Nový zákon o kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Jan Rudolf
oddělení regulace dodavatelů informačních technologií

23.09.2025

TLP:CLEAR

1. Zákon o kybernetické bezpečnosti

2. Regulace cloudových služeb

Zákon o kybernetické bezpečnosti

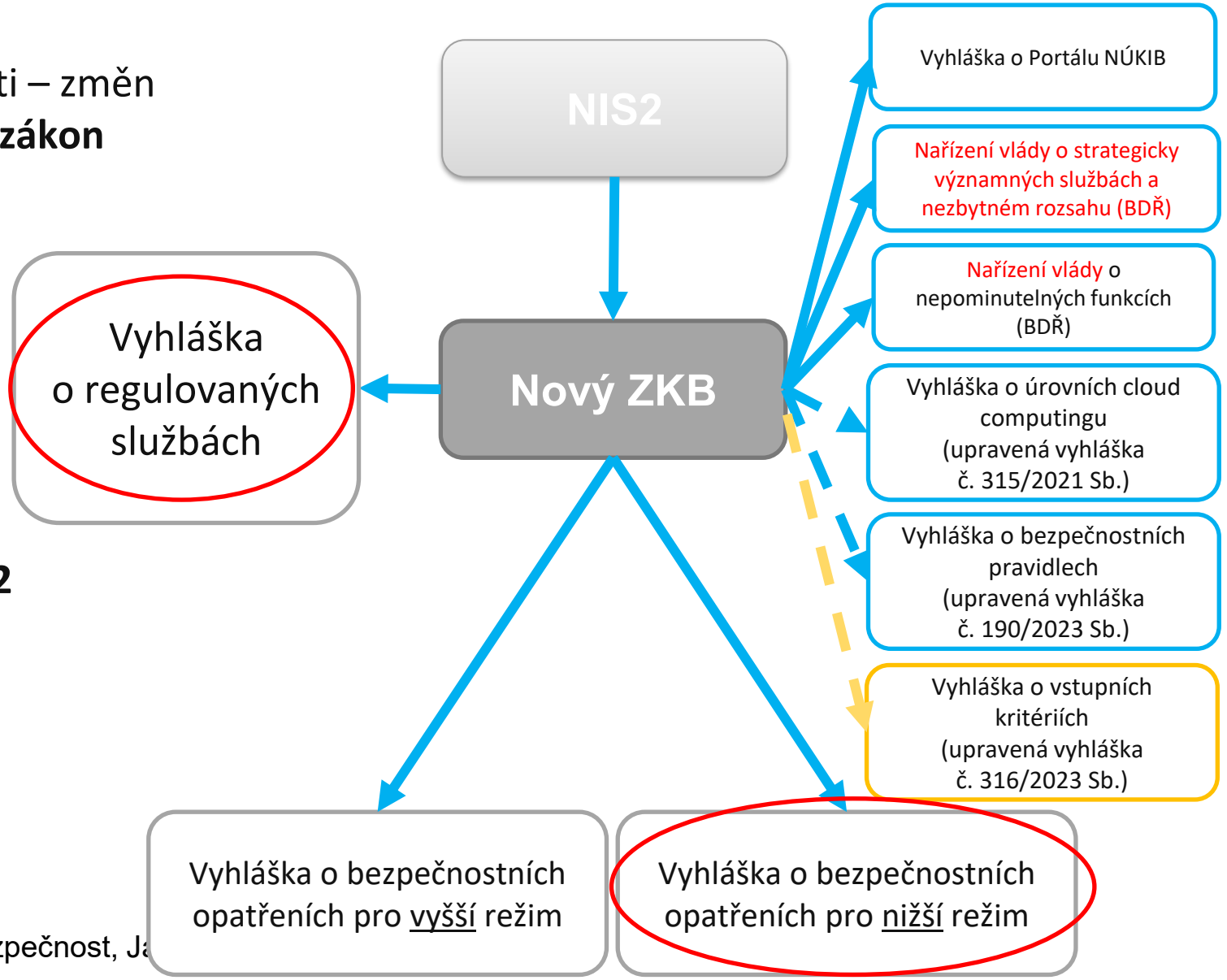
Nový zákon o kybernetické bezpečnosti

Nový zákon o kybernetické bezpečnosti – změn je tolik, že bylo **potřeba vytvořit nový zákon**

= zcela nová úprava – 73 paragrafů

Po průchodu poslaneckou sněmovnou jde o **8 vyhlášek a nařízení vlády.**

Reálně se ale bude upravovat ještě jedna vyhláška navíc, ale ne kvůli NIS2 (č.316/2023)



Vyhláška o regulovaných službách

1. Veřejná správa

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Českou národní bankou, g) Policejním prezidiem, h) útvarem policie s celostátní působností, i) Generální inspekcí bezpečnostních sborů j) Generálním ředitelstvím hasičského záchranného sboru, k) krajským ředitelstvím hasičského záchranného sboru, l) Kanceláří Veřejného ochránce práv, m) Nejvyšším kontrolním úřadem, n) Úřadem pro zastupování státu ve věcech majetkových o) Správou úložišť radioaktivních odpadů, p) orgánem soudní moci, q) státním zastupitelstvím, r) zdravotní pojišťovnou, s) krajem, nebo t) hlavním městem Praha. II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou[5], c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností, f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.

Vyhláška o regulovaných službách

	II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou[5], c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností, f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.

Vyhláška o regulovaných službách

1. Veřejná správa

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Českou národní bankou, g) Policejním prezidiem, h) útvarem policie s celostátní působností, i) Generální inspekcí bezpečnostních sborů j) Generálním ředitelstvím hasičského záchranného sboru, k) krajským ředitelstvím hasičského záchranného sboru, l) Kanceláří Veřejného ochránce práv, m) Nejvyšším kontrolním úřadem, n) Úřadem pro zastupování státu ve věcech majetkových o) Správou úložišť radioaktivních odpadů, p) orgánem soudní moci, q) státním zastupitelstvím, r) zdravotní pojišťovnou, s) krajem, nebo t) hlavním městem Praha. II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je a) územně dekoncentrovaným (specializovaným) orgánem státní správy, b) profesní komorou[5], c) vysokou školou, d) Akademií věd České republiky, nebo e) obcí s rozšířenou působností, f) městským obvodem nebo městskou částí, která vykonává rozšířenou působnost.

Obcí zřizované organizace:

- **Nespadají automaticky „protože obec“**
  - **Typicky tedy ne základní a mateřské školy či městské knihovny**
- Spadají jen ty zřizované organizace, které samy naplní kritéria v jiném odvětví
  - **Obce se** ale k nim v rámci počítání velikosti podniků **nepřipočítávají**
  - Příklad: *Do počtu zaměstnanců pro posouzení velikosti podniku např. vodárny, která je zřízena obcí, ale má samostatné IČO, se počet zaměstnanců obce nepřipočítává.*

Vyhláška o regulovaných službách

1. Veřejná správa

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
1.1. Výkon svěřených pravomocí	Orgán nebo osoba je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že je a) ústředním orgánem státní správy, b) jiným správním úřadem s celostátní působností neuvedeným v písm. a), a to včetně ústředí a generálního ředitelství územně dekoncentrovaných (specializovaných) orgánů státní správy, c) Kanceláří prezidenta republiky, d) Kanceláří Senátu, e) Kanceláří Poslanecké sněmovny, f) Českou národní bankou,

Vymezení rozsahu řízení bezpečnosti informací: výkon svěřených pravomocí

Přenesená působnost obcí

- Evidence obyvatel
- Matrika
- Vidimace a legalizace
- Poskytování informace
- Stavební a silniční správní úřad
- Dopravní agenda
- Životní prostředí
- Přestupky
- Místní poplatky
- Právo shromažďování
- Sociální agenda
- Krizové řízení

Samostatná působnost obcí

- Správa vlastního majetku
- Místní referenda
- Vyřizování petic a stížností
- Poskytování dotací
- Odpadové hospodářství
- Poskytování informací
- Zřizování příspěvkových organizací a obecní policie
- Vydávání obecně závazných vyhlášek

Základní povinnosti dle nZKB

Ohlášení

Ohlášení regulované služby a nahlášení kontaktní osoby

Portál NÚKIB

Do 60 dní od naplnění podmínek pro registraci

Bezpečnostní opatření

Vyhláška o bezpečnostních opatřeních – nižší/vyšší režim

11 opatření nižší režim

1 rok od doručení rozhodnutí o registraci

Hlášení incidentů

Vychází ze zákona a vyhlášky o bezpečnostních opatřeních

Významné incidenty – nižší režim

1 rok od doručení rozhodnutí o registraci

Provedení protiopatření

Vydá a doručí NÚKIB

Reaktivní protiopatření/varování

Lhůty dané protiopatřením

Hlášení incidentů

Režim nižších povinností

Hlásí incidenty

které se projevily ve stanoveném rozsahu, mají původ v kybernetickém prostoru, mají významný dopad na poskytování regulované služby* a nelze u nich ve lhůtě podle § 16 odst. 1 vyloučit úmyslné zavinění

Národní CERT (CZ.NIC)

*významnost stanoví sám subjekt dle postupu ve vyhlášce o bezpečnostních opatřeních pro nižší režim

Proces hlášení a lhůty

- Do 24 hodin **od zjištění** incidentu:
  - Prvotní hlášení
- Do 72 hodin od zjištění incidentu:
  - Doplnění informací o incidentu
- Do 30 dnů od hlášení incidentu:
  - Závěrečná zpráva – jak byl incident vyřešen

Bezpečnostní opatření – rozdíly vyšší a nižší režim

organizační opatření – **vyšší** režim

1. systém řízení bezpečnosti informací,
2. povinnosti pro vrcholové vedení,
3. bezpečnostní role,
4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
5. řízení aktiv,
6. řízení rizik,
7. řízení dodavatelů,
8. bezpečnost lidských zdrojů,
9. řízení změn,
10. akvizice, vývoj a údržba,
11. řízení přístupu,
12. zvládání kybernetických bezpečnostních událostí a incidentů,
13. řízení kontinuity činností a
14. audit kybernetické bezpečnosti

technická opatření – **vyšší** režim

1. fyzická bezpečnost,
2. bezpečnost komunikačních sítí,
3. správa a ověřování identit,
4. řízení přístupových oprávnění,
5. detekce kybernetických bezpečnostních událostí,
6. zaznamenávání událostí,
7. vyhodnocování kybernetických bezpečnostních událostí,
8. aplikační bezpečnost,
9. kryptografické algoritmy,
10. zajišťování dostupnosti regulované služby,
11. zabezpečení průmyslových, řídících a obdobných specifických aktiv

bezpečnostní opatření – **nižší** režim

1. zajišťování kybernetické bezpečnosti,
2. povinnosti vrcholového vedení,
3. bezpečnost lidských zdrojů,
4. řízení kontinuity činností,
5. řízení přístupu,
6. řízení identit a jejich oprávnění,
7. detekce a zaznamenávání kybernetických bezpečnostních událostí,
8. řešení kybernetických bezpečnostních incidentů,
9. bezpečnost komunikačních sítí,
10. aplikační bezpečnost,
11. kryptografické algoritmy

➢ **Redukovaná bezpečnostní opatření pro nižší režim**

Bezpečnostní opatření pro nižší a vyšší režim - rozdíl

NIŽŠÍ REŽIM

§ 7
Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

a) stanoví prioritu technických aktiv, pořadí a postupy jejich obnovy a zohlední přitom stanovenou prioritu relevantního primárního aktiva podle § 5 písm. f),

b) stanoví dílčí odpovědnosti a povinnosti pro zajištění kontinuity činností a k obnově podle písmene a), a

c)vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

VYŠŠÍ REŽIM

§ 16
Řízení kontinuity činností

1. Povinná osoba v rámci řízení kontinuity činností
a) stanoví metodiku pro provedení analýzy dopadů,
b) pomocí analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a zohlední hodnocení rizik podle § 9, v rámci kterého posoudí možná rizika související s ohrožením kontinuity činností,
c) na základě výstupů analýzy dopadů a hodnocení rizik podle písmene b) stanoví cíle řízení kontinuity činností formou určení
   i) minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu regulované služby,
   ii) doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb regulované služby a
   iii) bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání,
d) stanoví politiku řízení kontinuity činností, která obsahuje naplnění cílů podle písmene c) a stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role,
e) vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a plány obnovy související s poskytováním regulované služby a
f) realizuje bezpečnostní opatření pro zvýšení odolnosti podle § 27.
2. Cíle řízení kontinuity podle odst. 1 písm. c) tohoto ustanovení jsou stanoveným časem a kvalitou regulované služby podle § X [Zajištění dostupnosti strategicky významné služby] zákona. Stanoveným časem je doba obnovení chodu podle odst. 1 písm. c) bod ii) tohoto ustanovení a stanovenou kvalitou regulované služby je minimální úroveň poskytovaných služeb podle odst. 1 písm. c) bodu i) tohoto ustanovení.

Bezpečnostní opatření – povinné nevyloučitelné minimum

bezpečnostní opatření – **nižší** režim

1. **zajišťování kybernetické bezpečnosti,**
2. **povinnosti vrcholového vedení,**
3. **bezpečnost lidských zdrojů,**
4. **řízení kontinuity činností,**
5. řízení přístupu,
6. řízení identit a jejich oprávnění,
7. detekce a zaznamenávání kybernetických bezpečnostních událostí,
8. **řešení kybernetických bezpečnostních incidentů,**
9. bezpečnost komunikačních sítí,
10. aplikační bezpečnost,
11. kryptografické algoritmy.

Jak se na zákon připravit?

Přehled v organizaci

- Jaké vykonávám agendy a poskytuji služby?
- Co pro výkon agend potřebuji?

= rozsah, ve kterém KB řeším

Aktuální stav KB

- Mám již některá opatření?

= aktuální stav zavedených a nezavedených opatření

Určení priorit

- Jaké mám finanční a personální kapacity?
- Co je má prioritní služba?

= provedu analýzy, stanovím plán

Zavádění opatření

- Osoba zodpovědná za KB.
- Vzdělávání zaměstnanců (i vedení)
- Bezpečnostní politika

= pokračuji dle plánu

Zásada přiměřenosti:

- Náklady na zaváděné opatření by neměly převyšovat náklady na případnou realizaci kybernetického incidentu.
- Nechci všechno najednou, postupně se zlepšuji.

Vzdělávání:

- E-learning zdarma od NÚKIB

Regulace cloudových služeb

BEZPEČNOSTNÍ ÚROVNĚ

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

- Stanoví bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci
- 4 bezpečnostní úrovně:

NÍZKÁ

STŘEDNÍ

VYSOKÁ

KRITICKÁ

- Stanovení bezpečnostní úrovně dle úrovně dopadu kybernetického bezpečnostního incidentu

Úroveň dopadu	Oblast dopadu								
	A. Bezpečnost a zdraví lidí	B. Ochrana osobních údajů	C. Trestněprávní řízení	D. Veřejný pořádek	E. Mezinárodní vztahy	F. Řízení a provoz	G. Důvěryhodnost	H. Finanční model	I. Zajišťování služeb

BEZPEČNOSTNÍ ÚROVNĚ

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

Základní principy hodnocení dopadů:

- Nezkoumat příčiny narušení bezpečnosti
- Identifikovat opravdu nejhorší možné scénáře
- Neřešit pravděpodobnost výskytu těchto scénářů
- Neuvažovat jakákoliv bezpečnostní opatření

Národní centrum kybernetické bezpečnosti

Národní úřad pro kybernetickou a informační bezpečnost

Záznam o procesu stanovení bezpečnostní úrovně poptávaného cloud computingu

A: Údaje o orgánu veřejné moci

Název:

Adresa sídla:

Identifikační číslo (IČO):

B: Identifikace informačního nebo komunikačního systému, jehož provozování je poptáváno pomocí cloud computingu

Označení systému:

Je řešení pomocí cloud computingu poptáváno pro informační nebo komunikační systém jako pro celek?

V případě, že je řešení pomocí cloud computingu poptáváno jen pro část informačního nebo komunikačního systému, definujte ji z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti:

C: Výsledná bezpečnostní úroveň

Výsledná bezpečnostní úroveň informační nebo komunikačního systému nebo jeho části:

D: Zhodnocení bezpečnostní úrovně podle přílohy č. 1 vyhlášky

Oblast dopadu	Nejvyšší dosažená úroveň dopadu v příslušné oblasti	Odůvodnění*
A. Bezpečnost a zdraví lidí	z pohledu narušení dostupnosti z pohledu narušení důvěrnosti z pohledu narušení integrity	
B. Ochrana osobních údajů	z pohledu narušení dostupnosti z pohledu narušení důvěrnosti z pohledu narušení integrity	
C. Trestněprávní řízení	z pohledu narušení dostupnosti z pohledu narušení důvěrnosti z pohledu narušení integrity	
D. Veřejný pořádek	z pohledu narušení dostupnosti z pohledu narušení důvěrnosti z pohledu narušení integrity	

BEZPEČNOSTNÍ ÚROVNĚ

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

- Výsledná bezpečnostní úroveň

  = **nejvyšší úroveň dopadu**

- Nejvyšší stanovená bezpečnostní úroveň informačního nebo komunikačního systému jako celku musí být stanovena alespoň pro jednu část informačního nebo komunikačního systému

D: Zhodnocení bezpečnostní úrovně podle přílohy č. 1 vyhlášky		
Oblast dopadu	**Nejvyšší dosažená úroveň dopadu v příslušné oblasti**	**Odůvodnění**
A. Bezpečnost a zdraví lidí	z pohledu narušení dostupnosti	*Narušení dostupnosti, důvěrnosti či integrity Evidence žadatelů a uživatelů sociálních služeb (dále jen "Evidence") nemůže přímo jakkoli způsobit zranění jednotlivce ani skupiny lidí.* *Evidence slouží pouze jako jmenný seznam osob, není zde tedy jakákoli možnost ohrožení jejich zdraví či bezpečnosti.*
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	NÍZKÁ	
	z pohledu narušení integrity	
	NÍZKÁ	
B. Ochrana osobních údajů	z pohledu narušení dostupnosti	*Narušení bezpečnosti informací v rámci Evidence může negativně ovlivnit poptávaný cloud computing, který naplňuje dvě a více kritérií z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů. Konkrétně je naplněno kritérium a) a b) z druhé skupiny kritérií, jelikož jsou zpracovávány zvláštní kategorie osobních údajů uživatelů systému a tímto zpracováním bude určitě dotčeno více než 10000 subjektů údajů.*
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	VYSOKÁ	
	z pohledu narušení integrity	
	VYSOKÁ	

BEZPEČNOSTNÍ PRAVIDLA

Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

- Stanovuje obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu
- Každá z bezpečnostních úrovní dle vyhlášky o bezpečnostních úrovních má příslušná bezpečnostní pravidla
- Jejich účelem je zajištění bezpečnosti informací při využívání služeb cloud computingu OVM

- Výkladové zúžení NÚKIB – stejná množina povinných osob jako v případě ZoISVS

BEZPEČNOSTNÍ PRAVIDLA

Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

1. Obecné podmínky pro službu cloud computingu
2. Organizace bezpečnosti informací
3. Politiky
4. Fyzická bezpečnost
5. Zajištění provozu služby cloud computingu
6. Správa identit a řízení přístupu
7. Správa klíčů a šifrování
8. Zabezpečení komunikace
9. Přenositelnost, propojení a exit strategie
10. Nákup vývoj a úprava informačních systémů
11. Řízení dodavatelů
12. Správa kybernetických bezpečnostních událostí a incidentů
13. Řízení kontinuity činností
14. Soulad s předpisy a audit
15. Žádosti cizozemských orgánů o zpřístupnění nebo předání dat

POŽADAVKY NA POSKYTOVATELE

- § 6m ZoISVS – Požadavky na poskytovatele
  - *a) způsobilé zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy,*
  - *b) bezúhonné v rozsahu bezúhonnosti požadované po kvalifikovaném správci kvalifikovaného systému elektronické identifikace,*
  - *c) způsobilé pro poskytnutí cloud computingu orgánu veřejné správy z hlediska **veřejného pořádku, bezpečnosti a dodržování práv třetích osob**.*
- § 6n ZoISVS – Požadavky na služby
  - *b) který **umožňuje dosažení** alespoň **základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací** orgánu veřejné správy,*
  - *c) který umožňuje orgánu veřejné správy postupovat podle **bezpečnostních pravidel** pro orgány veřejné moci využívající služby cloud computingu podle právního předpisu upravujícího kybernetickou bezpečnost,*
  - *d) jehož **bezpečnostní úroveň je stejná nebo vyšší** než bezpečnostní úroveň informačního systému veřejné správy nebo jeho části, k zajištění jehož provozu je využíván,*

POŽADAVKY PRO ZÁPIS DO KATALOGU CC

Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

- Sada bezpečnostních požadavků a podmínek, které musí poskytovatel CC služeb splnit, aby mohl dodávat orgánům veřejné správy
- Cloudové služby rozděleny do 4 úrovní podle požadavku na bezpečnost

Strana 3772 Sbírka zákonů č. **316** / 2021 Částka 140

316

VYHLÁŠKA

ze dne 24. srpna 2021

o některých požadavcích pro zápis do katalogu cloud computingu

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 12 odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 261/2021 Sb., (dále jen „zákon"):

§ 1

Předmět úpravy

Tato vyhláška stanoví

a) požadavky na způsobilost poskytovatele cloud computingu (dále jen „poskytovatel") zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona,

b) požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nabízeným cloud computingem podle § 6n písm. b) zákona,

c) seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c) zákona, doklady o jejich splnění a intervaly pro předkládání těchto dokladů podle § 6t odst. 6 písm. g) a § 6t odst. 7 písm. h) zákona.

§ 2

Základní pojmy

Pro účely této vyhlášky se rozumí

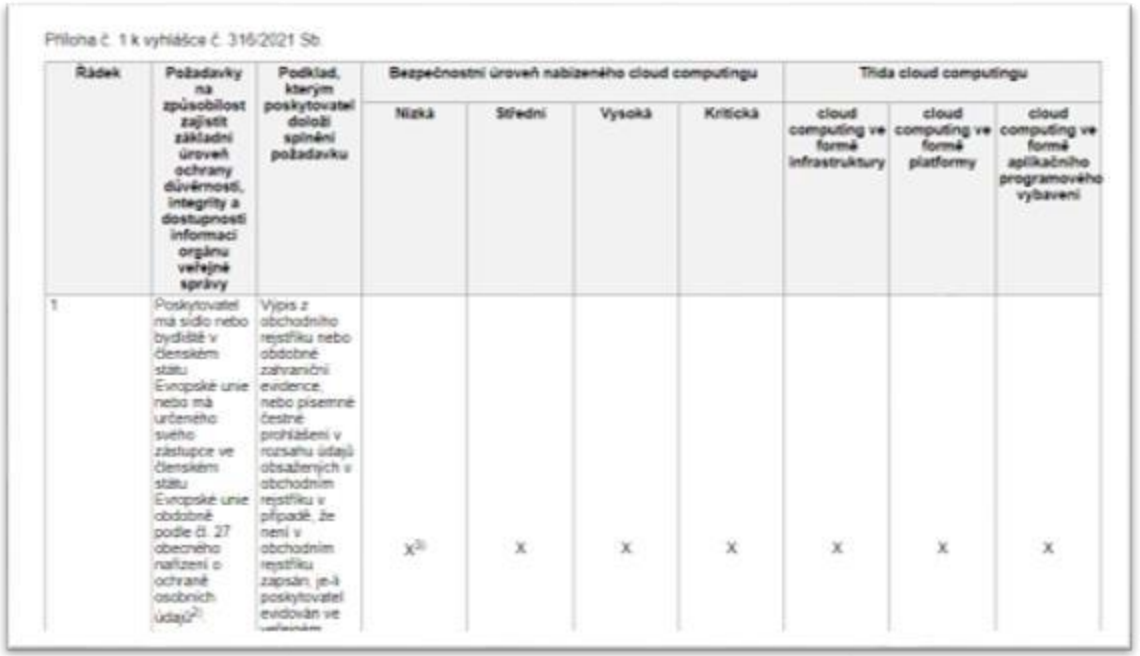
a) zákazníkem orgán veřejné správy využívající službu cloud computingu,

b) uživatelem ten, kdo službu cloud computingu prostřednictvím systému orgánu veřejné správy využívá nebo ji nastavuje,

c) zákaznickými daty všechna data, která jsou uživatelem poskytnuta poskytovateli v průběhu užívání služby cloud computingu,

d) zákaznickým obsahem textová, zvuková, audiovizuální, obrazová nebo jiná data, která byla uživatelem do služby cloud computingu vložena, a to bez jejich metadat, a indexy k těmto datům,

e) provozními údaji data vygenerovaná nebo odvozená poskytovatelem v souvislosti s poskyto-



Příloha č. 1 k vyhlášce č. 316/2021 Sb.

Řádek	Požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy	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	Poskytovatel má sídlo nebo bydliště v členském státu Evropské unie nebo má určeného svého zástupce ve členském státu Evropské unie obdobně podle čl. 27 obecného nařízení o ochraně osobních údajů[2])	Výpis z obchodního rejstříku nebo obdobné zahraniční evidence, nebo písemné čestné prohlášení v rozsahu údajů obsažených v obchodním rejstříku v případě, že není v obchodním rejstříku zapsán, je-li poskytovatel evidován ve	x[3])	x	x	x	x	x	x

NOVELIZACE 2025

- Přesun ze ZKB do ZoISVS
  - Povinnosti zařadit do BÚ a dodržovat BP
  - Zmocnění k vyhláškám o BÚ a BP
  - Sjednocení adresátů
  - Zavedení přestupků
- Znovuvydání všech cloudových vyhlášek
  - Vlastní legislativní proces
  - U vyhlášky o požadavcích pro zápis do katalogu cloud computingu **30 dní**

PŘEHLED HLAVNÍCH NOVELIZAČNÍCH BODŮ

- Nová koncepce bezúhonnosti za přestupky
- Zpřehlednění a zlepšení UX
- Rozšíření množiny akceptovatelných auditních zpráv
- Odstranění požadavku na dostupnost zapisované služby
- Úprava požadavků na penetrační testování a skeny zranitelnosti
- Úprava požadavků na šifrování
- Explicitně uvedená povinnost dokládat čestné prohlášení, pokud není zapisovaná služba jmenovitě uvedená v daném dokumentu

KDE NAJÍT INFORMACE?

- Podpůrné materiály:

  Obecně:

  - Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály (gov.cz)

  Ke cloud computingu:

  - Národní úřad pro kybernetickou a informační bezpečnost - Materiály k regulaci cloud computingu (gov.cz)

- Nejčastější dotazy:
  - Národní úřad pro kybernetickou a informační bezpečnost - FAQ (gov.cz)
- Služby, které trvale ukládají data mimo EU – Úřední deska NÚKIB
  - Národní úřad pro kybernetickou a informační bezpečnost - Cloud computing - výjimky z uložení dat (gov.cz)

Děkuji za pozornost

Kam s dotazy?

regulace@nukib.gov.cz

! https://portal.nukib.gov.cz/ !