Kybernetická bezpečnost veřejné správy

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

7. září 2021
TLP: WHITE

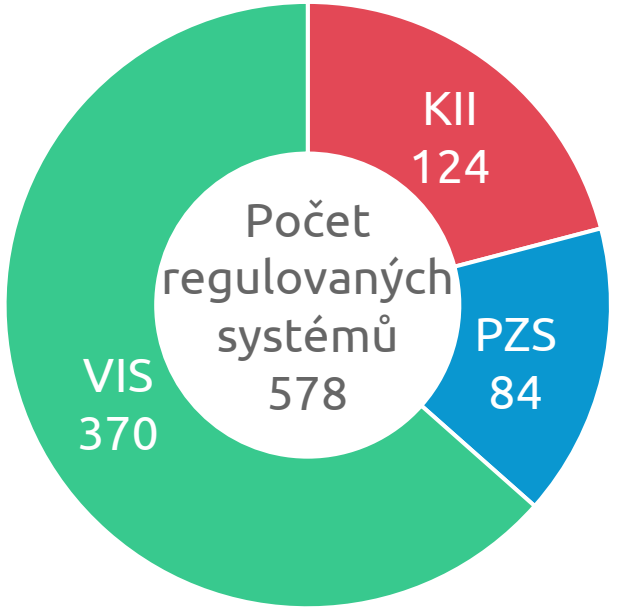
Adam Kučínský
ředitel
Odbor regulace

Obsah

- Počty povinných osob pod ZKB
- Vyhláška o VIS
- Regulace využívání cloud computingu veřejnou správou

Počty povinných osob pod ZKB a řešených incidentů

- V současné době spadá do působnosti ZKB 578 systémů z toho je:
  - VIS 370
  - KII 124
  - PZS 84
- Počty kybernetických incidentů řešených Vládním CERT



- Počet kybernetických útoků roste a útočníci se zlepšují.
- Dochází ke komoditizaci útoků.
- Dopady útoků se zvyšují s rostoucí závislostí na ICT.

Vyhláška o VIS

Cíl:

- Zjednodušit **a zpřehlednit proces identifikace**
- Zvýšit **efektivnost** vyhlášky
- Zvýšit **právní jistotu** adresátů

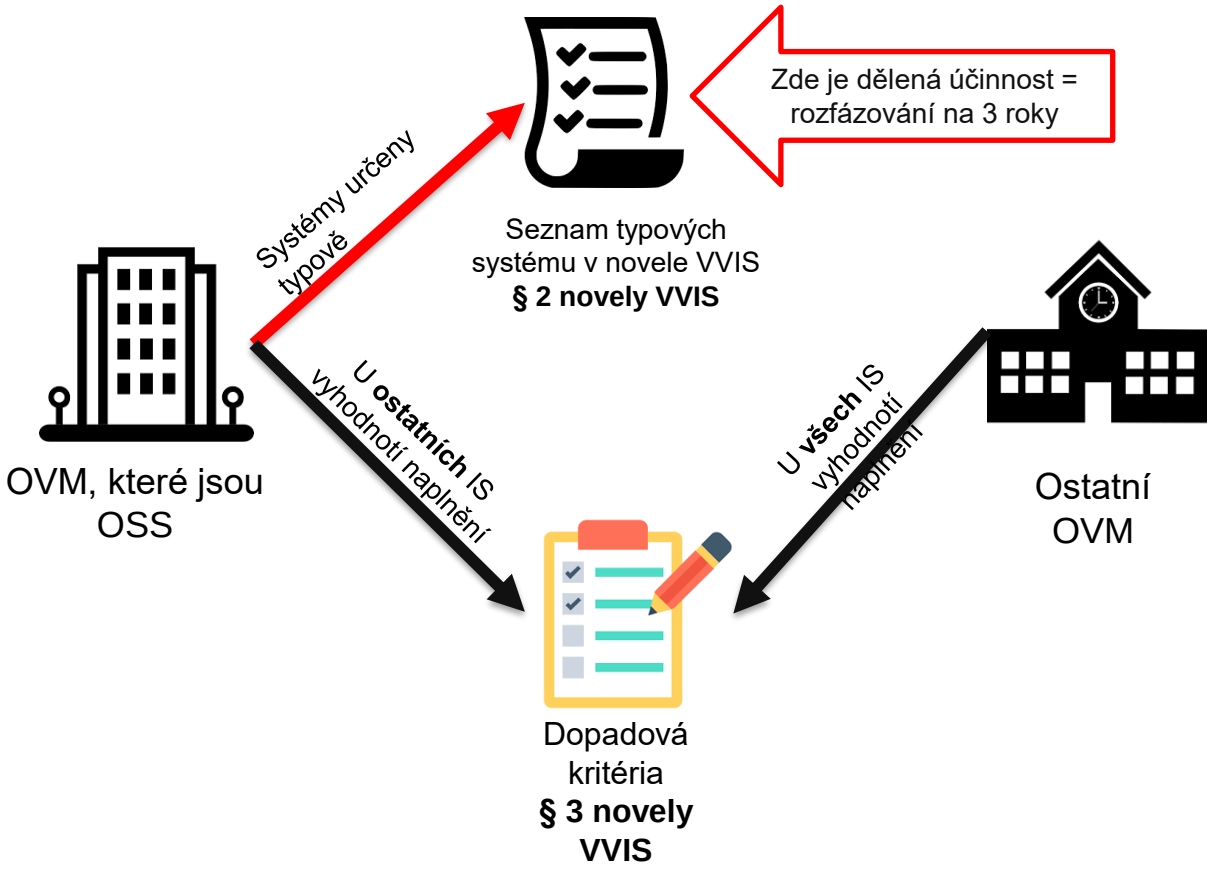
Fáze:

- Novela je od 1. 1. 2021 účinná
- Účinnost u § 2 vyhlášky je dělená - bude nabíhat postupně až do roku 2023

- Po první vlně účinnosti cca 200 NOVÝCH VIS

- Plná citace právního předpisu zní: Vyhláška č. 360/2020 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.

Vyhláška o VIS



Koncept vyhlášky:

- U organizačních složek státu (OSS) a krajů vyjmenuje vyhláška IS, které se určí „defaultně“ = vždy budou VIS
- Ostatní OVM (a OSS a kraje u těch nevyjmenovaných) posoudí kritéria = IS, které je naplní, budou VIS

Vyhláška o VIS

(1) Významný informační systém podle § 2 písm. d) zákona je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný k zajištění

a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,
b) kontrolní nebo inspekční činnosti anebo státního dozoru,

1. vlna – od 1. 1. 2021

c) výkonu veřejné moci při přípravě na krizové situace a jejich řešení,
d) výkonu spisové služby,
e) vedení úřední desky způsobem umožňujícím dálkový přístup,

2. vlna – od 1. 1. 2022

f) mezinárodní spolupráce, nebo
g) zadávání veřejných zakázek.

3. vlna – od 1. 1. 2023

(2) Významným informačním systémem podle § 2 písm. d) zákona je dále také informační systém spravovaný orgánem veřejné moci, který naplňuje určující kritéria stanovená v § 3.
(3) Významným informačním systémem **není informační systém, jehož správcem je obec.**
(4) Platí, že významný informační systém uvedený v odstavci 1 naplňuje určující kritéria.

Regulace využívání cloud computingu veřejnou správou

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Důvody regulace cloud computingu

- Využití cloudových služeb jak v soukromém tak ve veřejném sektoru rychle roste.
- Cloudové služby mohou přispět k ekonomičtějšímu a díky centrálnímu řízení, dohledu a aktualizaci i bezpečnějšímu provozu informačních systémů.
- Cloudové služby přináší nová rizika, zejména co se týče místa zpracování dat, které je často neznámé jednotlivým zákazníkům využívajících cloudové služby.
- Regulatorní rámec využívání cloud computingu je dán novelou zákona č. 365/2000 Sb., o informačních systémech veřejné správy a novelou zákona o kybernetické bezpečnosti.
- Tyto novely jsou provedeny zákonem o změně zákonů související s další elektronizací postupů orgánů veřejné moci (tzv. DEPO) k 1. 9. 2021.
- V souvislosti s tím NÚKIB vydal dvě vyhlášky a připravuje třetí, které by měly přispět k bezpečnějšímu využívání cloudových služeb veřejnou správou.

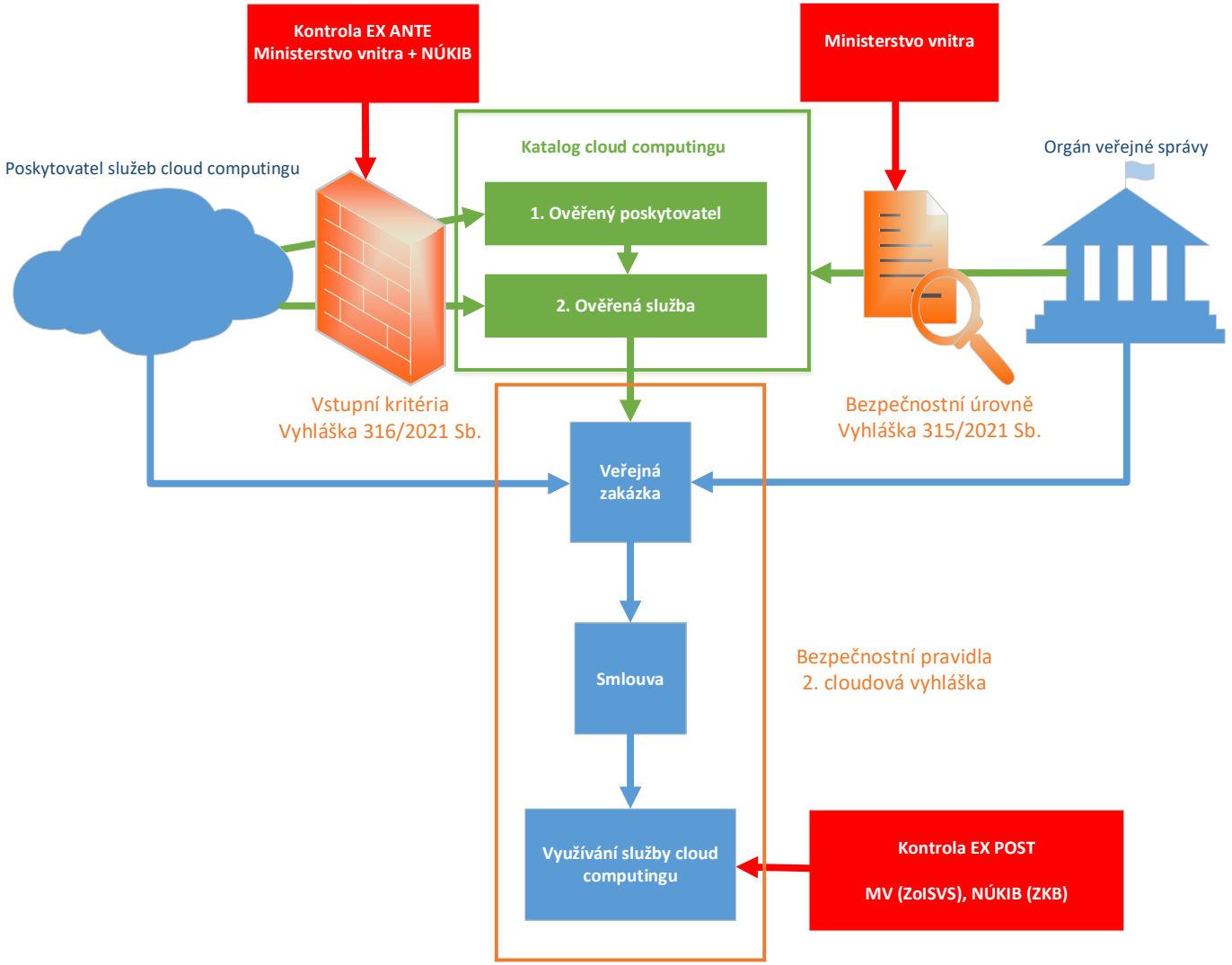
Regulace cloud computingu ve veřejné správě

- **Cíl:**
  - Původně – naplnit zmocnění § 6 písm. e) ZKB - vytvoření prováděcí vyhlášky k ZKB, která stanoví **obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu**
  - Nově – k původnímu cíli přidán novelou ZoISVS další – stanovení vstupních kritérií do katalogů cloud computingu

- **Východiska:**
  - Vychází z dokumentů projektu Příprava vybudování eGovernmentCloudu (usnesení vlády ČR č. 749 ze dne 14. listopadu 2018)
  - C5, ISO 27001, 27017 a 27018, Doporučení ČNB pro využívání cloudu bankami a další

- **Aktuální stav:**
  - Vyhlášky budou 3 (viz dále)
  - Z toho dvě účinné (od 1. 9. 2021), jedna ve výrobě

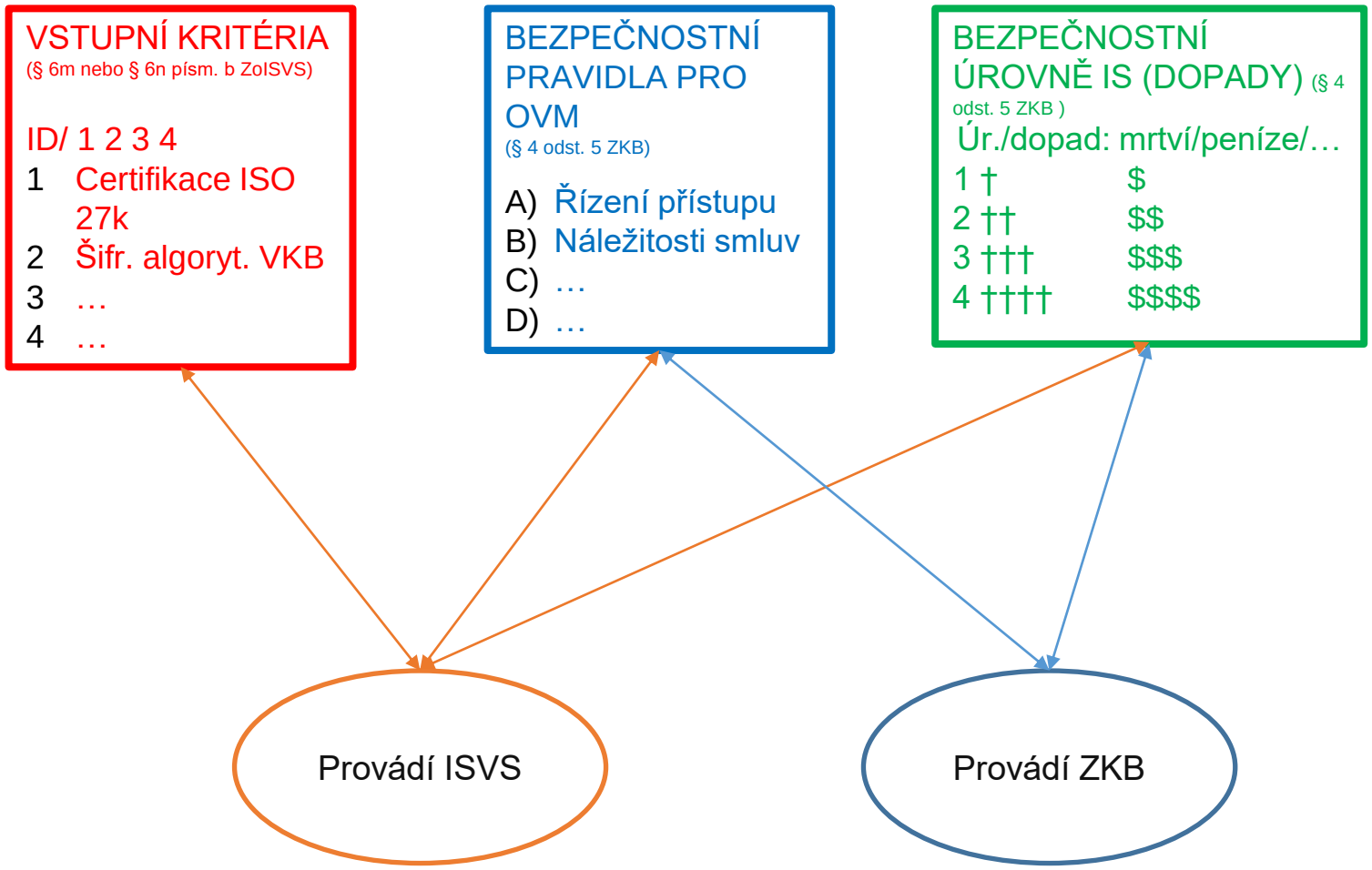
Schéma regulatorního rámce cloud computingu - ZoISVS



Hlavní body regulace cloud computingu

- Prověření poskytovatele cloud computingové služby z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.
- Rozdělení nabízených služeb cloud computingu do bezpečnostních úrovní – dle rozhodnutí poskytovatele – musí splnit odpovídající VSTUPNÍ KRITÉRIA pro zápis.
- Zařazení informačního systému veřejné správy do bezpečnostní úrovně – BEZPEČNOSTNÍ ÚROVNĚ.
- Podmínkou vypsání veřejné zakázky na službu cloud computingu je, že bezp. úroveň služby cloud computingu ≥ bezp. úroveň inf. syst. veřejné správy.
- Orgán veřejné moci zajistí splnění BEZPEČNOSTNÍCH PRAVIDEL při nákupu, uzavírání smlouvy a využívání služby cloud computingu.
- Transparentnost ve zpracování dat (kde, proč, jak dlouho), vývoz mimo EU pouze v nezbytných případech.

Tři cloudové vyhlášky



Tři cloudové vyhlášky I.

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

- VYHLÁŠKA JE 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
- Jednotliví dodavatelé služeb musí splnit vstupní požadavky
- Naplnění požadavků posoudí NÚKIB a MV

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,

Tři cloudové vyhlášky II.

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

- Dopad narušení bezpečnosti informací systému bude determinovat minimální úroveň bezpečnostních požadavků, které bude muset cloud splňovat
- Z pohledu systémů spadajících pod ZKB dopady determinuje zařazení systému do určité kategorie povinných osob podle ZKB (VIS, PZS, KII)
- Rozcestník pro hodnocení důležitosti systémů státní správy a pro určení požadavků na jejich zabezpečení
- Dopadá na všechny orgány veřejné moci
- Zařazení informačního systému nebo jeho části do bezpečnostní úrovně (BÚ)
- BÚ vyjadřují dopad narušení dostupnosti, důvěrnosti a integrity informačního systému nebo jeho části a jsou definovány nejhorším možným dopadem kybernetického bezpečnostního incidentu.
- BÚ jsou 4: nízká, střední, vysoká, kritická

Částka 139 Sbírka zákonů č. 315 / 2021 Strana 3763

315

VYHLÁŠKA

ze dne 24. srpna 2021

o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 28 odst. 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 205/2017 Sb., (dále jen „zákon"):

§ 1

Předmět úpravy

Tato vyhláška stanoví bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci podle § 6 písm. e) zákona.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) poptávaným cloud computingem informační nebo komunikační systém jako celek nebo jeho část, které mohou být provozovány pomocí cloud computingu a které je orgán veřejné moci povinen zařadit do bezpečnostní úrovně,

b) částí informačního nebo komunikačního systému taková část tohoto systému, která je jednoznačně oddělitelná, zabezpečuje cílevědomou a systematickou informační činnost[1]), může být provozována pomocí cloud computingu a je definována z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti,

c) oblastí dopadu vymezená oblast, v rámci které může mít dopad kybernetického bezpečnostního incidentu na poptávaný cloud computing vliv na bezpečnost a zdraví lidí, ochranu osobních údajů, trestněprávní řízení, veřejný pořádek, mezinárodní vztahy, řízení a provoz, důvěryhodnost, finanční model nebo zajišťování služeb,

d) úrovní dopadu nízká, střední, vysoká nebo kritická hodnota, která odpovídá dopadu kybernetického bezpečnostního incidentu na poptávaný cloud computing v každé oblasti dopadu.

§ 3

Bezpečnostní úrovně

Bezpečnostní úroveň pro využívání cloud computingu orgány veřejné moci vyjadřuje možné dopady kybernetického bezpečnostního incidentu na poptávaný cloud computing. Bezpečnostní úrovně jsou nízká, střední, vysoká nebo kritická.

§ 4

Zařazení poptávaného cloud computingu do bezpečnostní úrovně

(1) Zařazení poptávaného cloud computingu do bezpečnostní úrovně provede orgán veřejné moci podle přílohy k této vyhlášce. Orgán veřejné moci zhodnotí naplnění úrovně dopadu, které je poptávaný cloud computing schopen dosáhnout v rámci každé oblasti dopadu. Úroveň dopadu je v rámci každé oblasti dopadu dána nejhorším možným dopadem kybernetického bezpečnostního incidentu.

(2) Při zjišťování nejhoršího možného dopadu kybernetického bezpečnostního incidentu zohlední orgán veřejné moci možné narušení důvěrnosti, integrity a dostupnosti poptávaného cloud computingu a povahu informačního nebo komunikačního systému, který je poptávaným cloud computingem, jako celku. V případě, že je poptávaným cloud computingem pouze určitá část informačního nebo komunikačního systému, zohlední také vztah této části k bezpečnostní úrovni informačního nebo komunikačního systému jako celku.

(3) Bezpečnostní úroveň pro využívání poptá-

[1]) § 2 písm. a) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Tři cloudové vyhlášky III.

3. Vyhláška o bezpečnostních pravidlech

- Ve výrobě – vydání předpokládáme v 4Q/2021
- Každá z kategorií systémů (1-4) bude mít stanovena příslušná bezpečnostní opatření
- Dopadá na všechny orgány veřejné moci
- Obsahově blízké VKB, vychází z německého standardu C5
- Bude obsahovat povinná a volitelná bezpečnostní pravidla – celkem cca 250 pravidel (povinná 46)
- Subjekt zavede povinná opatření a zváží vhodnost volitelných
- Možnosti zajištění:
  - Prohlášení poskytovatele
  - Certifikace poskytovatele – ISO 27001, ISO 27017, ISO 27018, C5, SOC 2® Type 2, ISO 20000 nebo ISO 22301
  - Smluvní závazek poskytovatele

Přechodná ustanovení

- **Zákon č. 12/2020 Sb. § 17** (novelizován zákonem č. 261/2021 Sb.)
  - OVS musí do 3 měsíců od 1. 8. 2020 zapsat využívaný cloud computing (CC) do katalogu CC
  - OVS využívalo cloud computing k 1. 8. 2020 = může tento CC dále využívat 41 měsíců (1. 1. 2024)
- **Zákon č. 261/2021 Sb., Čl. LXXXI**
  - OVS využívalo CC nebo uzavřelo (rámcovou) smlouvu před 1. 9. 2021 = může tento CC využívat do 31. 12. 2023
  - CC v katalogu před 1. 9. 2021/zapsaný dle podmínek před 1. 9. 2021 = může využívat do 31. 12. 2023
  - OVS zahájilo využívaní CC od 1. 9. 2021 do 31. 1. 2022 = může využívat do 31. 12. 2022

pozn. v případě, že daný CC splňuje aktuální podmínky – zapsán v katalogu, splňuje požadavky cloudových vyhlášek – lze využívat bez časového omezení

Cloudové vyhlášky jak šel čas...

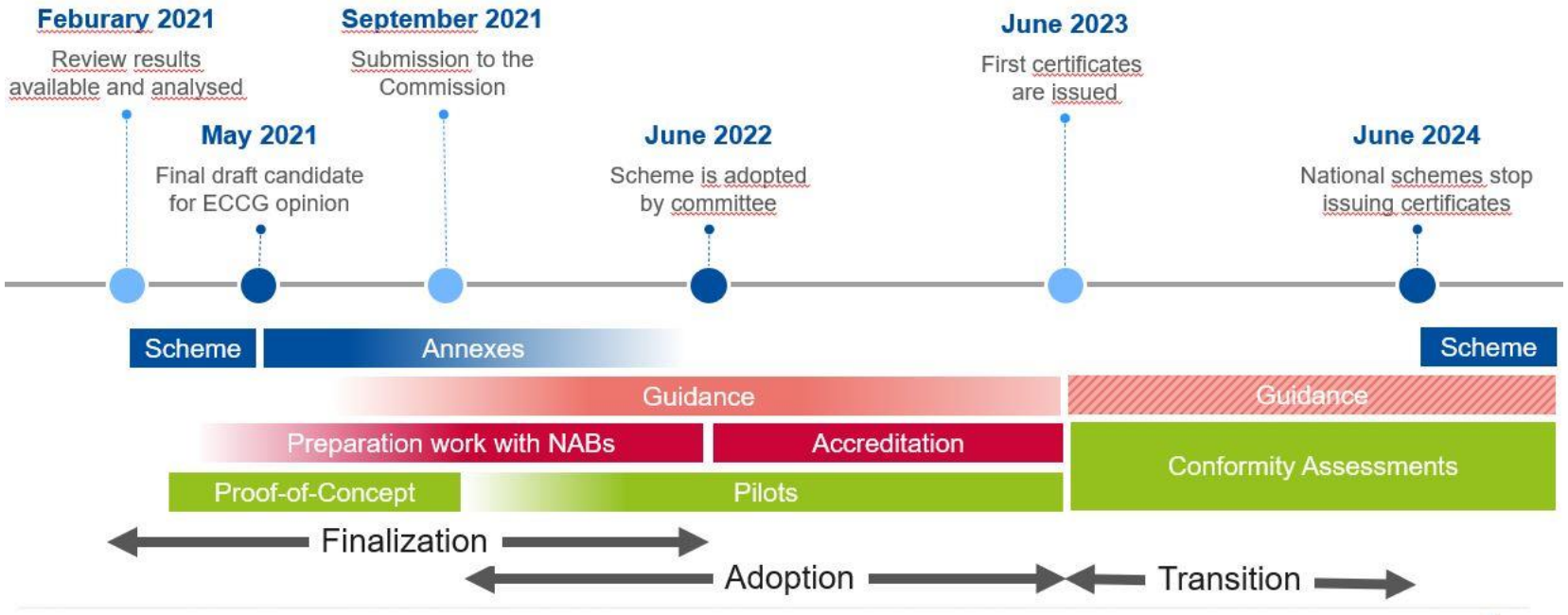
- 2017 – zmocnění NÚKIB vydat bezpečnostní pravidla pro využívání cloudu
- 2018 – listopad – schválení SAZ vládou = cloud first
- 2018 – NÚKIB ustavuje expertní skupinu ke cloudu
- 2019 – NÚKIB se dozvěděl, že kromě vyhlášky o bezpečnostních pravidlech bude muset vydat ještě vstupní kritéria
- 2020 – NÚKIB vytvořil a publikoval draft cloudových vyhlášek
- 2020 – řešení cloudových vyhlášek a vůbec požadavků regulatorního rámce na různých platformách, změny zákonného rámce – poslanci, SP ČR, ICT UNIE, ÚOOÚ, TOP mngmt vendorů..
- 2021 – předložení cloudových vyhlášek do MPŘ

Strategická rizika cloudu

- Zpracování dat mimo EU přináší rizika
  - jiné jurisdikce, obtížný přístup pro české „law enfforcement“ složky
  - jiné jurisdikce, jiná právní ochrana osobních údajů, jiné právní systémy..
  - dle vyjádření vendorů není v současné době možné zajistit zpracování výlučně na území EU tak, aby služby fungovaly
- V případě předání údajů do třetí země je třeba:
  - prověřit, zda vhodné záruky a ochranná opatření **v doložkách** skutečně zajišťují srovnatelnou úroveň ochrany zaručené v EU - GDPR
  - brát v úvahu i relevantní prvky **právního řádu** třetí země
  - každý správce předávající údaje do USA by měl hledat a navrhovat řešení v podobě dalších bezpečnostních záruk (např. uložení dat včetně metadat pouze na území EU, šifrování bez zadních vrátek apod.) – viz rozhodnutí SD EU Schrems II.
  - dodržovat zásadu **transparentnosti** a informovat subjekt údajů o konkrétních opatřeních a postupech, komu a do jakých zemí jsou údaje předány, za jakých podmínek, jak jsou chráněny, případně rizika s tím související

Evropská certifikace cloudových služeb = EUCS

= technický nástroj k poskytnutí informací zákazníkům pro učinění informovaného rozhodnutí



Výhrady NÚKIB k draftu EUCS

- EUCS není aktuálně dostatečně určitý – přímo v návrhu se počítá s doplňkovými pokyny (např. upřesnění šifrovacích algoritmů), které zatím nebyly vydány.
- EUCS aktuálně neobsahuje dostatečné požadavky pro zajištění harmonizace při získávání certifikátu uplatnitelného v celé EU a to jak pro akreditační, tak i certifikační orgány – nespecifikované kompetenční požadavky pro akreditační i certifikační orgány.
- EUCS neřeší nezbytnost zpracování dat v EU – pouze požadavek na transparentnost, ať zákazník ví, kde se data zpracovávají. Národní regulace zdůrazňuje, že zpracování mimo EU je možné pouze v nezbytných případech a v nezbytném rozsahu (vyjma specifikované cloudové služby).
- EUCS má nedostatečně propracované hodnotící metody – především nejasný certifikovaný (auditovaný) self-assement v úrovní záruky základní – podle EUCS se jedná o tzv. limited assurance.
- EUCS řeší posuzování cloudové služby a nikoli jejího poskytovatele z pohledu zajištění veřejného pořádku, bezpečnosti a dodržování práv třetích osob.

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
- Formuláře pro zápis nabídky
  - Proklik přes web NÚKIB: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/
  - Budou na webu MV – ZATÍM NEVYVĚŠENO
- Služby, které vyvážejí data mimo EU – Úřední deska NÚKIB - https://www.nukib.cz/cs/uredni-deska/

Dotazy?

Děkuji za pozornost!

regulace@nukib.cz