EGOVERNMENT_CLOUD_

ZÁPIS DO KATALOGU CLOUD COMPUTINGU_

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

NÚKIB

29. 2. 2024

CLOUD_COMPUTING_

- vymezeno **zákonem č. 356/2000 Sb., o informačních systémech veřejné správy**
  - stanovuje práva a povinnosti, které souvisejí s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy spravovaných *státními orgány, orgány územních samosprávných celků nebo státními právnickými osobami* = **orgány veřejné správy**

- **zajištění provozu** informačního systému veřejné správy nebo jeho části **prostřednictvím dálkového přístupu** k **sdílenému** technickému nebo programovému prostředku, který je **zpřístupněný** poskytovatelem cloud computingu a **nastavitelný** správcem informačního systému veřejné správy

- **VÝJIMKY**

zákon č. 365/2000 Sb.,
o informačních systémech veřejné správy

KATALOG_CLOUD_COMPUTINGU_

1) Poptávky OVS

- Společná
- Individuální

2) Poskytovatelé CC

- Státní – 4. kritická bezpečnostní úroveň, všechny kritické IS, část významných IS
- „Komerční“ – 1. až 3. bezpečnostní úroveň

3) Nabídky CC

- konkrétní služby CC

4) Využívaný CC

- Smlouva s poskytovatelem CC
- Finanční objem vynaložený na CC

Katalog CC na webu DIA

POVINNOSTI_PRO_OVS_1_

- Orgán veřejné správy může využívat **pouze** cloud computing, který je poskytovaný:
  - poskytovatelem státního cloud computingu nebo poskytovatelem cloud computingu **zapsaným v katalogu cloud computingu**,
  - v rámci vertikální nebo horizontální spolupráce nebo
  - v rámci obecné výjimky z povinnosti zadat veřejnou zakázku

- **VÝJIMKY**

zákon č. 365/2000 Sb., o informačních systémech veřejné správy

POVINNOSTI_PRO_OVS_2_

- **31. 12. 2023** – konec přechodných ustanovení

- pokud využívaný CC **nesplňuje podmínky ZoISVS**, musí OVS **do 12 měsíců** ukončit jeho využívání

POVINNOSTI_PRO_OVS_ PŘED_VYUŽÍVÁNÍM_CLOUD_COMPUTINGU_1_

- Dekompozice ISVS
  - dobrovolné
  - cílem je zařadit každou komponentu do nejvhodnější bezpečnostní úrovně a využít tak optimální technologie (a optimální finanční náklady)

- Stanovení bezpečnostní úrovně
  - **vyhláška č. 315/2021 Sb.**, o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

POVINNOSTI_PRO_OVS_ PŘED_VYUŽÍVÁNÍM_CLOUD_COMPUTINGU_2_

- Předběžné posouzení plánovaných nákladů výhodnosti zvoleného řešení
  - cloud mandatory-compare
  - on premise vs cloud

TCO kalkulátor na webu DIA

- Minimální smluvní standardy
  - **vyhláška č. 190/2023 Sb.**, o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

POVINNOSTI_PRO_OVS_ PŘI_VYUŽÍVÁNÍ_CLOUD_COMPUTINGU_

- Stanovení bezpečnostních pravidel v rámci OVS
  - **vyhláška č. 190/2023 Sb.**, o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu
  - podle dané bezpečnostní úrovně

- Zápis využívaného cloud computingu do katalogu CC a poskytování informací - § 6x a § 6y **ZoISVS**

POVINNOSTI_PRO_POSKYTOVATELE_

- Zápis **poskytovatele** cloud computingu do katalogu cloud computingu - § 6q a § 6r **ZoISVS**

- Zápis **nabídky** cloud computingu do katalogu cloud computingu - § 6t a § 6u **ZoISVS**

Metodiky, návody, formuláře na webu DIA

PROCES_ZÁPISU_DO_KATALOGU_CC_

- Doručení žádosti do datové schránky DIA
  - zahájení správního řízení
- Kontrola žádosti ze strany DIA
- Vyžádání si součinnosti (informace, závazná stanoviska)
- Výzva k odstranění nedostatků v žádosti
- Zapsání do katalogu CC
  - zveřejnění na webu + informace odeslaná poskytovateli

Metodiky, návody, formuláře na webu DIA

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

POVINNOSTI_PRO_POSKYTOVATELE_

- zapsat všechny poskytovatele z dodavatelského řetězce
- při podání žádosti za jiného poskytovatele dodat pověření
- používat aktuální verze formulářů

Metodiky, návody, formuláře na webu DIA
Aktuality na webu DIA
Otázky a odpovědi na webu DIA

KATALOG_CLOUD_COMPUTINGU_

Stav k 29. 2. 2024	Zapsáno	Podána žádost
Poskytovatelé CC	99	14
Nabídky CC	26 z toho 22 přímý prodej	10

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

DÍLČÍ_SHRNUTÍ_

- Co musí splnit **OVS**, aby mohl **využívat CC**?
  - Provést hodnocení bezpečnostní úrovně
  - Posoudit ekonomickou výhodnost zvoleného řešení
  - Využívat pouze CC zapsaný v katalogu CC
  - Nastavit bezpečnostní pravidla pro využívání CC
  - Zapsat využívaný CC do katalogu CC
- Co musí splnit **poskytovatel CC**, aby mohl **nabízet CC**?
  - Být zapsán v katalogu CC
  - Mít zapsané služby CC, které nabízí

Žádost o zápis služeb do katalogu cloud computingu

Úvod do problematiky, časté nedostatky

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

29. února 2024

TLP: CLEAR

Petr Kopřiva
Odbor regulace

Právní rámec

- Dle **§ 6n písm. b) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů** (dále jen „ZoISVS“) může orgán veřejné správy využívat a poskytovatel cloud computingu může orgánu veřejné správy nebo poskytovateli státního cloud computingu poskytovat pouze cloud computing, který umožňuje dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy.
- Konkrétní požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem podle § 6n písm. b) ZoISVS stanoví **vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu** (tzv. vyhláška o vstupních kritériích, dále jen „Vyhláška“) v **příloze č. 2**.

Příloha č. 2 Vyhlášky

- Požadavky, které musí služba cloud computingu splňovat, aby mohla být zapsána do katalogu cloud computingu

- Požadavky členěny do 10 oblastí:
  1. Místo zpracování a uložení dat
  2. Žádosti o zpřístupnění a předání dat
  3. Oprávnění k provedení kontroly
  4. Úrovně dostupnosti služby
  5. Připojení do výměnného uzlu internetu (IXP)
  6. Zajištění poskytování služby cloud computingu
  7. Nakládání s daty
  8. Certifikace služby cloud computingu
  9. Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty
  10. Testování služby cloud computingu

- Důvodová zpráva k dispozici na webu nukib.cz -> Kybernetická bezpečnost -> Regulace a kontrola -> Legislativa

Příloha č. 2 Vyhlášky

- Každý řádek představuje samostatný požadavek
- Požadavky se liší dle bezpečnostní úrovně a dle třídy nabízeného cloud computingu (IaaS, PaaS, SaaS)

Příloha č. 2 k vyhlášce č. 316/2021 Sb.

Řádek	Požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem	Podklad, kterým poskytovatel doloží splnění požadavku	Bezpečnostní úroveň nabízeného cloud computingu				Třída cloud computingu		
			Nízká	Střední	Vysoká	Kritická	cloud computing ve formě infrastruktury	cloud computing ve formě platformy	cloud computing ve formě aplikačního programového vybavení
1. Místo zpracování a uložení dat									
1.1	Poskytovatel uvádí informace o	Písemný popis, ze kterého bude							

Časté obecné nedostatky žádosti

- **Žádost zahrnuje služby, které nepodléhají regulaci a nemají být zapisovány**
  - Problém s doložením některých požadavků Vyhlášky vzhledem k podstatě těchto služeb
  - Definice cloud computingu v § 2 odst. 2 písm. b) ZoISVS: *„Cloud computingem způsob zajištění provozu informačního systému veřejné správy nebo jeho části prostřednictvím dálkového přístupu k sdílenému technickému nebo programovému prostředku, který je zpřístupněný poskytovatelem cloud computingu a nastavitelný správcem informačního systému veřejné správy.“*
  - Výjimky z regulace:
    - § 1 odst. 4 ZoISVS
    - § 6l odst. 4 ZoISVS

- **Nepřehlednost žádosti**
  - § 9 odst. 4 Vyhlášky: *„V případě, že je pro doložení splnění požadavků podle § 3 a 4 nezbytné odkázat do jiného dokumentu, který je k formuláři připojen, provede se tak ve formuláři uvedením kapitoly, strany, odstavce a případně i konkrétní věty.“*
  - Nutnost důsledně odkazovat na konkrétní části dokládaných dokumentů!

Časté obecné nedostatky žádosti

- **Dokládání odkazy na webové stránky**
  - Nelze, protože podoba webových stránek se mění v čase
  - Lze doložit snímek webové stránky

- **Nekonzistentnost pojmenování služeb a jejich nejasné zařazení do balíčků služeb**
  - Pojmenování služeb v žádosti i ve všech dokládaných dokumentech musí být jednotné
  - Při existenci balíčku služeb je nutné jednoznačně uvést, jaké jednotlivé služby jsou v balíčku služeb zahrnuty
  - Lze doložit přehledovým dokumentem

- **Doložení čestného prohlášení u řádků, u nichž Vyhláška tento způsob doložení požadavku nepřipouští**
  - U každého řádku Vyhláška uvádí, jakým způsobem má být řádek doložen
  - Některé řádky lze čestným prohlášením dokládat, jiné nikoliv

- **Doložení dokumentů, které pokrývají jen část služeb, které poskytovatel žádá zapsat**

Časté nedostatky v doložení jednotlivých řádků Vyhlášky

1 Místo zpracování a uložení dat

- Směšování/zaměňování používaných pojmů
  - Uložení vs. zpracování dat vs. výkon správy a dohledu
  - Zákaznická data vs. specifické provozní údaje
  - Vyhláška ≠ GDPR
  - Vymezení pojmů v § 2 Vyhlášky
  - Pokud je v dokládaných dokumentech používáno jiné pojmosloví, je nutné doložit vymezení těchto pojmů
- Řádek 1.1
  - Nestačí uvést, že zákaznická data jsou nebo mohou být uložena pouze v členských zemích EU a ESVO, je třeba jmenovat konkrétní země i v rámci EU a ESVO

2 Žádosti o zpřístupnění a předání dat

- Řádek 2.5
  - Nestačí deklarace poskytovatele, že data nezpřístupní
  - Je nutné doložit písemný popis povinností vyplývajících z právních předpisů všech států odlišných od členských států EU, EHP a států s tzv. Adequacy decision podle čl. 45 GDPR, v nichž poskytovatel předpokládá zpracování zákaznických dat a ve kterých má zároveň nějakou infrastrukturu

Časté nedostatky v doložení jednotlivých řádků Vyhlášky

4 Úrovně dostupnosti služby

- Doložení SLA, které nezahrnuje všechny zapisované služby
- Doložení dostupnosti služeb na jiné než měsíční bázi

6 Zajištění poskytování služby cloud computingu

- Řádek 6.4
  - Nestačí doložit, že poskytovatel umožňuje zálohování
  - Musí být doloženo, že záložní datové centrum je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra
  - Pokud jsou od sebe primární a záložní datacentrum vzdálené více než 50 km - je třeba doložit také aplikaci fyzické ochrany proti přírodních katastrofám, úmyslnému útoku nebo haváriím
  - Pokud jsou od sebe primární a záložní datacentrum vzdálené méně než 50 km – je třeba doložit zprávu o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka, která musí obsahovat náležitosti uvedené v příloze č. 5 Vyhlášky

Časté nedostatky v doložení jednotlivých řádků Vyhlášky

7 Nakládání s daty

- Řádek 7.2
  - Nestačí doložit, že poskytovatel nabízí šifrování
  - Musí být doloženo, že poskytovatel šifruje v úložištích a při přenosu v nabízených službách defaultně
- Řádek 7.3
  - Zde naopak stačí, že poskytovatel nabízí
  - Doporučení v oblasti kryptografických prostředků (nukib.cz)
- Řádek 7.8
  - Opět problematika pojmosloví: zákaznická data ≠ osobní údaje

Časté nedostatky v doložení jednotlivých řádků Vyhlášky

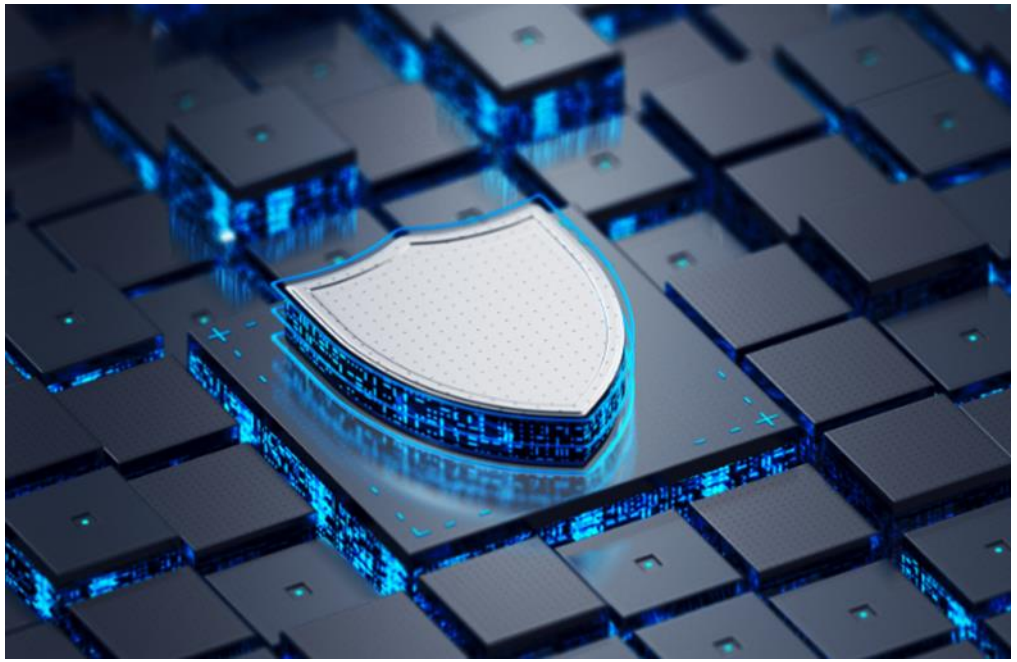
8 Certifikace služby cloud computingu

- Řádky 8.2 až 8.6.
  - V rozsahu certifikátů musí být všechny zapisované služby
  - Lze zhojit čestným prohlášením
- Řádky 8.3, 8.5 a 8.6 (BÚ vysoká a kritická)
  - Vyžadováno i příslušné prohlášení o aplikovatelnosti
  - Rozdíl oproti řádkům 8.2 a 8.4 (BÚ střední)
- Řádek 8.7
  - Auditní zpráva SOC 2 Type 2 musí být ve všech 5 doménách (tj. bezpečnost, dostupnost, procesní integrita, důvěrnost a soukromí)
  - Alternativně může poskytovatel doložit splnění požadavku auditní zprávou o vyhodnocení shody s aktuálními požadavky C5
  - Předkládaná auditní zpráva nesmí být v době podání žádosti starší než 24 měsíců
  - Do rozsahu předkládané auditní zprávy musí náležet jmenovitě všechny služby, které poskytovatel žádá zapsat
- Doplňkové informace k dokládání požadavků řádků 8.1 až 8.7 v příloze č. 3 Vyhlášky

Časté nedostatky v doložení jednotlivých řádků Vyhlášky

9 Kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty

- Směšování/zaměňování pojmů
  - Kybernetická bezpečnostní událost vs. kybernetický bezpečnostní incident
  - Pokud se v dokládaných dokumentech používá jiné pojmosloví, je třeba doložit jejich definici



Časté nedostatky v doložení jednotlivých řádků Vyhlášky

10 Testování služby cloud computingu

- Řádky 10.1, 10.2 a 10.3
  - V dokládaných skenech zranitelností a penetračních testech by měly být uvedeny všechny zapisované služby
  - Lze zhojit čestným prohlášením subjektu, který skeny zranitelností nebo penetrační testy provedl
- Řádek 10.1
  - Záznam o skenu zranitelností musí obsahovat datum
- Řádky 10.2 a 10.3
  - Řádek 10.2 je pro služby IaaS/PaaS,
  - Řádek 10.3 je pro služby SaaS
  - Liší se požadovanou metodikou, dle které má být penetrační test proveden
  - V odůvodněných případech je možné doložit pro PaaS OWASP, nebo pro SaaS NIST

Statistika posuzování poskytovatelů

- Dle § 6m odst. 1 písm. a) a c) ZoISVS

- Stav k 29. 2. 2024
  - Počet provedených posouzení poskytovatelů cloud computingu dle a): 114
  - Počet provedených posouzení poskytovatelů cloud computingu dle c): 114
  - Počet otevřených posouzení dle a): 8
  - Počet otevřených posouzení dle c): 8

Statistika posuzování služeb

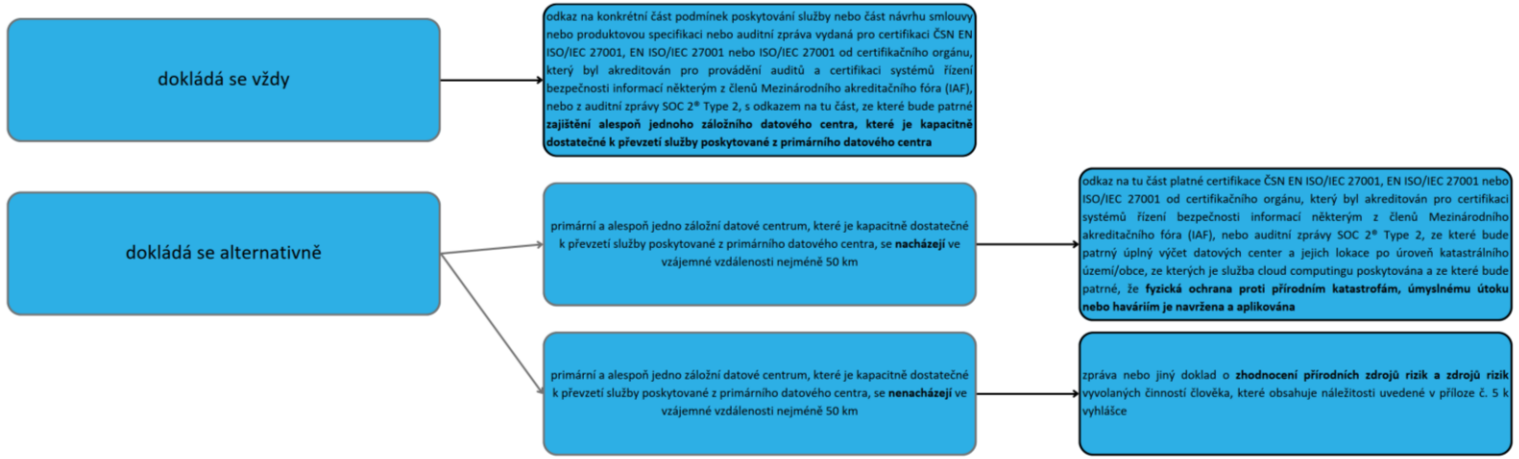
- Dle § 6n písm. b) a e) ZoISVS

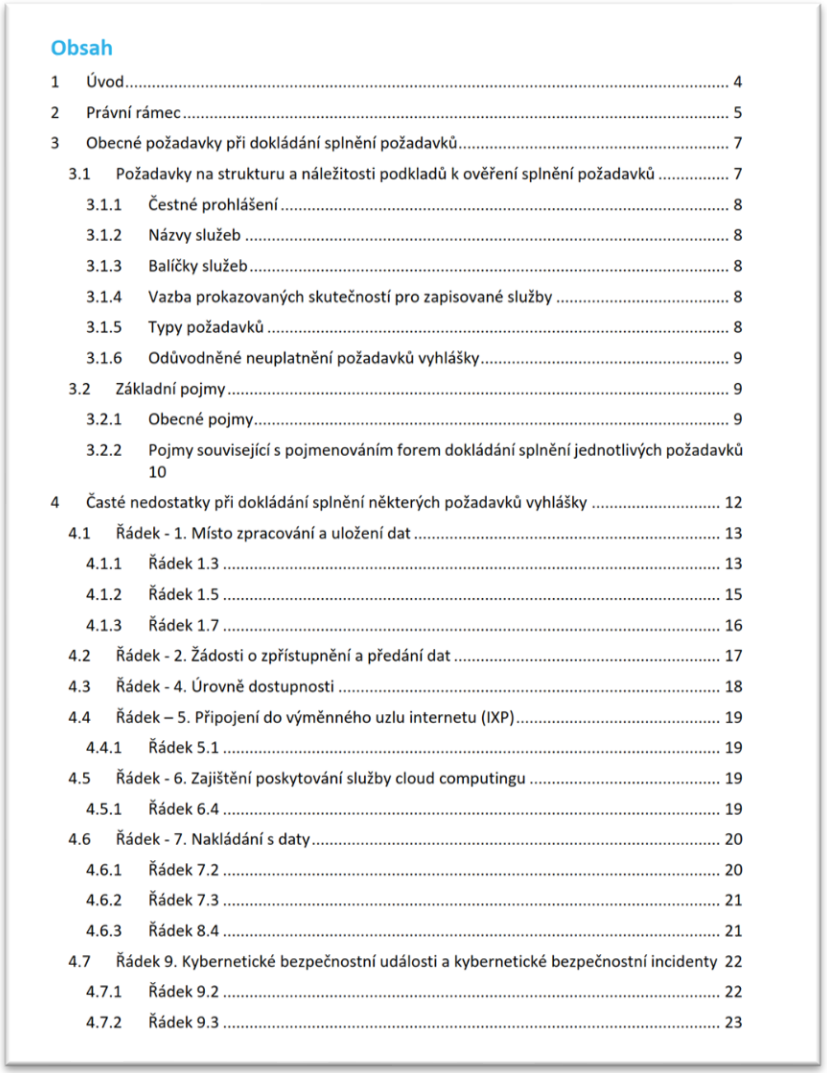
- Stav k 29. 2. 2024
  - Počet provedených posouzení nabídek služeb cloud computingu: 22
    - posouzené nabídky zahrnovaly celkem více než 250 jednotlivých služeb
  - Počet otevřených posouzení: 8
    - z toho 6 po výzvě k odstranění nedostatků a 2 nové žádosti

Průvodce dokládání požadavků pro zápis služeb CC

- Nový podpůrný materiál
  - Kapitola **o obecných požadavcích** při dokládání splnění požadavků
  - Kapitola **o častých nedostatcích** při dokládání splnění některých požadavků vyhlášky

- Podpůrné materiály





Obsah

DOTAZY_

egc@dia.gov.cz

regulace@nukib.cz

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

NÚKIB