PRŮVODCE ŘÍZENÍM AKTIV A RIZIK DLE VYHLÁŠKY O KYBERNETICKÉ BEZPEČNOSTI

Obsah

1 Úvod

Zajištění kybernetické bezpečnosti (dále jen „KB“) je nelehký úkol, na kterém se musí podílet celá řada organizačních celků a odpovědných osob. Jednotlivé procesy zaměřené na zvýšení KB musí být integrovány a formálně zakotveny do běžných procesů organizace. Aktivní podpora a zapojení vedení organizace je zcela klíčové, např. zajištění potřebných zdrojů, odpovědnost vedení, prosazování neustálého zlepšování atd., stejně tak jako zapojení dalších relevantních osob, mezi které kromě bezpečnostních rolí a zaměstnanců IT, patří často pověřenec pro ochranu osobních údajů (dále jen „DPO“), právní oddělení (především v oblasti výběrových řízení), personální oddělení (především v oblasti vzdělávání), bezpečnostní oddělení (především u fyzické bezpečnosti), oddělení krizového řízení (především v oblasti řízení kontinuity činností), interní audit, věcná oddělení, která vykonávají agendy za použití informačních a komunikačních systémů (dále jen „IS“) spadajících pod zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále také „ZKB“) apod.

ZKB a vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VKB“), které požadují zavedení systému řízení bezpečnosti informací (dále jen „ISMS“, zkratka z anglického „Information Security Management System“), stojí především na přístupu založeném na posuzování rizik (známý také jako „risk-based approach“) a kontinuálním zlepšování.

Tento podpůrný materiál byl vytvořen proto, aby přiblížil problematiku řízení aktiv a rizik dle VKB především těm, kteří s ní nemají žádné nebo minimální zkušenosti. Zkušenější manažeři KB (nebo jiné osoby odpovědné za řízení aktiv a rizik) mohou podpůrný materiál využít jako zdroj inspirace pro vylepšení již zavedených postupů.

Metody popsané v tomto podpůrném materiálu je nutné přizpůsobit potřebám organizace.

Podpůrný materiál vychází z VKB, ale je doplněn o řadu zkušeností s prováděním hodnocení rizik v praxi a většina uvedených informací představuje „good practice“. **Jedná se tedy o rozšíření VKB.**

Dokument obsahuje části teoretické, praktické a modelové příklady. V teoretické části jsou rozebírána jednotlivá ustanovení VKB, praktická část obecně popisuje, jak požadavky plynoucí z těchto ustanovení naplnit a modelový příklad obsahuje konkrétní aplikace obecných postupů v prostředí fiktivního Ministerstva pro certifikaci senzorů.

Účelem tohoto dokumentu není představit jediný správný postup řízení aktiv a rizik v souladu s VKB ale představit základní principy, které je nutné přizpůsobit prostředí organizace. Jedná se tedy o doporučení, které není vymahatelné podle ZKB a VKB. Všechny modelové příklady představují pouze jednu z možných variant naplnění požadavků VKB.

Řízení aktiv a rizik je jedna ze základních povinností daná VKB. Bez znalosti toho, jaká má organizace aktiva a jaká rizika ji ohrožují nelze efektivně plnit většinu dalších povinností daných VKB. Řízením aktiv organizace zjistí, co je pro ni důležité a co musí chránit. Řízením rizik organizace zjistí, jakým způsobem je potřeba aktiva chránit, tedy jaká bezpečnostní opatření je nutné zavést a dále prioritizuje zavádění těchto bezpečnostních opatření.

Kvůli názornosti byl pro modelový příklad zvolen informační systém kritické informační infrastruktury (dále jen „KII“), na kterém budou demonstrovány postupy pro řízení aktiv a rizik. Stejné povinnosti platí také pro informační systémy základní služby (dále jen „ISZS“). V případě využití tohoto materiálu pro

významné informační systémy (dále jen „VIS“) nebo pro informační systémy, které nespadají pod ZKB je **vhodné zavádět postupy přiměřeně.**

Ke zvýšení přehlednosti dokumentu byly využívány symboly označující Modelový příklad (části týkající se Ministerstva pro certifikaci senzorů), Tip a Upozornění.

Tabulka 1: Symboly

Symbol	Popis
	Modelový příklad
	Tip
	Upozornění

1.1 Jak pracovat s podpůrným materiálem

Všechny přílohy tohoto podpůrného materiálu slouží pouze jako inspirace a při jejich použití je nutné je upravit pro potřeby konkrétní organizace.

Jedná se pouze o ukázky sloužící pro pochopení principů vysvětlovaných v rámci tohoto podpůrného materiálu. Skutečnosti uvedené v přílohách slouží pouze jako příklady, nejedná se tedy o jejich kompletní výčet, např. katalogy aktiv nebo hodnocení rizik provedené v jednotlivých organizacích budou obsahovat až násobně větší množství položek, než je uvedeno v tomto ukázkovém materiálu modelové organizace.

Pro snazší pochopení jsou postupy doplněny konkrétními příklady v rámci smyšleného IS. Jedno hodnocení rizik však nemusí (a někdy to ani nelze) být provedeno nad aktivy pouze jednoho IS. Z pohledu VKB je rozhodující služba, kterou daný systém poskytuje, resp. jeho účel, např. IS podporující výrobu elektřiny, IS podporující provoz letecké dopravy, IS podporující službu přepravy ropy ropovodem, IS podporující bankovní služby, IS k zajištění elektronické pošty atd[1]. V jednom hodnocení rizik tak mohou být sloučena aktiva více IS nebo aktiva celé organizace. Naopak u větších organizací může být provedeno několik hodnocení rizik, které jsou rozděleny do logických celků, např. sdílená infrastruktura, jednotlivé aplikace atd.

1.1.1 Příloha 1: Vzorová politika systému řízení bezpečnosti informací

Tento dokument obsahuje politiku systému řízení bezpečnosti informací fiktivního Ministerstva pro certifikaci senzorů. V dokumentu lze nalézt:

[1] Více informací lze nalézt v podpůrném materiálu na webových stránkách NÚKIB: Pravidla určování KII https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/ případně ve vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby nebo ve vyhlášce č. 360/2020 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.

- cíle, principy a potřeby řízení bezpečnosti informací,
- rozsah a hranice systému řízení bezpečnosti informací,
- pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací,
- pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

1.1.2 Příloha 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik

Tento dokument obsahuje metodiku pro identifikaci a hodnocení aktiv a hodnocení rizik Ministerstva pro certifikaci senzorů včetně kritérií pro akceptovatelnost a postupu pro zvládání výjimek.

1.1.3 Příloha 3: Zjednodušená dopadová tabulka

Tento dokument obsahuje zjednodušenou dopadovou tabulku, která byla vytvořena za účelem zrychlení procesu hodnocení primárních aktiv. Více viz kapitola 4.1.4 Hodnocení primárních aktiv.

1.1.4 Příloha 4: Struktura podpůrných aktiv

Tento dokument obsahuje strukturu podpůrných aktiv, která může sloužit jako inspirace při identifikaci podpůrných aktiv viz kapitola 4.2.1.

1.1.5 Příloha 5: Vzorová pravidla ochrany jednotlivých úrovní aktiv

Tento dokument obsahuje pravidla ochrany jednotlivých úrovní aktiv fiktivního Ministerstva pro certifikaci senzorů. V dokumentu lze nalézt:

- pravidla pro klasifikaci informací,
- pravidla pro nakládání s aktivy,
- pravidla pro ochranu integrity,
- pravidla pro ochranu dostupnosti,
- pravidla pro likvidaci dat.

1.1.6 Příloha 6: Vzorové hodnocení aktiv a rizik

Tento dokument obsahuje evidenci primárních i podpůrných aktiv fiktivního Ministerstva pro certifikaci senzorů, včetně jejich vazeb a hodnocení. Dále je zde obsažen katalog zranitelností, katalog hrozeb a katalog rizik.

1.1.7 Příloha 7: Vzorové prohlášení o aplikovatelnosti[2]

Tento dokument obsahuje prohlášení o aplikovatelnosti Ministerstva pro certifikaci senzorů, který je jedním z **klíčových dokumentů** požadovaných VKB.

1.1.8 Příloha 8: Vzorový plán zvládání rizik

Tento dokument obsahuje plán zvládání rizik Ministerstva pro certifikaci senzorů, který je jedním z **klíčových dokumentů** požadovaných VKB.

[2] Vzorové Prohlášení o aplikovatelnosti obsahuje odkazy na další vzorové dokumenty, které byly pro Ministerstvo pro certifikaci senzorů vytvořeny, ale také na další dokumentaci, která je mimo rozsah tohoto podpůrného materiálu a nebyla vytvořena. Odkazy na ni byly použity pouze pro dokreslení ukázky vzorového Prohlášení o aplikovatelnosti.

1.1.9 Příloha 9: Vzorová zpráva o hodnocení rizik

Tento dokument obsahuje zprávu o hodnocení rizik, která slouží ke krátkému shrnutí procesu hodnocení aktiv a rizik. V případě fiktivní organizace slouží jako podklad pro Výbor KB.

1.1.10 Příloha 10: Vzorové hodnocení rizik pro veřejnou zakázku

Ministerstvo pro certifikaci senzorů se rozhodlo nakoupit nová aktiva a vzhledem k tomu, že se musí řídit zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, bude postupovat prostřednictvím veřejné zakázky. Pro plnění povinností VKB a tyto účely vypracovalo hodnocení rizik, které je obsahem tohoto dokumentu.

1.1.11 Příloha 11: Vzorová zpráva o hodnocení rizik pro veřejnou zakázku

Tento dokument obsahuje zprávu o hodnocení rizik fiktivního Ministerstva pro certifikaci senzorů, která slouží ke krátkému shrnutí procesu hodnocení aktiv a rizik aplikovanému na aktiva, která budou předmětem veřejné zakázky.

1.1.12 Příloha 12: Vzorové alternativní hodnocení rizik u primárních aktiv

Tento podpůrný materiál v kapitole 5.13 popisuje alternativu pro proces hodnocení rizik. Samotné alternativní hodnocení rizik je pak obsahem Přílohy 12: Vzorové alternativní hodnocení rizik u primárních aktiv.

1.1.13 Příloha 13: Vzorový plán zvládání rizik alternativního hodnocení

Tento dokument obsahuje plán zvládání rizik Ministerstva pro certifikaci senzorů, který navazuje na alternativní hodnocení rizik u primárních aktiv.

1.1.14 Příloha 14: Zkratky a používané pojmy

Tento dokument obsahuje seznam zkratek a používaných pojmů, které se vyskytují v rámci podpůrného materiálu.

1.2 Metoda popsaná v tomto materiálu

Metoda popsaná v tomto podpůrném materiálu patří mezi kvalitativní metody. Hodnocení je prováděno podle předem stanovených stupnic expertním odhadem. Kromě kvalitativních metod se používají také metody kvantitativní, které využívají přesné číselné ohodnocení, např. ve finančních jednotkách. Kvantitativní metody bývají zpravidla náročnější na provedení, ale umožňují snazší porovnání hodnot rizik s náklady na zavádění bezpečnostních opatření.

1.2.1 Výhody popsané metody

+ Univerzální metodika
+ Nižší náklady při použití nástroje MS Excel pro provedení hodnocení rizik u malých organizací
+ Soulad s ZKB a VKB
+ Komplexnost
+ Srozumitelnost a přehlednost

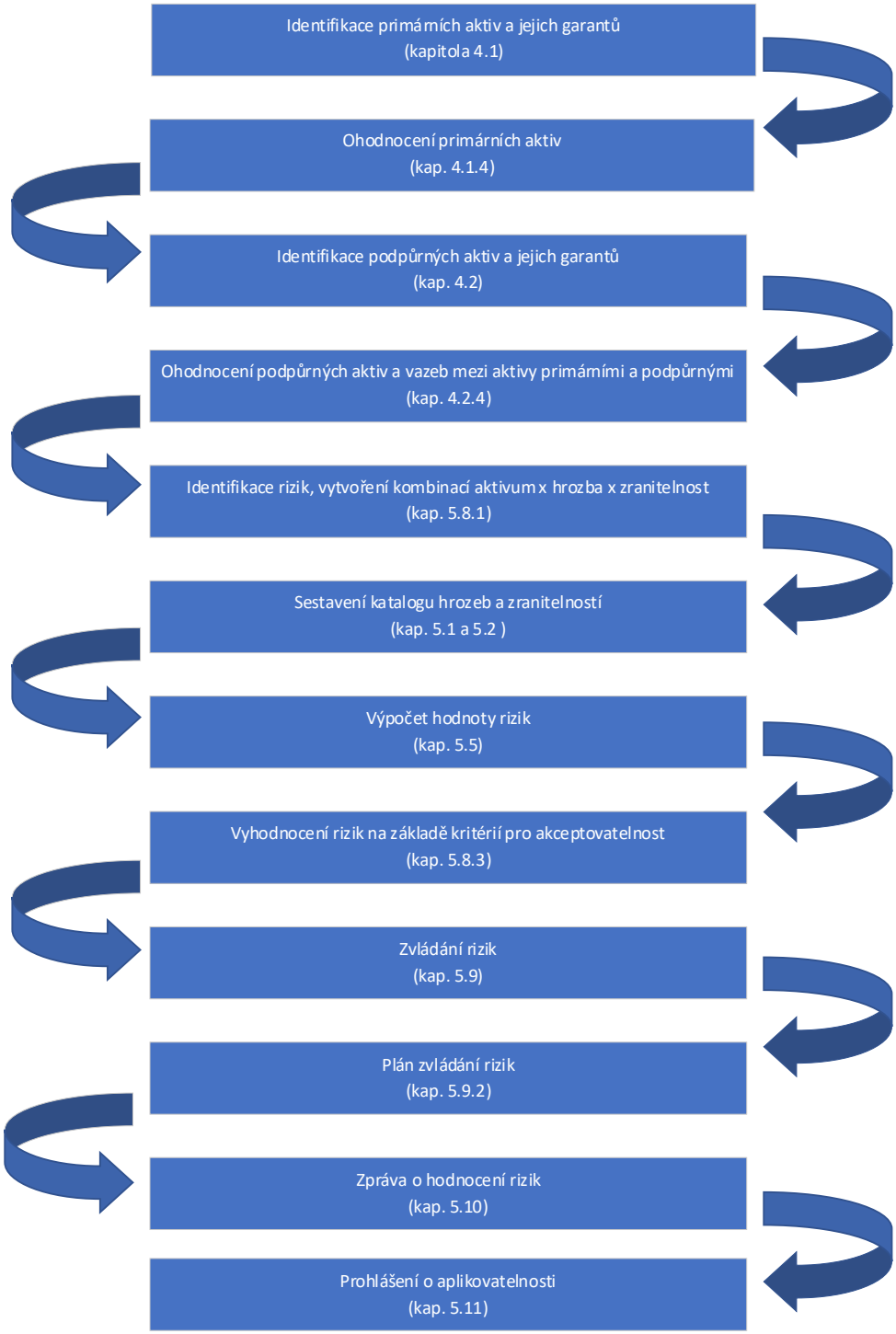
1.2.2 Nevýhody popsané metody

- Nutnost upravit si dle požadavků organizace

- Vyšší náročnost při použití nástroje MS Excel pro provedení hodnocení rizik u větších organizací
- Časová náročnost provedení procesu a seznámení se s metodou

1.3 Stručný přehled procesu řízení aktiv a rizik

Obrázek 1: Stručný přehled procesu řízení aktiv a rizik



Před zahájením je nutné mít zpracovanou metodiku pro hodnocení aktiv a řízení rizik, na základě které bude celý proces proveden. V metodice jsou uvedeny základní informace, jako je zvolená metoda, která bude použita, stupnice pro hodnocení aktiv i rizik, výpočet pro získání hodnot rizik apod., se kterými se následně v rámci celého procesu pracuje.

V průběhu hodnocení aktiv a následně při identifikaci a ohodnocení hrozeb a zranitelností je vyžadována součinnost garantů.

Výstupem z celého procesu je vytvoření **zprávy o hodnocení rizik,** která popisuje výsledky procesu, a také **prohlášení o aplikovatelnosti,** ve kterém je popsáno, která opatření stanovená VKB byla aplikována, v jakém rozsahu a která nebyla a z jakého důvodu. Stěžejním dokumentem je také **plán zvládání rizik**, který popisuje bezpečnostní opatření pro zvládání jednotlivých rizik.

Problematika řízení aktiv v oblasti KB je řešena v kapitole 4 tohoto podpůrného materiálu a problematice řízení rizik se věnuje kapitola č. 5.

Dokumentované informace:

- Metodika pro hodnocení aktiv a řízení rizik
- Seznam primárních a podpůrných aktiv včetně jejich garantů
- Seznam vazeb mezi primárními a podpůrnými aktivy
- Katalog hrozeb a zranitelností
- Seznam identifikovaných rizik
- Zpráva o hodnocení rizik
- Prohlášení o aplikovatelnosti
- Plán zvládání rizik

1.4 Představení modelové organizace

Pro představení postupů popsaných v tomto dokumentu na konkrétních příkladech bylo smyšleno Ministerstvo pro certifikaci senzorů (dále také označováno jen jako „ministerstvo“).

Ministerstvo ověřuje, zda předložené senzory splňují všechny požadavky na ně kladené a vyhovujícím zařízením uděluje 3letou certifikaci. Kromě kontroly dokumentace provádí také testování předložených senzorů ve vlastní laboratoři. Ministerstvo je jediným orgánem provádějícím certifikaci senzorů na území státu a příslušné subjekty mají povinnost používat pouze certifikovaná zařízení. Ministerstvo vede neveřejnou detailní evidenci informací o všech senzorech, které byly k certifikaci předloženy. Současně má na svých webových stránkách veřejně dostupný seznam certifikovaných senzorů. Ministerstvo má celkem 2 000 zaměstnanců.

Proces certifikace je zpracován v IS pro evidenci a zpracování procesu certifikace senzorů (dále také jako „agendový systém“). Tento IS byl určen jako prvek KII. Výrobci mohou žádosti o certifikace podávat prostřednictvím webové aplikace ministerstva, která je součástí tohoto IS a slouží pro externí uživatele, je ale nutná předchozí registrace. Veškerou dokumentaci potřebnou pro proces certifikace výrobci nahrávají do aplikace ve formátu pdf. Ministerstvo má lhůtu 30 dní, aby na podanou žádost reagovalo. S IS pracuje 1 400 interních uživatelů ministerstva a 300 externích uživatelů.

Webová aplikace slouží výrobcům k podávání žádostí o certifikaci senzorů. Žádost obsahuje formulář, jehož přílohou je technická dokumentace senzoru. Zároveň prostřednictvím této aplikace výrobce daný senzor registruje na laboratorní testy a zajistí jeho fyzické doručení na ministerstvo. IS slouží jako podpůrný nástroj zaměstnancům ministerstva, kteří jsou odpovědní za proces certifikace včetně jeho zdokumentování. Průběh jednotlivých kroků procesu je logován. IS také hlídá dodržování zákonných

lhůt. Webová aplikace slouží široké veřejnosti k zobrazení informací o tom, které senzory byly ministerstvem certifikovány. Certifikáty jsou automaticky po 3 letech zrušeny a senzory odebrány z veřejného seznamu certifikovaných zařízení.

IS je vyvíjen dodavatelskou firmou.

Ministerstvo má tyto dodavatele:

Dodavatel A

Dodavatel A dodává IS pro evidenci a zpracování procesu certifikace senzorů. IS je nasazen v provozním prostředí ministerstva, ale testovací a vývojové prostředí je u dodavatele. S dodavatelem byla uzavřena smlouva o dílo a servisní smlouva. Servisní smlouva obsahuje podporu ze strany dodavatele na 5 let, opravu chyb, vývoj nových funkcionalit a službu next business day. Dodavatel má vzdálený přístup do IS, provádí provozní monitoring a sběr logů. Komunikace s dodavatelem probíhá prostřednictvím ticketovacího nástroje – Helpdesku. Součástí dodávky je vývojová, testovací a provozní dokumentace a školící materiály pro uživatele. Školení pro práci s IS absolvují pouze vybraní klíčoví uživatelé, kteří následně musí proškolit ostatní. Školení proběhlo jednorázově při nasazení IS do provozu. Dodavatel A je informován o tom, že je provozovatelem IS určeného jako KII a zároveň významným dodavatelem ministerstva. Dodavatel může do IS aktivně zasahovat, např. může nasadit nové patche, provádět konfiguraci atd. Zdrojové kódy jsou ukládány do verzovacího nástroje u dodavatele.

Dodavatel B

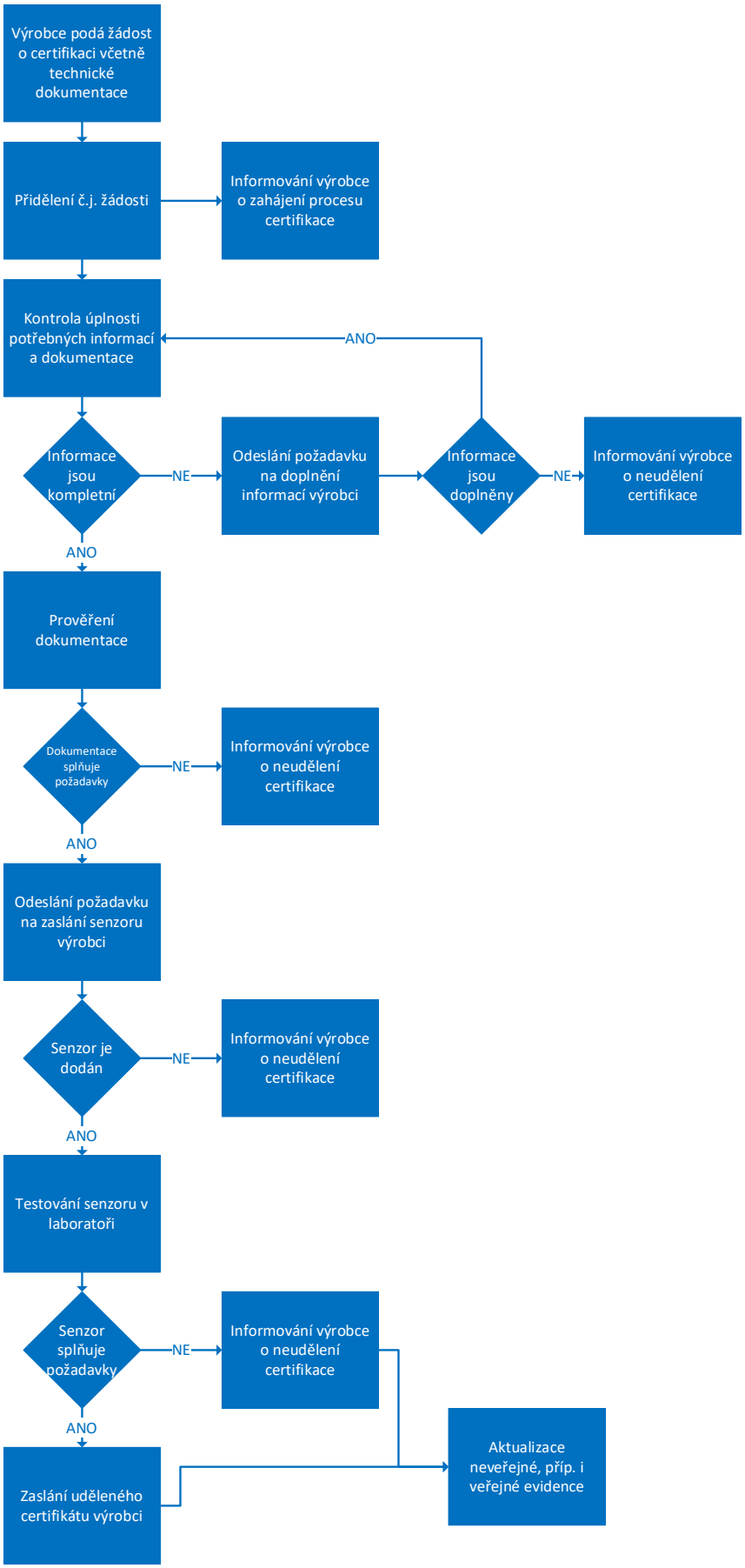
Dodavatel B dodává ministerstvu hardware (dále jen „HW“) včetně operačního systému (dále jen „OS“) a instalace. Součástí dodávky je servisní smlouva zajišťující podporu ze strany dodavatele na 5 let na životnost HW a službu next business day. Dodavatel provádí vzdálený provozní monitoring. Komunikace s dodavatelem probíhá prostřednictvím ticketovacího nástroje – Helpdesku. Dodavatel B je informován o tom, že je provozovatelem IS určeného jako KII a zároveň významným dodavatelem ministerstva. Dodavatel má vzdálený přístup, může aktivně zasahovat do IS a provádí pravidelnou údržbu a opravy technického vybavení.

Dodavatel C

Dodavatel C dodává ministerstvu aktivní a bezpečnostní prvky (např. switche a firewally) a provádí monitoring. Dodavatel C nemůže do sítě aktivně zasahovat. Dodavatel C se smluvně zavázal na 5 let, konkrétně vydávat aktualizace na tyto prvky a v případě poruchy zařízení je povinen ho vyměnit nebo opravit. Komunikace s dodavatelem probíhá prostřednictvím ticketovacího nástroje – Helpdesk. Dodavatel C byl informován o tom, že je významným dodavatelem ministerstva.

Proces certifikace:

Následující diagram zjednodušeně popisuje proces certifikace:



Obrázek 2: Přehled procesu certifikace

Popis jednotlivých úseků[3]:

Odbor kabinet ministra:

- Zajištění komunikace s veřejností a organizace agendy ministra
- Komunikace s ostatními ministerstvy a ostatními orgány státní správy, koordinace a realizace pravomocí ministerstva v legislativním procesu, poskytování výkladových stanovisek
- Rozvíjení mezinárodní spolupráce v oblasti působnosti ministerstva, navazování, udržování a rozvíjení kontaktů se zahraničními partnery, shromažďování a zpracovávání informací s cílem jejich optimálního využití v rámci ministerstva

Odbor interního auditu:

- Zajištění výkonu interního auditu v různých oblastech (finanční, kybernetické bezpečnosti, fyzické bezpečnosti atd.)
    - Spadá sem role auditora kybernetické bezpečnosti

Pověřenec pro ochranu osobních údajů (DPO):

- Poskytování informací a poradenství správci či zpracovateli osobních údajů, včetně zaměstnanců, kteří se na zpracování osobních údajů podílejí

Odbor bezpečnostní:

- Zajištění personální, administrativní, fyzické a kybernetické bezpečnosti, bezpečnosti IS, kryptografické ochrany
    - Oddělení bezpečnosti
        - Zajištění zabezpečení fyzického perimetru a objektů budov
        - Zajištění agendy požární bezpečnosti
    - Oddělení bezpečnosti ICT
        - Zajištění zabezpečení vnitřní sítě a IS
        - Správa bezpečnostní infrastruktury – monitoring
            - Spadá sem role manažera kybernetické bezpečnosti
            - Spadá sem role architekta kybernetické bezpečnosti

Sekce provozní:

- Odbor právní
    - Zajištění kompletního právního servisu pro zajištění činnosti ministerstva, administrátor výběrových a zadávacích řízení pro veřejné zakázky
- Odbor personální

[3] *Sekce a odbory/oddělení, které nejsou pro potřeby tohoto příkladu relevantní, nejsou rozpracovány.*

- Výkon činnosti v oblasti personalistiky a vzdělávání, platové a sociální politiky v souladu se zákoníkem práce, zajištění evidence zaměstnanců, vedení přijímacího řízení

- Odbor ICT
  - Oddělení provozu síťové infrastruktury
    - Správa aktivních prvků, firewallů (dále jen „FW“)
    - Serverová infrastruktura
  - Oddělení provozu aplikační infrastruktury
    - Podpora aplikace a webového rozhraní
    - Správa databáze
  - Oddělení uživatelské podpory
    - Helpdesk interní
    - Helpdesk externí
    - Interní správa pracovních stanic a mobilních zařízení
  - Oddělení správy laboratoře
    - Kompletní provoz a správa technologií pro laboratoř
    - Sekce certifikací

Sekce ekonomická:

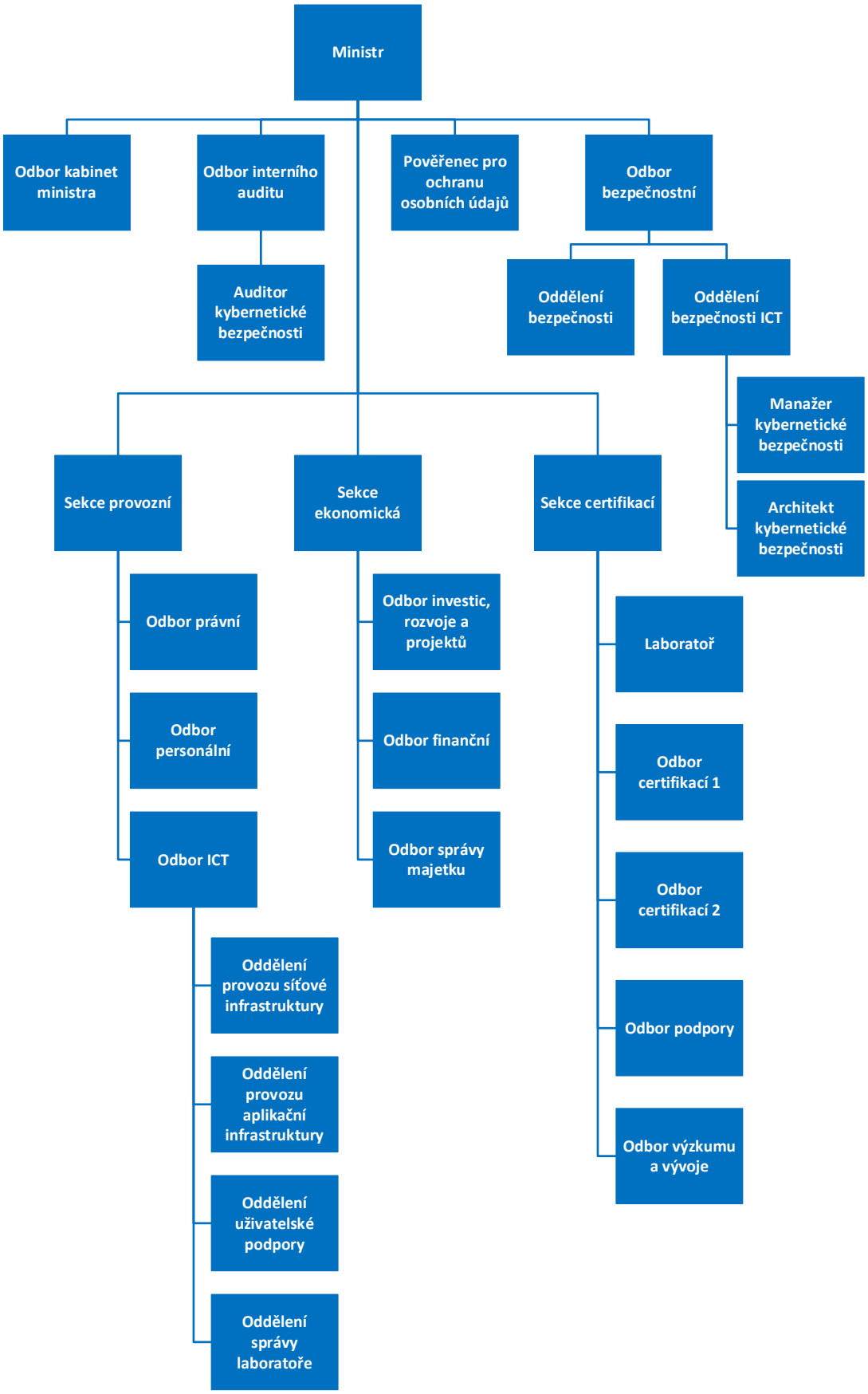
- Odbor finanční
  - Zajištění účetní agendy a agendy rozpočtu, provádění ekonomických rozborů, správa pokladních operací a zúčtovacího styku
- Odbor investic, rozvoje a projektů
  - Zajištění investičních projektů od jejich tvorby k realizaci, zajištění projektového řízení
- Odbor správy majetku
  - Zajištění správy majetku a údržby budov a areálu

Sekce certifikací:

- Laboratoř
  - Laboratoř pro testování a měření kvality průmyslových přístrojů4 před udělením certifikátu, k práci využívají speciální technologie, určené a vyvinuté pro měření kvality a bezpečnosti snímačů, výsledky měření následně předávají na odbory certifikací
- Odbor certifikací 1 a 2
  - Zajištění procesu certifikace, na základě vlastní činnosti a výsledků z laboratoře rozhodují o výsledku certifikace, informují žadatele a odbor podpory

[4] Nejedná se o senzory ve zdravotnictví.

- Odbor podpory
    - Poskytuje podporu interně i pro externí subjekty – spravuje žadatele
    - Správa podmínek pro příjem žádostí o certifikaci od externích žadatelů
    - Správa veřejného i neveřejného seznamu certifikátů
    - Vystavuje certifikáty
- Odbor výzkumu a vývoje
    - Koordinace výzkumu a vývoje v oblasti certifikací



Obrázek 3: Organizační struktura ministerstva

2 Kybernetická bezpečnost

Cílem KB je zajištění bezpečnosti informací vzniklých či zpracovávaných v kybernetickém prostoru. Dále všude tam, kde je to relevantní, musí být zahrnut i fyzický svět. KB tak zahrnuje v mnoha případech i fyzickou bezpečnost. Například datacentrum, ve kterém jsou ukládány informace, musí být pečlivě fyzicky chráněno, aby se do něj nedostala nepovolaná osoba, musí být zajištěna jeho odolnost vůči různým klimatickým vlivům, důvěrnost vytištěných dokumentů musí být chráněna na stejné úrovni jako jejich elektronické originály atd.

2.1 Bezpečnost informací

Bezpečnost informací znamená, že je v rámci celého životního cyklu informací zajištěna jejich důvěrnost, integrita a dostupnost (také známo pod pojmem CIA triáda: C-Confidentiality, I-Integrity, A-Availability)[5]:

- pro zachování důvěrnosti je nutné informace chránit proti neautorizovanému přístupu,
- pro zachování integrity je nutné chránit informace před neautorizovanou nebo náhodnou modifikací a zajistit jejich správnost a úplnost,
- pro zachování dostupnosti je nutné zabezpečit, aby informace byly dostupné v souladu s požadavky uživatelů tehdy, když to je potřebné.

Pro zjednodušení jsou pojmy KB a bezpečnost informací v rámci tohoto dokumentu vzájemně zaměnitelné.

2.2 Systém řízení bezpečnosti informací

ISMS je dokumentovaný proces, který je v organizacích zaváděn za účelem zajištění adekvátní úrovně KB. Základní rámec ISMS stanovují tzv. bezpečnostní politiky popisující základní principy, odpovědnosti a zásady ISMS.

ISMS je založeno na principu **řízení rizik** (anglicky známé pod pojmem „risk based approach“) a **neustálém zlepšování**.

ISMS zajišťuje funkční a úplnou ochranu služeb a informací, které jsou zahrnuty v jeho rozsahu. Z toho plyne, že v rozsahu ISMS musí být zahrnuto vše, co se těchto služeb či informací dotýká a má vliv na KB.

Kromě ISMS dle VKB je ISMS často zaváděno v souladu s mezinárodní normou ISO/IEC 27001. Oba přístupy se z velké části překrývají. ISMS dle VKB však obsahuje některá specifika, která jsou v normě uvedena obecně např. požadavek normy na soulad s právními předpisy. Dále VKB přesněji specifikuje a konkretizuje jednotlivá technická opatření, která požaduje implementovat, zatímco ISO/IEC 27001 pokrývá pouze některé z těchto oblastí, a navíc pouze částečně a uvádí jen obecné a nekonkrétní doporučení např. opatření A.9.4.3 Systém správy hesel, které říká pouze, že hesla mají být kvalitní, ale blíže požadavky na kvalitní hesla nespecifikuje – VKB oproti tomu přesně stanovuje požadavky na délku, komplexitu a omezení vztahující se k heslům.

[5] Existuje řada dalších kritérií, která se dají v případě potřeby zahrnout. Jedná se např. o nepopiratelnost, odpovědnost, spolehlivost, autentičnost, vlastnictví, použitelnost. Tyto parametry jsou však často vnímány jako součást základní CIA triády.

2.2.1 Rozsah systému řízení bezpečnosti informací

Vždy je nutné do rozsahu ISMS zahrnout určenou příp. určené služby dle ZKB a organizační části a aktiva, která mají na služby vliv z hlediska KB, tzn. přímo podporují výkon předmětných služeb v daném rozsahu a kvalitě**.** Je možné jej stanovit jak na celou organizaci, tak pouze na její dílčí části, např. na konkrétní IS, skupinu IS či organizační část. Žádoucí je ISMS stanovit v rozsahu celé organizace[6]. V případě, kdy je rozsah ISMS stanoven pouze na vybranou část organizace, je obzvláště důležité neopomenout do rozsahu zahrnout vše podstatné pro zajištění bezpečnosti informací regulovaného IS.

Rozsah ISMS z pohledu KB zahrnuje všechna **aktiva a organizační části** zahrnuté v daném ISMS. Rozsah ISMS je vhodné vymezit s ohledem na služby a informace, které chceme zabezpečit. Je možné jej vymezit např. jako rozsah primárních a podpůrných aktiv (bude popsáno níže) vybraného IS či jejich skupiny nebo v něm může být zahrnuta celá organizace.

U těchto aktiv a organizačních celků následně musí být přijata přiměřená bezpečnostní opatření, která zajistí, že bude zavedena adekvátní úroveň bezpečnosti informací, a to během celého životního cyklu služeb a informací a s ohledem na externí vazby.

Rozsah ISMS musí být dokumentovaná informace a k jeho určení může pomoci dokumentace daného systému (např. topologie, funkční schéma, související IS atd.), nebo organizace (organizační řád apod.).

Modelový příklad rozsahu dílčího informačního systému

Ministerstvo se rozhodlo určit rozsah ISMS pouze pro dílčí službu certifikace senzorů a příslušný systém: agendový (certifikační) systém. Vše, co je níže vyjmenováno, se týká pouze tohoto agendového systému.

Rozsah a hranice systému lze rozdělit do následujících aspektů:

Fyzické aspekty rozsahu

- **Fyzický perimetr**, který pokrývá všechny objekty a prostory, ve kterých je využíván a provozován agendový systém, tedy prostory, které jsou ve vlastnictví této organizace, ale i prostory, které nevlastní a má v nájmu. Tyto objekty se nacházejí na těchto adresách:
    - Smyšlená 1, Praha 1, 123 45,
    - Smyšlená 2, Praha 1, 123 45,
    - Smyšlená 3, Praha 1, 123 45.

Organizační a personální aspekty rozsahu

- **Všichni zaměstnanci organizace a další osoby**, které využívají agendový systém k výkonu činnosti ministerstva
- **Dodavatelé (včetně subdodavatelů)**, kteří participují na dodávkách primárních a podpůrných aktiv i ve smyslu poskytovaných služeb

[6] Doporučený postup je zavádět ISMS postupně po částech, dokud rozsah ISMS nepokryje celou organizaci.

Technologické aspekty rozsahu

- **Primární a podpůrná aktiva v rámci organizace**, která podporují službu certifikace a agendový systém
- **Primární a podpůrná aktiva spravovaná nebo provozovaná dodavateli**, která podporují službu certifikace a agendový systém

Konkrétní výčet primárních a podpůrných aktiv lze nalézt v katalogu aktiv (viz Příloha 6: Vzorové hodnocení aktiv a rizik). Rozsah ISMS agendového systému je také určen topologií systému.

2.2.2 Strategické cíle ISMS

Strategické cíle ISMS by měly být stanoveny v souladu se strategickými cíli organizace a mělo by je stanovit vrcholové vedení organizace ve fázi zavádění ISMS. Primárním cílem ISMS je zajištění bezpečnosti informací ve stanoveném rozsahu ISMS. Organizace by se měla snažit cíle co nejvíce konkretizovat v souladu se svými potřebami a vlastním důvodem zavádění ISMS.

Otázky, které mohou vést k nalezení strategických cílů ISMS:

- Čeho je potřeba dosáhnout zavedením ISMS?
- Co je účelem, proč zavádíme ISMS?
- Co po nás vyžadují legislativní požadavky, smlouvy s dodavateli/odběrateli v oblasti zajištění bezpečnosti informací?
- Proč a jak chceme chránit procesy, služby a informace v organizaci?

Modelový příklad strategických cílů ISMS

- Zajištění adekvátní úrovně důvěrnosti, integrity a dostupnosti
- Formalizace procesů a postupů
- Stanovení zodpovědností
- Zvýšení úrovně bezpečnostního povědomí zaměstnanců
- Soulad s legislativou, např.:
  - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
  - Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
  - Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR)
  - Zákon č. 110/2019 Sb., o zpracování osobních údajů
  - Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
  - Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
  - Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
  - Zákon č. 134/2016 Sb., o zadávání veřejných zakázek atd.

Přizpůsobení strategických cílů pro konkrétní službu

Specifické cíle musí být v souladu s těmi strategickými. Mělo by se jednat o konkretizaci strategických cílů do jasné podoby, ve které jsou promítnuty konkrétní požadavky na KB dané služby (zákonné, uživatelů atd.). Jako podklad pro stanovení cíle na dostupnost IS může sloužit příslušná smlouva o úrovni poskytovaných služeb (dále jen „SLA“).

Modelový příklad konkrétních cílů ISMS pro agendový systém

Pokud budeme uvažovat o službě certifikace a agendovém systému, je možné v rámci ISMS identifikovat následující cíle:

- ochrana informací dle zásad podle jednotlivých úrovní,
- zajištění výkonu služby certifikace a agendového systému v rámci běžné pracovní doby (v režimu 8/5),
- dodržování zákonných povinností.

3 Kontext organizace

Při zavádění ISMS musíme zohlednit specifické aspekty každé jednotlivé organizace, např. organizaci práce, důvod zřízení, strategické cíle či legislativní požadavky. Vzhledem k výše uvedenému je patrné, že kontext organizace je faktor, který má významný vliv na celkový ISMS, který se pro každou organizaci stává jedinečným.

Znalost kontextu organizace zajistí efektivnost a účelnost ISMS. Součástí úspěšného zavedení ISMS je přímá podpora vedení organizace, písemná deklarace této podpory, reálné prosazování ISMS napříč organizací, poskytování dostatečných zdrojů (lidských, finančních a časových) za účelem naplňování cílů ISMS a chování v souladu s požadavky ISMS.

3.1 Osoby podílející se na řízení aktiv a rizik

Jedním ze základních předpokladů zajištění bezpečnosti informací je správné nastavení procesu řízení aktiv a rizik. V samotném začátku je nutné stanovit osoby, které v tomto procesu budou mít svoji roli.

3.1.1 Vrcholové vedení

- Vrcholové vedení nese konečnou odpovědnost za ISMS ve společnosti. Je potřeba, aby demonstrovalo svoji podporu ISMS, problematikou se adekvátně zabývalo a zajistilo odpovídající podmínky klíčovým rolím, které se na ISMS aktivně podílejí.

Příklad vrcholového vedení:

- Úřad – vedoucí úřadu, ředitel, předseda atd.
- Ministerstvo – ministr (např. pro modelovou organizaci Ministerstvo pro certifikaci senzorů)
- Soukromá společnost – jednatel, představenstvo atd.
- Nemocnice – ředitel

3.1.2 Výbor pro řízení kybernetické bezpečnosti

Výbor pro řízení kybernetické bezpečnosti (dále jen „výbor KB“) je strategickým koordinačním orgánem pro implementaci a údržbu ISMS v působnosti organizace. Má odpovědnost za celkové řízení a rozvoj KB. **Členem musí být alespoň jeden zástupce vrcholového vedení nebo jím pověřená osoba a manažer kybernetické bezpečnosti**. Výbor KB by měl být ustanoven vrcholovým vedením.

Klíčové činnosti výboru:

- Tvorba rámce KB, zásad a celkové směrování povinné osoby (definování strategických cílů a směrování rozvoje v oblasti KB)
- Definice rolí a odpovědností v rámci ISMS
- Definice požadavků na podávání zpráv a kontrolu ISMS
- Kontrola aktuálního stavu KB v rámci povinné osoby a zjišťování, zda dochází k naplňování plánovaných cílů

Doporučené obsazení výboru:

Členy výboru KB s hlasovacími právy by měly být role odpovědné za:

- vrcholové vedení organizace, případně jím pověřený zástupce,

- bezpečnost,
- správu a/nebo provoz ICT prostředků,
- legislativní činnost,
- ekonomickou činnost,
- personální činnost,

a dále pak:

- manažer kybernetické bezpečnosti,
- architekt kybernetické bezpečnosti.

Také je možné další role přizvat (tzn. nebudou mít hlasovací práva) dle potřeby a předmětu konkrétního jednání výboru (např. garanty aktiv nebo auditora kybernetické bezpečnosti).

Modelový příklad složení výboru pro kybernetickou bezpečnost

V rámci modelové organizace je výbor KB výkonným rozhodovacím orgánem, jeho členem je samotný ministr. Rozhodnutí výboru KB jsou závazná a nemusí být dále schvalována. Ministr se nemusí účastnit všech jednání, v tomto případě za sebe pověří zástupce, ale účastní se všech rozhodovacích jednání. Program jednání výboru KB je vždy distribuován s dostatečným předstihem, aby se všichni účastníci mohli připravit. K jednání výboru KB mohou být přizváni i další účastníci, ale je preferován menší počet členů, který přispívá k snadnější diskusi a korigování jednotlivých jednání výboru KB. Ředitelé odborů předávají své podněty prostřednictvím svých náměstků. Z jednání výboru KB jsou vyhotoveny zápisy (vykonává předsedou pověřená osoba), které obdrží všichni členové výboru KB. Schvalování probíhá většinově, v případě shodného počtu hlasů má předseda výboru KB rozhodující hlas.

Předseda výboru:

- Ministr

Místopředseda výboru:

- Ředitel odboru bezpečnostního

Členové:

- Náměstek pro řízení sekce ekonomické
- Náměstek pro řízení sekce provozní
- Náměstek pro řízení sekce certifikací
- Manažer kybernetické bezpečnosti
- Architekt kybernetické bezpečnosti

3.1.3 Manažer kybernetické bezpečnosti

Manažer kybernetické bezpečnost je role, která v souladu s požadavky vrcholového vedení a výboru KB řídí celé ISMS. V praxi je manažer kybernetické bezpečnosti jakýmsi mezistupněm mezi strategickou úrovní managementu a operativní úrovní. Manažer kybernetické bezpečnosti musí mít pro výkon činnosti patřičné zázemí, pravomoci, zdroje, schopnosti, dostatečnou praxi a být adekvátně proškolen.

Manažer kybernetické bezpečnosti nesmí být pověřen výkonem rolí odpovědných za provoz. Tento požadavek cílí na riziko střetu zájmů, který by se u této role mohl projevit v případě, že by byla odpovědná jak za provoz, tak za bezpečnost.

Dá se říct, že manažer kybernetické bezpečnosti tvoří tzv. „SPOC – Single Point of Contact“ (jednotné kontaktní místo) pro všechny činnosti související s KB, přičemž některé činnosti vykonává sám a na některé pouze dohlíží a zajišťuje jejich korektní provedení.

Klíčové činnosti manažera kybernetické bezpečnosti:

- Odpovědnost za řízení ISMS
- Pravidelný reporting pro vrcholové vedení organizace
- Pravidelná komunikace s vrcholovým vedením organizace
- Předkládání zpráv o hodnocení aktiv a rizik, plánu zvládání rizik a prohlášení o aplikovatelnosti výboru KB
- Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT
- Komunikace s GovCERT/CSIRT
- Podílení se na procesu řízení aktiv a rizik
- Koordinace řízení kybernetických bezpečnostních incidentů
- Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření

Modelový příklad stanovení manažera kybernetické bezpečnosti

V rámci modelové organizace je stanovena role manažera kybernetické bezpečnosti, která je organizačně zařazena do Oddělení bezpečnosti ICT, které je součástí Odboru bezpečnosti. Odbor bezpečnosti je zařazen přímo pod ministra.

3.1.4 Garant aktiva

Garant aktiva je osoba, která má detailní znalost aktiva, jehož je garantem. V rámci procesu řízení aktiv a rizik se podílí především na hodnocení aktiv a rizik, případně na výběru příslušných bezpečnostních opatření.

Klíčové činnosti:

- Odpovědnost za zajištění rozvoje, použití a bezpečnosti aktiva
- Spolupráce s ostatními osobami zastávajícími bezpečnostní role

Modelový příklad stanovení garantů aktiv

Vzhledem k velikosti organizace bylo v rámci modelového příkladu použito dvouúrovňové stanovení garantů aktiv – gestor aktiva a garant aktiva.

Gestor aktiva je nejvýše postavený vedoucí pracovník organizačního celku, pod který dané aktivum přísluší. Gestor aktiva má příslušné pravomoci, aby mohl rozhodovat o nastavení požadavků nutných pro zajištění bezpečnosti aktiva.

Gestor aktiva stanovuje **garanta aktiva**, který má detailní znalosti daného aktiva. Garant aktiva se zpravidla zapojuje do procesu řízení aktiv a rizik, jehož výstupy schvaluje gestor aktiva.

Konkrétní příklady stanovených gestorů a garantů aktiv jsou uvedeny v katalogu aktiv a v kapitolách 4.1.3. Určení garantů primárních aktiv a 4.2.3. Určení garantů podpůrných aktiv.

3.1.5 Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti je bezpečnostní rolí, která zajišťuje bezpečnou architekturu IS s ohledem na potřeby organizace.

Klíčové činnosti architekta kybernetické bezpečnosti:

- Odpovědnost za návrh implementace bezpečnostních opatření
- Zajišťování architektury bezpečnosti

V praxi často dochází ke sloučení role architekta kybernetické bezpečnosti a architekta IT nebo vedoucího pracovníka IT. Sloučení architekta IT nebo vedoucího pracovníka IT s architektem kybernetické bezpečnosti neodpovídá doporučení VKB nebo „good practice“. Argumenty pro oddělení rolí jsou především náročnost agendy a množství činností, které musí obě role vykonávat a předcházení možnému střetu zájmů.

Architekt kybernetické bezpečnosti – osoba odpovědná za návrh implementace bezpečnostních opatření a zajišťování architektury bezpečnosti.

Architekt IT – osoba odpovědná za návrh vhodné aplikační i technologické architektury IS organizace. Navrhuje podklady pro konfiguraci HW a software (dále jen „SW“) pro optimalizaci provozu IS.

Modelový příklad stanovení architekta kybernetické bezpečnosti

V rámci modelové organizace je role architekta KB organizačně zařazena do Oddělení bezpečnosti ICT, které je součástí Odboru bezpečnosti. Odbor bezpečnosti je zařazen přímo pod ministra.

3.1.6 Auditor kybernetické bezpečnosti

Auditor KB je role odpovědná za provádění auditu KB. Klíčovou podmínkou je, že výkon této role je neslučitelný s výkonem rolí manažera KB a architekta KB. Tento požadavek vychází z podstaty role auditora, který musí být nestranný vůči předmětu auditu a jehož hlavní náplní je hodnocení míry souladu ISMS a realizovaných bezpečnostních opatření s definovanými požadavky VKB, stanovenými bezpečnostními politikami a vhodnými bezpečnostními standardy a poskytování nezávislé zpětné vazby o účelnosti a účinnosti ISMS a bezpečnostních opatření.

Klíčové činnosti auditora kybernetické bezpečnosti:

- Plánování činností auditu KB podle specifických podmínek auditované organizace
- Provedení auditu a vedení dokumentace o jeho průběhu podle stanovených metodik
- Vyhodnocení shromážděných nálezů z auditu a jejich srovnávání s kritérii auditu
- Sdělení výsledků auditu a návrh doporučení pro jejich řešení
- Zpracování závěrečných zpráv z auditu
- Kontrola přijatých opatření
- Příprava a realizace opakovaných auditů

Pokud se vrcholové vedení rozhodne pověřit externí osobu prováděním auditu KB, tak je potřeba určit osobu v organizaci, která bude dohlížet na průběh tohoto auditu. Osoba pověřená dohledem na průběh auditu KB by neměla zároveň vykonávat roli manažera nebo architekta KB, aby nemohla ovlivňovat nestrannost externího auditora KB.

Modelový příklad stanovení auditora kybernetické bezpečnosti

V rámci modelové organizace je stanovena role auditora KB, která je organizačně zařazena do Odboru interního auditu. Odbor interního auditu spadá přímo pod ministra.

3.1.7 Další organizační složky a osoby

V kontextu organizace se na řízení aktiv a rizik mohou podílet i další organizační složky a osoby. S nimi mohou role uvedené výše konzultovat např. identifikaci a hodnocení jednotlivých aktiv a rizik. Mohou to být oddělení pracující s aktivy, pracovníci IT, běžní uživatelé atp. Dále, např. při zjišťování garantů aktiv, bude nutné často jednat i s uživateli aktiv.

Modelový příklad další organizační složky a osoby

V rámci modelové organizace se na procesu řízení aktiv a rizik podílí také dodavatelé, provozovatelé, uživatelé, pověřenec pro ochranu osobních údajů, osoby řešící kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty atd.

3.2 Klíčové informace, procesy, služby

Klíčové informace, procesy a služby tvoří hodnotu nebo užitek organizace. Jsou základním stavebním kamenem každé efektivně fungující organizace. Jedná se o všechny informace, procesy a služby vztažené směrem k hlavnímu business cíli (účelu existence) organizace. Fungování procesů a služeb je v drtivé většině organizací provázáno s IS.

Doporučujeme v rámci organizace vytvořit seznam všech používaných IS (např. ekonomický systém, docházkový systém, agendové systémy, IS spisové služby apod.), seznam všech klíčových služeb organizace a vzájemných vazeb mezi těmito systémy a službami.

Modelový příklad evidence systémů a služeb

Identifikované služby, systémy a vazby mezi nimi v rámci Ministerstva certifikací senzorů byly zaevidovány v následujících tabulkách (jedná se pouze o ukázku principu, nikoliv o vyčerpávající výčet):

Tabulka 2: Zkrácený seznam služeb poskytovaných ministerstvem

Seznam služeb poskytovaných ministerstvem		
ID	Název	Kategorie
S1	Služba certifikace senzorů	KII
S2	Služba elektronické pošty	VIS
S3	Vedení úřední desky	VIS
S4	Vedení účetnictví	Ostatní
S5	Vedení personálních dat	Ostatní
S6	Vedení docházky	Ostatní
S7	Výkon spisové služby	VIS

Seznam služeb poskytovaných ministerstvem		
ID	Název	Kategorie
S8	Zadávání veřejných zakázek	VIS
S9	…	…

Tabulka 3: Zkrácený seznam systémů ministerstva

Seznam systémů ministerstva		
ID	Název	Vazba na poskytovanou službu
IS1	Informační systém pro evidenci a zpracování procesu certifikace senzorů	S1
IS2	Informační systém spisové služby	S7
IS3	Docházkový systém	S5, S6
IS4	Ekonomický systém	S4
IS5	…	…

3.3 RACI matice

V následující tabulce jsou přiřazeny odpovědnosti za jednotlivé činnosti.

U každé činnosti mohou být dále identifikovány i další osoby, jejichž přizvání by k řešení dané činnosti bylo vhodné.

Tabulka 4: RACI matice

Činnosti	Výbor KB	Manažer KB	Auditor KB	Architekt KB	Garant aktiva
Stanovení rozsahu a cílů ISMS, bezpečnostních rolí a jejich kompetencí	A, R	I	I	I	I
Vytvoření bezpečnostních politik a dokumentace	A	R			
Proces řízení aktiv a rizik	A	R		R, C	R, C
Přezkoumávání a aktualizace ISMS	A, R	R		C	C
Audit ISMS	I	C	A, R	C	C

Tabulka 5: Legenda k RACI matici

Zkratka	Popis
R	Responsible (ti, kteří práci / úkol vykonávají)
A	Accountable (ti, kteří zodpovídají za celkové splnění úkolu)
C	Consulted (ti, kteří by se k danému mohli vyjádřit a být nápomocni s jeho řešením)
I	Informed (ti, kteří mají být informováni)

Modelový příklad rozdělení odpovědností pomocí RACI matice

Tabulka 6: RACI matice ministerstva

Činnosti	Výbor KB	Odbor bezpečnostní	Manažer KB	Auditor KB	Architekt KB	Gestor PrA	Gestor PoA	Garant PrA	Garant PoA	Pověřenec pro OOÚ	Odbor ICT	Další osoby
Kontrola aktuálního stavu kybernetické bezpečnosti a kontrola naplňování plánovaných cílů	A	R	R									
Stanovení strategických cílů ISMS	A	R	R		C	C				C	C	
Stanovení rozsahu ISMS	C	A	R		C	C				C	C	
Stanovení výboru pro řízení KB a jeho kompetencí	I	I	I	I	I	I	I	I	I	I	I	A, R (ministr)
Stanovení manažera KB a jeho kompetencí	A, R	I	I	I	I	I	I	I	I	I	I	
Stanovení architekta KB a jeho kompetencí	A, R	I	I	I	I	I	I	I	I	I	I	
Stanovení auditora KB a jeho kompetencí	A, R	I	I	I	I	I	I	I	I	I	I	
Stanovení gestora aktiva	A, R	I	C	I	C	I	I					
Vytvoření bezpečnostních politik		A	R		C	C	C			C	C	
Schválení bezpečnostních politik a šablon bezpečnostní dokumentace	A	R	R									
Identifikace a evidence primárních aktiv		A	R		C	C		R				C (dodavatel, provozovatel, uživatel)
Identifikace a evidence garantů primárních aktiv		A	R			R		I				
Hodnocení primárních aktiv	I	A	R			R		R				
Identifikace a evidence podpůrných aktiv			A, R		C	C	R	C	R		C	
Identifikace a evidence vazeb mezi primárními a podpůrnými aktivy			A, R		C	R	R	R	R		C	

Činnosti	Výbor KB	Odbor bezpečnostní	Manažer KB	Auditor KB	Architekt KB	Gestor PrA	Gestor PoA	Garant PrA	Garant PoA	Pověřenec pro OOÚ	Odbor ICT	Další osoby
Identifikace a evidence garantů podpůrných aktiv		A	R			I	R	C	I		C	
Hodnocení podpůrných aktiv		A	R		C	I	R		R			
Vytvoření metodiky pro identifikaci a hodnocení rizik včetně kritérií pro akceptovatelnost a výjimek		A	R									
Vytvoření katalogu hrozeb		A	R		R	R	R	R	R	C	C	C (osoby, které řeší incidenty a události)
Vytvoření katalogu zranitelností		A	R		R	R	R	R	R	C	C	C (osoby, které řeší incidenty a události)
Schválení metodiky pro identifikaci a hodnocení rizik	A	R	I	I	I	I	I	I	I	I	I	
Identifikace kombinací aktiv, hrozeb a zranitelností (výstup – identifikovaná rizika)		A	R		R	R	R	R	R			
Stanovení konkrétních hodnot hrozeb a zranitelností pro aktiva		A	R		C	R	R	R	R			
Výpočet výsledné hodnoty rizika, návrh způsobu zvládání rizik a výběr bezpečnostních opatření do plánu zvládání rizik		A	R		R	R	R	R	R			
Vytvoření plánu zvládání rizik		A	R		C	C	C	C	C			
Schválení plánu zvládání rizik	A	R	I	I	I	I	I	I	I		I	
Vytvoření zprávy o hodnocení aktiv a rizik	I	A	R		I	I	I	I	I		I	
Souhlas se zbytkovými riziky	A, R											
Vytvoření prohlášení o aplikovatelnosti	I	A	R		C	C	C	C	C			
Zavádění bezpečnostních opatření		A	R		R	C	C	C	C		C	

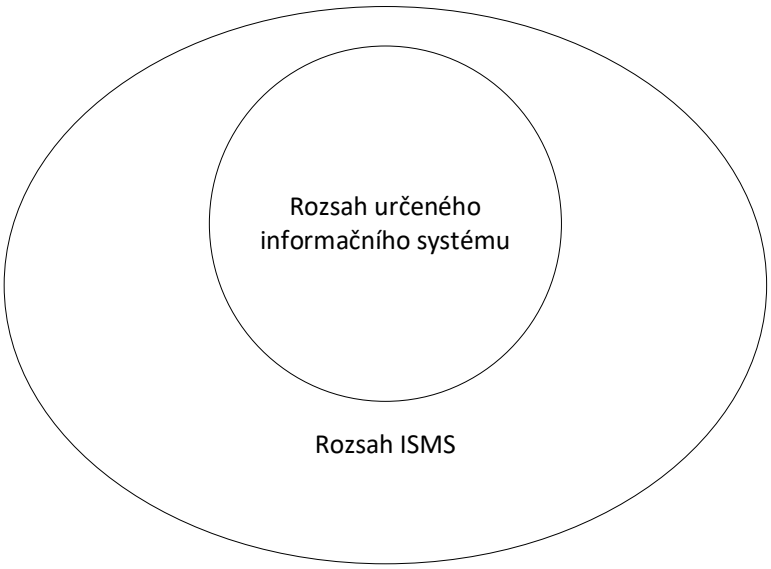
Činnosti	Výbor KB	Odbor bezpečnostní	Manažer KB	Auditor KB	Architekt KB	Gestor PrA	Gestor PoA	Garant PrA	Garant PoA	Pověřenec pro OOÚ	Odbor ICT	Další osoby
Sledování a přezkoumávání rizik, zohlednění výstupů interního auditu a významných změn, zohlednění opatření podle § 11 ZKB, pravidelná aktualizace celého procesu řízení aktiv a rizik	I	A	R		C	C	C	C	C	C	C	
Audit ISMS	I	I	C	A, R	C	C	C	C	C		C	

4 Řízení aktiv v oblasti kybernetické bezpečnosti

Aktivum je vše, co má pro organizaci hodnotu. S ohledem na KB jsou rozlišována aktiva primární (služby a informace) a podpůrná (technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti IS).

V rámci ISMS jsou řízena ta aktiva, která se nachází v jeho rozsahu. Z tohoto důvodu je nutné znát rozsah ISMS a identifikovat v něm všechna aktiva. Kdybychom nějaké aktivum omylem či záměrně opomněli, mohlo by to mít významný, v některých případech i fatální, vliv na výsledný ISMS. K tomu, abychom těmto situacím předcházeli, slouží přezkoumávání a neustálé zlepšování ISMS, kdy dochází mj. k aktualizaci rozsahu ISMS. Identifikovaná aktiva jsou následně evidována, jsou jim přiřazeni garanti, jsou ohodnocena a dále vstupují do procesu řízení rizik.

Dále je také potřeba si uvědomit rozdíl mezi aktivy, která jsou v rozsahu určené služby a příslušného IS a aktivy, která jsou v rozsahu ISMS. Aktiva v rozsahu IS jsou pouze ta aktiva, která mají přímou spojitost se službou poskytovanou IS, zatímco aktiva v rozsahu ISMS jsou aktiva, která nemají přímou vazbu na poskytovanou službu, ale mají vliv na bezpečnost aktiv v rozsahu určeného IS. Aktiva v rozsahu určeného IS jsou tedy podmnožinou aktiv spadajících do rozsahu ISMS. Detailněji je tato problematika vysvětlena v podpůrném materiálu *„Systém a rozsah ISMS“* dostupném na webových stránkách NÚKIB: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/.



Obrázek 4: Schéma rozsahu ISMS

V rámci tohoto dokumentu je pracováno s typovými aktivy (jak u primárních, tak u podpůrných aktiv). Jsou to uměle vytvořené skupiny aktiv, které mají společné vlastnosti, a tato aktiva z určitého důvodu nechceme nebo nemůžeme dále dělit. Seskupování aktiv je nutné podložit logickou úvahou. Jednotlivá aktiva seskupená do jednoho typového aktiva si musí být svou povahou natolik podobná, aby na ně působily stejné hrozby a zranitelnosti. Dále nelze seskupovat aktiva, jejichž hodnocení z pohledu důvěrnosti, integrity a dostupnosti se významně liší. Při seskupování podpůrných aktiv je třeba věnovat pozornost také vazbám na primární aktiva.

Vytvoření typového aktiva by nemělo vést k tomu, že bude výsledné hodnocení netransparentní a značně zkreslené. V případě, že jsou vytvořeny široké skupiny aktiv, stává se hodnocení příliš

obecným a ztrácí se jeho vypovídající hodnota, schopnost nalézat konkrétní rizika a prioritizovat jejich zvládání dle důležitosti.[7]

Kromě základních atributů bezpečnosti informací (důvěrnost, integrita a dostupnost) byl v rámci tohoto podpůrného materiálu definován ještě čtvrtý atribut – ztráta. V rámci hodnocení aktiv tedy posuzujeme i případ, kdy by došlo ke ztrátě dat. Atribut ztráta slouží pro potřeby stanovení vstupních ukazatelů kontinuity činností a je s ním dále pracováno v rámci procesu kontinuity činností, který však není předmětem tohoto materiálu. Při hodnocení aktiv, které zároveň slouží jako analýza dopadů (známá také jako BIA – Business Impact Analysis), je tedy možné získat potřebné informace i pro kontinuitu činností a maximálně tak využít informace získané od garantů aktiv.

Řízení aktiv je kontinuální proces a je nutné jej neustále zlepšovat. To, co se při prvotní identifikaci aktiv může jevit jako vhodně zvolená typová aktiva, se při přezkoumání nebo v průběhu hodnocení rizik může jevit jako nedostatečné. V praxi se často stává, že je nutné typové aktivum rozdělit na menší skupiny a vytvořit nová typová aktiva, naopak v některých případech může dojít ke sloučení typových aktiv do jednoho celku, současně aktiva vznikají a zanikají, proto je důležité přezkoumávání, zlepšování a neustálý vývoj celého procesu a jeho výstupů.

Pro prvotní identifikaci aktiv doporučujeme začínat s menším množstvím typových aktiv, ale **celý proces korektně dokončit.**

Veškerý postup týkající se identifikace aktiv, evidence aktiv, určení garantů aktiv, určení vazeb mezi aktivy a hodnocení aktiv musí být v dokumentované podobě – **metodice pro identifikaci a hodnocení aktiv a jejich garantů.** Metodika by měla být dostatečně návodná, srozumitelná a jednoznačná tak, aby byl celý proces opakovatelný, přezkoumatelný a vedl za stejných podmínek ke stejným výsledkům, bez závislosti na konkrétní osobě.

Evidence aktiv je často označovaná jako **Katalog aktiv**. Jedná se o jeden ze stěžejních dokumentů procesu řízení aktiv, který obsahuje detailní informace o jednotlivých aktivech, včetně jejich hodnocení, určených garantech atd.

Modelový příklad řízení aktiv

Ministerstvo řídí aktiva na základě stanoveného rozsahu, který je popsán v Příloze 1: Vzorová politika systému řízení bezpečnosti informací, dle platné metodiky popsané v Příloze 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik a evidence aktiv je součástí Přílohy 6: Vzorové hodnocení aktiv a rizik.

4.1 Primární aktiva

Primární aktiva je možné vnímat jako služby a informace, které jsou součástí vymezeného rozsahu ISMS, který stanovujeme za účelem ochrany těchto aktiv.

Ve většině případů jsou primární aktiva spojena především s výkonem určité agendy, poskytováním služby apod. Měla by mj. vycházet z určené služby a příslušného IS.

[7] Při prvotním hodnocení aktiv doporučujeme vytvářet a hodnotit typová aktiva, která budou detailněji rozpracována v následných cyklech přezkoumání a zlepšování celého ISMS. Tzn. soustředit se na obecnější prvotní pohled a nezahltit se přílišnými detaily. Při následných aktualizacích pak lze pracovat s větší mírou detailu, přidávat nová typová aktiva, rozdělovat stávající nebo je modifikovat atd.

Jsou to takové služby a informace, jejichž ztráta nebo narušení by mělo dopad na chod, funkčnost, účel a bezpečnost celé organizace, případně systému nebo služby s ohledem na vymezený rozsah ISMS z hlediska důvěrnosti, integrity a dostupnosti.

Jako primární aktiva je možné identifikovat např.:

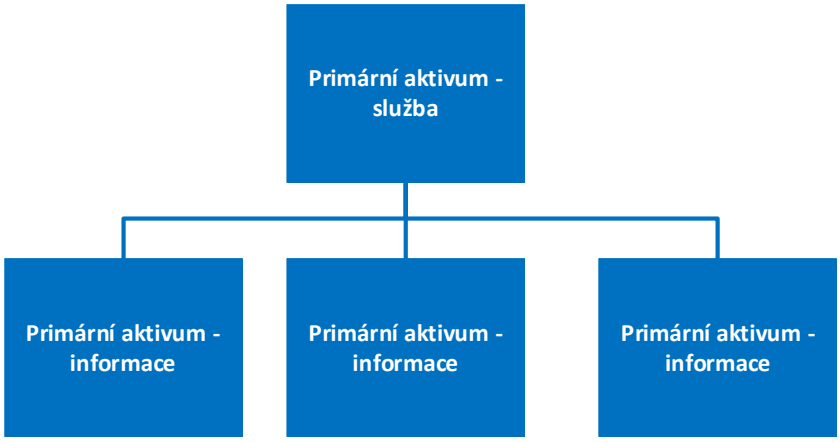
- služby – vykonávání jednotlivých činností organizace, získávání, poskytování, zpracování, shromažďování, vyhodnocování, ukládání, předávání, likvidování informací včetně jejich zobrazení, umožnění komunikace, např. výroba elektřiny, provoz ropovodu, prodej plynu, služba řízení letového provozu, činnost subjektu odpovědného za kontrolu řízení provozu, výkon činnosti úvěrové instituce, zajištění elektronické pošty atd.,
- informace – např. informace zpracovávané a vytvářené v rámci výkonu agendy nebo IS (včetně logů a metadat), vlastní data agendy, záznamy o provozu, data o uživatelích, přístupové údaje, data relací, konfigurační soubory, zdrojové kódy, zálohy, certifikáty.

4.1.1 Identifikace primárních aktiv

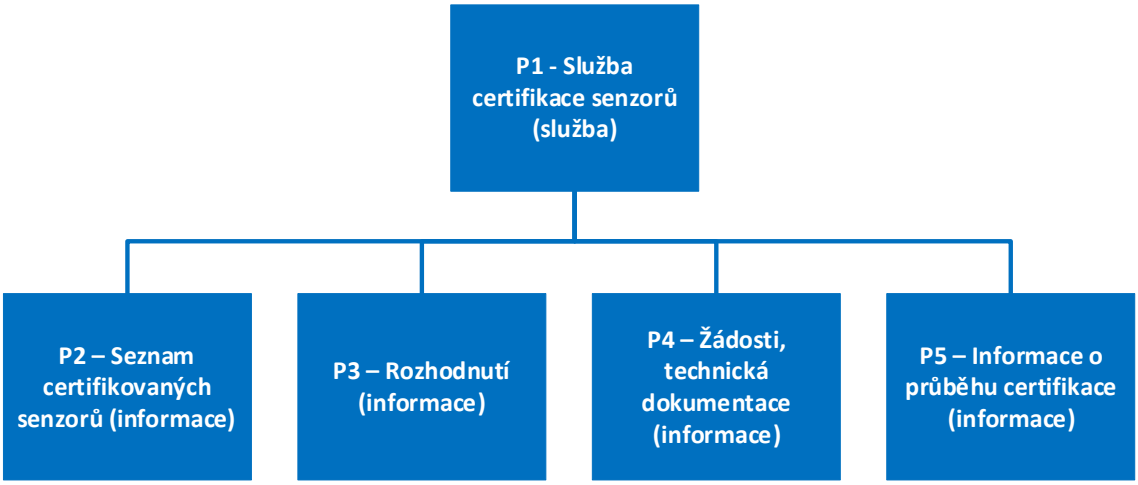
Při identifikaci primárních aktiv můžeme vycházet kromě určené služby a příslušného IS, například z prozkoumání hlavní činnosti celé organizace. Klíčovou součástí jsou tak rozhovory s vedoucími odborných útvarů. Dále je možné čerpat například z:

- organizačního řádu,
- zakládací listiny,
- legislativních zdrojů,
- smluv, směrnic, příruček, manuálů,
- interních aktů řízení organizace,
- a dalších.

Při identifikaci primárních aktiv IS je potřeba začít u jeho účelu, např. evidování a zpracování procesu certifikace senzorů. Z účelu odvodíme první primární aktivum, kterým bude služba, např. služba certifikace senzorů. Následně se můžeme zamyslet nad tím, s jakými informacemi daná služba pracuje, např. technická dokumentace, podané žádosti, evidence schválených senzorů, evidence neschválených senzorů, informace o průběhu certifikace, výsledky certifikačního procesu atd. Jednotlivé informace můžeme sloučit do typových aktiv a vznikají nám další primární aktiva, tentokrát typu informace.



Obrázek 5: Vazby mezi primárními aktivy



Obrázek 6: Vazby mezi primárními aktivy ministerstva

V některých případech nelze jednoznačně identifikovat a vytvořit primární aktiva z informací, které služba zpracovává. Tato situace nastává především u nestrukturovaných typů informací, např. e-mailové služby. V tom případě je možné pracovat pouze s primárním aktivem typu služba. Za zpracování informací – poskytnutí služby – se v tomto případě uvažuje i prosté zobrazení, např. zobrazení textu na obrazovce, přehrání zvuku atd. Jeden IS může poskytovat více služeb, jednotlivé služby lze dělit na menší typová aktiva typu služba, např. službu certifikace senzorů je možné rozdělit na službu zveřejňování informací o certifikovaných senzorech, službu certifikování výrobců, službu dokumentace procesu certifikace atd. Úroveň detailu záleží na velikosti a složitosti IS a maturitě organizace.

Vazby mezi jednotlivými primárními aktivy by měly být evidovány.

Otázky, které mohou vést k identifikaci primárních aktiv

- Jaká služba je určena podle ZKB?
- Jaký je účel této organizace, agendy či IS?
- Jaké jsou v rámci této organizace, agendy či IS klíčové procesy?
- Jací jsou klíčoví zákazníci či uživatelé této organizace, agendy či IS?
- Bez jakých informací nemůžete vykonávat svoji práci?
- Jaké činnosti jsou potřeba k vykonávání běžné agendy?
- Jakou pro mě má agenda či IS hodnotu (z pohledu významu/smyslu) a co je v něm to důležité?
- Jsou součástí této organizace, agendy či IS osobní údaje, citlivé osobní údaje nebo obchodní tajemství?
- Jsou s existencí této organizace, agendy či IS spojeny nějaké zákonné nebo smluvní požadavky?
- Zahrnuje vaše práce mezinárodní spolupráci?
- Může dojít k poškození pověsti při narušení bezpečnosti informací?
- Může mít narušení bezpečnosti informací vliv na bezpečnost či zdraví osob?
- Hrozí v nějaké situaci možnost finanční ztráty či nutnost nahrazovat škody (pokuty/sankce)?

- S jakými dalšími systémy pracujete v rámci výkonu běžné pracovní činnosti?

Modelový příklad identifikace primárních aktiv u agendového systému

Služby:

- Služba certifikace senzorů

Služba certifikace senzorů jako celek, je pro potřeby modelové organizace nezbytná a bez jejího výkonu nemůže plnit svůj účel. Hodnocení této služby je dáno nejvyšším hodnocení jednotlivých atributů (důvěrnost, integrita, dostupnost, ztráta) bezpečnosti informací, se kterými tato služba pracuje.

Informace:

- Seznam certifikovaných senzorů
- Evidence certifikátů
- Evidence uživatelů systému
- Rozhodnutí
- Žádosti, technická dokumentace
- Informace o průběhu certifikace

4.1.2 Evidence primárních aktiv

Všechna identifikovaná primární aktiva, která se nachází v rozsahu ISMS, musí být zaznamenána v dokumentované podobě[8]. Způsob, jakým tato evidence bude provedena, je na zvážení každé organizace.

Příklad atributů uchovávaných o primárním aktivu:

- ID aktiva
- Název
- Garant aktiva
- Hodnocení aktiva z hlediska důležitosti (CIA)
- Detailní popis9 – v případě, že se jedná o typové aktivum tak i specifikace toho, co zahrnuje
- Další informace o aktivu – např. kdo jsou jeho uživatelé, jaké agendy jej využívají, jaká legislativa se aktiva týká atd.

Modelový příklad evidence primárních aktiv u agendového systému

Modelová organizace má vytvořený Katalog primárních aktiv, který je součástí Přílohy 6: Vzorové hodnocení aktiv a rizik.

[8] Někdy označováno jako Katalog primárních aktiv.
[9] Z detailního popisu aktiva by mělo být zcela zřejmé, o jaké aktivum se jedná, aby při dalších revizích nevznikalo nedorozumění nebo zkreslení.

Tabulka 7: Ukázka z katalogu primárních aktiv

ID	Typové primární aktivum	Kategorie	Specifikace	Gestor aktiva	Garant aktiva
S1	Služba certifikace senzorů	služba	Zajištění procesu certifikace a evidence senzorů	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)
P1	Seznam certifikovaných senzorů	informace	Seznam všech úspěšně certifikovaných senzorů a certifikátů samotných	náměstek sekce certifikací (Martin Novotný)	ředitelka odboru podpory (Renata Malá)
P2	Rozhodnutí	informace	Výsledné rozhodnutí certifikačního procesu – negativní i pozitivní	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)
P3	Žádosti, technická dokumentace	informace	Technická dokumentace a žádost o certifikaci, kterou zasílají jednotliví výrobci ke svým senzorům	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)
P4	Informace o průběhu certifikace	informace	Informace o průběhu certifikace – kdo rozhodl, kdy došla žádost, průběh certifikace atd.	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)

Modelová organizace v katalogu primárních aktiv eviduje také informace o tom, zda je aktivum součástí určeného IS nebo rozsahu ISMS. Přičemž aktiva, která jsou součástí určeného IS jsou zároveň automaticky součástí rozsahu ISMS.

Modelová organizace zároveň eviduje vazby mezi jednotlivými primárními aktivy.

Tabulka 8: Evidence vazeb mezi primárními aktivy

Vazby mezi primárními aktivy		S1	P1	P2	P3	P4
		Služba certifikace senzorů	**Seznam certifikovaných senzorů**	**Rozhodnutí**	**Žádosti, technická dokumentace**	**Informace o průběhu certifikace**
S1	Služba certifikace senzorů		x	x	x	x
P1	Seznam certifikovaných senzorů	x				
P2	Rozhodnutí	x				
P3	Žádosti, technická dokumentace	x				
P4	Informace o průběhu certifikace	x				

4.1.3 Určení garantů primárních aktiv

Primární aktiva by měla být schválena na nejvyšší úrovni, např. prostřednictvím výboru KB. Je nezbytné k jednotlivým primárním aktivům přiřadit garanty a tyto garanty evidovat.

Manažer kybernetické bezpečnosti by měl jednotlivé garanty vytipovat, např. s pomocí organizačního řádu, a následně s nimi tuto skutečnost konzultovat. Stanovení garantů primárních aktiv by mělo být zaznamenáno formalizovaným způsobem (např. určení vedením organizace či výborem KB).

Garanty primárních aktiv bývají nejčastěji pracovníci zastávající role typu vedoucí oddělení, ředitelé odborů, vlastník procesu, ředitel výroby atd.

Garanti aktiv jsou vybíráni na základě jejich pracovního zařazení, procesních a odborných znalostí daného aktiva. Garant aktiva musí být schopen na základě možných dopadů ohodnotit aktivum tak, aby byla osoba odpovědná za zpracování hodnocení rizik schopna tato rizika adekvátně vyhodnotit a řídit.

Modelový příklad určení garantů primárních aktiv u agendového systému

IS pro evidenci a zpracování procesu certifikace senzorů je na ministerstvu využíván v Sekci certifikací, primárně je tento IS využíván Odbory certifikací, Odborem podpory a Laboratoří.

V souladu s využitím role gestora a garanta aktiva (viz kapitola 3.1.4 Garant aktiva) byl jako gestor aktiva stanoven náměstek Sekce certifikací – Martin Novotný. Gestor aktiva si dále ve spolupráci s manažerem kybernetické bezpečnosti zvolil jednotlivé garanty aktiv, které poučil o jejich odpovědnostech a zajistil, aby obdrželi pověření zaměstnance k provádění úkolů spojených s výkonem bezpečnostní role.

4.1.4 Hodnocení primárních aktiv

Pokud bychom chtěli hodnotit primární aktivum typu služba, nelze hodnocení provést bez toho, abychom uvažovali o hodnotě informací, se kterými služba pracuje. Z toho důvodu nejdříve ohodnotíme všechna primární aktiva typu informace, které služba zpracovává. Samotná služba pak přebírá nejvyšší hodnoty jednotlivých atributů (důvěrnost, integrita, dostupnost, ztráta) navázaných primárních aktiv (informací).

V případech, kdy nelze jednoduše identifikovat a vytvořit primární aktiva z informací, které služba zpracovává a je vytvořeno typové aktivum služba, ve kterém jsou zahrnuty i příslušné informace, se při hodnocení primárního aktiva typu služba zároveň uvažují i tyto informace.

V rámci hodnocení primárních aktiv je posuzován dopad narušení bezpečnosti informací, je tedy nutné tato aktiva hodnotit minimálně z pohledu důvěrnosti, integrity a dostupnosti. Dále je doporučeno, aby pro hodnocení aktiv byly použity stupnice o čtyřech úrovních. Při posuzování hodnoty aktiv je nutné uvažovat o **nejhorším možném scénáři a nebrat v úvahu bezpečnostní opatření.** Vhodné je zaměřit se pouze na přímý vliv narušení bezpečnosti informací.

V rámci posuzování dopadu narušení dostupnosti je možné další rozdělení na nedostupnost a úplnou ztrátu dat. Tyto informace jsou potřebné při provádění analýzy dopadů. Během získávání potřebných informací o aktivech od jejich garantů pro potřeby řízení aktiv a rizik je tak možné zároveň získat potřebné informace i pro řízení kontinuity činností. Rozdělení na nedostupnost a úplnou ztrátu dat také může hrát významnou roli při výběru adekvátních bezpečnostních opatření, např. režim vysoké dostupnosti vs. postup zálohování.

Následující tabulka uvádí stupnici o čtyřech úrovních převzatou z VKB doplněnou o číselné vyjádření jednotlivých úrovní.

Tabulka 9: Stupnice pro hodnocení důvěrnosti, integrity a dostupnosti

Úroveň		Důvěrnost	Integrita	Dostupnost
1	Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP: CLEAR.	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2	Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: GREEN nebo TLP: AMBER.	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.
3	Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: AMBER.	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.
4	Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: RED nebo TLP: AMBER.	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.

VKB požaduje, aby byly v rámci hodnocení primárních aktiv posuzovány minimálně vybrané oblasti, které jsou uvedeny v následující tabulce, včetně podrobnějšího popisu.

Tabulka 10: Oblasti hodnocení primárních aktiv

Dopad podle VKB	Popis	Příklad
a) rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů	Jakékoliv informace týkající se identifikované či identifikovatelné fyzické osoby, citlivé osobní údaje.	Únik osobních údajů fyzické osoby.
b) rozsah dotčených právních povinností nebo jiných závazků nebo obchodního tajemství	Nutnost řídit se právními předpisy.	Narušení povinnosti zveřejňovat dokumenty na elektronické úřední desce, která je nepřetržitě dostupná vzdáleným přístupem. Smlouvy a z nich plynoucí sankce. Hodnota obchodního tajemství. Pokuty za porušení legislativy.
c) rozsah narušení vnitřních řídicích a kontrolních činností	Narušení rozhodovacích možností.	Neúplnost či modifikace informací potřebných pro rozhodování vedení a kontrolní činnost.
d) poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty	Zajištění důležitých externích informací týkající se organizace např. od EU, regulátora atd. Narušení agendy organizace.	Nedostupnost informací o fakturách na základě nedostupnosti ekonomického systému. Nedostupnost informací o možných obchodních příležitostech a z toho plynoucí ušlý zisk. Nedostupnost např. webu, může vést k neinformování veřejnosti o důležitých skutečnostech (záplavy, ekologické katastrofy atd.).
e) dopady na poskytování důležitých služeb	Narušení klíčových informací, procesů a služeb tvořící hodnotu nebo užitek organizace.	Narušení všech informací, procesů a služeb vztažených směrem k určené službě a hlavnímu business cíli (účelu existence) organizace (např. v případě Ministerstva pro certifikaci senzorů by se jednalo o narušení vydávání certifikací).
f) rozsah narušení běžných činností	Narušení nezbytných provozních činností.	Narušení činností personálních, ekonomických, správy budov a autoparku, neschopnost přijímat datové zprávy apod.
g) dopady na zachování dobrého jména nebo ochranu dobré pověsti	Negativní ovlivnění reputace u jednotlivců, organizačních součástí organizace, veřejnosti nebo ostatních organizací.	Nedodržení závazků. Únik interních informací.
h) dopady na bezpečnost a zdraví osob	Týká se systémů s dopadem na bezpečnost a zdraví osob (např. nemocnice, chemická továrna apod.).	Neschopnost zajistit základní příjem, potraviny, přístup ke zdravotní péči, svobodu apod. Možnost zranění a ztrát na životech.
i) dopady na mezinárodní vztahy	V případě mezinárodní spolupráce se jedná o rizika spojená s vytvořením negativního obrazu na Českou	Únik informací od zahraničních partnerů.

Dopad podle VKB	Popis	Příklad
	republiku u EU, NATO nebo dalších zahraničních zemí a mezinárodních organizací.	V případě narušení bezpečnosti ztráta důvěryhodnosti.
j) dopady na uživatele informačního a komunikačního systému	Znemožnění výkonu činnosti interním i externím uživatelům.	Ztrátu možnosti přístupu uživatele ke službě vlivem její nedostupnosti (při výpadku internetového bankovnictví se tento problém dotkne velkého počtu uživatelů – nemožnost zadat platební příkaz online).
Dopady na trestně právní řízení (nad rámec VKB)	Narušení primárních aktiv ovlivní trestně-právní řízení.	Vyzrazení informací v rámci trestního řízení, čímž by mohlo být trestní řízení zastaveno.

Hodnocení aktiv může probíhat na společném jednání pracovníka, který je odpovědný za provedení celého procesu hodnocení aktiv a rizik v dané organizaci a jednotlivými garanty aktiv. Před samotným hodnocením doporučujeme seznámit garanty s metodikou identifikace a hodnocení aktiv, např. formou zaslání manuálu nebo formou školení. Odpovědnost za provedení hodnocení aktiv by měl mít manažer kybernetické bezpečnosti, avšak může touto odpovědností pověřit jiného, kvalifikovaného pracovníka v rámci organizace. Pracovník, který řídí schůzku, pokládá jednotlivým garantům otázky a dbá na to, aby byl zachován postup uvedený v metodice a jednotné hodnocení podle zvolených škál v rámci celé organizace, tzn. v průběhu jednání koriguje případné nadhodnocování nebo podhodnocování jednotlivých hodnot aktiva. Postup hodnocení je nutné všem respondentům dostatečně vysvětlit a popsat jednotlivé kroky hodnocení.

Výsledek hodnocení primárních aktiv musí být zaznamenán, nejlépe i s odůvodněním, proč byly zvoleny dané hodnoty. Toto odůvodnění je užitečné zejména při aktualizaci a zpětné dohledatelnosti.

Jedním ze způsobů, jak lze hodnocení primárních aktiv provést, je vytvořit dopadovou tabulku dle jednotlivých oblastí se scénáři (někdy také označována jako matice dopadu), která slouží jako vodítko pro garanty primárních aktiv, kteří samotné hodnocení provádějí.

V rámci hodnocení jednotlivých atributů (důvěrnost, integrita, dostupnost) je vhodné vytvořit jemnější členění podle závažnosti dopadu U důvěrnosti je hodnoceno, k jak velkému úniku informací došlo. U integrity je posuzováno, k jak velkým modifikacím došlo. U dostupnosti a ztráty dat jsou vytvářeny časové řezy (předem stanovené časové úseky, ve kterých posuzujeme, jaké hodnoty aktivum v daném úseku nabude).

Při volbě tohoto jemnějšího členění by měly být brány v úvahu specifické podmínky organizace a dodržováno hledisko reálnosti, např. pokud je pro organizaci kritická dostupnost, měla by se soustředit na časové řezy od řádu minut, a naopak pro ni nemá smysl posuzovat časové řezy v délce měsíců či let.

V průběhu hodnocení pak může odpovědný pracovník pokládat respondentům otázky jako např.:

- Jaký bude dopad na aktivum při porušení dostupnosti? Berme v potaz ten nejhorší možný scénář, a to celková nedostupnost aktiva v řádu měsíců. Představte si tedy, že vaše aktivum nebude vůbec dostupné a co tím pádem hrozí.
- Může to ovlivnit bezpečnost a zdraví osob? Pokud ano, jak závažné budou dopady?

- Má nedostupnost vliv na ochranu osobních údajů? Pokud ano, jak závažné budou dopady?
- Budou narušeny zákonné a smluvní povinnosti? Pokud ano, jak závažné budou dopady?
- Atd.

Toto se musí opakovat u všech atributů bezpečnosti podle jednotlivých oblastí.

Zásady pro hodnocení primárních aktiv

- Zamezit nadhodnocování a podhodnocování aktiv
- Brát v úvahu nejhorší možný scénář (reálný)
- Nebrat v úvahu zavedená bezpečnostní opatření
- Nezkoumat možné příčiny narušení bezpečnosti informací
- Neurčovat pravděpodobnost výskytu jednotlivých scénářů

Modelový příklad hodnocení primárních aktiv

Pro hodnocení dopadů primárních aktiv modelové organizace byla vytvořena dopadová tabulka včetně tabulek pro stanovení výsledného hodnocení jednotlivých atributů bezpečnosti informací.

Bylo rozhodnuto, že v rámci hodnocení primárních aktiv bude posuzována, důvěrnost, integrita, dostupnost a ztráta dat.

Tyto atributy jsou dále členěny na:

- důvěrnost: prozrazení v rámci organizace, prozrazení smluvním partnerům, prozrazení vně organizace,
- integrita: modifikace dat malého rozsahu, modifikace dat velkého rozsahu,
- nedostupnost: 15 min, 1 h, 4 h, 8 h, 16 h, 1 den, 2 dny, 1 týden, 14 dní, měsíc a více,
- ztráta dat od zálohy: 15 min, 1 h, 4 h, 8 h, 16 h, 1 den, 2 dny, 1 týden, 14 dní, úplná ztráta dat.

Hodnocení primárních aktiv bylo zaznamenáno do tabulky – Katalogu primárních aktiv. V průběhu hodnocení byly nejdříve identifikovány relevantní oblasti, např. ochrana osobních údajů, zákonné a smluvní povinnosti, finanční ztráty atd. a u těchto bylo provedeno hodnocení z pohledu důvěrnosti, integrity, dostupnosti a ztráty dat.

Např. během rozhovoru manažera kybernetické bezpečnosti s garantem primárního aktiva Seznam certifikovaných senzorů byla jako relevantní identifikována oblast Zákonné a smluvní povinnosti. Podle dopadové tabulky byla pro důvěrnost stanovena hodnota na úrovni nízká (1): může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností. Výsledek byl zaznamenán do Katalogu aktiv.

Přehled se všemi příslušnými tabulkami lze nalézt v Příloze 6: Vzorové hodnocení aktiv a rizik. V tomto dokumentu je pro přehlednost vybráno jen několik ilustračních příkladů.

Tabulka 11: Stupnice pro hodnocení aktiv

		Dostupnost													Ztráta									Důvěrnost			Integrita	
Výsledná hodnota		Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků s měsíčním vyhodnocováním	Nedostupnost 15 min	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (15 min)	Ztráta dat od zálohy (1 h)	Ztráta dat od zálohy (4 h)	Ztráta dat od zálohy (8 h)	Ztráta dat od zálohy (1 den)	Ztráta dat od zálohy (2 dny)	Ztráta dat od zálohy (1 týden)	Ztráta dat od zálohy (14 dní)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizace	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
0	**Nerelevantní**																											
1	**nízká**	96,16 %	Provozní doba pod SLA: minimálně určených 10 hodin v pracovní dny. Nezapočítávají se dny pracovního volna a dny pracovního klidu stanovené pro ČR. Např. r. 2018 má 250 pracovních dní, na bázi 10 hod. pod SLA denně, což dává max. měsíční výpadek 8,3 hod. při dostupnosti 96 % (vztaženo na dobu pod SLA).	Max. 8 hod., avšak pouze v rámci definované pracovní doby	1	1	1	1	1	1	2	2	2	nejvyšší hodnota									nejvyšší hodnota			nejvyšší hodnota	
2	**střední**	99,45 %	Provozní doba pod SLA: 24x7 (připravenost pro služby související s úplným el. podáním). Avšak určité služby, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu. To znamená, že el. podání bude obvykle fungovat nepřetržitě, ale reakce poskytovatele na nahlášené incidenty je omezena.	Max. 4 hod. na bázi 24x7	1	1	1	2	2	3	3	3	3															

		Dostupnost												Ztráta									Důvěrnost			Integrita	
Výsledná hodnota		Dostupnost	Provozní doba pod SLA	Přípustná doba kumulovaných výpadků s měsíčním vyhodnocováním	Nedostupnost 15 min	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (15 min)	Ztráta dat od zálohy (1 h)	Ztráta dat od zálohy (4 h)	Ztráta dat od zálohy (8 h)	Ztráta dat od zálohy (1 den)	Ztráta dat od zálohy (2 dny)	Ztráta dat od zálohy (1 týden)	Ztráta dat od zálohy (14 dní)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizace	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
3	**vysoká**	99,90 %	Provozní doba pod SLA: 24x7 (připravenost pro služby úplného el. podání). Určité služby, u nichž to lze předpokládat vzhledem k provozním aspektům, lze nabízet s omezením Provozní doby pod SLA na pracovní dny a vymezenou pracovní dobu.	Max. 43 min. na bázi 24x7	1	1	3	3	3	3	4	4	4	nejvyšší hodnota									nejvyšší hodnota			nejvyšší hodnota	
4	**kritická**	99,99 %	Plně fault-tolerantní systém s georedundancí a replikací transakčních dat. Smluvní penále při výpadku dostupnosti služby delší než celkem 52 minut za rok (odpovídá 99,99 %).	Jednotlivý výpadek max. 15 min. Max. kumulovaný roční výpadek 52 min. (odpovídá 99,99 %)	1-2	3-4																						

Způsob získání výsledné hodnoty dostupnosti na základě výše uvedené tabulky:

Výše uvedená tabulka je pouze orientační. Hodnoty nedostupnosti pro jednotlivé časové řezy u hodnoceného aktiva se nemusí přesně rovnat hodnotám uvedeným v této tabulce. Pro určení výsledné hodnoty dostupnosti je potřeba porovnat všechny údaje v tabulce uvedené a vybrat úroveň dostupnosti, která nejvíce odpovídá reálným potřebám při práci s aktivem.

Dopadová tabulka

Při přípravě dopadové tabulky byly oblasti týkající se ochrany osobních údajů upraveny na základě metodiky vydané Úřadem pro ochranu osobních údajů (dále jen „ÚOOÚ“). Tento postup byl zvolen z toho důvodu, že se povinnosti ZKB a VKB v tomto bodě prolínají s GDPR a může tak dojít k synchronizaci v rámci organizace. Metodiku lze nalézt na webových stránkách ÚOOÚ: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=46487.

Tabulka 12: Dopadová tabulka (matice dopadu)[10]

Úroveň		Ochrana osobních údajů – dopady na subjekty údajů (písmeno a) VKB)	Ochrana osobních údajů – finanční újma subjektů údajů (písmeno a) VKB)	Obchodní tajemství (písmeno a) VKB)	Zákonné a smluvní povinnosti (písmeno b) VKB)	Narušení vnitřních řídících a kontrolních činností (písmeno c) VKB)	Veřejný pořádek (písmeno d) VKB)	Finanční ztráty (písmeno d) VKB)	Zajišťování nezbytných nebo základních služeb[11] (písmeno e) VKB)	Narušení běžných činností (písmeno f) VKB)	Ztráta důvěryhodnosti (písmeno g) VKB)	Bezpečnost a zdraví osob (písmeno h) VKB)	Mezinárodní vztahy (písmeno i) VKB)	Dopad na uživatele IS nebo KS (písmeno j) VKB)	Trestně-právní řízení (nad rámec VKB)
1	**nízká**	Může vést k **nepohodlí subjektu osobních údajů** (podrážděnost, krátkodobé časové nároky pro opětovné zadávání údajů, nutnost další komunikace s organizací).	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	Může přímo nebo nepřímo vést ke **ztrátám menším než 0,05 %** ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit **drobné komplikace pro malé množství osob.**	K narušení běžných činností nedochází, nanejvýše ke **zvýšeným časovým nárokům** při provádění běžných činností.	Může **negativně ovlivnit vztahy** s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na **bezprostřední okolí** a **nebude mít dlouhé trvání**. Např. pro osobní údaje – nepříjemnosti s klienty, nutnost jednání s dalšími klienty, nutnost jednání s dalšími subjekty, negativní někdy i veřejná reakce subjektů údajů apod.	*žádné vodítko*	Může mít **negativní vliv na spolupráci organizace** se zahraniční společností. Např. pro osobní údaje – může vyvolat nutnost jednání mezi organizací a zahraničním partnerem o charakteristikách zpracování osobních údajů.	Může způsobit **krátkodobé nepříjemnosti** při používání IS nebo KS (zdržení a podráždění uživatelů, jiné zdravotní dopady na uživatele nehrozí).	*žádné vodítko*
2	**střední**	Může vést k **menší újmě subjektu osobních údajů** (stres, nepohodlí, drobné fyzické obtíže, nedostatek porozumění, omezení přístupu ke	Odhadovaná finanční **újma do 5000 Kč/subjekt údajů.**	Může mít **negativní dopad** na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou	Může zapříčinit **porušení interních předpisů a postupů**, nikoli však porušení zákonných a smluvních povinností, např. provozní důvody,	Může mít **negativní dopad** na řídící a kontrolní činnosti organizace.	Může zapříčinit rozsahem, formou nebo místem **omezené protesty (lokální nepokoje).**	Může přímo nebo nepřímo vést ke **ztrátám mezi 0,05 % a 2 %** ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit **omezení či narušení** nezbytných nebo základních služeb pro **malé množství osob,** může způsobit **krátkodobý**	Může **omezit** provádění běžných činností, **narušit řádné řízení nebo fungování** části nebo celé organizace.	Může **negativně ovlivnit vztahy** s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat **omezené zájmové skupiny nebo bude široká, avšak krátkodobá.** Např. pro osobní údaje – úbytek klientů o 10 % u organizace,	Může vést k **újmě** (ohrožení osobní bezpečnosti, svobody nebo zranění) **jedné nebo několika osob.**	Může vytvářet **negativní obraz organizace v jednom teritoriu, popř. v jednom státě**. Např. pro osobní údaje – může vést k dočasnému omezení	Může **negativně ovlivnit výkon činnosti** interního nebo externího uživatele IS nebo KS (např. zvýšené časové	Může vytvořit podmínky pro **páchání trestné činnosti** nebo může ztížit její vyšetřování.

[10] V Příloze 3: Zjednodušená dopadová tabulka lze najít zjednodušenou verzi dopadové tabulky.

[11] Nezbytnou službou se rozumí služba naplňující odvětvová a průřezová kritéria podle nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury nebo služba naplňující kritéria dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Základní službou se rozumí služba naplňující odvětvová a dopadová kritéria podle vyhlášky č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby.

Úroveň		Ochrana osobních údajů – dopady na subjekty údajů (písmeno a) VKB)	Ochrana osobních údajů – finanční újma subjektů údajů (písmeno a) VKB)	Obchodní tajemství (písmeno a) VKB)	Zákonné a smluvní povinnosti (písmeno b) VKB)	Narušení vnitřních řídících a kontrolních činností (písmeno c) VKB)	Veřejný pořádek (písmeno d) VKB)	Finanční ztráty (písmeno d) VKB)	Zajišťování nezbytných nebo základních služeb[11] (písmeno e) VKB)	Narušení běžných činností (písmeno f) VKB)	Ztráta důvěryhodnosti (písmeno g) VKB)	Bezpečnost a zdraví osob (písmeno h) VKB)	Mezinárodní vztahy (písmeno i) VKB)	Dopad na uživatele IS nebo KS (písmeno j) VKB)	Trestně-právní řízení (nad rámec VKB)
		službám organizace nebo jiných subjektů, časové nároky spojené s řešením dopadů).		nebo alespoň potenciální materiální či nemateriální hodnotu.	nedostatek zaměstnanců.				**výpadek** služeb organizace. Může způsobit méně závažné finanční ztráty.		krátkodobé omezení přístupu ke službám využívaným správcem, negativní, avšak krátkodobé ohlasy v médiích.		zahraniční participace na zpracování osobních údajů.	nároky, stres uživatelů, drobné fyzické a zdravotní obtíže uživatelů).	
3	**vysoká**	Může vést k **závažné újmě subjektu osobních údajů** (napadení, nepříznivý zdravotní stav, deprese, ztížené uplatnění, ekonomické znevýhodnění (černé listiny), krádež identity, předvolání vyšetřujícími orgány).	Odhadovaná finanční **újma od 5000 Kč do 50 000 Kč/subjekt údajů** (zneužití finančních prostředků subjektu údajů, poškození majetku).	Může mít **podstatný dopad** na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu.	Může zapříčinit **správní nebo občanskoprávní řízení** vedoucí k pokutě nebo k náhradě škody.	Může mít **podstatný dopad** na řídicí a kontrolní činnosti organizace a zapříčinit **dočasné zastavení chodu či podstatný zásah do fungování organizace**, značné finanční ztráty související s obnovením chodu.	Může zapříčinit rozsahem, formou nebo místem **omezené protesty na úrovni významné části správního území obce s rozšířenou působností,** jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může přímo nebo nepřímo vést ke **ztrátám vyšším než 2 % a nižším či rovným 10 %** ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit **závažné omezení či narušení** nezbytných nebo základních služeb **pro větší množství osob, omezení** nebo **krátkodobé zastavení** přístupu ke službám.	Může způsobit **dočasné zastavení nebo podstatné narušení** běžných činností organizace nebo **poškodit** rozvoj nebo prosazování cílů a zájmů organizace.	Může **závažně ovlivnit vztahy** s jinými organizacemi nebo veřejností s následkem **celostátní negativní publicity. Např. pro osobní údaje – úbytek klientů 10-50 % u organizace, masivní negativní, avšak krátkodobé ohlasy v médiích.**	Může vést k **újmě** (ohrožení osobní bezpečnosti, svobody nebo zranění) **větší skupiny osob, nebo ohrožení na životě jednotlivců.**	Může vytvářet **negativní obraz organizace ve světě.** Např. pro osobní údaje – může být spojené s trvalým nebo dlouhodobým omezením participace zahraničních partnerů na zpracování osobních údajů.	Může způsobit **závažné krátkodobé omezení výkonu činnosti** interního nebo externího uživatele IS nebo KS (zhoršení zdravotního stavu uživatelů, krátkodobá pracovní neschopnost).	Může vést k **narušení vyšetřování trestné činnosti** nebo soudního řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).
4	**kritická**	Může vést k **velmi vážné újmě subjektu osobních údajů, přímému ohrožení či ztrátě života** (smrt, invalidita, dlouhodobě	Odhadovaná finanční **újma od 50 000 Kč/subjekt údajů** (neschopnost splácet dluh, ztráta majetku).	Může mít **závažný dopad** na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají	Může zapříčinit **porušení právních předpisů** vedoucí k zahájení trestního stíhání.	Může mít **závažný dopad** na řídicí a kontrolní činnosti a zapříčinit **dlouhodobé zastavení chodu** celé organizace.	Může zapříčinit **hromadné nepokoje,** např. generální stávku, nebo jinak závažně narušit veřejný pořádek s	Může přímo nebo nepřímo vést ke **ztrátám přesahujícím 10 %** ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit **rozsáhlé dlouhodobé omezení, narušení či nedostupnost** poskytování nezbytných nebo základních služeb pro	Může způsobit **dlouhodobé zastavení** běžných činností organizace.	Může **závažně a dlouhodobě ovlivnit vztahy** s jinými organizacemi nebo veřejností s následkem **celostátní či nadnárodní negativní publicity, s dlouhodobými účinky** a požadavky přijetí politické odpovědnosti. **Např.**	Může vést k **přímému ohrožení či ztrátě života** osob.	Může **negativně ovlivnit nebo poškodit diplomatické vztahy** a tím způsobit nevýhodu pro zájmy **ČR**. Např. pro osobní údaje – dlouhodobé	Může způsobit **závažné dlouhodobé omezení výkonu činnosti** interního nebo externího uživatele IS nebo KS	Může vést k **závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost,** popřípadě zpochybnění soudních řízení a

Úroveň	Ochrana osobních údajů – dopady na subjekty údajů (písmeno a) VKB)	Ochrana osobních údajů – finanční újma subjektů údajů (písmeno a) VKB)	Obchodní tajemství (písmeno a) VKB)	Zákonné a smluvní povinnosti (písmeno b) VKB)	Narušení vnitřních řídících a kontrolních činností (písmeno c) VKB)	Veřejný pořádek (písmeno d) VKB)	Finanční ztráty (písmeno d) VKB)	Zajišťování nezbytných nebo základních služeb[11] (písmeno e) VKB)	Narušení běžných činností (písmeno f) VKB)	Ztráta důvěryhodnosti (písmeno g) VKB)	Bezpečnost a zdraví osob (písmeno h) VKB)	Mezinárodní vztahy (písmeno i) VKB)	Dopad na uživatele IS nebo KS (písmeno j) VKB)	Trestně-právní řízení (nad rámec VKB)
	nepříznivý zdravotní stav a pracovní neschopnost, ztráta zaměstnání, velmi ztížené uplatnění, vyloučení, omezení práv).		skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu.			celostátními dopady.		**větší množství osob, může způsobit újmu** (např. soudní proces, likvidace, vznik nesplatitelného dluhu).		**pro osobní údaje – úbytek klientů nad 50 % u organizace, černé listiny, ztráta konkurenceschopnosti, masivní negativní dlouhodobé ohlasy v médiích včetně zahraničních.**		nebo trvalé omezení participace zahraničních subjektů nebo i států na zpracování osobních údajů.	(útoky na uživatele, odchod zaměstnanců, dlouhodobá pracovní neschopnost uživatelů, úmrtí).	rozhodnutí (závažná kriminalita, celkové zpochybnění systému).
Popis kategorie	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv přímo na subjekty údajů, tedy na jednotlivé osoby, jejichž údaje jsou v daném IS zpracovávány. Jak moc budou jednotlivé osoby po fyzické nebo psychické stránce dotčeny, když budou narušeny jejich osobní údaje.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv přímo na subjekty údajů, tedy na jednotlivé osoby, jejichž údaje jsou v daném IS zpracovávány. Jaká finanční újma vznikne jednotlivým osobám, když budou narušeny jejich osobní údaje.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na ochranu obchodního tajemství organizace.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na plnění zákonných a smluvních povinností, kterými je organizace zavázána.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na vnitřní řídící a kontrolní činnosti organizace (kontrolní mechanismy organizace, její vedení, správu apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajištění veřejného pořádku.	V této kategorii je posuzováno, jak velké finanční ztráty může narušení primárních aktiv organizaci způsobit. Kategorie je relevantní zejména pro organizace generující zisk.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování nezbytných nebo základních služeb.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na zajišťování běžných činností organizace (schopnost komunikovat v rámci organizace a mimo ni, přijímat zaměstnance apod.).	V této kategorii je posuzováno, jak narušení primárních aktiv ovlivní důvěryhodnost (reputaci) organizace.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na bezpečnost a zdraví osob.	V této kategorii je posuzováno, jak narušení primárních aktiv ovlivní mezinárodní vztahy organizace, případně také celého státu např. s EU, NATO nebo dalšími zahraničními zeměmi a mezinárodními organizacemi.	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na uživatele využívající daný IS nebo KS (neschopnost jeho činnosti apod.).	V této kategorii je posuzováno, jaký dopad bude mít narušení primárních aktiv na vyšetřování trestné činnosti nebo soudního řízení.
Příklady	Únik osobních údajů fyzické osoby z IS (např. o	Neoprávněná modifikace osobních údajů fyzické	Odcizení patentů evidovaných v IS	• Nemožnost vydání rozhodnutí v zákonné lhůtě z důvodu	Neúplnost či modifikace informací potřebných	•Nedostupnost informací zveřejňovaných na webu organizace	• Nedostupnost informací o fakturách na základě	Narušení všech informací, procesů a služeb vztažených	• Narušení činností personálních, ekonomických, správy	Vlivem úniku citlivých informací organizace na internet bude	V důsledku nedostupnosti informací evidovaných v	Únik informací, které organizace získala od	Ztráta možnosti přístupu uživatele ke službě	Z důvodu úniku informací v policejním IS v rámci

Úroveň	Ochrana osobních údajů – dopady na subjekty údajů (písmeno a) VKB)	Ochrana osobních údajů – finanční újma subjektů údajů (písmeno a) VKB)	Obchodní tajemství (písmeno a) VKB)	Zákonné a smluvní povinnosti (písmeno b) VKB)	Narušení vnitřních řídících a kontrolních činností (písmeno c) VKB)	Veřejný pořádek (písmeno d) VKB)	Finanční ztráty (písmeno d) VKB)	Zajišťování nezbytných nebo základních služeb[11] (písmeno e) VKB)	Narušení běžných činností (písmeno f) VKB)	Ztráta důvěryhodnosti (písmeno g) VKB)	Bezpečnost a zdraví osob (písmeno h) VKB)	Mezinárodní vztahy (písmeno i) VKB)	Dopad na uživatele IS nebo KS (písmeno j) VKB)	Trestně-právní řízení (nad rámec VKB)
	zdravotním stavu apod.) a jejich následné zveřejnění na internetu.	osoby v IS způsobí výplatu sociálních dávek jiné fyzické osobě.	konkurenční firmou.	nedostupnosti IS. • Narušení povinnosti zveřejňovat dokumenty na elektronické úřední desce, která je nepřetržitě dostupná vzdáleným přístupem.	h pro rozhodování vedení a kontrolní činnost.	může vést k neinformování veřejnosti o důležitých skutečnostech (záplavy, ekologické katastrofy atd.). • Dlouhodobá nedostupnost informací potřebných pro výplatu sociálních dávek, důchodů apod.	nedostupnosti ekonomického systému. • Nedostupnost informací o možných obchodních příležitostech a z toho plynoucí ušlý zisk.	směrem k hlavnímu business cíli (účelu existence) organizace (např. v případě Ministerstva pro certifikaci senzorů by se jednalo o narušení vydávání certifikací).	budov a autoparku, neschopnost přijímat datové zprávy apod. • Neschopnost přijímat nové zaměstnance z důvodu nedostupnosti personálního systému.	narušena její reputace.	nemocničním IS není možné provést nezbytné operace a pacienti jsou ohroženi na životě.	zahraničních partnerů.	vlivem její nedostupnosti (např. při výpadku internetového bankovnictví se tento problém dotkne velkého počtu uživatelů – nemožnost zadat platební příkaz online).	trestního řízení bude zastaveno trestní řízení.

Tabulka 13: Katalog primárních aktiv modelové organizace

ID	Typové primární aktivum	Název	Kategorie	Specifikace	Gestor aktiva	Garant aktiva	Osobní údaje	Legislativa	Určený IS	Rozsah ISMS	Dostupnost	Ztráta	Důvěrnost	Integrita
S1	Služba certifikace senzorů	S1: Služba certifikace senzorů	služba	Zajištění procesu certifikace a evidence senzorů	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	ano	Zákon o certifikaci	ano	ano	3	4	3	3
P1	Seznam certifikovaných senzorů	P1: Seznam certifikovaných senzorů	informace	Seznam všech úspěšně certifikovaných senzorů a certifikátů samotných	náměstek sekce certifikací (Martin Novotný)	ředitelka odboru podpory (Renata Malá)	ne	Zákon o certifikaci	ano	ano	2	1	1	3

ID	Typové primární aktivum	Název	Kategorie	Specifikace	Gestor aktiva	Garant aktiva	Osobní údaje	Legislativa	Určený IS	Rozsah ISMS	Dostupnost	Ztráta	Důvěrnost	Integrita
P2	Rozhodnutí	P2: Rozhodnutí	informace	Výsledné rozhodnutí certifikačního procesu – negativní i pozitivní	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	ano	Zákon o certifikaci, zákon č. 500/2004 Sb., správní řád	ano	ano	2	3	3	3
P3	Žádosti, technická dokumentace	P3: Žádosti, technická dokumentace	informace	Technická dokumentace a žádost o certifikaci, kterou zasílají jednotliví výrobci ke svým senzorům	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	ano	Zákon o certifikaci	ano	ano	3	3	3	3
P4	Informace o průběhu certifikace	P4: Informace o průběhu certifikace	informace	Informace o průběhu certifikace – kdo rozhodl, kdy došla žádost, průběh certifikace atd.	náměstek sekce certifikací (Martin Novotný)	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	ano	Zákon o certifikaci, zákon č. 500/2004 Sb., správní řád	ano	ano	3	4	3	3

Tabulka 14: Tabulka výsledného hodnocení primárního aktiva Služba certifikace senzorů

Název primárního aktiva:	Služba certifikace senzorů	
Gestor primárního aktiva:	náměstek sekce certifikací (Martin Novotný)	
Garant primárního aktiva:	ředitel odboru certifikací 1 (Jan Novák), ředitelka odboru certifikací 2 (Tereza Černá)	
Datum hodnocení:	02.11.2020	
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	*Dostupnost*	3
	Ztráta	4
	Důvěrnost	3
	Integrita	3

Tabulka 15: Tabulka hodnocení primárního aktiva Služba certifikace senzorů

	Dostupnost									Ztráta									Důvěrnost			Integrita	
Oblasti dopadu	Nedostupnost 15 min	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1den	Nedostupnost 2 dny	Nedostupnost 1 týden	Nedostupnost 14 dní	Nedostupnost měsíc a více	Ztráta dat od zálohy (15 min)	Ztráta dat od zálohy (1 h)	Ztráta dat od zálohy (4 h)	Ztráta dat od zálohy (8 h)	Ztráta dat od zálohy (1 den)	Ztráta dat od zálohy (2 dny)	Ztráta dat od zálohy (1 týden)	Ztráta dat od zálohy (14 dní)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizace	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
Ochrana osobních údajů – dopady na subjekty osobních údajů	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
Ochrana osobních údajů – finanční újma subjektů údajů	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
Obchodní tajemství	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Zákonné a smluvní povinnosti	1	1	1	1	1	2	2	2	3	1	1	1	1	1	2	2	2	2	2	3	3	3	3
Narušení vnitřních řídících a kontrolních činností	1	1	1	1	1	2	2	2	3	1	1	1	1	1	2	2	2	2	1	1	1	3	3
Veřejný pořádek	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Finanční ztráty	1	1	1	1	1	2	2	2	3	1	1	1	1	1	2	2	2	2	2	3	3	3	3
Zajišťování nezbytných nebo základních služeb	1	1	1	1	1	2	2	2	3	1	1	1	1	1	2	2	2	2	1	1	1	3	3
Narušení běžných činností	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ztráta důvěryhodnosti	1	1	1	1	1	2	2	2	3	1	1	1	1	1	2	2	2	2	1	2	3	3	3
Bezpečnost a zdraví osob	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Dopad na uživatele IS nebo KS	1	1	2	3	3	3	4	4	4	1	1	1	1	1	3	3	3	4	1	1	1	3	3
Mezinárodní vztahy	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Trestně-právní řízení	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Komentář k dopadům *(uveďte odůvodnění k následkům narušení dostupnosti-odkdy a proč začíná mít nedostupnost negativní dopad, narušení důvěrnosti-např. porušení pravidel obecného nařízení GDPR, narušení integrity dat-např. chyba při zpracování dat agendy)*	Hodnoty služby certifikace senzorů jsou nejvyšší hodnoty, které byly stanoveny pro jednotlivá primární aktiva P1-P4.

4.2 Podpůrná aktiva

Jedná se o aktiva nutná pro správnou funkčnost, zpracování, uchování a zajištění bezpečnosti primárních aktiv. Sama o sobě podpůrná aktiva netvoří hodnotu pro organizaci. Podpůrná aktiva jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti IS.

Technickým aktivem je takové technické vybavení, komunikační prostředky, programové vybavení IS a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na IS.

Možné kategorie podpůrných aktiv

- Technické vybavení
- Komunikační prostředky
- Programové vybavení
- Objekty
- Lidské zdroje
- Dodavatelé
- Externí systémy a služby

Technické vybavení

Do technického vybavení (HW) spadají fyzické komponenty (zpravidla si na ně můžeme sáhnout) IS nebo jejich části. Typickými příklady technického vybavení jsou pracovní stanice (včetně periferií), datová úložiště, servery, ale také mobilní zařízení. Do této kategorie též spadají výměnná média (včetně CD, DVD apod.).

Komunikační prostředky

Do komunikačních prostředků spadají komponenty, které spojují jednotlivá technická vybavení dohromady a vytváří z nich síť. Do této kategorie jsou zahrnuta jak drátová (ethernet, optické vlákno atd.), tak i bezdrátová (Wi-Fi atd.) připojení a veškeré komponenty, které jsou potřebné pro realizaci těchto připojení – tedy mimo aktivních prvků, např. síťová zařízení jako jsou směrovače (router), přepínače (switch) apod.

Programové vybavení

Do programového vybavení (SW) spadají veškeré programy/aplikace, které běží na technickém vybavení a komunikačních prostředcích. Bez nich by technické vybavení a komunikační prostředky byly pouze kusem železa bez využití. Programové vybavení zajišťuje, že je možné technické vybavení a komunikační prostředky ovládat a vykonávat na nich požadované úkony. Do této kategorie jsou zahrnuty např. OS, firmware, kancelářské balíky, ale i přístupové a bezpečnostní aplikace apod.

Objekty

Do objektů spadají fyzické prostory, ve kterých se IS nebo jeho části nachází. Do této kategorie spadají areály, objekty, inženýrské sítě apod.

Lidské zdroje

Do lidských zdrojů spadá veškerý personál, který má vliv na IS nebo jeho části. Do této kategorie jsou zahrnuti např. uživatelé, administrátoři, vývojáři, bezpečnostní role, ale také vedení organizace nebo administrátoři dodavatele.

Dodavatelé

Do kategorie dodavatelů spadají např. provozovatelé, subdodavatelé, výrobci nebo cloud computing.

Externí systémy a služby

Do externích systémů a služeb spadají veškeré externí systémy a služby, které jsou nezbytné pro zajištění funkčnosti IS nebo jeho částí. Do této kategorie jsou zahrnuty např. dodávky elektřiny, certifikační služby apod.

Podpůrná aktiva mohou být velmi komplexní a spadat do více z těchto kategorií, pro potřeby navazujících činností, např. hodnocení aktiv a rizik, je možné vytvořit jedno typové aktivum, které bude obsahovat více kategorií. V navazujícím hodnocení rizik je ale **nutné identifikovat relevantní hrozby a zranitelnosti pro všechny kategorie** příslušného typového aktiva**.**

4.2.1 Identifikace podpůrných aktiv

Při identifikaci podpůrných aktiv je nutné vycházet z architektury systému a potřeby pro funkčnost primárního aktiva. Je možné inspirovat se kategoriemi výše a klást následující otázky:

- Co je potřeba k tomu, aby primární aktivum bylo dostupné?
- Kdo se o aktiva stará?
- Kdo jsou uživatelé/původci primárních aktiv?
- Které role využívají primární aktiva?
- Kde všude jsou primární aktiva umístěna?
- Kdo je zodpovědný za technickou správu?
- Kdo je dodavatel jednotlivých skupin podpůrných aktiv?
- Kdo má celkové povědomí o podpůrném aktivu?
- Kdo je odpovědný za podpůrné aktivum?

Co se týče míry detailu podpůrných aktiv, organizace by měla zvolit takový detail, aby byla schopna adekvátně identifikovat a řídit rizika s aktivy spojená.

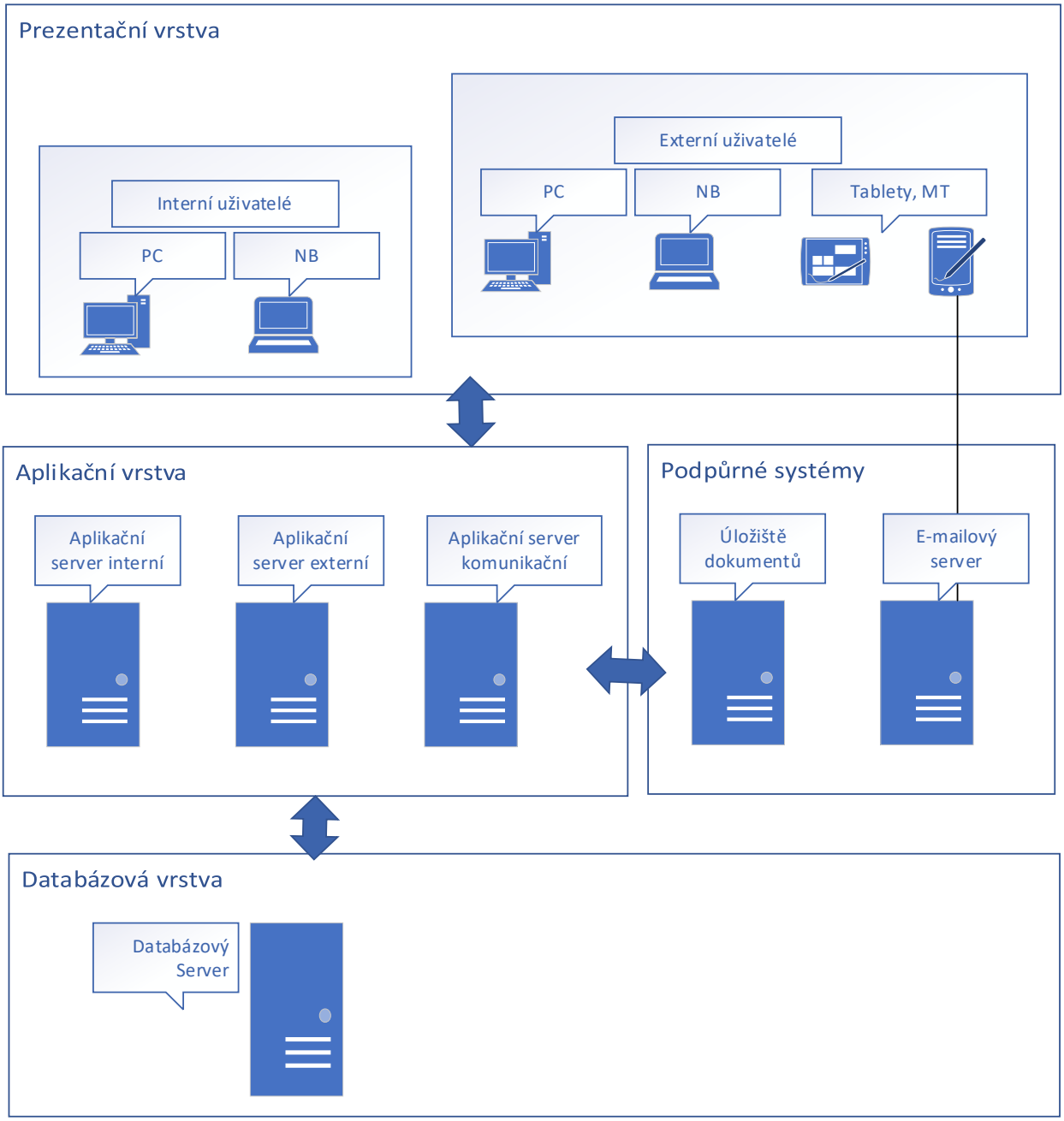
Pokud je detail příliš malý (např. celá budova), budou se muset řídit rizika i pro její nerelevantní součásti. Tento přístup často vede ke zvýšeným nákladům, neboť rozlišovací schopnost hodnocení rizik je potlačena a bezpečnostní opatření jsou zaváděna plošně. Současně je identifikace vhodných bezpečnostních opatření mnohem náročnější u rizik, která vznikla obecně definovanou kombinací aktivum-zranitelnost-hrozba.

Pokud je detail příliš velký, vzniká velké množství podpůrných aktiv. V tomto případě je zde hrozba nedostatečných kapacit pro jejich adekvátní řízení.

Modelový příklad identifikace podpůrných aktiv

Agendový systém modelové organizace je založen na třívrstvé architektuře (Three-tier architecture).

Následující obrázek zobrazuje architekturu modelového systému:



Obrázek 7: Architektura agendového systému modelové organizace

Následující tabulka popisuje agendový systém modelové organizace:

Tabulka 16: Popis agendového systému ministerstva

Oblast	Popis
Serverová infrastruktura (HW prostředí)	• HW DB serveru (1x standalone Server) • HW aplikačního serveru (3x standalone Server)
Serverová infrastruktura (operační systémy)	• operační systémy databázové vrstvy (OS Linux) • operační systémy aplikační vrstvy (OS Windows)
Databázové prostředí	• standardní DB prostředí od známého výrobce
Aplikační infrastruktura	• standardní DB prostředí od známého výrobce
Vývojové prostředí	• oddělené vývojové prostředí u dodavatele A
Uživatelé systému – interní	• interní uživatelé pracují na PC a NB s Windows 10, cca 1/4 na Windows 7 • jedná se o 1400 zaměstnanců
Uživatelé systému – externí	• externí uživatelé se mohou hlásit pouze pomocí Internet Explorer • jedná se o cca 300 žadatelů
Identita	• interní a registrovaní uživatelé jsou vedeni pomocí MS Active directory • licence 1. - 1400 interní uživatelů, licence 2. - 300 externích uživatelů
Síťová infrastruktura	• jsou standardizovány aktivní prvky velkého světového výrobce • typ 1. - velké L3 switche, cca 10 ks • typ 2. - malé L2 switche, cca 50 ks
Segmentace sítě	• jsou zavedeny VLAN
Ochrana perimetru a DMZ	• je použit nový NGFW v HA režimu
Ochrana před škodlivým kódem	• na Windows Serverech je provozován antivirový SW • na Linux serverech není provozován antivirový SW • na PC a NB interních uživatelů je provozován antivirový SW
Logování událostí	• log registrovaného systému je pouze lokální ve správě Dodavatele A • log doménového kontroleru pro přihlašování uživatelů ve správě Odboru ICT
Fyzická bezpečnost	• v areálu ministerstva je jedna serverovna • rackové skříně rozmístěny po areálu
Zálohování a obnovení systému	• zálohování je prováděno standardními prostředky
Monitoring	• administrátor vykonává dohled nad serverovou infrastrukturou
Vzdálený přístup	• dodavatel A má vzdálený přístup
Kontrola administrátorů	• možná pouze na žádost ministerstva, Dodavatel A musí dodat logy, které lze potom ad hoc zkontrolovat
Dokumentace systémů	• vývojová dokumentace, testovací a provozní dokumentace, školící dokumentace pro uživatele
Školení uživatelů pro práci s aplikací	• školení absolvují pouze vybraní klíčoví uživatelé, kteří musí proškolit ostatní

Na základě těchto informací byla identifikována typová podpůrná aktiva agendového systému. Jako inspirace byla využita obecná struktura podpůrných aktiv (viz Příloha 4: Struktura podpůrných aktiv), která byla upravena pro potřeby modelové organizace (upravenou strukturu podpůrných aktiv je možné nalézt na listu Struktura podpůrných aktiv v Příloze 6: Vzorové hodnocení aktiv a rizik).

Na identifikaci podpůrných aktiv mělo vliv také varování NÚKIB (viz kapitola 7.1.1 Zohlednění varování NÚKIB ze dne 17. prosince 2018).

4.2.2 Evidence podpůrných aktiv

Stejně jako všechna primární aktiva, je nezbytné zaznamenat i podpůrná aktiva. U podpůrných aktiv je vhodné evidovat tyto údaje:

- ID aktiva,
- název,
- garant aktiva,
- hodnocení aktiva z hlediska důvěrnosti, integrity a dostupnosti,
- detailní popis – v případě, že se jedná o typové aktivum tak i specifikace toho, co zahrnuje,
- další informace o aktivu – např. kdo jsou jeho uživatelé, jaké agendy jej využívají, jaké mají dodavatele, zda se jedná o významné dodavatele či provozovatele atd.

K evidenci všech podpůrných aktiv jsou často využívány konfigurační databáze nebo jiné Asset Management nástroje.

Pro potřeby řízení aktiv a rizik je nutná evidence na úrovni typových podpůrných aktiv.

Modelový příklad evidence podpůrných aktiv

Následující tabulka obsahuje ukázku z Katalogu podpůrných aktiv (katalog lze nalézt v Příloze 6: Vzorové hodnocení aktiv a rizik).

Tabulka 17: Ukázka z Katalogu podpůrných aktiv

ID	Kategorie podpůrného aktiva	Skupina podpůrného aktiva	Typové podpůrné aktivum	Název	Popis podpůrného aktiva	Gestor aktiva	Garant aktiva
PO1	Technické vybavení (HW)	Servery	Aplikační server (HW)	PO1: Aplikační server (HW)	2x standalone Server	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu síťové infrastruktury (Aleš Pokorný)
PO2	Technické vybavení (HW)	Servery	Databázový server (HW)	PO2: Databázový server (HW)	1x standalone Server	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu síťové infrastruktury (Aleš Pokorný)
PO3	Technické vybavení (HW)	Servery	Webový server (HW)	PO3: Webový server (HW)	1x standalone Server, servery výrobce, na nějž se vztahuje varování NÚKIB ze 17.12.2018	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu síťové infrastruktury (Aleš Pokorný)
PO4	Programové vybavení (SW)	Systémový SW	Operační systém – aplikační server	PO4: Operační systém – aplikační server	2x standalone Server, licence	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu aplikační infrastruktury (Tomáš Fiala)

ID	Kategorie podpůrného aktiva	Skupina podpůrného aktiva	Typové podpůrné aktivum	Název	Popis podpůrného aktiva	Gestor aktiva	Garant aktiva
PO5	Programové vybavení (SW)	Systémový SW	Operační systém – databázový server	PO5: Operační systém – databázový server	1x standalone Server, licence	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu aplikační infrastruktury (Tomáš Fiala)

Modelová organizace v Katalogu podpůrných aktiv eviduje také informace o tom, zda je aktivum součástí určeného IS nebo rozsahu ISMS. Přičemž aktiva, která jsou součástí určeného IS jsou zároveň automaticky součástí rozsahu ISMS.

Dále modelová organizace eviduje také významné dodavatele těchto podpůrných aktiv. Přičemž provozovatel je zároveň i významný dodavatel.

Obrázek 8: Schéma typů dodavatelů

4.2.3 Určení garantů podpůrných aktiv

Stejně jako primární aktiva musí mít podpůrná aktiva přiřazené a evidované garanty. Stanovení garantů podpůrných aktiv by mělo být zaznamenáno formalizovaným způsobem.

Určení jednotlivých garantů podpůrných aktiv je vhodné provést ve spolupráci manažera kybernetické bezpečnosti, garantů primárních aktiv a vedoucích oddělení pracovníků, kteří mají za podpůrná aktiva odpovědnost.

Garanty podpůrných aktiv mají být určeni pracovníci, kteří se podílí na provozu, rozvoji, správě a bezpečnosti daného podpůrného aktiva.

Garanty podpůrných aktiv bývají často konkrétní zaměstnanci IT, u podpůrných aktiv typu dodavatel to bývají zaměstnanci, kteří jsou odpovědní za daný smluvní vztah.

Modelový příklad určení garantů podpůrných aktiv

Stejně jako u primárních aktiv bylo i u podpůrných aktiv použito dvouúrovňové stanovení garantů aktiv – gestora a garanta aktiva (viz. Kapitola 3.1.4. Garant aktiva). Dále uvádíme několik příkladů stanovení gestorů a garantů podpůrných aktiv modelové organizace.

Většina podpůrných technických aktiv spadá do správy odboru ICT, proto byl u těchto aktiv jako gestor zvolen ředitel odboru ICT, který dále ve spolupráci s manažerem kybernetické bezpečnosti vytipoval vhodné osoby pro role garantů aktiv. Např. správu DB provádí oddělení provozu aplikační infrastruktury a garantem byl stanoven vedoucí tohoto oddělení.

Dodavatelům dodávajícím ICT prostředky byl rovněž jako gestor stanoven ředitel odboru ICT. Jako garanti byly určeny osoby, které mají vzhledem k náplni práce nejlepší předpoklady pro správný výkon

přidělených odpovědností této bezpečnostní role – osoby, které jsou odpovědné za smluvní vztah a slouží mj. jako kontaktní osoby pro dodavatele.

Podpůrná aktiva typu uživatelé jsou rozdělena na několik typů, např. správu externích žadatelů a další procesy, které se jich týkají má na starosti odbor podpory, a proto byla garantem stanovena jeho ředitelka.

4.2.4 Hodnocení podpůrných aktiv a určení vazeb mezi podpůrnými a primárními aktivy

Hodnocení podpůrných aktiv musí být v souladu s hodnocením primárních aktiv. Stejně jako u primárních aktiv je nutno provést jejich hodnocení a posoudit dopad narušení bezpečnosti informací – je tedy nutné tato aktiva hodnotit minimálně z pohledu důvěrnosti, integrity a dostupnosti. V rámci posuzování dopadu narušení dostupnosti je možné další rozdělení na nedostupnost a úplnou ztrátu dat. Dále je doporučeno, aby pro hodnocení aktiv byly použity stupnice o čtyřech úrovních. Při posuzování hodnoty aktiv je nutné uvažovat o nejhorším možném scénáři a nebrat v úvahu bezpečnostní opatření.

Při hodnocení podpůrných aktiv je klíčové zohlednit vazby mezi podpůrnými a primárními aktivy. Existuje několik variant, jak toho lze dosáhnout:

Varianta A: Podpůrná aktiva dědí hodnoty primárních aktiv

KLADY

+ Nejméně časově náročné,
+ lze jednoduše automatizovat.

ZÁPORY

- Hodnoty podpůrných aktiv mohou být značně zkreslené, může docházet k jejich nadhodnocení, v důsledku čehož mohou vznikat vyšší náklady při zavádění bezpečnostních opatření.

Varianta B: Podpůrná aktiva jsou posuzována individuálně s ohledem na hodnotu primárních aktiv

KLADY

+ Hodnocení podpůrných aktiv je nejpřesnější,
+ mohou být zohledněny specifické podmínky/situace.

ZÁPORY

- Časově a kapacitně náročné, u velkého množství aktiv může být vyčerpávající.

Varianta C: Podpůrná aktiva přebírají hodnoty primárních aktiv prostřednictvím vzorce

KLADY

+ Lze automatizovat.

ZÁPORY

- Vytvoření vhodného vzorce je komplikované.

Modelový příklad hodnocení podpůrných aktiv

Pro hodnocení podpůrných aktiv v rámci modelového příkladu byla zvolena varianta C v kombinaci s variantou B. Tzn. podpůrná aktiva byla hodnocena na základě vzorce, ale v některých případech došlo k individuálnímu přehodnocení podpůrného aktiva.

Pro podpůrná aktiva byla použita čtyřstupňová škála, byla hodnocena důvěrnost, integrita, dostupnost, a ztráta.

U těch podpůrných aktiv, která mají vazbu na primární aktivum, byla hodnocena tzv. váha vlivu. Váha vlivu je číselně ohodnocena síla vazby mezi primárním a podpůrným aktivem, přičemž váha vlivu je posuzována individuálně pro jednotlivé atributy bezpečnosti informací (důvěrnost, integrita, dostupnost a ztráta) a individuálně pro každou dvojici primárního a podpůrného aktiva.

Váha vlivu nabývá hodnot podle následující tabulky:

Tabulka 18: Váha vlivu

Úroveň		Popis
1	Nízká	Hodnocený atribut bezpečnosti informací nemá vliv na stejný atribut daného primárního aktiva.
2	Střední	Hodnocený atribut bezpečnosti informací má vedlejší vliv na stejný atribut daného primárního aktiva.
3	Vysoká	Hodnocený atribut bezpečnosti informací má hlavní vliv na stejný atribut daného primárního aktiva, může způsobit významnou škodu.
4	Kritická	Hodnocený atribut bezpečnosti informací má kritický vliv na stejný atribut daného primárního aktiva, může způsobit jeho znehodnocení.

Následně došlo k výpočtu dopadu podpůrného aktiva pro jednotlivé atributy bezpečnosti informací, který je dán následujícím vzorcem:

Hodnota podpůrného aktiva = váha vlivu x hodnota primárního aktiva

Vzhledem k tomu, že podpůrné aktivum může mít více vazeb na primární aktiva, je pro účely hodnocení podpůrných aktiv vybrána nejvyšší hodnota dle jednotlivých atributů bezpečnosti informací.

Dopad podpůrného aktiva je hodnota v intervalu <1-16>, musí tedy dojít k úpravě výsledné hodnoty podpůrného aktiva na čtyřstupňovou škálu použitou pro primární aktiva. Tato úprava je dána následující tabulkou:

Tabulka 19: Hodnota podpůrného aktiva

Hodnota podpůrného aktiva = váha vlivu x hodnota primárního aktiva		Hodnota primárního aktiva			
		1	2	3	4
Váha vlivu podpůrného aktiva na primární aktivum	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

Výsledná hodnota podpůrného aktiva	
1-4	1
5-8	2
9-12	3
13-16	4

Nakonec byla vybraná aktiva individuálně přehodnocena.

Seznam hodnocených podpůrných aktiv viz Příloha 6: Vzorové hodnocení aktiv a rizik.

4.3 Klasifikace informací

Na základě hodnocení aktiv lze určit možné způsoby zacházení s jednotlivými aktivy, které obsahují informace a stanovit možné způsoby likvidace dat pro jednotlivé úrovně aktiv. Způsoby zacházení s jednotlivými aktivy by měly být zvoleny přiměřeně k jednotlivým úrovním aktiv. Klasifikaci informací by měl provést odpovědný garant aktiva nebo původce informace.

Příkladem pro klasifikaci informací může být příloha č. 1 VKB (možné způsoby ochrany aktiv), která odkazuje i do přílohy č. 4 VKB (likvidace dat) a použití např. TLP pro sdílení informací.

Systém označování informací pomocí TLP nenahrazuje náležitosti označování a nakládání s utajovanými informacemi ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Další informace, včetně podmínek použití lze nalézt na webových stránkách NÚKIB: https://www.nukib.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/.

Modelový příklad klasifikace informací

Modelová organizace má na základě hodnocení aktiv zpracován dokument Příloha 5: Vzorová pravidla ochrany jednotlivých úrovní aktiv.

4.4 Pravidla pro nakládání s aktivy

Pravidla pro manipulaci a evidenci aktiv platí pro všechna aktiva, která obsahují informace. Týká se to tedy i listinných dokumentů a médií. Aktiva jsou označována v souladu s nastavenými pravidly podle jejich klasifikace.

Modelový příklad pravidel pro nakládání s aktivy

Modelová organizace má na základě hodnocení aktiv zpracován dokument Příloha 5: Vzorová pravidla ochrany jednotlivých úrovní aktiv.

4.5 Likvidace dat

Pro likvidaci dat jsou v příloze č. 4 VKB definovány způsoby mazání dat a způsoby likvidace technických nosičů informace, provozních údajů, informací a jejich kopií. Tato tabulka je rozdělena do 4 úrovní podle důvěrnosti informací. Pravidla pro likvidaci dat by měla být stanovena přiměřeně hodnotě a důležitosti aktiv.

Modelový příklad likvidace dat

Modelová organizace má na základě hodnocení aktiv zpracován dokument Příloha 5: Vzorová pravidla ochrany jednotlivých úrovní aktiv.

5 Řízení rizik v oblasti kybernetické bezpečnosti

Veškerý postup týkající se hodnocení rizik musí být v dokumentované podobě – **metodice pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik.** Metodika by měla být dostatečně návodná, srozumitelná a jednoznačná tak, aby byl celý proces opakovatelný, přezkoumatelný a vedl za stejných podmínek ke stejným výsledkům bez závislosti na konkrétní osobě.

Hodnocení rizik vs. Analýza rizik

Dle VKB v sobě hodnocení rizik zahrnuje identifikaci rizik, analýzu rizik a vyhodnocení rizik. Zatímco analýza rizik podle VKB znamená pouze ohodnocení kombinace hrozby a zranitelnosti s ohledem na aktiva a výpočet finální hodnoty.

V praxi se však pojem analýza rizik používá pro celý proces a jedná se tak de facto o synonymum pojmu hodnocení rizik, a ne jeho podmnožinu.

Modelový příklad řízení rizik

Ministerstvo řídí rizika na základě stanoveného rozsahu popsaného v dokumentu Příloha 1: Vzorová politika systému řízení bezpečnosti informací, dle platné metodiky Příloha 2: Vzorová metodika pro identifikaci a hodnocení aktiv a rizik a evidenci rizik je součástí Přílohy 6: Vzorové hodnocení aktiv a rizik.

5.1 Katalog zranitelností

Zranitelností se rozumí vlastnost aktiva, jeho slabina či nedostatek, který může být zneužit jednou či více hrozbami a generovat tak nežádoucí vliv. Jedná se o citlivost aktiva vzhledem ke konkrétní hrozbě.

Dle § 5 odst. 1 písm. b) VKB je nutné vytvořit katalog zranitelností a využít zejména její přílohu č. 3, která obsahuje vybrané kategorie zranitelností, které budou dále upraveny pro potřeby organizace.

- Nedostatečná údržba IS
- Zastaralost IS
- Nedostatečná ochrana vnějšího perimetru
- Nedostatečné bezpečnostní povědomí uživatelů a administrátorů
- Nevhodné nastavení přístupových oprávnění
- Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování
- Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí
- Nedostatečná ochrana aktiv
- Nevhodná bezpečnostní architektura
- Nedostatečná míra nezávislé kontroly

- Neschopnost včasného odhalení pochybení ze strany zaměstnanců
- Nedostatek zaměstnanců s potřebnou odbornou úrovní
- Další známé a relevantní zranitelnosti

Modelový příklad vytvoření katalogu zranitelností

Pro modelovou organizaci byly obecně definované zranitelnosti VKB doplněny o příklady konkrétních zranitelností a o kategorie aktiv, u kterých se tyto zranitelnosti mohou vyskytovat.

Následující tabulky pro ilustraci zobrazují první zranitelnost popsanou ve VKB, ostatní je možné najít v Příloze 2: Metodika pro identifikaci a hodnocení aktiv a hodnocení rizik a v Příloze 6: Vzorové hodnocení aktiv a rizik.

Tabulka 20: Ukázka z katalogu zranitelností

ID	Typové zranitelnosti	Označení	Příklady zranitelností	Technické vybavení (HW)	Programové vybavení (SW)	Komunikační prostředky	Objekty	Lidské zdroje	Dodavatelé a externí systémy a služby
1	Nedostatečná údržba aktiv	Z1: Nedostatečná údržba aktiv	1) Proces pro správu a řízení technických zranitelností není zdokumentován ani plně zaveden do praxe. Není používán nástroj pro řízení technických zranitelností. Není nasazena technologie pro skenování zranitelností. 2) Stává se, že seznam ICT komponent nově zaváděné techniky není kompletní, v organizaci se vyskytuje neevidovaný ICT HW. V případě krádeže je HW administrativně nedohledatelný. 3) Nedostatečná dokumentace interní sítě. 4) Pro testování jsou používaná produkční data. 5) Nejsou stanoveny priority obnovy informačních systémů ze zálohy. 6) Neprobíhá profylaxe a údržba. 7) Jsou vydávány aktualizace dodavatelem/výrobcem, ale nejsou aplikovány do provozního prostředí. 8) Neprobíhá pravidelné čištění skladových prostor, hromadí se hořlavý materiál. 9) Servery jsou zanášeny prachem a nejsou pravidelně čištěny. 10) Informace popsané v dokumentaci nejsou pravidelně aktualizovány. 11) Aktualizace nejsou dostatečně testovány před nasazením do provozního prostředí. 12) Nejsou odstraňovány nedostatky identifikované v průběhu skenování zranitelností nebo penetračního testování.	x	x	x	x		

5.2 Katalog hrozeb

Hrozbou se rozumí událost či aktivita, která má vliv na bezpečnost a může zapříčinit škodu. Hrozba může být úmyslná, neúmyslná či na základě vyšší moci.

Dle § 5 odst. 1 písm. b) VKB je nutné vytvořit katalog hrozeb a využít zejména její přílohu č. 3, která obsahuje vybrané kategorie hrozeb, které budou dále upraveny pro potřeby organizace.

- Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů
- Poškození nebo selhání technického anebo programového vybavení
- Zneužití identity
- Užívání programového vybavení v rozporu s licenčními podmínkami
- Škodlivý kód (například viry, spyware, trojské koně)
- Narušení fyzické bezpečnosti
- Přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie
- Zneužití nebo neoprávněná modifikace údajů
- Ztráta, odcizení nebo poškození aktiva
- Nedodržení smluvního závazku ze strany dodavatele
- Pochybení ze strany zaměstnanců
- Zneužití vnitřních prostředků, sabotáž
- Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb
- Cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik
- Zneužití vyměnitelných technických nosičů dat
- Napadení elektronické komunikace (odposlech, modifikace)
- Další známé a relevantní hrozby

V rámci modelové organizace došlo k přeřazení hrozby z přílohy č. 3 VKB „nedostatek zaměstnanců s potřebnou odbornou úrovní“ mezi zranitelnosti, protože modelová organizace nevnímá „nedostatek zaměstnanců s potřebnou odbornou úrovní“ jako hrozbu, která působí vůči zranitelnostem jednotlivých typů podpůrných aktiv, ale jako zranitelnost podpůrného aktiva typu lidské zdroje, kterou lze snížit vhodným opatřením. Zpravidla proti pravděpodobnosti hrozby není možné působit opatřením a zůstává v daném čase stejná, kdežto proti míře zranitelnosti působit opatřením lze.

Opatření působící proti hrozbě jsou zpravidla spojena se změnou podmínek, např. přesun datového centra ze záplavové oblasti do jiné lokality.

Modelový příklad vytvoření katalogu hrozeb

Stejně jako zranitelnosti byly hrozby pro modelovou organizaci doplněny o příklady konkrétních hrozeb. Dále byl katalog hrozeb doplněn o vektor útoku a zasažený atribut bezpečnosti v případě realizace hrozby.

Následující tabulky pro ilustraci zobrazují první hrozbu popsanou ve VKB, ostatní je možné najít v Příloze 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik a v Příloze 6: Vzorové hodnocení aktiv a rizik.

Tabulka 21: Ukázka z katalogu hrozeb

ID	Typové hrozby	Označení	Příklady hrozeb	Vektor útoku	Je relevantní varování NÚKIB ze dne 17. prosince 2018?	Dův.	Int.	Dost.
1	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	H1: Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů	1) Zaměstnanec nedodrží interní předpisy organizace. 2) Nedodržení zákonných předpisů dopadajících na organizaci. 3) Zaměstnanec nebo dodavatel záměrně poruší bezpečnostní politiku organizace. 4) Zaměstnanec nebo dodavatel záměrně eskaluje svá oprávnění. 5) Zaměstnanec nebo dodavatel do infrastruktury organizace připojí neschválený HW. 6) Zaměstnanec (vývojář) provede neoprávněné změny v aplikačním kódu a jiné změny vyvíjeného SW. 7) Zaměstnanec se seznámí s informacemi, které pro něj nebyly určeny. 8) Zaměstnanec sdílí informace s osobami, pro které nebyly určeny.	Interní/Externí	NE	x	x	x

5.3 Příprava scénářů

Dle VKB je nutné zohledňovat relevantní kombinace aktivum-zranitelnost-hrozba. Je logické, že všechna aktiva nemají stejné zranitelnosti a nepůsobí na ně stejné hrozby, např. zranitelnosti typu nedostatečné bezpečnostní povědomí uživatelů a administrátorů cílí na aktivum typu lidské zdroje, naopak zranitelnost zastaralost IS míří na technická aktiva. Stejná situace nastává i u hrozeb, např. hrozba porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů cílí na aktiva typu lidské zdroje a hrozba poškození nebo selhání technického nebo programového vybavení míří na technická aktiva.

Analogicky postupujeme i při hodnocení toho, zda má hrozba vliv na důvěrnost, integritu nebo dostupnost.

Z toho důvodu je klíčové správné vytváření typových aktiv tak, aby na jednotlivá aktiva ve skupině působily shodné hrozby a zranitelnosti a rozdíly v hodnocení z pohledu důvěrnosti, integrity a dostupnosti takových aktiv byly zanedbatelné.

Není účelné hodnotit takové kombinace, které z praktického pohledu nedávají smysl.

Z toho důvodu lze přistoupit k přípravě scénářů, které představují vhodné zkombinování hrozby a zranitelnosti.

Modelový příklad vytvoření scénářů

V rámci modelové organizace bylo v katalogu zranitelností definováno, jaké kategorie aktiv mohou tuto zranitelnost obsahovat.

Dále bylo v katalogu hrozeb popsáno, zda daná hrozba působí na důvěrnost, integritu nebo dostupnost.

Dalším krokem bylo vytvoření vhodných kombinací hrozeb a zranitelností.

Vše lze najít v Příloze 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik a v Příloze 6: Vzorové hodnocení aktiv a rizik.

5.4 Katalog opatření

V rámci modelové organizace bylo rozhodnuto o vytvoření Katalogu opatření. Tento katalog má několik funkcí, jednou z nich je sloužit jako Prohlášení o aplikovatelnosti (viz kap. 5.11 Prohlášení o aplikovatelnosti), dále slouží jako GAP[12] analýza a tím, že popisuje aktuální stav v organizaci včetně hodnocení úrovně zavedení bezpečnostních opatření, může sloužit jako pomůcka pro následné hodnocení zranitelností.

Jednotlivá aplikovatelná bezpečnostní opatření jsou hodnocena na úrovni 1-4, v závislosti na tom, jak je jejich zavedení účinné. Zároveň jsou zmapovány vazby mezi bezpečnostními opatřeními a zranitelnostmi. Na základě hodnocení úrovně účinnosti zavedených bezpečnostních opatření je vypočítána výsledná hodnota pro úroveň zranitelnosti, která slouží jako výchozí hodnota pro hodnocení zranitelnosti v rámci procesu hodnocení rizik. Při hodnocení kombinace aktivum-

[12] Tento typ analýzy je používán jako rozdílová analýza mezi skutečným stavem v organizaci oproti požadavkům VKB.

zranitelnost-hrozba může být výchozí hodnota zranitelnosti zvýšena nebo snížena na základě konkrétních okolností souvisejících s identifikovaným rizikem.

Katalog opatření lze najít v Příloze 7: Vzorové prohlášení o aplikovatelnosti.

5.4.1 Identifikace vazeb mezi bezpečnostními opatřeními a zranitelnostmi

Každé bezpečnostní opatření působí na jednu nebo více zranitelností (tedy snižuje jejich míru). Při identifikaci vazeb mezi bezpečnostními opatřeními a zranitelnostmi v tomto podpůrném materiálu byla využita zejména následující pravidla:

- Byla hledána tzv. primární vazba mezi bezpečnostním opatřením a zranitelnostmi, kdy bylo zjišťováno, na jaké zranitelnosti působí posuzované bezpečnostní opatření nejvíce. Pokud by byly hledány i sekundární vazby, tak by téměř všechna bezpečnostní opatření působila alespoň v malé míře na všechny zranitelnosti.
- Bezpečnostním opatřením, která se týkala dokumentace, pravidel, nebo postupů byla vždy přiřazena primární vazba na zranitelnost „Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností lidských zdrojů“.
- Vzhledem k obecnější míře detailu jednotlivých zranitelností nebylo vždy možné najít adekvátní konkrétní zranitelnosti, v takovém případě byla využita vazba na zranitelnost „Nedostatečná ochrana aktiv“.

5.5 Vzorec pro výpočet rizika

Pro výpočet rizika jsou nejčastěji využívány funkce, které ovlivňuje dopad, hrozba a zranitelnost. VKB uvádí jako vhodnou následující funkci[13]:

Tabulka 22: Vzorec pro výpočet rizika

Riziko = dopad (hodnota aktiva) x hrozba x zranitelnost

Dopad

Dopad představuje hodnotu škody, která by vznikla v případě narušení bezpečnosti informací (důvěrnosti, integrity, dostupnosti). Pro hodnocení dopadu je využito hodnocení aktiv podle § 4 VKB viz také kapitoly 4.1.4 Hodnocení primárních aktiv a 4.2.4 Hodnocení podpůrných aktiv a určení vazeb mezi podpůrnými a primárními aktivy.

Hrozba

U hrozby hodnotíme pravděpodobnost, s jakou nastane.

Tabulka 23: Hodnocení úrovně hrozby

STUPNICE PRO HODNOCENÍ HROZEB		
1	nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.

[13] Ve VKB znaky „x“ představují zástupné znaky, které mohou být nahrazeny různými matematickými funkcemi, např. sčítání nebo násobení. Funkce sčítání se však jeví jako méně vhodná než funkce násobení. Násobení poskytuje širší škálu výsledných hodnot rizika a usnadňuje tak jejich prioritizaci.

STUPNICE PRO HODNOCENÍ HROZEB		
2	střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let
3	vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
4	kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Zranitelnost

U zranitelnosti hodnotíme, jak je pravděpodobné její zneužití a jestli existují bezpečností opatření, která by vedla ke snížení možnosti jejího zneužití.

Tabulka 24: Hodnocení úrovně zranitelnosti

STUPNICE PRO HODNOCENÍ ZRANITELNOSTÍ		
1	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.
2	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.
3	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.
4	kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Alternativa

V případě používání metody vytváření scénářů je možné upravit vzorec a hodnotit vhodnou kombinaci hrozby a zranitelnosti jako jeden celek.

Tabulka 25: Alternativní vzorec pro výpočet rizika

Riziko = dopad (hodnota aktiva) x scénář

Tento postup by však neměl vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Hodnotu scénáře lze např. doplnit komentářem.

Modelový příklad určení vzorce pro výpočet rizika

Ministerstvo ve své metodice použilo funkci z VKB a zvolilo metodu násobení.

Tabulka 26: Vzorec pro výpočet rizika modelové organizace

Riziko = dopad (hodnota příslušného atributu aktiva) x hrozba x zranitelnost

5.6 Kritéria pro akceptovatelnost rizik

Kritéria pro akceptovatelnost představují „risk appetite“ organizace, který by mělo stanovit její vrcholové vedení. Jinými slovy lze říct, že je to stanovení hranice mezi riziky, která jsme schopni přijmout a těmi, na která musíme hledat bezpečnostní opatření, protože jejich realizace je vysoce pravděpodobná nebo jsou jejich dopady závažné. Např. pokud necháme na parkovišti v centru města celý den stát odemknuté auto, existuje určitá pravděpodobnost, že ho někdo odcizí nebo poškodí. Bezpečnostním opatřením může být auto zamknout, auto zaparkovat na hlídaném parkovišti, auto zaparkovat v garáži atd. Možná je také kombinace více různých bezpečnostních opatření. Záleží na každé osobě, která varianta je pro ni přijatelná, tedy jaký má „risk appetite“.

Modelový příklad určení kritérií pro akceptovatelnost

Na jednání výboru KB byla řešena problematika stanovení kritérií pro akceptovatelnost. Schválena byla následující tabulka, která je součástí metodiky pro identifikaci a hodnocení rizik.

Tabulka 27: Kritéria pro akceptovatelnost rizik ministerstvem

Úroveň	Hranice míry rizika	Popis	Proces zvládání rizika
Nízká	**1-16**	Riziko je považováno za přijatelné – akceptovatelné.	Riziko akceptuje manažer KB ve spolupráci s gestorem aktiva. Dále riziko monitorují. V případě zájmu se výbor KB může o těchto rizicích informovat.
Střední	**17-31**	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.	V případě způsobu zvládání rizika „Akceptovat“ riziko akceptuje manažer KB ve spolupráci s gestorem aktiva. V případě způsobu zvládání rizika „Snížit“ navrhuje bezpečnostní opatření architekt KB ve spolupráci s manažerem KB. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje manažer KB Výboru pro KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání.
Vysoká	**32-47**	Riziko je dlouhodobě nepřípustné a musí být	Způsob zvládání rizika navrhuje manažer KB ve spolupráci s gestorem aktiva. V případě návrhu způsobu zvládání rizika „Snížit“

Úroveň	Hranice míry rizika	Popis	Proces zvládání rizika
		zahájeny systematické kroky k jeho odstranění.	navrhuje bezpečnostní opatření architekt KB ve spolupráci s manažerem KB. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje manažer KB Výboru pro KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání.
Kritická	**48-64**	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.	Způsob zvládání rizika navrhuje manažer KB ve spolupráci s gestorem aktiva. V případě návrhu způsobu zvládání rizika „Snížit" navrhuje bezpečnostní opatření architekt KB ve spolupráci s manažerem KB. Navržený způsob zvládání rizik včetně bezpečnostního opatření prezentuje manažer KB Výboru pro KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládání. V případě naléhavosti zvládnutí rizika lze postupovat způsobem popsaným v metodice.

Tabulka 28: Rozložení úrovní rizika

		Hrozba × zranitelnost								
		1	**2**	**3**	**4**	**6**	**8**	**9**	**12**	**16**
Hodnota dopadu aktiva	**1**	1	2	3	4	6	8	9	12	16
	2	2	4	6	8	12	16	18	24	32
	3	3	6	9	12	18	24	27	36	48
	4	4	8	12	16	24	32	36	48	64

5.7 Postup zvládání výjimek

V praxi se často stává, že některé věci nelze standardizovat a je potřeba vytvořit výjimky. Organizace by měla mít stanovený postup, v jakých případech a za jakých podmínek lze výjimku udělit.

Organizace by měla usilovat o to, aby byly výjimky udělovány jen ve výjimečných případech a co nejdříve odstraňovány.

Modelový příklad stanovení postupu zvládání výjimek

V případě, že riziko na úrovni vysoká nebo kritická nelze snížit zavedením bezpečnostního opatření do 1 roku (a uvést ho v plánu zvládání rizik pro daný rok), je nutné sepsat odůvodnění, např. je zavedení bezpečnostního opatření časově a finančně náročné. Toto odůvodnění slouží jako základ pro žádost o výjimku. Součástí odůvodnění je návrh na odstranění výjimky.

Žádosti o výjimky posuzuje výbor KB, který může udělit výjimku na dobu nezbytně nutnou (dobu nutnou pro realizaci příslušného bezpečnostního opatření), čímž akceptuje riziko s výjimkou spojené. Po roce[14] je nutné provést přezkoumání výjimek a způsobů jejich odstranění.

Výjimky eviduje manažer kybernetické bezpečnosti.

5.8 Hodnocení rizik

5.8.1 Identifikace rizik

Identifikace rizik je vytváření relevantních kombinací aktivum-zranitelnost-hrozba. Účelem identifikace rizik není vytvoření kombinací všeho se vším, např. u aktiv typu lidské zdroje nemá smysl vytvářet kombinace obsahující zranitelnosti typu nedostatečná údržba a hrozby typu poškození nebo selhání technického nebo programového vybavení. Je potřeba zvážit všechny možné varianty s ohledem na celou trojici aktivum-zranitelnost-hrozba.

Modelový příklad identifikace rizik

Identifikace rizik v rámci modelové organizace probíhala tak, že bylo nejdříve vybráno aktivum z katalogu aktiv, u kterého byla identifikace prováděna, následně byla z katalogu zranitelností vybrána zranitelnost, kterou může daný typ aktiva obsahovat, a nakonec byla vybrána hrozba, která na danou zranitelnost působí. Takto vznikla první kombinace aktivum-zranitelnost-hrozba. Postup byl následně opakován, dokud nebyly identifikovány všechny relevantní kombinace.

Jako pomůcka pro identifikaci rizik byla vytvořena matice zobrazující možné kombinace hrozeb a zranitelností (viz vytváření scénářů v kapitole 5.3 Příprava scénářů). Matice hrozeb a zranitelností je v tomto případě postavena na principu existence různých hrozeb, které využívají zranitelností konkrétních aktiv[15].

5.8.2 Analýza rizik

Analýza rizik je v souladu s VKB ohodnocení relevantních kombinací aktivum-zranitelnost-hrozba a výpočet výsledné hodnoty rizika podle příslušného vzorce.

Modelový příklad analýzy rizik

Hodnoty aktiv (z pohledu důvěrnosti, integrity a dostupnosti) již byly v rámci modelové organizace identifikovány v rámci řízení aktiv a zaznamenány do katalogu aktiv. Pro účely analýzy rizik byly příslušné hodnoty přebrány. Pro určení hodnoty zranitelností byl použit katalog opatření, kde jsou zaznamenaná zavedená bezpečnostní opatření v rámci modelové organizace a jejich účinnost. Základní hodnota zranitelnosti vychází z průměru účinnosti všech opatření, které na danou zranitelnost působí. Tato hodnota je však pouze orientační a v některých případech je nutné ji upravit s ohledem na specifickou kombinaci aktivum-zranitelnost-hrozba, např. v některých případech nebudou na zranitelnost působit všechna opatření. Hodnota hrozby byla stanovena s ohledem na kombinaci aktivum-zranitelnost-hrozba podle příslušné stupnice uvedené v metodice.

[14] U VIS je možné provádět přezkoumání po 3 letech (spojeno s povinností provést hodnocení rizik alespoň jednou za 3 roky).

[15] Je možné k této problematice přistupovat i obráceně, tzn. existence různých zranitelností, které jsou využívány hrozbami, záleží tedy na konkrétním příkladu a řešiteli, který přístup zvolí a bude v rámci hodnocení rizik používat.

5.8.3 Vyhodnocení

Vyhodnocení znamená porovnání výsledné hodnoty rizika s kritérii pro akceptovatelnost a rozhodnutí, zda bude riziko akceptováno nebo bude snižováno.

Modelový příklad vyhodnocení

Výsledné hodnoty rizik byly porovnány se stanovenými kritérii pro akceptovatelnost. V nástroji excel dochází automaticky k obarvení výsledné hodnoty rizika barvou přidělenou příslušnému stupni – nízká, střední, vysoká a kritická. Dále byl vyplněn sloupec *„Způsob zvládání rizika“*, podle toho, jak bude s příslušnými riziky dále nakládáno.

5.9 Zvládání rizik

Identifikovaná a ohodnocená rizika je potřeba vhodným způsobem ošetřit tak, aby nebyla organizací ignorována. V závislosti na výstupu z hodnocení rizik je potřeba určit způsob jejich zvládnutí.

V případě preventivního řešení by náklady na dané opatření neměly přesahovat hodnotu rizika.

V případě reaktivního řešení jsou dodatečné náklady investovány až ve chvíli, kdy scénář nastává. Zpravidla jde o riziko, které nebylo nijak ošetřeno, nebo zavedené opatření nebylo účinné.

Vhodné je vytváření záložních plánů, a to i pro vysoká rizika, na které jsme nalezli opatření k jejich zmírnění (redukci) nebo jsme je přenesli.

Všechna rizika je vhodné monitorovat a přezkoumávat metody jejich zvládání z toho důvodu, že pravděpodobnost výskytu rizik, či jejich dopad se může v čase měnit. Stejně tak se může změnit schopnost organizace tato rizika zvládat. Méně závažná rizika je vhodné periodicky monitorovat a přezkoumávat. U závažných rizik je potřeba rizika sledovat a neustále přezkoumávat.

V případě, kdy výsledná hodnota rizika překročí hranici akceptovatelnosti, je potřeba vybrat vhodná bezpečnostní opatření, snížit hodnotu rizika nebo eliminovat riziko a zajistit požadovanou úroveň bezpečnosti informací. Pokud je finanční náročnost opatření nepřiměřená vůči riziku, které má ošetřit, je potřeba zvolit jiné, méně účinné opatření či pokrýt riziko několika dílčími opatřeními i za předpokladu, že takové ošetření rizika nebude dlouhodobě dostatečné. Tato situace může nastat např. při využívaní zastaralé technologie. V takovémto případě je třeba začít vytvářet strategii pro odstavení aktiv, se kterými riziko souvisí a jejich nahrazení aktivy novými, které již toto riziko neponesou.

Akceptace rizika

Akceptace může být **pasivní** (např. u malých a středních rizik, kde nebyla nalezena smysluplná opatření), což znamená, že skutečně nezavádíme žádné opatření kromě záznamu daného rizika (evidence rizik je často označována jako registr rizik) anebo také **aktivní** (u středních rizik), což znamená, že vytvoříme v plánování lidských a finančních zdrojů určitou rezervu, která by měla případný výskyt rizika pokrýt.

U vysokých rizik je třeba alokovat zdroje na zavedení opatření.

Akceptace rizika musí probíhat v souladu s metodikou a kritérii pro akceptovatelnost rizik (viz kapitola 5.6 Kritéria pro akceptovatelnost rizik).

Akceptovaná rizika nejsou dále řešena, nicméně je třeba je dále v průběhu realizace monitorovat a prověřovat, zdali se jejich parametry nemění.

Redukce a eliminace rizika

Nejběžnější metodou zvládání rizik je **redukce rizika** neboli snížení rizika**.** Jedná se o aktivní přístup, jehož cílem je výběr vhodného bezpečnostního opatření tak, aby byla rizika snížena na přijatelnou úroveň.

Bezpečnostní opatření jsou uvedená ve VKB, nejedná se však o konečný výčet možných bezpečnostních opatření. Zavádění bezpečnostních opatření je prováděno na základě hodnocení rizik a v nezbytném rozsahu pro zajištění KB. Výsledná hodnota rizika definuje požadavky na ochranu, tedy na konkrétní bezpečnostní opatření.

Zaváděním bezpečnostních opatření zpravidla dochází ke snižování hodnoty zranitelnosti. Hrozby jsou zpravidla v daném čase a místě stejné, bez ohledu na opatření. Některé hrozby a jejich hodnocení lze ovlivnit změnou okolností, např. přesunutím datového centra z jedné lokality do jiné.

Riziko je tvořeno kombinací aktivum-zranitelnost-hrozba a snižováním hodnoty zranitelnosti prostřednictvím zavádění bezpečnostních opatření dochází zároveň ke snižování výsledné hodnoty rizika.

Princip **eliminace rizika** (ukončení rizika) spočívá v nalezení jiného řešení dané situace, které rizikovou událost neobsahuje.

Vyhnutí se riziku

Tato metoda spočívá v **utlumení** (velmi omezeném využití) nebo **vypnutí** (nepoužívání) daného aktiva. Využití tohoto způsobu zvládání rizik je nutné v případech, kdy výskyt rizika je jistý a dopad na organizaci kritický.

Přenesení nebo sdílení rizika

V případech, kdy organizace nemá kapacity na zavedení bezpečnostních opatření, lze přenést odpovědnost za vhodné opatření na externí společnost. S rizikem se buď nic neděje, pouze je přesměrováno na „třetí stranu“ s jejím vědomým souhlasem (např. pojištění, kde opatření má obecně dopad do nákladů a škodu zaplatí někdo jiný) nebo je přeneseno na dodavatele. Zároveň je ale potřeba mít na paměti, že organizace má vždy nepřenositelnou odpovědnost za to, že riziko bude nějakým způsobem řešeno (např. že jej dodavatel vyřeší správně).

Modelový příklad zvládání rizik

Zvládání rizik probíhá v souladu s metodikou ministerstva viz Příloha 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik.

5.9.1 Výběr opatření

Výběr opatření zahrnuje volbu vhodných bezpečnostních opatření, kterými bude snižována hodnota příslušných rizik.

Co to je bezpečnostní opatření

Opatření představuje formu zavádění a prosazování specifických bezpečnostních postupů organizačního charakteru a/nebo implementaci technických nastavení či bezpečnostních technologií.

Opatřením organizačního charakteru může být zajištění personální bezpečnosti, požadavky na chování uživatelů, organizaci řízení kybernetické bezpečnosti, souhrn zákonných a smluvních požadavků

organizace, předpis či metodiky technického standardu či požadavky na řízení dodavatelů a požadavky do smluv s dodavateli. Formou opatření pak může být interní či provozní předpis (např. směrnice). Dokument pro zavedení organizačního opatření obsahuje podrobný popis toho, co je opatřením myšleno a jakým způsobem by opatření mělo být implementováno a prosazováno. Organizační opatření popisuje VKB v § 3 až § 16.

Opatření technické povahy (fyzická ochrana, SW, HW, …) se odvíjí od samotného nasazení zvolené bezpečnostní technologie či jejím nastavením, souvisí s přímou ochranou bezpečnosti komunikační sítě, prvků komunikační sítě a technických a programových prostředků pro specifická prostředí. Může se jednat např. o nástroj ke správě a ověřování identit, technické řízení přístupových oprávnění, SW k ochraně před škodlivým kódem, systém k zaznamenávání (monitoring) událostí IS, jeho uživatelů a administrátorů, nástroj k detekci kybernetických bezpečnostních událostí, ale i provádění penetračních testů a používání kryptografických prostředků. Technická opatření popisuje VKB v § 17 až § 29.

Proč se opatření zavádí

Opatření se zavádí s cílem identifikovaná rizika (hrozby a zranitelnosti) skutečně a účinně snížit a dosáhnout tak efektivní ochrany informací v potřebných atributech viz. kapitola 2.1. Bezpečnost informací.

V praxi je možné, že jsou rizika snížena zavedením bezpečnostních opatření, ale i přes toto snížení zůstane hodnota rizika na neakceptovatelné úrovni. V takovém případě je nutné zavádět další bezpečnostní opatření, dokud nebude hodnota rizika akceptovatelná.

Zavádění bezpečnostních opatření je nutno provádět v kontextu všech ostatních rizik.

V případě, že bezpečnostní opatření není možné zavést ihned, např. z důvodu ekonomické náročnosti nebo doby potřebné k jeho zavedení, je nutné v mezičase riziko snížit dodatečnými bezpečnostními opatřeními.

Jak postupovat při výběru bezpečnostních opatření – Praktické rady

Při výběru bezpečnostních opatření je vhodné:

- cílit opatření na zjištěná rizika (hrozby a zranitelnosti ve vazbě na CIA),
- postupovat v souladu s požadavky VKB,
- opírat se o odborné znalosti technických garantů a expertů pro fyzickou a KB,
- zohlednit přiměřenost opatření ve vztahu k požadovanému cíli (významnosti zabezpečovaného aktiva),
- zohlednit přiměřenost opatření k nákladům a procesům, které jsou s implementací opatření spojeny (technické, lidské, finanční aj. zdroje),
- provést analýzu procesu implementace / zavedení opatření,
- popsat rozsah možného působení zavedeného opatření (cíle a přínosy).

Kroky nezbytné k realizaci opatření:

- Postupovat v souladu s interními předpisy,
    - Postup informování odpovědných osob

- Postup návrhu a schvalování opatření dle náročnosti na zdroje (manažer kybernetické bezpečnosti, výbor KB, porada vedení apod.)
- Vlastní návrh technického či organizačního opatření (nebo jeho koncepce, dle složitosti opatření či celého souboru opatření)

- Stanovení odpovědností za následné postupy, termíny předpokládaných dílčích plnění, předpokládaný termín finálního plnění a termín následného přezkoumání
- Objednávka / výběrové řízení / implementace nebo zavedení organizačního nebo technického opatření

Modelový příklad výběru opatření

Na základě provedeného hodnocení rizik byla nejdříve posouzena rizika s úrovní kritická, na která byla navržena bezpečnostní opatření. Stejný postup byl posléze zopakován s riziky na úrovni vysoká. Následně byla posouzena rizika na úrovni střední, zda je možné zavést vhodná méně náročná bezpečnostní opatření. Dále byly analyzovány vazby mezi jednotlivými riziky a bezpečnostními opatřeními. Všechna navržená bezpečnostní opatření byla zaznamenána v plánu zvládání rizik (viz Příloha 8: Vzorový plán zvládání rizik).

Plán zvládání rizik byl následně předložen ke schválení výboru KB.

5.9.2 Plán zvládání rizik

Plán zvládání rizik (známý také jako RTP = Risk Treatment Plan) je jedním z klíčových dokumentů, který vychází z procesu hodnocení rizik.

Při jeho sestavování je potřeba vycházet nejen z hodnocení rizik, ale také z dalších souvisejících procesů, jako je např. audit kybernetické bezpečnosti, proběhlé kybernetické bezpečnostní incidenty, varování či reaktivní opatření vydané NÚKIB, plánované významné změny apod.

Cílem plánu zvládání rizik je zejména systematický přístup k zavádění bezpečnostních opatření, stanovení prioritizace při eliminaci rizik, stejně tak jako efektivní plánování finančních i lidských zdrojů potřebných pro zajištění kybernetické bezpečnosti.

Plán zvládání rizik je přehledový dokument obsahující:

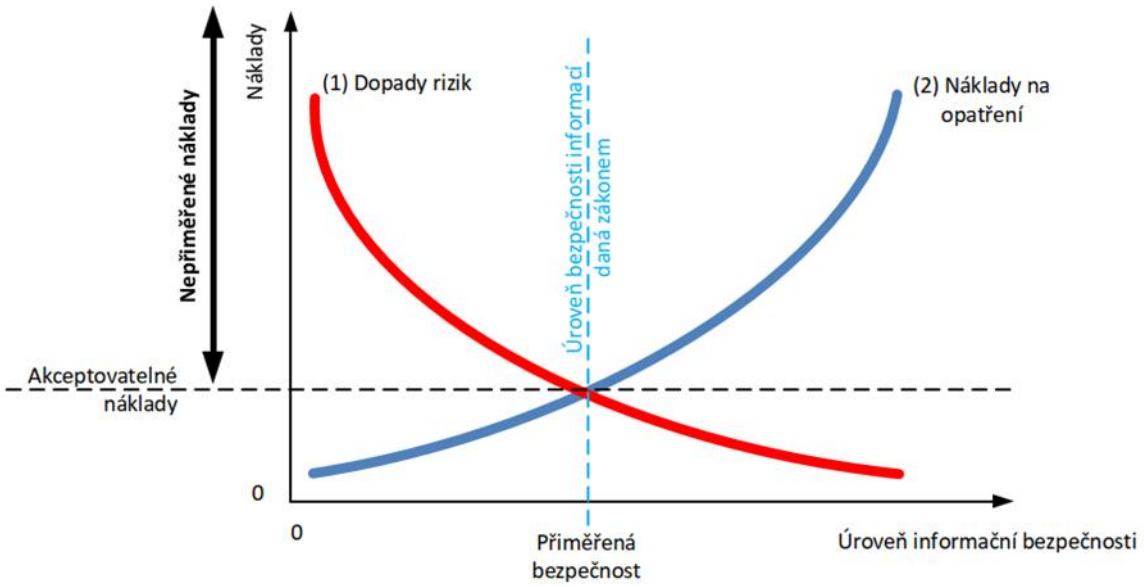
- cíle a přínosy bezpečnostních opatření pro zvládání rizik,
- určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik,
- potřebné finanční, technické, lidské a informační zdroje,
- termíny zavedení opatření,
- popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními,
- způsob realizace bezpečnostních opatření,
- způsob hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik.

S plánem zvládání rizik by mělo být **aktivně pracováno** a měl by být aktualizován v souvislosti se zaváděním bezpečnostních opatření. Tento plán se může odkazovat na další dokumenty obsahující podrobnější informace, např. projektovou dokumentaci apod.

5.9.3 Zavádění opatření

Náklady na bezpečnostní opatření by měly být přiměřené a neměly by převýšit náklady spojené s následky realizace rizika.

Proces zavádění bezpečnostních opatření musí být plánován. Pro plánování zavádění bezpečnostních opatření slouží plán zvládání rizik.



Obrázek 9: Odvození nepřiměřených nákladů[16]

Modelový příklad zavádění opatření

Modelová organizace prostřednictvím výboru KB schválila plán zvládání rizik a v souladu s ním zavádí bezpečnostní opatření. Plán zvládání rizik je uveden v dokumentu Příloha 8: Vzorový plán zvládání rizik.

Bezpečnostní opatření byla prioritizována přidělením hodnoty 1-4, kde 1 znamená, že opatření je nutné zavádět co nejdříve.

5.10 Zpráva o hodnocení rizik

Zpráva o hodnocení rizik shrnuje výsledky hodnocení rizik pro relevantní zainteresované strany a slouží jako stručný přehled výsledných rizik, jejich akceptovatelnosti či neakceptovatelnosti a příp. navržení potřebných bezpečnostních opatření pro redukci či eliminaci rizik. Zpráva o hodnocení rizik by měla být projednána a schválena výborem KB či jiným obdobným schvalovacím orgánem organizace.

Modelový příklad zprávy o hodnocení

Zprávu o hodnocení rizik modelové organizace projednal a schválil její výbor KB. Zpráva o hodnocení rizik je obsahem dokumentu Příloha 9: Vzorová zpráva o hodnocení rizik.

[16]Převzato z podpůrného materiálu „Nepřiměřené náklady“ dostupném na: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/.

5.11 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti (SoA = Statement of Applicability) je dokument, ve kterém jsou popsána zavedená bezpečnostní opatření včetně způsobu jejich implementace i opatření nezavedená a odůvodnění z jakého důvodu nedošlo k jejich zavedení. Jedná se o stěžejní dokument, který je předkládán výboru KB (či jinému obdobnému schvalovacímu orgánu organizace), který jej musí odsouhlasit.

Prohlášení o aplikovatelnosti je společně s plánem zvládání rizik klíčovým dokumentem ISMS a měl by podávat přesné a aktuální informace o stavu bezpečnostních opatření v organizaci. Tento strategický dokument poskytuje náhled na zabezpečení organizace jako celku.

Při zavádění ISMS lze vypracovat prohlášení o aplikovatelnosti prostřednictvím GAP analýzy, která porovnává stav zavedených bezpečnostních opatření v organizaci s požadavky stanovenými VKB.

Prohlášení o aplikovatelnosti musí obsahovat všechna bezpečnostní opatření požadovaná VKB.

Modelový příklad prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti modelové organizace projednal a schválil její výbor KB. Prohlášení o aplikovatelnosti je obsahem dokumentu Příloha 7: Vzorové prohlášení o aplikovatelnosti.

U každého bezpečnostního opatření bylo posuzováno, zda je zavedeno, dokumentováno a je kontrolována jeho účinnost. Pokud opatření nejsou zavedena nebo jsou minimální, tak se mu přiřadí hodnota 4. Pokud opatření je, tak se dále ptáme, zda je účinné a zda nás ochrání. Pokud nás ochrání vždy, tak uvedeme 1, pokud ve většině případů, tak uvedeme 2, pokud jen někdy, tak uvedeme 3 a pokud vůbec, tak je k ničemu a uvedeme 4.

5.12 Sdílení informací o riziku

Sdílení informací o riziku je proces, kdy osoba odpovědná za rozhodnutí, co se s rizikem bude dít a případně jaká bezpečnostní opatření budou zavedena, sdílí informace s dalšími zainteresovanými stranami.

Modelový příklad sdílení informací o riziku

V rámci ministerstva je aktivován a komunikován proces sdílení informací o riziku. Komunikace a sdílení informací je primárně řízena výborem KB, s ohledem na citlivost informací. V rámci společného jednání je o souboru opatření uvědoměn jak gestor, tak garant primárního a podpůrného aktiva. Cílem společné komunikace je zajištění nastavení souboru organizačních a technických bezpečnostních opatření, která budou zavedena do organizace nebo systému, včetně nastavení procesu monitorování, vyhodnocování a eskalace problémů. V případě potřeby je diskuse dále vedená do úrovně významného dodavatele a provozovatele.

5.13 Alternativní hodnocení rizik u primárních aktiv

Hodnocení rizik u primárních aktiv může být zapracováno do postupu uvedeného výše. V některých organizacích však může nastat situace, že povinnosti vyplývající ze ZKB a VKB musí najednou začít plnit pro několik služeb a IS. Z tohoto důvodu byla vypracována alternativa, která stojí na hodnocení aktiv.

Tuto alternativu však nelze použít dlouhodobě, slouží pouze pro nastartování procesu řízení aktiv a rizik a při následném provedení hodnocení rizik je nutné hodnocení rizik rozpracovat do většího detailu a zahrnout do něj i podpůrná aktiva.

Metoda spočívá v tom, že dojde k identifikaci, evidenci a hodnocení primárních aktiv dle postupu uvedeného v kapitole 4.1 Primární aktiva. Následně však nejsou identifikována podpůrná aktiva, ale je provedeno hodnocení rizik pouze u primárních aktiv.

Pro tento postup je nutné upravit tabulky s hodnocením rizik a kritéria akceptace.

Modelový příklad úpravy stupnice hodnocení rizik a kritérií akceptace

Pro výpočet hodnoty rizika alternativní metodou byl použit tento vzorec:

Riziko = dopad (hodnota aktiva) * pravděpodobnost realizace scénáře

Pro hodnoty dopadu byly použity stejné stupnice jako v předchozím případě, viz kapitola 4.1.4. Hodnocení primárních aktiv.

Pro hodnocení pravděpodobnosti realizace scénáře byla použita následující stupnice:

Tabulka 29: Stupnice pro hodnocení pravděpodobnosti realizace scénáře

PRAVDĚPODOBNOST REALIZACE SCÉNÁŘE		
1	nízká	Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití a využití zranitelností hrozbou neexistuje nebo je málo pravděpodobné a není častější než jednou za 5 let.
2	střední	Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena a zneužití zranitelností hrozbou je málo pravděpodobné až pravděpodobné a v rozpětí od 1 roku do 5 let.
3	vysoká	Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Zneužití zranitelností hrozbou je pravděpodobné až velmi pravděpodobné a v rozpětí od 1 měsíce do 1 roku.
4	kritická	Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Zneužití zranitelností hrozbou je velmi pravděpodobné až víceméně jisté a častější než jednou za měsíc.

Pro hodnocení rizik byla použita následující stupnice:

Tabulka 30: Stupnice pro alternativní hodnocení rizik

STUPNICE PRO HODNOCENÍ RIZIK		
1-4	nízká	Riziko je považováno za přijatelné – akceptovatelné.
5-8	střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
9-12	vysoká	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
13-16	kritická	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

5.13.1 Postup alternativního hodnocení rizik u primárních aktiv

Hodnocení rizik se musí účastnit všechny relevantní osoby, např. manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, garanti primárních aktiv, zástupci IT, DPO atd.

Následně dojde k vytvoření obecných rizikových scénářů ohrožujících primární aktiva, např. používáme zastaralé technologie a z důvodu technické závady nebude fungovat IS podporující službu certifikace senzorů.

Hodnota dopadu je stanovena na základě hodnocení primárních aktiv, přičemž se v úvahu bere nejvyšší hodnota relevantního atributu, např. pro hrozbu poškození nebo selhání technického nebo programového vybavení není relevantní atribut důvěrnosti, a proto bude bráno v úvahu hodnocení příslušného primárního aktiva pouze z pohledu integrity a dostupnosti.

Pravděpodobnost realizace scénáře se odvíjí od vlastního prostředí organizace, např. zavedených bezpečnostních opatření, stáří používaných technologií, umístění organizace apod. Z toho důvodu je důležité mít pro hodnocení rizik k dispozici všechny relevantní osoby, které jsou schopny danou situaci vyhodnotit kvalifikovaným odhadem.

Vyhodnocení znamená porovnání výsledné hodnoty rizika s upravenými kritérii pro akceptovatelnost a rozhodnutí, zda bude riziko akceptováno nebo bude snižováno.

Následně je nutné navrhnout bezpečnostní opatření včetně termínu pro hodnocení rizik zahrnující podpůrná aktiva, připravit plán zvládání rizik, zprávu o hodnocení rizik a prohlášení o aplikovatelnosti.

Modelový příklad hodnocení rizik u primárních aktiv

V rámci ministerstva byl vytvořen expertní tým, který vytvářel rizikové scénáře k identifikovaným primárním aktivům a následně je expertním odhadem hodnotil. Výsledky hodnocení rizik jsou uvedeny v Příloze 12: Vzorové alternativní hodnocení rizik u primárních aktiv.

5.14 Další povinnosti dle VKB

Kromě povinností popsaných v předchozích kapitolách, stanovuje VKB ještě tyto požadavky:

- Provádět hodnocení rizik při významných změnách (§ 5 odst. 1 písm. c))
- Při hodnocení rizik a v plánu zvládání rizik zohlednit (§ 5 odst. 1 písm. h)):
    - Významné změny
    - Změny rozsahu ISMS (viz kapitola 2.2.1 Rozsah systému řízení bezpečnosti informací)
    - Opatření podle § 11 ZKB (viz kapitola 7 Opatření podle § 11 zákona)
    - Kybernetické bezpečnostní incidenty, včetně dříve řešených
- V souladu s plánem zvládání rizik zavádět bezpečnostní opatření

5.14.1 Významné změny

Významnou změnou je změna, která má nebo může mít vliv na KB a představuje vysoké riziko.

Významnou změnou může být např.:

- změna rozsahu ISMS,
- změna primárních aktiv,
- vznik nové služby (aktiva), pořízení nového IS pro její podporu,
- změna/obnova technických aktiv, na kterých jsou informace/služby (primární aktiva) ministerstva jako např. DB servery,
- varování nebo nápravné opatření od NÚKIB, které je relevantní pro IS,
- nová hrozba nebo zranitelnost,
- změny v systému fyzického zabezpečení (EZP, EPS),
- rozšíření/změna topologie sítě,
- změna umístění v síti, např. přesun do jiné VLAN,
- upgrade FW,
- změna/obnova technických aktiv, které zajišťují bezpečnost provozu v síti jako např. FW, IDS, IPS, SIEM,
- nová velká SW verze např v1-v2, např. Windows 10 na Windows 11,
- výměna/upgrade HW, který bude mít vliv na bezpečnost informací,
- modernizace aplikačního řešení – např. kontejnerizaci, kdy jednotlivé dílčí funkcionality jsou osamostatněny ze stávajícího aplikačního balíku do tzv. mikroslužeb a budou provozovány na novém HW prostředí podporující spouštění mikroslužeb v kontejnerech,
- větší změna v SW jako např. změna operačního systému serverů z Windows Server 2012 na 2016,
- integrace nového IS, např. datové schránky, NIA,
- nasazení nové technologie (např. SIEM, virtualizace),

- upgrade OS serverů,
- implementace nového modulu do stávajícího IS.

6 Kontinuální zlepšování

VKB stejně jako norma ISO/IEC 27001 využívá modelu PDCA pro zajištění kontinuálního procesu zlepšování nejen řízení aktiv a rizik, ale i celého ISMS v organizaci.

V praxi to může znamenat, že prvotně identifikovaná typová aktiva budou při přezkoumání nedostatečná či nevhodná pro použití a bude nutné je pro další použití aktualizovat nebo upravit včetně aktualizace garantů aktiv (např. rozdělení typového aktiva na menší skupiny, vytvoření nových typových aktiv, sloučení typových aktiv do větších celků apod.).

Stejně jako aktiva musí být sledována a přezkoumávána také rizika včetně zbytkových rizik s ohledem na změny v organizaci, identifikované hrozby a zranitelnosti a účinnost zavedených bezpečnostních opatření (např. identifikace nové zranitelnosti, obměna HW komponent, implementace SIEM apod.).

S dokumenty jako je plán zvládání rizik a prohlášení o aplikovatelnosti je potřeba také neustále pracovat a pravidelně tyto dokumenty přezkoumávat a aktualizovat, aby odrážely skutečný stav.

Přezkoumávání a neustálý vývoj celého procesu a jeho výstupů je důležitý pro kontinuální zlepšování řízení aktiv a rizik v organizaci.

Správci a provozovatelé KII a správci a provozovatelé ISZS mají povinnost provést hodnocení rizik alespoň 1x ročně. Správci a provozovatelé VIS mají povinnost provést hodnocení rizik alespoň 1x za 3 roky.

Hodnocení rizik je jedním ze vstupů do procesu pravidelného vyhodnocování účinnosti ISMS a přezkoumání ISMS (§ 3 písm. g) VKB), společně s hodnocením stavu ISMS, revizí hodnocení rizik, posouzením výsledků pravidelných auditů KB a dopadů kybernetických bezpečnostních incidentů na ISMS. Z tohoto procesu vzniká zpráva z přezkoumání ISMS obsahující vyhodnocení opatření z předchozích přezkoumání ISMS, zpětnou vazbu o výkonnosti ISMS (neshody a nápravná opatření, výsledky monitorování a měření, výsledky auditů KB, naplnění cílů ISMS), výsledky hodnocení rizik a stav plánu zvládání rizik, identifikaci možností pro neustálé zlepšování, doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností. Cílem tohoto opatření je komplexní posouzení stavu ISMS v organizaci a zajištění jeho kontinuálního zlepšování.

Modelový příklad kontinuálního zlepšování

Ministerstvo si interními předpisy stanovilo povinnost provádět každoročně vyhodnocování účinnosti ISMS a přezkoumání ISMS. Podklady pro tento proces připravuje manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti a auditor kybernetické bezpečnosti. Samotné vyhodnocení provádí výbor KB, který schvaluje také finální zprávu z přezkoumání ISMS.

7 Opatření podle § 11 ZKB

Opatřeními se rozumí úkony, jichž je třeba k ochraně IS nebo služeb a sítí elektronických komunikací před hrozbou v oblasti KB nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.

V souladu s § 5 písm. h) bodem 3 VKB je nutné **při hodnocení rizik a v plánu zvládání rizik tato opatření zohlednit.** Zároveň je nutné zajistit naplnění podmínek vydaného opatření, mezi kterými může být např. konkrétní forma bezpečnostního opatření nebo lhůta pro jeho implementaci.

Aktuálně účinná opatření zveřejňuje NÚKIB povinně na své úřední desce a jsou proto dostupná zde: https://www.nukib.cz/cs/uredni-deska/.

7.1 Varování podle § 12 ZKB

Vychází z vlastního šetření NÚKIB nebo na základě podnětů národního CERTu, případně orgánů působících v oblasti KB v zahraničí a plošně varuje před hrozbou v oblasti KB.

7.1.1 Zohlednění varování NÚKIB ze dne 17. prosince 2018

NÚKIB vydal varování před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation včetně jejich dceřiných společností.

K tomuto varování byla vydána metodika (Metodika k varování ze dne 17. prosince 2018), která je dostupná na webových stránkách NÚKIB: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/.

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.** V případě užití jiné stupnice hodnocení hrozby, jak umožňuje § 5 odst. 3 VKB, je nutno tuto hrozbu ohodnotit způsobem odpovídajícím příslušné úrovni podle VKB.

Povinné osoby musí v souladu s § 8. odst. 2 písm. a) VKB varování zohlednit také v rámci výběrového řízení. Pro povinné osoby, které jsou současně zadavateli ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, byl vytvořen podpůrný materiál (Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení) dostupný na webových stránkách NÚKIB: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/.

Stěžejním je správné provedení hodnocení rizik. Hodnocení rizik musí být provedeno před vypsáním výběrového řízení na veřejnou zakázku a musí být v souladu se schválenou metodikou pro hodnocení rizik. V provedeném hodnocení rizik musí být jasně vidět rozdíl mezi riziky bez zohlednění varování a riziky se zohledněním varování.

Modelový příklad zohlednění varování v rámci běžného hodnocení rizik

V modelové organizaci byla identifikována podpůrná aktiva, na které má varování NÚKIB vliv. V případě, že se varování vztahovalo pouze na některé prvky v typovém aktivu, bylo toto typové aktivum rozděleno na 2 nová typová aktiva (např. PO20 Switch (přepínač) a PO21 Switch (přepínač). U těchto aktiv byla v Katalogu rizik identifikována příslušná rizika. U těchto rizik došlo k přehodnocení hrozby na hodnotu 4. Následně byl u neakceptovatelných rizik navržen vhodný způsob jejich zvládání v souladu s metodikou.

Samotné hodnocení rizik lze nalézt v dokumentu Příloha 6: Vzorové hodnocení aktiv a rizik.

Modelový příklad zohlednění varování u veřejné zakázky

Předmětem hodnocení rizik jsou komunikační prostředky a technické vybavení (HW) pořizované pro zajištění chodu agendového IS pro evidenci a zpracování procesu certifikace senzorů, jehož správce je Ministerstvo pro certifikaci senzorů. Tento IS byl určen jako prvek KII dle ZKB a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Celý postup probíhal v souladu s metodikou Ministerstva certifikací pro identifikaci a hodnocení aktiv a rizik popsanou v Příloze 2: Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik přiměřeně vzhledem k předmětu veřejné zakázky.

Vzhledem k tomu, že při hodnocení podpůrných aktiv musí být vzata v úvahu hodnota relevantních primárních aktiv, bylo analyzováno, jaká primární aktiva budou mít vazbu na podpůrná aktiva, která jsou předmětem výběrového řízení. S ohledem na to, že primární aktivum Služba certifikace senzorů pracuje se všemi informacemi v agendovém IS a přebírá nejvyšší hodnoty těchto informací dle jednotlivých atributů, postačuje pro hodnocení rizik v souvislosti s výběrovým řízením zohlednit hodnotu primárního aktiva Služba certifikace senzorů.

Jelikož je potřeba postupovat v souladu s Varováním NÚKIB, musí být hodnota hrozby u dotčených aktiv rovna nejvyšší možné, tedy hodnotě 4.

Byla vypracována zpráva o hodnocení rizik, která popisuje aplikovaný postup. Zpráva je k dispozici v dokumentu Příloha 11: Vzorová zpráva o hodnocení rizik pro veřejnou zakázku.

Detailní hodnocení lze nalézt v dokumentu Příloha 10: Vzorové hodnocení rizik pro veřejnou zakázku.

7.2 Reaktivní opatření podle § 13 ZKB

Vydává NÚKIB většinou na základě kybernetického bezpečnostního incidentu a předává jej buď konkrétním subjektům, kterých se to týká, nebo může vydat opatření obecné povahy s plošnou účinností.

7.3 Ochranné opatření podle § 14 ZKB

Vydává NÚKIB na základě již vyšetřeného kybernetického bezpečnostního incidentu formou opatření obecné povahy, včetně způsobu zvýšení ochrany IS a přiměřené lhůty pro jejich zavedení.

8 Q&A

Q1: Musí být při hodnocení rizik vytvořeny všechny možné kombinace aktivum-zranitelnost-hrozba?
A1: Ne. Je nutné identifikovat pouze ty relevantní.

Q2: Kolik aktiv je nutné identifikovat?
A2: Pro prvotní identifikaci aktiv doporučujeme začínat s menším množstvím typových aktiv, ale celý proces korektně dokončit. Při opakovaném hodnocení aktiv je nutné množství aktiv revidovat dle potřeby, např. je rozdělit na menší skupiny. Organizace by měla zvolit takový detail, aby byla schopna adekvátně identifikovat a řídit rizika s aktivy spojená.

Q3: Je možné použít jiný způsob řízení aktiv a rizik než uvedený v této metodice?
A3: Ano, uvedený způsob je pouze jeden z možných řešení, které je navíc nutné upravit dle potřeb organizace.

Q4: Je dostačující pracovat při hodnocení rizik pouze s hrozbami a zranitelnostmi uvedenými ve VKB?
A4: Ne, VKB poskytuje pouze přehled vybraných typových hrozeb a zranitelností a je vždy nutné identifikovat jednotlivé hrozby a zranitelnosti přímo pro konkrétní potřeby organizace a její systémy.

Q5: Je nutné hodnotit samostatně všechny oblasti hodnocení důležitosti primárních aktiv (§ 4 odst. 2 VKB), když se v naší organizaci tyto oblasti prolínají?
A5: Ne. Jednotlivé oblasti lze slučovat do větších oblastí, jako k tomu bylo přistoupeno např. v Příloze 3: Zjednodušená dopadová tabulka. Tento postup by však neměl vést ke ztrátě schopnosti rozlišení nebo vynechání jednotlivých oblastí, nově vytvořené oblasti je nutné popsat v příslušné metodice a samotné hodnocení lze např. doplnit komentářem.

Q6: Budou k dispozici prázdné šablony připravené podle metody popsané v tomto podpůrném materiálu?
A6: Ne. Veškeré modelové příklady a dokumenty byly vytvořeny pouze jako zdroj inspirace a konkrétní postupy a dokumenty si musí jednotlivé organizace přizpůsobit svým potřebám a schopnostem. Navíc jsou popsané způsoby řízení aktiv a rizik pouze jedním z možných řešení.

Q7: Jak se určují hodnoty hrozeb a zranitelností?
A7: Určení hodnoty hrozby a zranitelnosti vychází z přílohy č. 2 k VKB. Především vycházíte z osobních zkušeností nebo se opíráte o dostupné statistiky.

Q8: Předpokládám správně, že přijímáním opatření se snižuje pouze hodnota zranitelnosti, ale hodnota hrozby, která se odvíjí od aktuálního stavu úrovně působících hrozeb, se nemění?
A8: Ano, primárně to tak je, opatřením ovlivňujete míru zranitelnosti, pravděpodobnost hrozby v daném čase a místě je stejná bez ohledu na opatření. Např. v případě útoků se jejich počet opatřením nesníží, pouze se sníží jejich úspěšnost. Pravděpodobnost hrozby se samozřejmě v čase vyvíjí a může ji ovlivnit varování NÚKIB, politická situace apod. Některé hodnoty hrozeb lze ovlivnit změnou okolností, např. přesunutím datového centra z jedné lokality do jiné.

Q9: Jak snížím hodnotu rizika?
A9: Snížení hodnoty rizika nejčastěji probíhá zaváděním bezpečnostních opatření. Bezpečnostní opatření snižují zpravidla hodnotu zranitelnosti, která vstupuje do výpočtu výsledné hodnoty rizika.

9 Seznam obrázků a tabulek

9.1 Seznam obrázků

9.2 Seznam tabulek

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách www.nukib.cz/cs/infoservis/doporuceni/1862-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci-2/). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	**Podmínky použití**
Červená TLP: RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová TLP: AMBER	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta.
Oranžová TLP: AMBER+STRICT	Informace může být sdílena pouze v rámci organizace, které byla informace poskytnuta.
Zelená TLP: GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá TLP: CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
Datum	**Verze**	**Změněno**	**Popis změny**
18. 8. 2022	1.0	NÚKIB, MV, SPCSS, MZe, MŠMT, MPO, FN Plzeň	Vytvoření dokumentu