Úřad vlády České republiky
Odbor Rady pro výzkum, vývoj a inovace

Metodika identifikace a hodnocení aktiv IS VaVaI

Metodika stanovující 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: kolektiv RELSIE
Schválil: Marek Jan
Verze: 1.0
Datum: 4. prosince 2018

Obsah

1 Úvod

1.1 Účel

Tento dokument slouží jako návod pro identifikaci a správu aktiv 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 a podpůrných aktiv a jejich následná analýza a hodnocení je základním předpokladem pro možnost efektivního řízení jejích bezpečnosti IS VaVaI; ať už v rámci procesů analýzy a následného řízení rizik v kontextu SŘBI, nebo procesů správy informačního systému a informačních technologií v kontextu ITSM.

1.3 Dotčení pracovníci

Tento dokument je určen pro všechny „role“ zainteresované na správě aktiv IS VaVaI, tzn. zejména Garanty aktiv IS VaVaI a další bezpečnostní role.
Poznámka: bezpečnostní role a další role při správě a zajištění bezpečnosti IS VaVaI jsou stanoveny v interním předpisu „Příručka ISMS“.

1.4 Navazující dokumenty a výstupy

Navazující dokumenty této metodiky jsou následující:

- Zpráva o hodnocení rizik – identifikace rizik
- Metodika analýzy rizik a stanovení kritérií přijatelnosti rizik

Na základě této metodiky vzniknou v organizaci následující dokumenty:

- Evidence a hodnocení aktiv informačního systému

1.5 Seznam zkratek

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

2 Aktiva systému

Aktiva systému IS VaVaI jsou identifikována v rámci „rozsahu ISMS“, kde je provedeno rozdělení IS na jednotlivé komponenty, tj. aktiva.
Poznámka – při identifikaci aktiv je potřeba každé aktivum přesně popsat (=identifikovat), včetně jeho umístění, vlastností, úlohu v informačním systému a následně též určit jeho garanta (tj. osobu plně odpovídající za aktivum, jeho stav, funkčnost, údržbu a bezpečnost).
Přehled aktiva IS VaVaI je veden v „**Registru aktiv“** IS VaVaI, viz níže.

2.1 Základní klasifikace aktiv

Základní kategorie aktiv z pohledu řízení bezpečnosti, resp. kybernetické bezpečnosti[1] informačního systému je následující:

- **Primární aktivum** – někdy též „informační aktivum“ , rozumí informace nebo služba, kterou zpracovává nebo poskytuje informační systém;
- **Podpůrné aktivum** – rozumí se tím: technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému;
- **Technické aktivum** – rozumí se specifické podpůrné aktivum, kterým je technické vybavení, komunikační prostředky a programové vybavení informačního systému a objekty; kterých jsou tyto systémy umístěny.

2.2 Primární aktiva

Primárním aktivem se rozumí informace nebo služba, kterou zpracovává nebo poskytuje IS VaVaI, tzn.:

- 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, jako je:
    - 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.

Metodická pomůcka k identifikaci primárních aktiv:

- 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.

2.3 Podpůrná – technická aktiva

Podpůrná – technická aktiva jsou určena (identifikována) pomocí analýzy informačního systému a dekompozice jeho jednotlivých částí, které zajišťují podporu pro činnost systému, resp. provádění potřebných činností s primárními aktivy v informačním systému.
Ve vztahu k primárním aktivům jsou identifikována technická aktiva, resp. následující skupiny technických aktiv:

- Datová aktiva (databáze a datové soubory, systémová dokumentace a příručky, provozní postupy, plány kontinuity činnosti systému, …

[1] Viz vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

- **Softwarová aktiva (**aplikační SW, systémový SW, vývojové nástroje, obslužné a podpůrné aplikace a programy).
- **Hardwarová aktiva** (počítače a komunikační zařízení, magnetická média, odborné technické vybavení, napájecí zdroje a klimatizační jednotky, ostatní zařízení apod.).
- **Podpůrné služby** (výpočetní a komunikační služby, technické služby – otop, osvětlení, energie, klimatizace, služby v oblasti bezpečnosti apod.).

2.4 Podpůrná aktiva

Podpůrná aktiva (mimo technická aktiva) patří:

- **Zaměstnanci** – v návaznosti na primární a technická aktiva jsou identifikováni klíčoví zaměstnanci, kteří jsou bezprostředně zapojeni do správy nebo užívání daného aktiva.
- **Dodavatelé a partneři** – v návaznosti na primární a technická aktiva jsou identifikováni klíčoví dodavatelé (resp. obchodní partneři), kteří jsou bezprostředně zapojeni do správy nebo užívání daného aktiva.
- **Objekty** – v návaznosti na primární a technická aktiva jsou identifikovány objekty (resp. další prostory), které jsou bezprostředně spojeny s fyzickým umístěním, správou nebo užíváním daného aktiva.
- **Procesy** – v návaznosti na primární a technická aktivy jsou identifikovány procesy, které jsou bezprostředně spojeny se správou a užíváním daného aktiva.

2.5 Identifikace aktiv

Dekompozicí systému IS VaVaI a využívané ICT infrastruktury jsou identifikována jednotlivá aktiva a jsou určovány závislosti mezi primárními a podpůrnými aktivy IS VaVaI. Úroveň dekompozice systému na jednotlivá aktiva (resp. skupiny aktiv) musí přinést výsledek (tzn. přehled aktiv a jejich závislostí), který lze využít v rámci řízení bezpečnosti systému.

Základem při identifikaci aktiv je stanovení vhodné míry „úrovně dekompozice“ aktiv systému. V této problematice je potřebné vycházet z architektury použitých ICT technologií, z rozsahu systému a z potřeb řízení bezpečnosti informací v daném systému.

Poznámka – příliš detailní dekompozice by byla nejen pracná, ale i zbytečná, neboť ve svém důsledku neumožní praktické řízení bezpečnosti systému.

Na identifikaci aktiv by se kromě Manažera KB IS VaVaI a Garantů primárních aktiv jako gestorů, kteří definují bezpečnostní SLA, měli podílet též Architekt KB IS VaVaI (jako autor celkového konceptu řešení KB systému) a dále Administrátoři jako osoby zajišťující plnění SLA.

2.5.1 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.

2.5.2 Největší míra detailu dekompozice aktiva

Proces rozpadání aktiv může pokračovat i tehdy, jestliže je dosaženo kritéria uvedeného v předchozí kapitole. 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 nejen 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.

2.5.3 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.

3 Metodika hodnocení aktiv

3.1 Hodnocení aktiv

Hodnocení důležitosti primárních aktiv se provede řízeným a dokumentovaným postupem tak, že jsou hodnoceny požadavky na zajištění důvěrnosti, integrity a dostupnosti identifikovaných aktiv, a to zařazením do jednotlivých úrovní 1–4 hodnotící stupnice (viz tabulky níže).

Poznámka: aktiva jsou hodnocena z pohledu jejich významu pro organizaci a souvisejících poskytovaných služeb v IS VaVaI. Je posuzován „jaký dopad“ by mělo porušení bezpečnosti u jednotlivých aktiv. Lze provádět hodnocení na základě „finančních aspektů“ (=finanční dopad) a též „dopadových aspektů“ (dopad na obyvatelstvo).

Výsledky hodnocení aktiv jsou uchovávány v evidenci aktiv systému – s hodnotami podle jednotlivých oblastí bezpečnosti. Hodnocení aktiv provádí provádějí určení pracovníci.
Pro hodnocení primárních aktiv jsou využity stupnice dle vyhlášky č.82/2018 Sb., příloha č.1.

3.1.1 Stupnice pro hodnocení důvěrnosti

Úroveň		Popis	Požadavky na ochranu aktiva
1	**Nízká**	Aktiva jsou veřejně přístupná nebo jsou určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy Správce systému	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká
2	**Střední**	Aktiva nejsou veřejně přístupná a tvoří know-how Správce systému, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední
3	**Vysoká**	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství, osobní údaje).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Vysoká
4	**Kritická**	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (např. zvláštní kategorie osobní údaje).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Kritická

3.1.2 Stupnice pro hodnocení integrity

Úroveň		Popis	Požadavky na ochranu aktiva
1	Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy Správce systému	Není vyžadována žádná ochrana.
2	Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů Správce systému a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).
3	Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů Správce systému s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
4	Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů Správce systému s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

3.1.3 Stupnice pro hodnocení dostupnosti

Úroveň		Popis	Požadavky na ochranu aktiva
1	Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
2	Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení zájmů Správce systému	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
3	Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů Správce systému Aktiva jsou považována jako velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
4	Kritická	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení zájmů Správce systému. Aktiva jsou považována jako kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

3.1.4 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			

3.1.5 Hodnocení aktiv a jejich zahrnutí do systému řízení KB

Z uvedených hodnot pro jednotlivé oblasti se následně vypočítává hodnota aktiva sloužící k stanovení koeficientu jejich důležitosti, který je vypočten podle následujícího vzorce:

$$\mathbf{KHA_{A(1)} = Dů_{A(1)} \times Do_{A(1)} \times In_{A(1)}}$$

kde $KHA_{(A1)}$ .....koeficient hodnoty aktiva (pro aktivum A1),
$Dů_{(A1)}$ .....hodnocení požadavků na Důvěrnost aktiva (pro aktivum A1),
$Do_{(A1)}$ .....hodnocení požadavku na Dostupnost aktiva (pro aktivum A1),
$In_{(A1)}$ .....hodnocení požadavků na Integritu aktiva (pro aktivum A1).

Výsledky provedené klasifikace jsou zaznamenány do databáze aktiv a jsou využity při provedení analýzy rizik.

4 Evidence aktiv

Pro potřeby řízení bezpečnosti informací IS VaVaI je veden „**registr aktiv**“, obsahující všechna identifikovaná primární a podpůrná (technická) aktiva a závislosti mezi jednotlivými aktivy. U každého aktiva je uveden garant daného aktiva.

Rozsah evidovaných informací v registru aktiv:

- 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 je periodicky aktualizován a opakovaně validován při každé revizi analýzy rizik systému; případně při závažné změny systému.

Skupiny aktiv

Aktiva evidovaná v registru aktiv jsou 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 Identifikace/určení garantů aktiv

Garant aktiva je bezpečnostní role (osoba) odpovědná za zajištění rozvoje, použití a bezpečnost daného aktiva. Pro každé identifikované aktivum musí být ustavena odpovědná osoba = garant aktiva, tzn. dle typu aktiva buď

- „Garant primárního aktiva“ (GpA), anebo
- „Garant podpůrného aktiva“ resp. Garant technického aktiva“ (GtA).

Metodická poznámka:

Garant primárního aktiva (GpA):

- GpA je fyzická osoba pověřená 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. Je zodpovědný za správné zpracování aktiva. Jedná se tedy např. o správce aplikace.
- Jeho úkolem je nadefinovat požadavky na zabezpečení primárního aktiva (důvěrnosti, dostupnosti, integrity). Ve většině případů jsou tyto požadavky následně řešeny garanty podpůrných (technických) aktiv.

Garant podpůrného aktiva (GtA):

- GtA je fyzická osoba pověřená k zajištění – VE **SMYSLU "REALIZACE** (= plnění SLA)**"**, způsobu 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 pokud nedisponují k výkonu role garanta patřičnými kompetencemi nebo zdroji, vznáší podněty v rámci organizační struktury organizace. Povinnosti garantů aktiv jsou definovány ve směrnici systému řízení bezpečnosti informací, v rámci, které jsou též stanovena pravidla pro řízení aktiv.