Žádost o zápis služeb do katalogu cloud computingu

Úvod do problematiky, postup před zahájením řízení, časté obecné nedostatky

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

25. února 2025

TLP: CLEAR

Vítězslav Orava
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							

Jak na zápis nabídky prakticky – 3 kroky

- **Připravit si první verzi formuláře**
- **Požádat o předběžnou konzultaci (dobrovolné)**
- **Poslat kompletní přihlášku**

Příprava první verze formuláře

- **Přečíst si vyhlášku a identifikovat si základní věci**
  - Služby, které je třeba nachystat k zápisu
  - BÚ
  - Požadavky, jejichž splnění je třeba doložit
- **V dokumentaci najít relevantní doklady splnění požadavků**
  - Pozor na přípustné způsoby doložení (ČP apod.)
  - V případě nejistoty se podívat do Průvodce.
  - Pokud nejasnosti přetrvávají, konzultovat důvodovou zprávu
- **Vyplnit první verzi formuláře dle nejlepších informací**
  - Pečlivost odstraní řadu častých chyb
  - Žádný učený z nebe nespadl

Předběžná konzultace

- **!!!Závisí na aktuálních kapacitách NÚKIB. Bez výjimek mají přednost posouzení ve správním řízení, kde běží správní lhůty!!!**
- **Mám připravenou první verzi formuláře**
  - Kontaktuji NÚKIB na adrese regulace@nukib.gov.cz spolu s návrhem několika termínů s odstupem cca 14 dní
  - Zašlu NÚKIB první verzi formuláře spolu se všemi dokumenty, na které ve formuláři odkazuji
  - Doplním případné dotazy a nejasnosti
- **K čemu předběžná konzultace slouží**
  - Abych si ujasnil věci, které nejsou jasné a k nimž mám dotazy
  - K odfiltrování nejkřiklavějších nedostatků
- **K čemu předběžná konzultace neslouží**
  - Aby byla přihláška kompletně zkontrolována a následně „jen“ schválena
  - Abychom prošli podrobně všechny dokumenty a nalezli všechny nedostatky
  - Ke konzultaci hypotetických scénářů bez vazby k reálným problémům

- **Z naší zkušenosti předběžná konzultace významně snižuje množství problémů a celkově zkracuje následné vlastní řízení, ale je zcela dobrovolná.**

Zaslání vlastní žádosti

- **Příprava konečné verze žádosti**
  - Poskytovatel vytvoří konečnou verzi žádosti
  - Doporučujeme důkladnou kontrolu odkazů, názvů služeb v různých kartách formuláře, rozsahů certifikací apod.
- **Zaslání konečné verze žádosti**
  - Před odesláním doporučujeme zkontrolovat všechny přílohy a jejich funkčnost
  - Upozorňujeme na požadavek vyhlášky na zasílání příloh ve strojově čitelném formátu.

Časté obecné nedostatky žádosti

- **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!
  - „Viz dokument VOP_CZ“ je nepřijatelné a poskytovatel je vyzýván k doplnění!
  - „Viz dokument VOP_CZ, str. 28, kapitola 5.13 Bezpečnost, odst. 3, druhá věta“ je ideální stav odkazu
  - „Viz dokument VOP_CZ, str. 31-32, kapitola 5.14 Penetrační testování“ je přijatelné, pokud je odkazem delší text
  - V případě odkazu na text delší než např. kapitola je dobré uvést zdůvodnění takového odkazu např.: „V této části dokumentu je popsána metodika, kterou poskytovatel používá…“

  - Pokud je doložení splnění požadavku nalezeno při kontrole jiné části dokumentu (jiného požadavku), než na nějž je odkazováno, NÚKIB k němu samozřejmě přihlíží

Časté obecné nedostatky žádosti

- **Nadbytečně odkazy**
  - Poskytovatelé v řadě případů odkazují na dokumenty, které nejsou pro doložení splnění požadavků relevantní
- **Strojově nečitelné dokumenty**
  - Vyhláška v § 9 odst. 5 vyhlášky požaduje, aby žádost i veškeré přílohy byly ve strojově čitelném formátu
- **Doložení dokumentů, které pokrývají jen část služeb, které poskytovatel žádá zapsat**
  - Stává se, že dokument, které mají osvědčovat splnění podmínek se vztahují jen k části zapisovaných služeb či v nich některé jednotlivé služby absentují
- **Pozor na rozdíly v listu IaaS a PaaS a Podklady k ověření IaaS-PaaS**
  - Často se oba seznamy neshodují a pak je to zmatečné
  - Důležité je, aby podklady k zápisu pokrývaly všechny služby, jež se mají zapisovat

Časté obecné nedostatky žádosti

- **Dokládání odkazy na webové stránky**
  - § 9 odst. 5 stanoví, že formulář i veškeré přílohy se předkládají v elektronické podobě, ve strojově čitelném formátu zaručujícím neměnnost obsahu jednotlivých dokumentů

- **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

Časté obecné nedostatky žádosti

- **Zaheslované dokumenty**
  - Takový postup není v souladu s požadavky vyhlášky, zejm. § 9 odst. 5, se správním řádem ani s běžným postupem v obdobných věcech
  - Jde i proti principu přezkoumatelnosti správního rozhodnutí.

- **Rozsah služeb**
  - Velké množství certifikátů neobsahuje kompletní rozsah služeb, které poskytovatel žádá zapsat

- **Obecný popis služeb a nejasné zařazení služeb do jednotlivých „rodin“**
  - Není zcela jasné, zda předložené dokumenty pokrývají všechny služby
  - Poskytovatel odkazuje na rodinu služeb bez bližší specifikace služeb v ní obsažených

- **Špatná verze formuláře**
  - Používá se standardizovaný elektronický formulář DIA
  - Pokud v Žádosti absentuje většina listů tohoto formuláře, mohlo se stát, že poskytovatel omylem doložil formulář ve verzi 1.3, která byla využívána k zápisu služeb do 31. srpna 2021

Nové doporučení pro kryptografii

- **Úřad na začátku února vydal nové Minimální požadavky na kryptografické algoritmy, které se vztahuje k řádku 7.3**
- Doporučení

- **Důležité změny**
  - Vyřazení dosluhujících kryptografických algoritmů nesplňujících bezpečnostní požadavky
  - Aktualizace algoritmů na základě finálního znění postkvantových kryptografických standardů NIST vydaných v srpnu 2024 – upřesnění názvů a parametrů
  - Přidání dvou módů ochrany integrity (KMAC a GMAC)
  - Úprava parametrů algoritmů pro ukládání hesel

Statistika posuzování poskytovatelů

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

- Stav k 27. 2. 2025
  - Počet provedených posouzení poskytovatelů cloud computingu dle a): 151
  - Počet provedených posouzení poskytovatelů cloud computingu dle c): 150
  - Počet otevřených posouzení dle a): 11
  - Počet otevřených posouzení dle c): 12

Statistika posuzování služeb

- Dle § 6n písm. b) a e) ZoISVS

- Stav k 27. 2. 2025
  - Počet provedených posouzení nabídek služeb cloud computingu: 80
    - posouzené nabídky zahrnovaly celkem více než 500 jednotlivých služeb
  - Počet otevřených posouzení: 15
    - z toho 9 po výzvě k odstranění nedostatků a 6 nové žádosti
    - zahrnuta jsou i průběžná dokládání certifikátů

Dotazy?

Děkuji za pozornost!

regulace@nukib.gov.cz