Aktuality v regulaci KB

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

15. února 2022
TLP: WHITE

Daniela Procházková
Odbor regulace

Obsah

- Úkoly z Akčního plánu k Národní strategii KB
- Další vlna účinnosti vyhlášky o významných informačních systémech
- Směrnice NIS2 a její dopad na veřejnou správu
- Regulace cloud computingu ve veřejné správě
- Prostor pro dotazy

Úkoly z Akčního plánu k Národní strategii KB ČR 2021

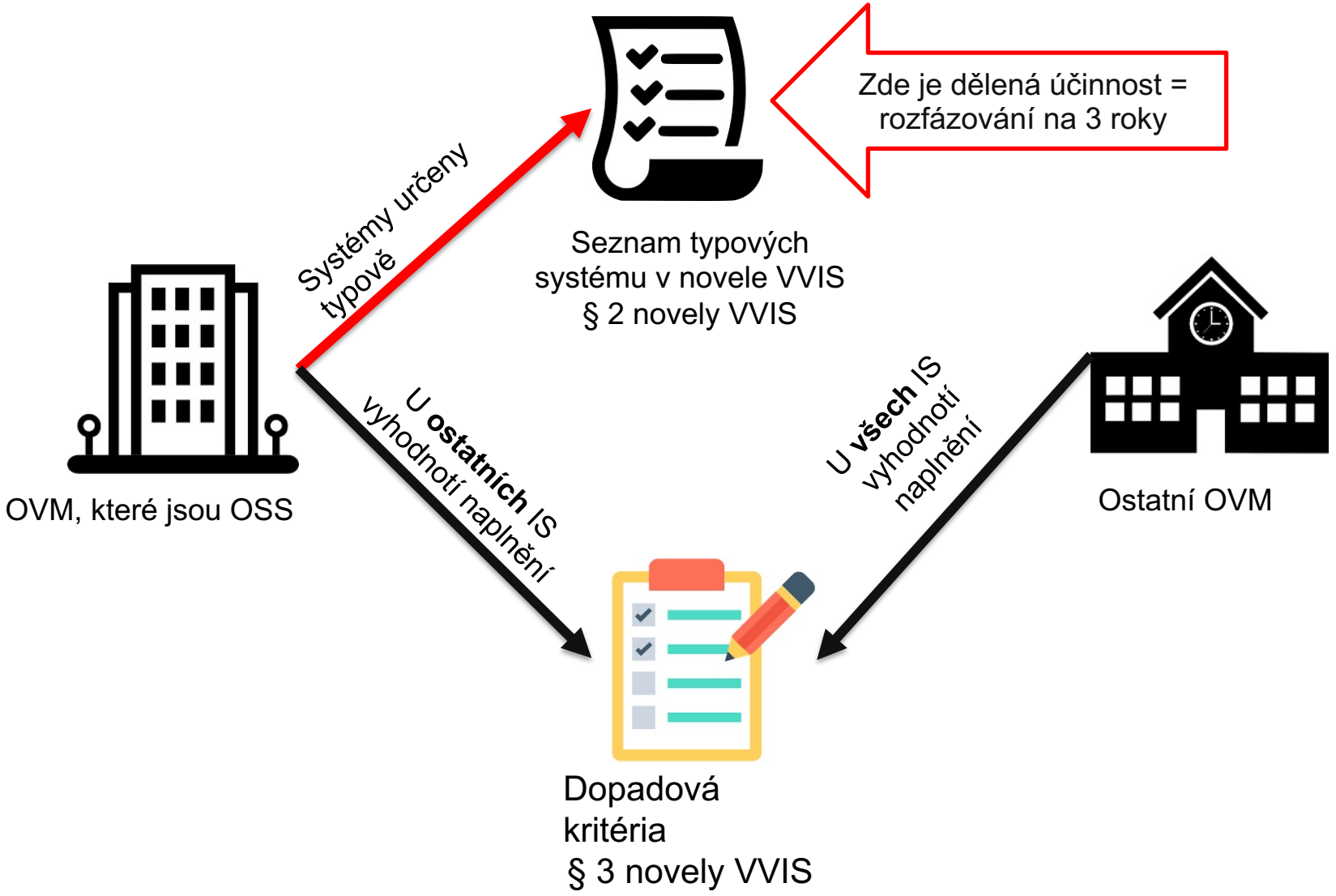
- Analýza právních možností rychlého **operativního nákupu ICT prostředků** k provádění opatření dle ZKB za krizových stavů (úkol č. 41)
  - Konzultováno s MV a MMR;
  - Legislativa toto umožňuje, nedojde k návrhu její změny
- **Zabezpečení systémů e-Governmentu od počátku vytváření** („security by design“) (úkol č. 79)
  - Doplnění procesu žádosti o schválení projektů OHA MV o bezpečnostní otázky
- Podpůrný materiál: **zabezpečení distančního vzdělávání** (ZŠ a SŠ) (úkol č. 94)
  - Ve spolupráci s MŠMT: Standard konektivity a bezpečnosti školy v 21. století a již existuje bezpečnostní standard pro videokonference: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

- **Akční plán a Národní strategie**: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/strategie-akcni-plan/

Úkoly z Akčního plánu k Národní strategii KB ČR: budoucnost

- Porovnat vybrané v současnosti užívané **metody analýzy rizik** s cílem ověřit, zda jsou v souladu s požadavky VKB a zda jsou současně efektivně použitelné pro různé organizace.
  - Výstup tohoto projektu bude v obecné rovině nabídnut orgánům a osobám povinným dle ZKB i široké veřejnosti. (Q2 2022)
- Návrh **jednotného postupu hlášení kybernetických bezpečnostních incidentů** relevantním orgánům (Q4 2022)
- Metodický dokument k **řízení bezpečnosti dodavatelů** pro povinné osoby dle ZKB. (Q4 2022)
- Návrh **aktualizace standardů šifrování** pro osoby povinné dle ZKB zohledňující nástup kvantových počítačů a s tím související hrozbu prolomení současných metod šifrování. (Q1 2024)
- **Vydefinovat systémy, které jsou důležité pro chod státu** a jeho bezpečnost a dosud nespadají pod regulaci. V případě existence takových systémů navrhnout příslušné změny legislativy. (od Q4 2024)
- Analyzovat a případně zpracovat návrh legislativy upravující **odbornou způsobilost osob vykonávajících některou z rolí podle VKB**. (Q2 2025)

Další vlna účinnosti vyhlášky o VIS



Další vlna účinnosti vyhlášky 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 - 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 - 2022

f) mezinárodní spolupráce, nebo

g) zadávání veřejných zakázek.

3. vlna - 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.

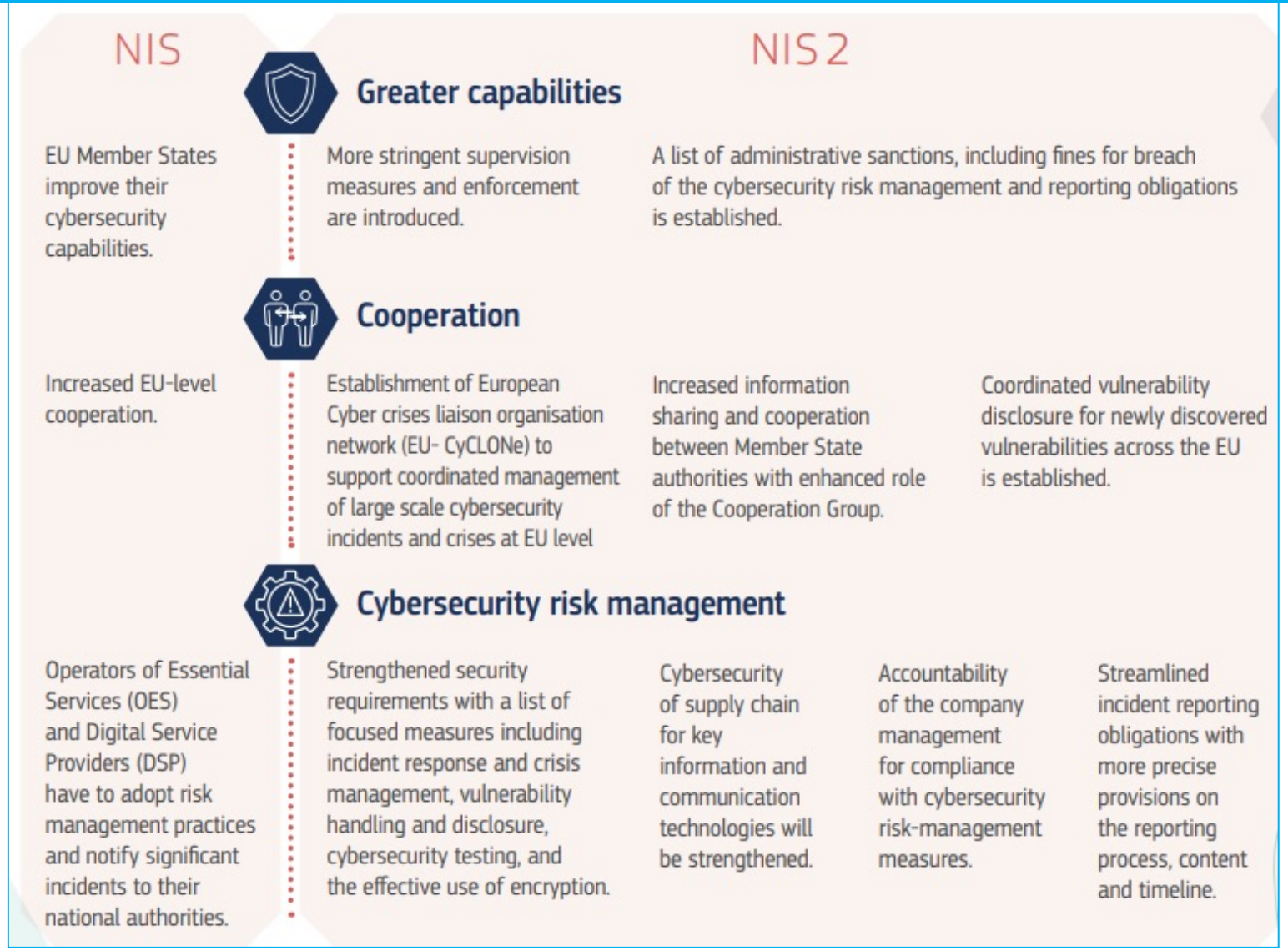
Evidence VIS

Seznam informačních systémů orgánu veřejné moci podle § 3 odst. 2 vyhlášky č. 317/2014 Sb. (Ministerstvo)				Verze	1.0	Vyplnil/a	Anna Nováková manažer kybernetické bezpečnosti
				Poslední změna	1. ledna 2021		
Pořadové číslo	Označení informačního systému	Výkon působnosti podporovaný systémem	Významný informační systém	Naplněné kritérium	Důvod (ne)naplnění definice významného informačního systému		Komentář
Vzor 1	Spisová služba	Vedení správních řízení, spisová služba	ANO	§ 2 odst. 1 písm. a) § 3 odst. 1 písm. c)	Bez systému nelze vykonávat základní činnosti. Nahrazení není možné bez vynaložení nepřiměřených nákladů (…)		
Vzor 2	Rejstřík X	Zákonná povinnost vedení rejstříku podle zákona č. X	NE	---	Rejstřík X je součástí určené kritické informační infrastruktury XY. (…)		
Vzor 3	Docházkový systém	Vedení docházky v rámci OSS	NE	---	Neslouží k výkonu působnosti orgánu veřejné moci.		
Vzor 4	Web – kulturní akce ministerstva	Web pro pořádání kulturních akcí OSS	NE	---	Neslouží k výkonu působnosti orgánu veřejné moci		
Vzor 5	Databáze XY	Slouží pro podporu činnosti XY	NE	---	Narušení bezpečnosti informací systému lze nahradit bez vynaložení nepřiměřených nákladů – činností běžných zaměstnanců v rámci fyzické podoby obsahu databáze; neobsahuje citlivá data		
Datum	5. ledna 2021	Schválil/a a podepsal/a		Jan Novák, ředitel		Jan Novák, v. r.	Interní

Podpůrné materiály:
https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Směrnice NIS 2 a její dopad na veřejnou správu

- Na konci roku 2020 zahájena z podnětu Evropské Komise revize směrnice NIS **– tzv. směrnice NIS2.**
  - prvotní návrh zveřejněn zde: [Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)]
- Aktuální návrh zachovává původní strukturu a mnoho institutů z původní směrnice NIS, většinu z nich však prohlubuje



Zdroj schématu: [Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu)]

Rozdíly mezi NIS a NIS2

Minimální rozdíly oproti ZKB/VKB:

- Větší pravomoci dozorových orgánů (NÚKIB)
- Větší pravomoci CSIRT týmů
- Podrobnější bezpečnostní opatření, risk-based approach

Novinky:

- Hlášení relevantních událostí a hrozeb, sdílení informací o zranitelnostech (registr ENISA)
- Povinné vzdělávání managementu, větší odpovědnost (+ dočasný zákaz výkonu fce – netýká se veřejné správy)
- Vyšší pokuty za porušení povinností (inspirace GDPR, nicméně zde stanoven strop; až 2 % z obratu / 4 mil EUR)
- Spolupráce členských států na kontrolách a na výměně informací
- Sdílení informací mezi povinnými subjekty (stát má zajistit platformu)
- Užší spolupráce NÚKIB s dozorovými orgány z jiných oblastí (ÚOOÚ, ČTÚ, …)
- Do budoucna možnost povinných certifikací produktů
- Cloud computing = standardní povinná osoba
- Rozšíření působnosti NIS2, zahrnutí veřejné správy (viz dále)
- Způsob identifikace povinné osoby (viz dále)
- Rozsah regulovaných systémů (viz dále)

Návrh NIS2 veřejní správa

Regulace veřejné správy

- Sporné téma, sporná souvislost s vnitřním trhem, otázka národní bezpečnosti
- Vývoj:
  - → Definice, regulace centrálních orgánů, NUTS1 a NUTS2
  - → Definice, upuštění od podmínky právní osobnosti, přidání regionálních orgánů, odebrání NUTS
  - → Definice, centrální orgány povinně, regionální dobrovolně, diskuze nad tvrdým seznamem po vzoru zakázkových směrnic
  - → Final: zmírnění definice, centrální orgány povinně, regionální dobrovolně

→ **= ústřední orgány státní správy**

(23) 'pu
the
(a)
(b)
(c)
(d)
Pub
law

(23) 'public administration entity' means, an entity **recognized as such in a Member State in accordance with national law,** ~~in a Member State~~ that complies with the following criteria:

(a) it is established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character;

(b) it has legal personality **or it is entitled by law to act on behalf of another entity with legal personality**;

(c) it is financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or it is subject to management supervision by those authorities or bodies; or it has an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law;

(d) it has the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services or capital.

2a. Regardless of their size, this Directive also applies to public administration entities of central governments recognised as such in a Member State in accordance with national law and referred to in point 9 of Annex I. Member States may establish that this Directive also applies to public administration entities at regional and local levels.

local levels ~~that comply with the criteria provided for i~~

9. Public administration **entities**		— Public administration entities of central governments **as defined by a Member State in accordance with national law** — ~~Public administration entities of NUTS level 1 regions listed in Annex I of Regulation (EC) No 1059/2003 (65)~~ — ~~Public administration entities of NUTS level 2 regions listed in Annex I of Regulation (EC) No 1059/2003~~

Návrh NIS2 z pohledu povinného subjektu

- **Určené subjekty zůstanou určeny** (kromě bank)
  - kritérium velikosti organizace
  - kritérium důležitosti pro sektor (bez ohledu na obrat nebo počet zaměstnanců)
  - národní úprava (KII, VIS)
- **Dosavadní PZS (KII, VIS)** – zachována dosavadní úroveň regulace
- **Rozsah zabezpečení informačních systémů se rozšíří na celou organizaci**, nejen na systém používaný pro výkon základní služby
- **Větší zapojení Evropské komise** – prováděcí akty Komise – bezpečnostní opatření, hlášení incidentů

  ! ISO 27k → VKB
- **Vyšší pokuty** za neplnění bezpečnostních opatření (dnes max. 5 mil. Kč)
- **Větší důraz** na sdílení informací mezi určenými subjekty

Regulace cloud computingu ve veřejné správě: Důvody

- 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.

Provedení regulace cloud computingu

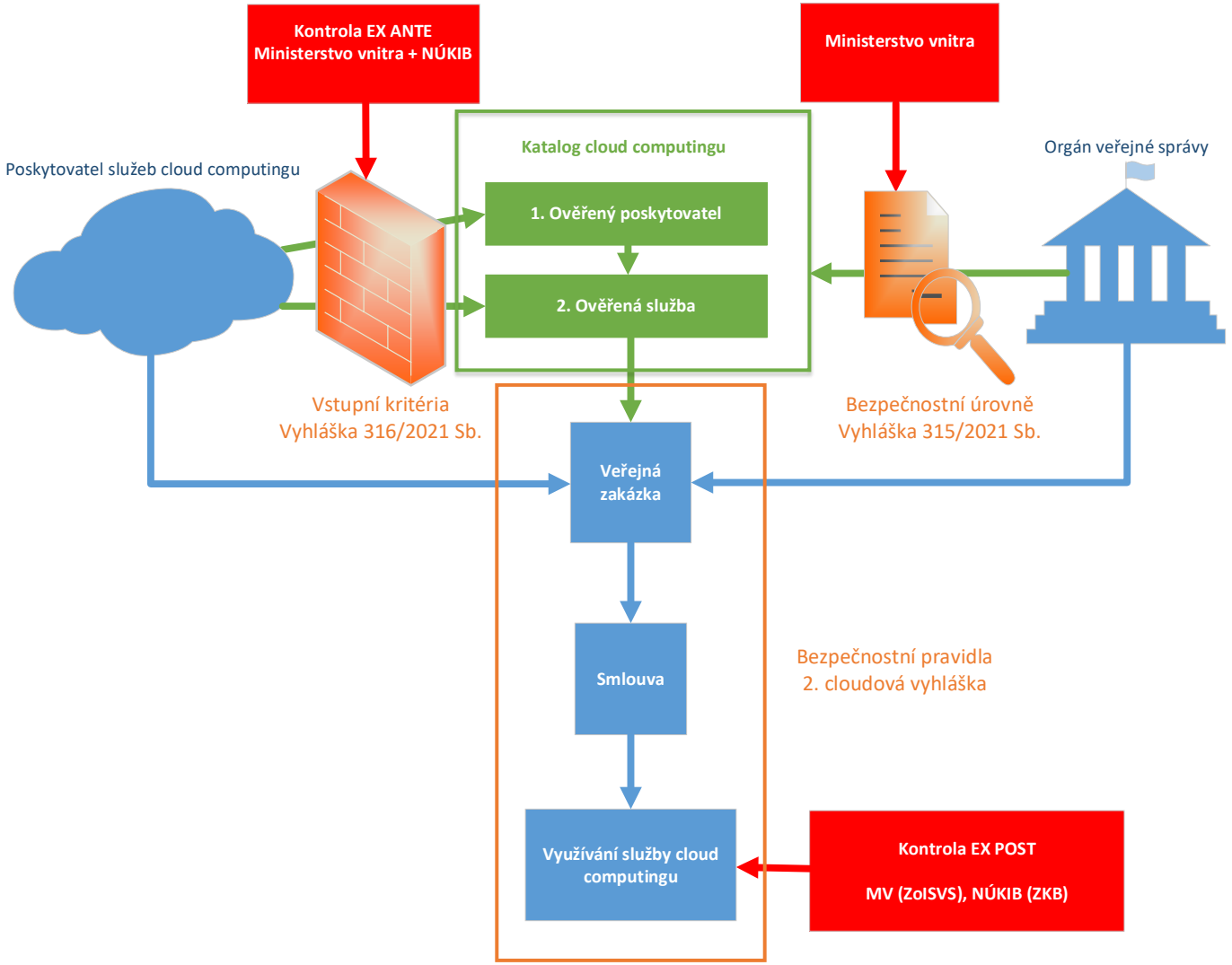
- **Regulatorní rámec**
  - zákon č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS)
  - zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB)
- základní úprava od 1. 8. 2020 – řada nedostatků – bylo nutné novelizovat
- novely provedeny zákonem č. 261/2021 Sb., tzv. DEPO účinnost od **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 (tzv. vstupní kritéria)
  - vyhláška č. 315/2021 Sb., **o bezpečnostních úrovních** pro využívání cloud computingu orgány veřejné moci (tzv. vyhláška o bezpečnostních úrovních)

Regulace cloud computingu ve veřejné správě

- Personální působnost úpravy:
  - **Orgány veřejné správy s ISVS**
    - Nabídky poskytovatele a poptávky orgánů veřejné správy musí být v **katalogu cloud computingu**
    - Podle § 2 ZoISVS – menší množina, než množina orgánů veřejné správy – některé orgány mají **výjimku**
    - Dopadá jen na ty systémy, které jsou zařazeny v ISVS
  - **Orgány veřejné moci**
    - Musí postupovat podle §4/5 ZKB
    - Budou postupovat podle připravované **vyhlášky o bezpečnostních pravidlech**, to znamená, že pokud zároveň nejsou ISVS, tak na ně dopadá jen vyhláška o bezpečnostních pravidlech, která následně mají požadovat v rámci nákupu cloudu (typicky požadavky do smluv)
  - Všichni výše jmenovaní by ale měli zařadit své informační systémy do bezpečnostní úrovně předtím, než uzavřou smlouvu s poskytovatelem a v závislosti na tom zajistit dodržení bezpečnostních pravidel/nakoupit v rámci katalogu této úrovni odpovídající cloudovou službu

Schéma regulatorního rámce cloud computingu - ZoISVS



Tři cloudové vyhlášky

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 = vstupní kritéria pro poskytovatele i službu
- Cloudové služby rozděleny do 4 úrovní podle požadavku na bezpečnost
- Naplnění požadavků posoudí MV a NÚKIB = správní řízení

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, která 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
- Bezpečnostní úrovně jsou 4: nízká, střední, vysoká (= komerční), kritická (= státní)

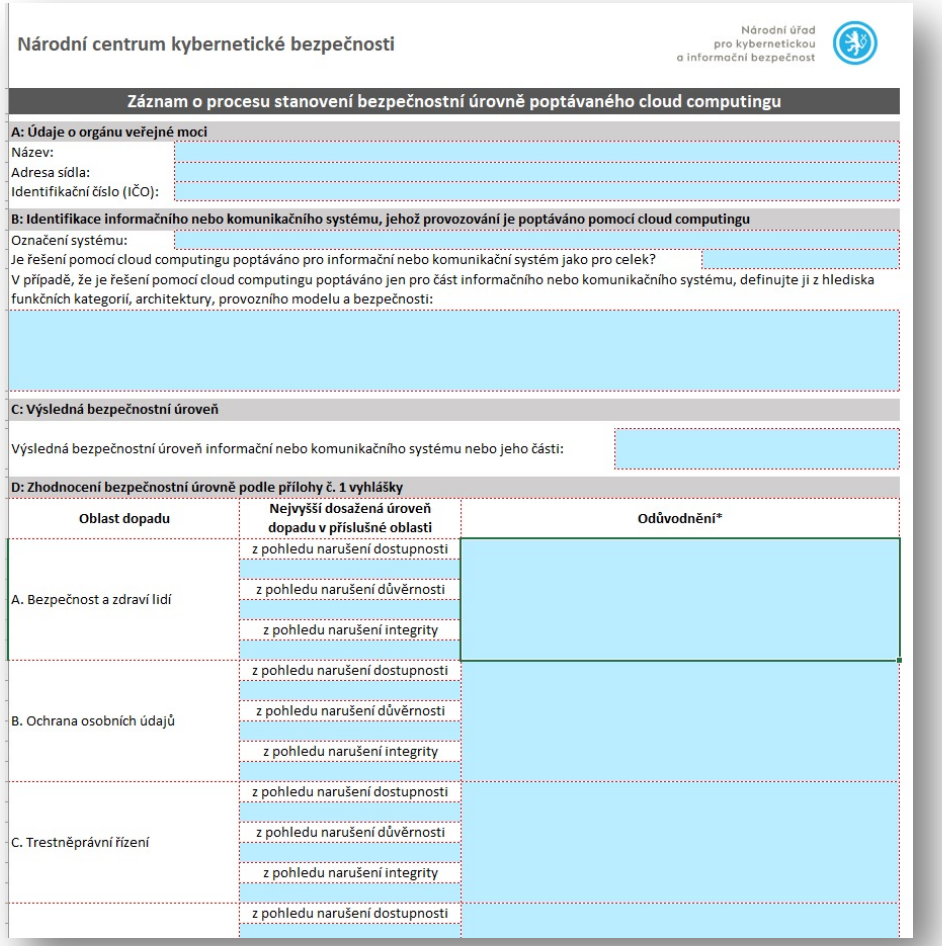
Tři cloudové vyhlášky - formulář

https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/

Formulář hodnocení bezpečnostních úrovní

Pro splnění povinnosti podle § 4 odst. 5 zákona o kybernetické bezpečnosti ve spojení s vyhláškou 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci.

› ke stažení zde



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	
	z pohledu narušení dostupnosti	

Tři cloudové vyhlášky

3. Vyhláška o bezpečnostních pravidlech

- Ve výrobě – vydání předpokládáme v průběhu roku 2022, v blízké době do MPŘ
- 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 pravidla a zváží vhodnost volitelných s ohledem na jejich aplikovatelnost a nezbytnost pro zajištění bezpečnosti informací.
- **Možnosti zajištění splnění vyhlášky:**
  - Prohlášení poskytovatele
  - Certifikace poskytovatele – ISO 27001, ISO 27017, ISO 27018, C5, SOC 2® Type 2, ISO 20000 nebo ISO 22301, v budoucnu evropská certifikace (EUCS)
  - 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 do 1. 1. 2024
- **Zákon č. 261/2021 Sb., Čl. LXXXI**
  - OVS využívalo CC nebo uzavřelo smlouvu před 1. 9. 2021 dle pravidel platných od 1. 8. 2020 = 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 (mimo platná pravidla) 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 - 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
- Podpůrné materiály: Průvodce zařazením poptávaného cloud computingu do bezpečnostní úrovně a Požadavky na zprávy z penetračních testů v souvislosti se zápisem cloud computingu do katalago cloud computingu
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Dotazy?

Děkuji za pozornost!

regulace@nukib.cz