



Průvodce řízením aktiv a rizik dle vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

TLP:CLEAR

1. října 2026
Verze 1.0

Obsah

1	Co se dozvím v tomto dokumentu?	4
1.1	Jak pracovat s podpůrným materiálem?	4
1.2	Metoda popsaná v tomto materiálu	7
1.3	Stručný přehled procesu řízení aktiv a rizik	7
1.4	Představení modelové organizace	9
1.4.1	Proces certifikace	11
1.4.2	Popis jednotlivých úseků	12
2	Kybernetická bezpečnost	15
2.1	Bezpečnost informací	15
2.2	Systém řízení bezpečnosti informací	15
2.2.1	Stanovení rozsahu řízení kybernetické bezpečnosti	16
2.2.2	Cíle systému řízení bezpečnosti informací	16
3	Kontext organizace	18
3.1	Osoby podílející se na řízení aktiv a rizik	18
3.1.1	Vrcholné vedení	18
3.1.2	Výbor pro řízení kybernetické bezpečnosti	18
3.1.3	Manažer kybernetické bezpečnosti	19
3.1.4	Garant aktiva	19
3.1.5	Architekt kybernetické bezpečnosti	20
3.1.6	Auditor kybernetické bezpečnosti	20
3.1.7	Další organizační složky a osoby	20
3.2	Klíčové informace, procesy, služby	21
3.3	RACI matice	22
4	Řízení aktiv ve vztahu ke kybernetické bezpečnosti	23
4.1	Primární aktiva	25
4.1.1	Určení primárních aktiv	25
4.1.2	Evidence primárních aktiv	28
4.1.3	Určení garantů primárních aktiv	30
4.1.4	Hodnocení primárních aktiv	30
4.2	Podpůrná aktiva	44
4.2.1	Určení podpůrných aktiv	45
4.2.2	Evidence podpůrných aktiv	48
4.2.3	Určení garantů podpůrných aktiv	49
4.2.4	Hodnocení podpůrných aktiv a určení vazeb mezi podpůrnými a primárními aktivy	49

4.3	Klasifikace informací	52
4.4	Pravidla pro nakládání s aktivy	52
4.5	Likvidace dat	52
5	Řízení rizik v oblasti kybernetické bezpečnosti.....	53
5.1	Katalog zranitelností.....	53
5.2	Katalog hrozeb	56
5.3	Příprava scénářů	59
5.4	Katalog bezpečnostních opatření.....	59
5.4.1	Určení vazeb mezi zranitelnostmi a bezpečnostními opatřeními	60
5.5	Kritéria pro akceptovatelnost rizik	62
5.6	Postup zvládání výjimek	64
5.7	Hodnocení rizik.....	64
5.7.1	Určení rizik.....	64
5.7.2	Analýza rizik.....	64
5.7.3	Vyhodnocení.....	65
5.8	Zvládání rizik	65
5.8.1	Výběr opatření	66
5.8.2	Plán zvládání rizik.....	68
5.8.3	Zavádění bezpečnostních opatření.....	68
5.9	Zpráva o hodnocení rizik.....	69
5.10	Prohlášení o aplikovatelnosti	69
5.11	Sdílení informací o riziku.....	70
5.12	Alternativní hodnocení rizik u primárních aktiv	70
5.12.1	Postup alternativního hodnocení rizik u primárních aktiv	72
5.13	Další povinnosti dle vyhlášky	73
5.13.1	Významné změny	73
6	Kontinuální zlepšování	74
7	Protiopatření podle § 20 zákona	75
7.1	Varování podle § 22 zákona	75
7.1.1	Zohlednění varování NÚKIB	75
7.2	Reaktivní protiopatření podle § 23 zákona	76
8	Q&A.....	78
	Podmínky využití informací	80

1 Co se dozvím v tomto dokumentu?

Dokument slouží jako průvodce procesem řízení aktiv a rizik podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon“), a zejména jeho prováděcí **vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností** (dále jen „vyhláška“). Dokument je určen zejména organizacím, které zavádějí nebo rozvíjejí systém řízení kybernetické bezpečnosti (dále jen „ISMS“) v souladu s požadavky zákona a vyhlášky.

Účelem tohoto dokumentu není představit jediný správný postup řízení aktiv a rizik v souladu se zákonem a vyhláškou, ale představit základní principy, které je nezbytné přizpůsobit prostředí organizace. Dokument obsahuje teoretický a praktický popis jednotlivých kroků procesu, včetně modelových příkladů od stanovení rozsahu řízení kybernetické bezpečnosti (dále jen „KB“), přes určení primárních a podpůrných aktiv a jejich garantů, tvorbu katalogu hrozeb a zranitelností, až po výpočet rizik a návrh bezpečnostních opatření. Jedná se o aktualizovanou verzi původního „Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti“, který vznikl ve spolupráci s Ministerstvem vnitra, Státní pokladnou Centrem sdílených služeb, Ministerstvem průmyslu a obchodu, Ministerstvem zemědělství, Ministerstvem školství, mládeže a tělovýchovy a Fakultní nemocnicí Plzeň a reflektuje novou legislativu.

Cílem dokumentu je umožnit organizacím efektivně zavést a udržovat proces řízení aktiv a rizik tak, aby byla zajištěna adekvátní úroveň dostupnosti, důvěrnosti a integrity aktiv, které jsou součástí jejich regulované služby.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

! Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno. Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

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 popsanych v tomto podpůrném materiálu. Skutečnosti uvedené v přílohách slouží pouze jako příklady, nejedná se tedy o jejich kompletní výčet, například 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 popisované postupy doplněny konkrétními příklady s využitím smyšleného informačního systému (dále jen „IS“). Hodnocení rizik není nutné dělat pro každý IS zvlášť, nicméně je důležité vždy zohlednit vztah k regulované službě. Je tedy možné v rámci jednoho hodnocení rizik posoudit aktiva několika IS nebo i celé organizace najednou. Naopak ve velkých organizacích může být hodnocení rizik rozděleno do více částí, které jsou rozděleny do logických celků, například zvlášť pro sdílenou infrastrukturu, jednotlivé aplikace nebo jiné logické oblasti.

Seznam příloh a jejich popis:**Příloha 1: Vzorová politika systému řízení bezpečnosti informací**

Tento dokument obsahuje politiku ISMS fiktivního Ministerstva pro certifikaci senzorů (dále jen „ministerstvo“). V dokumentu lze nalézt:

- Cíle, principy a potřeby ISMS
- Rozsah a hranice ISMS
- Pravidla a postupy pro přezkoumání ISMS
- Pravidla a postupy pro nápravná opatření a zlepšování ISMS

Příloha 2: Vzorová metodika pro určování a hodnocení aktiv a rizik

Tento dokument obsahuje metodiku pro určování a hodnocení aktiv a rizik ministerstva, včetně kritérií pro akceptovatelnost rizik a postupu pro zvládání výjimek.

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](#).

Příloha 4: Struktura podpůrných aktiv

Tento dokument obsahuje strukturu podpůrných aktiv, která může sloužit jako inspirace při určení podpůrných aktiv viz kapitola [4.2.1 Určení podpůrných aktiv](#).

Příloha 5: Vzorová pravidla ochrany jednotlivých úrovní aktiv

Tento dokument obsahuje pravidla ochrany jednotlivých úrovní aktiv ministerstva. 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

Příloha 6: Vzorové hodnocení aktiv a rizik

Tento dokument obsahuje evidenci primárních i podpůrných aktiv ministerstva, včetně jejich vazeb a hodnocení. Dále je zde obsažen katalog zranitelností, katalog hrozeb a katalog rizik.

Příloha 7: Vzorové prohlášení o aplikovatelnosti

Tento dokument obsahuje prohlášení o aplikovatelnosti ministerstva, který je jedním z klíčových dokumentů požadovaných vyhláškou.

Příloha 8: Vzorový plán zvládání rizik

Tento dokument obsahuje plán zvládání rizik ministerstva, který je jedním z klíčových dokumentů požadovaných vyhláškou.

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 ministerstva slouží jako podklad pro výbor pro řízení KB.

Příloha 10: Vzorové hodnocení rizik pro veřejnou zakázku

Ministerstvo 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 vyhlášky a tyto účely vypracovalo hodnocení rizik, které je obsahem tohoto dokumentu.

Příloha 11: Vzorová zpráva hodnocení rizik pro veřejnou zakázku

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

Příloha 12: Vzorové alternativní hodnocení rizik u primárních aktiv

Tento podpůrný materiál v kapitole [5.13 Další povinnosti dle vyhlášky](#) popisuje alternativu pro proces hodnocení rizik. Samotné alternativní hodnocení rizik je pak obsahem této přílohy.

Příloha 13: Vzorový plán zvládání rizik alternativního hodnocení

Tento dokument obsahuje plán zvládání rizik ministerstva, který navazuje na alternativní hodnocení rizik u primárních aktiv.

Příloha 14: Zkratky a používané pojmy

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

Pro zvýšení přehlednosti dokumentu jsou využívány následující symboly:

	Upozornění Důležitá informace, na kterou je třeba upozornit, protože má zásadní význam.
	Informace Doplnující vysvětlení nebo podrobnosti, které pomohou lépe porozumět tématu.
	Modelový příklad Příklad aplikace informací a postupů vztahujících se k danému tématu.

1.2 Metoda popsaná v tomto materiálu

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

Výhody popsané metody:

- + Komplexní metodika (obecný návod)
- + Nižší náklady při použití nástroje MS Excel pro provedení hodnocení rizik u malých organizací
- + Soulad se zákonem a vyhláškou
- + Srozumitelnost a přehlednost

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

Před zahájením je nutné mít stanovenou metodiku pro určování a hodnocení aktiv a určování a hodnocení 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 pracuje v celém procesu.

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



Výstupem celého procesu je zpráva o hodnocení rizik, která popisuje výsledky procesu a prohlášení o aplikovatelnosti, ve kterém je popsáno, která bezpečnostní opatření stanovená vyhláškou byla aplikována, v jakém rozsahu a která nebyla aplikována, včetně uvedení důvodu a přijatých náhradních opatření. 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 Řízení aktiv v oblasti kybernetické bezpečnosti](#) tohoto podpůrného materiálu a problematice řízení rizik se věnuje kapitola [5 Řízení rizik v oblasti kybernetické bezpečnosti](#).

Dokumentované informace v rámci procesu řízení aktiv a rizik:

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





Obrázek 1: Stručný přehled procesu řízení aktiv a rizik

1.4 Představení modelové organizace

Pro představení postupů popsaných v tomto dokumentu na konkrétních příkladech bylo smyšleno fiktivní ministerstvo.

Ministerstvo ověřuje, zda předložené senzory splňují všechny požadavky na ně kladené dle platné legislativy a norem a vyhovujícím zařízením uděluje tříletou certifikaci. Tento proces zahrnuje nejen kontrolu předložené dokumentace výrobcí, ale také podrobné laboratorní testování senzorů v technické laboratoři ministerstva. Výsledkem certifikačního procesu je kromě udělení certifikace také podrobná neveřejná evidence obsahující informace o všech předložených testovaných senzorech. Současně je na webových stránkách ministerstva veřejně dostupný seznam certifikovaných senzorů.

Ministerstvo je jediným orgánem provádějícím certifikaci senzorů na území státu a příslušné subjekty mají povinnost používat pouze certifikovaná zařízení. Ministerstvo má celkem 2 000 zaměstnanců. Ministerstvo je poskytovatel regulované služby 1.1 Výkon svěřených pravomocí v režimu vyšších povinností, jedná se o ústřední orgán státní správy¹. Proces certifikace je probíhající v IS pro evidenci a zpracování procesu certifikace senzorů (dále také jako „agendový systém“). Výrobci senzorů mohou žádosti o certifikaci podávat prostřednictvím webové aplikace ministerstva, která je součástí tohoto IS a slouží pro externí uživatele (výrobce senzorů), je ale nutná předchozí registrace. Veškerou dokumentaci potřebnou pro proces certifikace výrobci senzorů nahrávají do aplikace ve formátu PDF. Ministerstvo má třicetidenní lhůtu na to, aby na podanou žádost reagovalo. S agendovým systémem pracuje 1 400 interních uživatelů ministerstva a 300 externích uživatelů.

Agendový systém slouží jako nástroj pro zaměstnance ministerstva, kteří jsou odpovědní za proces certifikace senzorů včetně jeho zdokumentování. Průběh jednotlivých kroků procesu certifikace je logován a agendový systém také dohlíží na dodržování zákonných lhůt. Součástí agendového systému je zmíněná webová aplikace, která umožňuje výrobcům podávat žádosti o certifikaci senzorů. Prostřednictvím této aplikace výrobce registruje daný senzor na laboratorní testy a zajišťuje jeho fyzické doručení na ministerstvo. Aplikace také slouží široké veřejnosti k zobrazení informací o certifikovaných senzorech. Certifikáty jsou automaticky po 3 letech zrušeny a senzory jsou odebrány z veřejného seznamu certifikovaných zařízení. Agendový systém je vyvíjen dodavatelskou firmou.

Na ministerstvu je také využíván personální systém, který kromě evidence údajů o zaměstnancích a správy jejich docházky slouží také pro přidělování přístupů do budovy ministerstva a jednotlivých místností, jako jsou například kanceláře, jednací místnosti, či serverovny.

Ministerstvo provozuje pro své zaměstnance dětskou skupinu jako jeden ze zaměstnaneckých benefitů. Z důvodu flexibility zapisují zaměstnanci své děti do této skupiny vždy předem na následující měsíc, a to prostřednictvím webové aplikace. Ta je dostupná z Internetu a je fyzicky i logicky oddělena od služeb a IS, které se zabývají agendou certifikace senzorů či správou docházky. Její nefunkčnost by tedy neměla na fungování ministerstva a výkon svěřené agendy žádný vliv.

¹ Příloha k vyhlášce č. 408/2025 Sb., o regulovaných službách.

Ministerstvo má tyto dodavatele:**Dodavatel A**

Dodavatel A dodává IS pro evidenci a zpracování procesu certifikace senzorů (tj. agendový systém). IS je nasazen v provozním prostředí ministerstva, ale testovací a vývojové prostředí se nachází u dodavatele. S dodavatelem byla uzavřena smlouva o dílo a servisní smlouva. Součástí smlouvy o dílo je vývojová, testovací a provozní dokumentace, školicí materiály pro uživatele a realizace jednorázového školení pro klíčové uživatele při nasazení IS do provozu. Školení dalších uživatelů IS probíhá pomocí dodaných školicích materiálů, musí proběhnout vždy při udělení přístupu k IS a za jeho provedení jsou zodpovědní výše zmínění klíčoví zaměstnanci. 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 provozně bezpečnostní monitoring IS a sběr logů. Komunikace s dodavatelem probíhá prostřednictvím ticketovacího nástroje – Helpdesku provozovaného ministerstvem. Dodavatel A je informován o tom, že je významným dodavatelem ministerstva. Dodavatel může do IS aktivně zasahovat, například může nasadit nové patche, provádět konfiguraci. Zdrojové kódy jsou ukládány do verzovacího nástroje u dodavatele.

Dodavatel B

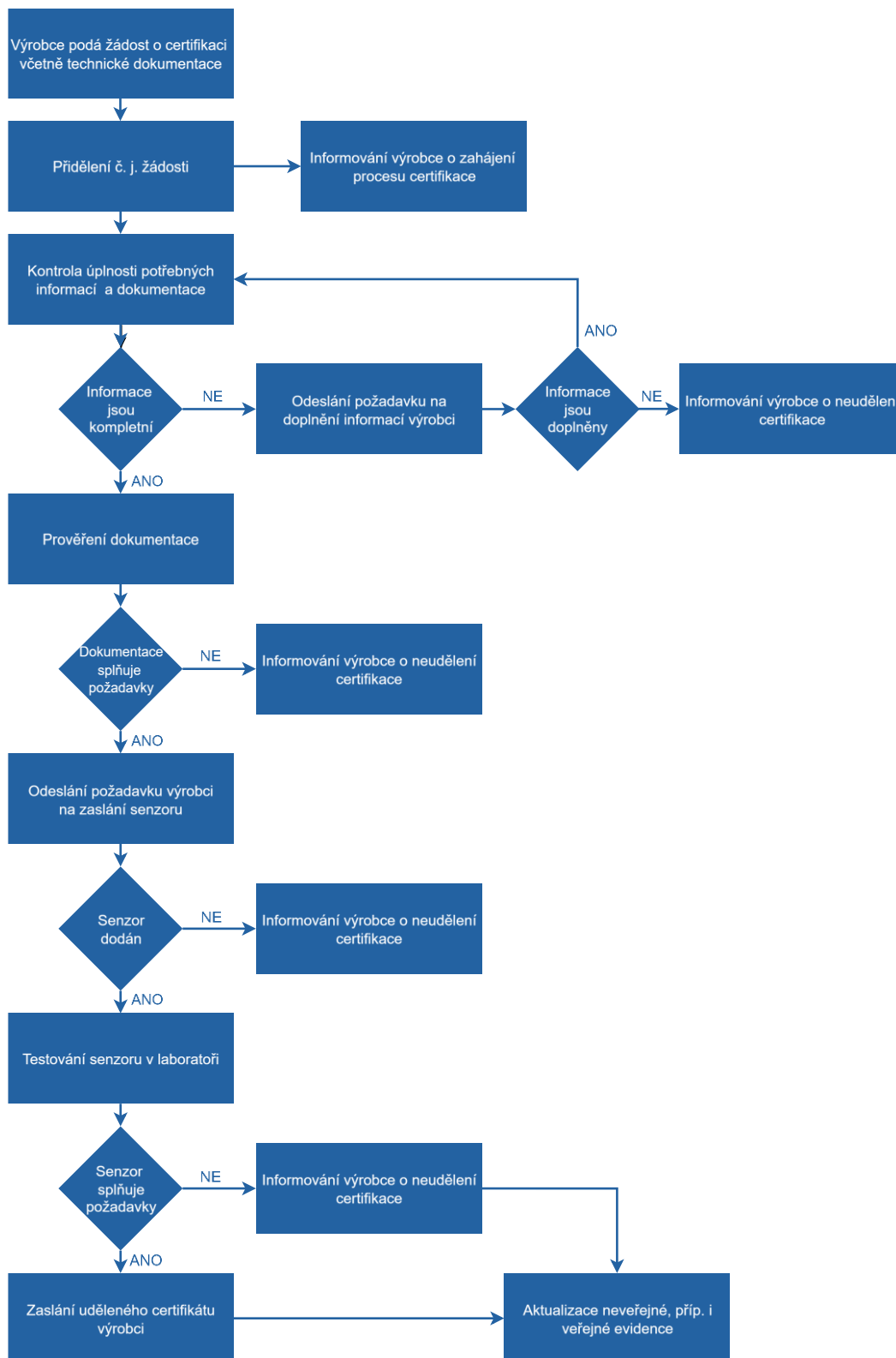
Dodavatel B dodává ministerstvu hardware (dále jen „HW“) včetně operačního systému (dále jen „OS“) určeného pro provoz a instalaci serverové infrastruktury, a dále aktivní a bezpečnostní prvky, například switche a firewally (dále jen „FW“). Dodavatel B nemůže do sítě aktivně zasahovat. Doba trvání smlouvy s dodavatelem je 5 let, přičemž dodavatel se zavázal, že bude vydávat aktualizace na tyto prvky a v případě poruchy zařízení je povinen ho vyměnit nebo opravit. Komunikace s dodavatelem probíhá prostřednictvím ticketovacího nástroje – Helpdesku provozovaného ministerstvem. Dodavatel B byl informován o tom, že je významným dodavatelem ministerstva.

Dodavatel C

Dodavatel C dodává ministerstvu koncová zařízení (například notebooky a mobilní telefony) včetně OS. Součástí dodávky je servisní smlouva zajišťující podporu ze strany dodavatele na 5 let na životnost koncových zařízení a službu Next Business Day.

1.4.1 Proces certifikace

Následující diagram zjednodušeně popisuje proces certifikace:



Obrázek 2: Přehled procesu certifikace

1.4.2 Popis jednotlivých úseků²

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, KB, fyzické bezpečnosti atd.)
 - Spadá sem role auditora KB

Pověřenec pro ochranu osobních údajů (dále jen „DPO“):

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

Odbor bezpečnostní:

- Zajištění personální, administrativní bezpečnosti, fyzické bezpečnosti a KB, bezpečnosti IS, kryptografické ochrany
 - Oddělení bezpečnosti
 - Zajištění zabezpečení stanoveného fyzického perimetru a objektů budov
 - Zajištění agendy bezpečnosti práce a požární bezpečnosti
 - Oddělení bezpečnosti ICT
 - Spadá sem role manažera KB
 - Spadá sem role architekta KB
 - Zajištění zabezpečení interní komunikační a informační sítě a IS
 - Správa bezpečnostní infrastruktury – monitoring

Sekce provozní:

- Odbor právní
 - Zajištění právního servisu pro zajištění činnosti ministerstva, administrátor výběrových a zadávacích řízení pro veřejné zakázky
- Odbor personální
 - 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, FW
 - Serverová infrastruktura
 - Oddělení provozu aplikační infrastruktury
 - Podpora aplikace a webového rozhraní

² Sekce a odbory/oddělení, které nejsou pro potřeby tohoto příkladu relevantní, nejsou rozpracovány.

- Správa databáze
- Oddělení uživatelské podpory
 - Helpdesk pro interní uživatele
 - Helpdesk pro externí uživatele
 - Interní správa pracovních stanic a mobilních zařízení
- Oddělení správy laboratoře
 - Kompletní provoz a správa technologií pro laboratoř

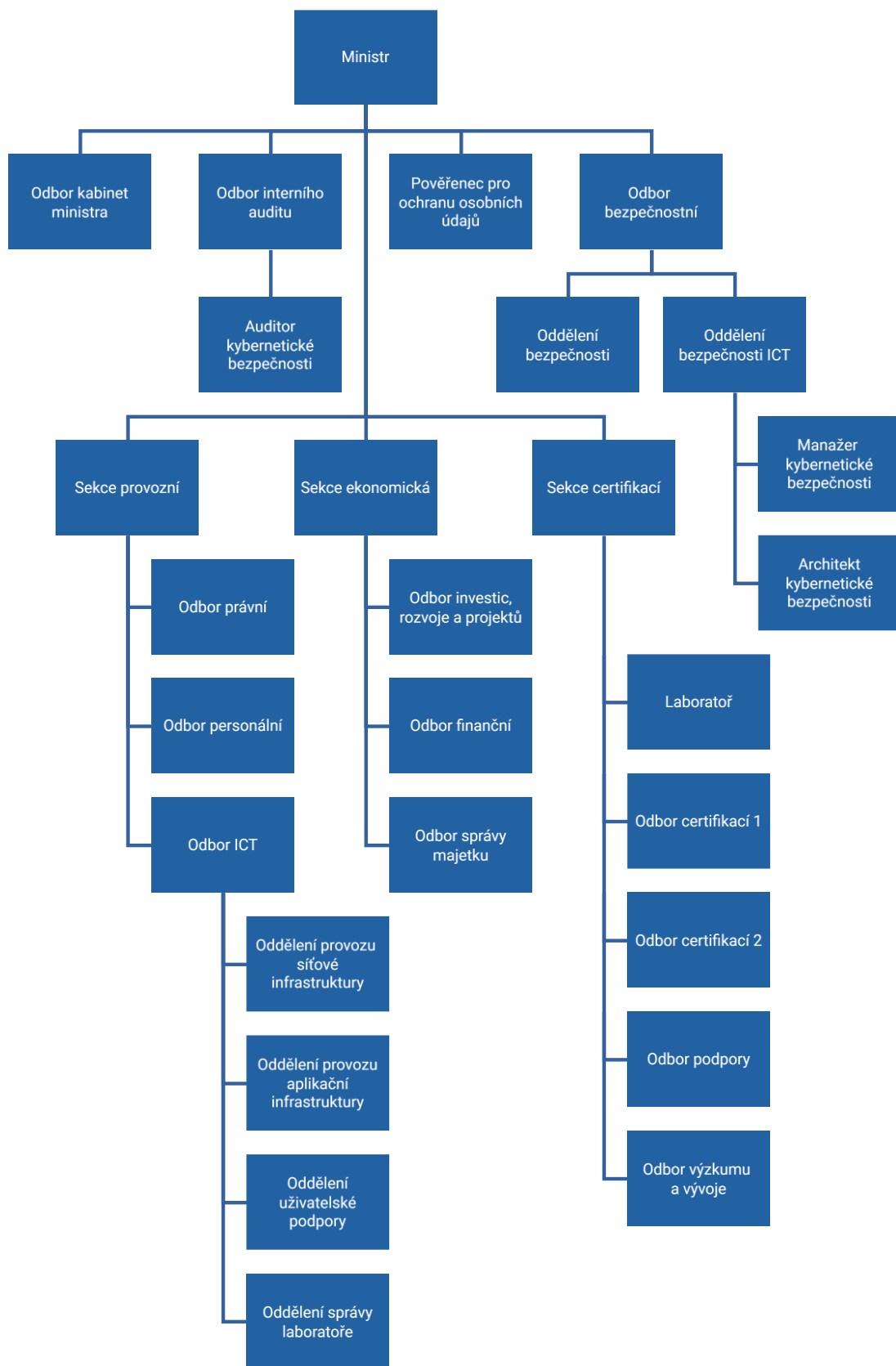
Sekce ekonomická:

- 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 přístrojů³ 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
- Odbor podpory
 - Správa žadatelů o certifikace – poskytování podpory interně i pro externí subjekty
 - 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

³ Nejedná se o senzory ve zdravotnictví.



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 oblast. Například datacentrum, ve kterém jsou ukládány informace, musí být pečlivě fyzicky chráněno, aby se do něj nedostala nepovolaná osoba a musí být zajištěna jeho odolnost vůči různým klimatickým vlivům. Důvěrnost vytištěných dokumentů musí být chráněna na stejné úrovni jako jejich elektronické originály.

2.1 Bezpečnost informací

Bezpečnost informací znamená, že je v rámci celého životního cyklu informací zajištěna jejich důvěrnost, dostupnost a integrita (také známo pod pojmem CIA triáda: C – Confidentiality, I – Integrity, A – Availability)⁴:

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



Upozornění: Pro zjednodušení jsou pojmy KB a bezpečnost informací v tomto 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 rozsahu řízení KB. Z toho plyne, že v rozsahu řízení KB musí být zahrnuto vše, co se těchto služeb či informací dotýká a má vliv na KB.



Regulované subjekty zavádějí ISMS v souladu s požadavky vyhlášky. Současně mohou při jeho zavádění vycházet také z mezinárodní normy ISO/IEC 27001. Oba přístupy se z velké části překrývají, vyhláška však některé požadavky stanovuje konkrétněji, zejména v oblasti technických bezpečnostních opatření. Norma ISO/IEC 27001 naproti tomu vymezuje požadavky obecněji a ponechává větší prostor pro volbu způsobu jejich naplnění. Například u správy autentizačních údajů stanoví obecný požadavek na jejich bezpečné řízení, zatímco vyhláška podrobněji upravuje požadavky na délku, komplexitu a další pravidla používání hesel.

⁴ Existuje řada dalších kritérií, která se dají v případě potřeby zahrnout. Jedná se například o nepopiratelnost, odpovědnost, spolehlivost, autentičnost, vlastnictví, použitelnost. Tyto parametry jsou však často vnímány jako součást základní CIA triády.



2.2.1 Stanovení rozsahu řízení kybernetické bezpečnosti

Rozsah řízení KB definuje oblasti, ve kterých je potřeba řešit zavádění bezpečnostních opatření. Více informací o stanovení rozsahu řízení KB lze nalézt v podpůrném materiálu na Portálu NÚKIB [Stanovení rozsahu řízení kybernetické bezpečnosti | Portál NÚKIB](#).

2.2.2 Cíle systému řízení bezpečnosti informací

Strategické cíle ISMS by měly být stanoveny v souladu se strategickými cíli organizace a mělo by je stanovit vrcholné vedení organizace ve fázi zavádění ISMS. Primárním cílem ISMS je zajištění bezpečnosti informací ve stanoveném rozsahu řízení KB. 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 dostupnosti, důvěrnosti a integrity
- Formalizace procesů a postupů
- Stanovení zodpovědností
- Zvýšení úrovně bezpečnostního povědomí zaměstnanců
- Soulad s legislativou, například:
 - Zákon č. 264/2025 Sb., o kybernetické bezpečnosti
 - Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
 - 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
 - Nařízení vlády č. 127/2026 Sb., o základních službách a kritériích významnosti podle zákona o kritické infrastruktuře
 - 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

Přizpůsobení strategických cílů pro konkrétní službu

Specifické cíle musí být souladné 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 stanovit následující cíle:

- Ochrana informací podle pravidel podle jednotlivých úrovní aktiv

- Zajištění výkonu služby certifikace a agendového systému během běžné pracovní doby (v režimu 8/5)
- Dodržování zákonných povinností

3 Kontext organizace

Při zavádění ISMS musíme zohlednit specifické aspekty každé jednotlivé organizace, například 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. Na samotném začátku je nutné stanovit osoby, které v tomto procesu budou mít svoji roli. V této kapitole jsou uvedeny pouze modelové příklady a klíčové činnosti zapojení jednotlivých osob a orgánů do procesu řízení aktiv a rizik. Detailní popis bezpečnostních rolí, jejich kompetencí, odpovědností a požadavků stanovuje samostatný podpůrný materiál NÚKIB věnovaný bezpečnostním rolím, dostupný na Portálu NÚKIB [Požadavky na bezpečnostní role | Portál NÚKIB](#). Níže jsou tak uvedeny pouze příklady praktického uspořádání a role v modelové organizaci a jejich možné začlenění do procesu řízení aktiv a rizik.

3.1.1 Vrcholné vedení

Vrcholné vedení společnosti nese konečnou odpovědnost za ISMS. Je potřeba, aby vrcholné vedení projevovalo aktivní podporu ISMS a systematicky se zabývalo problematikou KB. Dále musí zajistit adekvátní podmínky a zdroje pro klíčové role, které se na implementaci a udržování ISMS podílejí.

Příklad vrcholného vedení:

- Úřad – vedoucí úřadu, ředitel, předseda atd.
- Ministerstvo – ministr (například 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 KB je strategickým koordinačním orgánem pro implementaci a údržbu ISMS v působnosti organizace. Členem musí být alespoň jeden zástupce vrcholného vedení nebo jím pověřená osoba a dále manažer KB. Je také možné přizvat další role podle potřeby a tématu konkrétního jednání výboru pro řízení KB, přičemž tyto osoby nebudou mít hlasovací práva. Může se jednat například o garanty aktiv nebo auditora KB.



Modelový příklad složení výboru pro kybernetickou bezpečnost

V modelové organizaci je výbor pro řízení KB výkonným rozhodovacím orgánem, jehož členem je mj. i ministr. Rozhodnutí výboru pro řízení 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 pro řízení KB je vždy distribuován s dostatečným předstihem, aby se všichni účastníci mohli připravit. K jednání výboru pro řízení KB mohou být přizváni i další účastníci, ale je preferován menší počet členů, který přispívá k snadnější diskusi a korigování jednotlivých jednání výboru pro řízení KB. Ředitelé odborů předávají své podněty prostřednictvím svých náměstků. Z jednání výboru pro řízení KB jsou vyhotoveny zápisy (vykonává předsedou pověřená osoba), které obdrží všichni členové výboru pro řízení KB. Schvalování probíhá většinově, v případě shodného počtu hlasů má předseda výboru pro řízení KB rozhodující hlas.

Předseda výboru:

- Ministr

Místopředseda výboru:

- Ředitel odboru bezpečnosti

Členové:

- Náměstek pro řízení sekce ekonomické
- Náměstek pro řízení sekce provozní
- Náměstek pro řízení sekce certifikací
- Manažer KB
- Architekt KB

3.1.3 Manažer kybernetické bezpečnosti

Manažer KB je role, která v souladu s požadavky vrcholného vedení a výboru pro řízení KB řídí celé ISMS. Manažer KB nesmí být pověřen výkonem rolí odpovědných za provoz technických aktiv regulované služby. Tento požadavek cílí na riziko střetu zájmů, který by se u této bezpečnostní role mohl projevit v případě, že by byla odpovědná jak za provoz, tak za bezpečnost.



Modelový příklad stanovení manažera kybernetické bezpečnosti

V modelové organizaci je role manažera KB začleněna do Oddělení bezpečnosti ICT, které spadá pod Odbor bezpečnosti. Tento odbor je přímo podřízen ministrovi.

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. Tato bezpečnostní role má za úkol zajistit správný rozvoj, efektivní využívání a bezpečnost daného aktiva.



Modelový příklad stanovení garantů aktiv

Vzhledem k velikosti organizace bylo v modelovém 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 KB je bezpečnostní role, která zajišťuje bezpečnou architekturu IS s ohledem na potřeby organizace.

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

Architekt KB – 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 modelové organizaci je role architekta KB organizačně zařazena do Oddělení bezpečnosti ICT, které je součástí Odboru bezpečnosti. Odbor bezpečnosti je organizačně zařazen přímo pod ministra.

3.1.6 Auditor kybernetické bezpečnosti

Auditor KB je role odpovědná za provádění auditu KB, která zaručuje, že provedení auditu KB je nestranné. Klíčovou podmínkou je, že výkon této role je neslučitelný s výkonem rolí manažera KB a architekta KB i garanta aktiv.

Pokud se vrcholné 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 KB nebo architekta KB, aby nemohla ovlivňovat nestrannost externího auditora KB.

Modelový příklad stanovení auditora kybernetické bezpečnosti

V modelové organizaci 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 například určení a hodnocení jednotlivých aktiv a rizik. Mohou to být oddělení pracující s aktivy, pracovníci IT, běžní uživatelé atp. Dále, například 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, významní dodavatelé, uživatelé, DPO, osoby řešící kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty atd.

3.2 Klíčové informace, procesy, služby

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

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



Modelový příklad evidence služeb

Na ministerstvu byly určeny služby zaevidovány v následující tabulce (jedná se pouze o ukázkou principu, nikoliv o vyčerpávající výčet):

Tabulka 1: Zkrácený seznam služeb poskytovaných ministerstvem

Seznam služeb poskytovaných ministerstvem		
ID	Název	V rozsahu řízení KB?
S1	Služba certifikace senzorů	Ano
S2	Služba elektronické pošty	Ano
S3	Vedení úřední desky	Ano
S4	Vedení účetnictví	Ano
S5	Vedení personálních dat	Ano
S6	Vedení docházky	Ano
S7	Výkon spisové služby	Ano
S8	Zadávání veřejných zakázek	Ano
S9	Provoz dětské skupiny	Ne – nesouvisí s poskytováním regulované služby a nemá vliv na bezpečnost regulované služby
S10	...	...



3.3 RACI matice

V této kapitole je níže uvedena zjednodušená ukázka RACI matice, jejímž cílem je přehledně ilustrovat základní zapojení hlavních rolí do procesu řízení aktiv a rizik. Tato ukázka slouží pouze pro orientaci v rozdělení odpovědností, přičemž podrobná RACI matice pro celý proces řízení aktiv a rizik je uvedena v *Příloze 2 – Metodika pro určování a hodnocení aktiv a rizik*.

V praxi mohou být u jednotlivých činností dále určeny i další osoby, jejichž zapojení je vzhledem ke konkrétním podmínkám organizace vhodné.

Tabulka 2: Zjednodušená RACI matice

Činnosti	Výbor KB	Manažer KB	Auditor KB	Architekt KB	Garant aktiva
Stanovení rozsahu řízení KB 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
Přezkoumání a aktualizace ISMS	A, R	R		C	C
Audit KB	I	C	A, R	C	C

Legenda:

R – Responsible (ti, kteří práci / úkol vykonávají)

A – Accountable (ti, kteří zodpovídají za celkové splnění)

C – Consulted (ti, kteří by se k danému mohli vyjádřit a být nápomocni s jeho řešením)

I – Informed (ti, kteří mají být informováni)

4 Řízení aktiv ve vztahu ke kybernetické bezpečnosti

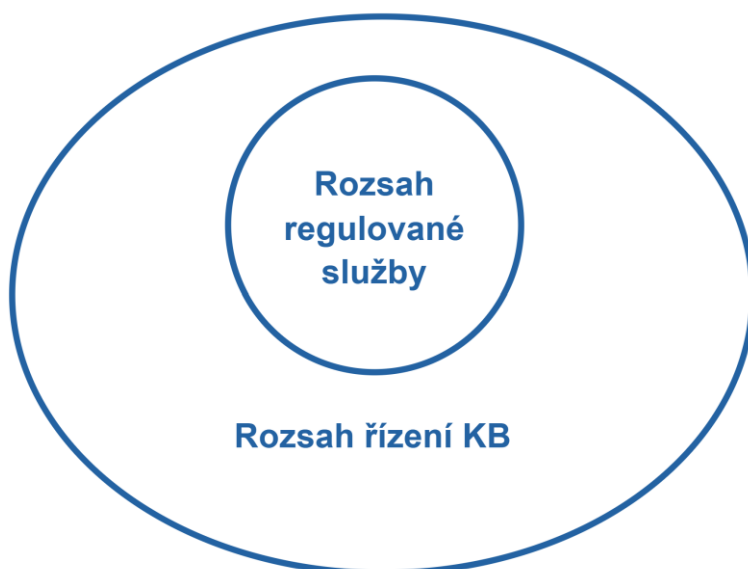
Aktivem je fyzický nebo digitální prostředek, osoba nebo činnost související se zpracováním informací a dat v elektronické podobě.

S ohledem na KB jsou rozlišována aktiva:

- **primární** (zpracovávané informace nebo poskytované služby)
- **podpurná** (zajišťující fungování primárních aktiv – zejména zaměstnanci, dodavatelé, technická aktiva, budovy a jiné ohraničené prostory, ve kterých se nachází aktiva regulované služby)

V rámci ISMS jsou řízena ta aktiva, která se nachází v rozsahu řízení KB. Z tohoto důvodu je nutné znát rozsah řízení KB a určit všechna aktiva, která do něj spadají. Pokud by došlo k vyloučení aktiv souvisejících s regulovanou službou z rozsahu řízení KB, mohlo by to mít významný, v některých případech až fatální dopad na výsledný stav ISMS. K tomu, abychom těmto situacím předcházeli, slouží pravidelné přezkoumávání a neustálé zlepšování ISMS, kdy dochází mj. k aktualizaci rozsahu řízení KB. Určená aktiva jsou následně evidována, jsou jim přiřazeni garanti, jsou ohodnocena a vstupují do procesu řízení rizik.

Dále je také potřeba si uvědomit rozdíl mezi aktivy, která jsou v rozsahu regulované služby a aktivy, která jsou v rozsahu řízení KB. Aktiva v rozsahu regulované služby jsou pouze ta aktiva, která mají přímou spojitost s regulovanou službou poskytovanou IS, zatímco aktiva v rozsahu řízení KB jsou aktiva, která nemají přímou vazbu na regulovanou službu, ale mají vliv na bezpečnost aktiv v rozsahu regulované služby. Aktiva v rozsahu regulované služby jsou tedy podmnožinou aktiv spadajících do rozsahu řízení KB.



Obrázek 4: Schéma rozsahu řízení KB

V tomto dokumentu je pracováno s typovými aktivy (jak u primárních, tak u podpůrných aktiv).

Typová aktiva jsou uměle vytvořené skupiny aktiv, která 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 není možné 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 vypovídací hodnota, schopnost nalézat konkrétní rizika a prioritizovat jejich zvládání dle důležitosti.

Kromě základních atributů bezpečnosti informací (**důvěrnost, integrity a dostupnost**) byl v tomto podpůrném 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 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 a přezkoumávat jeho výsledky. Typová aktiva, která se při prvotním určení aktiv zdála jako vhodně zvolená, mohou být při přezkoumání nebo v průběhu hodnocení rizik vyhodnocena jako nedostatečná. 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. Aktiva také vznikají a zanikají, proto je důležité přezkoumávání, zlepšování a neustálý vývoj celého procesu a jeho výstupů.

Pro prvotní určení aktiv je doporučeno začínat s menším množstvím typových aktiv, ale celý proces korektně dokončit.

Veškerý postup týkající se určení aktiv, evidence aktiv, určení garantů aktiv, určení vazeb mezi aktivy a hodnocení aktiv musí být popsán v dokumentované podobě, například v **metodice pro určení a hodnocení aktiv**. 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 hodnotící osobě.

Evidence aktiv, často označovaná také jako katalog aktiv, je jedním ze stěžejních dokumentů procesu řízení aktiv, který obsahuje detailní informace o jednotlivých aktivech, včetně jejich hodnocení, určených garantů atd.



Modelový příklad řízení aktiv

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



4.1 Primární aktiva

Primární aktiva jsou vnímána jako poskytované **služby a zpracovávané informace**, které jsou součástí vymezeného rozsahu řízení KB. Rozsah musí být stanoven za účelem ochrany těchto aktiv.

i Ve většině případů jsou primární aktiva spojena především s výkonem určité agendy, poskytováním služby apod. Jsou to takové služby a informace, jejichž ztráta nebo narušení by mělo dopad na chod, funkčnost, účel a bezpečnost celé organizace, případně IS nebo služby s vazbou na vymezený rozsah řízení KB z hlediska důvěrnosti, integrity a dostupnosti.

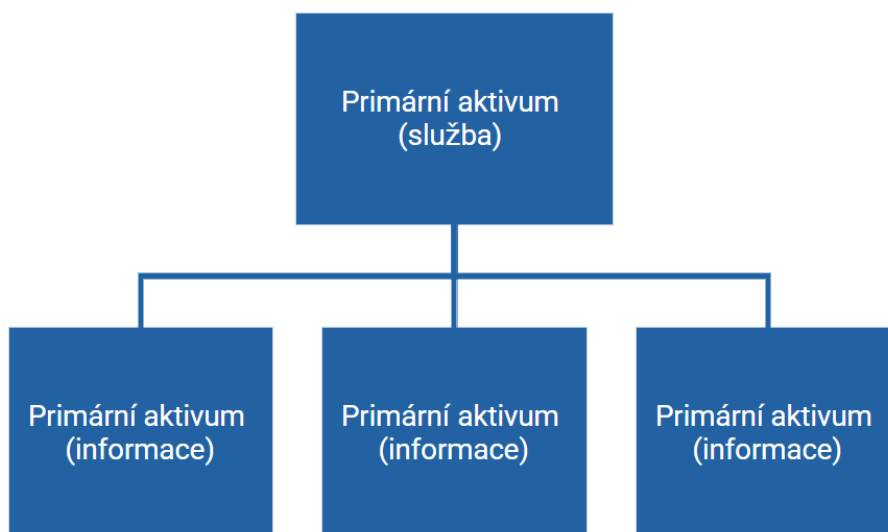
Jako primární aktiva je možné určit například:

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

4.1.1 Určení primárních aktiv

Při určení primárních aktiv můžeme vycházet nejen z povahy regulované služby, ale například i z analýzy hlavních činností celé organizace. Klíčovou součástí tohoto procesu jsou tedy rozhovory s vedoucími odborných útvarů. Dále je možné čerpat například z:

- Organizačního řádu
- Zakladací listiny
- Legislativních zdrojů
- Smluv, směrnic, příruček, manuálů
- Interních aktů řízení organizace



Obrázek 5: Vazby mezi primárními aktivy

V některých případech nelze jednoznačně určit a vytvořit primární aktiva z informací, které jsou v rámci služby zpracovávány. Tato situace nastává především u nestrukturovaných typů informací, například e-mailové služby. V tom případě je možné pracovat pouze s primárním aktivem typu služba. Za zpracování informací – poskytnutí služby – se v tomto případě považuje i prosté zobrazení, například zobrazení textu na obrazovce, přehrání zvuku. Jeden IS může poskytovat více služeb, jednotlivé služby lze dělit na menší typová aktiva typu služba; například službu certifikace senzorů je možné rozdělit na službu zveřejňování informací o certifikovaných senzorech, službu certifikování výrobců, službu dokumentace procesu certifikace. 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 určení primárních aktiv

- O kterou kategorii regulované služby se jedná podle zákona?
- Jaký je účel této organizace, agenty či poskytované služby?
- Jaké jsou v rámci této organizace, agenty či poskytované služby klíčové procesy?
- Jací jsou klíčoví zákazníci či uživatelé této organizace, agenty či poskytované služby?
- Bez jakých informací nemůžete vykonávat svoji práci?
- Jaké činnosti jsou potřeba k vykonávání běžné agenty?
- Jakou pro mě má agenda či poskytovaná služba hodnotu (z pohledu významu/smyslu) a co je v něm to důležité?
- Jsou součástí této organizace, agenty či IS osobní údaje, citlivé osobní údaje nebo obchodní tajemství?
- Jsou s existencí této organizace, agenty 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 souvislosti s výkonem běžné pracovní činnosti?



Modelový příklad určení primárních aktiv

Při určení primárních aktiv regulované služby ministerstvo zkoumá organizaci jako celek a určí všechna primární aktiva zahrnující služby a informace, které zpracovává a poskytuje. Tato aktiva představují poskytované služby, jako jsou například certifikace senzorů, spisové služby či provoz dětské skupiny. Dále sem spadají informace jako technická dokumentace, podané žádosti a výsledky certifikačního procesu.

V dalším kroku ministerstvo posoudí, která z určených primárních aktiv jsou skutečně aktivně používána a relevantní pro poskytování regulované služby. V případě, kdy organizace chce rozsah řízení KB zúžit, je nutné specifikovat primární aktiva, která byla vyjmuta z tohoto rozsahu, a uvést důvody pro jejich vyloučení. Například služba provozování dětské skupiny bude vyjmuta, protože neodpovídá hlavním činnostem zaměřeným na poskytování regulované služby.

Služby:

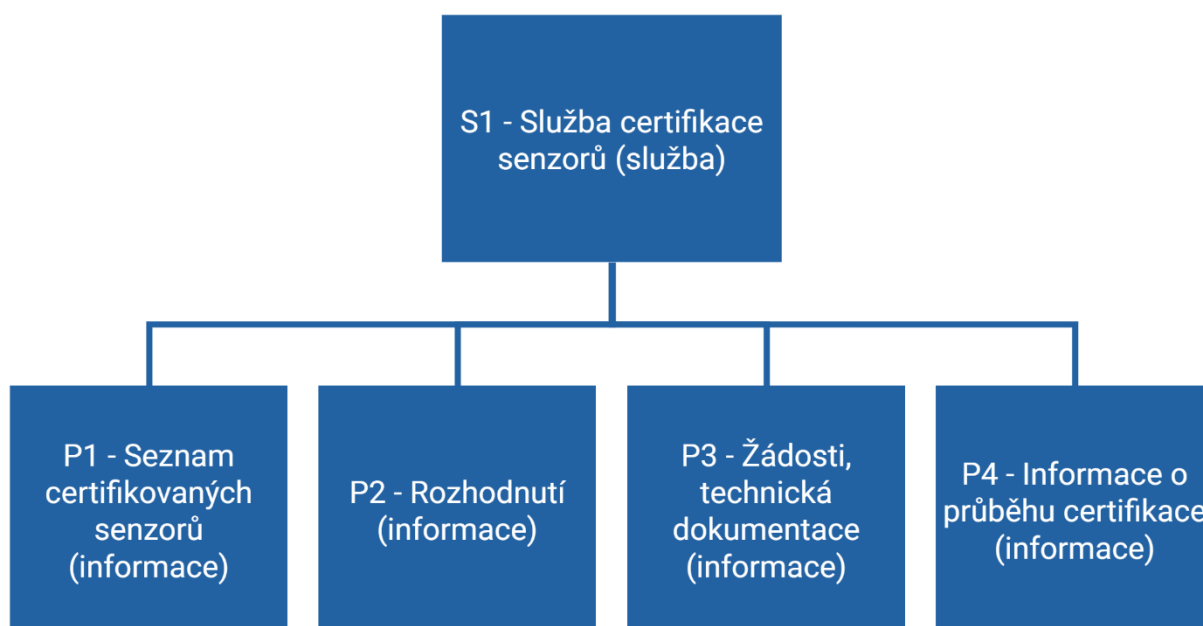


- Služba certifikace senzorů

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 hodnocením jednotlivých atributů bezpečnosti informací (důvěrnost, integrita, dostupnost, ztráta), se kterými tato služba pracuje.

Informace:

- Seznam certifikovaných senzorů
- Rozhodnutí
- Žádosti, technická dokumentace
- Informace o průběhu certifikace



Obrázek 6: Vazby mezi primárními aktivy ministerstva

Obdobný postup bude použit i u dalších primárních aktiv, která jsou součástí stanoveného rozsahu řízení KB dané organizace.

4.1.2 Evidence primárních aktiv

Všechna určená primární aktiva, která se nachází v rozsahu řízení KB, musí být zaznamenána v dokumentované podobě⁵. Způsob, jakým tato evidence bude provedena, je na zvážení každé organizace.

Příklad atributů uchovávaných o primárním aktivu:

- ID aktiva
- Název
- Garant aktiva

⁵ Někdy označováno jako Katalog primárních aktiv.

- Hodnocení aktiva z hlediska důležitosti (CIA)
- Detailní popis⁶ – v případě, že se jedná o typové aktivum tak i specifikace toho, co zahrnuje
- Další informace o aktivu – například kdo jsou jeho uživatelé, jaké agendy jej využívají, jaká legislativa se aktiva týká


Modelový příklad evidence primárních aktiv

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

Tabulka 3: 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)

Modelová organizace zároveň eviduje vazby mezi jednotlivými primárními aktivy.

⁶ Z detailního popisu aktiva by mělo být zcela zřejmé, o jaké aktivum se jedná, aby při dalších revizích nevznikalo nedorozumění nebo zkreslení.



Tabulka 4: 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, například prostřednictvím výboru pro řízení KB. Je nezbytné k jednotlivým primárním aktivům přiřadit guaranty aktiv a evidovat je.

Manažer KB by měl jednotlivé guaranty primárních aktiv vytipovat, například s pomocí organizačního řádu, a následně s nimi tuto skutečnost konzultovat. Stanovení garantů primárních aktiv by mělo být zaznamenáno formalizovaným způsobem (například určení vrcholným vedením organizace či výborem pro řízení KB).

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

Guaranti 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

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 KB zvolil jednotlivé guaranty 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 určit 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.

Při hodnocení primárních aktiv je posuzován dopad narušení bezpečnosti informací, je tedy nutné tato aktiva hodnotit **minimálně z pohledu důvěrnosti, integrity a dostupnosti**.

! Při posuzování hodnoty aktiv je nutné uvažovat o **nejhorším možném scénáři a nebrat v úvahu již aplikovaná 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, například režim vysoké dostupnosti vs. postup zálohování.

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

Tabulka 5: Stupnice pro hodnocení důvěrnosti, integrity a dostupnosti

Úroveň		Důvěrnost	Dostupnost	Integrita	Ztráta
1	Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.	Narušení dostupnosti aktiva, například v případě výpadku v jednotkách týdnů, je běžně tolerováno a nemá žádný nebo zanedbatelný dopad na poskytovanou regulovanou službu.	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Ztráta aktiva nemá žádný nebo pouze zanedbatelný dopad na činnost povinné osoby. Aktivum je snadno obnovitelné bez významných nákladů či důsledků.
2	Střední	Aktiva nejsou veřejně přístupná, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Narušení dostupnosti aktiva by nemělo překročit dobu například jednoho pracovního dne, dlouhodobější výpadek vede k možnému ohrožení poskytování regulované služby povinné osoby.	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.	Ztráta aktiva může způsobit provozní komplikace, jejichž řešení nevyžaduje vysoké úsilí nebo náklady. Ztráta neohrožuje činnost povinné osoby jako celek, ale může způsobit nepříjemnosti nebo zdržení.
3	Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).	Narušení dostupnosti aktiva by nemělo překročit dobu například několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení poskytování regulované služby. Aktiva jsou považována za velmi důležitá.	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Ztráta aktiva má negativní dopad na činnost povinné osoby. Obnova je složitá, nákladná nebo časově náročná. Může vést k poškození oprávněných zájmů, dobrého jména nebo dočasnému výpadku poskytovaných služeb.
4	Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).	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.	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.	Ztráta aktiva má zásadní a okamžitý dopad na činnost povinné osoby. Aktivum je nenahraditelné nebo jeho ztráta vede k vážným právním dopadům, ztrátě schopnosti plnit smluvní závazky nebo dlouhodobému výpadku poskytovaných služeb.

Dále je při hodnocení primárních aktiv potřeba posoudit alespoň ty relevantní oblasti uvedené v tabulce č. 4 přílohy č. 1 vyhlášky. Organizace by však měla při hodnocení aktiv rozšířit zaměření i na další oblasti podle svých potřeb a specifikací.

Následující tabulka vymezuje minimálně vybrané oblasti pro hodnocení primárních aktiv, včetně podrobného popisu.

Tabulka 6: Oblasti hodnocení primárních aktiv

Dopad podle vyhlášky	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 musí být nepřetržitě dostupná vzdáleným přístupem. Porušení smlouvy a z ní plynoucí sankce. Únik obchodního tajemství. Porušení legislativy a z toho plynoucí pokuty.
c) rozsah narušení vnitřních řídicích a kontrolních činností	Narušení rozhodovacích možností.	Neúplnost nebo modifikace informací potřebných pro rozhodování vedení a kontrolní činnost.
d) poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty	Zajištění důležitých externích informací týkajících se organizace například 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. Například nedostupnost internetových stránek, může vést k neinformování veřejnosti o důležitých skutečnostech (záplavy, ekologické katastrofy atd.).
e) dopady na poskytování důležitých služeb	Narušení klíčových informací, procesů a služeb tvořících hodnotu nebo užitek organizace.	Narušení všech informací a služeb vztažených směrem k regulované službě a hlavnímu cíli (účelu existence) organizace.
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 (například nemocnice, chemická továrna).	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.

	republiku u EU, NATO nebo dalších zahraničních zemí a mezinárodních organizací.	Únik informací od partnera, který je součástí mezinárodního koncernu.
j) dopady na uživatele regulované služby	Znemožnění výkonu činnosti interním i externím uživatelům.	Ztráta možnosti přístupu uživatele ke službě vlivem její nedostupnosti.

Hodnocení aktiv může probíhat na společném manažera KB s jednotlivými garanty aktiv. Před samotným hodnocením doporučujeme seznámit garanty s metodikou pro určování a hodnocení aktiv, například formou zaslání manuálu nebo formou školení. Odpovědnost za provedení hodnocení aktiv by měl mít manažer KB, avšak může touto odpovědností pověřit jiného, kvalifikovaného pracovníka v organizaci. Tato osoba (či samotný manažer KB) 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.

Při hodnocení jednotlivých atributů (důvěrnost, integrita a 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, například 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 například:

- 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?

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 ministerstva byla vytvořena dopadová tabulka uvedená v Příloze č. 3 Zjednodušená dopadová tabulka.

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.

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

Tyto atributy jsou dále členěny:

- **důvěrnost:** prozrazení v organizaci, 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 určeny relevantní oblasti, například ochrana osobních údajů, zákonné a smluvní povinnosti, finanční ztráty a u těch bylo provedeno hodnocení z pohledu důvěrnosti, integrity, dostupnosti a ztráty dat.

Například během rozhovoru manažera KB 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 primárních aktiv.



Tabulka 7: 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 1 den	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. Například 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															

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 musíme porovnat všechny údaje v tabulce a vybrat úroveň dostupnosti, která nejlépe odpovídá našim 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. Tento postup byl zvolen z toho důvodu, že se povinnosti zákona a vyhlášky v tomto bodě prolínají s GDPR a může tak dojít k synchronizaci v organizaci. Samotná dopadová tabulka je uvedena v Příloze č. 2: *Vzorová metodika pro určování a hodnocení aktiv a rizik*.

Metodiku lze nalézt na [webových stránkách Úřadu pro ochranu osobních údajů](#).

Tabulka 8: Katalog primárních aktiv modelové organizace

ID	Typové primární aktivum	Název	Kategorie	Specifikace	Gestor aktiva	Garant aktiva	Osobní údaje	Legislativa	Rozsah řízení KB	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	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	2	1	1	3
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	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	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	3	4	3	3

P5	Provoz dětské skupiny	P5: Provoz dětské skupiny	služba	Zajištění provozu dětské skupiny pro děti zaměstnanců ministerstva	náměstek sekce provozní (Tomáš Dvořák)	vedoucí odboru personálního (Anna Veselá)	ano	Zákon č. 247/2014 Sb. o poskytování služby péče o dítě v dětské skupině a o změně souvisejících zákonů	ne	3	2	2	1
----	-----------------------	---------------------------	--------	--	--	---	-----	--	----	---	---	---	---

Tabulka 98: 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:	02.11.2025		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	<i>Dostupnost</i>	3	
	<i>Ztráta</i>	4	
	<i>Důvěrnost</i>	3	
	<i>Integrita</i>	3	

Tabulka 10: 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 1 den	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 řídicích 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 regulované služby	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 <i>(uveďte odůvodnění k následkům narušení dostupnosti-odkdy a proč začíná mít nedostupnost negativní dopad, narušení důvěrnosti-například porušení pravidel GDPR, narušení integrity dat-například chyba při zpracování dat agendy)</i>	Hodnoty služby certifikace senzorů přebírají nejvyšší hodnoty, které byly stanoveny pro jednotlivá primární aktiva P1-P4. Dostupnost je pro tuto službu stanovena na hodnotu „3“, jelikož kritický dopad v této tabulce nastává při nedostupnosti 1 týden a více, nikoliv v případě nedostupnosti v řádu minut, jak stanovuje hodnocení „4“ dle vyhlášky.																						

4.2 Podpůrná aktiva

Jedná se o aktiva nutná pro správnou funkčnost, zpracování a uchování primárních aktiv. Podpůrná aktiva jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti aktiv regulované služby. Dále jsou jako podpůrná aktiva vnímány budovy a jiné ohraničené prostory, ve kterých se tato aktiva nacházejí.

Technickými aktivy jsou technické nebo programové prostředky nebo vybavení, tvořící informační systémy nebo průmyslové, řídicí a jiná obdobná specifická aktiva tvořící například průmyslové a řídicí systémy.

Možné kategorie podpůrných aktiv

- Technické vybavení
- Komunikační prostředky
- Programové vybavení
- Budovy a jiné ohraničené prostory
- Lidské zdroje
- Dodavatelé
- Externí systémy a služby

Technické vybavení (HW)

- Do technického vybavení (tzv. HW) spadají fyzické komponenty (zpravidla si na ně můžeme sáhnout) regulované služby 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 a datové nosiče (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, ...), tak i bezdrátová (Wi-Fi, ...) připojení a veškeré komponenty, které jsou potřebné pro realizaci těchto připojení – tedy mimo aktivních prvků, například síťová zařízení jako jsou směrovače (router) či přepínače (switch).

Programové vybavení (SW)

- Do programového vybavení (tzv. 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 například OS, firmware, kancelářské balíky, ale i přístupové a bezpečnostní aplikace.

Budovy a jiné ohraničené prostory

- Do budov a jiných ohraničených prostor spadají fyzické prostory, ve kterých se regulované služby nebo jejich části nachází. Do této kategorie spadají areály, objekty, inženýrské sítě apod.

Lidské zdroje

- Do lidských zdrojů spadá veškerý personál, který má vliv na regulované služby nebo jejich části. Do této kategorie jsou zahrnuti například uživatelé, administrátoři, vývojáři, bezpečnostní role, ale také vedení organizace nebo administrátoři dodavatele.

Dodavatelé

- Do kategorie dodavatelů spadají například významní dodavatelé, subdodavatelé, výrobci nebo poskytovatelé cloud computingu.

Externí systémy a služby

- Do externích systémů a služeb spadají veškeré externí systémy a služby, které jsou nezbytné pro zajištění funkčnosti regulované služby nebo jejich částí. Do této kategorie jsou zahrnuty například dodávky elektřiny, certifikační služby.

! Některá podpůrná aktiva nelze zařadit pouze do jedné z těchto kategorií. Proto je možné vytvořit typové aktivum, které bude obsahovat více kategorií. Pro hodnocení rizik je však nezbytné **určit relevantní hrozby a zranitelnosti pro všechny kategorie** příslušného typového aktiva.

4.2.1 Určení podpůrných aktiv

Při určení podpůrných aktiv je nutné vycházet z architektury systému a potřeby pro funkčnost primárního aktiva.

Otázky, které mohou vést k určení podpůrných aktiv

- 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 určit a řídit rizika s aktivy spojená.

Pokud je detail příliš malý (například celá budova), budou se muset rizika řídit 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 stanovení vhodných

bezpečnostních opatření mnohem náročnější u rizik, která vznikla obecně definovanou kombinací aktivum-zranitelnost-hrozba.

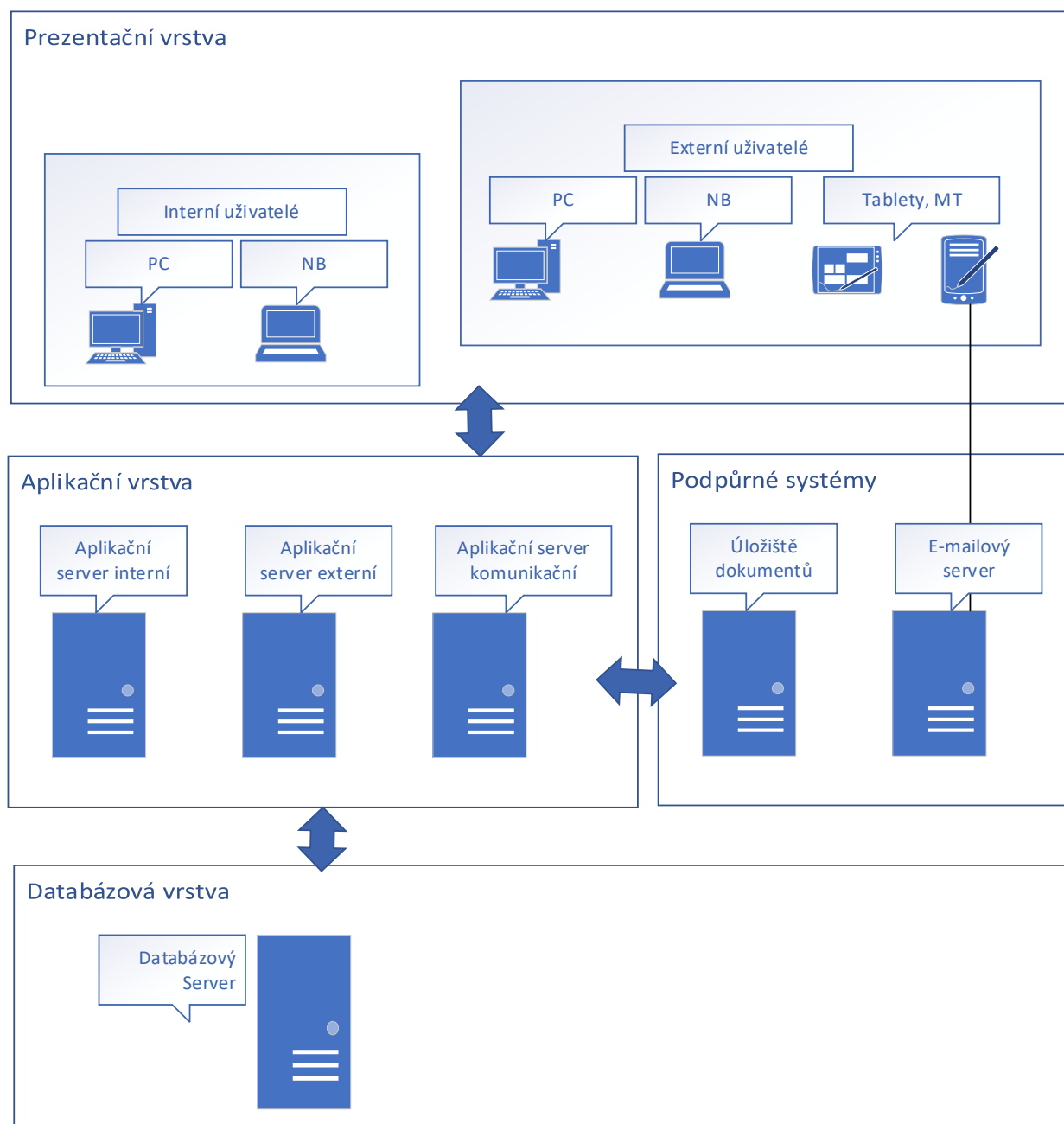
Pokud je detail příliš velký, vzniká velké množství podpůrných aktiv. V tomto případě je zde hrozba nedostatečných kapacit pro jejich adekvátní řízení.



Modelový příklad určení 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 11: Popis agendového systému ministerstva

Oblast	Popis
Serverová infrastruktura (HW prostředí)	- HW DB serveru (1x standalone server) - HW aplikačního serveru (3x standalone server)
Serverová infrastruktura (OS)	- OS databázové vrstvy (OS Linux) - OS 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 11, cca 1/4 na Windows 10 - Jedná se o 1400 zaměstnanců
Uživatelé systému – externí	- Externí uživatelé se mohou hlásit pouze pomocí Microsoft Edge - 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, školicí dokumentace pro uživatele
Školení uživatelů pro práci s aplikací	Školení absolvují pouze vybraní klíčoví uživatelé, kteří musí proškolit ostatní

Na základě těchto informací byla určena typová podpůrná aktiva spadající do rozsahu řízení KB. 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 určení podpůrných aktiv mělo vliv také varování od 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, dostupnosti a integrity
- Detailní popis – v případě, že se jedná o typové aktivum tak i specifikace toho, co zahrnuje
- Další informace o aktivu – například kdo jsou jeho uživatelé, jaké agendy jej využívají, jaké mají dodavatele, zda se jedná o významné dodavatele

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 ukázkou z Katalogu podpůrných aktiv (katalog lze nalézt v *Příloze 6: Vzorové hodnocení aktiv a rizik*).

Tabulka 12: Ukázka z Katalogu podpůrných aktiv

ID	Kategorie podpůrného aktiva	Skupina podpůrného aktiva	Typové podpůrné aktivum	Název	Popis podpůrného aktiva	Gestor aktiva	Garant aktiva
P01	Technické vybavení (HW)	Servery	Aplikační server (HW)	P01: Aplikační server (HW)	2x standalone server	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu síťové infrastruktury (Aleš Pokorný)
P02	Technické vybavení (HW)	Servery	Databázový server (HW)	P02: Databázový server (HW)	1x standalone server	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu síťové infrastruktury (Aleš Pokorný)
P03	Technické vybavení (HW)	Servery	Webový server (HW)	P03: Webový server (HW)	1x standalone server, servery výrobce, na něž se vztahuje varování NÚKIB ze 17.12.2018	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu síťové infrastruktury (Aleš Pokorný)
P04	Programové vybavení (SW)	Systémový SW	OS–aplikační server	P04: OS–aplikační server	2x standalone server, licence	ředitel odboru ICT (Josef Dvořák)	vedoucí oddělení provozu aplikační infrastruktury (Tomáš Fiala)
P05	Programové vybavení (SW)	Systémový SW	OS – databázový server	P05: OS–databázový server	1x standalone	ředitel odboru ICT	vedoucí oddělení provozu aplikační



					server, licence	(Josef Dvořák)	infrastruktury (Tomáš Fiala)
--	--	--	--	--	--------------------	-------------------	---------------------------------

i Modelová organizace v Katalogu podpůrných aktiv eviduje také významné dodavatele těchto podpůrných aktiv.

4.2.3 Určení garantů podpůrných aktiv

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

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

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

Guaranty 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 je uvedeno 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 KB vytipoval vhodné osoby pro role garantů aktiv. Například správu databází 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, například správu externích žadatelů 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 nutné provést jejich hodnocení a posoudit dopad případného narušení bezpečnosti informací. Tato aktiva je tedy nezbytné hodnotit minimálně z pohledu důvěrnosti, integrity a dostupnosti.

Při posuzování dopadu narušení dostupnosti je možné další rozdělení na nedostupnost a úplnou ztrátu dat. Tento podpůrný materiál používá pro hodnocení aktiv, stejně jako vyhláška, 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 kapacitě 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 dostupnost, integrita, důvěrnost a ztráta.

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



Váha vlivu nabývá hodnot podle následující tabulky:

Tabulka 13: *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:

$$\text{Hodnota podpůrného aktiva} = \text{váha vlivu} \times \text{hodnota primárního aktiva}$$

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 14: *Hodnota podpůrného aktiva*

Hodnota podpůrného aktiva = váha vlivu × 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 je dále potřeba stanovit a zavést pravidla ochrany nutná pro zabezpečení bezpečnosti informací jednotlivých aktiv. Tato pravidla mají obsahovat:

- Přípustné způsoby používání aktiv
- Pravidla pro manipulaci s aktivy, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášání aktiv
- Pravidla pro klasifikaci informací
- Pravidla pro označování aktiv
- Pravidla správy výměnných médií
- Pravidla pro určení způsobu likvidace informací a dat a jejich kopií a likvidace technických aktiv, která jsou nosiči informací a dat s ohledem na úroveň aktiv v souladu s přílohou č. 2 vyhlášky

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 vyhlášky (možné způsoby ochrany aktiv), příloha č. 2 vyhlášky (likvidace dat) a použití například 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: [Národní úřad pro kybernetickou a informační bezpečnost - Sdílení informací](#).

Modelový příklad klasifikace informací

Ministerstvo 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 výměnných médií. Aktiva jsou označována v souladu s nastavenými pravidly podle jejich klasifikace.

Modelový příklad pravidel pro nakládání s aktivy

Ministerstvo 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. 2 vyhlášky definovány způsoby mazání dat a způsoby likvidace technických nosičů informací, provozních údajů, informací a jejich kopií. 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 vyhlášky v sobě hodnocení rizik zahrnuje určení rizik, analýzu rizik a vyhodnocení rizik. Zatímco analýza rizik dle vyhlášky 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 řízení KB popsaného v dokumentu *Příloha 1: Vzorová politika systému řízení bezpečnosti informací*, dle platné metodiky *Příloha 2: Vzorová metodika pro určování a hodnocení aktiv a rizik* a evidence rizik je součástí *Přílohy 6: Vzorové hodnocení aktiv a rizik*.

5.1 Katalog zranitelností

Zranitelností se rozumí slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou či více hrozbami a tím vyvolat nežádoucí vliv. Jedná se o citlivost aktiva vůči konkrétní hrozbě.

Dle § 8 odst. 1 písm. b) vyhlášky je nutné vytvořit a vést katalog zranitelností a využít zejména její přílohu č. 3, která obsahuje vybrané kategorie zranitelností, které budou dále upraveny pro potřeby organizace.

Zranitelnosti dle přílohy č. 3 vyhlášky jsou:

- Nedostatečná údržba aktiv
- Zastaralost aktiv
- Nedostatečná ochrana perimetru
- Nedostatečné bezpečnostní povědomí uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
- Nedostatečné zálohování
- Nevhodné nastavení přístupových oprávnění
- Nedostatečné postupy a procesy pro detekování kybernetických bezpečnostních událostí a identifikování kybernetických bezpečnostních incidentů
- Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit činnost, která může mít vliv na bezpečnost regulované služby
- Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
- Nedostatečná ochrana aktiv



- Nevhodně navržená bezpečnostní architektura
- Nedostatečná míra nezávislé kontroly
- Neschopnost včasného odhalení pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
- Nedostatek zaměstnanců s potřebnou odbornou úrovní znalostí
- Umístění aktiva mimo fyzickou kontrolu (například na území cizího státu)
- Umístění aktiva na území státu, o jehož právním prostředí nemá povinná osoba dostatečné povědomí
- Zranitelnosti odhalené při skenování zranitelností a penetračním testování

**Modelový příklad vytvoření katalogu zranitelností**

Pro ministerstvo byly obecně definované zranitelnosti vyhláškou 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 vyhlášce, ostatní je možné najít v Příloze 2: *Metodika pro určování a hodnocení aktiv a rizik* a v Příloze 6: *Vzorové hodnocení aktiv a rizik*.



Tabulka 15: 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 používána produkční data. 5) Nejsou stanoveny priority obnovy informačních systémů ze zálohy. 6) Neprobíhá profylaxe a údržba. 7) Jsou vydávány aktualizace dodavatelem/výrobce, 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 jakákoliv potenciální okolnost, událost nebo jednání, které mohou být příčinou kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, a která může poškodit, narušit nebo jinak nepříznivě ovlivnit aktiva, jejich uživatele nebo další osoby. Hrozba může být úmyslná, neúmyslná či na základě vyšší moci.

Dle § 8 odst. 1 písm. b) vyhlášky je nutné vytvořit katalog hrozeb a využít zejména její přílohu č. 3, která obsahuje vybrané kategorie hrozeb, které budou dále upraveny pro potřeby organizace.

Hrozby dle přílohy č. 3 vyhlášky jsou:

- Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
- Poškození nebo selhání technického anebo programového vybavení
- Zneužití identity
- Užívání programového vybavení v rozporu s licenčními podmínkami
- Škodlivý kód
- Narušení fyzické bezpečnosti
- Přerušení poskytování služeb elektronických komunikací, družicových služeb nebo dodávek elektrické energie nebo jiných důležitých služeb
- Narušení dostupnosti primárních nebo podpůrných aktiv umístěných mimo území České republiky
- Zneužití nebo neoprávněná modifikace informací
- Ztráta, odcizení nebo poškození aktiva
- Nedodržení smluvního závazku ze strany dodavatele
- Pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení
- Zneužití vnitřních prostředků, sabotáž
- Dlouhodobé přerušení poskytování služeb elektronických komunikací, družicových služeb, dodávky elektrické energie nebo jiných důležitých služeb
- Zaměstnanci s nedostatečnou odbornou úrovní znalostí
- Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik
- Zneužití vyměnitelných technických nosičů dat
- Napadení (odposlech, modifikace, podvržení) elektronické komunikace, družicových služeb nebo jiných důležitých služeb
- Závislost na dodavateli
- Zneužití cizí státní moci pro přístup k aktivům
- Zpřístupnění nebo předání aktiv na základě žádosti jiného státu

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



Modelový příklad vytvoření katalogu hrozeb

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



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

Tabulka 16: Ukázka z katalogu hrozeb

ID	Typové hrozby	Označení	Příklady hrozeb	Vektor útoku	Je relevantní varování NÚKIB ze dne 17. prosince 2018?	Dův. (C)	Int. (I)	Dost. (A)
1	Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení	H1: Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení	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. 9) Člen vrcholného vedení nedodrží heslovou politiku stanovenou bezpečnostními politikami. 10) Dodavatel nainstaluje neautorizovaný software.	Interní/Externí	NE	x	x	x

5.3 Příprava scénářů

Dle vyhlášky je nutné zohledňovat relevantní kombinace aktivum-zranitelnost-hrozba. Je logické, že všechna aktiva nemají stejné zranitelnosti a nepůsobí na ně stejné hrozby, například zranitelnost typu „nedostatečné bezpečnostní povědomí uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení“ cílí na aktivum typu lidské zdroje, naopak zranitelnost „zastaralost aktiv“ míří na technická aktiva. Stejná situace nastává i u hrozeb, například hrozba „porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení“ 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 ministerstva 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 určování a hodnocení aktiv a rizik a v Příloze 6: Vzorové hodnocení aktiv a rizik.

5.4 Katalog bezpečnostních opatření

Na ministerstvu bylo rozhodnuto o vytvoření Katalogu opatření. Tento katalog má několik funkcí, jednou z nich je, že slouží jako Prohlášení o aplikovatelnosti (viz kapitola [5.10 Prohlášení o aplikovatelnosti](#)), dále slouží jako GAP⁷ 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 procesu hodnocení rizik. Při hodnocení kombinace aktivum-zranitelnost-hrozba může být výchozí hodnota zranitelnosti zvýšena nebo snížena na základě konkrétních okolností souvisejících s určeným rizikem.

⁷ Tento typ analýzy je používán jako rozdílová analýza mezi skutečným stavem v organizaci oproti požadavkům vyhlášky.



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

5.4.1 Určení vazeb mezi zranitelnostmi a bezpečnostními opatřeními

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

- Byla hledána tzv. primární vazba mezi zranitelnostmi a bezpečnostním opatřením, 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 uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení*“.
- 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*“.

Vzorec pro výpočet rizika

Pro výpočet rizika jsou nejčastěji využívány funkce, které zohledňují dopad, hrozbu a zranitelnost. Vyhláška uvádí jako vhodnou následující funkci⁸:

$$\text{Riziko} = \text{dopad (hodnota aktiva)} \times \text{hrozba} \times \text{zranitelnost}$$

Dopad

Dopad představuje hodnotu škody, která by vznikla v případě narušení bezpečnosti informací (důvěrnosti, integrity, dostupnosti). Pro hodnocení dopadu je využito hodnocení aktiv podle § 7 vyhlášky viz také kapitoly [4.1.4 Hodnocení primárních aktiv](#) a [4.2.4 Hodnocení podpůrných aktiv a určení vazeb mezi podpůrnými a primárními aktivy](#).

⁸ Ve vyhlášce znaky „x“ představují zástupné znaky, které mohou být nahrazeny různými matematickými funkcemi, například 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.

Hrozba

U hrozby hodnotíme pravděpodobnost, s jakou nastane.

Tabulka 17: Hodnocení úrovně hrozby

Úroveň		Popis
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
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 bezpečnostní opatření, která by vedla ke snížení možnosti jejího zneužití.

Tabulka 18: Hodnocení úrovně zranitelnosti

Úroveň		Popis
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 bezpečnostních opatření je omezena. Nejsou známy 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 známy 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 známy úspěšné pokusy o překonání bezpečnostních opatření.

Alternativa

V případě používání metody vytváření scénářů je možné upravit vzorec a hodnotit vhodnou kombinací hrozby a zranitelnosti jako jeden celek. To znamená, že namísto samostatného hodnocení hrozeb a zranitelností je vytvořen scénář, který integruje obě hodnocení. Je však důležité, aby i po jejich sloučení bylo možné jednoznačně určit hodnotu hrozby i zranitelnosti. K tomuto účelu lze použít komentář, který jasně vyjádří hodnotu hrozby a zranitelnosti. Komentář by měl obsahovat dostatečné informace, aby bylo možné pochopit, jaké riziko představuje daná kombinace hrozby a zranitelnosti

$$\text{Riziko} = \text{dopad (hodnota aktiva)} \times \text{scénář}$$

Tento postup by však neměl vést ke ztrátě schopnosti rozlišení hodnoty hrozby a zranitelnosti.

Modelový příklad určení vzorce pro výpočet rizika

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

$$\text{Riziko} = \text{dopad (hodnota příslušného atributu aktiva)} \times \text{hrozba} \times \text{zranitelnost}$$

5.5 Kritéria pro akceptovatelnost rizik

Kritéria pro akceptovatelnost představují „risk appetite“ organizace, který by mělo stanovit její vrcholné 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. Například 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. Možná je také kombinace více různých bezpečnostních opatření. Zaleží na každé osobě, která varianta je pro ni přijatelná, tedy jaký má „risk appetite“.

Modelový příklad určení kritérií pro akceptovatelnost

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

Tabulka 19: Kritéria pro akceptovatelnost rizik ministerstvem

Úroveň	Hranice míry rizika	Popis	Proces zvládnání 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 pro řízení KB může o těchto rizicích informovat.
Střední	17-31	Riziko může být sníženo méně náročnými bezpečnostními opatřeními nebo v případě vyšší náročnosti bezpečnostních opatření je riziko akceptovatelné.	V případě způsobu zvládnání rizika „Akceptovat“ riziko akceptuje manažer KB ve spolupráci s gestorem aktiva. V případě způsobu zvládnání rizika „Snížit“ navrhuje bezpečnostní opatření architekt KB ve spolupráci s manažerem KB. Navržený způsob zvládnání rizik včetně bezpečnostního opatření prezentuje manažer KB výboru pro řízení KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládnání.
Vysoká	32-47	Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.	Způsob zvládnání rizika navrhuje manažer KB ve spolupráci s gestorem aktiva. V případě návrhu způsobu zvládnání rizika „Snížit“ navrhuje bezpečnostní opatření architekt KB ve spolupráci s manažerem KB. Navržený způsob zvládnání rizik včetně bezpečnostního opatření prezentuje manažer KB výboru pro řízení KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládnání.
Kritická	48-64	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.	Způsob zvládnání rizika navrhuje manažer KB ve spolupráci s gestorem aktiva. V případě návrhu způsobu zvládnání rizika „Snížit“ navrhuje bezpečnostní opatření architekt KB ve spolupráci s manažerem KB. Navržený způsob zvládnání rizik včetně bezpečnostního opatření prezentuje manažer KB výboru pro řízení KB, který jej buď schválí, nebo rozhodne o jiném způsobu zvládnání. V případě naléhavosti zvládnutí rizika lze postupovat způsobem popsaným v metodice.

Tabulka 20: 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

5.6 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 v ojedinělých případech a co nejdříve odstraňovány, případně v pravidelných intervalech přezkoumávány.



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, například zavedení bezpečnostního opatření je 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 pro řízení KB, který může udělit výjimku na dobu nezbytně nutnou (dobu nutnou pro realizaci příslušného bezpečnostního opatření), čímž akceptuje riziko s výjimkou spojené. Po roce je nutné provést přezkoumání výjimek a způsobů jejich odstranění.

Výjimky eviduje manažer KB.

5.7 Hodnocení rizik

5.7.1 Určení rizik

Určení rizik je proces vytváření relevantních kombinací aktivum-zranitelnost-hrozba. Účelem určení rizik není vytvoření kombinací všeho se vším, například u aktiv typu lidské zdroje nemá smysl vytvářet kombinace obsahující zranitelnosti typu nedostatečná údržba aktiv 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 určení rizik

Určení rizik v rámci ministerstva probíhalo tak, že bylo nejdříve vybráno aktivum z katalogu aktiv, u kterého bude hodnocení rizik prováděno, 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 určeny všechny relevantní kombinace.

Jako pomůcka pro určení 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 aktiv⁹.

5.7.2 Analýza rizik

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



Modelový příklad analýzy rizik

Na ministerstvu byly hodnoty aktiv (z pohledu důvěrnosti, integrity a dostupnosti) již stanoveny v rámci řízení aktiv a zaznamenány do katalogu aktiv. Pro účely analýzy rizik byly příslušné hodnoty přebrány.

⁹ 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.



Hodnota zranitelnosti byla stanovena podle účinnosti relevantních bezpečnostních opatření evidovaných v katalogu bezpečnostních opatření. V případě potřeby byla upravena s ohledem na konkrétní kombinaci aktiva, zranitelnosti a hrozby. Hodnota hrozby byla určena podle metodiky na základě posuzované kombinace aktiva, zranitelnosti a hrozby.

5.7.3 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 MS Excel dochází automaticky k obarvení výsledné hodnoty rizika barvou přidělenou příslušnému stupni – nízká, střední, vysoká a kritická. Dále byl vyplněn sloupec „Způsob zvládnutí rizika“, podle toho, jak bude s příslušnými riziky dále nakládáno.

5.8 Zvládání rizik

Určená 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 bezpečnostní 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 bezpečnostní opatření nebylo účinné.

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

Všechna rizika je potřeba průběžně monitorovat a pravidelně přezkoumávat metody jejich zvládnutí z toho důvodu, že pravděpodobnost výskytu rizik, či jejich dopad se může v čase měnit. Stejně tak se může změnit schopnost organizace tato rizika efektivně zvládat. Méně závažná rizika je vhodné periodicky monitorovat a přezkoumávat, zatímco závažná rizika je vhodné 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 bezpečnostního opatření nepřiměřená vůči riziku, které má ošetřit, je potřeba zvolit jiné, méně účinné bezpečnostní opatření či pokrýt riziko několika dílčími bezpečnostními opatřeními i za předpokladu, že takové ošetření rizika nebude dlouhodobě dostatečné. Tato situace může nastat například při využívání 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** (například u malých a středních rizik, kde nebyla nalezena smysluplná bezpečnostní opatření), což znamená, že skutečně nezavádíme žádné bezpečnostní 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 bezpečnostních opatření.



Akceptace rizika musí probíhat **v souladu s metodikou pro určování a hodnocení rizik a kritérii pro akceptovatelnost rizik** (viz kapitola [5.5 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 pro poskytovatele regulované služby v režimu vyšších povinností jsou uvedena ve vyhlášce, 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 bezpečnostní opatření. Některé hrozby a jejich hodnocení lze ovlivnit změnou okolností, například 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 zajištění vhodného bezpečnostního opatření na externí společnost. S rizikem se buď nic neděje, pouze je přesměřováno na „třetí stranu“ s jejím vědomým souhlasem (například pojištění, kde bezpečnostní opatření má obecně dopad do nákladů a škodu zaplatí někdo jiný) nebo je přeneseno na dodavatele. Zároveň je ale třeba mít na paměti, že organizace má vždy nepřenositelnou odpovědnost za to, že riziko bude nějakým způsobem řešeno (například že jej dodavatel vyřeší správně).



Modelový příklad zvládání rizik

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

5.8.1 Výběr opatření

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

Co to je bezpečnostní opatření?

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



Bezpečnostním opatřením organizačního charakteru může být zajištění personální bezpečnosti, požadavky na chování uživatelů, organizaci řízení KB, souhrn zákonných a smluvních požadavků organizace, předpis či metodiky technického standardu či požadavky na řízení dodavatelů a požadavky do smluv s dodavateli. Formou bezpečnostních opatření pak může být interní či provozní předpis (například směrnice). Dokument pro zavedení organizačního opatření obsahuje podrobný popis toho, co je bezpečnostním opatřením myšleno a jakým způsobem by bezpečnostní opatření mělo být implementováno a prosazováno. Organizační opatření popisuje vyhláška v § 3 až § 16.

Bezpečnostní 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 například o nástroj ke správě a ověřování identit, nástroj pro řízení přístupových oprávnění, nástroj pro zaznamenávání událostí technických aktiv a činností jeho uživatelů a administrátorů, nástroj pro detekci kybernetických bezpečnostních událostí, ale i provádění penetračních testů a používání kryptografických prostředků. Technická opatření popisuje vyhláška v § 17 až § 27.

Proč se bezpečnostní opatření zavádí?

Bezpečnostní opatření se zavádí s cílem určená rizika (hrozby a zranitelnosti) skutečně a účinně snížit a dosáhnout tak efektivní bezpečnosti informací v potřebných attributech 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, například z důvodu ekonomické náročnosti nebo doby potřebné k jeho zavedení, je nutné v mezích riziko snížit prostřednictvím dalších bezpečnostních opatření.

Jak postupovat při výběru bezpečnostních opatření?

Při výběru bezpečnostních opatření je vhodné:

- Cílit bezpečnostní opatření na zjištěná rizika (hrozby a zranitelnosti ve vazbě na důvěrnost, integritu a dostupnost)
- Postupovat v souladu s požadavky vyhlášky
- Opírat se o odborné znalosti technických garantů a expertů pro fyzickou a KB
- Zohlednit přiměřenost bezpečnostního opatření ve vztahu k požadovanému cíli (významnosti zabezpečovaného aktiva)
- Zohlednit přiměřenost bezpečnostního opatření k nákladům a procesům, které jsou s implementací bezpečnostního opatření spojeny (technické, lidské, finanční aj. zdroje)
- Provést analýzu procesu implementace / zavedení bezpečnostního opatření
- Popsat rozsah možného působení zavedeného bezpečnostního opatření (cíle a přínosy)

Kroky nezbytné k realizaci bezpečnostního opatření:

- Postupovat v souladu s interními předpisy
- Informování odpovědných osob
- Návrh a schvalování bezpečnostního opatření dle náročnosti na zdroje (manažer KB, výbor pro řízení KB, porada vrcholného vedení apod.)
- Vlastní návrh technického či organizačního opatření (nebo jeho koncepce, dle složitosti bezpečnostních opatření či celého souboru bezpečnostních 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 bezpečnostních opatření

Na základě provedeného hodnocení rizik byla nejdříve posouzena rizika s úrovní kritická, na která byla navržena bezpečnostní opatření. Následně byla posouzena rizika střední úrovně a byla pro ně navržena přiměřená bezpečnostní opatření. Dále byly analyzovány vazby mezi jednotlivými riziky a bezpečnostními opatřeními. Všechna navrhovaná bezpečnostní opatření byla zaznamenána v plánu zvládání rizik (viz *Příloha 8: Vzorový plán zvládání rizik*).

Plán zvládání rizik byl následně předložen ke schválení výboru pro řízení KB.

5.8.2 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 například audit KB, proběhlé kybernetické bezpečnostní incidenty, varování či reaktivní protiopatření vydané NÚKIB, plánované významné změny.

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 KB.

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 bezpečnostních opatření
- Popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními
- Způsob realizace bezpečnostních opatření
- Způsob hodnocení úspěšnosti zavedení jednotlivých bezpečnostních opatření pro zvládání rizik

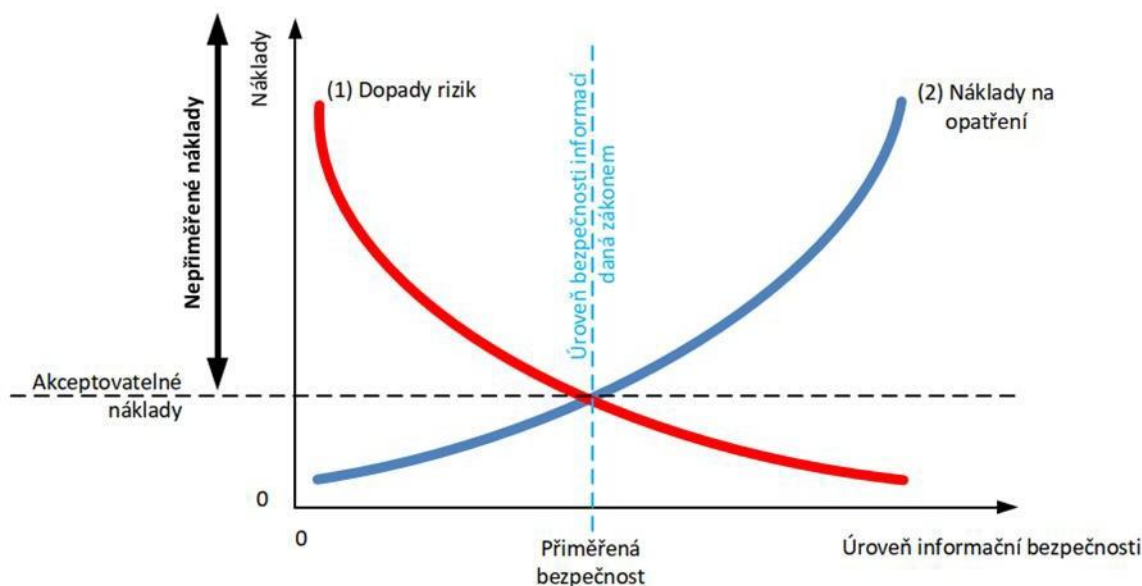
S plánem zvládání rizik by mělo být **aktivně pracováno** a měl by být aktualizován v souvislosti se zaváděním bezpečnostních opatření. Tento plán se může odkazovat na další dokumenty obsahující podrobnější informace, například projektovou dokumentaci.

5.8.3 Zavádění bezpečnostních 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 8: Odvození nepřiměřených nákladů

Modelový příklad zavádění bezpečnostních opatření

Ministerstvo prostřednictvím výboru pro řízení KB schválilo 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 zavést co nejdříve.

5.9 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 případně navržené potřebných bezpečnostních opatření pro redukci či eliminaci rizik. Se zprávou o hodnocení rizik má být prokazatelně seznámeno vrcholné vedení a měla být projednána a schválena výborem pro řízení KB či jiným obdobným schvalovacím orgánem organizace.



Modelový příklad zprávy o hodnocení

Zprávu o hodnocení rizik ministerstva projednal a schválil její výbor pro řízení KB. Zpráva o hodnocení rizik je obsahem dokumentu *Příloha 9: Vzorová zpráva o hodnocení rizik*.

5.10 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti (známé také jako **SoA = Statement of Applicability**) je dokument, ve kterém jsou popsána:

- zavedená bezpečnostní opatření včetně způsobu jejich implementace a
- nezavedená bezpečnostní opatření, včetně odůvodnění, z jakého důvodu nedošlo k jejich zavedení a uvedení případných přijatých náhradních bezpečnostních opatření.



Jedná se o stěžejní dokument, který je předkládán výboru pro řízení KB (či jinému obdobnému schvalovacímu orgánu organizace), který jej musí odsouhlasit.

Prohlášení o aplikovatelnosti je společně s plánem zvládnutí 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 vyhláškou. **Prohlášení o aplikovatelnosti musí obsahovat všechna bezpečnostní opatření požadovaná vyhláškou.**



Modelový příklad prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti ministerstva projednal a schválil její výbor pro řízení 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 bezpečnostní opatření nejsou zavedena nebo jsou minimální, tak se mu přiřadí hodnota 4. Pokud bezpečnostní opatření zavedeno 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, pak bezpečnostní opatření neplní svůj účel a uvedeme 4.

5.11 Sdílení informací o riziku

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



Modelový příklad sdílení informací o riziku

Na ministerstvu je aktivován a komunikován proces sdílení informací o riziku. Komunikace a sdílení informací je primárně řízeno výborem pro řízení KB, s ohledem na citlivost informací. Během společného jednání je o souboru bezpečnostních opatření uvědomen jak gestor, tak garant primárního a podpůrného aktiva. Cílem společné komunikace je nastavení souboru organizačních a technických bezpečnostních opatření, která budou zavedena v organizaci nebo systému, včetně nastavení procesu monitorování, vyhodnocování a eskalace problémů. V případě potřeby je diskuse dále vedena do úrovně významného dodavatele.

5.12 Alternativní hodnocení rizik u primárních aktiv

Hodnocení rizik u primárních aktiv může být zpracováno dle postupu uvedeného výše. V některých organizacích však může nastat situace, že povinnosti vyplývající ze zákona a vyhlášky musí najednou začít plnit pro několik regulovaných služeb. 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 hodnocení rizik je nutné tento proces rozpracovat do většího detailu a zahrnout do něj i podpůrná aktiva.

Metoda spočívá v tom, že dojde k určení, evidenci a hodnocení primárních aktiv dle postupu uvedeného v kapitole [4.1 Primární aktiva](#). Následně však nejsou určena 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:

$$\text{Riziko} = \text{dopad (hodnota aktiva)} \times \text{pravděpodobnost realizace scénáře}$$

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 21: Stupnice pro hodnocení pravděpodobnosti realizace scénáře

Úroveň		Popis
1	Nízká	Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití. 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. 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 22: Stupnice pro alternativní hodnocení rizik

Úroveň		Popis
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 nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.
13-16	Kritická	Riziko je nepřijatelné a musí být neprodleně zahájeny kroky k jeho odstranění.

5.12.1 Postup alternativního hodnocení rizik u primárních aktiv

Hodnocení rizik se musí účastnit všechny relevantní osoby, například manažer KB, architekt KB, garanti a gestoři primárních aktiv, zástupci IT, DPO.

Následně dojde k vytvoření obecných rizikových scénářů ohrožujících primární aktiva. Příkladem je výpadek informačního systému pro certifikaci senzorů způsobený technickou závadou na zastaralé technologii.

Hodnota dopadu je stanovena na základě hodnocení primárních aktiv, přičemž se bere v úvahu nejvyšší hodnota relevantního atributu, například 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, například zavedených bezpečnostních opatření, stáří používaných technologií, umístění organizace. 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 zvládnutí rizik, zprávu o hodnocení rizik a prohlášení o aplikovatelnosti.



Modelový příklad hodnocení rizik u primárních aktiv

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



5.13 Další povinnosti dle vyhlášky

Kromě povinností popsanych v předchozích kapitolách, stanovuje vyhláška ještě tyto požadavky:

- Provádí hodnocení rizik v pravidelných intervalech a při významných změnách, přitom zohlední:
 - Relevantní hrozby a zranitelnosti podle písmene b) a posoudí možné dopady na aktiva, přičemž vychází z hodnocení aktiv podle § 7 vyhlášky
 - Významné změny
 - Změny stanoveného rozsahu podle § 12 zákona
 - Protipatření podle § 20 zákona
 - Kybernetické bezpečnostní incidenty, včetně dříve řešených
 - Výsledky auditů KB a kontrol v oblasti KB
 - Výsledky penetračního testování a skenování zranitelností
 - Výsledky vyhodnocení účinnosti ISMS
- V souladu s plánem zvládání rizik zavádí bezpečnostní opatření

5.13.1 Významné změny

Významnou změnou se rozumí každá změna ovlivňující bezpečnost informací, u níž povinná osoba, bez ohledu na již zavedená bezpečnostní opatření, může předpokládat ohrožení bezpečnosti informací. Definici významné změny si však může poskytovatel regulované služby přizpůsobit dle svých potřeb.

Významnou změnou může být například:

- Změna rozsahu řízení KB
- 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 například databázové servery
- Varování nebo nápravné opatření od NÚKIB, které je relevantní pro regulovanou službu
- Nová hrozba nebo zranitelnost
- Změny v systému fyzického zabezpečení (EZP, EPS)
- Rozšíření/změna topologie sítě
- Změna umístění v síti, například přesun do jiné VLAN
- Upgrade FW
- Změna/obnova technických aktiv, které zajišťují bezpečnost provozu v síti jako například FW, IDS, IPS, SIEM
- Velká aktualizace nebo nová velká verze SW například v1-v2, Windows 10 na Windows 11
- Výměna/upgrade HW, který bude mít vliv na bezpečnost informací
- Modernizace aplikačního řešení – například 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 například změna OS serverů z Windows Server 2016 na 2025
- Integrace nového IS, například datové schránky, NIA
- Nasazení nové technologie, například SIEM, virtualizace
- Upgrade OS serverů
- Implementace nového modulu do stávajícího IS
- Změna významného dodavatele nebo urgentní změna

6 Kontinuální zlepšování

Vyhláška 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 určená typová aktiva budou při přezkoumání nedostatečná či nevhodná pro použití a bude nutné je pro další použití aktualizovat nebo upravit, včetně aktualizace garantů aktiv, například rozdělení typového aktiva na menší skupiny, vytvoření nových typových aktiv, sloučení typových aktiv do větších celků.

Aktiva i rizika musí být sledována a přezkoumávána, a to včetně zbytkových rizik s ohledem na změny v organizaci, určené hrozby a zranitelnosti a účinnost zavedených bezpečnostních opatření, například určení nové zranitelnosti, obměna HW komponent, implementace SIEM.

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 jsou důležité pro kontinuální zlepšování řízení aktiv a rizik v organizaci.

! Poskytovatelé regulované služby v režimu vyšších povinností mají povinnost provést hodnocení rizik v pravidelných intervalech alespoň 1× ročně a při významných změnách určených dle § 11 odst. 1 písm. c) vyhlášky.

Hodnocení rizik je jedním ze vstupů do procesu pravidelného vyhodnocování účinnosti ISMS a přezkoumání ISMS, které probíhá alespoň jednou ročně (§ 3 písm. f vyhlášky), a které obsahuje:

- vyhodnocení cílů ISMS směřujících k zajištění KB regulované služby,
- posouzení naplňování plánu zvládání rizik,
- hodnocení stavu ISMS včetně revize hodnocení rizik,
- posouzení výsledků provedených auditů KB a kontrol v oblasti KB,
- výsledky předchozího hodnocení účinnosti ISMS,
- posouzení dopadů kybernetických bezpečnostních incidentů na oblast KB a poskytované služby a
- posouzení významných změn.

Na základě tohoto přezkoumání následně 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 KB, architekt KB a auditor KB. Samotné vyhodnocení provádí výbor pro řízení KB, který schvaluje také finální zprávu z přezkoumání ISMS.



7 Protiopatření podle § 20 zákona

Protiopatřeními se rozumí úkony, které vydává NÚKIB a slouží k ochraně regulované služby před hrozbou nebo zranitelností v oblasti KB, kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.

V souladu s § 8 písm. c) bodem 4 vyhlášky je nutné **při hodnocení rizik a v plánu zvládání rizik tato protiopatření zohlednit**. Zároveň je nutné zajistit naplnění podmínek vydaného protiopatření, mezi kterými může být například konkrétní forma bezpečnostního opatření nebo lhůta pro jeho implementaci.

Aktuálně účinná protiopatření jsou dostupná na úřední desce NÚKIB: [Národní úřad pro kybernetickou a informační bezpečnost - Úřední deska](#).

7.1 Varování podle § 22 zákona

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

7.1.1 Zohlednění varování NÚKIB

NÚKIB vydal již několik varování, např. před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation včetně jejich dceřiných společností, dále varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací, před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím, před některými produkty společnosti DeepSeek nebo před předáváním dat a vzdálenou správou z Číny.

K varování, které je potřeba zohlednit v procesu řízení rizik, vydává NÚKIB metodiku, která je dostupná na webových stránkách NÚKIB. Metodika slouží ke snadnější orientaci a pochopení vydaného varování a jeho správnému zapracování do procesu hodnocení rizik v organizaci. Např. k varování před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation včetně jejich dceřiných společností je vydaná Metodika k varování ze dne 17. prosince 2018, která je dostupná na webových stránkách NÚKIB: https://nukib.gov.cz/publikace/podpurne_materialy/metodika-k-varovani-ze-dne-17-12-2018_v1.0.pdf.

Ze skutečností uvedených v tomto vydaném varování vyplývá, že **hrozbu**, na kterou varování upozorňuje, je v souladu s tabulkou č. 1 přílohy č. 4 vyhlášky potřeba hodnotit jako **velmi pravděpodobnou až více méně jistou**. V případě užití jiné stupnice hodnocení hrozby, jak umožňuje § 8 odst. 3 vyhlášky, je nutno tuto hrozbu ohodnotit způsobem odpovídajícím příslušné úrovni podle vyhlášky.

Povinné osoby musí v souladu s § 9 odst. 2 písm. a) vyhlášky varování zohlednit také při zadávacím řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek. Při hodnocení rizik souvisejících se zadávacím řízením a hodnocení rizik před uzavřením smlouvy je nutné zohlednit také protiopatření podle § 20 zákona.

Pro povinné osoby, které jsou současně zadavateli ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek, vytvořil NÚKIB několik podpurných materiálů. Mezi ně patří dokument *Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení*, dostupný na webových stránkách NÚKIB: https://nukib.gov.cz/publikace/podpurne_materialy/zohledneni-varovani-v-zadavacim-izeni_v1.2.pdf.

Širší problematice bezpečného pořizování ICT se dále věnuje podpurný materiál *Zadávací řízení veřejných zakázek v oblasti ICT a kybernetické bezpečnosti*, který je dostupný na Portálu NÚKIB: <https://portal.nukib.gov.cz/podpurne-materialy/zadavani-verejnych-zakazek-v-oblasti-ict-a-kyberneticke-bezpecnosti/>.

Stěžejním je správné provedení hodnocení rizik. Hodnocení rizik musí být provedeno před vysláním zadávacího řízení na veřejnou zakázku a musí být v souladu se schválenou metodikou pro určování a hodnocení rizik. V provedeném hodnocení rizik musí být jasně rozlišena rizika posuzovaná bez zohlednění varování a rizika posuzovaná s jeho zohledněním. Nerelevantnost konkrétního rizika pro daný subjekt musí být řádně odůvodněna.



Modelový příklad zohlednění varování před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation včetně jejich dceřiných společností v běžného hodnocení rizik.

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

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

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

Celý postup probíhal v souladu s metodikou ministerstva pro určování a hodnocení aktiv a rizik popsanou v *Příloze 2: Vzorová metodika pro určování a hodnocení aktiv a 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 zadávacího 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 se zadávacím řízením zohlednit hodnotu primárního aktiva Služba certifikace senzorů.

Jelikož je potřeba postupovat v souladu s vydaným 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 protipatření podle § 23 zákona

Reaktivní protipatření vydává NÚKIB většinou na základě kybernetického bezpečnostního incidentu za účelem jeho odvrácení či ke zmírnění jeho dopadů a předává jej buď konkrétním subjektům (například dle konkrétního odvětví), kterých se to týká, nebo může vydat opatření obecné povahy s plošnou účinností. Zákon rozlišuje dvě formy reaktivních protipatření, a to rozhodnutí a opatření obecné povahy. Smyslem tohoto dělení je pokrýt oba typické případy vyskytující se při ochraně před kybernetickými bezpečnostními incidenty. Prvním případem je výskyt kybernetického bezpečnostního incidentu v rámci určité organizace. Reaktivní protipatření lze v takovém případě vydat formou rozhodnutí konkrétně specifikujícího povinnosti pro určeného adresáta (povinnou



osobu). Druhým případem je výskyt kybernetického bezpečnostního incidentu, jehož rozsah je větší, nebo jehož rozsah nelze kvůli složitosti tohoto incidentu či jeho rychlému vývoji přesně určit. Takový incident je pak možno řešit vydáním reaktivního protiopatření formou opatření obecné povahy, v němž budou specifikovány konkrétní povinnosti k jeho odvrácení neurčitěmu okruhu poskytovatelů regulovaných služeb definovanému za užití generických znaků odpovídajících charakteru tohoto okruhu poskytovatelů.

8 Q&A

Q1: Musí být při hodnocení rizik vytvořeny všechny možné kombinace aktivum-zranitelnost-hrozba?

A1: Ne. Je nutné určit pouze ty relevantní.

Q2: Kolik aktiv je nutné určit?

A2: Pro prvotní určení aktiv doporučujeme začínat s menším množstvím typových aktiv, ale celý proces korektně dokončit. Při opakovaném hodnocení aktiv je nutné množství aktiv revidovat dle potřeby, například je rozdělit na menší skupiny. Organizace by měla zvolit takový detail, aby byla schopna adekvátně určit 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 potřebné upravit dle specifik dané organizace.

Q4: Je dostačující pracovat při hodnocení rizik pouze s hrozbami a zranitelnostmi uvedenými ve vyhlášce?

A4: Ne, vyhláška poskytuje pouze přehled vybraných typových hrozeb a zranitelností a je vždy nutné určit jednotlivé hrozby a zranitelnosti přímo pro konkrétní potřeby organizace a její regulované služby.

Q5: Je nutné hodnotit samostatně všechny oblasti hodnocení důležitosti primárních aktiv (Tab. 4 v příloze č. 1 vyhlášky pro poskytovatele regulované služby v režimu vyšších povinností), když se v naší organizaci tyto oblasti prolínají?

A5: Ne. Jednotlivé oblasti lze slučovat do větších oblastí, jako k tomu bylo přistoupeno například 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 například 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 popsány 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. 4 vyhlášky. 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. Například v případě kybernetických 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, například 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.

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou [Traffic Light Protocol](#). Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva

Podmínky použití

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.

TLP: AMBER+STRICT

Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.

TLP: AMBER

Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.

TLP: GREEN

Informace může být sdílena 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.

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
1. října 2026	1.0	Odbor kontroly	Vytvoření dokumentu