SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Návrh vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat
Č. J.	GŘ/10/SHP/2018
DATUM ZPRACOVÁNÍ	9. března 2018
KONTAKTNÍ OSOBA	Mgr. Ondřej Ferdus
TELEFON	225 279 207
E-MAIL	oferdus@spcr.cz

OBECNÉ PŘIPOMÍNKY

Účelem navrhované vyhlášky o kybernetické bezpečnosti by mělo být, stejně jako u novely zákona o kybernetické bezpečnosti implementující požadavky směrnice NIS z roku 2016, stanovit taková pravidla kybernetické bezpečnosti, která nepůjdou nad rámec stávajících povinností subjektů (správců a provozovatelů) prvků kritické informační infrastruktury (KII), resp. je omezí v co možná nejmenším rozsahu. Předkládaný návrh vyhlášky jde však zjevně nad rámec tohoto obecného vztahu obou právních předpisů (směrnice / zákona) a fakticky tak rozšiřuje povinnosti nejen pro nové provozovatele základních služeb, ale i pro stávající subjekty KII.

KONKRÉTNÍ ZÁSADNÍ PŘIPOMÍNKY

Připomínka k § 2
a) Do definic požadujeme doplnit definici vrcholového vedení s využitím textu definice uvedené v ČSN EN ISO/IEC 27000 bod 2.84 s následujícím textem:
„Vrcholové vedení osoba nebo skupina lidí, kteří na nejvyšší úrovni řídí a kontrolují orgán nebo osobu, jež je povinna zavést bezpečnostní opatření podle zákona. Vrcholové vedení má pravomoc delegovat oprávnění a poskytovat zdroje v rámci tohoto orgánu nebo osoby.“

Odůvodnění:
Z navrženého znění § 3 odst. 1 písmeno a), kde je uvedena tzv. nepřímá definice vrcholového vedení (ovšem bez bližšího popisu), není zřejmé, kdo konkrétně je tímto vrcholovým vedením míněn. Protože návrh vyhlášky přebírá ustanovení zakotvená ČSN EN ISO/IEC 27001 požadujeme jednoznačně definovat pojem vrcholového vedení, tak aby byl v souladu s definicí uvedenou v ČSN EN ISO/IEC 27000 bod 2.84.

b) Definovat i další pojmy použité z výše uvedené normy ČSN EN ISO/IEC 27000.

Odůvodnění:
Norma ČSN EN ISO/IEC 27001 je přepsána do návrhu vyhlášky. Pro účely této normy platí definice pojmů uvedené ČSN EN ISO/IEC 27000, které jsou jednoznačné a jasně pochopitelné, což vyhláška nedělá. To následně vede k nejednoznačnosti/nepochopení/ resp. možnosti odlišného výkladu textace vyhlášky a uvedených norem, což by mohlo vést k obtížné naplnitelnosti některých požadavků stanovených vyhláškou.

Připomínka k § 6 odst. 1 písm. d) a l)
Požadujeme vypustit tato písmena z úkolů, které zajišťuje vrcholové vedení a doporučujeme i u některých dalších písmen zvážit jejich přesun do zodpovědnosti výboru pro řízení kybernetické bezpečnosti.

Odůvodnění:
Komunikace s dotčenými stranami by měla plně spadat do kompetence výboru pro řízení kybernetické bezpečnosti stejně jako testování plánů kontinuity, který je výkonným orgánem určeným pro oblast kybernetické bezpečnosti. V tomto výboru má vrcholové vedení své zastoupení jedním ze svých členů. Jde o to nezatěžovat nad únosný rámec celé vrcholové vedení, a to zejména u organizací, jejichž hlavní business je zcela jiný a proto doporučujeme i u některých dalších písmen zvážit jejich přesun do zodpovědnosti výboru pro řízení kybernetické bezpečnosti.

a) Připomínka k § 7 odst. 1 písm. c)
Stávající text požadujeme nahradit následujícím zněním:
„c) bezpečnostní opatření navržená manažerem kybernetické bezpečnosti musí být schválena výborem pro kybernetickou bezpečnost nebo vrcholovým vedením.“

Úplné znění s vyznačením změn:
~~*c) nesmí vykonávat role odpovědné za provoz informačních a komunikačních systémů.*~~
„c) bezpečnostní opatření navržená manažerem kybernetické bezpečnosti musí být schválena výborem pro kybernetickou bezpečnost nebo vrcholovým vedením.“

b) Připomínka k § 7 odst. 2 písm. c)
Stávající text požadujeme nahradit následujícím zněním:
„c) bezpečnostní opatření navržená architektem kybernetické bezpečnosti musí být schválena výborem pro kybernetickou bezpečnost nebo vrcholovým vedením.“

Úplné znění s vyznačením změn:
~~*c) nesmí vykonávat role odpovědné za provoz informačních a komunikačních systémů.*~~
„c) bezpečnostní opatření navržená architektem kybernetické bezpečnosti musí být schválena výborem pro kybernetickou bezpečnost nebo vrcholovým vedením.“

Odůvodnění k oběma připomínkám:
Vyhláška ukládá oddělení manažera i architekta kybernetické bezpečnosti od provozu a zároveň povinnost zajistit zastupitelnost těchto rolí, přičemž zajištění externími partnery vnímáme jako značně problematické. Z reálné praxe víme, že osoba zodpovědná za provoz informačních a komunikačních systémů je nejlépe informována a zkušená v dané problematice, zná detailně problematiku daného prostředí a příslušných systémů.
Proto navrhujeme oddělit pravomoci manažera i architekta kybernetické bezpečnosti při navrhování opatření na snížení rizik od schvalovacího procesu tak aby návrhy těchto odborně znalých osob podléhaly následnému schválení výboru pro KB nebo vrcholovému vedení.

Připomínka k § 14 odst. 1 písm. b) bod 1. a k § 24 – pojmy „průběžné vyhodnocování“ a „nepřetržité vyhodnocování“:

Navrhujeme do vyhlášky sjednotit oba pojmy a použít všude jen pojem „průběžné vyhodnocování“, doplnit jeho definici a rovněž to, na základě jakých kritérií se stanoví interval vyhodnocování. Jedním z možných přístupů je, aby to bylo plně v kompetenci správce či provozovatele, pak by to mělo být explicitně v textu uvedeno.

Odůvodnění:
Není zřejmý rozdíl mezi použitými pojmy **„průběžné vyhodnocování“ a „nepřetržité vyhodnocování“,** přičemž podle našeho názoru mají v použitém kontextu prakticky stejný význam a proto se navrhuje jejich sjednocení. Tím, že návrh vyhlášky nedefinuje pojem „průběžné vyhodnocování“, se opět umožňuje odlišný výklad a nestanovuje se jednotný základ pro pochopení a implementaci.

Připomínka k § 19 odst. 5
Požadujeme za slova „podle odstavců 3 nebo 4“ vložit slova „**a je-li to technicky možné**“.

Úplné znění s vyznačením změn:
(5) V případě, kdy není možné splnit požadavek podle odstavců 3 nebo 4 ***a je-li to technicky možné,*** *musí nástroj pro ověřování identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, vynucovat pravidla*

Odůvodnění:
Řídící a dohledové systémy SCADA zpravidla díky svému stáří nebo použité technologii neumožňují zavedení pravidel zakotvených pod některými písmeny odst. 5, zejména pokud jde o minimální délku hesla, a to z technologického hlediska. Jejich plné zavedení by si v řadě případů vyžádalo neúměrně vysoké náklady na nové systémy či technologická zařízení, což by si vyžádalo přesun finančních prostředků z jiných oblastí hospodářských aktivit, včetně těch, které jsou předmětem hlavní činnosti orgánu nebo osoby, a to i na úkor jejich dalšího rozvoje, a to by byla celospolečenská ztráta.
Dále se domníváme, že heslo se 14 znaky povede k tomu, že si jej budou uživatelé zaznamenávat na papírky (pod klávesnici apod.)

Připomínka k § 22 odst. 1 a § 25 odst. 1 – pojem „důležitá aktiva“
Požadujeme upřesnit, tento pojem s využitím následujících možností:
a) Certifikovaný subjekt na základě provedeného hodnocení aktiv, určí důležitá aktiva v rámci vyhlášky o kybernetické bezpečnosti.
b) „Důležitá aktiva“ = „důležitá aktiva“
c) Každý správce či provozovatel si definuje metodiku a postupy vyhodnocení a zařazení mezi důležitá aktiva sám, nebo definovat metodiku či základní principy.

Odůvodnění:
Vyhláška nedefinuje, co je myšleno důležitými aktivy. Poskytuje tak opět prostor k různým výkladům, nepopisuje ani základní principy, jak je např. stanovit, nedefinuje povinnost stanovit metodiku, nebo třeba odvození od hodnocení aktiv.

Připomínka k § 28 odst.1
Stávající text požadujeme nahradit následujícím zněním: ***Orgán nebo osoba, které jsou povinny zavést bezpečnostní opatření podle zákona, pro zajištění bezpečnosti průmyslových a řídících systémů primárně používají nástroje a opatření, které zajistí***

Odůvodnění:

Na §28 by mělo být nahlíženo jako na speciální ustanovení, které má vždy v rámci aplikace na ICS a výkladu přednost před ostatními „obecnými“ ustanoveními vyhlášky.

Připomínka k § 28 odst.2
Primárním posláním ICS je zajištění principů SAFETY (např. vysoké dostupnosti a stability), teprve na 2. místě IT bezpečnosti (např. důvěrnosti). Striktní aplikace technických opatření předcházejících §§ může mít fatální dopady.

Připomínka k § 36 účinnost vyhlášky

Nesouhlasíme s navrženou účinností vyhlášky a požadujeme její odloženou účinnost od vyhlášení ve Sbírce zákonů, a to v závislosti na charakteru a rozsahu nově stanovených požadavků a době a nákladům na jejich realizaci, takže u těch nejnáročnějších by to mělo být až 18 měsíců od jejího vyhlášení ve Sbírce zákonů.Toto je možno vyřešit také zakotvením ustanovení do přechodných ustanovení, které by řešilo do kdy je nutné uvést dokumentaci do souladu s novou vyhláškou. Nová vyhláška přináší změny, jež se promítnou do dokumentace a navržený termín účinnosti 10. května 2018 by bez přechodného ustanovení znamenal, že povinné subjekty by měly mít dokumentaci „opravenou“ k tomuto datu, což je nereálné. Z tohoto důvodu navrhujeme tedy doplnit do vyhlášky přechodné období 1 rok od účinnosti nebo odložit její účinnost, jak je navrhováno výše.

Odůvodnění:

K datu účinnosti uvedeného v návrhu vyhlášky nebude s největší pravděpodobností ani dokončen legislativní proces. Přitom každé nové opatření či požadavek si vyžádá určitý čas na realizaci. Vzhledem k tomu, že finanční zdroje pro rok 2018 jsou již alokovány a není možné přesun rozpočtu na implementaci nových opatření, je nutné pro realizaci těch finančně a časově nejnáročnějších vytvořit dostatečný časový prostor. Dle návrhu má účinnost vyhlášky nastat za méně než tři měsíce ode dne zaslání připomínek, a to včetně povinnosti dle § 8 odst. 1 písm. f) vyhlášky zajistit „aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti uvedené v příloze č. 7 k této vyhlášce. Toto v praxi znamená, že všechny povinné osoby dle vyhlášky budou mít méně než tři měsíce na to, aby zrevidovaly obsah svých smluv s významnými dodavateli, a buď tyto smlouvy doplnily dodatkem, nebo je ukončily. Vzhledem k rozsahu požadavků uvedených v Příloze č. 7 se domníváme se, že takto stanovená povinnost nebude v řadě případů objektivně realizovatelná v navrhovaném krátkém čase do účinnosti vyhlášky. Je nutno vzít v potaz skutečnost, že pro řadu povinných osob se jedná o zcela nový požadavek, zasahující do již uzavřených smluv, které povinné osoby uzavíraly v dobré víře v době, kdy žádné požadavky na takovéto obsahové náležitosti stanoveny nebyly.

Splnění uvedené povinnosti totiž v oblasti soukromého práva naráží na zásadu „pacta sunt servanda“, tedy již jednou uzavřená smlouva zavazuje povinnou osobu po celou dobu její účinnosti. Povinná osoba samozřejmě může zahájit jednání o doplnění chybějících požadavků, nicméně tento proces do zajištění plného souladu s Přílohou č. 7 bude s vysokou mírou pravděpodobnosti trvat delší dobu než tři měsíce, a samozřejmě je podmíněn tím, že druhá strana bude s návrhem souhlasit. Pokud významný dodavatel návrh nebude akceptovat (například proto, že není objektivně schopen povinnost splnit, nebo i proto, že změnu smlouvy akceptovat nechce), povinná osoba bude muset smlouvu ukončit a přejít k jinému významnému

dodavateli. Ani tento proces ovšem není otázkou jednotek týdnů, ale spíše měsíců. Ukončení uzavřených smluv v některých případech nemusí být flexibilně možné, což platí zejména u smluv na nějakou delší dobu určitou, popřípadě u smluv, které předpokládají delší výpovědní doby či ukončení pouze k určitému výročí (automaticky a opakovaně se prodlužující smlouvy). I kdyby ukončení smlouvy bylo možné relativně flexibilně, povinný subjekt bude muset provést nové výběrové řízení a vybrat jiného významného dodavatele, který bude schopen plnění převzít a který bude splňovat veškeré požadavky vyhlášky – pokud má povinná osoba provést skutečně důkladný výběr nového významného dodavatele s přihlédnutí k významu dodávky, a uzavřít s ním smlouvu, opět toto nelze reálně zajistit v řádu několika málo týdnů.

Připomínka k celému textu vyhlášky

Vzhledem k tomu, že vyhláška je, až na některé body, obsahově shodná s ČSN EN ISO/IEC 27001. Pro praktickou aplikaci vyhlášky požadujeme vypracovat rozdílovou tabulku mezi návrhem této vyhlášky i její finální verzí vyhlášky a touto normou, aby bylo jasně definováno, co musí subjekt certifikovaný z hlediska normy ČSN EN ISO/IEC 27001 splnit nad rámec dané normy.

Připomínka k přechodným ustanovením

Požadujeme do přechodných ustanovení zakotvit problematiku vztahu a podoby dokumentace podle „staré“ vyhlášky č. 316/2014 Sb. a nové vyhlášky, která by stanovila nějakou formu – metodu, umožňující nezpracovávat z ekonomických důvodů úplně plně novou dokumentaci z důvodů pouhého přečíslování paragrafů a odstavců.

Připomínka k RIA

V důvodové zprávě není uvedena a zpracována RIA, a to z důvodu udělené výjimky a písmeno d) Předpokládaný hospodářský a finanční dosah navrhované právní úpravy na veřejné rozpočty a dopad na podnikatelské prostředí České republiky neobsahuje konkrétní počty a finanční vyčíslení. U některých společností odhadujeme náklady v řádů milionů korun. Požadujeme dopracovat a pokud nebude uvedeno nepokračovat v dalším legislativním procesu.

Připomínka k písm. f) Přílohy č. 7

Požadavek na smluvní zajištění, že dodavatel bude dodržovat interní politiky orgánu nebo osoby, které jsou povinny zavést bezpečnostní opatření dle zákona, považujeme v praxi za opět za velmi těžko realizovatelný, zejména pokud jde o nadnárodní korporace, které uplatňují celosvětově své vlastní bezpečnostní politiky. Například u globálních poskytovatelů cloudových služeb, nelze předpokládat, že by poskytovatel akceptoval konkrétní bezpečnostní politiku každého svého zákazníka, naopak sám má vytvořenou bezpečnostní politiky, které uplatňuje jako standard při poskytování služeb všem svým zákazníkům.

Z tohoto hlediska doporučujeme místo požadavku na smluvní zajištění povinnosti dodavatele dodržovat bezpečnostní politiky povinných osob stanovit povinnost povinné osoby před uzavřením smluvního vztahu si ověřit, zda bezpečnostní politiky významného dodavatele odpovídají úrovni bezpečnostních politiky povinné

osoby, případně jej v rozsahu, který není pokrytý interními politikami významného dodavatele, zavázat dodržovat požadavky na úrovni odpovídající interním politikám.

Připomínka k písm. h) Přílohy č. 7

Z věcného hlediska chápeme uvedený požadavek v kontextu změn ICT prostředí a rizik. Nepovažujeme však za vhodné stanovit toto opatření jako obligatorní součást smlouvy. Z hlediska závazkového práva a jeho principů totiž samotný závazek stran přezkoumat smlouvu nezajistí, že obsah smlouvy skutečně bude nějakým způsobem aktualizován. Ustanovení tedy nebude mít z právního hlediska materiální relevanci, ale bude se jednat pouze o závazek vyjednávat změnu v „dobré víře". Z tohoto důvodu bychom spíše navrhovali místo stanovení takto formální náležitosti smlouvy stanovit povinnost orgánu nebo osoby, které jsou povinny zavést bezpečnostní opatření, aby ve svých interních předpisech zakotvily povinnost na pravidelné bázi ověřovat aktuálnost obsahu smlouvy s významným dodavatelem z hlediska změn IT a rizik a případně zahájit jednání o aktualizaci smlouvy s významným dodavatelem

Připomínka k písm. j) bod 3) Přílohy č. 7

Dle našeho názoru je takto formulovaná povinnost zcela neurčitá, jelikož není nijak vymezeno, co je považováno za „významnou změnu kontroly". Není zřejmé, zda je tak myšleno např. „ovládání" společnost ve smyslu § 75 zákona č. 90/2012 Sb., o obchodních korporacích, nebo i něco jiného. Zároveň by bylo nutné rovněž vyjasnit pojem „významnosti" jelikož formulace naznačuje, že předmětem oznámení nemá být jakákoliv změna kontroly, ale pouze významná změna (předpokládáme, že pokud by se jednalo o změnu ovládající osoby např. nebude do tohoto spadat restrukturalizace společností ve skupině, ale např. vyvedení kontroly nad dodavatelem mimo skupinu již ano).

Takto neurčitě formulovaný požadavek by z právního hlediska bylo možné považovat dle našeho názoru za neplatný, při doslovném zakotvení požadavku do smlouvy by se k takovému jednání pro neurčitost v souladu s § 553 odst. 1 zák. č. 89/2012 Sb., občanského zákoníku zřejmě nepřihlíželo. Z tohoto důvodu navrhujeme ustanovení vyhlášky buď vypustit, nebo zpřesnit jeho obsah.

Zpřesnění považujeme za zcela klíčové i s ohledem na bod 3 písm. o) vyhlášky a právo odstoupit od smlouvy v případě významné změny. Pokud totiž nebude zcela jednoznačné, jaká situace z objektivního hlediska představuje „významnou změnu kontroly", uplatnění takového práva bude pro *orgán nebo osobu, které jsou povinny zavést bezpečnostní opatření podle zákona* extrémně rizikové kvůli potenciálním sporům s dodavatelem o ušlý zisk, pokud by soud následně tento neurčitý pojem vyložil jinak, případně celé ustanovení vyhodnotil jako zdánlivé právní ujednání pro neurčitost. Za takové situace by předmětné ustanovení jen těžko mohlo sloužit svému účelu, jelikož oprávněné osoby se budou zdráhat smlouvu ukončit s ohledem na riziko sporu ohledně objektivně nejasného vymezeného důvodu pro odstoupení.