Požadavky na poskytovatele cloud computingu – nová regulace

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

8. března 2022
TLP: WHITE

Martin Klumpar
Odbor regulace

Co je cloud computing?

Definice zákona č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS)

§ 2 písm. x) 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

Důvody regulace cloud computingu

- Využití cloudových služeb jak v soukromém tak ve veřejném sektoru rychle roste.
- Cloudové služby mohou přispět k:
  - ekonomičtějšímu provozu a
  - bezpečnějšímu provozu informačních systémů (centrálnímu řízení, dohled a aktualizace).
- Cloudové služby však přináší i nová rizika:
  - místo zpracování dat mnohdy v zahraničí a často neznámé jednotlivým zákazníkům využívajících cloudové služby;
  - nutnost brát v úvahu i relevantní prvky **právního řádu** třetí země – přístup cizozemských orgánů k datům (GDPR, SD EU Schrems II);
  - velká závislost na poskytovateli a omezené možnosti prověření poskytovatele;
  - obtížný přístup pro české „law enfforcement“ složky k datům o trestné činnosti.

Hlavní body regulace cloud computingu

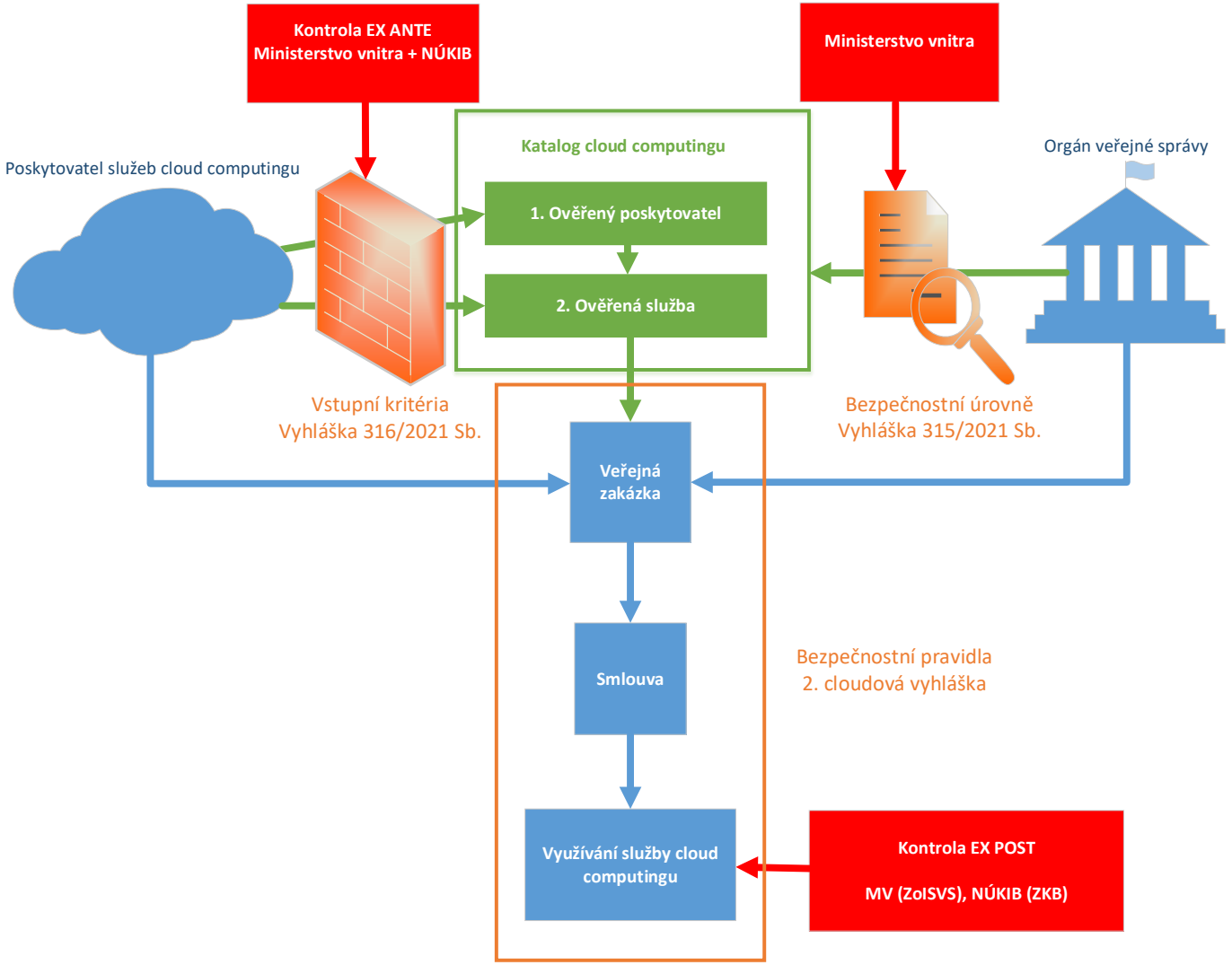
- DŮVĚRA
  - prověření **poskytovatele** cloud computingové služby z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob
  - požadavky na službu cloud computingu = VSTUPNÍ KRITÉRIA
  - prověření poskytovatele i služby omezené – ex ante, kapacity = závislost na vyjádření poskytovatele

- TRANSPARENTNOST
  - požadavky na informování o zpracování dat (kde, proč, jak dlouho), vývoz mimo EU pouze v nezbytných případech

- ODPOVĚDNOST
  - orgán veřejné moci stále nese odpovědnost za bezpečnost informací i v případě využití cloudových služeb
  - klasifikace informačního systému orgánu veřejné moci = BEZPEČNOSTNÍ ÚROVNĚ
  - zajistit splnění BEZPEČNOSTNÍCH PRAVIDEL

- Podmínkou vypsání veřejné zakázky na službu cloud computingu je, že bezp. úroveň nabízené služby cloud computingu ≥ bezp. úroveň inf. syst. veřejné správy (ZoISVS).

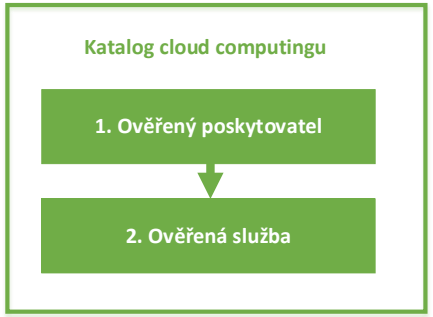
Regulatorní rámec cloud computingu – ZoISVS + ZKB



Požadavky na správce ISVS- ZoISVS

§ 6l ZoISVS
Základní pravidla využívání cloud computingu orgánem veřejné správy
(1) Orgán veřejné správy může využívat pouze cloud computing, který splňuje požadavky podle § 6n a je poskytovaný

a) poskytovatelem státního cloud computingu nebo poskytovatelem cloud computingu zapsaným v katalogu cloud computingu na základě nabídky cloud computingu tohoto poskytovatele zapsané v okamžiku jejího přijetí orgánem veřejné správy v katalogu cloud computingu,
b) v rámci vertikální nebo horizontální spolupráce podle právního předpisu upravujícího zadávání veřejných zakázek nebo
c) v rámci obecné výjimky z povinnosti zadat veřejnou zakázku v zadávacím řízení podle právního předpisu upravujícího zadávání veřejných zakázek. (…)



Požadavky na správce ISVS- ZoISVS

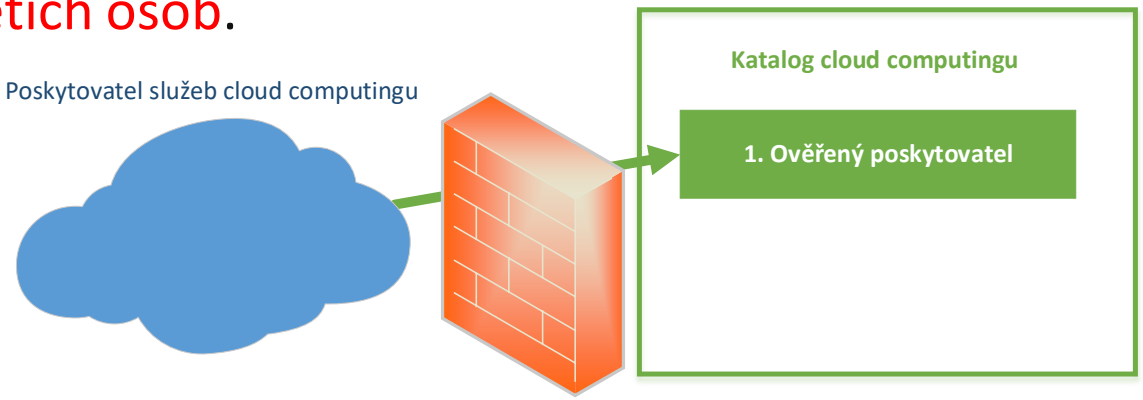
§ 6l ZoISVS
Základní pravidla využívání cloud computingu orgánem veřejné správy
(4) Odstavce 1 až 3 se nepoužijí v případě cloud computingu, který slouží výlučně
a) ke správě a řešení technických potíží nebo diagnostice programových anebo technických prostředků, případně k zabezpečení nebo přenosu s tím souvisejících signálů,
b) ke správě nebo využívání prostředků pro elektronickou identifikaci využívajících vícefaktorové autentizace,
c) k aktualizaci nebo opravě programového prostředku, nebo
d) ke shromažďování nebo výměně provozních údajů,
e) ke zkušebnímu provozu informačního systému veřejné správy, pokud při něm nebudou využity údaje, které se v informačním systému veřejné správy vedou nebo povedou anebo které jsou nebo budou v souvislosti s poskytováním služby informačního systému veřejné správy využívány.

Požadavky na poskytovatele cloud computingu - ZoISVS

§ 6m ZoISVS

Požadavky na poskytovatele cloud computingu poskytujícího cloud computing orgánu veřejné správy

- **(1)** Poskytovatelem cloud computingu poskytujícím cloud computing orgánu veřejné správy může být pouze osoba nebo jiné právní uspořádání, které jsou
- **a)** způsobilé zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy, *= vyhláška č. 316/2021 Sb.*
- **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.



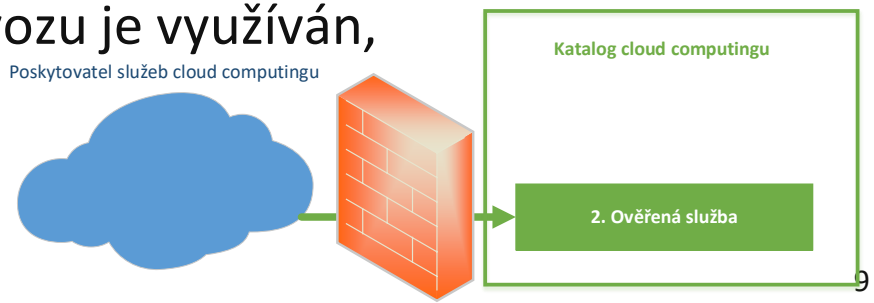
Požadavky na cloud computingu - ZoISVS

§ 6n ZoISVS

Požadavky na cloud computing využívaný orgánem veřejné správy

- Orgán veřejné správy může využívat a poskytovatel cloud computingu může orgánu veřejné správy nebo poskytovateli státního cloud computingu poskytovat pouze cloud computing,
- **a)** který umožňuje splnění požadavků kladených na informační systém veřejné správy informační koncepcí České republiky,
- **b)** který umožňuje dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy, *= vyhláška č. 316/2021 Sb.*
- **c)** který umožňuje orgánu veřejné správy postupovat podle bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu podle právního předpisu upravujícího kybernetickou bezpečnost, *= připravovaná vyhláška o bezpečnostních pravidlech*
- **d)** jehož bezpečnostní úroveň je stejná nebo vyšší než bezpečnostní úroveň informačního systému veřejné správy nebo jeho části, k zajištění jehož provozu je využíván,

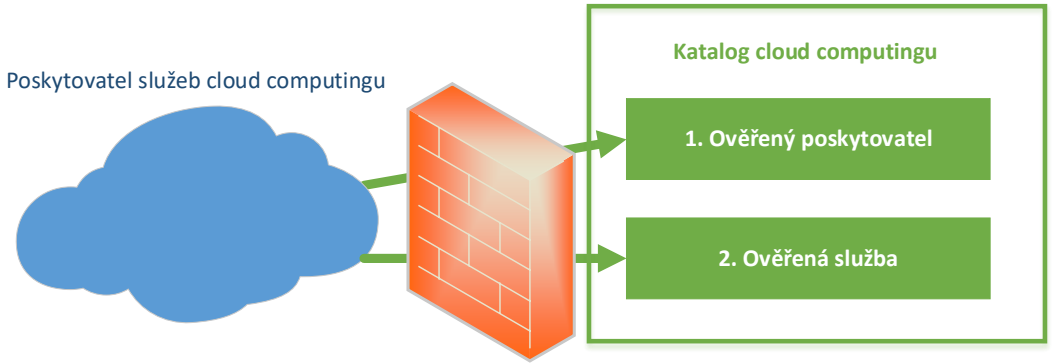
(…)



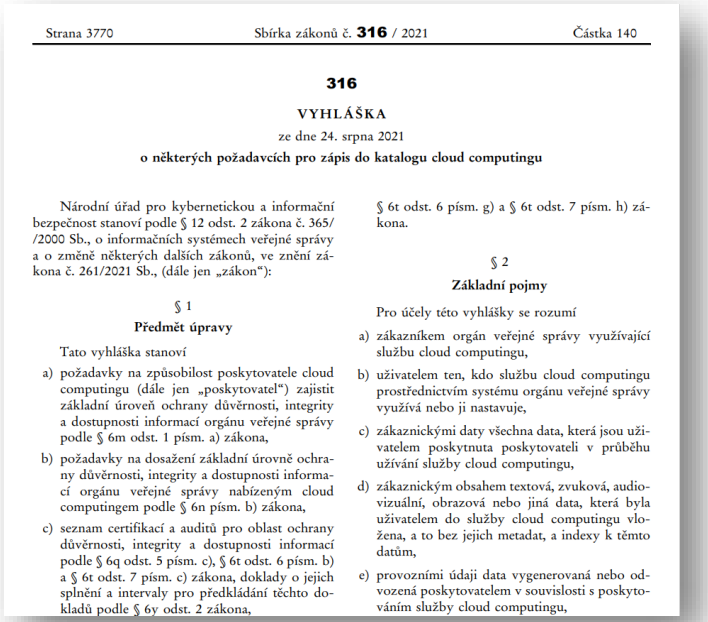
Vyhláška o požadavcích pro zápis do katalogu

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

- ÚČINNÁ OD 1. 9. 2021
- Tzv. vyhláška o vstupních kritériích
- Sada 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
  - 4. BÚ pouze státní poskytovatel
- Jednotliví dodavatelé služeb musí splnit vstupní požadavky
- Naplnění požadavků posoudí MV a NÚKIB = správní řízení



Vstupní kritéria
Vyhláška 316/2021 Sb.



Strana 3770 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 § 6y odst. 2 zákona,

§ 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 poskytováním služby cloud computingu,

Uložení a zpracování dat

§ 6k odst. 2, písm. c, bod 3 ZoISVS

- údaje o **předpokládaném místu zpracování informací** orgánu veřejné správy a **předpokládané době**, **předpokládaném rozsahu** a **předpokládaném účelu** zpracování informací orgánu veřejné správy v tomto místě, případně o tom, že nabízený cloud computing **vyžaduje dlouhodobé uložení informací orgánu veřejné správy** mimo území Evropské unie,

Příloha č. 2, část 1 vyhlášky 316/2021 Sb.

ULOŽENÍ NEAKTIVNÍCH ZÁKAZNICKÝCH DAT A SPECIFICKÝCH PROVOZNÍCH ÚDAJŮ

- Uložení neaktivních dat v EU nebo výjimka uvedená na webu NÚKIB

https://www.nukib.cz/cs/uredni-deska/cloud-computing/

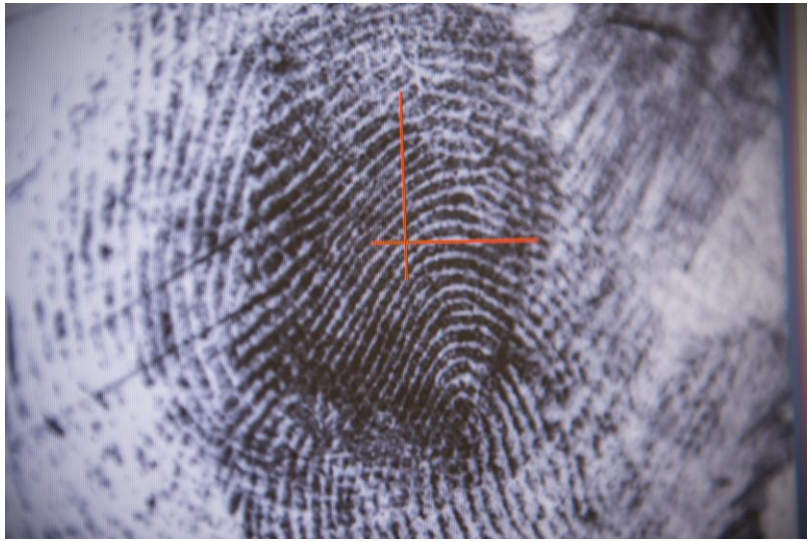
ZPRACOVÁNÍ ZÁKAZNICKÝCH DAT A SPECIFICKÝCH PROVOZNÍCH ÚDAJŮ

- Buď v EU nebo v Katalogu eGC informace o předpokládaném místě, době, času zpracování
- Ve 4. BÚ zpracování dat na území ČR – mimo ČR s explicitním souhlasem zákazníka (servis)

Zpřístupňování a předávání dat

Příloha č. 2, část 2 vyhlášky 316/2021 Sb.

- v případě žádostí cizozemských orgánů
- informovat zákazníka, pokud zakázáno informovat tak usilovat o zrušení zákazu informovat
- zkoumat legálnost žádosti + záznam o zkoumání
- usilovat o nevydání dat před soudem
- popsat právní povinnosti ke zpřístupňování a předávání dat ve státech, kde jsou data zpracovávána
- 4. BÚ – žádost cizozemského orgánu odmítnout, data nevydat



Oprávnění k provedení kontroly

§ 6i odst. 2 a 3 ZoISVS

- Ministerstvo kontroluje, zda cloud computing poskytovaný orgánům veřejné správy **splňuje požadavky podle § 6n** a kvalitu tohoto cloud computingu
- Národní úřad pro kybernetickou a informační bezpečnost kontroluje, zda cloud computing poskytovaný orgánům veřejné správy **splňuje požadavky podle § 6n**, v případě, že je využíván k provozování informačního systému veřejné správy, který je informačním nebo komunikačním systémem kritické informační infrastruktury, významným informačním systémem nebo informačním systémem základní služby podle právního předpisu upravujícího kybernetickou bezpečnost.

Příloha č. 2, část 3 vyhlášky 316/2021 Sb.

- Požadavek na poskytovatele umožnit provést kontrolu MV a NÚKIB – jednou ročně nebo v případě opakovaných kybernetických bezpečnostních incidentů

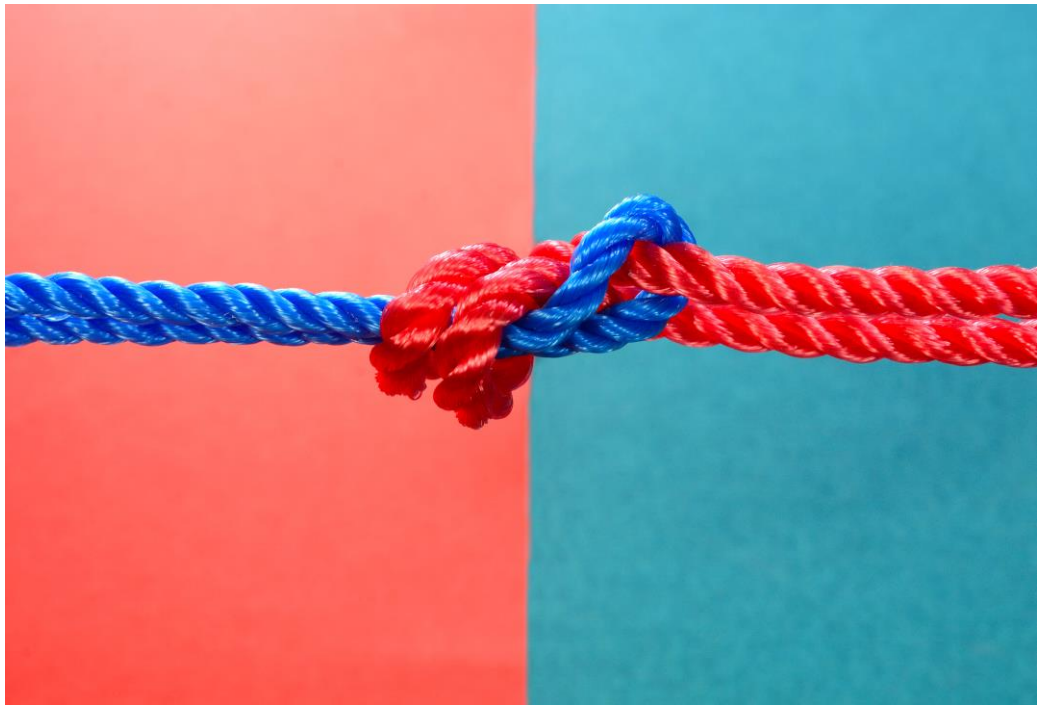
Úrovně dostupnosti služby & připojení do IXP

Příloha č. 2, část 4 vyhlášky 316/2021 Sb.

- směřuje na schopnost poskytovatele, orgán veřejné správy může dojednat nižší dostupnost
- od 96,16 % po 99,99%

Příloha č. 2, část 5 vyhlášky 316/2021 Sb.

- poskytovatel připojen do výměnného uzlu internetu v ČR



Kontinuita & zálohy & odolnost datacenter

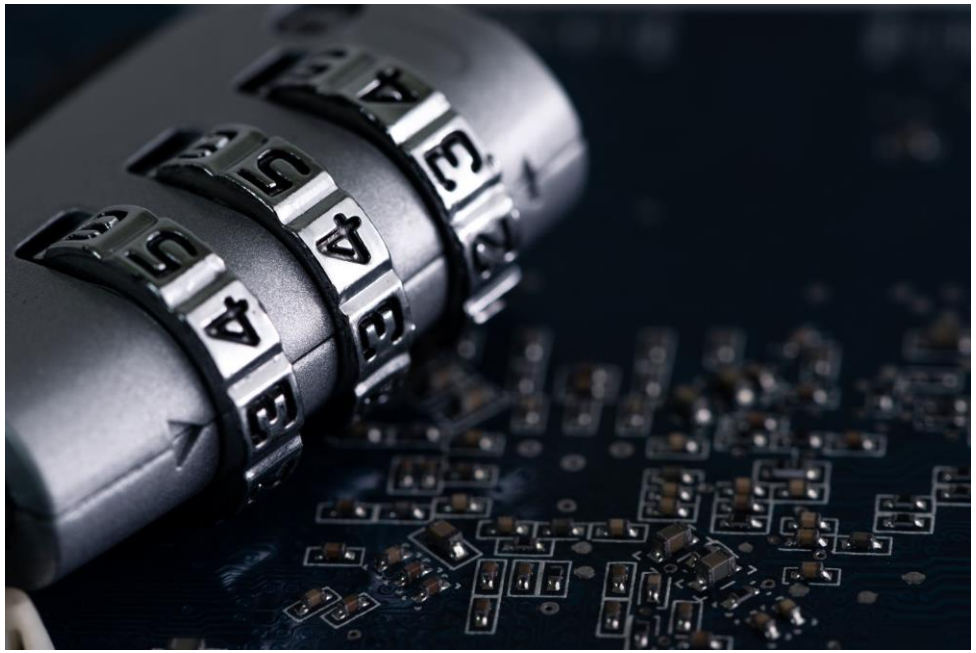
Příloha č. 2, část 6 vyhlášky 316/2021 Sb.

- plán kontinuity a plán na obnovu po havárii
- OVS by mělo mít vytvořeny své BCDR plány, mělo by zohlednit plány poskytovatele
- synchronní zálohy alespoň do jednoho záložního datového centra – je na OVS za využije
- dostatečná vzdálenost datacenter (50km) nebo přijetí odpovídajících opatření ke snížení rizik – výčet rizik, která třeba zohlednit jsou v příloze č. 5
- datacentra alespoň ve dvou státech nebo v ČR, 4. BÚ datacentra jen v ČR (vyjma zašifrované zálohy na území jiného státu EU/ESVO– ozbrojený konflikt atp.)
- poskytovatel nabízí ochranu před DoS/DDoS útoky

Nakládání s daty

Příloha č. 2, část 7 vyhlášky 316/2021 Sb.

- poskytovatel nabízí export dat na vyměnitelných médiích
- ochrana dat při přenosu a uložení šifrováním, nabízí algoritmy dle doporučení NÚKIB
- vlastní klíč generovaný nebo uložený v HSM
- likvidace klíčů při ukončení služby
- záznam o přístupu pracovníků poskytovatele k datům OVS (bez souhlasu OVS)
  - umožnit přístup OVS k záznamům o přístupu k datům



Certifikace

Příloha č. 2, část 8 vyhlášky 316/2021 Sb.

- ISO 27001 - akreditované
- ISO 27017, ISO 27018
- od 1. 1. 2024 i SOC2 nebo C5 (možná EUCS dle vývoje)

- aktuální certifikáty dokládat každých 15 měsíců evidence v katalogu

Monitoring KBU a informování o KBI

Příloha č. 2, část 9 vyhlášky 316/2021 Sb.

- nástroj na sledování událostí (SIEM)
  - události ve vztahu je konkrétnímu OVS zpřístupnit do 24 hodin

- informovat OVS v případě bez odkladu nejpozději do 72 hodin

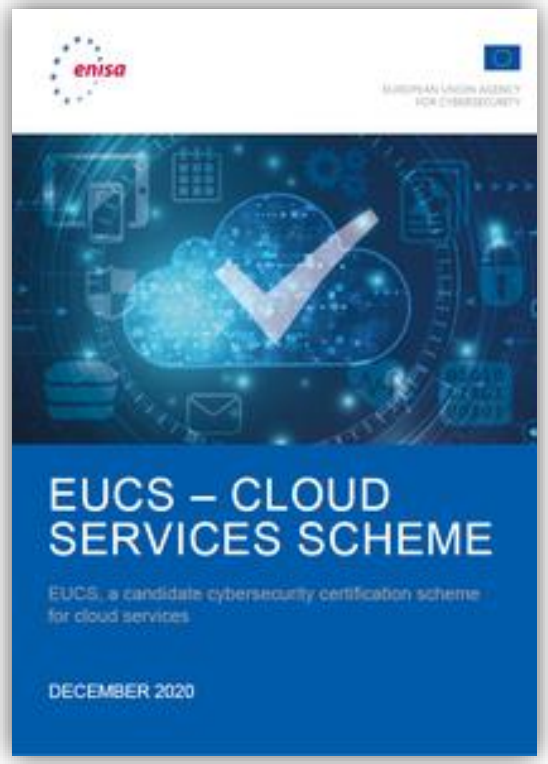
Skeny a penetrační testy

Příloha č. 2, část 10 vyhlášky 316/2021 Sb.

- Pravidelné skeny zranitelností
  - 3 skeny při zápisu, 4 skeny každých 24 měsíců nebo auditní zpráva, že provádí skeny
- Pravidelné penetrační testy
  - provedené subjektem, který je nezávislý na poskytovateli
  - při zápisu do katalogu ne starší 24 měsíců a pak každých 24 měsíců

Pohled do budoucna a EU

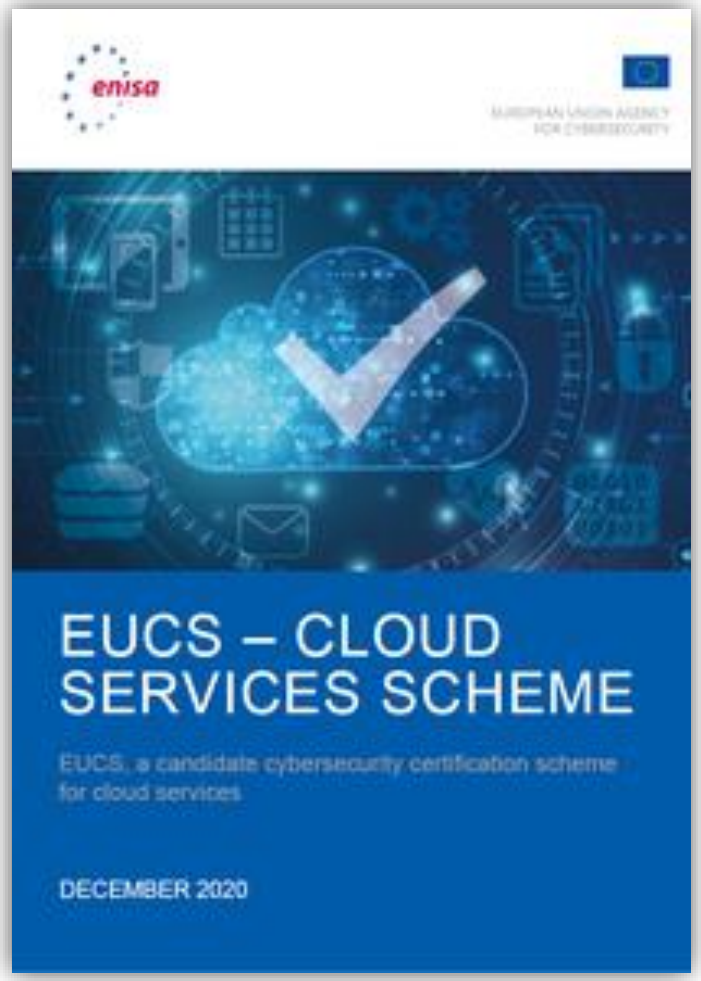
EUCS – Evropská certifikace cloudových služeb



Směrnice NIS/2

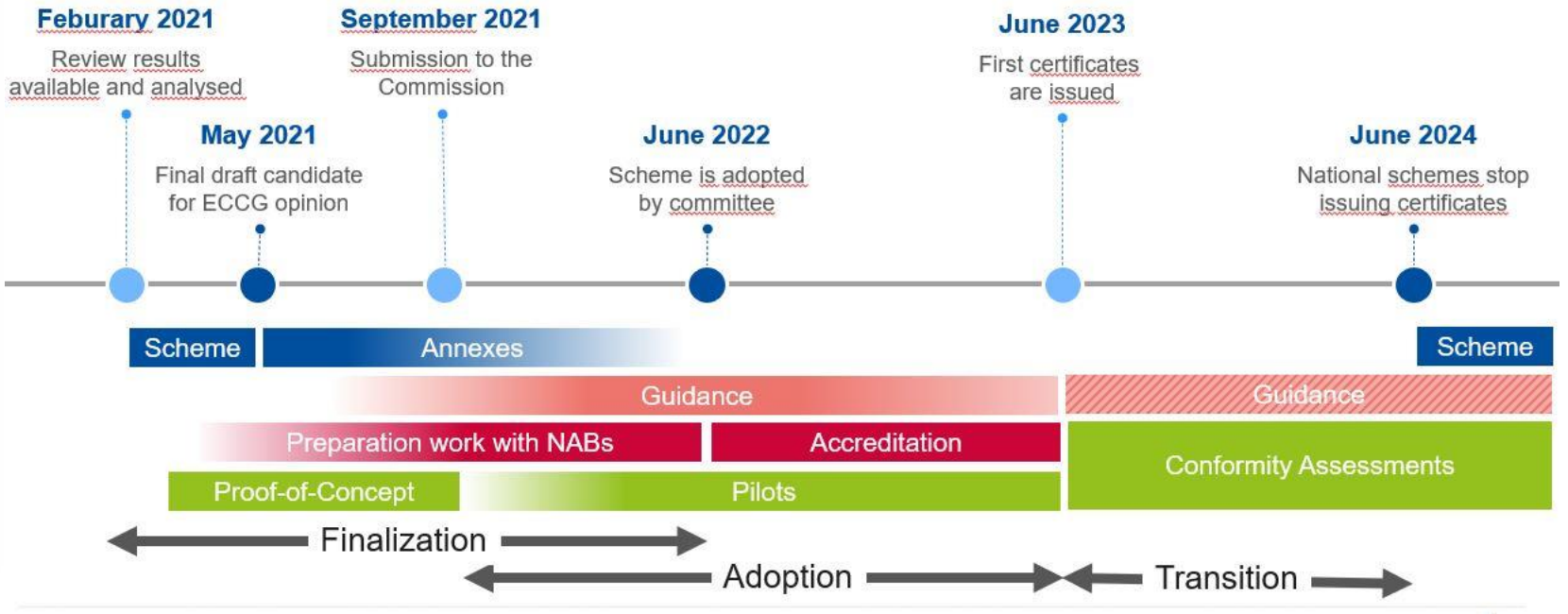
- Směrnice NIS
  - Poskytovatelé cloudových služeb = DSP
- Směrnice NIS2 (2022?)
  - Poskytovatelé cloudových služeb = Essential and important entities

Evropská certifikace cloudových služeb = EUCS



= technický nástroj k poskytnutí informací zákazníkům pro učinění informovaného rozhodnutí

- aktuálně zpoždění +6m



Vztah regulace cloudu v ČR a EUCS

- Po zavedení EUCS a vyřešení některých výhrad bude možné přizpůsobit národní regulaci EUCS:
  - úprava VSTUPNÍCH KRITÉRIÍ
    - umožnění předložení EUCS certifikátu + dodatečné požadavky k místu zpracování dat a prověření poskytovatele cloudové služby
  - úprava BEZPEČNOSTNÍCH PRAVIDEL
    - sjednocení znění bezpečnostních pravidel s požadavky na poskytovatele cloudových služeb v EUCS + požadavky týkající se výhradně orgánu veřejné moci

Cloudové vyhlášky - kde najít informace

- Vyhlášky, včetně odůvodnění:
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/
- Nejčastější dotazy:
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/
- Katalog cloud computingu – zapsané nabídky a poptávky:
  - https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09NQ%3d%3d
- Služby, které trvale ukládají data mimo EU – Úřední deska NÚKIB - https://www.nukib.cz/cs/uredni-deska/ - od nové právní úpravy – zatím prázdné

Dotazy?

Děkuji za pozornost!

regulace@nukib.cz