Metodika řízení rizik kybernetické bezpečnosti IS VaVaI

Metodika definující způsob naplnění vybraných povinnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti v oblasti identifikace, analýzy a řízení rizik informačního systému pro výzkum, vývoj a inovace (IS VaVaI)

Zpracoval: Tomáš Bezouška, garant aktiva IS VaVaI

Schválil: doplnit

Verze: 0.1

Datum: 22. června 2017

Obsah

Seznam zkratek a pojmů

Zkratka	Význam
KB	Kybernetická bezpečnost
ÚV ČR	Úřad vlády České republiky
RVVI	Rada pro vědu, výzkum a inovace, poradní orgán Vlády České republiky
IS VaVaI	Informační systém výzkumu, vývoje a inovací
ZKB	Zákon o kybernetické bezpečnosti
ISMS	Systém řízení bezpečnosti informací
Sb.	Sbírka zákonů České republiky
ČR	Česká republika
VIS	Významný informační systém
NCKB	Národní centrum kybernetické bezpečnosti
RACI	Matice odpovědností
IT	Informační technologie
EU	Evropská unie
ISO	Mezinárodní organizace pro standardizaci
IEC	International Electrotechnical Commission

1 Úvod

1.1 Účel

Tato dokument popisuje metodiku provedení analýzy a řízení rizik. Implementace procesu řízení rizik vychází z požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Dále metodika řízení rizik vychází z vrcholové dokumentace systému řízení kybernetické bezpečnosti, zejména pak z dokumentu **Politika bezpečnosti informací IS VaVaI**.

1.2 Východiska

Pro užití této metodiky organizace samostatně vypracuje a připraví podklady a vstupy pro analýzu rizik, jmenovitě:

- vymezení rozsahu SŘBI,
- dekompozice aktiv,
- hodnocení zranitelností,
- hodnocení hrozeb,
- hodnocení dopadů.

Postupy jsou uvedeny v tomto dokumentu, který dává v několika bodech možnost volby a nastavení systému organizací samotnou. Výsledný způsob (konkrétní metodika přístupu k jednotlivým činnostem) ale musí být jednoznačně dokumentován, aby podle něj mohlo být postupováno a byla umožněna kontrola správného provedení činností.

.

1.3 Dotčení pracovníci

Tento dokument je určen pro Garanta aktiva IS VaVaI, Garanty podpůrných aktiv a další pracovníky podílející se na řízení rizik KB. Zároveň slouží jako podklad pro kontrolu, že řízení rizik KB je realizováno dle odsouhlaseného postupu.

- **Garant aktiva IS VaVaI** (primární role, odpovědná za provedení analýzy rizik, aplikaci stanovených opatření a následné provádění procesu řízení rizik)
- **Garanti podpůrných aktiv** (role dotčená zejména v oblasti provádění analýzy rizik a následně provádění stanovených preventivních a kontingenčních opatření)
- **Manažer kybernetické bezpečnosti** (této role se problematika týká hlavně v oblasti kontroly procesů řízení rizik a začlenění do kontextu řízení rizik ÚV ČR)
- **Další pracovníci** (dalších pracovníků se problematika týká hlavně v oblasti identifikace aktiv)

1.4 RACI matice

Popis činnosti	Role: povinná osoba dle § 3 ZKB (a její statutární orgány)				Role: bezpečnostní role dle §6, VKB						Role: výkonné role		Uživatel dle §2, písm. n) VKB
	správce IS KII dle písm. c)	**správce KS KII** dle písm. d)	**správce VIS** dle písm. e)	**Statutární orgán**	**Výbor pro řízení KB**	**Manažer KB**	**Architekt KB**	**Auditor KB**	Garant aktiv	**Garant primárních aktiv**	**Garant podpůrných aktiv**	**Administrátor** dle §2, písm. o) VKB	
Identifikace a ohodnocení rizik aktiv (vybraných = kterých se týká SŘBI)													
stanoví metodiku pro identifikaci a hodnocení rizik	**n/a**	**n/a**	**√**	**A**	**C, I**	**C, I**	**C, I**			**R**	**I**	**I**	
identifikuje rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k této vyhlášce	**n/a**	**n/a**		**A**	**C, I**	**C, I**	**C, I**			**R**	**C, I**	**C, I**	
identifikuje rizika, při kterých zohlední hrozby a zranitelnosti, posoudí možné dopady na primární aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k této vyhlášce a zpracuje zprávu o hodnocení aktiv a rizik	**n/a**	**n/a**	**√**	**A**	**C, I**	**C, I**	**C, I**			**R**		**I**	
Rozhodnutí o (ne) přijatelnosti rizik													
stanoví metodiku pro stanovení kritérií pro přijatelnost rizik	**n/a**	**n/a**		**A**	**C, I**	**C, I**	**C, I**			**R**	**I**	**I**	
stanoví metodiku pro stanovení kritérií pro přijatelnost rizik	**n/a**	**n/a**	**√**	**A**	**C, I**	**C, I**	**C, I**			**R**	**I**	**I**	
návrh pořadí nebezpečnosti rizik (stanovení finanční nákladovosti eliminace dopadů, dopadů na reputaci, ..)	**n/a**	**n/a**		**A**	**C, I**	**C, I**	**C, I**			**R**	**C, I**	**I**	
určení možných opatření k eliminaci vybraných rizik (pro jednotlivá aktiva), nebo alespoň k jejich potlačení na přijatelnou mez	**n/a**	**n/a**			**C, I**	**C, I**	**R**			**A**	**C, I**	**I**	

Popis činnosti	Role: povinná osoba dle § 3 ZKB (a její statutární orgány)				Role: bezpečnostní role dle §6, VKB						Role: výkonné role		Uživatel dle §2, písm. n) VKB
	správce IS KII dle písm. c)	**správce KS KII** dle písm. d)	**správce VIS** dle písm. e)	**Statutární orgán**	**Výbor pro řízení KB**	**Manažer KB**	**Architekt KB**	**Auditor KB**	Garant aktiv	**Garant přiřazených aktiv**	**Garant podpůrných aktiv**	**Administrátor** dle §2, písm. o) VKB	
ocenění (odhad nákladů na realizaci) a časové náročnosti možných opatření k eliminaci vybraných rizik, nebo alespoň k jejich potlačení na přijatelnou mez	**n/a**	**n/a**	**√**		**C, I**	**C, I**	**R**			**A**	**C, I**	**I**	
v rámci disponibilního rozpočtu a času stanovení návrhu přijatelných rizik (včetně návrhu "ještě přijatelné míry rizika")	**n/a**	**n/a**	**√**	**A**	**R**	**I**	**I**			**C, I**			
určí a schválí přijatelná rizika - včetně stanovení limitu finančních prostředků na eliminaci nepřijatelných rizik	**n/a**	**n/a**		**A**	**R**	**I**	**I**			**C, I**	**I**	**I**	
zpracuje zprávu o hodnocení aktiv a rizik	**n/a**	**n/a**		**A**	**R**	**I**	**C, I**			**C, I**	**C, I**	**I**	
zpracuje zprávu o hodnocení aktiv a rizik	**n/a**	**n/a**	**√**	**A**	**R**	**I**	**C, I**			**C, I**	**C, I**	**I**	

Řízení rizik

Aktualizace analýzy rizik	**n/a**	**n/a**	**√**	**A**	**C, I**	**C, I**	**C, I**			**R**	**I**		
Aplikace preventivních opatření	**n/a**	**n/a**	**√**	**A**	**C, I**	**C, I**	**C, I**			**R**	**I**		
Aplikace kontingenčních opatření	**n/a**	**n/a**	**√**	**A**	**C, I**	**C, I**	**C, I**			**R**	**I**		

Popis činnosti	Role												
	povinná osoba dle § 3 ZKB (a její statutární orgány)				bezpečnostní role dle §6, VKB						výkonné role		Uživatel dle §2, písm. n) VKB
	správce IS KII dle písm. c)	**správce KS KII** dle písm. d)	**správce VIS** dle písm. e)	**Statutární orgán**	**Výbor pro řízení KB**	**Manažer KB**	**Architekt KB**	**Auditor KB**	Garant aktiv	**Garant primárních aktiv**	**Garant podpůrných aktiv**	**Administrátor** dle §2, písm. o) VKB	
Hodnocení účinností opatření	**n/a**	**n/a**	**V**	**A**	**C, I**	**C, I**	**C, I**			**R**	**I**		

Tabulka 1 – RACI matice

2 Navazující dokumenty a výstupy

2.1 Dokumenty

Navazující dokumenty této metodiky jsou následující:

- Identifikace a analýza informačních aktiv
- Zpráva o stanovení kritérií přijatelnosti rizik včetně stanovení přijatelné míry zbytkového rizika
- Analýza rizik

2.2 Související metodiky

Související metodiky jsou následující:

- Metodika identifikace a správy informačních aktiv
- Metodika identifikace a hodnocení rizik
- Metodika stanovení kritérií přijatelnosti rizik

2.3 Výstupy

Na základě této metodiky nevzniknou v organizaci nové dokumenty, pouze bude udržována a aktualizována dokumentace vytvořená v rámci úvodní analýzy rizik:

- **Analýza rizik** pro účely funkcí zajišťujících systém řízení informační bezpečnosti v souladu s požadavky ZKB, ve smyslu příslušných prováděcích předpisů, zejména VKB.
- **Prohlášení o aplikovatelnosti**, které obsahuje přehled vybraných a zavedených bezpečnostních opatření,
- **Plán zvládání rizik**, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.

3 Proces řízení rizik

ÚV ČR vytvoří a bude udržovat systémový přístup k procesům řízení rizik. Cíle řízení rizik v kontextu ÚV ČR jsou následující:

- Zajistit, že řízení rizik je jasně a konzistentně integrované a evidované.
- Rizika jsou řízena v souladu se ZKB, Strategii bezpečností a Metodikami bezpečnosti a s nejlepší praxí.
- Předvídání a odpovědnost za sociální změny, environmentální politiku a legislativní rámec.
- Bere v úvahu dodržování pravidel ochrany zdraví a legislativních požadavků jako minimální standard.
- Bránit škodám a vysokým nákladům na rizika
- Informační politika a provozní rozhodování s pomocí identifikovaných rizik a jejich pravděpodobného dopadu.
- Zajistit nutnost řízení rizik všemi zainteresovanými stranami uvnitř organizace

Tyto cíle budou naplněny následovně:

- Jasně definované role, odpovědnosti a linie reportingu v rámci schválené Politiky a navazující řídící dokumentace.
- Zahrnutí problematiky risk managementu do reportingu a rozhodovacích procesů.
- Udržování a průběžná aktualizace registru rizik.
- Průběžný monitoring a zlepšování.

3.1 Aktualizace analýzy rizik

Revize významných dokumentů v oblasti řízení rizik (viz kapitolu 2) budou vznikat v pravidelných intervalech nejméně jednou ročně, současně se nové hodnocení rizik, aktualizace plánu zvládání rizik i prohlášení o aplikovatelnosti aktualizují po provedení jakéhokoliv rozsáhlejšího zásahu do informačního systému nebo při významné změně vnějších okolností.

3.2 Bezpečnostní opatření

Bezpečnostní opatření jsou základním kamenem řešení kybernetické bezpečnosti a z operačního hlediska i její zdaleka nejdůležitější součástí . Primárním účelem kybernetické bezpečnosti totiž není řešení jednotlivých kybernetických bezpečnostních incidentů ale vytvoření prostředí, v němž jsou kritická informační a komunikační infrastruktura státu a další zájmové informační systémy a sítě preventivně chráněny tak, že pro ně žádná kybernetická bezpečnostní událost nepředstavuje bezpečnostní riziko. ZKB zavádí povinným subjektům pouze základní povinnost mít bezpečnostní opatření v taxativně vymezených kategoriích, přičemž technické podrobnosti upravuje VKB.

Zákon je postaven na dokumentačním modelu, tj. ukládá povinným subjektům povinnost především dokumentovat jednotlivé typy bezpečnostních opatření a následně pak dává právo NBÚ kontrolovat, zda je dokumentace v souladu nejen s konkrétními požadavky zákona a vyhlášky, ale samozřejmě též s aktuální skutečností. Smyslem bezpečnostních opatření je primárně vytvoření takových preventivních mechanismů, které ÚV ČR umožní vyrovnávat se autonomně s kybernetickými bezpečnostními událostmi (ať už jde o prevenci jejich samotného vzniku nebo o nástroje a mechanismy k jejich následnému pokrytí).

3.2.1 Typy bezpečnostních opatření

Z pohledu řízení rizik jsou klíčovým nástrojem především opatření, jejichž smyslem je připravit se na aktivaci možných hrozeb a minimalizovat pravděpodobnost vzniku nepříznivé události, případně minimalizovat její dopady.

Jednou ze dvou hlavních strategií řízení rizika je **aplikace preventivních opatření**, tedy opatření, která jsou realizována v průběhu procesu řízení rizika před jeho aktivací. Za základní strategie v oblasti preventivních opatření lze považovat následující postupy:

- **Minimalizovat pravděpodobnost rizika** přijímáním opatření, která zvyšují odolnost systému vůči identifikovaným hrozbám (např. zvyšování redundance kritických komponent systému ve fail-over režimu);
- **Minimalizovat dopady**, které může nepříznivá situace způsobit (např. vytvářením záloh a jejich uchovávání v off-site lokalitě vč. pravidelného testování DRP procedur).
- **Přenést riziko** na jiný subjekt (např. delegováním vybraných služeb na specializovaný subjekt, nebo pojištěním kritických komponent, systémů či procesů).

Druhou složkou v mixu strategií řízení rizika jsou **opatření kontingenční**, tedy taková, která jsou zaměřena na minimalizaci dopadů v situaci, kdy se hrozba aktivovala a nepříznivá situace se stala skutečností.

3.2.2 Plánování a implementace

Plánování a implementace opatření jsou základními kroky řízení rizika. Po provedení analýzy rizik by alespoň pro skupinu nejvýznamnějších rizik (rizika s největším dopadem a současně největší pravděpodobností výskytu) musí být vypracován Plán zvládání rizik. Tento plán pro každé vybrané riziko navrhne vhodná bezpečnostní opatření, a posoudí náklady a přínosy jednotlivých opatření pro chráněné aktivum a systém jako celek.

Následně po schválení Plánu zvládání rizik jsou realizována jednotlivá preventivní opatření.

3.3 Hodnocení účinností opatření

V rámci navazujících iterací analýzy rizik, prováděných po aplikaci opatření uvedených v Plánu zvládání rizik je vyhodnocení jejich účinnosti, tedy snížení míry rizika, jeho případných negativních dopadů nebo jiných souvisejících jevů. Zjištění z této analýzy pak slouží jako

vstup do další iterace plánování opatření tak, aby posílily funkční strategie eliminace rizika nebo zvládání jeho následků.

4 Nástroje a techniky

V rámci procesu řízení rizik jsou uplatňovány následující nástroje:

- **Evidence aktiv** (případně CMDB)
  Slouží jako nástroj pro evidenci a analýzu aktiv a následně jako východisko pro analýzu a řízení rizik
- **Registr bezpečnostních rizik**
  Slouží jako evidence rizik a jejich parametrů a jako nástroj posouzení závažnosti rizika.
- **Registr bezpečnostních opatření**
  Představuje znalostní bázi známých postupů pro odvracení rizika a eliminaci následků nepříznivých událostí.