Zákon o kybernetické bezpečnosti a jeho implementace aktuálně

Aktuality z oblasti regulace

Adam Kučínský
ředitel
odbor regulace

Národní úřad
pro kybernetickou
a informační bezpečnost

Disclaimer

- Prezentace obsahuje informace platné ke dni její realizace, tedy k 02.04.2019.
- Informace, fakta a údaje obsažené v prezentaci mají informační charakter.
- Pro zajištění souladu se zákonem o kybernetické bezpečnosti je nutno vycházet z aktuálně účinné legislativy. Aplikaci takových informací či opatření je nutné vždy vztahovat ke konkrétním systémům a institucím.

Počet povinných osob ze ZKB

- KII – správci cca 50, systémy cca 110
- VIS – správce cca 60, systémy cca 160
- ISZS (PZS) – cca 35 správců/systému
- Provozovatelé – cca 60 subjektů

Návrh novely vyhlášky o VIS (2019)

Usnesení vlády

- Usnesení vlády č. 241 z 18. dubna 2018, které ukládá:
  - řediteli NÚKIB provést ve vyhlášce takové změny, aby „**byly jako významné informační systémy určeny všechny informační systémy spravované orgány veřejné moci, u kterých by narušení bezpečnosti informací mohlo omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci** a které nejsou kritickou informační infrastrukturou nebo informačním systémem základní služby“
  - členům vlády a vedoucímu Úřadu vlády, **aby informační a komunikační technologie využívané jimi řízenými ústředními správními úřady zabezpečili** podle požadavků vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), **alespoň na stejné úrovni, která je touto vyhláškou stanovena pro významné informační systémy.**

Návrh novely vyhlášky o VIS

- Východiska navrhované změny právní úpravy:
  - **Zrušit přílohu č. 1** vyhlášky o VIS
  - Zjednodušit **a zpřehlednit proces identifikace**
  - Zvýšit **efektivnost** vyhlášky
  - Zvýšit **právní jistotu** adresátů
  - Obsahové a rozsahové naplnění **zmocnění § 6 písm. d) ZKB**:
    - „Prováděcí právní předpis **stanoví významné informační systémy** a jejich určující kritéria.“
- Došlo k **zapracování připomínek** z mezirezortního připomínkového řízení
- V současné době **probíhá nové kolo projednání aktualizovaného návrhu** se zástupci spolupředkladatele (MV)

- 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

Postup identifikace VIS po novele

- Princip „síta“
- Zákonná definice (§ 2 písm. d) ZKB):
  - Informační systém **spravovaný** orgánem veřejné moci
  - a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit **výkon působnosti orgánu veřejné moci**
  - Informační systémy, které **slouží k výkonu působnosti orgánu veřejné moci**, nikoli veškeré IS dané organizace a jejichž správcem je orgán veřejné moci

- Vyhláška o významných informačních systémech
  - § 2 navrhovaného znění: Organizační složky státu a vyšší územně samosprávné celky – určeny všechny systémy, které budou v § 2 vyjmenovány
  - § 3 navrhovaného znění: Dopadová kritéria - Další orgány veřejné moci a zbylé informační systémy organizačních složek státu a vyšších územně samosprávných celků s výjimkou obcí

Návrh § 2 nové vyhlášky o VIS

§ 2

Významné informační systémy

(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,

d) přípravy na krizové situace a jejich řešení,

e) elektronické pošty,

f) vedení úřední desky způsobem umožňujícím dálkový přístup,

g) mezinárodní spolupráce nebo

h) zadávání veřejných zakázek.

(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.**

Systémy, které byly vypuštěny z §2

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

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

Návrh § 3 nové vyhlášky o VIS

§ 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**.

Vyhláška o způsobu likvidace kopií dat a provozních údajů informačního systému veřejné správy a náležitosti protokolu o průběhu likvidace kopií

(Likvidační vyhláška)

Likvidační vyhláška

- **Cíl:**
  - stanovit **způsob likvidace** kopií dat a provozních údajů **informačního systému veřejné správy** a **náležitosti protokolu o průběhu likvidace** kopií
  - Vytvořit prováděcí předpis k zákonu o informačních systémech veřejné správy tak, aby v případě překryvu povinností dle ISVS a ZKB, byly požadavky na likvidaci zastupitelné.
- **Fáze:**
  - Mezirezortní připomínkové řízení
- **Účinnost:**
  - květen 2019

Způsoby likvidace kopií

§ 2

Způsob likvidace kopií

(1) Provozovatel informačního systému veřejné správy (dále jen „provozovatel“) zlikviduje kopii

a) vymazáním,

b) přepsáním nahodilými daty,

c) likvidací kryptografických klíčů k zašifrovaným datům nebo provozním údajům, nebo

d) likvidací nosiče, na němž je kopie uložena.

- **Každý stupeň likvidace odpovídá stupni důvěrnosti dané informace, ty jsou hodnoceny na základě přílohy č. 1 k likvidační vyhlášce (nízká, střední, vysoká a kritická)**
- Způsob je volen dle klasifikace důvěrnosti informací jako **odpovídající nebo vyšší**
- O likvidaci je veden **protokol o průběhu likvidace kopií,** vyhláška stanovuje obsah tohoto protokolu.
- **Pro zajištění souladu se zákonem u postupu při likvidaci u systému, který je ISVS a zároveň i VIS stačí dodržení postupu podle jedné z vyhlášek (VKB nebo likvidační)**

Vyhláška o obsahu a rozsahu bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

(Cloudová vyhláška)

Cloudová vyhláška

- **Cíl:**
  - Vytvoření prováděcí vyhlášky k ZKB, která stanoví **obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu**
  - **Naplnit zmocnění:** § 6 písm. e) ZKB:
    - Stanovit vyhláškou obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.
- **Východiska:**
  - Vychází z dokumentů projektu Příprava vybudování eGovernmentCloudu (usnesení vlády ČR č. 749 ze dne 14. listopadu 2018)
  - ISO 27001, 27017 a 27018
- **Fáze:**
  - Probíhá příprava textace – schůzky expertních skupiny
  - Finální návrh vyhlášky bude předložen připomínkám odborné veřejnosti

- **Účinnost:**
  - 4Q 2019

Obsah:

1. **Bezpečnostní úrovně systémů – Hodnocení dopadu narušení informací**
   - 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)
2. **Jednotlivé úrovně bezpečnostních opatření**
   - Stanoveny jednotlivé kategorie cloudu, které budou odpovídat jednotlivým úrovním dopadu narušení CIS systému
   - Každá z kategorií bude mít stanovena příslušná bezpečnostní opatření
   - Příslušně kategorizovaný systém (podle bodu 1) bude moci využít pouze tu kategorii cloudu, která odpovídá kategorií systému, nebo vyšší (podle bodu 2).
- **Smluvní podmínky – standard pro dodavatelské smlouvy**
   - CC služby jsou zajišťovány dodavatelsky – mnoho opatření bude smluvních
   - Obecně jsou požadavky na smlouvy povinných osob ze ZKB (VIS, PZS, KII) stanoveny v příloze č. 7 VKB
   - Vyhláška se bude týkat všech OVM, tedy nejen KII, VIS a PZS.
   - Je třeba zajistit, aby požadavky na smlouvy s poskytovateli CC služeb nebyly v rozporu s výše zmíněnými požadavky VKB a spíše je doplňovaly pro případ specifického řešení – CC.

Varování podle § 12 ZKB
-
použití a dopady

Institut Varování

§ 12 ZKB – Varování

(1) **Úřad vydá varování**, **dozví-li se** zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, **o hrozbě v oblasti kybernetické bezpečnosti**.

(2) Varování **Úřad zveřejní na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3**, jejichž kontaktní údaje jsou vedeny v evidenci podle § 16 odst. 4.

Co varování znamená

- Prostřednictvím varování NÚKIB **upozorňuje na existenci hrozby** v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat.
- **Subjekty,** které spadají pod zákon ZKB, **jsou povinny se touto hrozbou dále zabývat a zohlednit ji v analýze rizik**, kterou v souladu s požadavky ZKB a příslušné vyhlášky již pravidelně provádí.
- Varování neznamená bezpodmínečný zákaz používání daných technických a programových prostředků, ale nutnost zvážit případné bezpečnostní riziko související s jejich užíváním.
- Dovolí-li to výsledky analýzy rizik, uvedené technické nebo programové prostředky je možné i nadále používat.
- **Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně tak jako široké veřejnosti, nezakládá varování NÚKIB povinnosti**. Tyto subjekty tedy nejsou podle ZKB povinny varování NÚKIB zohlednit. Další kroky s tím spojené jsou pouze na nich.

Implementace varování

- KII, VIS a PZS jsou povinni podle § 5 VKB pro určené IS a KS provádět pravidelnou analýzu rizik, identifikovat rizika a identifikovaná rizika řídit.
- Na základě vyhodnocení rizik potom výše uvedené subjekty zavádějí a provádějí bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti v souladu s § 4 odst. 2 ZKB.
- Bezpečnostní opatření jsou blíže specifikována ve VKB.
- V souvislosti s řízením rizik musejí podle § 5 odst. 1 písm. h) bod 3 VKB tyto subjekty zohlednit mimo jiné i opatření podle § 11 ZKB, tedy i varování vydané podle § 12 ZKB.
- **Na základě vydaného varování tedy musejí výše zmíněné povinné osoby v rámci zavedeného řízení rizik provést analýzu rizik, ve které zohlední hrozbu, a následně na riziko reagovat přijetím bezpečnostních opatření, která musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika.**

Analýza rizik I.

- Riziko = možnost či pravděpodobnost, že hrozba využije zranitelnosti aktiva a způsobí škodu
- Řízení rizik = souhrn činností vedoucích k nalezení a eliminaci rizik
  - Nutno stanovit rozsah aktiv, kterých se řízení rizik týká a ohodnotit je
  - Dále jim přiřadit a ohodnotit hrozby a zranitelnosti.
- Aktivum = cokoliv, co má pro organizaci hodnotu.
  - Primární aktivum = informace nebo služba, kterou zpracovává nebo poskytuje IS/KS
  - Podpůrné aktivum = technická aktiva (technické vybavení, komunikační prostředky a programové vybavení, objekty), zaměstnanci a dodavatelé.
- Zranitelnost = každé aktivum má zpravidla jednu či více **zranitelností**
  - např. nevhodnou bezpečnostní architekturu, nedostatečnou míru nezávislé kontroly, nevhodně nastavená přístupová oprávnění apod.
- Hrozba = hrozba využívá zranitelností aktiva
  - např. škodlivý kód (viry, spyware, trojské koně apod.), zneužití nebo neoprávněná modifikace údajů, cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik apod.

Analýza rizik II.

- Jakmile je známa hodnota aktiva (viz příloha č. 1 k VKB) a hodnota s ním spojených hrozeb a zranitelností (viz příloha č. 2 k VKB), je nutné určit hodnotu rizika.
- Riziko je kombinací hrozby, zranitelnosti a dopadu na aktivum (dopad bude vycházet z hodnoty aktiva).
  - **Riziko = Dopad (hodnota aktiva) x Zranitelnost x Hrozba**
- Výsledná míra rizika následně indikuje požadavky na ochranu, tedy na konkrétní bezpečnostní opatření - bezpečnostní opatření snižují možnost naplnění nežádoucích jevů.
- Náklady na bezpečnostní opatření by však měly být vždy přiměřené a neměly by převýšit náklady spojené s následky realizace rizika.
- Ze skutečností uvedených ve vydaném varování vyplývá, že **hrozbu, na kterou varování upozorňuje, je v souladu s tabulkou č. 1 přílohy č. 2 VKB potřeba hodnotit jako velmi pravděpodobnou až více méně jistou. = pokud používám stupnici dle VKB bude mít Hrozba spojená s Varováním hodnotu 4 ze 4. Tuto hodnotu dosadím do výše uvedené rovnice a tak získám novou hodnotu rizika.**

Analýza rizik III. - stepplan

1. Analýza prostředí a prošetření, zda a kde jsou dané technické nebo programové prostředky v rámci informačních a komunikačních systémů využívány
   - Např. v seznamu podpůrných aktiv nebo v seznamu majetku organizace
2. U aktiv souvisejících s vydaným varováním je potřeba provést aktualizaci analýzy rizik a zohlednit nové hrozby plynoucí z vydaného varování
   - Důležitá spolupráce manažera kybernetické bezpečnosti, který má znalost procesu analýzy rizik, s garantem aktiva, který je schopný ohodnotit aktivum
3. Výsledkem aktualizace analýzy rizik je nová hodnota rizika
   - V případě překročení akceptovatelné míry rizika, kterou má povinná osoba stanovenu v souladu s požadavky § 5 VKB, je nutné přistoupit k zavedení bezpečnostních opatření a tím k snížení rizika
4. Bezpečnostní opatření
   - např. postupná náhrada daných technických a programových prostředků a jejich vyloučení z výběrového řízení, úprava pravidel pro dodavatele…
   - Bezpečnostní opatření definuje VKB

Příklady zranitelností a hrozeb

Katalogy zranitelností a hrozeb lze najít například ve VKB

Příloha č. 3 k vyhlášce č. 82/2018 Sb.

Zranitelnosti a hrozby

Upozornění: Tato příloha obsahuje jen vybrané kategorie zranitelností a hrozeb. Ident
povinné osoby.

Zranitelnosti

1. nedostatečná údržba informačního a komunikačního systému,
2. zastaralost informačního a komunikačního systému,
3. nedostatečná ochrana vnějšího perimetru,
4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5. nedostatečná údržba informačního a komunikačního systému,
6. nevhodné nastavení přístupových oprávnění,
7. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů bezpečnostních incidentů,
8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit j
9. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné bezpečnostních rolí,
10. nedostatečná ochrana aktiv,
11. nevhodná bezpečnostní architektura,
12. nedostatečná míra nezávislé kontroly,
13. neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Hrozby

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. škodlivý kód (například viry, spyware, trojské koně),
6. narušení fyzické bezpečnosti,
7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické ene
8. zneužití nebo neoprávněná modifikace údajů,
9. ztráta, odcizení nebo poškození aktiva,
10. nedodržení smluvního závazku ze strany dodavatele.

Příloha č. 2 k vyhlášce č. 82/2018 Sb.

Hodnocení rizik

(1) Jednoznačné stanovení funkce pro určení rizika je nezbytnou součástí metodiky pro hodnocení rizik podle § 5.

(2) Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost.

(3) Pro hodnocení rizik lze použít například tuto funkci:

Riziko = dopad x hrozba x zranitelnost.

(4) Dopad je v tomto případě odvozen z hodnocení aktiv podle přílohy č. 1.

(5) V případě, že povinná osoba využívá metodu pro hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně se postupuje i v případech, kdy povinná osoba používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.

Tab. 1: Stupnice pro hodnocení hrozeb

Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Tab. 2: Stupnice pro hodnocení zranitelností

Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté.

ZZVZ a varování I.

- ZZVZ v § 36 odst. 1 = zadavatel nesmí vytvářet při stanovování zadávacích podmínek "bezdůvodné překážky hospodářské soutěže".
  - V případě, že oprávněná autorita (zde NÚKIB), která k tomu disponuje zákonným zmocněním (zde v § 22 písm. b) ZKB), vydává akt (zde varování), který může v konkrétních případech vést k omezení hospodářské soutěže, nemůže být dodržení tohoto omezení při tvorbě zadávacích podmínek považováno za vytváření bezdůvodné překážky hospodářské soutěže.
  - Tedy hospodářskou soutěž v tomto případě lze omezit již při stanovení zadávacích podmínek a nejedná se tím o porušení ZZVZ.
- Nadto § 4 odst. 4 ZKB stanoví:
  - Povinné osoby jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém nebo informační systém základní služby a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou.
  - **Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle ZKB nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.**

ZZVZ a varování II.

Je potřeba zvolit odpovídající postupy ve vztahu k tomu, v jaké fázi se dané výběrové řízení nachází:

1. Fáze přípravy na veřejnou zakázku
   - Je nutné provedení analýzy rizik podle § 5 VKB a následné zapracování jejího výsledku přímo do zadávací dokumentace.
2. Fáze probíhajícího zadávacího řízení
   a. Neuplynula lhůta pro podání žádosti o účast, předběžných nabídek nebo nabídek
      - V takovém případě lze po provedení analýzy rizik v souladu s ustanovením § 99 ZZVZ změnit nebo doplnit zadávací podmínky obsažené v zadávací dokumentaci a prodloužit lhůtu pro podání.

   b. Lhůta uplynula
      - Po provedení analýzy rizik lze buď pokračovat v zadávacím řízení a případně přijmout bezpečnostní opatření ke snížení rizika (aniž by tím byl dotčen postup v zadávacím řízení), nelze-li, pak zrušit zadávací řízení z důvodů podle § 127 odst. 2 písm. d) ZZVZ.
3. Fáze po skončení zadávacího řízení a zadání zakázky uchazeči.
   - V souladu s § 8 odst. 1 písm. e) VKB řídit rizika spojená s dodavateli. Je nutné provedení analýzy rizik podle § 5 VKB a na základě jejího výsledku provést jedno z následujících:
     - Nasazení bezpečnostních opatření ke snížení rizik
     - Pokud není možné přijmout bezpečnostní opatření ke snížení rizika, je nutné podniknout kroky k postupnému nahrazení HW a SW – podle možností

ZZVZ a varování III.

- Je nutné mít na paměti, že vydání varování nelze automaticky považovat za důvod pro vyloučení **uchazeče** ze zadávacího řízení.
  - I nadále platí, že zadavatel je oprávněn vyloučit uchazeče ze zadávacího řízení pouze z důvodů stanovených v ZZVZ (zadavatel by tedy musel varování NÚKIB, resp. důsledky plynoucí z jeho vydání, podřadit pod některý z důvodů uvedených v § 48 ZZVZ).
  - Toto se vztahuje k osobě účastníka
- Vyloučit technické a programové prostředky uvedené ve varování lze, a to cestou **technické specifikace**
- **Vyloučení technických a programových prostředků je nutné odůvodnit**
  - Odůvodnění poskytne právě provedená analýza rizik
- **Tedy na základě varování a následně provedené analýzy rizik je možné vyloučit technické a programové prostředky a nikoli osobu konkrétního účastníka**

Průzkum nákladů na kybernetickou bezpečnost

- Průzkum nákladů na kybernetickou bezpečnost

Celkové náklady na kybernetickou bezpečnost			
2015-2017	Pořízení	Provoz	Celkem
MD	0	58 272	58 272
MF	46 876	27 600	74 476
MK	0	0	0
MO	14 320	2 506	16 826
MMR	3 677	16 197	19 874
MPSV	24 800	66 150	90 950
MPO	10 553	6 295	16 848
MŠMT	240	2 400	2 640
MsP	0	0	0
MV	238 930	77 180	316 110
MZV	2 820	1 900	4 720
Mze	0	0	0
MZd	71 919	59 658	131 577
MZP	3 979	400	4 379

Celkové náklady na kybernetickou bezpečnost			
2018	Pořízení	Provoz	Celkem
MD	0	10 594	10 594
MF	7 058	18 699	25 757
MK	0	0	0
MO	6 015	1 004	7 019
MMR	189	6 610	6 799
MPSV	33 650	41 550	75 200
MPO	9 603	5 361	14 964
MŠMT	4 390	800	5 190
MsP	39 900	0	39 900
MV	77 660	55 320	132 980
MZV	1 850	1 750	3 600
MZe	0	0	0
MZd	62 355	21 372	83 727
MZP	23 039	150	23 189

Celkové náklady na kybernetickou bezpečnost			
2019	Pořízení	Provoz	Celkem
MD	8 000	12 700	20 700
MF	141 836	21 380	163 216
MK	0	0	0
MO	51 015	12 204	63 219
MMR	0	6 228	6 228
MPSV	44 500	173 500	218 000
MPO	11 142	6 491	17 633
MŠMT	62 500	900	63 400
MsP	33 000	0	33 000
MV	209 240	91 490	300 730
MZV	60 950	6 320	67 270
MZe	52 873	810	53 683
MZd	179 036	19 000	198 036
MZP	88 577	1 753	90 330

- **Hlavním cílem průzkumu** bylo zjistit, jaké jsou náklady na zajištění kybernetické bezpečnosti **jednotlivých ministerstev spadajících do působnosti ZKB**.
- **Dílčím cílem průzkumu** bylo stanovení nákladů, které ministerstvům vznikly v souvislosti s naplněním požadavků, jež jsou obsahem vyhlášky č. 82/2018 Sb.

Podpůrné materiály

Pro určované subjekty:

- Proces určování významných informačních systémů

Další užitečné materiály:

- Povinnosti orgánů a osob
- Metodika k varování
- Lhůty pro plnění povinností
- Vodítka pro hodnocení dopadů
- Informace o institutu provozovatele informačního nebo komunikačního systému
- Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost
- Bezpečnostní role
- Požadavky na smlouvy s dodavateli

➢ Ke stažení na www.govcert.cz – sekce „regulace a kontrola“

Děkuji Vám za pozornost!

a.kucinsky@nukib.cz

regulace@nukib.cz

- Zdroje:
  - Varování ze dne 17. 12. 2018
  - Metodika k varování ze dne 17. 12. 2018
  - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
  - Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
  - Podpůrné materiály NÚKIB: https://www.govcert.cz/cs/regulace-a-kontrola/regulace-a-kontrola/
- Zkratky
  - VKB = Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
  - ZKB = Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
  - ZZVZ = zákon o zadávání veřejných zakázek
  - IS = informační systém
  - KS = komunikační systém
  - Varování = Varování NÚKIB ze dne 17. 12. 2018