Novela vyhlášky o významných informačních systémech

Adam Kučínský
Ředitel odboru regulace
Národní úřad pro kybernetickou a informační bezpečnost
Odbor regulace
11. 2. 2020

Novela vyhlášky o významných informačních systémech vyhl. č. 317/2014 Sb.

Cíl:

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

Fáze:

- Za NÚKIB je návrh hotov
- Záleží na spolupředkladateli – MV
- Následovat bude fáze vypořádání připomínek s ostatními připomínkovými místy

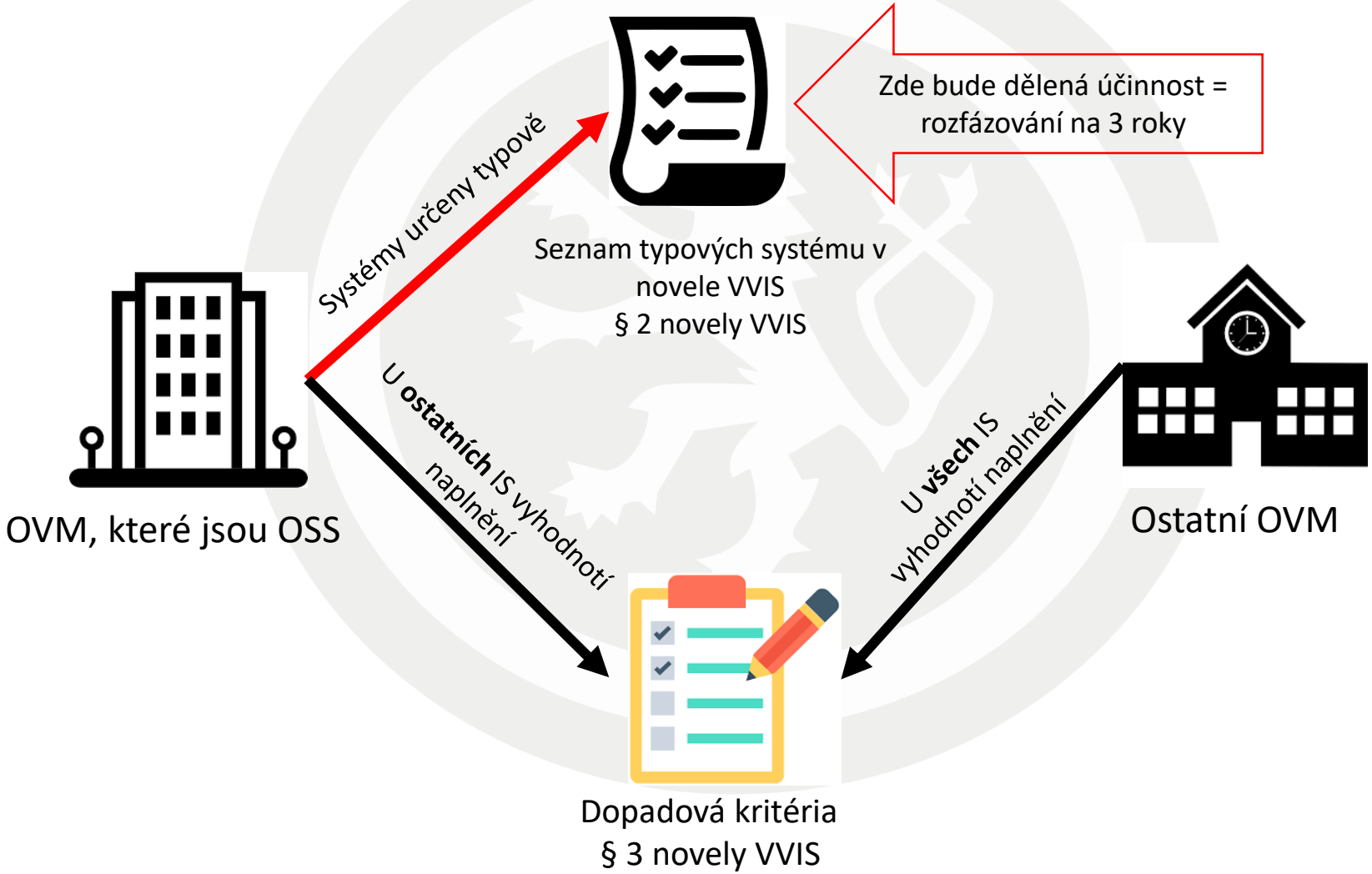
Účinnost:

- ??

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 naplní budou VIS

Novela vyhlášky o VIS – schéma určování



Nový systém určení významného informačního systému po novele

1. **Pevně „defaultně“ vyjmenované informační systémy**

- omezení či výrazné ohrožení výkonu působnosti organizační složky státu, kraje, hl. města Prahy je implicitně obsaženo
- VIS = informační systém využívaný při výkonu působnosti orgánu veřejné moci k zajištění

nebo

2. **Naplnění dopadových kritérií**

- obdobně jako dnes např. omezení či narušení fungování orgánu veřejné moci a zároveň omezení, narušení, zásah či ohrožení nebude možné odvrátit bez vynaložení nepřiměřených nákladů

Nový systém určení významného informačního systému po novele

(1) Významný informační systém podle § 2 písm. d) zákona je informační systém spravovaný orgánem veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při **výkonu působnosti orgánu veřejné moci** k zajištění

a) **výkonu spisové služby,**

b) **výkonu státního dozoru,**

c) **kontrolní a inspekční činnosti,**

1. vlna - 2020

d) **přípravy na krizové situace a jejich řešení,**

e) **elektronické pošty,**

f) **vedení úřední desky způsobem umožňujícím dálkový přístup,**

2. vlna - 2021

g) **mezinárodní spolupráce nebo**

h) **zadávání veřejných zakázek.**

3. vlna - 2022

(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.**

NÚKIB

Systémy, které byly vypuštěny z § 2 (po MPŘ)

Oproti předchozímu návrhu (v MPŘ) byly z „povinného“ § 2 vypuštěny následující typy IS:

- vedení správního řízení,
- databáze obsahující osobní údaje,
- hospodaření orgánu veřejné moci,
- tvorba právních předpisů,
- vedení internetových stránek,
- mezirezortní spolupráce,
- státní statistická služby.

Návrh § 3 nové vyhlášky o VIS

Bude platit od začátku – nebude dělená účinnost

§ 3

Určující kritéria

(1) Určujícím kritériem je skutečnost, že narušení bezpečnosti informací v informačním systému, který není uveden v § 2 odst. 1, by mohlo způsobit

a) omezení či narušení **fungování orgánu veřejné moci**,

b) omezení či narušení **poskytování služeb nebo informací** orgánem veřejné moci veřejnosti,

c) omezení či narušení hospodaření orgánu veřejné moci,

d) omezení či narušení fungování, poskytování služeb nebo informací veřejnosti, nebo hospodaření **jiného** orgánu nebo osoby podle § 3 zákona,

e) zásah do osobního života nebo do práv fyzických nebo právnických osob postihující **nejméně 50 000 osob**, nebo

f) ohrožení či narušení **veřejného zájmu**,

a toto omezení, narušení, zásah či ohrožení **nebude možné odvrátit bez vynaložení nepřiměřených nákladů**.

Analýza dopadu regulace - RIA

- Na základě připomínek z MPŘ a domluvy se spolupředkladatelem (MV) zpracováno hodnocení dopadů regulace RIA.
- Snahou je zejména vypracovat odhad nákladů novely VVIS (I přes specifickou povahu vyhlášky o kybernetické bezpečnosti, kde náklady závisí na každé jednotlivé analýze rizik.).
- Zvolený postup:
  - Zjistit co nejpřesněji objem vynaložených **nákladů na zabezpečení jednoho typového informačního systému.**
  - Zjistit co nejpřesněji **počet systémů**, které budou nově zařazeny pod vyhlášku o významných informačních systémech.
  - Vzájemným vynásobením těchto hodnot získat odhad nákladů na novelu vyhlášky o významných informačních systémech.

RIA: Náklady na zabezpečení typového systému

- Snahou bylo nezatěžovat znovu subjekty dalším dotazníkovým šetřením
- Vycházelo se z dat průzkumu „Nákladů na ministerstvech“
  - Konkrétněji se jedná o **medián nákladů na typický informační systém jednotlivých respondentů očištěný o významné extrémy**.
  - Započítány byly náklady na pořízení a provoz bezpečnostních opatření a na personální zabezpečení.

Typ nákladů	Medián nákladů na 1 typický systém v jednotkách Kč	
Každoroční	Náklady na zaměstnance za 1 rok	60 000 Kč
Každoroční	Provoz bezp. opatření za 1 rok	221 290 Kč
Jednorázový	Pořízení bezp. opatření	540 540 Kč
Každoroční	Provozní náklady v každém dalším roce na 1 systém – součet provoz + personál	281 290 Kč
	Celkové náklady na 1 systém za 1 rok	**821 830 Kč**

RIA: počet systémů

Velký resort	§ 2- První vlna	§ 2 - Druhá vlna	§ 2- třetí vlna	**celkem**
MD	11	10	3	**24**
MF	22	9	2	**33**
MK	13	2	0	**15**
MMR	5	8	0	**13**
MO	0	3	1	**4**
MPO	22	18	1	**41**
MPSV	4	5	1	**10**
MSP	64	4	6	**74**
MŠMT	0	1	0	**1**
MV	13	84	7	**104**
MZD	2	18	0	**20**
MZE	22	10	11	**43**
MZV	1	1	0	**2**
MŽP	7	6	1	**14**
ÚVČR	2	2	0	**4**
PS PČR	2	1	0	**3**
S PČR	1	1	0	**2**
Hrad	1	1	0	**2**
ČSSZ	0	0	0	**0**
Celkem	**192**	**184**	**33**	**409**
Odhad další OSS § 2 a § 3	173	80	50	**303**
Celkem systému pod VIS	365	264	83	**712**

RIA: Počet systémů a náklady na novelu

Náklady na variantu ochrany prioritních IS v jednotkách Kč		
Období	Počet systémů	Náklady
Rok 2020	365	299 967 950 Kč
Rok 2021	264	216 963 120 Kč
Rok 2022	83	68 211 890 Kč
Celkem	712	585 142 960 Kč

VS.

Náklady na variantu ochrany všech ISVS v jednotkách Kč	
Počet systémů	Náklady
7783	6 396 302 890 Kč

RIA: Náklady na zabezpečení typového systému - postup

Prakticky tedy bylo postupováno následovně:

- Sečetly se náklady na bezpečnostní opatření na všechny systémy v organizaci (vyjma těch již pod ZKB určených),
- To bylo poděleno počtem systémů v organizaci (vyjma těch již pod ZKB určených).
- Tím byly získány průměrné náklady na zabezpečení 1 systému na úroveň VIS na každém ministerstvu.
- Tím bylo získáno 15 hodnot.
- Z těchto hodnot byl následně vypočten medián.
- Tato operace byla provedena třikrát - pro každý typ nákladů - pořízení, provoz, personál.

DĚKUJI ZA POZORNOST

Adam Kučínský

Národní úřad pro kybernetickou a informační bezpečnost
Odbor regulace

regulace@nukib.cz
www.nukib.cz | www.govcert.cz

NÚKIB