Zápis nabídek cloud computingu do katalogu cloud computingu

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

NÚKIB

8. 12. 2023

Právní předpisy upravující oblast CC

- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
  - *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***
- vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu
- vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci
- vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
- vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

Zápis do katalogu CC

- po novelizaci ZoISVS je od 1. 9. 2021 stanovena povinnost provést
  1) zápis poskytovatele CC
  2) zápis nabídky CC

- návody a formuláře na webu DIA

  https://www.dia.gov.cz/oha/egovernment-cloud/metodiky-navody-formulare/

Proces zápisu nabídky CC

- Doručení žádosti do datové schránky DIA
- Kontrola žádosti ze strany DIA
  - závazné stanovisko NÚKIB
    - nevyžaduje se
      - *u nabídky CC zařazené do nejnižší bezpečnostní úrovně*
      - *pro služby, které daný poskytovatel využívá nebo přeprodává (a jsou zapsané v katalogu CC)*
- Výzva k odstranění nedostatků v žádosti
- Zapsání do katalogu CC (zveřejnění na webu + informace odeslaná poskytovateli)

Katalog CC (stav k 7. 12. 2023)

Stav k 7. 12. 2023	Zapsáno	Podána žádost
Poskytovatelé CC	87 (+ 1)	**14**
Nabídky CC	3 (+ 2)	**6**

Úprava metodiky (na základě praxe)

- úprava identifikace zapsaných služeb do katalogu CC
  - aktualizace formulářů pro zápis nabídky

- služby nabízené, auditované, zapsané v katalogu
  - možnost "balíčkování"

Žádost o zápis služeb do katalogu cloud computingu

Úvod do problematiky, časté nedostatky

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

8. prosince 2023
TLP: CLEAR

Ivan Senčák
Odbor regulace

Statistika posuzování poskytovatelů

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

- Stav k 7. 12. 2023
  - Počet provedených posouzení poskytovatelů cloud computingu dle a): 45
  - Počet provedených posouzení poskytovatelů cloud computingu dle c): 72
  - Počet otevřených posouzení dle a): 3
  - Počet otevřených posouzení dle c): 6

Statistika posuzování služeb

- Dle § 6n písm. b) a e) ZoISVS

Počet provedených posouzení nabídek služeb cloud computingu:		**12**
Z toho kladných stanovisek/výzev k odstranění nedostatků/záporných stanovisek:		
	Kladné stanovisko	3
	Výzva k odstranění nedostatků	9
	Záporné stanovisko	0
Pozn.: Posouzené nabídky služeb zahrnovaly celkem více než 250 jednotlivých služeb cloud computingu.		
Počet otevřených posouzení k 7. 12. 2023:		**4**
Z toho po výzvě k odstranění nedostatků/nové žádosti:		
	Po výzvě k odstranění nedostatků	2
	Nové žádosti	2

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							

Bezpečnostní úrovně nabízeného cloud computingu

Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

- Provádí zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Stanovení bezpečnostní úrovně dle úrovně dopadu kybernetického bezpečnostního incidentu
  - např. počet zranění či ohrožení lidí, počet mrtvých, finanční ztráty, omezení nebo narušení dostupnosti služeb, narušení veřejného pořádku, …
- Celkem 4 úrovně:
  - nízká
  - střední
  - vysoká
  - kritická (pouze státní poskytovatel)

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, v nichž poskytovatel předpokládá zpracování zákaznických dat

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 (požadováno Vyhláškou)

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
  - Zpráva o zhodnocení přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka 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

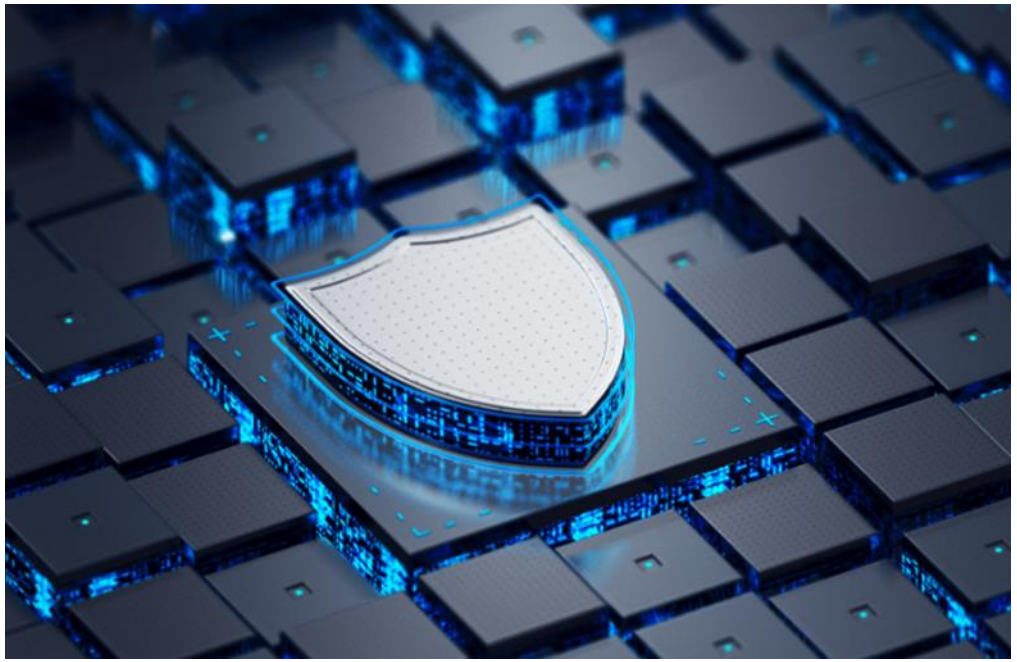
8 Certifikace služby cloud computingu

- 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
- Podpůrný materiál k pentestům

Dotazy

egc@dia.gov.cz

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

regulace@nukib.cz

NÚKIB