Metodika identifikace a správy informačních aktiv IS VaVaI

Metodika definující způsob naplnění vybraných povinnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti v oblasti identifikace a správy informačních aktiv 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

Tento dokument slouží jako návod pro identifikaci a další správu informačních aktiv, a to zejména v kontextu systému řízení bezpečnosti informací IS VaVaI. Dokument popisuje principy, na kterých je identifikace a následně správa aktiv založena, definuje rozsah zapojení a odpovědnost jednotlivých rolí, použité nástroje a postupy.

1.2 Východiska

Identifikace informačních aktiv a jejich následná analýza je základním předpokladem pro možnost efektivního řízení jejích bezpečnosti, ať už v rámci procesů analýzy a následného řízení rizik v kontextu SŘBI, nebo procesů správy informačního systému a informačních technologií v kontextu ITSM.

Informační aktiva jsou řazena v hierarchické struktuře, počínaje samotnými informacemi, přes informační systémy, které data a informace zpracovávají, až po konkrétní technologie a komponenty, které provoz těchto informačních systémů zajišťují. Aby byla identifikace a analýza aktiv informačního systému úplná, je proto nutné široké zapojení celého týmu odborníků ze všech oblastí správy IS/ICT.

1.3 Klasifikace aktiv dle ZKB

V kontextu ZKB jsou rozlišovány tři základní kategorie informačních aktiv:

- **Primárním aktivem** se rozumí informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém
- **Podpůrným aktivem** se rozumí technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému
- **Technickým aktivem** se rozumí specifické podpůrné aktivum – technické vybavení, komunikační prostředky a programové vybavení informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a objekty, ve kterých jsou tyto systémy umístěny

1.3.1 Klasifikace technických aktiv dle typu

Technická aktiva je dále možné členit podle jejich typu, a to následujícím způsobem:

- **Datová aktiva** (databáze a datové soubory, systémy dokumentace, uživatelské příručky, školící materiály, provozní a podpůrné postupy, plány kontinuity obchodní činnosti, přípravná opatření pro návrat do kontrolního bodu)

- **Softwarová aktiva** (aplikační software, systémový software, vývojové nástroje a obslužné programy)
- **Hardwarová aktiva** (počítač a komunikační zařízení, magnetická média – pásky a diskety – odborné technické vybavení, napájecí zdroje, klimatizační jednotky, nábytek apod.
- **Informační služby** (výpočetní a komunikační služby, technické služby – otop, osvětlení, energie, klimatizace)

1.4 Dotčení pracovníci

Tento dokument je určen pro Garanta aktiva IS VaVaI a další pracovníky podílející se na správě aktiv. Zároveň slouží jako podklad pro kontrolu, že Identifikace a analýza informačních aktiv byla realizována dle odsouhlaseného postupu.

- **Garant aktiva IS VaVaI** (primární role, odpovědná za provedení identifikace a analýzy aktiv a za průběžnou aktualizace databáze informačních aktiv nebo CMDB)
- **Garanti podpůrných aktiv** (role odpovědná za detailní popis a správu jednotlivých podpůrných aktiv)
- **Manažer kybernetické bezpečnosti** (této role se problematika týká hlavně v oblasti kontroly procesů správy informačních aktiv)
- **Další pracovníci** (dalších pracovníků se problematika týká hlavně v oblasti identifikace aktiv)

1.5 RACI matice

Popis činnosti	Role: povinná osoba dle § 3 ZKB (a její statutární orgány)				Role: bezpečnostní role dle §6, VKB					Role: výkonné role			
	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	**Uživatel** dle §2, písm. n) VKB
Identifikace aktiv													
Identifikace aktiv	**n/a**	**n/a**	**√**	**A**	**C, I**	**I**	**C, I**			**R**	**I**		
Stanovení vlastnictví aktiv	**n/a**	**n/a**	**√**	**A**	**C, I**	**I**	**C, I**			**R**	**I**		
Klasifikace aktiv													
Klasifikace aktiv	**n/a**	**n/a**	**√**	**A**	**C, I**	**I**	**C, I**			**R**	**I**		

Tabulka 1 – RACI matice

2 Navazující dokumenty a výstupy

Navazující dokumenty této metodiky jsou následující:

- Zpráva o hodnocení rizik – identifikace rizik

2.1 Související metodiky

Související metodiky jsou následující:

- Metodika analýzy rizik
- Metodika stanovení kritérií přijatelnosti rizik

2.2 Výstupy

Na základě této metodiky vzniknou v organizaci následující dokumenty:

- Evidence a klasifikace informační aktiv

3 Identifikace aktiv

U rozsáhlých a složitých informačních systémů hrozí vždy nebezpečí, že při identifikaci aktiv dojde k opomenutí některého aktiva, což může mít za následek, že v konečné fázi nebude nijak chráněno. Prvním krokem při identifikaci aktiv je tedy vymezení hranic a rozsahu zkoumaného informačního systému.

V rámci těchto hranic je následně provedeno systematické rozdělení na jednotlivé komponenty – aktiva.

Během identifikace aktiv je potřeba každé aktivum přesně popsat, jeho identifikaci, umístění, vlastnosti, úlohu v informačním systému a hlavně jeho garanta – vlastníka, osobu plně odpovídající za aktivum, jeho stav, funkčnost, údržbu a bezpečnost.

3.1 Primární aktiva

Jak již je uvedeno výše, Primárním aktivem se rozumí informace nebo služba, kterou zpracovává nebo poskytuje informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém:

- Informace = data (bez ohledu na to, zda jsou uložena centrálně, nebo distribuovaná)
- Služby = funkce, které jednotlivým uživatelům dle jejich přístupových oprávnění umožňují přístup k datům a práci s daty:
    - pořizování
    - ukládání / uchování - včetně tvorby kopií
    - přenos
    - transformace / modifikace (včetně: změn formátu, šifrování a zničení dat)
    - prezentace, a to jak digitální publikování (na webových stránkách, promítání,…), tak tisk.

K identifikaci a posouzení primárních aktiv slouží následující seznam:

- Primární aktivum je logický koncept, který by mělo být možné popsat pomocí podstatných jmen
- Primární aktivum je rozpoznáno/pojmenováno nezávisle na konkrétním systému nebo aplikaci
- Primární aktivum je rozpoznáno/pojmenováno s využitím běžné provozní terminologie organizace
- Primární aktivum je využíváno v rámci hlavních nebo rozhodovacích procesů, případně má životní cyklus
- Primární aktivum je definováno na takové úrovni detailu, že je možné jeho součásti spravovat jako ucelené jednotky
- Referenční informační zdroje nejsou považovány za primární aktiva organizace

- Primární aktivum, které je vyměňováno, přijímáno nebo získáváno externě musí být identifikováno jako aktivum jak v dané organizaci, tak protistraně informační výměny
- Informace obsažené ve dvou oddělených typech obsahu představují dvě samostatná primární aktiva
- Primární aktiva by měla představovat skupiny informací

3.2 Podpůrná aktiva

3.2.1 Technická aktiva

Na základě identifikace primárních aktiv jsou následně promocí analýzy informačního systému a dekompozice jeho jednotlivých částí identifikována podpůrná aktiva, která zajišťují podporu a fungování primárních aktiv.

Pro každé primární aktivum jsou identifikovány následující skupiny technických aktiv:

- **Softwarová aktiva**
  - aplikační software,
  - systémový software,
  - vývojové nástroje,
  - obslužné a podpůrné aplikace a programy.
- **Datová aktiva**
  - databáze a datové soubory,
  - systémy dokumentace, uživatelské příručky, školící materiály, provozní a podpůrné postupy,
  - plány kontinuity obchodní činnosti, plány obnovy po havárii,
  - přípravná opatření pro návrat do kontrolního bodu.
- **Hardwarová aktiva**
  - počítače a komunikační zařízení,
  - magnetická média – pásky a diskety –
  - odborné technické vybavení,
  - napájecí zdroje a klimatizační jednotky,
  - nábytek apod.
- **Informační služby**
  - výpočetní a komunikační služby,
  - technické služby – otop, osvětlení, energie, klimatizace,
  - služby v oblasti bezpečnosti,
  - apod.

3.2.2 Zaměstnanci

V souvislosti s identifikovanými primárními a technickými aktivy jsou pro jednotlivá aktiva identifikováni klíčoví zaměstnanci, kteří jsou bezprostředně zapojeni do správy nebo užívání daného aktiva.

3.2.3 Dodavatelé a partneři

V souvislosti s identifikovanými primárními a technickými aktivy jsou pro jednotlivá aktiva identifikováni klíčoví dodavatelé a obchodní partneři, kteří jsou bezprostředně zapojeni do správy nebo užívání daného aktiva.

3.2.4 Objekty

V souvislosti s identifikovanými primárními a technickými aktivy jsou pro jednotlivá aktiva identifikovány objekty, které jsou bezprostředně spojeny s fyzickým umístěním, správou nebo užíváním daného aktiva.

3.2.5 Procesy

V souvislosti s identifikovanými primárními a technickými aktivy jsou pro jednotlivá aktiva identifikovány procesy, které jsou bezprostředně spojeny se správou a užíváním daného aktiva.

3.3 Identifikace aktiva

Identifikace aktiv je povinností povinného subjektu uloženou mu VKB. Důvodem pro přistoupení k identifikaci aktiv procesem dekompozice je nutnost splnit následující povinnosti:

- hodnocení důležitosti aktiv (VKB, § 4, odst. (2), písm. b)),
- stanovení zda mají či nemají patřit do rozsahu systému řízení bezpečnosti informací (VKB, § 4, odst. (2), písm. b)),
- posouzení možných dopadů identifikovaných rizik (hrozeb a zranitelností) na aktiva (VKB, § 4, odst. (1), písm. c)),
- určení a schválení přijatelných rizik (VKB, § 4, odst. (1), písm. c)),
- stanovení – s ohledem na aktiva (a organizační bezpečnost) rozsahu a hranic systému řízení bezpečnosti informací, ve kterém určí, kterých organizačních částí a technických prvků se systém řízení bezpečnosti informací týká (VKB, § 3, odst. (1), písm. a)),
- určení garantů aktiv, kteří jsou odpovědní za primární aktiva (VKB, § 8, odst. (1), písm. b)) = Garantů primárních aktiv,
- určení garantů aktiv, kteří jsou odpovědní za podpůrná aktiva (VKB, § 8, odst. (3), písm. b)) = Garantů podpůrných aktiv,

3.3.1 Kompetence a odpovědnost za identifikaci aktiv

Na rozhodování o identifikaci aktiv by se kromě Manažera KB a Garantů primárních aktiv jako gestorů, kteří definují bezpečnostní SLA, měli podílet i Architekt KB jako autor celkového konceptu řešení KB organizace, Garanti podpůrných aktiv a Administrátoři jako osoby zajišťující plnění SLA.

3.3.1.1 Přiměřenost dekompozice aktiva

Otázkou je určení nezbytné úrovně dekompozice aktiv pro identifikaci aktiv. Příliš detailní dekompozice by byla nejen pracná, ale i zbytečná. Bez dekompozice aktiv by bezpečnost informací nemusela být prakticky řiditelná.

Řešení otázky se rozpadá do dvou dílčích podmínek, z nichž každá je sama o sobě důvodem pro přistoupení k dekompozici aktiva:

a) je-li složitost aktiva tak vysoká, že řízení bezpečnosti informací není rozumně zvládnutelné; nebo
b) je-li aktivum složeno z natolik různorodých podsystémů, že u nich nelze rozumně řídit bezpečnost informací jednotným způsobem.

3.3.1.2 Nejmenší míra detailu dekompozice aktiva

Rozpad aktiva na podaktiva, tj. dekompozici aktiva (kdy podaktivum je rovněž aktivem), je třeba provádět tak dlouho, dokud bude složitost aktiva z hlediska řízení bezpečnosti informací nepřiměřeně vysoká nebo dokud v jednom aktivu budou zahrnuta vzájemně nesrovnatelná aktiva. Jde tedy o iterativní proces, při kterém lze vymezovaná aktiva uspořádat do stromové struktury.

Účelem procesu dekompozice aktiv je dosáhnout stavu, kdy každý uzel vzniklého stromu bude reprezentovat aktivum, jehož bezpečnost informací je již rozumně řiditelná a současně, jehož obsah je z hlediska řízení bezpečnosti informací druhově konzistentní.

3.3.1.3 Největší míra detailu dekompozice aktiva

Proces rozpadání aktiv může pokračovat i tehdy, jestliže je dosaženo kritéria uvedeného v kapitole Nejmenší míra detailu dekompozice aktiva. Důvodem pro další dekompozici aktiva je zejména míra schopnosti u něj rozumně řídit bezpečnost informací. Tato míra bude posuzována především z hlediska složitosti tohoto aktiva, přičemž v praxi se uplatní některé limity:

- finanční - sledování více aktiv, nebo komplexnějších aktiv, je nákladnější,
- technické - sledování znamená ne jen instalaci více sond, ale i větší zatížení sítě a zejména větší nároky na datová úložiště,
- personální - hlavní otázkou je vyhodnotitelnost shromažďovaných dat jak z hlediska jejich množství, tak z hlediska profesní odbornosti pracovníků,
- organizační – tj. primárně stanovit časové schéma sledování jednotlivých dat. Je třeba stanovit co sledovat stále, co namátkou, co až když je identifikována bezpečnostní událost, co je nutné pro dosledování zdroje incidentu a co pro eliminaci jeho následků a pro zlepšení prevence.

3.3.2 Zastavení procesu rozpadu

Proces rozpadání aktiv je nicméně potřeba zastavit tehdy, jestliže aktivum, tj. uzel vzniklého stromu, je:

a) nejmenší hospodářskou jednotkou z hlediska činnosti organizace, tj. nejmenší jednotkou, vůči které organizace sjednává služby údržby, technické podpory apod., přičemž žádné další aktivum na tomto aktivu již z hlediska bezpečnosti informací nezávisí; nebo

b) dále objektivně nedělitelné.

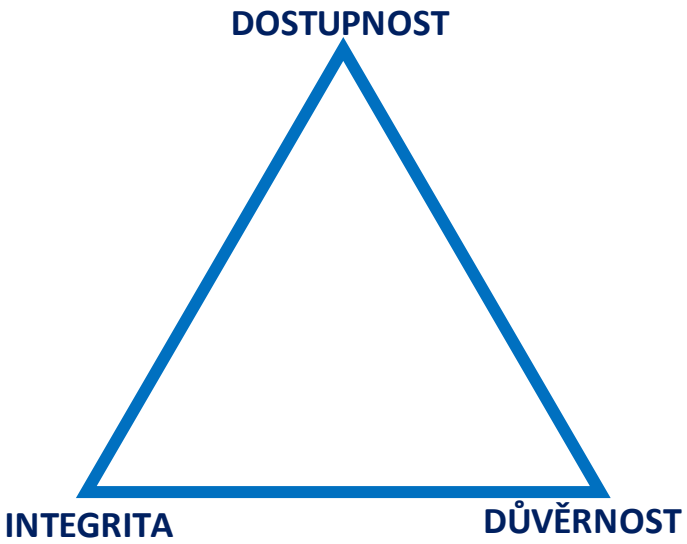
4 Klasifikace aktiv

4.1 Hodnocení aktiv

Hodnocení identifikovaných aktiv provede organizace řízeným a dokumentovaným postupem tak, že vezme výsledky prvního kroku dekompozice aktiv a na tomto rozsahu provede hodnocení pro všechny 3 oblasti (Důvěrnost, Integrita, Dostupnost) ve škále určeného hodnocení.

Toto hodnocení provádějí určení garanti aktiv.

Identifikovaná aktiva budou pro účely řádného postupu v následně prováděné analýze rizik ohodnocena z pohledu jejich významu pro organizaci a jí poskytované služby. U definovaných aktiv, které je potřeba chránit, se musí určit nejdůležitější vrchol z pomyslného trojúhelníku, viz následující obrázek.



Můžeme chtít zajistit všechny vrcholy trojúhelníku na maximální úrovni, ale většinou narazíme na omezené zdroje. Proto je nutné určit, která z vlastností informace je pro organizaci nejdůležitější a té přiřadit nejvyšší prioritu.

Hodnocení bude provedeno na syntetické škále od 1 do 4 bodů, kdy nejzávažnější dopad je hodnocen 4 body, nejméně závažný 1 bodem. Stupnice vychází z přílohy č. 1 VKB, nicméně zařazení aktiva do dané kategorie, stejně jako její detailní popis je na individuálním nastavení organizace.

Při hodnocení důvěrnosti, dostupnosti a integrity na základě finančních aspektů dochází k posouzení finančních dopadů v případech porušení některého z parametrů. Nastavení stupnice od – do je na posouzení organizace. Tato stupnice však musí být poté aplikována na

všechna aktiva organizace jednotně, tzn. že v jedné organizaci bude existovat pouze jedna metodika hodnocení.

Při hodnocení důvěrnosti, dostupnosti a integrity na základě dopadových aspektů dochází k posouzení dopadů na počet obyvatel v případech porušení některého z parametrů. Nastavení stupnice od – do je na posouzení organizace. Tato stupnice však musí být poté aplikována na všechna aktiva organizace jednotně, tzn., že v jedné organizaci bude existovat pouze jedna metodika hodnocení.

4.1.1 Stupnice pro hodnocení důvěrnosti

Úroveň		Popis
1	Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění (např. na základě zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů). Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.
2	Střední	Aktiva nejsou veřejně přístupná a tvoří know-how orgánu a osoby uvedené v § 3 písm. c) až e) zákona, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.
3	Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů).
4	Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. citlivé osobní údaje, data chráněná podle zvláštních předpisů o utajovaných skutečnostech, apod.).

4.1.2 Stupnice pro hodnocení integrity

Úroveň		Popis
1	Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona.
2	Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona a může se projevit méně

Úroveň		Popis
		závažnými dopady na primární aktiva.
3	Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s podstatnými dopady na primární aktiva.
4	Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona s přímými a velmi vážnými dopady na primární aktiva.

4.1.3 Stupnice pro hodnocení dostupnosti

Úroveň		Popis
1	Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2	Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona.
3	Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována jako velmi důležitá.
4	Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona. Aktiva jsou považována jako kritická.

Výsledkem hodnocení aktiv je zápis evidenci aktiv s hodnotami podle jednotlivých oblastí.

4.1.4 Využití časového hlediska pro stanovení úrovně

Níže je uvedena tabulka, dle které je možno zařazovat aktiva do úrovní dle dostupnosti, důvěrnosti a integrity s využitím časového hlediska, které může ovlivňovat finální zařazení. Hodnotí se každé hledisko zvlášť. Jestliže porušení dostupnosti aktiva způsobí uvedené škody (alespoň jednu z nich), pak je dostupnost ohodnocena dle přiřazené hodnoty. Totéž platí pro

důvěrnost a integritu. Hraniční hodnoty uvedené v tabulce jsou příkladem, každá organizace si musí stanovit a průběžně upravovat hranice dle platné legislativy.

Úroveň		Časové hledisko			
		do 8 hodin	**1 den**	**1 týden**	**1 měsíc**
1	nízká	0 mrtvých nebo XY zraněných osob	0 mrtvých nebo XY zraněných osob	0 mrtvých nebo XY zraněných osob	0 mrtvých nebo XY zraněných osob
		hospodářská ztráta <XYZ Kč	hospodářská ztráta <XYZ Kč	hospodářská ztráta <XYZ Kč	hospodářská ztráta >XYZ Kč
		omezení nezbytných služeb/závažný zásah do každodenního života <XYX osob	omezení nezbytných služeb/závažný zásah do každodenního života <XYX osob	omezení nezbytných služeb/závažný zásah do každodenního života <XYX osob	omezení nezbytných služeb/závažný zásah do každodenního života >XYX osob
2	střední	<X mrtvých nebo XY zraněných osob	<X mrtvých nebo XY zraněných osob	>X mrtvých nebo XY zraněných osob	
		hospodářská ztráta <XYZ Kč	hospodářská ztráta <XYZ Kč	hospodářská ztráta >XYZ Kč	
		omezení nezbytných služeb/závažný zásah do každodenního života <XYX osob	omezení nezbytných služeb/závažný zásah do každodenního života <XYX osob	omezení nezbytných služeb/závažný zásah do každodenního života >XYX osob	
3	vysoká	<X mrtvých nebo XY zraněných osob	>X mrtvých nebo XY zraněných osob		
		hospodářská ztráta <XYZ Kč	hospodářská ztráta >XYZ Kč		
		omezení nezbytných služeb/závažný zásah do každodenního života <XYX osob	omezení nezbytných služeb/závažný zásah do každodenního života >XYX osob		
4	kritická	>100 mrtvých nebo 1000 zraněných osob			
		hospodářská ztráta >500 mil. Kč			
		omezení nezbytných služeb/závažný zásah do každodenního života >25000 osob			

4.1.5 Klasifikace aktiv a jejich zahrnutí do systému řízení KB

Z uvedených hodnot pro jednotlivé oblasti se následně vypočítává hodnota aktiva sloužící k jeho klasifikaci. Je stanoven koeficient klasifikace aktiva pro jednotlivá identifikovaná a obodovaná aktiva, který je vypočten podle následujícího vzorce:

$$\mathbf{KKA_{A1} = H_{A1} + K_{A1} + C_{A1}}$$

kde KKA_{A1} .....koeficient klasifikace aktiva pro aktivum A1,
H_{A1} .....hodnocení hodnoty aktiva pro aktivum A1,
K_{A1} .....hodnocení kritičnosti aktiva pro aktivum A1,
C_{A1} .....hodnocení citlivosti aktiva pro aktivum A1.

Výsledky provedené klasifikace jsou zaznamenány do databáze aktiv, a slouží následně pro provedení analýzy rizik.

5 Evidence aktiv

Organizace pro účely řízení systému informační bezpečnosti a plnění povinností vyplývajících z identifikace organizace jako povinné osoby dle ZKB ustaví vlastní registr aktiv, kde provede evidenci hodnocení aktiv, rozdělení na primární a podpůrná aktiva, přidělené garanty a závislosti mezi primárními a podpůrnými aktivy. Doporučení je mít registr aktiv a Analýzu rizik jako jeden dokument shrnující veškeré informace (viz ukázka analýzy rizik v příloze).

5.1 Skupiny aktiv

Aktiva evidovaná v registru aktiv budou uspořádána a seskupena hierarchicky s příslušnými vazbami, a to po skupinách aktiv, jak byly identifikovány při dekompozici směrem dolů, tj. od hlavního aktiva směrem k nejmenšímu identifikovanému detailu.

5.2 Minimální rozsah evidovaných informací

- ID Aktiva
- Název aktiva
- Popis aktiva
- Nadřízené aktivum
- Typ aktiva
- Kategorizace aktiva
- Hodnocení dostupnosti (A)
- Hodnocení důvěrnosti (C)
- Hodnocení integrity (I)
- Celkové hodnocení aktiva
- Garant aktiva
- Lokalizace aktiva
- Datum identifikace aktiva

Registr aktiv bude aktualizován průběžně a opakovaně validován v každé iteraci revize analýzy rizik organizace, jakož i v případě změny podmínek, jež platná analýza ošetřuje.

5.3 Identifikace garantů aktiv

Pro každé identifikované aktivum musí být ustavena odpovědná osoba, kterou ZKB definuje jako fyzickou osobu pověřenou orgánem nebo osobou uvedenou v § 3 písm. c) až e) ZKB k zajištění rozvoje, použití a bezpečnosti aktiva.

VKB stanovuje povinnosti povinných osob, které se dotýkají řízení aktiv. Garant je osobou zařazenou v systému řízení bezpečnosti informací organizace na nejnižším stupni řízení tak, že jeho pravomoci a odpovědnosti jsou vždy vztaženy na konkrétní aktiva, resp. aktivum. Není tedy osobou s pravomocemi na úrovni koncepčního řízení zasahujícího generálně všechna aktiva, popř. generálně všechna aktiva určité kategorie, resp. kategorií.

Povinnosti týkající se aktiv, které jsou ZKB a VKB stanoveny povinným osobám uvedeným v § 3, písm. c) až e) ZKB, směřují k nastavení pravidel pro jejich řízení. Pravidla by měla směřovat k zajištění důvěrnosti, celistvosti a dostupnosti aktiva, samozřejmě rozsahem a způsoby odpovídajícími jeho povaze.

GA by tedy - pro konkrétní systém, měl mít pravomoc a povinnost:

1. zajišťovat dodržování těchto pravidel,
2. vymáhat jejich dodržování,
3. navrhovat úpravy těchto pravidel.

Aktiva jsou dle § 2 písm. b) VKB primární a podpůrná (viz kapitola **Chyba! Nenalezen zdroj odkazů.**).

Aktiva jsou tedy velmi různorodé prvky a obsah pojmů rozvoj, používání a bezpečnost se bude měnit podle jejich podstaty (u technických systémů bude rozvoj znamenat např. aktualizaci systému za účelem zvýšení odolnosti vůči novým bezpečnostním hrozbám, zatímco u osob půjde např. o jejich poučení o nových bezpečnostních hrozbách). Podstatné je, aby pravomoci a povinnosti GA vždy směřovaly k naplnění účelu role GA, tj. k zajištění a udržení potřebné úrovně bezpečnosti daného konkrétního elementárního prvku v běhu času.

Vzhledem k rozdělení aktiv na primární a podpůrná je pro dosažení adresnějšího rozdělení jak kompetencí, tak povinností (zejména ty jsou nezbytným předpokladem i vymahatelnosti plnění) žádoucí použít toto rozdělení i u GA a rozdělit je na:

- **garant primárního aktiva** (dále jen „GpA“)
- **garant podpůrného** (technického) **aktiva** (dále jen „GtA“)

Pak by platilo:

a) pro **garanta primárního aktiva** toto:
   - GpA je fyzická osoba pověřená orgánem nebo osobou uvedenou k zajištění - **VE SMYSLU "NÁVRHU** (= stanovení SLA) **a DOZORU"**, rozvoje, použití a bezpečnosti primárního aktiva.
   - GpA je jeho vlastník z pohledu nikoliv majetkového, ale odpovědnostního. Jedná se o osobu, která je zodpovědná za jeho chod po obsahové stránce. Jedná se tedy např. o správce aplikace.
   - Jeho úkolem je nadefinovat požadavky na zabezpečení primárního aktiva a to jak zabezpečení důvěrnosti, dostupnosti, tak i integrity dat. Ve většině případů je toto řešeno definováním požadavků, které následně řeší garanti podpůrných aktiv.

b) pro **garanta podpůrného aktiva** toto:
   - GtA je fyzická osoba pověřená orgánem nebo osobou uvedenou k zajištění - **VE SMYSLU "REALIZACE** (= plnění SLA)**"**, použití a bezpečnosti technického aktiva.

- GtA tak nejčastěji budou administrátoři, techničtí správci serverů, sítě apod. = osoby odpovědné za chod zařízení s dodržením nastavených parametrů poskytovaných služeb.

Obecně pro garanty aktiv platí, že nedisponují-li k výkonu svých funkcí patřičnými kompetencemi nebo zdroji, vznáší podněty v rámci organizační struktury organizace.

Povinné osoby tedy především musí v organizaci nastavit systém řízení bezpečnosti informací, v rámci kterého vytvoří i sadu pravidel pro řízení aktiv, která přiřadí jednotlivým GA. Pravomoci a povinnosti GA má smysl odvozovat až od těchto pravidel, která budou vycházet z konkrétní faktické situace dané organizace.