních zájmů České republiky.
Trestněprávní řízení	Může vést k závažnému a dlouhodobému narušení schopnosti vyšetřovat trestnou činnost nebo zpochybnění soudního řízení v rámci orgánů činných v trestním řízení.
Veřejný pořádek	**Může způsobit závažné omezení řádného fungování kritické infrastruktury** ~~Může být dotčena kritická infrastruktura~~ a může zapříčinit hromadné nepokoje nebo jinak závažně narušit veřejný pořádek s celostátními dopady.
Mezinárodní vztahy	Může negativně ovlivnit nebo poškodit diplomatické vztahy České republiky.
Řízení a provoz	**Může způsobit závažné omezení řádného fungování kritické infrastruktury** ~~Může být dotčena kritická infrastruktura~~ a může narušit řádné fungování části nebo celého orgánu veřejné moci, přičemž může závažně omezit nebo zastavit provádění důležitých

	činností orgánu veřejné moci a narušit řízení, poškodit rozvoj nebo poškodit prosazování cílů a zájmů orgánu veřejné moci.
Důvěryhodnost	**Může způsobit závažné omezení řádného fungování kritické infrastruktury** ~~Může být dotčena kritická infrastruktura~~ a může negativně ovlivnit vztahy s jinými částmi orgánu veřejné moci, jinými organizacemi nebo vztahy s veřejností a negativní následky mohou být dlouhodobě mezinárodní.
Finanční model	Může vést k finančním ztrátám přesahujícím 10 % běžných výdajů ročního rozpočtu orgánu veřejné moci a tyto ztráty odpovídají částce 10 000 000 Kč a vyšší, nebo může způsobit hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu. V případě, že výše finanční ztráty odpovídá částce nižší než 10 000 000 Kč, použije se úroveň dopadu vysoká.
Zajišťování služeb	**Může způsobit závažné omezení řádného fungování kritické infrastruktury** ~~Může být dotčena kritická infrastruktura~~ a může dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125 000 osob.

Odůvodnění:

Bezpečnostní úroveň „4. Kritická“ je určena pro nejvýznamnější informační systémy České republiky. Podle § 6l odst. 2 ZoISVS platí, že *„poskytovatelem cloud computingu zařazeného do nejvyšší bezpečnostní úrovně orgánu veřejné správy může být pouze státní poskytovatel cloud computingu.“*. Podle § 6m odst. 2 DEPO ZoSVS pak obdobně platí, že *„poskytovatelem cloud computingu poskytujícím orgánu veřejné správy cloud computing zařazený do nejvyšší bezpečnostní úrovně může být pouze poskytovatel státního cloud computingu.“*

Vzhledem k tomuto omezení je nezbytné, aby nejvyšší bezpečnostní úroveň (tj. „4. Kritická“) byla vymezena pouze ve vztahu k nejvýznamnějším informačním systémům provozovaným orgány veřejné moci. V opačném případě může docházet k nežádoucímu výkladovému rozšiřování těchto kritérií, což může vést k uzavření trhu se službami cloud computingu – tj. došlo by k nežádoucímu rozšiřování služeb cloud computingu, které by mohly být poskytovány pouze státním poskytovatelem cloud computingu, čímž by došlo k vyřezaní komerčních služeb z trhu. Z tohoto důvodu je nezbytné, aby veškeré služby cloud computingu zařezané do této bezpečnostní úrovně byly co nejužším způsobem vázány na bezpečnost státu a tedy na prvky kritické infrastruktury. Pro určování prvků kritické infrastruktury přitom existuje daný postup podle zákona č. 240/2000 Sb., krizový zákon, a souvisejícího nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Touto vyhláškou by nemělo docházet k vytváření nového procesu určování těchto kritických prvků, které jsou zásadní pro fungování státu, ale pouze k provázání s již existujícími pravidly. Navrhujeme proto, aby bylo stanoveno, že dopady kybernetického bezpečnostního incidentu musejí mít zásadní vliv na řádné fungování takto určeného prvku kritické infrastruktury. Takový zásadní vliv by pak měl být vykládán ve smyslu nařízení vlády č. 432/2010 Sb., kde bude platit, že by takový poptávaný cloud computing by nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin.

Alternativně by pak bylo možné stanovit, že se kybernetický incident může způsobit závažné omezení řádného fungování kybernetické informační infrastruktury, čímž by bylo vyjasněno, že poptávaný cloud computing musí mít zásadní dopad na nejzásadnější informační systémy státu.

PŘIPOMÍNKA Č. 3

K důvodové zprávě k oblasti dopadu „poskytování služeb“ v bezpečnostní úrovni „4. Kritická“

Pro zařazení poptávaného cloud computingu do bezpečnostní úrovně „4. Kritická“ v rámci oblasti dopadu „Poskytování služeb“ (ve výše navrhovaném znění) platí, že kybernetický bezpečnostní incident *„může způsobit závažné omezení řádného fungování kritické infrastruktury a může dojít k rozsáhlému omezení poskytování nezbytných služeb nebo jinému závažnému zásahu do každodenního života postihujícího více než 125 000 osob.“*

Pro vyloučení pochybností a dosažení žádoucí míry právní jistoty navrhujeme v důvodové zprávě (důvodová zpráva k příloze č. 1, poslední odstavec bodu I, str. 26) vyjasnit pojem *„závažný zásah“*, a to následovně:

„Narušení dostupnosti, důvěrnosti nebo integrity systému nebo jeho části může narušit kvalitu plnění zákonných povinnosti orgánu veřejné moci, což se projeví na kvalitě služeb poskytovaných pro více než 125 000 osob, přičemž musí platit, že ~~je potenciálním~~ dopadem **kybernetického incidentu je závažně omezeno řádné fungování** ~~dotčen prvek~~ **prvku** kritické infrastruktury. **Za takový závažný zásah kybernetického incidentu nelze považovat pouze potenciální dopady, ale reálné a iminentní dopady do každodenního života těchto osob, které v důsledku takového kybernetického incidentu ztratí možnost využívat nezbytné služby poskytované státem, resp. ztratí možnostse státem jakýmkoliv způsobem komunikovat. Omezení se musí týkat nezbytných služeb poskytovaných občanům a jejichž omezení tedy může znamenat závažný zásah do každodenního života těchto osob. Za takový závažný zásah přitom nelze považovat situace, kde osoby mají alternativní způsoby takových elektronických služeb nebo elektronické komunikace se státem. Proto např. platí, že portály určené pro komunikaci s orgány veřejné moci nebo portály sloužící jako rozcestníky pro služby poskytované orgány veřejné moci (jako je např. Portál občana) nelze zařadit do bezpečnostní úrovně „4. Kritická“, pokud existuje obdobně komfortní a bezpečná alternativa takového elektronického portálu nebo možností bezpečné komunikace s tímto orgánem veřejné moci – zde např. prostřednictvím datových schránek. Toto omezení je však rozhodné toliko pro nezbytné služby, nikoliv potom pro jiný závažný zásah, neboť ten je doplňující alternativou k omezení poskytování nezbytných služeb. V případě dostupnosti alternativ (pro jiné než nezbytné služby) nelze uvažovat o naplnění daného kritéria.** Hranice 125 000 osob odpovídá průřezovému kritériu pro určení kritické informační infrastruktury podle nařízení č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.“

DOPORUČUJÍCÍ PŘIPOMÍNKY

PŘIPOMÍNKA Č. 1

K důvodové zprávě k oblasti dopadu „finanční model“

V důvodové zprávě k finančnímu modelu (tj. důvodová zpráva k příloze č. 1, bod h, str. 23 a násl.) rovněž pro vyloučení pochybností navrhujeme důvodovou zprávu doplnit o následující upřesnění výkladu oblasti dopadu Finančního modelu v rámci kritické bezpečnostní úrovně:

Kritérium „Finančního modelu“ nezahrnuje ani nijak neodráží vstupní investici do daného cloud computingu, resp. informačního či komunikačního systému. Zvažovaná ztráta musí odpovídat skutečně vzniklé škodě, a to v souladu s pravidly pro vyčíslování škody (újmy), např. ve smyslu § 2894 an. zákona č. 89/2012 Sb., občanský zákoník, nebo např. zákona č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem. Vstupní investice do daného informačního nebo komunikačního systému tak nemůže představovat zvažovanou hodnotu pro naplnění tohoto kritéria. Výpadkem provozu daného ICT systému nikdy nemůže dojít k jeho úplné destrukci, která by mohla v krajním případě odpovídat skutečné škodě ve výši vstupní investice, považujeme za vhodné toto kritérium v důvodové zprávě uvést výslovně jako nepřípustné pro posuzování výše finanční ztráty.