Aktuální vývoj legislativy

v oblasti kybernetické bezpečnosti

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

21. září 2021
TLP: WHITE

Martin Klumpar
Odbor regulace

Obsah

- Regulace využití cloudových služeb orgány veřejné moci
- Novelizace vyhlášky o významných informačních systémech
- Návrh směrnice NIS 2
- Novelizace vyhlášky o kritériích pro určení provozovatele základní služby

Regulace využití cloudových služeb orgány veřejné moci

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.

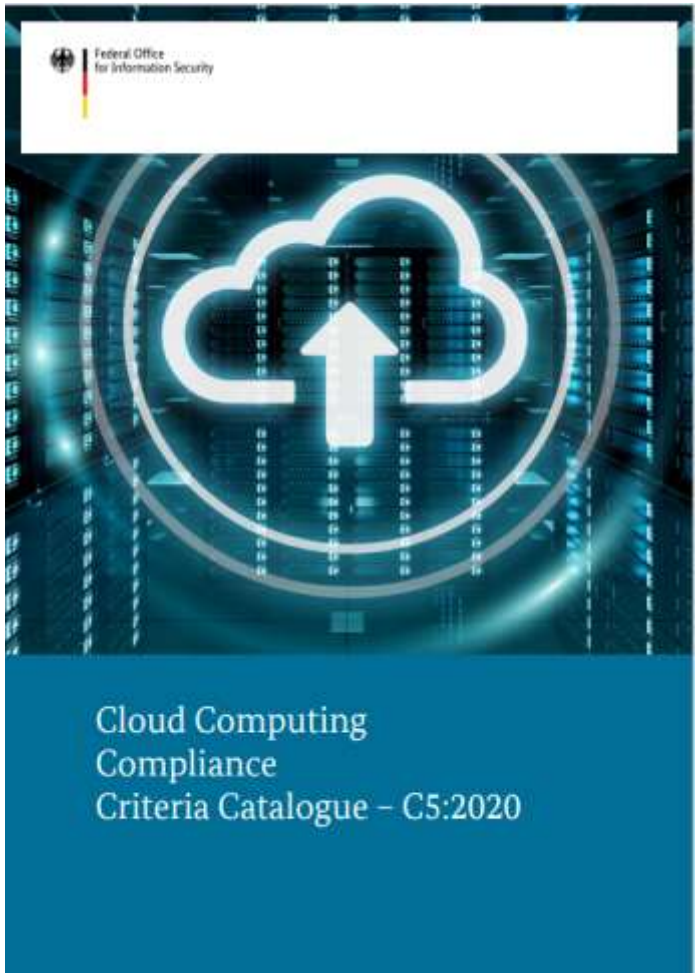
Provedení regulace cloud computingu

- Regulatorní rámec
  - novela zákona č. 365/2000 Sb., o informačních systémech veřejné správy
  - novela zákona č. 181/2014 Sb., o kybernetické bezpečnosti
- Tyto novely jsou provedeny zákonem o změně zákonů související s další elektronizací postupů orgánů veřejné moci (tzv. DEPO) účinnost od **1. 9. 2021**.
- V souvislosti s tím NÚKIB vydal dvě vyhlášky a připravuje třetí.
  - Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu
  - Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (Vyhláška o bezpečnostních úrovních systémů)

Východiska regulace cloud computingu

- Souhrnná analytická zpráva projektu Příprava vybudování eGovernmentCloudu (usnesení vlády ČR č. 749 ze dne 14. listopadu 2018)
- Mezinárodní standardy C5, ISO 27001, 27017 a 27018
- Doporučení ČNB pro využívání cloudu bankami
- Připomínky odborné veřejnosti k věcnému záměru
- Výstupy z jednání s poskytovateli a orgány veřejné moci

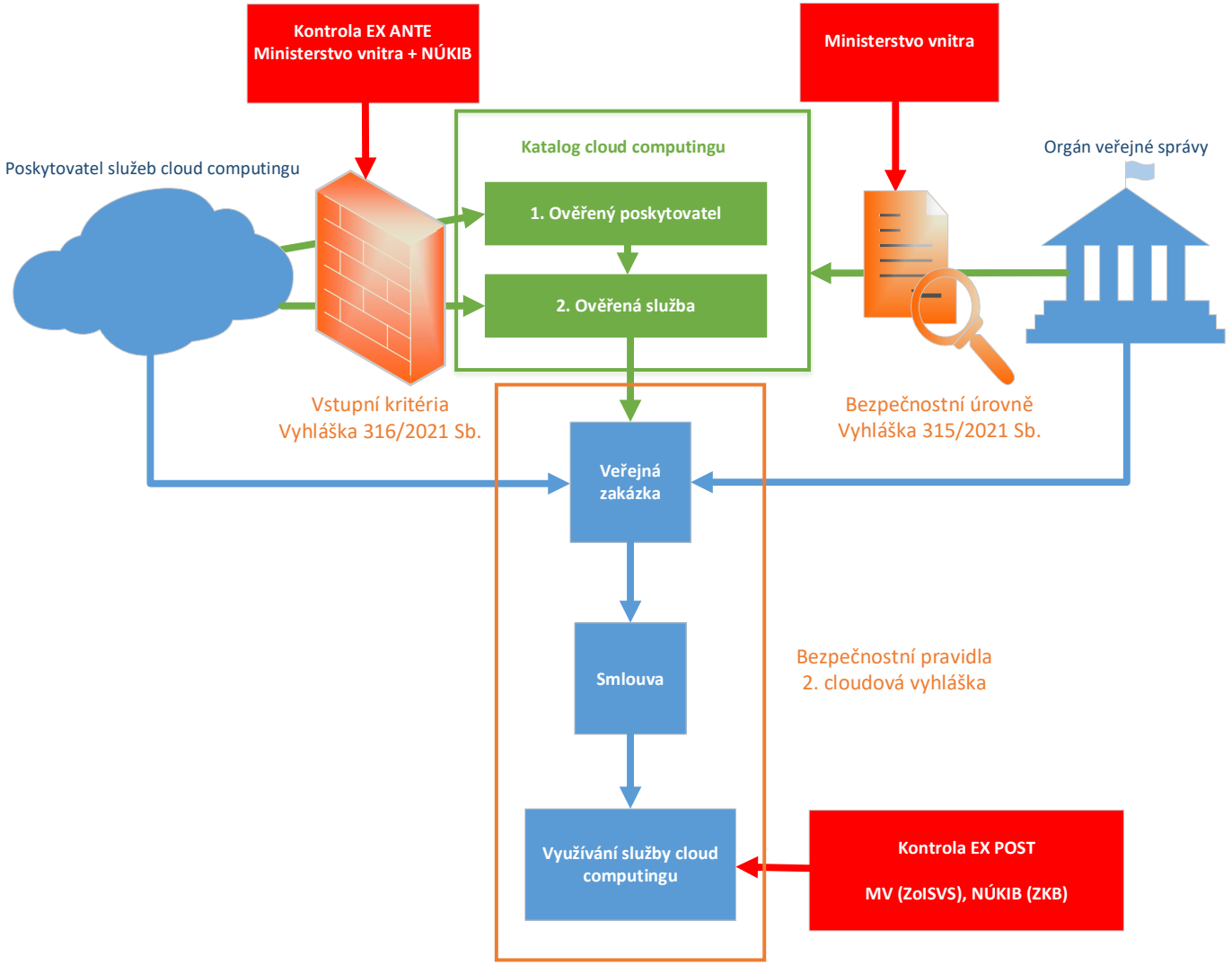
ISO 27017
International Organization for Standardization



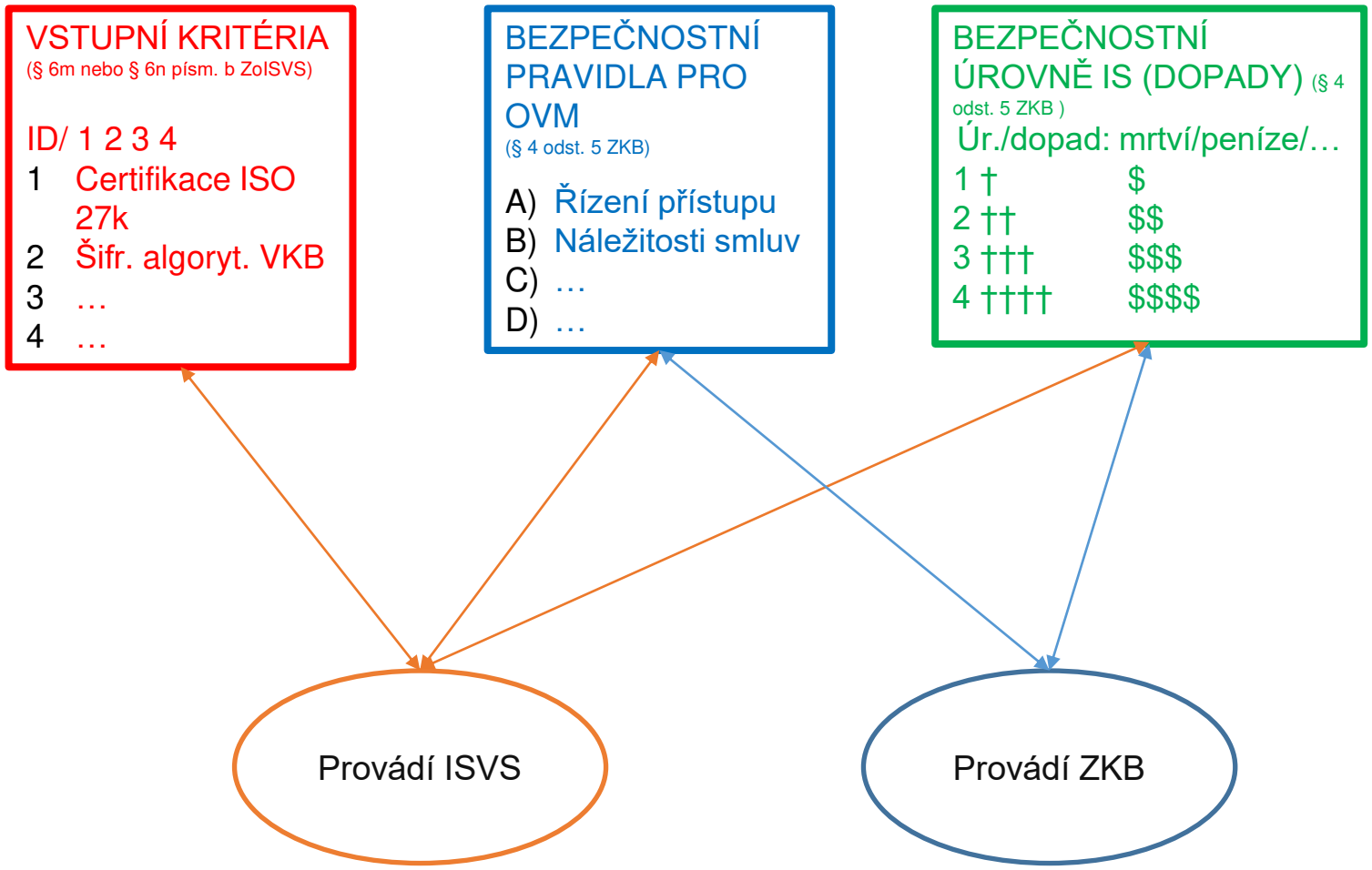
Hlavní body regulace cloud computingu

- Prověření **poskytovatele** cloud computingové služby z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.
- Transparentnost ve zpracování dat (kde, proč, jak dlouho), vývoz mimo EU pouze v nezbytných případech.
- Orgán veřejné moci nese stále nese odpovědnost za bezpečnost informací i v případě využití cloudových služeb.
- Stanovení bezpečnostních požadavků na služby cloud computingu – musí splnit VSTUPNÍ KRITÉRIA.
- Klasifikace informačního systému orgánu veřejné moci – BEZPEČNOSTNÍ ÚROVNĚ.
- Podmínkou vypsání veřejné zakázky na službu cloud computingu je, že bezp. úroveň nabízené služby cloud computingu ≥ bezp. úroveň inf. syst. veřejné správy (ZoISVS).
- Orgán veřejné moci zajistí splnění BEZPEČNOSTNÍCH PRAVIDEL při nákupu, uzavírání smlouvy a využívání služby cloud computingu.

Schéma regulatorního rámce cloud computingu - ZoISVS



Tři cloudové vyhlášky



Tři cloudové vyhlášky I.

1. 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
- Jednotliví dodavatelé služeb musí splnit vstupní požadavky
- Naplnění požadavků posoudí MV a NÚKIB = správní řízení

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 § 6o 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 § 6z 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 § 6z odst. 7 písm. b) 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)

- ÚČINNÁ OD 1. 9. 2021
- Zařazení informačního systému nebo jeho části do bezpečnostní úrovně (BÚ)
- Bezpečnostní úroveň určuje možný dopad narušení bezpečnosti informací
- Rozcestník pro hodnocení důležitosti systémů státní správy a pro určení požadavků na jejich zabezpečení
- Dopadá na všechny orgány veřejné moci
- BÚ jsou 4: nízká, střední, vysoká (= komerční), kritická (= státní)

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. c) 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 takové části tohoto systému, které 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 zájmy lidí, ochranu osobních údajů, nestrannost řízení, veřejný pořádek, mezinárodní vztahy, řízení a provoz, důvěryhodnost, finanční model nebo zajišťované služby,

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 1Q/2022
- Každá z bezpečnostních úrovní (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

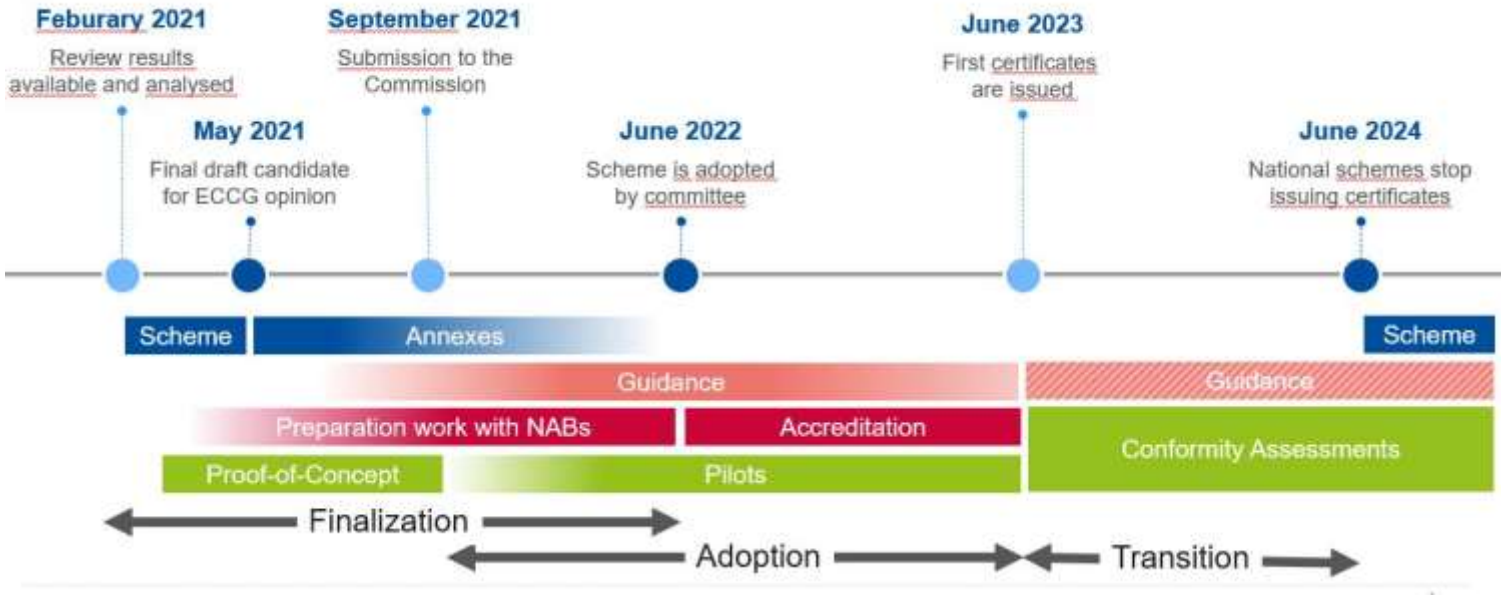
Přechodná ustanovení

- **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

Evropská certifikace cloudových služeb = EUCS

= technický nástroj k poskytnutí informací zákazníkům pro učinění informovaného rozhodnutí



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)

Novelizace vyhlášky o významných informačních systémech

Vyhláška o VIS

Cíl:

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

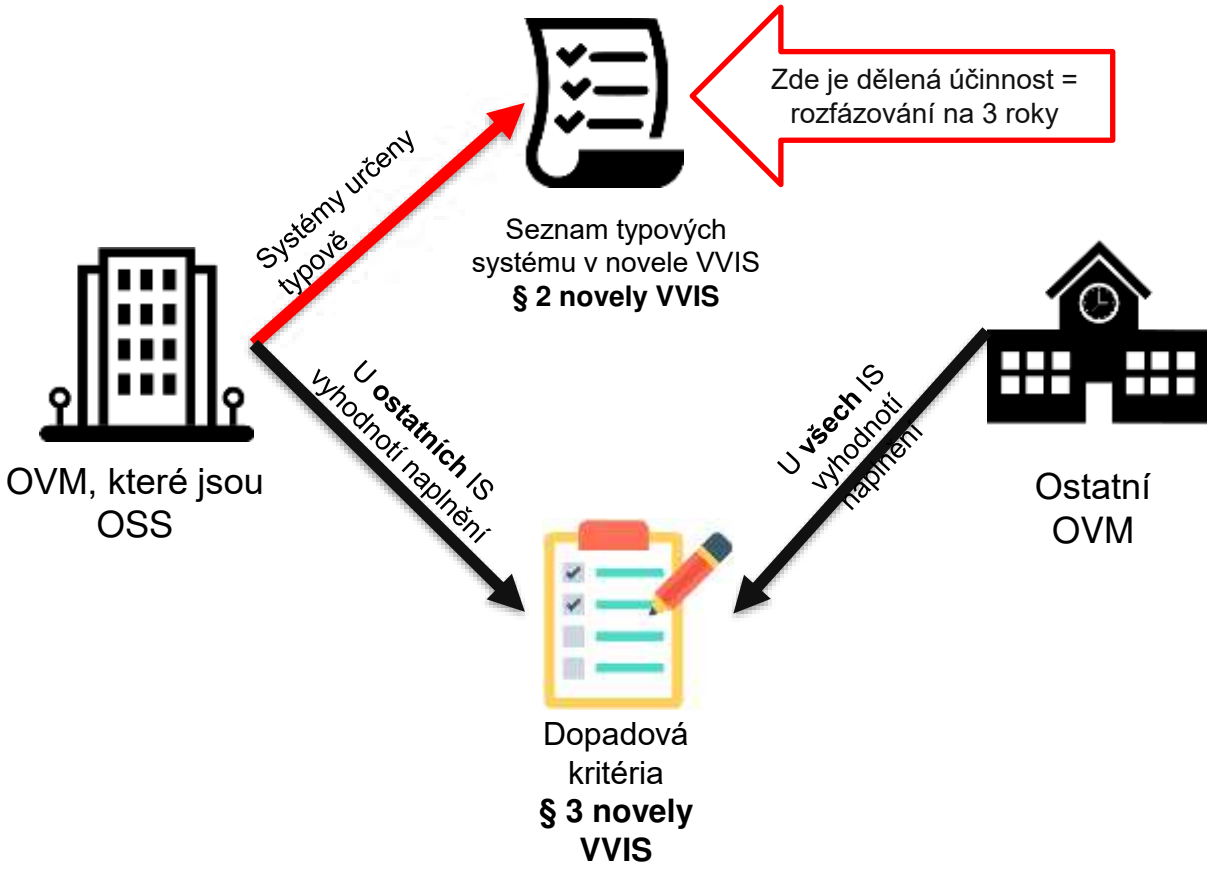
Fáze:

- 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.

Návrh směrnice NIS 2

Návrh směrnice NIS 2

- Návrh směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii = tzv. NIS 2

Změny oproti současnému stavu:

- Konec určování, automatické naplnění definičních znaků IE/EE
- Regulace celé společnosti, nejen „důležitého“ systému x risk based approach
- Výčet BO přímo ze směrnice, implementační akty Komise, prostor pro vnitrostátní úpravu (ZKB, VKB)

Definiční znaky IE/EE:

- **Střední / velký podnik** (tj. počet zaměstnanců min. 50, roční obrat min. 10 mil. EUR)
- **Odvětvová kritéria**
- NEBO subjekt je označen za kritický podle směrnice Evropského parlamentu a rady o odolnosti kritických subjektů (**návrh CER směrnice**)

Aktuální stav: projednáváno v EU
Předpokládané nabytí účinnosti: cca za 2 roky (+ transpoziční lhůta)
Zachována možnost vnitrostátní úpravy nad rámec směrnice (nad rámec rozsahu; národní bezpečnost) (PZS, KII)

Novelizace vyhlášky o kritériích pro určení provozovatele základní služby

Novelizace vyhlášky o PZS

- V reakci na řadu kybernetických incidentů ve zdravotnictví.
- Účinné od 1. 1. 2021.
- Určeno dalších 28 nemocnic jako PZS
  (v prosinci 2020 bylo v odvětví zdravotnictví 16 PZS, nyní jich je 44).

Odvětvová kritéria			Dopadová kritéria
Druh služby	**Druh subjektu**	**Speciální kritéria druhu subjektu**	
5.1. Poskytování zdravotních služeb	Poskytovatel zdravotních služeb podle zákona o zdravotních službách	a) Celkový počet akutních lůžek v posledních třech kalendářních letech nejméně 800, **nebo** b) statut centra vysoce specializované traumatologické **onkologické, cerebrovaskulární, kardiovaskulární a komplexní kardiovaskulární péče** podle zákona o zdravotních službách, **c) zajišťování urgentního příjmu podle zákona o zdravotnické záchranné službě v zařízení s celkovým počtem lůžek intenzivní péče v posledních třech kalendářních letech nejméně 40 nebo** **d) poskytovatel akutní lůžkové péče s průměrným počtem unikátních ošetřených pacientů v posledních třech kalendářních letech nejméně 100 000 za jeden kalendářní rok.**	Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit I. závažné omezení druhu služby postihující více než 50 000 osob, II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury, III. nedostupnost druhu služby pro více než 1 600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů, IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření, V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému, nebo VI. kompromitaci citlivých osobních údajů o více než 200 000 osobách.

Bílá kniha zákona o kybernetické bezpečnosti

- Výzva odborné veřejnosti – návrhy na zlepšení zákona o kybernetické bezpečnosti
  - bude zveřejněno v blízké době na webu NÚKIB

Dotazy?

Děkuji za pozornost!

regulace@nukib.cz