Varování podle § 12 ZKB
-
použití a dopady

Adam Kučínský
ředitel
odbor regulace

Národní úřad
pro kybernetickou
a informační bezpečnost

Disclaimer

- Prezentace obsahuje informace platné ke dni její realizace, tedy k 16. 4. 2019.
- Informace, fakta a údaje obsažené v prezentaci mají informační a osvětový 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.

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 žádnou povinnost**, a to ani zprostředkovaně. 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**
  - Půjde o technické podmínky stanovené pomocí odkazu na konkrétního dodavatele nebo výrobky (§ 89 odst. 5 ZZVZ, nejpravděpodobněji písm. a)),
  - nikoli o požadavky na osobu dodavatele (vyloučeny jsou technické a programové prostředky, nikoli sám dodavatel, prakticky se ZŘ může účastnit i daná společnost, nicméně nemůže nabídnout vlastní výrobky).
  - V případě, že dodavatel nabídne plnění, které prostředky vyloučených společností obsahuje, pak bude jeho nabídka ze ZŘ vyřazena pro nesplnění zadávacích podmínek (§ 48 odst. 2 ZZVZ).

Děkuji Vám za pozornost

Prostor pro dotazy

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