Novinky v oblasti regulace a ohlédnutí za loňským rokem

CyberCon Brno 2020

Adam Kučínský
Národní úřad pro kybernetickou a informační bezpečnost
Odbor regulace

17. září 2020

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

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

Cíl:

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

Fáze:

- **ZVEŘEJNĚNO VE SBÍRCE ZÁKONŮ = novela je platná**
- 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.
- Příslušnou částku Sbírky zákonů lze nalézt zde: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=360/2020&typeLaw=zakon&what=Cislo_zakona_smlouvy
- Novelizovaná vyhláška je již dostupná i zde: https://www.zakonyprolidi.cz/cs/2020-360/zneni-20210101

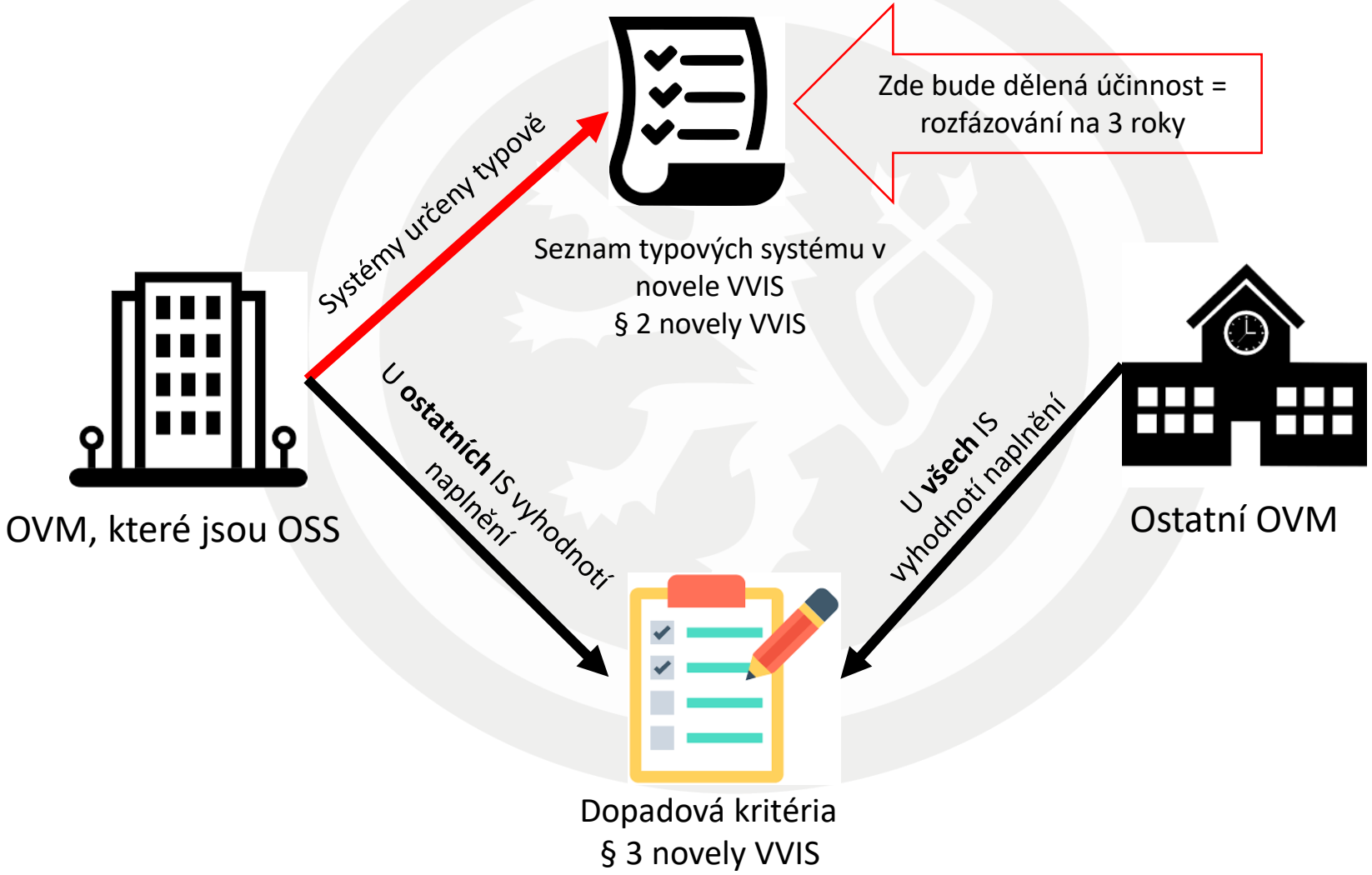
Účinnost:

- 1. 1. 2021

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

Novela vyhlášky o VIS – schéma určování



Pevně „defaultně“ vymezené systémy - § 2

(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.

Naplnění dopadových kritérií - § 3

Platí od začátku – bez dělené účinnosti

§ 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 **poskytování služeb nebo informací** orgánem veřejné moci veřejnosti,

b) omezení či narušení **hospodaření** orgánu veřejné moci,

c) jiné omezení či narušení **fungování orgánu veřejné moci,**

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

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**.

Evidence systémů

§ 3

(2) Orgán veřejné moci vede seznam všech informačních systémů, kterých je správcem, a u každého informačního systému, který **není uveden v § 2 odst. 1**, posoudí naplnění určujících kritérií podle odstavce 1. O výsledku posouzení vede správce informačního systému písemný záznam, který je součástí seznamu podle věty první.

Prakticky:

- Systémy, které nejsou určeny typově podle seznamu v § 2 a podléhají tak posouzení dle § 3 jsou přidány na tento seznam
- Po posouzení těchto systémů je výsledek (identifikace/neidentifikace VIS a důvody pro toto rozhodnutí) uveden rovněž v seznamu

Cíle:

- Přenositelnost obsahu úvahy o posouzení ne/naplnění kritérií VIS pro budoucí zodpovědné zaměstnance
- Získat auditní stopu, že k posouzení došlo a jakou úvahou bylo vedeno

Novely zákona o kybernetické bezpečnosti

Vývoj:

- Za poslední rok jedna novelizace ZKB od 1. 2. 2020, další novelizace v procesu

Novelizace přestupků a drobné opravy:

- Novelizace opravuje chyby z ZKB v § 5 (bezpečnostní opatření) a § 25 (přestupky)
- Účinná od 1. 2. 2020

Novelizace kontaktních údajů, přestupků v souvislosti s cyber security aktem a předávání informací z evidence kybernetických bezpečnostních incidentů:

- Hlášení rozsahu veřejných IP adres systému, přestupky v oblasti certifikace kybernetické bezpečnosti a neposkytování informací z evidence, které by ohrozily zájem chráněný zákonem o kybernetické bezpečnost
- Účinná v budoucnu

Novelizace v souvislosti s regulací cloudů (+ zákon o ISVS):

- Úprava zmocnění k vydání cloudové vyhlášky a k stanovení místa zpracování údajů v rámci cloudu
- Účinná v budoucnu

Nové podpůrné materiály

Nový web NÚKIB

V průběhu srpna spojil NÚKIB své dosavadní weby www.nukib.cz a www.govcert.cz do aktuálního a jediného

www.nukib.cz

Podpůrné materiály a další informace od odboru regulace a odboru kontroly naleznete nově na

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola

Podpůrné materiály – VTC standard

- **Cíl:** Stanovit minimální požadavky na bezpečnost a funkcionality VTC aplikací s ohledem na důvěrnost informací (primární adresáti státní správa)
- **Nosné části:** Klasifikace informací, funkční požadavky, bezpečnostní požadavky, pravidla pro uživatele
- **Použití v ZVZ:** Jako inspirace, požadavky je nutno si odůvodnit, může být i přísnější
- **Vztah k ZKB:** Nelze bez dalšího aplikací standardu mít ZKB za splněný
- **Termín vydání:** Vydáno
- **Vymahatelnost**: Dobrovolné
- Vydáno ve spolupráci s:
  - NAKIT
  - a dalšími – VZ, BIS, ÚZSI, AFCEA, AČR, CISCO, MICROSOFT, GESTO, ATS TELCOM

Dokument zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

Podpůrné materiály – Minimální bezpečnostní standard

- **Cíl:** Stanovit minimální bezpečnostní požadavky na systémy mimo ZKB
- **Nosné části:**
  - Manažerská část – organizační opatření,
  - Technická část – technické opatření;
  - ➢ Bez analýz, seznam požadavků.
- **Použití v ZVZ:** Jako inspirace, požadavky je nutno si odůvodnit, může být i přísnější
- **Vztah k ZKB:** Nelze bez dalšího aplikací standardu mít ZKB za splněný
- **Termín vydání:** Vydáno
- **Vymahatelnost**: Dobrovolné
- Vydáno ve spolupráci s MV a NAKIT
- V plánu je ještě zpracovat přílohu k požadavkům na logování

Dokument zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

Podpůrné materiály – Bezpečnostní doporučení v kyberprostoru pro vrcholové vedení

- **Cíl:** vytvořit pro premiéra/vládu/poslance a další vrcholové vedení bezpečnostní doporučení pro pohyb v kyberprostoru
  - Cílí primárně na uživatele, kteří často nejsou úplně v moci interního IT/bezpečnosti
- **Nosné části:** Práce s firemním počítačem a smartphonem, bezpečná komunikace, zabezpečení online účtů
  - Dokument obsahuje téměř 30 základních bezpečnostních opatření, kterými by se mělo vrcholové vedení organizací a jejich čelní představitelé řídit. Opatření jsou rozdělena do výše uvedených témat.
- **Použití v ZVZ:** nerelevantní
- **Vztah k ZKB:** Nelze bez dalšího aplikací doporučení mít ZKB za splněný
- **Termín vydání:** Vydáno 2020
- **Vymahatelnost**: Dobrovolné

Podpůrné materiály – (Ne)poskytování informací o bezpečnosti

NÚKIB aktualizoval a přepracoval dokument k (ne)poskytování informací v oblasti kybernetické bezpečnosti a bezpečnosti systémů nakládajících s utajovanými informacemi.

Dokument je rozdělen do tří částí a shrnuje doporučení NÚKIB k poskytování informací na žádost veřejnosti. Omezení poskytování informací rozpracovává z těchto pohledů:

1. **§ 10a zákona o kybernetické bezpečnosti** – informace, jejíž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti
   - vhodné pro použití u bezpečnostní dokumentace (aktiva s vysokým hodnocením)
2. **§ 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím** – informace, jejíž poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření
   - vhodné pro použití u informací o bezpečnostních opatřeních
3. **§ 7 zákona o svobodném přístupu k informacím** – utajované informace

Dokument zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

(Ne)poskytování informací o bezpečnosti

NÚKIB navrhuje změnu zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Návrh ze strany NÚKIB:

V § 11 se doplňuje odstavec 7, který včetně poznámky pod čarou č. 21 zní:

„(7) Povinný subjekt neposkytne informaci o seznamu prvků kritické infrastruktury[21)] a informace, jejichž poskytování je vyloučeno zákonem o kybernetické bezpečnosti.

_____

[21)] § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.“

Důvod:

Nutno chránit seznam prvků KI/KII

Aktuální fáze legislativního procesu:

26. 8. 2020 ukončeno připomínkové řízení, nyní jsou vypořádávány připomínky

Podpůrné materiály – Provozovatel systému - informování

NÚKIB plánuje aktualizovat podpůrný materiál k provozovateli systému a doplnit do něj vzory informování provozovatele systému a významného dodavatele, který má vliv na bezpečnost.

Vzor informování obsahuje povinné náležitosti podle:

- § 8 odst. 1 písm. b) a c) a odst. 3 vyhlášky o kybernetické bezpečnosti,
- tzn. zohledňuje obsah podpůrného materiálu k provozovateli systému:

„(Informování) *by však mělo být provedeno **prokazatelně**, **adresně** a ve vztahu ke každému jednotlivému provozovateli **samostatně**. Podstatnými náležitostmi prokazatelnosti bude **informace o tom, že se jedná o provozovatele konkrétního systému podle zákona o kybernetické bezpečnosti**, s čímž je neodmyslitelně spjato také **stanovení systému** spadajícího do působnosti zákona o kybernetické bezpečnosti, vymezení technických a programových prostředků, které tvoří určený systém, resp. **vymezení činností dodavatele v rámci určeného systému**, **a to tak, aby došlo k dostatečné identifikaci toho, pro co se dodavatel stává provozovatelem daného systému**“.*

Dokument bude zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

Zkušenosti z kybernetických útoků na sektor zdravotnictví

Vybrané činnosti NÚKIB v souvislosti s útoky na nemocnice

- 11.12. 2019 – Incident v nemocnici v Benešově
- 12. 3. 2020 – Incident ve FN Brno
- 17. 3. 2020 – Vydáno reaktivní opatření (RO) pro nemocnice
- 18. 3. 2020 – vydána metodika k RO
- 18. 3. 2020 – vydáno a rozesláno doporučení pro poskytovatele zdravotních služeb vč. metodiky
- 27. 3. 2020 - Nabídka služeb nemocnicím – e-learning, sken zranitelností, Turris Mox (ve spolupráci s CZ.NIC)
- 16. 4. 2020 – Varování
- 17. 4. 2020 – Doporučení k varování

Průběžně:

- **Řešení větších či menších incidentů a událostí – konzultace, výměna informací, pomoc s vyšetřováním**

Reaktivní opatření pro nemocnice a metodika I.

- 17. 3. 2020 – Vydáno reaktivní opatření (RO) pro nemocnice
- Postup podle § 13 odst. 1 zákona č. 181/2014 Sb.
- Závazné pro adrésáty - nemocnice pod ZKB
- **Důvod vydání**: Na základě proběhnuvšího incidentu
- **Cíl**: Minimalizace rizika vzniku podobných incidentů – zabezpečení systémů před incidentem
- **Náplň**: Provést 4 sady úkonů, celkem 20 konkrétních opatření
- **Legitimizace neprovedení úkonu**: Pokud by provedení úkonu způsobilo větší dopad než incident samotný
- K RO byla vydána metodika, která jej konkretizovala, uváděla cíle jednotlivých úkonů a doporučení k provedení

Doporučení pro poskytovatele zdravotních služeb vč. metodiky

- 18. 3. 2020 – vydáno a rozesláno doporučení pro poskytovatele zdravotních služeb vč. metodiky
- Velmi podobné RO
  - vypuštěny některé body
  - nezávazné
- Rozesláno na 85 zdravotnických zařízení, které byly označeny ze strany MZD jako „páteřní“

Nabídka služeb nemocnicím

- 27. 3. 2020 - Nabídka služeb nemocnicím

1. Sdružení CZ.NIC nabídlo nemocnicím pod ZKB bezplatně **routery TURRIS MOX vč. zaškolení a asistence** – umožnění splnění segmentace sítě z reaktivního opatření
2. NÚKIB nabídl **monitoring zranitelností**
3. NÚKIB nabídl **školení uživatelů pomocí e-learnigu** – s možností zajištění „na klíč“ nebo k nasazení na vlastní infrastruktuře

Bohužel těchto služeb využilo jen malé množství oslovených.

Varování ze dne 16. 4. 2020 a doporučení k němu

- 16. 4. 2020 – Varování
- 17. 4. 2020 – Doporučení k varování
- Varování před hrozbou spočívající v realizaci **rozsáhlé kampaně závažných kybernetických útoků** na informační a komunikační systémy v České republice, zejména pak na systémy zdravotnických zařízení
- Obsahovalo doporučení
  - Varovat uživatele před spear-phisingem
  - Zabránit spouštění maker
  - Zablokovat zbytné přístupy z vnějšku
  - Offline zálohy vč. kontroly funkčnosti
- K tomu vydáno doporučení s dalšími opatřeními

Shrnutí - zkušeností z kybernetických útoků na sektor zdravotnictví

- **Ukázalo se, že:**
  - Narušení informačních systémů nemocnic má reálné dopady
  - Některé nemocnice pod ZKB nemají zavedena některá opaření podle ZKB
  - Počet nemocnic pod ZKB je nízký
  - Lidí, kteří v nemocnicích dělají bezpečnost je málo
  - NÚKIB nemá efektivní komunikační nástroj směrem k nemocnicím
  - NÚKIB je „dimenzován“ na povinné osoby

- **Co s tím?**
  - Koordinace a standardizace v KB pro nemocnice
  - Zvýšení počtu nemocnic pod ZKB
  - Oborový CERT pro zdravotnictví – nutno mít protějšek v nemocnicích

Bilance a výzvy pro regulaci v nejbližší době

- Posunout určování povinných osob
- Zlepšit zohledňování bezpečnosti v prostředí veřejných zakázek – bude nový podpůrný materiál
- Dokončit projekt metodiky k analýze rizik – bude nový podpůrný materiál
- Sjednocení hlášení kybernetických incidentů
- Zlepšení pokrytí odvětví zdravotnictví
- Navázání užší spolupráce s dalšími regulátory (zejména u kritické infrastruktury)
- **Dotáhnout problematiku regulace cloudu**
- **Neustále zvyšovat úroveň poskytovaných služeb**

Povinné osoby pod ZKB

Doposud určeno:

- 52 subjektů kritické informační infrastruktury se 120 systémy
  - V případě kritické informační infrastruktury aktuálně probíhá revize dosavadního určení

- 50 provozovatelů základních služeb s 55 systémy
  - V případě provozovatelů základní služby aktuálně probíhá proces určování (určují se vždy celá odvětví najednou)
  - Celkový počet finálně určených subjektů se odhaduje kolem 200 provozovatelů základní služby

Typické problémy určování jsou celková vytíženost odboru regulace (především cloudová vyhláška) a snaha subjektů vyhnout se regulaci za každou cenu.

DĚKUJI ZA POZORNOST

regulace@nukib.cz