AFCEA – SEMINÁŘ EGOVERMENT CLOUD
4. února 2020
-
Procesy eGC a jejich úprava z pohledu ZKB a jeho vyhlášek
-
Strategická rizika, vyplývající z využívání cloud computingu z pohledu regulátora
-
Kvalifikace dodavatelů, role "provozovatele" IS/KS ve smyslu ZKB

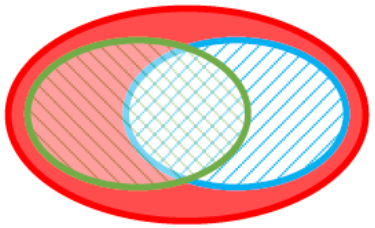
NÚKIB – ODBOR REGULACE

Procesy eGC a jejich úprava z pohledu ZKB a jeho vyhlášek

Cloudová vyhláška

- **Cíl – původně**
  - Vytvoření prováděcí vyhlášky k ZKB, která stanoví **obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu**
  - **Naplnit zmocnění:** § 6 písm. e) ZKB:
    - Stanovit vyhláškou obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.
- **Cíl – nově**
  - **Vedle výše uvedeného ještě ověření, zda cloudový poskytovatel splňuje základní bezpečnostní požadavky**
- **Východiska – věcná:**
  - Vztah zákona o ISVS k ZKB
  - Vychází z dokumentů projektu Příprava vybudování eGovernmentCloudu (usnesení vlády ČR č. 749 ze dne 14. listopadu 2018)
  - ISO 27001, 27017 a 27018 a další
- **Fáze:**
  - Vzhledem k změně cíle se hledá vhodná varianta
- **Účinnost:**
  - ?? 2020

Jak by mělo vypadat schéma schvalování cloudu - ZoPDS



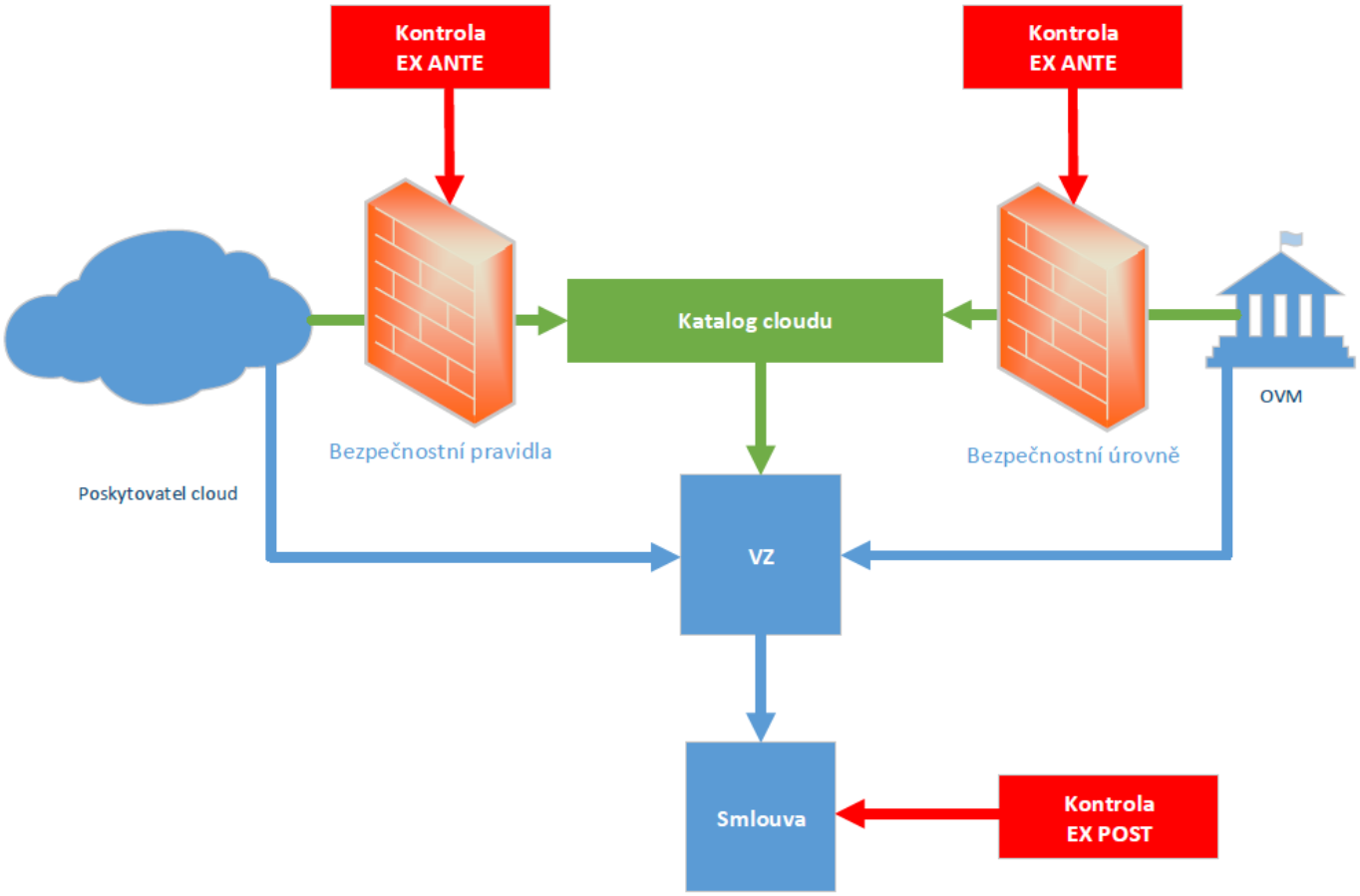
OVM

ZKB

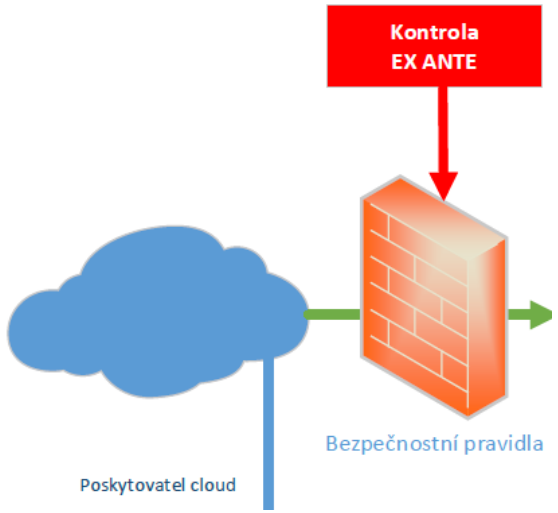
ZoISVS

4 varianty

1) OVM regulovaný ZKB a ZoISVS
2) OVM regulovaný ZKB, který není regulován ZoISVS
3) OVM regulovaný ZoISVS, který není regulován ZKB
4) OVM, který není regulován ZKB ani ZoISVS

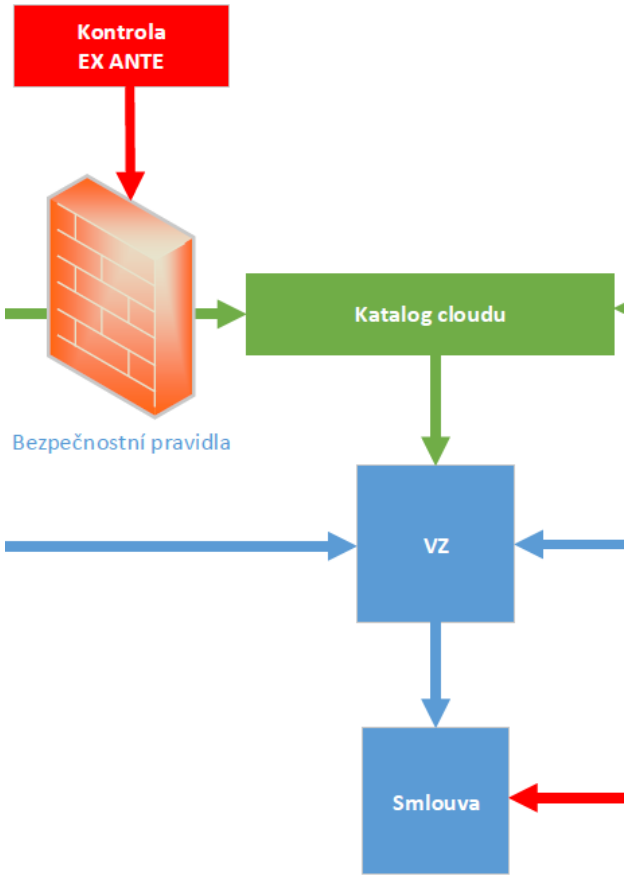


EX ANTE kontrola – vstup poskytovatele cloudu



- **Aby mohl cloudový poskytovatel dodávat státní správě (OSS) musí projít tzv. EX ANTE kontrolou**
  - Jde o ověření, zda splňuje přístupová pravidla do katalogu cloudu
  - Přístupová pravidla bude definovat cloudová vyhláška
  - Tuto kontrolu má udělat MV ve spolupráci s NÚKIB
- Procesně (aktuální stav):
  - Bezpečnostní pravidla = přístupová pravidla = kvalifikační kritéria
  - Cloud, který bude chtít poskytovat služby OVM (resp. OSS podle ISVS) požádá MV o zařazení do katalogu
  - Spolu s žádostí doloží naplnění pravidel stanovených cloudovou vyhláškou
  - MV ve spolupráci s NÚKIB posoudí, zda cloud naplňuje pravidla/kritéria - pokud naplní – bude vpuštěn do katalogu
  - **Otázky k dořešení:**
    - **Z pohledu NÚKIB je vhodné rozdělit:**
      - **Bezpečnostní pravidla (co má chtít OVM - konkrétní)**
      - **Kvalifikační kritéria (co musí cloud splňovat - obecné)**
    - **Obsah bezpečnostních pravidel a kvalifikačních kritérií = obsah cloudové vyhlášky**
    - **Lhůta, do kdy bude cloud posouzen**
    - **Formát žádosti – stanoví vyhláška MV**
    - **Opravné prostředky, když cloud nebude schválen…**

Katalog cloudu a DNS

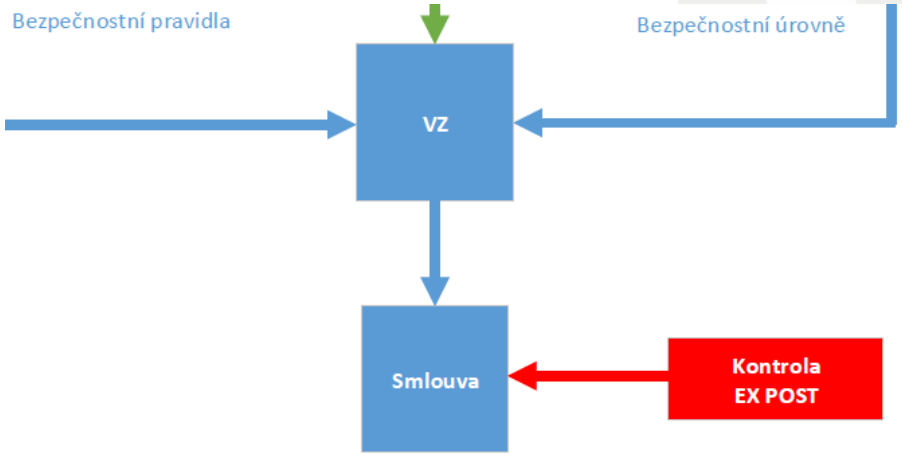


- **Pokud cloud splní pravidla pro vpuštění do katalogu, budou tam jeho služby zařazeny**
- Z katalogu mohou vybírat OVM (resp. OSS podle ISVS) služby
- Ve chvíli, kdy OVM uvidí v katalogu službu, kterou chce, může ji poptat
- V poptávce musí vyspecifikovat detaily poptávané služby
- Následně dojde k samotné soutěži – na poptávku mohou reagovat pouze schválení cloudoví poskytovatelé se službami zapsanými v katalogu služeb
- Pokud se poptávka potká s nabídkou, dojde k uzavření smlouvy a následné plnění

EX POST kontrola

- **U KII a VIS systému je povinnost plnit ZKB a vyhlášku o kybernetické bezpečnosti** a to bez ohledu na model dodávek (cloud, on premise,…)
  - plnění ZKB a VKB kontroluje NÚKIB
- **Pokud jde o systém, který pod ZKB nespadá**, NÚKIB jej nebude kontrolovat, ale měla by nastoupit kontrola ze strany MV (na základě zákona o ISVS)
- **Pokud subjekt nespadá pod ZKB, ani pod ISVS** – kontrola prakticky není

- Ti, kteří nejsou pod ISVS, ale jsou OVM, prakticky nemusí jít ani výše nastíněným procesem katalogu cloudu, ale vždy musí dodržet bezpečnostní pravidla stanovená cloudovou vyhláškou



Cloudová vyhláška - obsah

1. **Bezpečnostní úrovně systémů – Hodnocení dopadu narušení informací**
   - Dopad narušení bezpečnosti informací systému bude determinovat minimální úroveň bezpečnostních požadavků, které bude muset cloud splňovat (resp. umožnit OVM, aby tyto bezpečnostní požadavky splnilo)
   - Z pohledu systémů spadajících pod ZKB dopady determinuje zařazení systému do určité kategorie povinných osob podle ZKB (VIS, PZS, KII)
2. **Jednotlivé úrovně bezpečnostních pravidel**
   - Budou stanoveny jednotlivé kategorie, které budou odpovídat jednotlivým úrovním dopadu narušení C-I-A systému
   - Každá z kategorií bude mít stanovena příslušná bezpečnostní opatření
   - Příslušně kategorizovaný systém nebo jeho část – systém možno dekomponovat (podle bodu 1) bude moci využít pouze tu kategorii cloudu, která odpovídá kategorií systému, nebo vyšší (podle bodu 2).
   - **Aktuálně je to nastaveno tak, že tato pravidla budou zároveň fungovat jako vstupní kontrola cloudového poskytovatele** (pro proces katalogu cloudu a subjekty regulované zákonem o ISVS)
     - NÚKIB se spíše přiklání k tomu aby byla pravidla/kvalifikace zvlášť:
       - Pravidla – konkrétnější – guide pro OVM
       - Kvalifikace – obecnější – na začátku nevím jaké konkrétní požadavky bude OVM chtít

Cloudová vyhláška – 1. bezpečností úrovně systémů

Regulace odpovídající úrovni dopadu	Úroveň dopadu	Vodítka (kategorie) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita) - NUKIB v1.0 / 23.02.2018									
		A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Zákonné a smluvní povinnosti	D. Trestně-právní řízení	E. Veřejný pořádek	F. Mezinárodní vztahy	G. Řízení a provoz organizace	H. Ztráta důvěryhodnosti	I. Finanční ztráty	J. Zajišťování nezbytných služeb
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS, ZKB - KII, ISZS, ZJI	1 nízká	*žádné vodítko*	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	Může narušit řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	*žádné vodítko*
	2 střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.
	3 vysoká *	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Může vést k narušení vyšetřování trestné činnosti nebo soudní řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může vytvářet negativní obraz ČR ve světě.	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25 000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví viz vyhláška č. 437/2017 Sb.).
	4 kritická **	Může vést k přímému ohrožení či ztrátě života skupiny osob.	*žádné vodítko*	*žádné vodítko*	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě KII je hranice ztráty stanovena na 0,5% HDP.	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.
	ZJI	Narušení bezpečnosti informací v oblasti "důvěrnosti" může způsobit újmu zájmům České republiky anebo nevýhodnost pro zájmy České republiky a zároveň je informace typově uvedena v seznamu utajovaných informací (§ 2 písm. a) zákona č. 412/2005 Sb.). Na základě tohoto dopadu by se za splnění dalších legislativně stanovených podmínek mělo jednat o utajované informace. Pro určení odpovídajícího stupně utajení je třeba postupovat v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. A to za splnění dalších stanovených podmínek, např. uvedených v nařízení vlády č. 522/2005 Sb.									

- Posoudit je potřeba narušení důvěrnosti, dostupnosti, integrity
- Úroveň systému determinuje nehorší možný dopad v některé ze scénářů

➢ Tabulka dostupná zde: https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/

Cloudová vyhláška – 2. jednotlivé úrovně bezp. pravidel

Popis opatření	Regulace/norma	N (1)	S (2)	V (3)	K (4)	Poznámka	Realizace / způsob ověření
Část „S“ – Smluvní podmínky mezi zákazníkem a poskytovatelem služby eGC							
S.1 – Součástí smluvních podmínek je SLA, zahrnující úroveň dostupnosti (vazba na přílohu č. 5 *Minimální smluvní podmínky* a přílohu č. 4 *Metodika hodnocení bezpečnostních dopadů*)	ČSN ISO/IEC 27001 A.15	96,16 %	99,45 %	99,90 %	99,99 %	Poskytovatel služeb eGC musí nabízet služby v této úrovni SLA, avšak v případě požadavku zákazníka může v dané bezpečnostní úrovni nabízet alternativu služby s nižší nebo vyšší úrovní dostupnosti v SLA.	Dodavatel nabízí smlouvu o úrovni služeb (SLA), která je součástí smluvní dokumentace. Dodavatel se musí ve smlouvě zavázat k úrovni dostupnosti, která je rovna nebo lepší než hodnoty v dané bezpečnostní úrovni, a to dle bližší specifikace v Příloze 5 SAZ, kap. 2.1. Dodavatel musí dále jako součást obchodní smlouvy nebo separátní smlouvou o podpoře nabídnout podporu dané služby, a to minimálně s uvedením denní doby podpory, s úrovněmi nabízené podpory a s prioritizací incidentů dle Přílohy 5 SAZ, kap. 2.2.
S.2 – Smlouva obsahuje závazek účinného zavedení bezpečnostních opatření v rozsahu dané bezpečnostní úrovně	ČSN ISO/IEC 27001 A.15, ZoISVS §5b	X	X	X	X		Dodavatel má jako součást smluvních podmínek též závazek zavedení bezp. opatření, která odpovídají rozsahu opatření dané bezp. úrovně. Účinnost těchto opatření musí být ověřena auditními zprávami podle mezinárodních standardů, uvedených v této tabulce.
S.3 – Deklarace místa uložení zákaznických dat v rámci jurisdikce EU	ČSN ISO/IEC 27001 A.9, A.11	x	X	X		Pokud by nastalo předání a zpracování dat (širší definice) mimo jurisdikci EU, provozovatel služby eGC objasní důvody předávání a aplikuje některý způsob ošetření dle nařízení GDPR čl. 44 až 48.	Dodavatel komerční části eGC má jako součást smluvních podmínek závazek místa trvalého uložení zákaznických dat (Data at Rest) jako jsou databáze, dokumenty, obsahy emailů atd. včetně jejich záloh v rámci jurisdikce EU. Pokud by nastalo předání a zpracování dat (širší definice) mimo jurisdikci EU, provozovatel služby eGC objasní důvody předávání a aplikuje některý způsob ošetření dle nařízení GDPR čl. 44 až 48.
S.4 – Deklarace místa uložení zákaznických dat v rámci jurisdikce ČR	ČSN ISO/IEC 27001 A.9, A.11				X	Pro bezpečnostní úroveň „4“ se vyžaduje uložení dat v jurisdikci ČR. Výjimkou mohou být případy dekompozice IS a s tím související scénáře hybridního cloudu, kdy funkční části IS s nižší bezpečnostní úrovní (1 až 3) mohou být uloženy v rámci jurisdikce EU.	Dodavatel státní části eGC má jako součást smluvních podmínek pro bezp. úroveň „4“ uložení dat v rámci jurisdikce ČR. Výjimkou mohou být případy dekompozice IS (se souhlasem správce ISVS) a s tím související scénáře hybridního cloudu, kdy funkční části IS s nižší bezpečnostní úrovní (1 až 3) mohou být uloženy u provozovatelů KeGC v rámci jurisdikce EU.
S.5 – Smlouva uvádí způsob poskytnutí informací o zavedených	ČSN ISO/IEC 27001 A.15, ZoISVS §5b	X	X	X	X	Poskytovatel služeb eGC dá zadavatelům vhodným způsobem k dispozici popis, jakým způsobem jsou bezpečnostní	Dodavatel má jako součást smluvních podmínek informaci, resp. odkaz na podrobnější dokumentaci, jakým způsobem jsou bezpečnostní opatření realizována. Přístup k této

Řízení strategických rizik vyplývajících z využívání cloud computing z pohledu regulátora

Cloudová vyhláška – koncepční otázka

Kde budou data/systémy?

3 možnosti:

- Všechno v ČR – nelze
- Všechno v EU – u všech systému nelze
- Část v EU, část v ČR – tudy vede cesta

- Změna zákona o ISVS říká, že:
  - Státní část eGC – systémy kat. 1-4
  - Komerční část eGC – pouze systémy 1-3

Cloudová vyhláška – problémové oblasti – otázky k řešení

- Dekompozice systému
  - Systém půjde dekomponovat, jednotlivé jeho části mohou mít různou kritičnost (dopad)
  - Při dekompozici systému je nutné brát v úvahu bezpečnost, relaci mezi systémem, službou cloudu a architekturou řešení.
  - Popsat dekompozici, aby bylo jasné, jestli je na úrovni systému nebo služby – úroveň systému – po funkčních celcích.
  - Brát v úvahu rozdělení podle typu IaaS, PaaS, SaaS.
  - Brát v úvahu rozdělení podle dopadu narušení CIA.
  - **Poměrně složité – pokud se to udělá špatně, dojde k poddimenzování bezpečnosti**
  - **Bude se těžko kontrolovat**
  - **Pokud dojde k dekompozici je nutno hodnotit jednotlivé komponenty nikoli samostatně, ale ve vztahu a s vazbami k ostatním komponentům i systému jako celku.**

Cloudová vyhláška – problémové oblasti – otázky k řešení

- Budou poskytovatelé cloudu provozovatelé systému podle ZKB?
  - Ano, zde dojde k naplnění definice provozovatele systému v případě každé cloudové služby pro systém určený dle ZKB
- Budou poskytovatelé cloudu KII (minimálně té státní části)?
  - Řešena otázka, zda pokud bude v CC více VIS, zda bude KII – nebude vždy – záleží na kritériích, bude řešeno case by case.
  - Těžko se hodnotí – cloud neví co spravuje za data
  - Cloud zde bude spíše provozovatelem.
  - Bezpečnost cloudu bude definována zejména požadavky zákazníků.
  - CC budou určeny jako KII, pokud naplní kritéria pro KII.
- Kontrola zahraničních cloudů regulátorem je složitá (ale ne nemožná)

Cloudová vyhláška – problémové oblasti – otázky k řešení

- Jak se bude kontrolovat cloudová vyhláška
  - Často půjde o zahraniční subjekty, je třeba definovat požadavky na audit třetí stranou.
  - Pokud bude v ČR – lze to kontrolovat – „provozovatel“ i zákon o kontrole
  - Pokud bude v zahraničí je to problém – je třeba mít dobře udělané smlouvy
    - Základní náležitosti smluv budou v cloudové vyhlášce
    - Pro KII/VIS platí i VKB – také jsou tam náležitosti smluv
    - Pracujeme s požadavkem, že smlouva musí obsahovat právo NÚKIB provést u cloudu kontrolu
    - Bude zajištěn audit třetími stranami podle definovaných standardů – ISO a SOC (SAE reporty) – to bude třeba ze strany cloudu doložit
    - Zavedení povinnosti dát k dispozici auditní zprávy zákazníkovi i regulátorovi.

Cloudová vyhláška – problémové oblasti – otázky k řešení

- Vendor lock
  - Je třeba definovat taková opatření, aby k vendor lock nemohlo dojít
  - Nutno předem myslet na migraci dat a exit strategie
  - V cloudové vyhlášce je:
    - Nutné definovat strategii migrace dat a transferu znalostí včetně stanovení nákladů spojených s replikací dat.
    - Nutné nadefinovat smluvní zajištění .
    - Smluvní pokuta v případě porušení pravidel musí být minimálně ve výši migračních nákladů.
    - Nutné nadefinovat exit strategie
    - Nutno myslet na to, že pokud cloud přestane splňovat požadavky – spouští se exit strategie
- Chování cloudu v případě vydání varování, či jiného opatření NÚKIB
  - …

Cloudová vyhláška – problémové oblasti – otázky k řešení

- Jakým způsobem se dohodnou podmínky zálohování – jak, kdy, kdo odpovídá, kdy a jak často se testují zálohy
- Jakým způsobem se bude postupovat, když se změní bezpečnostní úroveň IS OVM/zákazníka
- Vazby na ZKB, VKB, GDPR
  - Pozor na rozpory (např. smlouvy).
  - Jelikož, se ne u všech subjektů protínají všechny regulace, bude muset být v cloudové vyhlášce svébytná komplexní úprava, která bude v souladu s ostatními regulacemi.
- Likvidace dat/aktiv
  - Reálné je pouze šifrování

Cloudová vyhláška – problémové oblasti – otázky k řešení

- Překryv povinností DSP (digital service provider) a poskytovatele eGC
  - Obecně cloudová vyhláška klade požadavky na zákazníky cloudu, povinnosti DSP jsou kladeny přímo cloudu – ke konfliktu nedochází
- Jak se budou řešit situace, např. orgán veřejné moci sdílí cloudovou službu podřízené organizaci, bude identifikován jako poskytovatel cloudové služby?
- Může být provoz systémů, které nespadají pod ZKB, zajištěn prostřednictvím státní části eGovcloudu?
  - Ano. Do eGC mohou i systémy, které nespadají pod ZKB.
- Vztah mezi VKB a cloudovou vyhláškou.
  - Nebudou v rozporu
  - Musí fungovat jak samostatně tak dohromady

PROVOZOVATEL INFORMAČNÍHO NEBO KOMUNIKAČNÍHO SYSTÉMU

podle § 2 písm. g) zákona o kybernetické bezpečnosti

Dodavatelé

Lze rozlišovat tři druhy dodavatelů podle ZKB

Provozovatel informačního nebo komunikačního systému - § 2 písm. g) ZKB

Orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém

- sám má povinnosti podle ZKB

Významný dodavatel - § 2 písm. n) VKB

Provozovatel a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému

- vyšší úroveň řízení dodavatelů podle VKB

„Běžný“ dodavatel

- běžné řízení dodavatelů podle VKB

Definice provozovatele

Provozovatelem systému se podle § 2 písm. g) zákona o kybernetické bezpečnosti rozumí „orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém“.

Zajišťování

- nelze považovat jednotlivé a jednorázové dodávky technických a programových prostředků, bez dalších navazujících (typicky servisních nebo provozních) činností

Funkčnost

- nejen dodání, ale také zajištění oprav, aktualizace atd.

Technické a programové prostředky

- technické vybavení, komunikační prostředky a programové vybavení (hardware + software) tvořící systém

Určeného systému

- viz dále

Určený informační systém

Určený nebo identifikovaný informační nebo komunikační systém je z pohledu zákona o kybernetické bezpečnosti definován službou, kterou zajišťuje.

- Technické vybavení, komunikační prostředky a programové vybavení určeného nebo identifikovaného informačního nebo komunikačního systému je tedy potřeba identifikovat z pohledu služby, kterou takový systém poskytuje. Vedle toho existuje v organizaci řada jiných systémů, které se skládají z technického vybavení, komunikačních prostředků a programového vybavení, které nepodporují službu určeného nebo identifikovaného informačního nebo komunikačního systému.

- Univerzální otázka – **Podporuje toto technické vybavení, komunikační prostředek nebo programové vybavení určenou službu (resp. službu systému), a to bez ohledu na jeho důležitost?** Pokud ano, je součástí určeného systému.
  - následně se důležitost a vazby zohlední u zavádění ISMS

Provozovatel může být pouze dodavatel technického vybavení, komunikačních prostředků a programového vybavení určeného systému – pokud bude dodavatelem mimo určený systém (např. v rámci rozsahu ISMS), nemůže být provozovatelem systému z definice

Naplnění definice

Informování

Plnění povinností

Obecné příklady

PROVOZOVATEL TYPICKY ANO

- provádění technických bezpečnostních opatření
- správa uživatelských nebo administrátorských (privilegovaných) účtů
- zajištění role garanta aktiva
- nasazování nových aplikací a patchů do produkce (vč. vývoje, pokud je spjat s nasazením)

a další, kteří splní výše uvedenou definici

PROVOZOVATEL TYPICKY NE

- osoba, která určitým způsobem ovlivňuje fungování systému (např. provádí hodnocení rizik, nebo zajišťuje pouze školení pro uživatele a administrátory), nicméně jeho činnost nepředstavuje zajišťování funkčnosti technických a programových prostředků tvořících systém.
- uživatel systému, tedy osoba, která nezajišťuje funkčnost, ale pouze využívá technická aktiva tvořící systém
- dodavatel provozovatelů (tedy subdodavatele)
- zajištění penetračního testování

a další, kteří nesplní byť i část výše uvedené definice

Specifické situace

Security Operations Center?

- Pokud SOC pouze vyhodnocuje události a incidenty a sám neprovádí reaktivní opatření v systému, pak provozovatelem není. Pokud může aktivně zasahovat do technických a programových prostředků produkčního systému, pak provozovatelem je. V tomto případě bude nutné zahrnout i technická podpůrná aktiva SOC týmu, ze kterých je možné zajišťovat technické a programové prostředky dohledovaného systému do určeného systému.

Active Directory?

- AD může mít v závislosti na organizační struktuře společnosti několik vzájemně provázaných úrovní. Koncernové AD, AD národní firmy, AD technologické sítě, samostatné AD určeného systému. Provozovatelem je AD, na které se uživatelé systému autentizují – tedy ta nejnižší úroveň AD a současně by toto AD mělo být zahrnuto do rozsahu systému. Bez tohoto AD se do systému nikdo nepřihlásí a tudíž nebude zajištěna dostupnost.

Dodavatel bezpečnostních řešení?

- Pouze konzultantské činnosti ne. Zásahy do systému (dle výše uvedené definice) ano.

Poznámka na okraj…

Může být správce systému 1 současně provozovatelem u jiného systému 2, který služby systému 1 využívá? (Typicky mobilní operátoři, kteří jsou současně správci svého komunikačního systému a zároveň služby jejich komunikačního systému slouží k zajištění komunikací jiných, například bankovních systémů, systémů státní správy, či systémů zajišťujících řídicí systémy energetických sítí).
Rozhodně ano (pokud naplní výše uvedenou definici), ale provozovatelem bude pouze v rozsahu části systému 2.

Pokud je orgán či osoba již dle § 3 ZKB určena jako správce svého systému, je nutné, aby byla správcem jiného systému informována jako provozovatel (viz předchozí příklad)?
Rozhodně ano, jedná se o jiný systém, tedy jinou situaci.

Vztah mezi správcem a provozovatelem - informování

- Identifikací provozovatele je nutno chápat proces vyhledání dodavatelů, kteří definici provozovatele naplňují, a to za účelem jejich informování o tom, že se stali povinnými osobami podle zákona o kybernetické bezpečnosti.
- Provozovatelem se dodavatel stává ze zákona, naplněním definičních znaků, správce tedy neprovádí žádné určení, ani nevybírá na základě své vůle, který dodavatel provozovatelem bude a který ne.
- **Správce systému je však tím, kdo má vždy jako jediný možnost objektivně a informovaně porovnat zákonnou definici provozovatele s činností svých dodavatelů a takového dodavatele pak identifikovat provozovatelem systému.**
- **Dodavatelé bez zapojení správce nemohou mít dostatek informací k tomu, aby sami posoudili, zda část systému, který provozují, spadá pod zákon o kybernetické bezpečnosti, anebo zda činnost, kterou vůči takto určenému systému vykonávají, představuje zajišťování funkčnosti technických a programových prostředků tvořících takový systém ve smyslu zákona, a tedy zda jsou provozovatelem podle tohoto zákona.**

- **Náležitá identifikace provozovatele je povinností správce a nese za ní odpovědnost.**

Vztah mezi správcem a provozovatelem – obecný model informování

- **Obecný model procesu identifikace provozovatele plyne z § 8 vyhlášky č. 82/2018 Sb., o** kybernetické bezpečnosti, **konkrétně z odst. 1 písm. c) a odst. 3 písm. d) tohoto ustanovení. Zmíněná ustanovení konkretizují povinnost správce v rámci řízení dodavatelů, a to na prokazatelné písemné informování svých významných dodavatelů** (tj. provozovatele informačního nebo komunikačního systému a každého, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému) **o jejich evidenci**, **přičemž náležitostí prokazatelného informování je mj. též vyrozumění o skutečnosti, že významný dodavatel je zároveň provozovatelem.**
- Z pohledu povinnosti informovat provozovatele není podstatné, zda provoz systému je z pohledu správce plně outsourcován k dodavateli nebo dodavatelům nebo je provoz systému správcem systému zajišťován částečně, přičemž zbývající části zajišťuje dodavatel nebo dodavatelé. (Postup podle § 4a ZKB je již v zásadě překonán)

- Nesplněním povinnosti vyplývající z § 8 vyhlášky o kybernetické bezpečnosti se pak správce dostává se do rozporu se zákonnou povinností řídit své dodavatele [bezpečnostní opatření podle § 5 odst. 2 písm. e) zákona o kybernetické bezpečnosti], za což mu může být uložena pokuta až ve výši 5 000 000 Kč.

Vztah mezi správcem a provozovatelem – náležitosti informování

- Informování může být provedeno samostatným dokumentem, který bude informováním o vedení dodavatele v evidenci významných dodavatelů, nebo může být součástí pověření provozováním, seznámení dodavatelů s pravidly pro dodavatele, pokud jsou určeny pro konkrétního dodavatele nebo jiným dokumentem. Ve všech případech by však mělo být provedeno prokazatelně, adresně a ve vztahu ke každému jednotlivému provozovateli samostatně.

- **Podstatnými náležitostmi prokazatelnosti je informace o tom, že se jedná o provozovatele systému podle zákona o kybernetické bezpečnosti, s čímž je neodmyslitelně spjato také stanovení části systému spadajícího do působnosti zákona o kybernetické bezpečnosti.**

- Informování je ze své podstaty jednostranný právní akt učiněný správcem systému. Informování je však nutno důsledně odlišovat od procesu smluvního zajištění zavádění a provádění bezpečnostních opatření a vymezení práv a povinností mezi správcem a provozovatelem systému

Vztah mezi správcem a provozovatelem – plnění povinností

- **V případě, že byl provozovatel systému správcem informován, je povinen plnit povinnosti podle zákona o kybernetické bezpečnosti, tzn. začít konat.**

- Bude se jednat především o povinnost hlásit kybernetické bezpečnostní incidenty (§ 8 odst. 1 a 5 zákona), provádět reaktivní a ochranná opatření (§ 11 zákona) a hlásit kontaktní údaje (§ 16 zákona), ale také předat správci data, provozní údaje a informace na vyžádání (§ 6a odst. 2 zákona), povinnost předat správci data, provozní údaje a informace při ukončení spolupráce (§ 6a odst. 3 zákona), nebo předat správci data, provozní údaje a informace na základě rozhodnutí vydaného NÚKIB (§ 15a zákona).

- **Díky informování ze strany správce systému, které obsahuje výše uvedené náležitosti, tedy bude obsahovat informaci o tom, že se jedná o provozovatele systému podle ZKB a vymezení rozsahu systému a činností, pro které se stává dodavatel provozovatelem, má provozovatel systému dostatek informací pro plnění těchto povinností. – Pokud tyto potřebné informace nemá, musí učinit kroky k tomu, aby je získal od správce (pro účely vyvinění se z neplnění právních povinností)**

Vztah mezi správcem a provozovatelem – cílený stav

- **Správce ví, kdo jsou jeho provozovatelé a co od nich očekává**
- **Provozovatel ví, že je provozovatelem, pro jaké činnosti a byly mu řečeny, nebo alespoň řízeny, způsoby jak**
- **S tím souvisí správné informování se všemi náležitostmi a jasné vymezení toho kdo co dělá**
- **Středobodem všeho je, zda je systém dostatečně ochráněn**
- **Požadavkem je také promítnutí takto rozvržených rolí a povinností do smluv**

Specifické otázky

Otázka náhrady finančních prostředků

- Náhrada vynaložených nákladů za zavádění a provádění bezpečnostních opatření není zákonem o kybernetické bezpečnosti nijak regulována, konkrétní podoba dohody správce s provozovatelem ohledně úhrady nákladů je tedy věcí smluvní volnosti (s případnými specifiky vyplývajícími z jiného právního předpisu).

Vztah významného dodavatele a provozovatele

- Významným dodavatelem je provozovatel a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti systému. **Po zhodnocení všech dodavatelů a případné identifikaci některých jako provozovatelů je potřeba zhodnotit zbylé dodavatele také z toho pohledu, zda s povinnou osobou vstupují do právního vztahu, který je významný z hlediska bezpečnosti určeného systému.** V tomto případě je především potřeba věnovat velkou pozornost těm dodavatelům, kteří mají vztah k aktivům v rozsahu systému řízení bezpečnosti informací a nebyli identifikováni jako provozovatelé systému (pokud nejsou v rozsahu ISMS a mají vliv na bezpečnost, je velmi vhodné rozšíření rozsahu ISMS).

DĚKUJI ZA POZORNOST

regulace@nukib.cz