

Kybernetická bezpečnost územního samosprávného celku

Bc. Václav Zavadil

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav krizového řízení

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Václav Zavadil
Osobní číslo:	L23351
Studijní program:	N1032A020002 Bezpečnost společnosti
Specializace:	Rizikové inženýrství
Forma studia:	Kombinovaná
Téma práce:	Kybernetická bezpečnost územního samosprávného celku

Zásady pro vypracování

- Zpracujte teoretický vstup do tématu kybernetické bezpečnosti v prostředí územně samosprávných celků.
- Zvolte územně samosprávný celek a tento pro potřeby práce anonymizujte.
- Analyzujte současný stav kybernetické bezpečnosti v komparaci s požadavky vybraných právních norem a identifikujte případné nedostatky.
- Navrhněte změny v oblasti zajištění kybernetické bezpečnosti v prostředí vybraného územně samosprávného celku a diskutujte získané výsledky.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. CALDER, Alan. *Cyber Security: Essential principles to secure your organisation*. Ely, Cambridgeshire: IT Governance Publishing, 2020. ISBN 978-1-78778-210-5.
2. DOUCEK, Petr; KONEČNÝ Martin a NOVÁK Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti Informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
3. KOLOUCH, Jan a BAŠTA Pavel. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o, 2019. ISBN 978-80-88168-31-7.
4. SEDLÁK, Petr a KONEČNÝ Martin. *Kybemetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
5. SMEJKAL, Vladimír; SOKOL Tomáš a KODL Jindřich. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Jakub Rak, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **2. prosince 2024**
Termín odevzdání diplomové práce: **25. dubna 2025**

L.S.

prof. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne 25.04.2025

.....
podpis autora

ABSTRAKT

Tato diplomová práce se zaměřuje na problematiku kybernetické bezpečnosti územního samosprávného celku, konkrétně vybrané obce. V úvodní části jsou definovány důležité pojmy související s kybernetikou a bezpečností. Následuje přehled právních předpisů, které se vztahují ke kybernetické bezpečnosti a veřejné správě. V rámci praktické části byla provedena analýza rizik podle metodiky NÚKIB a dalších relevantních metodických postupů. Dále byla realizována komplexní analýza zranitelností a hodnocení informačních aktiv s využitím principů CIA. Na základě získaných poznatků byla navržena a doporučena bezpečnostní opatření vedoucí ke zvýšení úrovně kybernetické bezpečnosti ve zkoumané obci.

Klíčová slova: obec, bezpečnost, data, analýza, informace, zlepšení

ABSTRACT

This thesis focuses on the issue of cyber security of a local government unit, specifically a selected municipality. In the introductory part, important terms related to cybernetics and security are defined. This is followed by an overview of legal regulations that relate to cybersecurity and public administration. In the practical part, a risk analysis has been carried out according to the National Cyber and Information Security Agency (NUKIB) methodology and other relevant methodologies. Furthermore, a comprehensive vulnerability analysis and assessment of information assets was performed using CIA principles. Based on the obtained findings, security measures were proposed and recommended to increase the level of cybersecurity in the studied community.

Keywords: municipality, security, data, analysis, information, improvement

Děkuji panu Ing. Jakubu Rakovi, Ph.D., vedoucímu mé diplomové práce, za odborné vedení, konzultace, podnětné připomínky a cenné rady. Dále děkuji kolegyním a kolegům, zaměstnancům obce, za poskytnutou pomoc při řešení odborných otázek, poskytnutá interview a za nezbytné podklady, díky nimž jsem mohl dané téma zpracovat. Děkuji rovněž celé své rodině, všem svým blízkým za podporu a trpělivost po celou dobu mého magisterského studia a při psaní diplomové práce.

OBSAH

ÚVOD	13
I TEORETICKÁ ČÁST	14
1 CÍLE PRÁCE A POUŽITÉ METODY.....	15
2 LITERÁRNÍ REŠERŠE	17
2.1 CYBER SECURITY	17
2.2 ŘÍZENÍ KYBERNETICKÉ BEZPEČNOSTI A BEZPEČNOSTI INFORMACÍ	17
2.3 CYBERSECURITY	17
2.4 KYBERNETICKÁ (NE)BEZPEČNOST: PROBLEMATIKA BEZPEČNOSTI V KYBERPROSTORU	18
2.5 BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ PODLE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI	18
3 ZÁKLADNÍ POJMY	19
3.1 BEZPEČNOST	19
3.2 INFORMACE.....	19
3.3 KYBERPROSTOR – KYBERNETICKÝ PROSTOR	19
3.4 INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST.....	20
3.4.1 Bezpečnost informací	20
3.4.2 Kybernetická bezpečnost	20
3.5 INFORMAČNÍ AKTIVA.....	21
3.5.1 Primární aktiva	21
3.5.2 Podpůrná aktiva	21
3.6 DATA.....	22
3.7 RIZIKO	22
3.8 HROZBA.....	23
3.9 ZRANITELNOST	23
3.10 INCIDENT	23
3.11 ÚTOK.....	23
4 KYBERNETICKÉ ÚTOKY	24
4.1 DDoS ÚTOKY	24
4.2 RANSOMWARE	24
4.3 PHISHINGOVÉ ÚTOKY	25
4.4 DALŠÍ TYPY KYBERNETICKÝCH ÚTOKŮ	25
5 TRIÁDA CIA	26
5.1 DŮVĚRNOST.....	27
5.2 INTEGRITA	30

5.3	DOSTUPNOST	31
6	PRÁVNÍ PŘEDPISY, NORMALIZACE A METODIKA	32
6.1	PRÁVNÍ PŘEDPISY EU V OBLASTI KYBERNETICKÉ BEZPEČNOSTI.....	32
6.2	PRÁVNÍ PŘEDPISY ČR V OBLASTI KYBERNETICKÉ BEZPEČNOSTI.....	34
6.2.1	Zákony	34
6.2.2	Vyhlášky a nařízení	35
6.3	NORMY.....	38
6.4	METODIKA.....	40
6.5	PRÁVNÍ PŘEDPISY V OBLASTI VEŘEJNÉ SPRÁVY	41
7	MANAGEMENT RIZIK	44
7.1	ČSN ISO 31000 – OBECNÝ PŘÍSTUP K ŘÍZENÍ RIZIK.....	44
7.2	ČSN EN ISO/IEC 27005 – MANAGEMENT KYBERNETICKÝCH RIZIK.....	45
7.3	KOMPARACE NOREM ČSN ISO 31000 A ČSN EN ISO/IEC 27005.....	47
8	SHRnutí TEORETICKÉ ČÁSTI	48
II	PRAKTICKÁ ČÁST	49
9	ÚVOD DO PRAKTICKÉ ČÁSTI	50
10	PŘEDSTAVENÍ ŘEŠENÉHO ÚZEMNĚ SAMOSPRÁVNÍHO CELKU	51
10.1	POPIS BUDOVY OBECNÍHO ÚŘADU.....	52
10.2	OSTATNÍ BUDOVY OBECNÍHO ÚŘADU	53
10.3	ZAMĚSTNANCI ÚŘADU.....	53
10.4	ORGANIZAČNÍ STRUKTURA OBCE.....	55
11	ANALYTICKO-METODOLOGICKÁ ČÁST	56
11.1	ANALYTICKÁ ČÁST	56
11.1.1	Stanovení kontextu.....	56
11.1.2	Identifikace rizik	56
11.1.3	Analýza rizik.....	56
11.1.4	Hodnocení rizik.....	57
11.1.5	Zvládání rizik	57
11.1.6	Monitorování a přezkoumání	57
11.2	METODOLOGICKÁ ČÁST	57
12	STANOVENÍ KONTEXTU	59
13	POSOUZENÍ RIZIK	61
13.1	IDENTIFIKACE RIZIK	61
13.2	AKTIVA	62
13.2.1	Garant aktiva.....	62
13.2.2	Identifikace primárních aktiv	63
13.2.3	Hodnocení primárních aktiv	69
13.2.4	Identifikace podpůrných aktiv	81

13.2.5	Hodnocení podpůrných aktiv	83
14	ANALÝZA RIZIK	87
14.1	IDENTIFIKACE ZRANITELNOSTÍ A JEJICH HODNOCENÍ.....	87
14.2	IDENTIFIKACE A HODNOCENÍ HROZEB.....	89
14.3	VÝPOČET RIZIKA	91
14.4	VYHODNOCENÍ PROVEDENÉ ANALÝZY	100
15	NÁVRHOVÁ ČÁST.....	101
15.1	ORGANIZAČNÍ OPATŘENÍ	102
15.2	OPATŘENÍ V OBLASTI LIDSKÝCH ZDROJŮ	103
15.3	OPATŘENÍ FYZICKÉ BEZPEČNOSTI	103
15.4	TECHNOLOGICKÁ OPATŘENÍ	104
15.5	SHRnutí KAPITOLY	104
	ZÁVĚR	105
	SEZNAM POUŽITÉ LITERATURY	107
	SEZNAM OBRÁZKŮ.....	114
	SEZNAM TABULEK	115
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	117
	SEZNAM PŘÍLOH	119

ÚVOD

Kybernetická bezpečnost je v současné době velmi aktuálním tématem. Internetová komunikace zasahuje do všech oblastí našeho života. Prakticky vše, co každodenně používáme k uspokojování svých potřeb, je dnes spojeno s internetem. Jde zejména o tzv. chytré mobilní telefony, přenosná zařízení určená ke zpracování a ukládání dat, jako jsou tablety či notebooky, ale i běžné domácí spotřebiče, například televize, lednice nebo kávovary. Do rukou internetu jsme vložili velkou část lidské existence, čímž se stal velmi mocným nástrojem. Čím více je však lidstvo na internetové komunikaci závislé, tím častěji dochází ke kybernetickým útokům s cílem ovládnout tento kyberprostor. Důsledkem takových útoků bývá ztráta nebo odcizení cenných dat, jejich znepřístupnění, poškození softwaru i hardwaru, narušení běžných služeb a řada dalších nežádoucích aktivit. Kybernetické útoky jsou prováděny především za účelem finančního, či politického zisku, protože informace jsou dnes považovány za nejcennější komoditu.

Institut kybernetické bezpečnosti vznikl právě za účelem ochrany proti kybernetickým útokům. Bezpečnost kyberprostoru je často podceňována a ohrožené subjekty si mnohdy riziko vůbec neuvědomují. Tento laxní přístup vede k tomu, že pravidla nejsou dostatečně nastavena a ohrožení uživatelé nejsou dostatečně edukováni. Neznalost způsobů obrany proti kybernetickým útokům pak dále zvyšuje jejich pravděpodobnost i dopady.

Tato diplomová práce se věnuje problematice kybernetické bezpečnosti u vybraného subjektu, kterým je reálně existující obec, jež byla pro potřeby této práce anonymizována. Práce je rozdělena do dvou částí. První, teoretická část vymezuje základní pojmy z dané oblasti a zabývá se tématy jako jsou právní předpisy, normalizace a metodika, ochrana informací, standard CIA a celkově oblast kybernetické bezpečnosti. Tyto oblasti tvoří teoretický rámec, ze kterého je dále čerpáno v následujících kapitolách. Druhá, praktická část práce, se zabývá charakteristikou zvoleného subjektu a vlastním řešením kybernetické a informační bezpečnosti. Toto řešení zahrnuje identifikaci aktiv a hrozeb. Po provedení těchto kroků následuje analýza rizik, jejímž výstupem je návrh doporučení a opatření ke zlepšení současného stavu.

I. TEORETICKÁ ČÁST

1 CÍLE PRÁCE A POUŽITÉ METODY

Tato kapitola se zaměřuje na vymezení hlavního cíle diplomové práce. Dále jsou zde popsány dílčí cíle práce a použité metody, které byly využity k naplnění stanovených cílů.

Hlavní cíl práce:

Hlavním cílem této diplomové práce je analyzovat současný stav kybernetické bezpečnosti ve vybrané obci jakožto územním samosprávném celku a navrhnout opatření vedoucí ke snížení kybernetických rizik. Práce se zaměřuje na identifikaci hrozeb, zranitelností a rizik, která mohou ohrozit bezpečnost informačních aktiv obce, a to s využitím metodiky Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a dalších souvisejících analytických nástrojů.

Dílčí cíle diplomové práce:

Pro dosažení hlavního cíle této práce byly zvoleny následující kroky:

- Literární rešerše – spolu s odbornými články představují úvodní fázi při zkoumání problematiky kybernetické bezpečnosti. Tato část poskytuje základní znalosti a důležité informace o významu kybernetické bezpečnosti pro veřejnou správu. Cílem literární rešerše je vytvořit ucelený přehled o řešené problematice a získat tak potřebný teoretický základ pro další postup práce.
- Analýza rizik – pro hodnocení rizik je zvolena metoda matice rizik, která umožňuje výpočet rizika na základě pravděpodobnosti výskytu hrozeb a závažnosti jejich dopadů.
- Vytvoření přehledného a prakticky využitelného materiálu, který by mohl pomoci obci, při zavádění požadavků vyplývajících z nové legislativy v oblasti kybernetické bezpečnosti.

Použité metody:

- Literární rešerše – byla aplikována zejména v teoretické části práce k osvětlení problematiky pomocí odborných tuzemských i zahraničních bibliografických zdrojů. Dále byly použity právní předpisy, technické normy, metodiky a jiné odborné zdroje.
- Popis – byl využit při zpracování teoretické i praktické části. Byla popsána problematika kybernetické bezpečnosti a také řešený subjekt.

- Dotazování – bylo využito v rámci osobních rozhovorů se zaměstnanci vybrané obce.
- Dedukce – byla využita při identifikaci rizikových oblastí vyplývajících z charakteristiky obce.
- Analýza – byla využita k analýze současného stavu obce v oblasti řešené problematiky. Analýza byla provedena pomocí identifikační metody, maticového výpočtu hodnoty rizika, jejímž výstupem jsou semikvantitativní hodnocení, která vychází z metody FMEA. Autorem modifikovaná metoda FMEA byla zvolena z toho důvodu, že umožňuje systematicky identifikovat a prioritizovat potenciální kybernetické hrozby na základě jejich dopadů, pravděpodobnosti výskytu hrozeb a zranitelností. Oproti jiným metodám, jako je například kvalitativní analýza rizik, poskytuje FMEA jasnější kvantifikaci a přehlednější strukturu výsledků. Díky tomu lze efektivněji navrhnout opatření a tím minimalizovat kybernetická rizika.
- Syntéza – byla využita při vyhodnocení získaných informací.
- Indukce – v závěru byla uplatněna subjektivní analýza autora této diplomové práce, která vycházela z celkového zhodnocení zkoumané problematiky.

Omezení práce:

Práce se nezaměřuje na detailní analýzu lidského faktoru, jako je například bezpečnostní povědomí zaměstnanců obce nebo jejich školení, ale pouze na obecnou úroveň opatření v oblasti řízení kybernetické bezpečnosti. Důvodem tohoto omezení je skutečnost, že opatření, která jsou v současnosti v obci přijímána, se právě na bezpečnostní povědomí nebo školení zaměstnanců spoléhají. Tato opatření však nepřinášejí v oblasti kybernetické bezpečnosti očekávaný přínos.

2 LITERÁRNÍ REŠERŠE

Tato kapitola obsahuje přehled relevantních zdrojů, které byly prostudovány za účelem lepšího pochopení tématu, získání orientace v problematice a jejich následného využití při zpracování diplomové práce.

2.1 Cyber Security

Kniha Cyber Security: Essential principles to secure your organisation se, jak je patrné z jejího názvu, zabývá problematikou kybernetické bezpečnosti ve vztahu k organizaci. Tento stručný knižní průvodce poskytuje přehled základů kybernetické bezpečnosti, včetně jejich klíčových principů, běžných zranitelností, potenciálních hrozeb a typů útočníků, kteří tyto slabiny využívají. Zároveň nabízí doporučení, jak se proti těmto hrozbám efektivně bránit, a jak na jejich základě vytvořit robustní program kybernetické bezpečnosti pro vaši organizaci. (Alan Calder, 2020)

2.2 Řízení kybernetické bezpečnosti a bezpečnosti informací

Publikace Řízení kybernetické bezpečnosti a bezpečnosti informací poskytuje komplexní přehled informací zásadních pro zabezpečení dat a systémů v různých typech organizací, od malých podniků až po velké korporace. Podrobně se zaměřuje na analýzu platných norem, standardů a legislativních požadavků, jejichž důsledné dodržování je důležité pro dosažení efektivní ochrany citlivých informací a minimalizaci rizik spojených s kybernetickými hrozbami. Dále kniha ukazuje, jak správně implementované a spolehlivě zabezpečené informační systémy mohou dlouhodobě přispívat ke konkurenční výhodě organizací, a to díky zvýšení důvěryhodnosti, vyšší provozní stabilitě a schopnosti rychle reagovat na bezpečnostní incidenty. (Doucek, Petr, 2019)

2.3 CyberSecurity

Kniha CyberSecurity se zaměřuje na širokou problematiku kybernetické bezpečnosti a nabízí ucelený přehled principů, které je nutné dodržovat při práci s informačními technologiemi. Věnuje se nejen technickým aspektům ochrany dat a systémů, ale také právním předpisům a normám, které v této oblasti platí. Díky svému komplexnímu přístupu slouží jako cenný zdroj informací pro odborníky z oblasti informačních technologií (IT), kteří zde naleznou užitečné poznatky pro zajištění bezpečnosti systémů, prevenci kybernetických hrozeb a plnění zákonných požadavků. Kniha také poskytuje praktické rady

a doporučení pro efektivní zavádění bezpečnostních opatření v různých typech organizací. (Kolouch a Bašta, 2019).

2.4 Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru

Tato publikace rozšiřuje a navazuje na předchozí autorův titul "Problematika ISMS v manažerské informatice", a přináší aktuální poznatky týkající se kybernetické bezpečnosti a souvisejících oblastí. Jejím hlavním cílem je zdůraznit důležitost této problematiky a upozornit na různé aspekty kybernetické bezpečnosti, které jsou v současnosti relevantní prakticky pro všechny subjekty, od jednotlivců po velké organizace. Publikace je určena především odborníkům působícím v oblasti managementu informačních a komunikačních technologií, správcům sítí, bezpečnostním specialistům a širší odborné veřejnosti. Téma kybernetické bezpečnosti je zde zasazeno do širšího kontextu, přičemž se zaměřuje na současné přístupy k ochraně v kyberprostoru, vývoj nových technologií a jejich vliv na bezpečnostní strategie. Důraz je kladen také na systémovou integraci kybernetické bezpečnosti, a její význam při budování komplexních a odolných bezpečnostních řešení. (Sedlák a Konečný, 2021)

2.5 Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti

Kniha je určena odborníkům zabývajícím se správou a ochranou IS/IT, včetně právních odborníků a provozovatelů kritických systémů důležitých pro bezpečnost státu. Zaměřuje se na komplexní přístup k bezpečnosti IS/IT, zahrnující právní předpisy, technické normy, doporučené postupy a jejich aplikaci v praxi. Kniha se dělí na tři hlavní části: první se věnuje obecným otázkám bezpečnosti a legislativním základům, druhá popisuje různé typy kybernetických útoků a analyzuje zákon o kybernetické bezpečnosti včetně prováděcích předpisů (zejména vyhláška č. 82/2018 Sb.). Třetí část se zaměřuje na technické normy, doporučené postupy řízení rizik a také na právní odpovědnost fyzických a právnických osob vyplývající ze zákona o kybernetické bezpečnosti. Publikace je cenným zdrojem nejen pro správce IS/IT a jejich dodavatele, ale také pro vysoké školy, kde se problematika bezpečnosti IS/IT vyučuje. (Smejkal a kol. 2019)

3 ZÁKLADNÍ POJMY

V této kapitole jsou uvedeny důležité termíny a definice, které jsou nezbytné pro pochopení problematiky kybernetické bezpečnosti. Seznámení s těmito pojmy umožňuje jednotný výklad a usnadňuje orientaci v dalších částech práce.

3.1 Bezpečnost

Pojem bezpečnost se objevuje v různých vědních disciplínách, přičemž v každé z nich má odlišný význam a specifické charakteristiky. V české legislativě, ani odborné literatuře, zatím neexistuje jednotná a závazná definice tohoto pojmu. Bezpečnost je často chápána jako notorieta – něco, co je považováno za obecně známé, snadno pochopitelné a intuitivně srozumitelné, aniž by bylo nutné jej přesně vymezovat nebo dokazovat. V oblasti informačních systémů chybí v právním řádu i odborné literatuře univerzální definice bezpečnosti informačních systémů. Tento pojem je proto také vnímán jako nejasně vymezený a závislý na konkrétním kontextu. Obecně lze bezpečnost informačních systémů popsat jako stav, kdy jsou rizika a potenciální hrozby působící na tyto systémy minimalizovány na přijatelnou úroveň prostřednictvím vhodných technických, organizačních a právních opatření. Tento přístup zahrnuje prevenci, detekci, reakci na incidenty i neustálé zlepšování ochranných mechanismů. (Smejkal a kol., 2019)

3.2 Informace

Informace vznikají tehdy, když datům přiřadíme určitý význam, čímž vyřadíme nejasnosti nebo neznalost týkající se konkrétního jevu či události. Takto zpracovaná data se stávají pro uživatele srozumitelná a využitelná. V oblasti informatiky je informace chápána jako strukturovaná data, která lze technickými prostředky přenášet, ukládat, zpracovávat a interpretovat tak, aby poskytovala užitečné poznatky nebo odpovědi na specifické otázky. (IT-slovník.cz, 2024)

3.3 Kyberprostor – Kybernetický prostor

Kyberprostor představuje digitální prostředí, kde lidé komunikují, sdílejí informace a provádějí různé aktivity prostřednictvím propojených počítačových sítí a internetu. Tento virtuální prostor není omezen fyzickými hranicemi a umožňuje uživatelům přistupovat k širokému spektru služeb, jako je komunikace, online obchod, bankovníctví nebo vzdělávání. Je to dynamický a neustále se rozšiřující digitální ekosystém, který funguje na základě

propojených technologií a platforem. Kyberprostor zahrnuje všechny online prostředí, jako jsou webové stránky, sociální sítě, e-maily, cloudové služby či virtuální komunity, které uživatelé využívají ke vzájemné interakci a výměně informací. Přestože tento prostor neexistuje ve fyzické podobě, jeho fungování podléhá právním regulacím a bezpečnostním standardům. Zajištění ochrany kyberprostoru je důležité pro bezpečný přenos dat, ochranu soukromí a prevenci proti různým digitálním hrozbám. Tento digitální svět se stal zásadní součástí moderní společnosti, kde osobní, ekonomické i sociální aktivity nacházejí své místo a platformy. (Monga, 2025)

3.4 Informační a kybernetická bezpečnost

Termíny „bezpečnost informací“ a „kybernetická bezpečnost“ bývají často zaměňovány, přestože každý z těchto pojmů vyjadřuje specifické aspekty ochrany dat, ačkoliv spolu vzájemně souvisejí a prolínají se. (Calder, 2019)

3.4.1 Bezpečnost informací

Bezpečnost informací zahrnuje ochranu důvěrnosti, integrity a dostupnosti všech informací, které organizace spravuje. Přitom nezáleží na tom, zda jsou data v elektronické nebo fyzické (například tištěné) formě. Z tohoto důvodu se při řízení informační bezpečnosti kromě technologických opatření klade velký důraz také na fyzické a environmentální zabezpečení, jako jsou například uzamykatelné skříně, bezpečnostní dveře s kontrolou přístupu, či sledování pohybu osob v prostorách organizace. (Calder, 2019)

3.4.2 Kybernetická bezpečnost

Kybernetická bezpečnost představuje dílčí oblast informační bezpečnosti a specificky se věnuje elektronickým informacím a systémům, které tato data uchovávají, zpracovávají a přenášejí. Zatímco informační bezpečnost zaujímá komplexní přístup k ochraně všech druhů informací, kybernetická bezpečnost se soustředí především na digitální prostředí a elektronickou komunikaci, včetně technických a fyzických opatření, která tyto elektronické systémy zabezpečují. Oblast kybernetické bezpečnosti je charakterizována dynamickým vývojem, kdy se téměř denně objevují nová rizika a hrozby, na které organizace musí aktivně reagovat, aby si zachovaly konkurenceschopnost a bezpečnost svých dat. (Calder, 2019)

3.5 Informační aktiva

Informační aktiva zahrnují zařízení, software a data, na kterých je závislý provoz organizace nebo instituce. Jedná se především o informace uložené v informačních systémech, firemní dokumentaci a jejich zálohách. Aktiva můžou být základně dělena na hmotná (např. hardware) a nehmotná (např. software). Dále lze informační aktiva rozdělit na primární a podpůrná, kdy je toto rozdělení z hlediska hodnocení rizik vhodnější. (Security Risk Analysis for Information Asset, 2022)

3.5.1 Primární aktiva

Tato aktiva tvoří základní pilíře činnosti organizace a jsou nezbytná pro plnění jejích hlavních úkolů. Bez nich by organizace nemohla plnohodnotně fungovat.

- Informační aktiva – Data uložená v informačních systémech a firemních dokumentech. Jsou klíčová pro rozhodování a naplňování cílů dotčeného subjektu.
- IT služby – Informační a komunikační služby zajišťující podporu důležitých činností organizace.
- Znalosti – Know-how a odborné znalosti zaměstnanců, které jsou stěžejní pro efektivní fungování společnosti. Uchovávání a předávání těchto znalostí je zásadní pro zajištění kontinuity provozu. (Smejkal et al., 2019)

3.5.2 Podpůrná aktiva

Tato aktiva slouží k podpoře a zabezpečení primárních aktiv, čímž umožňují jejich bezproblémové fungování.

- Objekty – Prostředky zajišťující fyzickou bezpečnost, například budovy, trezory, zámky, elektronické zabezpečovací systémy nebo bezpečnostní dveře.
- Technologie – Hardwarová a softwarová infrastruktura, která neobsahuje data, ale zajišťuje jejich zpracování a správu.
- IT procesy – Definovaná pravidla, postupy a aktivity, které podporují provoz informačních technologií.
- Lidské zdroje – Zaměstnanci, kteří se starají o provoz a správu primárních aktiv, například administrátoři, programátoři nebo pracovníci helpdesku.

- Dodavatelé – Externí pracovníci nebo firmy, které poskytují služby spojené s funkcí IT systémů, aniž by byli zaměstnanci organizace.

Efektivní ochrana informačních aktiv je možná pouze tehdy, pokud jsou tato aktiva důkladně identifikována a popsána. Bez přehledu klíčových digitálních aktiv a hodnot organizace není možné správně stanovit náklady na jejich ochranu a minimalizovat rizika spojená s jejich provozem. (Smejkal et al., 2019)

3.6 Data

Data jsou soubory faktů, číselných údajů, textů, obrazů, zvuků, či jiných informací zaznamenaných v určité podobě, vhodné pro uchování, přenos, zpracování nebo interpretaci. Data sama o sobě nemusí být vždy srozumitelná – získávají význam až v určitém kontextu, kdy se přeměňují na informace. Příklad rozdílu mezi daty a informacemi, data – samotné údaje bez bližšího významu (např. čísla: 10, 20, 30), informace – data zasazená do souvislostí, získávající význam. (např. „Průměrná teplota v březnu byla 10°C“). (Ministerstvo školství, mládeže a tělovýchovy ČR, 2024)

3.7 Riziko

Před tím, než přistoupíme k definování pojmů jako hrozba, zranitelnost, událost, incident a útok, je vhodné nejprve stručně objasnit pojem riziko, který je s uvedenými pojmy úzce spojený. Výkladový slovník kybernetické bezpečnosti uvádí, že riziko zahrnuje nebezpečí, či možnost vzniku škody, ztráty nebo neúspěchu. Dále je riziko vnímáno jako důsledek nejistoty při dosahování stanovených cílů, či pravděpodobnost, že určité hrozby využijí existující zranitelnosti aktiv a způsobí organizaci škody.

Riziko lze rovněž chápat jako situaci, kdy potenciální hrozba skutečně využije slabých míst aktiva. Podle směrnice NIS je rizikem každá dostatečně identifikovatelná okolnost nebo událost s potenciálem negativně ovlivnit bezpečnost sítí a informačních systémů. V digitálním prostředí riziko ohrožuje nejen uživatele, ale také počítačové systémy, aplikace a další prvky ICT infrastruktury.

Pojem riziko tedy označuje pravděpodobnost výskytu nežádoucích událostí. Analýza rizik slouží k vyjádření této pravděpodobnosti, přičemž standardizované metody pro identifikaci, analýzu, hodnocení a ošetření rizik stanovuje norma ČSN ISO 31000. (Kolouch a Bašta, 2019)

3.8 Hrozba

Hrozbu lze jednoduše chápat jako faktor nebo okolnost, která může narušit standardní nebo očekávaný stav a zasáhnout do práv či zájmů jiných subjektů. Jedná se o negativní vliv, jehož působení nemusí být nutně dokončeno. Podstatné je, že nebezpečí vzniku negativního stavu existuje a je realistické. V širším smyslu znamená hrozba potenciální důvod vzniku nežádoucího incidentu, jehož následkem může být poškození organizace či systému. Pojem bezpečnostní hrozba, který s tím úzce souvisí, označuje možnou příčinu nežádoucí události, která může vést k poškození systému a jeho aktiv, například ke zničení, neoprávněnému zpřístupnění (kompromitaci), změně dat nebo ztrátě dostupnosti služeb. (Smejkal et al., 2019)

3.9 Zranitelnost

Zranitelnost informačních aktiv představuje slabé místo nebo nedostatek v zabezpečení informačních systémů, technologií, procesů nebo lidského faktoru, které může být využito potenciální hrozbou k narušení důvěrnosti, integrity nebo dostupnosti informací a informačních aktiv. Jinými slovy, jde o jakoukoli nedokonalost či mezeru v systému, aplikaci nebo organizaci, která umožňuje kybernetickým hrozbám způsobit škodu, či jinak ohrozit chod informačního systému. (Strupczewski, 2021)

3.10 Incident

Informační incident představuje nežádoucí nebo neočekávanou událost, která způsobuje (nebo může způsobit) narušení bezpečnosti informací, ohrožuje jejich důvěrnost, integritu nebo dostupnost. Informační incidenty mohou mít různou podobu a intenzitu, od méně závažných narušení, až po závažné kybernetické útoky. (Klein a Zwilling, 2023)

3.11 Útok

Kybernetický útok je cílený a úmyslný pokus o narušení bezpečnosti informačních systémů, sítí nebo dat pomocí různých technik, jako jsou malware, phishing, DDoS útoky nebo zneužití bezpečnostních zranitelností. Cílem těchto útoků je zpravidla získání neoprávněného přístupu, narušení provozu, krádež informací nebo způsobení škody organizaci či jednotlivcům. Prevence a efektivní reakce na kybernetické útoky jsou zásadními prvky kybernetické bezpečnosti. (Legislativa s.r.o., 2022)

4 KYBERNETICKÉ ÚTOKY

V posledních letech se Česká republika potýká s rostoucím množstvím kybernetických útoků. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) zaznamenal v roce 2024 historicky nejvyšší počet incidentů, který činil 268. Nejčastějším typem útoků byly DDoS útoky, za nimiž často stála ruskojazyčná skupina NoName057(16). Tyto útoky způsobovaly dočasnou nedostupnost napadených webů, avšak nedošlo k výrazným dlouhodobým škodám. Kromě DDoS útoků zůstávají hrozbou také ransomware útoky, které mohou vést k zašifrování dat a narušení poskytování služeb. V průběhu roku 2024 byly zaznamenávány jednotky těchto útoků měsíčně, s jejich nárůstem zejména během podzimních měsíců. Rovněž se zvyšuje počet incidentů, při kterých útočníci využívají pokročilé technologie, jako je umělá inteligence, pro sofistikované phishingové kampaně a tvorbu škodlivého softwaru. Tento trend poukazuje na nutnost pravidelné aktualizace bezpečnostních strategií, investic do nových technologií a vzdělávání pracovníků veřejné správy v oblasti kybernetické bezpečnosti. (NÚKIB, 2025)

4.1 DDoS útoky

DDoS útoky (Distributed Denial of Service) představují jeden z nejběžnějších typů kybernetických útoků zaměřených na narušení dostupnosti služby nebo sítě. Princip těchto útoků spočívá v zahlcení cílového serveru nebo sítě obrovským množstvím požadavků z mnoha různých zdrojů současně, čímž dochází k vyčerpání systémových prostředků a následnému výpadku nebo výraznému zpomalení služeb. Tyto útoky mohou být realizovány pomocí botnetů, tedy sítí infikovaných zařízení, která jsou řízena útočníkem. (Burgess, 2022).

4.2 Ransomware

Ransomware je typ škodlivého softwaru, který po proniknutí do systému zašifruje data oběti a následně požaduje výkupné za jejich dešifrování. Tento druh útoku patří mezi nejvýznamnější kybernetické hrozby současnosti, protože může mít devastující dopady na organizace i jednotlivce. Útočníci často využívají techniky phishingu nebo zranitelností v softwaru k proniknutí do systému a následnému šifrování citlivých dat. Podle Kshetriho představují ransomware útoky významnou hrozbu zejména pro finanční instituce, kde mohou způsobit vážné finanční i reputační škody. (Kshetri et al., 2024)

4.3 Phishingové útoky

Tyto útoky jsou jednou z nejrozšířenějších forem kybernetických hrozeb, které se zaměřují na získání citlivých informací, jako jsou přihlašovací údaje, finanční informace nebo osobní údaje. Útočníci se často vydávají za důvěryhodné instituce nebo osoby a pomocí falešných e-mailů, webových stránek nebo textových zpráv se snaží přimět oběť k odhalení svých údajů. Existuje několik typů phishingových útoků, včetně spear phishingu, který je cílený na konkrétní jednotlivce nebo organizace, a whalingu, jenž se zaměřuje na vysoce postavené osoby, jako jsou vedoucí pracovníci firem. Další variantou je smishing (phishing prostřednictvím textových zpráv) a vishing (hlasový phishing), které využívají jiné komunikační kanály než klasický e-mail. (Alkhalil et al., 2021)

4.4 Další typy kybernetických útoků

V předchozích kapitolách byly představeny tři vybrané a často se vyskytující typy kybernetických útoků – DDoS útoky, phishingové útoky a ransomware. Tyto tři typy útoků představují v současnosti největší hrozbu pro řešenou obec. Je však třeba zdůraznit, že výše uvedené útoky nepředstavují vyčerpávající výčet všech hrozeb v oblasti kybernetické bezpečnosti. Mezi další významné typy útoků patří například man-in-the-middle útoky, SQL injection, malware aj. Spektrum kybernetických útoků je velmi široké a neustále se vyvíjí, což jen potvrzuje důležitost pravidelné aktualizace bezpečnostních opatření a sledování aktuálních trendů v oblasti kybernetických hrozeb.

5 TRIÁDA CIA

CIA triáda představuje základní princip v oblasti ochrany informací, zaměřený na zajištění důvěrnosti, integrity a dostupnosti dat. Tento koncept se stal důležitým vodítkem pro bezpečnostní postupy v IT a kybernetické bezpečnosti. S rostoucí digitalizací a rozvojem informačních technologií se výrazně zvýšila potřeba chránit citlivé informace před neoprávněným přístupem či zneužitím. CIA triáda se proto stala základním modelem, který pomáhá organizacím i jednotlivcům efektivně chránit data. Jejím cílem je minimalizovat rizika spojená s únikem, ztrátou nebo manipulací s daty, a zajistit jejich ochranu na základě principů důvěrnosti, integrity a dostupnosti. Každý prvek této triády má svůj specifický účel a společně tvoří pevný základ pro budování bezpečnostních strategií a ochranu dat v digitálním prostředí. Tyto tři prvky jsou základem, ale lze je doplňovat a modifikovat o další prvky, které rozšiřují efektivitu ochrany. Lze například rozšířit prvek dostupnosti o prvek ztráty, kdy nedochází jen k dočasnému omezení dostupnosti aktiva, ale k jeho úplné ztrátě. Tohoto bylo využito i v této práci. (Vaněk, 2023)



Obrázek 1 Triáda CIA

(zdroj: Pochopení triády CIA, 2024)

5.1 Důvěrnost

Opatření zaměřená na důvěrnost, která jsou často spojována s ochranou osobních údajů, mají za cíl zabránit neoprávněnému přístupu k citlivým informacím. Data bývají zpravidla klasifikována na základě potenciálních škod, které by mohly vzniknout, pokud by se dostala do nepovolaných rukou. Na základě této klasifikace jsou pak přijímána různě přísná bezpečnostní opatření, přizpůsobená konkrétní míře rizika. (Informa TechTarget, 2024)

Bezpečnostní standardy ISO/IEC 27000 definují že:

- „Informace by měly být klasifikovány, a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.“
- „Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.“
- „Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.“ (Kolouch a Bašta, 2019)

Aby se zabránilo přístupu neoprávněných osob k informacím, je nutné stanovit jasná pravidla pro jejich manipulaci, přístup a ukládání. (Kolouch a Bašta, 2019)

Klasifikace informací dle § 4 zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti:

- *Přísně tajné, neoprávněné nakládání s informacemi by mohlo způsobit mimořádně vážnou újmu zájmům České republiky.*
- *Tajné, neoprávněné nakládání s informacemi by mohlo způsobit vážnou újmu zájmům České republiky.*
- *Důvěrné, neoprávněné nakládání s informacemi by mohlo způsobit prostou újmu zájmům České republiky.*
- *Vyhrazené, neoprávněné nakládání s informacemi by mohlo být nevýhodné pro zájmy České republiky.* (ČESKO, 2005)

Pro subjekty, které se neřídí zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, může být využívána klasifikace informací dle přílohy 5 Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti. (NÚKIB, 2022, b)

Tato metodika rozděluje informace do čtyř kategorií:

Veřejné - Informace je veřejně přístupná nebo byla určena ke zveřejnění. Informace může být dále poskytována a šířena bez omezení. Narušení důvěrnosti informací neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takové informace s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP: WHITE.

Interní - Informace nejsou veřejně přístupné, ochrana informací není vyžadována žádným právním předpisem nebo smluvním ujednáním. 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. V případě sdílení takové informace s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: GREEN nebo TLP: AMBER.

Citlivé - Informace nejsou veřejně přístupné a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například osobní údaje). Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta informovaným partnerům. Jiným osobám než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit. V případě sdílení takové informace s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: AMBER.

Diskrétní - Informace nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické informace, zvláštní kategorie osobních údajů). 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. V případě sdílení takové informace s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: RED nebo TLP: AMBER.

(NÚKIB, 2022, c)

Kromě zmíněných klasifikací existuje mnoho dalších systémů označování, které jsou využívány organizacemi nebo jednotlivci na základě právních předpisů nebo vlastního uvážení. Tyto klasifikace mohou být přizpůsobeny konkrétním potřebám a požadavkům uživatelů. (Kolouch a Bašta, 2019)

Traffic Light Protocol (TLP) je nástroj určený pro jasné stanovení úrovně citlivosti informací a pravidel jejich sdílení. Informace jsou označovány specifickými štítky, které určují, za jakých podmínek mohou být dále šířeny. Tento systém je vhodné využívat při práci s chráněnými, citlivými nebo důvěrnými údaji, které je třeba bezpečně a kontrolovaně sdílet s dalšími subjekty či organizacemi. (NÚKIB, 2020)

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	Informace může být sdílena v rámci organizace, které byla informace poskytnuta. Dále může být poskytnuta pouze těm partnerům, kteří splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci. Jiným osobám, než výše uvedeným, nesmí být informace poskytnuta. Původce informace může rozsah sdílení dále omezit.
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:WHITE	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.

Obrázek 2 Traffic Light Protocol

(NÚKIB, 2020)

TPL představuje jednoduchý, ale přitom velmi účinný nástroj pro řízení sdílení citlivých informací. Díky barevnému označení umožňuje jasně určit, jakým způsobem a v jakém rozsahu lze informace dále šířit. Jeho správné používání přispívá k ochraně citlivých údajů.

5.2 Integrita

Integrita dat zahrnuje soubor opatření a mechanismů, které zajišťují, že data zůstávají úplná, konzistentní a přesná během celého jejich životního cyklu. Aby byla data spolehlivá, měla by splňovat zásady ALCOA, což znamená, že musí být:

- přiřaditelná (s jasně určeným autorem),
- čitelná,
- zaznamenaná v reálném čase (nikoli později nebo předčasně),
- původní,
- správná.

Důraz na integritu dat se uplatňuje od jejich prvotního pořízení, přes veškeré úpravy, zpracování, uchovávání a archivaci, až po jejich bezpečnou likvidaci po skončení doby uchovávání. Systém pro zajištění integrity dat by měl umožnit rychlou identifikaci chyb, opomenutí nebo změn, které by mohly ohrozit jejich správnost a konzistenci. Tyto požadavky se vztahují jak na papírové, tak na elektronické záznamy. (EffiChem, s.r.o., 2021)

Ve vyhlášce o kybernetické bezpečnosti v příloze č. 1 je uvedena stupnice pro hodnocení integrity.

- *Nízká - Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy orgánu a osoby uvedené v § 3 písm. c) až e) zákona o KB.*
- *Střední - Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona o KB a může se pro jevit méně závažnými dopady na primární aktiva.*
- *Vysoká - Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona o KB s podstatnými dopady na primární aktiva.*
- *Kritická - Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů orgánu a osoby uvedené v § 3 písm. c) až e) zákona o KB s přímými a velmi vážnými dopady na primární aktiva.*

(ČESKO, 2018)

5.3 Dostupnost

Dostupnost představuje poslední složku triády CIA a zaměřuje se na to, aby byla data a systémy přístupné v okamžiku, kdy jsou potřeba. To znamená, že autentizační procesy, přístupové cesty a technologické systémy musí fungovat správně a bez přerušení, aby uživatelé měli vždy zajištěný přístup k potřebným informacím.

Systémy s vysokou dostupností (HA systémy) jsou speciálně navržené infrastruktury, které mají za cíl minimalizovat výpadky a maximalizovat dostupnost služeb a dat. Tyto systémy mohou zahrnovat redundantní hardware, pravidelné softwarové aktualizace či mechanismy pro obnovu při selhání. Dle konkrétního návrhu mohou HA systémy řešit například hardwarové poruchy, plánované údržby, výpadky napájení nebo přerušení síťového připojení. Navíc mohou obsahovat i více síťových spojení, která umožňují směrování provozu při výpadcích části sítě. Tím se zvyšuje celková spolehlivost a dostupnost kritických služeb. (Forcepoint, 2024)

6 PRÁVNÍ PŘEDPISY, NORMALIZACE A METODIKA

Tato kapitola se zaměřuje na právní a normativní rámec, který tvoří základ pro řízení kybernetické bezpečnosti, konkrétně na úrovni obcí. Přehled právních předpisů, technických norem a doporučených metodik poskytuje potřebný přehled pro pochopení požadavků na ochranu informačních aktiv a pro správné nastavení bezpečnostních opatření. Pozornost je věnována jak národním předpisům, tak i evropským směrnicím a standardům, které v současnosti ovlivňují oblast kybernetické bezpečnosti v České republice.

6.1 Právní předpisy EU v oblasti kybernetické bezpečnosti

Evropská unie reguluje oblast kybernetické bezpečnosti prostřednictvím směrnic a nařízení, která jsou závazná pro všechny členské státy, včetně České republiky. Nařízení jsou přímo použitelná a platí jednotně ve všech členských státech bez nutnosti jejich začlenění do národní legislativy. Naopak směrnice stanovují požadované cíle, ale členským státům ponechávají prostor pro zvolení vhodných prostředků a postupů, jak těchto cílů dosáhnout.

(NÚKIB, 2024)

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 – Směrnice NIS

Směrnice NIS (Network and Information Security Directive) byla přijata 6. července 2016 s cílem zajistit vysokou společnou úroveň bezpečnosti sítí a informačních systémů v rámci Evropské unie. Tento právní předpis ukládá členským státům povinnost přijmout opatření k posílení kybernetické bezpečnosti na národní úrovni, včetně:

- Vytváření strategií pro kybernetickou bezpečnost.
- Zavádění povinností pro poskytovatele základních služeb a poskytovatele digitálních služeb.
- Zajištění spolupráce mezi členskými státy.

(EU, 2016)

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 – Směrnice NIS 2

Směrnice NIS 2 byla přijata 14. prosince 2022 jako modernizace a rozšíření původní Směrnice NIS. Tato nová směrnice si klade za cíl zajistit vysokou společnou úroveň kybernetické bezpečnosti v Evropské unii a reagovat na nové hrozby a technologický

pokrok. Směrnice NIS 2 mění některá ustanovení Nařízení (EU) č. 910/2014 a Směrnice (EU) 2018/1972 a zároveň ruší původní Směrnici NIS (EU) 2016/1148.

(EU, 2022)

Hlavní novinky zahrnují:

- Rozšíření působnosti na více subjektů a oblastí, včetně obcí III. stupně (ORP).
- Zavedení přísnějších požadavků na kybernetickou odolnost a hlášení incidentů.
- Vytvoření mechanismů pro efektivnější spolupráci mezi členskými státy.

Tato směrnice nebyla dosud implementována do právního systému České republiky. Nyní probíhá legislativní schvalování předloženého návrhu zákona. V současné době (jaro 2025) je zákon ve druhém čtení Poslanecké sněmovny Parlamentu ČR. Přijetí nového zákona o KB je prozatím plánováno na polovinu roku 2025.

Nařízení Evropského parlamentu a Rady (EU) 2019/881 – Akt o kybernetické bezpečnosti

Toto nařízení, přijaté 17. dubna 2019, se zaměřuje na posílení role agentury ENISA (Agentura Evropské unie pro kybernetickou bezpečnost) a zavádí evropský rámec pro certifikaci kybernetické bezpečnosti informačních a komunikačních technologií. Nařízení nahrazuje předchozí Nařízení (EU) č. 526/2013 a posiluje pravomoci ENISA zejména v následujících oblastech:

- Podpora členských států při prevenci kybernetických incidentů a jejich řešení.
- Vytváření společných bezpečnostních standardů pro produkty, služby a procesy.
- Posilování evropské certifikace kybernetické bezpečnosti.

(EU, 2019)

Prováděcí nařízení Komise (EU) 2024/482 – Evropský systém certifikace kybernetické bezpečnosti

Prováděcí nařízení Komise (EU) 2024/482, přijaté 31. ledna 2024, stanovuje prováděcí pravidla k Nařízení (EU) 2019/881 v oblasti certifikace kybernetické bezpečnosti. Jedním z hlavních cílů tohoto nařízení je vytvoření evropského systému certifikace kybernetické bezpečnosti založeného na tzv. Společných kritériích (EUCC).

Hlavní oblasti zahrnují:

- Přijetí jednotného systému certifikace platného ve všech členských státech EU.
- Zavedení standardizovaných postupů a kritérií pro hodnocení bezpečnosti.
- Posílení důvěry ve výrobky a služby prostřednictvím certifikace.

(EU, 2024)

6.2 Právní předpisy ČR v oblasti kybernetické bezpečnosti

6.2.1 Zákony

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (KB)

Zákon č. 181/2014 Sb. představuje zásadní legislativní rámec zaměřený na oblast kybernetické bezpečnosti v České republice. Tento právní předpis stanovuje práva a povinnosti subjektů v oblasti kybernetické bezpečnosti a definuje pravomoci orgánů veřejné správy, zejména Národního bezpečnostního úřadu (NBÚ) a Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Zákon zahrnuje implementaci příslušných předpisů Evropské unie a specifikuje opatření pro zabezpečení elektronických komunikací, informačních systémů a sítí.

Je důležité zmínit, že tento zákon se nevztahuje na informační a komunikační systémy, které zpracovávají utajované informace dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Zákon č. 181/2014 Sb. se věnuje především následujícím oblastem:

- Definice základních pojmů a terminologie v oblasti kybernetické bezpečnosti.
- Zavedení bezpečnostních opatření pro zajištění ochrany informačních systémů a sítí.
- Rozlišení mezi bezpečnostními událostmi a bezpečnostními incidenty.
- Procesy spojené s hlášením a evidencí bezpečnostních incidentů.
- Reaktivní a ochranná opatření v případě ohrožení kybernetické bezpečnosti.
- Vyhlášení stavu kybernetického nebezpečí a s tím spojené postupy.
- Výkon státní správy v oblasti kybernetické bezpečnosti.
- Mechanismy kontrol, nápravných opatření a postihů při porušení povinností.
- Vymezení způsobu kontroly činnosti příslušných úřadů.

(ČESKO, 2014)

Právní předpisy související se zákonem o KB

Kromě zákona č. 181/2014 Sb. existují i další zákony, které se přímo, či nepřímo vztahují k problematice kybernetické a informační bezpečnosti. Mezi tyto právní předpisy patří:

- Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů – upravuje principy krizového řízení včetně ochrany kritické infrastruktury (dále KI) na základě Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvků KI.
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy – specifikuje pravidla pro správu a zabezpečení informačních systémů veřejné správy.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti – řeší problematiku elektronických komunikací a poskytování služeb informační společnosti.
- Zákon č. 127/2005 Sb., o elektronických komunikacích – obsahuje pravidla pro provozování a zabezpečení sítí elektronických komunikací.
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti – stanovuje požadavky na ochranu utajovaných informací a bezpečnostní způsobilost osob a subjektů.

(Legislativa s.r.o., 2022)

6.2.2 Vyhlášky a nařízení

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb., známá jako vyhláška o kybernetické bezpečnosti, upravuje pravidla a postupy související s bezpečnostními opatřeními, kybernetickými incidenty, reaktivními opatřeními, náležitostmi podání v oblasti kybernetické bezpečnosti a procesem likvidace dat. Jejím cílem je implementovat příslušné předpisy Evropské unie a zajistit tak ochranu vybraných informačních systémů.

Hlavní oblasti upravené touto vyhláškou zahrnují:

- Strukturu a obsah povinné dokumentace kybernetické bezpečnosti.
- Bezpečnostní opatření pro zajištění ochrany informačních systémů.
- Kategorizaci kybernetických incidentů podle závažnosti.
- Procesy hlášení incidentů a následná reaktivní opatření.

- Komunikační protokoly s příslušnými orgány.
- Pravidla pro likvidaci dat, údajů a informací.

(ČESKO, 2018)

Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu

Vyhláška č. 315/2021 Sb. stanovuje požadavky na bezpečnostní úrovně při využívání cloud computingu orgány veřejné moci, zahrnující ministerstva, úřady, soudy, policii a další instituce. Reguluje poskytování cloudových služeb v oblastech jako jsou servery, vzdálená úložiště, databáze, sítě, software a analytika.

Zaměřuje se především na:

- Definování klíčových pojmů v oblasti cloud computingu.
- Specifikaci bezpečnostních úrovní při využívání cloudových služeb.
- Kritéria pro zařazení cloud computingu do odpovídající bezpečnostní úrovně.
- Přehled oblastí dopadů a jejich členění.
- Skupiny kritérií vztahující se k ochraně osobních údajů.

(ČESKO, 2021)

Vyhláška č. 316/2021 Sb., o požadavcích pro zápis do katalogu cloud computingu

Vyhláška č. 316/2021 Sb. se zaměřuje na požadavky, které musí poskytovatelé cloudových služeb splnit, aby mohli být zapsáni do katalogu cloud computingu spravovaného Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). Tento katalog slouží jako oficiální seznam poskytovatelů, kteří mohou poskytovat služby veřejné správě.

Obsah vyhlášky zahrnuje:

- Požadavky na ochranu důvěrnosti, integrity a dostupnosti informací.
- Seznam doporučených certifikací a auditů.
- Postupy a požadavky na provádění penetračních testů.
- Náležitosti zpráv z penetračních testů a auditů.
- Požadavky na dokumentaci a její strukturu pro hodnocení rizik.

(ČESKO, 2021)

Vyhláška č. 317/2014 Sb., o významných informačních systémech

Vyhláška č. 317/2014 Sb. upravuje identifikaci a kritéria pro určení tzv. významných informačních systémů. Tuto oblast společně spravuje NÚKIB a Ministerstvo vnitra ČR.

Hlavní oblasti zahrnují:

- Vymezení pojmu významný informační systém.
- Kritéria pro identifikaci významných informačních systémů.

(ČESKO, 2014)

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby

Vyhláška č. 437/2017 Sb. stanovuje kritéria pro identifikaci provozovatelů základních služeb. Tento právní předpis se zaměřuje na subjekty, jejichž činnost závisí na elektronických komunikacích nebo informačních systémech a jejichž narušení by mohlo mít zásadní dopad na oblasti jako energetika, zdravotnictví, doprava, bankovníctví či digitální infrastruktura.

Tato vyhláška zahrnuje:

- Implementaci příslušných předpisů Evropské unie.
- Odvětvová a dopadová kritéria pro určení provozovatelů základních služeb.
- Vymezení významu narušení základních služeb.

(ČESKO, 2017)

Další související vyhlášky

Kromě výše uvedených existují i další právní předpisy zaměřené na kybernetickou a informační bezpečnost nebo ochranu utajovaných informací. Patří sem:

- Vyhláška č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších zařízení pracujících s utajovanými informacemi.
- Vyhláška č. 525/2005 Sb. o certifikaci při zajišťování kryptografické ochrany utajovaných informací.
- Vyhláška č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků.

Nařízení vlády

Nařízení vlády č. 432/2010 Sb., ve znění Nařízení vlády č. 315/2014 Sb., definuje kritéria pro určení prvků kritické infrastruktury v České republice. Kritická infrastruktura zahrnuje systémy, zařízení a služby, jejichž narušení nebo zničení by mělo zásadní negativní dopad na bezpečnost státu, jeho ekonomiku nebo životní prostředí.

Toto nařízení se vztahuje na širokou škálu oblastí, mezi které patří:

- Veřejná správa: Úřady, policie, veřejné instituce a další subjekty, jejichž činnost je nezbytná pro fungování státu.
- Komunikační a informační systémy: Mobilní sítě, poštovní služby, televizní vysílání a další klíčové informační a komunikační služby.
- Nouzové služby: Zdravotnická záchranná služba, hasiči, policie a další subjekty poskytující nezbytnou pomoc v krizových situacích.
- Energetická infrastruktura: Systémy zajišťující distribuci a dodávku energií (elektrina, plyn, teplo).
- Nařízení vlády stanovuje následující klíčové oblasti:
- Průřezová kritéria: Obecná kritéria, která se vztahují na více sektorů nebo mají obecný význam pro funkčnost infrastruktury.
- Odvětvová kritéria: Specifická kritéria určená pro jednotlivé sektory kritické infrastruktury, které jsou významné pro fungování státu nebo jeho bezpečnost.

(ČESKO, 2010)

6.3 Normy

Normy ISO v oblasti kybernetické bezpečnosti

Soubor norem ISO 27000 se zaměřuje na řízení informační bezpečnosti. Má úzkou souvislost se zákonem o kybernetické bezpečnosti, jelikož technická a organizační opatření stanovená v tomto zákoně vycházejí z principů obsažených v normě ISO 27001. V praxi lze splnění požadavků zákona a příslušných vyhlášek doložit certifikací, kterou provádí akreditovaný certifikační orgán podle § 29 Vyhlášky o kybernetické bezpečnosti nebo § 3 odst. 2 novely této vyhlášky. (NÚKIB, 2025)

Normy ISO 27000 zahrnují:

ISO 27000: Obsahuje definice klíčových termínů používaných v oblasti informační bezpečnosti napříč celou sadou ISO 27000.

ISO 27001: Specifikuje požadavky na vytvoření, implementaci, udržování a zlepšování systému řízení bezpečnosti informací (ISMS) v souladu s kontextem organizace. Jednotlivé bezpečnostní cíle a opatření jsou odvozeny z normy ISO 27002.

ISO 27002: Poskytuje doporučení pro bezpečnostní opatření rozdělená do 35 hlavních kategorií s celkem 114 kontrolami. Jde o souhrn osvědčených postupů pro informační bezpečnost.

ISO 27003: Zaměřuje se na podporu při zavádění procesu řízení bezpečnosti informací, poskytuje pokyny pro přípravu plánu implementace ISMS podle normy ISO 27001 a nabízí doporučení pro úspěšné zavedení systému.

ISO 27004: Poskytuje návod na tvorbu a používání metrik pro měření efektivity zavedených opatření a fungování ISMS.

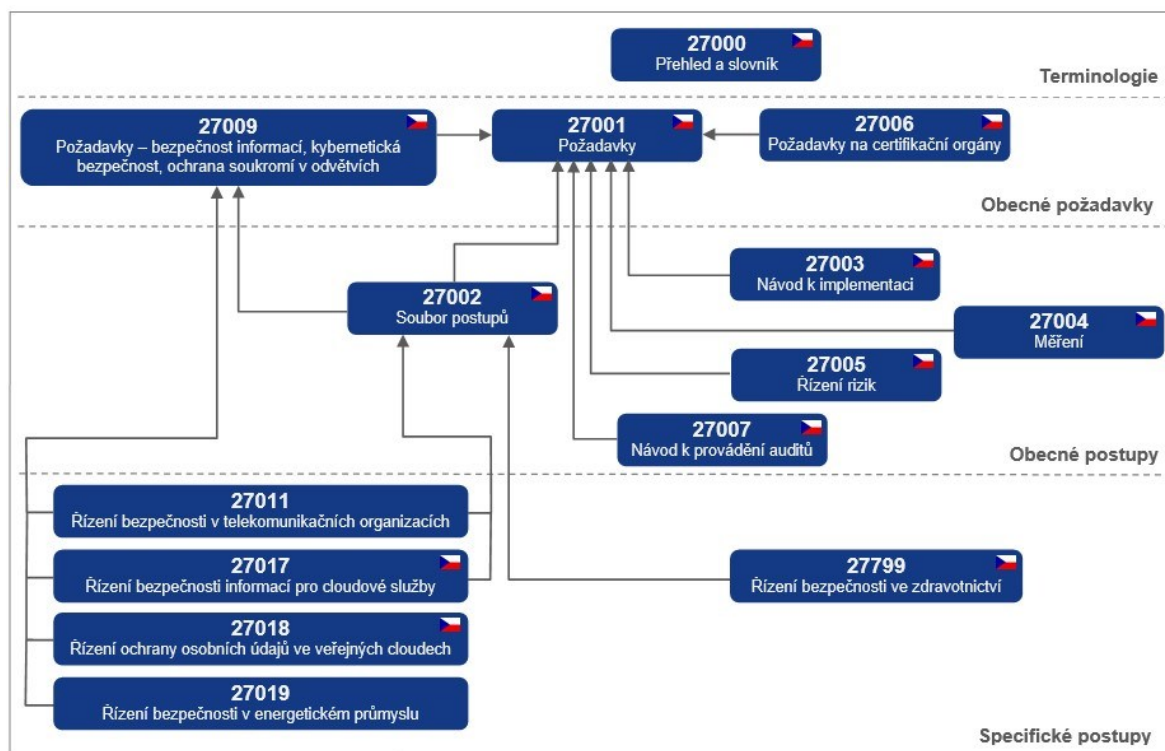
ISO 27005: Zabývá se řízením rizik v oblasti bezpečnosti informací, zahrnuje identifikaci aktiv, hrozeb, zranitelností a potenciálních dopadů. Dále se věnuje hodnocení a ošetření identifikovaných rizik v souladu s požadavky ISO 27001.

ISO 27006: Stanovuje požadavky pro certifikační orgány, které provádějí audity a certifikaci ISMS. Doplněním normy ISO 17021-1 poskytuje kritéria pro akreditaci certifikačních orgánů a podporuje interní hodnocení nebo jiné auditorské procesy.

ISO 27007: Nabízí doporučení pro řízení auditu ISMS a jeho provádění v souladu s ISO 27001. Doplnuje pokyny uvedené v normě ISO 19011, přizpůsobuje je specifickým potřebám auditování ISMS.

ISO 27032: Poskytuje pokyny pro zlepšení kybernetické bezpečnosti, včetně přípravy na útoky, jejich detekce, monitorování a reakce. Zahrnuje také spolupráci mezi subjekty a koordinaci při zvládání incidentů.

(DQS Slovakia s.r.o., 2022)



Obrázek 3 Struktura norem řady ISO 27000

(zdroj: Q-COM s.r.o., 2019)

Výše znázorněný obrázek ukazuje základní strukturu norem řady ISO/IEC 27000, která poskytuje přehled o jejich vzájemných vztazích a zaměření jednotlivých částí.

6.4 Metodika

Podpůrný materiál k řízení aktiv a rizik dle vyhlášky o kybernetické bezpečnosti

Národní úřad pro kybernetickou a informační bezpečnost 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 vytvořil metodický materiál zaměřený na problematiku řízení aktiv a rizik dle ustanovení § 4 a § 5 vyhlášky o kybernetické bezpečnosti.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, spolu s vyhláškou č. 82/2018 Sb., která se zabývá bezpečnostními opatřeními, kybernetickými incidenty, reaktivními opatřeními a dalšími souvisejícími oblastmi, staví své požadavky především na přístupu založeném na analýze rizik. V této souvislosti NÚKIB společně s dalšími organizacemi připravil Průvodce řízením aktiv a rizik, který má usnadnit pochopení a aplikaci požadavků vyhlášky o kybernetické bezpečnosti.

Tento metodický materiál je určen zejména pro osoby s minimálními nebo žádnými zkušenostmi v oblasti řízení aktiv a rizik. Současně jej mohou využít i pokročilejší uživatelé jako inspiraci pro zdokonalení vlastních zavedených postupů. Dokument má sloužit jako podpůrný nástroj k aplikaci principů řízení aktiv a rizik tak, aby vyhovoval požadavkům vyhlášky.

Podpůrný materiál poskytuje jeden z možných postupů pro správné řízení aktiv a rizik v souladu s vyhláškou o kybernetické bezpečnosti. Přestože se jedná o doporučení, které by mělo být přizpůsobeno specifickému prostředí dané organizace, nabízí základní principy a postupy k dosažení souladu s právními požadavky.

Dokument zahrnuje teoretické i praktické části spolu s modelovými příklady. V teoretické části jsou podrobně vysvětleny jednotlivé požadavky vyhlášky, zatímco praktická část se zaměřuje na jejich aplikaci v praxi. Modelové příklady pak ilustrují obecné postupy na příkladu fiktivního Ministerstva pro certifikaci senzorů. Tento metodický materiál je založen na požadavcích vyhlášky o kybernetické bezpečnosti a doplněn o praktické zkušenosti z reálného prostředí. (NÚKIB, 2022)

Kybernetická bezpečnost obcí

Tento metodický materiál NÚKIB je zaměřen na problematiku kybernetické bezpečnosti obcí. Jednotlivé kapitoly tohoto metodického dokumentu poskytují čtenářům informace o tom, jak správně plnit povinnosti vyplývající z aktuálního zákona o kybernetické bezpečnosti a související vyhlášky týkající se bezpečnostních opatření u poskytovatelů regulované služby v režimu nižších povinností, které jsou zvláště důležité pro obce s rozšířenou působností. (NÚKIB, 2024)

6.5 Právní předpisy v oblasti veřejné správy

Ústavní zákon č. 1/1993 Sb. Ústava České republiky

Územní samospráva je zakotvena v Ústavě České republiky v Hlavě VII.

Územní uspořádání České republiky tvoří obce a kraje, přičemž obce představují základní jednotky samosprávy a kraje fungují jako vyšší územní samosprávné celky. Tyto celky tvoří společenství obyvatel, kterým právní řád přiznává možnost samostatně rozhodovat o vybraných záležitostech veřejného života. V některých případech plní i roli správních obvodů, kdy vykonává státní správu formou přenesené působnosti, přičemž rozsah jejich

pravomocí v této oblasti vymezuje zákon. Jakékoli změny ve struktuře vyšších územních celků, tedy jejich zřízení nebo zrušení, jsou možné pouze prostřednictvím ústavního zákona. (ČESKO, 1993)

Zákon č. 128/2000 Sb. o obcích

Obce a kraje jako územní samosprávné celky vykonávají svou správu prostřednictvím zastupitelstev, která jsou volena občany. Jejich fungování se řídí příslušnými právními předpisy – konkrétně u obcí jde o zákon o obcích, u krajů o zákon o krajích a v případě hlavního města Prahy o speciální zákon, který upravuje jeho specifické postavení. Tyto samosprávné celky jsou veřejnoprávními korporacemi, mají právní subjektivitu, vlastní majetek a hospodaří dle svého rozpočtu. Stát může do jejich záležitostí zasahovat pouze v odůvodněných případech, kdy je třeba chránit veřejný zájem nebo zajistit dodržování zákonů, a to výhradně v rámci pravomocí, které mu stanoví zákon. (ČESKO, 2000)

Zákon č. 314/2002 Sb. o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností

Obecní úřady obcí s rozšířenou působností, tzv. ORP, vznikly od 1. ledna 2003 podle zákona č. 314/2002 Sb. o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností. Tyto ORP jsou nástupnickými úřady po zaniklých Okresních úřadech (převzali jejich agendu). Obcí s rozšířenou působností je i obec, která je řešena v této diplomové práci. Do jejího výkonu spadá řada působností, a to nejen pro vlastní správní obvod, ale i pro dalších třináct obcí ve svém správním obvodu.

Jde zejména následující agendy přenesené státní působnosti:

- registr obyvatel
- evidence osobních a cestovních dokladů
- registr řidičů
- registr vozidel
- živnostenský úřad
- stavební úřad
- sociální úřad
- sociální ochrana dětí OSPOD
- vodoprávní úřad

- oblast odpadového hospodářství
- životního prostředí
- státní správa v oblasti lesního hospodářství, myslivosti a rybářství
- silniční správní úřad
- projednávání přestupků

Jde o činnosti vykonávané na základě zákonů, tedy jasně a konkrétně definované činnosti vykonávané podobně na úrovni všech ostatních ORP, kterých je v ČR celkem 205. K zajištění výkonu všech agend využívají obce zpravidla více informačních systémů, některé jsou celostátně unifikované (například činnost registru vozidel a řidičských průkazů), jiné se mohou značně lišit (spisová služba). (ČESKO, 2002)

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy ISVS

Co se týče legislativy České republiky v oblasti ICT veřejné správy, je pro provozování ISVS nejvýznamnější zákon č. 365/2000 Sb., o informačních systémech veřejné správy ve znění pozdějších předpisů. Zákon byl již mnohokrát novelizován právními úpravami, reagujícími na současné potřeby ISVS. Poslední novelou je zákon č. 471/2022 Sb.

Neméně důležité jsou i navazující prováděcí vyhlášky, které byly vytvořeny k výše uvedenému zákonu. Opět se dá říct, že nejvýznamnější je vyhláška č. 528/2006 Sb., o informačním systému o ISVS. Vyhláška stanovuje povinnost správcům ISVS podávat informace o provozu ISVS do informačního systému o ISVS. Dále vyhláška obsahuje informace o dostupnosti a obsahu zpřístupněných informačních systémů. (ČESKO, 2000)

7 MANAGEMENT RIZIK

Řízení rizik je systematický proces identifikace, analýzy, hodnocení a následné ošetření rizik, které mohou negativně ovlivnit dotčený subjekt. Zahrnuje analýzu pravděpodobnosti a dopadu rizik, vývoj strategií k minimalizaci škod a monitorování účinnosti přijatých opatření. (Harvard Business School, 2023)

Management rizik podle ČSN ISO 31000 a ČSN EN ISO/IEC 27005

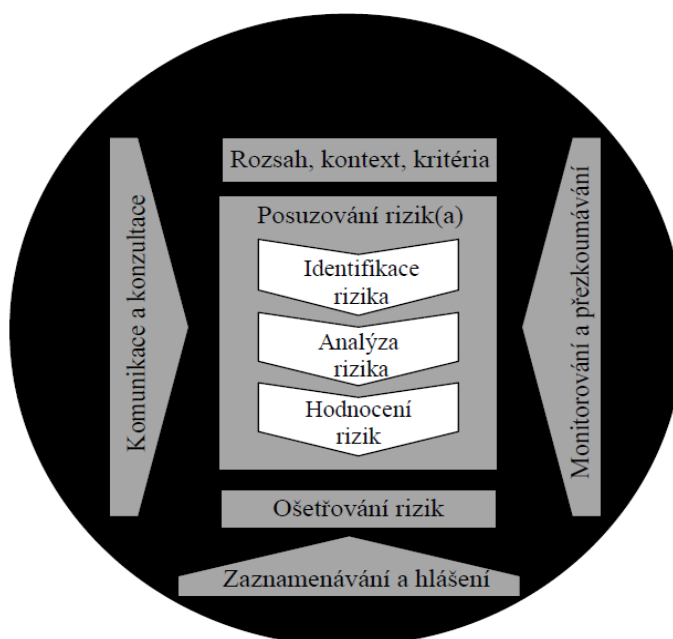
Řízení rizik je klíčovým prvkem zabezpečení informačních systémů a obecně celkového managementu dotčených subjektů. Při efektivním řízení rizik je nutné aplikovat metodické postupy, které umožňují komplexní zvládání rizik, což zajišťuje minimalizaci negativních dopadů a maximalizaci příležitostí. V oblasti kybernetické bezpečnosti je problematika řízení rizik řešena nejen obecně uznávanou normou ČSN ISO 31000, ale i specializovanou normou ČSN EN ISO/IEC 27005, která je zaměřena na kybernetická rizika.

7.1 ČSN ISO 31000 – Obecný přístup k řízení rizik

Norma ČSN ISO 31000 představuje obecný rámec pro řízení rizik, který lze aplikovat v jakémkoliv oboru. Tento standard poskytuje pokyny pro návrh, implementaci, udržování a neustálé zlepšování procesu řízení rizik. Hlavními kroky procesu jsou:

- Rozsah, kontext, kritéria: Zahrnuje identifikaci externích a interních faktorů, které mohou ovlivnit dosažení cílů působením nežádoucích faktorů na chráněné zájmy, a vymezení rozsahu a kritérií pro řízení rizik.
- Identifikace rizik: Vyhledávání, nalezení, rozpoznání a popsání rizik, která mohou ovlivnit dosažení stanovených cílů organizace. Tento krok zahrnuje identifikaci hrozeb, zranitelností, aktiv a jejich vzájemných vztahů.
- Analýza rizik: Proces hodnocení pravděpodobnosti a dopadů identifikovaných rizik za účelem stanovení jejich významnosti pro rozhodování.
- Hodnocení rizik: Zahrnuje porovnání výsledků analýzy rizik se stanovenými kritérii rizika, aby bylo možné stanovit, jaká opatření a kde je potřeba je učinit.
- Ošetření rizik: Navržení a aplikace opatření ke zmírnění nebo eliminaci rizik, včetně přijetí rizika, jeho přenosu nebo zmírnění dopadů.

- Zaznamenávání a hlášení: Dokumentování a hlášení výsledků prostřednictvím vhodných mechanismů.



Obrázek 4 Proces řízení rizik dle normy ČSN ISO 31000

(zdroj: ČSN ISO 31000, 2018)

Norma ČSN ISO 31000 se vyznačuje svou flexibilitou a univerzálností, což umožňuje její aplikaci takřka ve všech oblastech, kde je třeba řešit řízení rizik, tedy i v oblasti informačních technologií. (zdroj: ČSN ISO 31000, 2018)

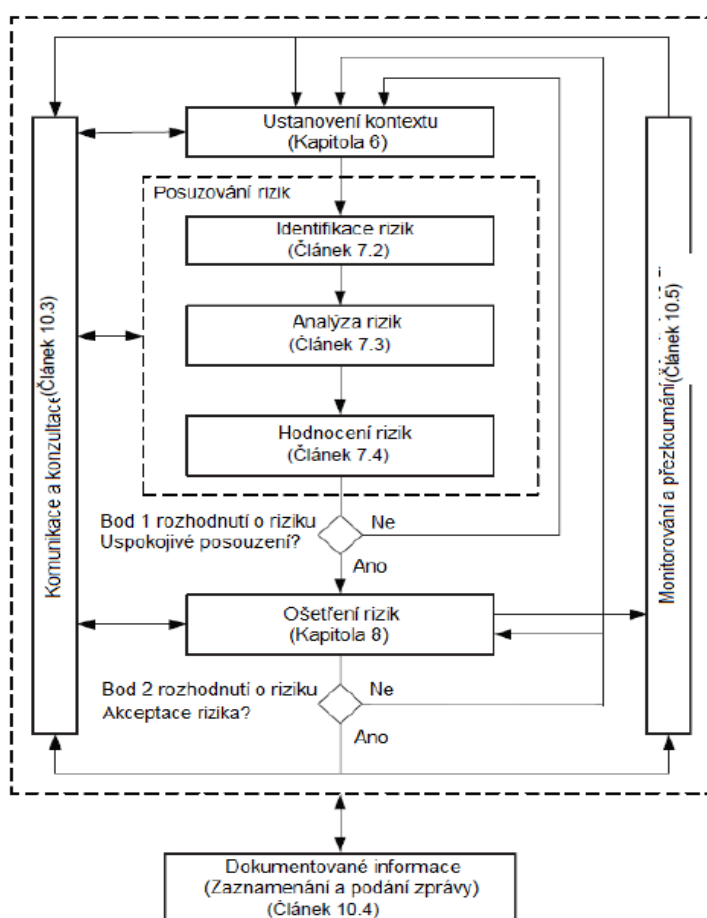
7.2 ČSN EN ISO/IEC 27005 – Management kybernetických rizik

Norma ČSN EN ISO/IEC 27005 poskytuje specifický rámec pro řízení rizik v oblasti informační bezpečnosti. Vychází z principů stanovených v ČSN ISO 31000, ale zaměřuje se konkrétně na identifikaci a řízení rizik spojených s informačními a komunikačními technologiemi.

Klíčové prvky této normy zahrnují:

- Ustanovení kontextu: Specifikaci externího i interního prostředí, ve kterém řešený subjekt funguje, stanovení objektů řízení rizik v návaznosti na strategii organizace.
- Identifikaci rizikových aktiv: Určení hodnotných prvků (informační aktiva) v rámci organizace, které je třeba chránit.

- Identifikaci hrozeb a zranitelností: Analýza možných zranitelností, hrozeb a jejich vazeb na identifikovaná aktiva.
- Analýza rizik: Stanovení pravděpodobnosti hrozeb a jejich dopadů na identifikovaná aktiva organizace.
- Ošetření rizik: Navržení vhodných bezpečnostních opatření ke zmírnění identifikovaných rizik.
- Dokumentované informace: Uchovávání dokumentovaných informací týkajících se procesu posuzování rizik a procesu ošetření informačních rizik.



Obrázek 5 Proces řízení informačních rizik dle normy ČSN EN ISO/IEC 27005

(zdroj: ČSN EN ISO/IEC 27005, 2022)

ČSN EN ISO/IEC 27005 poskytuje metodické pokyny pro práci s riziky v oblasti kybernetické bezpečnosti a úzce souvisí s implementací systému řízení informační bezpečnosti (ISMS) podle normy ČSN EN ISO/IEC 27001. (zdroj: ČSN EN ISO/IEC 27005, 2022)

7.3 Komparace norem ČSN ISO 31000 a ČSN EN ISO/IEC 27005

I když jsou obě normy zaměřeny na řízení rizik, jejich zaměření a rozsah se poněkud liší. Norma ČSN ISO 31000 poskytuje obecný rámec, který je vhodný pro široké spektrum oblastí řízení rizik, zatímco ČSN EN ISO/IEC 27005 se specializuje výhradně na kybernetickou bezpečnost.

Obě normy zdůrazňují cyklický charakter řízení rizik, což zahrnuje pravidelný přezkum a aktualizaci přijatých opatření. Norma ČSN EN ISO/IEC 27005 však nabízí detailnější pokyny pro identifikaci hrozeb a zranitelností specifických pro oblast kybernetické bezpečnosti.

Význam aplikace obou norem.

Úspěšné řízení rizik v organizaci závisí na efektivním využití obou norem. ČSN ISO 31000 poskytuje univerzální rámec pro analýzu rizik, který lze aplikovat na různé oblasti činností organizace. Na druhé straně ČSN EN ISO/IEC 27005 poskytuje konkrétní postupy a doporučení zaměřené přímo na informační a kybernetickou bezpečnost.

Kombinace těchto dvou přístupů umožňuje organizacím efektivně identifikovat, hodnotit a řídit rizika spojená s informačními systémy a komunikačními technologiemi. V oblasti kybernetické bezpečnosti je klíčové průběžně monitorovat změny v rizikovém prostředí a přizpůsobovat ochranná opatření aktuálním hrozbám.

Rizika je nutné pravidelně sledovat, vyhodnocovat a přijímat odpovídající opatření pro jejich zvládnutí. Stejně jako jiné strategické plány se rizika stanovují periodicky a následně se upravují podle vývoje situace. Tento proces se obvykle přehodnocuje minimálně jednou ročně, ale v případě potřeby může být prováděn i častěji. (Aptien Labs s.r.o., 2024)



Obrázek 6 Proces sledování a zlepšování řízení rizik

(zdroj: Aptien Labs s.r.o., 2024)

8 SHRUTÍ TEORETICKÉ ČÁSTI

V teoretické části byla zkoumaná problematika charakterizována pomocí literární rešerše. Základní literární zdroje, ze kterých bylo převážně čerpáno při její tvorbě, jsou stručně uvedeny v úvodu práce. Teoretická část dále blíže vysvětluje klíčové pojmy z oblasti kybernetické bezpečnosti tak, aby bylo čtenáři objasněno základní názvosloví a lépe se orientoval v daném tématu.

Byly popsány v současnosti nejčastější kybernetické útoky na veřejnou správu. Dále je zde představen koncept triády CIA, který tvoří základní princip ochrany informací a je zaměřen na zajištění důvěrnosti, integrity a dostupnosti dat. Tento koncept je zásadní i pro praktickou část práce, neboť jeho pomocí bylo prováděno hodnocení všech identifikovaných aktiv a byl využíván po celou dobu analýzy rizik.

Významnou součástí teoretické části je také kapitola věnovaná legislativě, standardizaci a metodikám, jak v oblasti analýzy rizik, tak v oblasti kybernetické bezpečnosti. Popsány byly klíčové legislativní předpisy českého i evropského práva, které jsou povinně implementovány do právního řádu ČR.

Dále je přiblížen management rizik, zejména mezinárodně uznávané normy pro systémy řízení rizik ČSN ISO 31000 a s ní úzce související norma pro systém řízení informačních rizik ČSN EN ISO/IEC 27005, která z předchozí normy vychází. Rovněž je zmíněna metodika, která upravuje postup při analýze aktiv a rizik se zaměřením na kybernetickou bezpečnost obcí. Tato metodika byla využita jako hlavní východisko při tvorbě této práce.

Teoretická část poskytuje ucelený přehled teoretických poznatků, které tvoří základ pro analyticko-empirickou a aplikační část diplomové práce. Jejím cílem je usnadnit pochopení zkoumané problematiky a vytvořit pevný rámec pro následné praktické analýzy a návrhy.

II. PRAKTICKÁ ČÁST

9 ÚVOD DO PRAKTICKÉ ČÁSTI

Pro zodpovězení hlavní výzkumné otázky diplomové práce, která je orientována na analýzu způsobu řízení rizik kybernetické bezpečnosti ve vybrané obci, bylo nezbytné podrobně analyzovat a zhodnotit celý systém řízení rizik v konkrétní organizaci. Praktická část práce proto zahrnuje podrobné představení vybrané obce včetně popisu její základní struktury, zaměření a specifických podmínek týkajících se kybernetické bezpečnosti. Důraz je kladen na procesní aspekty, organizační rámec a aktuálně využívané metody řízení rizik.

Následně je podrobně rozpracován celý proces řízení rizik v této obci. Proces je rozčleněn do několika přehledných a logicky navazujících kroků, od stanovení kontextu, identifikace, analýzy a hodnocení potenciálních hrozeb až po implementaci opatření a následný monitoring jejich účinnosti. Každý krok je detailně popsán a analyzován v kontextu reálného fungování obce, což umožňuje srovnat teoretické předpoklady s praktickým výkonem řízení rizik.

Na základě provedené analýzy jsou následně formulována konkrétní doporučení vedoucí k optimalizaci a zefektivnění stávajícího procesu řízení rizik. Doporučení se týkají například zlepšení metodik řízení rizik podle nových legislativních norem NIS2 a ČSN EN ISO/IEC 27001, rozšíření použití nástrojů pro sledování kybernetických hrozeb a navržení efektivnějších bezpečnostních strategií uvnitř organizace. Tato doporučení cílí nejen na zvýšení kvality celého systému, ale rovněž na posílení schopnosti obce včas reagovat na nové hrozby v oblasti kybernetické bezpečnosti.

10 PŘEDSTAVENÍ ŘEŠENÉHO ÚZEMNĚ SAMOSPRÁVNÍHO CELKU

Územně samosprávný celek se nachází v jednom z moravských krajů. Jedná se o obec, která má status města a zároveň je obcí s rozšířenou působností (ORP), tedy obec III. kategorie dle zákona o obcích. Rozloha území činí přibližně 33 km², skládá se ze čtyř katastrálních území a trvale zde žije zhruba 5000 obyvatel, včetně obyvatel tří integrovaných obcí.

Z pohledu infrastruktury prochází obcí jedna hlavní pozemní komunikace, silnice II. třídy, nachází se zde konečná stanice železniční trati a od roku 2010 také veřejné sportovní letiště. Díky této infrastruktuře má obec kvalitní dopravní spojení s okolními městy i dalšími regiony České republiky.

Z hlediska geografické polohy se obec nachází v hornatém terénu a je obklopena zalesněnými vrchy, které jsou z velké části součástí Chráněné krajinné oblasti (CHKO). Zastavěná část obce se rozkládá v údolí, jímž protéká menší řeka. Jednotlivé budovy jsou rozmístěny po obou stranách údolí a v obci je evidováno okolo 1100 domů. Především v severozápadní části obce se nachází lokalita s nalezištěm léčivých zdrojů. Tato oblast je velmi atraktivní pro turisty a je celoročně hojně navštěvována. Obec je známá svou architekturou, která je ovlivněna secesním stylem a lidovým uměním. Nejvýznamnější architektonické památky se nacházejí v památkové zóně poblíž uvedeného naleziště léčivých zdrojů, kde se zároveň pořádá řada kulturních akcí.

K informování obyvatelstva slouží především kvalitně zpracovaný a pravidelně aktualizovaný web obce, který poskytuje informace o dění v obci a nabízí potřebné údaje občanům i návštěvníkům. Obec rovněž zajišťuje občanům kontakt s veřejnou správou prostřednictvím služby Czech POINT, kde mohou získat výpisy z různých rejstříků. V centru obce se nachází náměstí s kruhovým objezdem a fontánou. Nad tímto náměstím je umístěna dominantní budova, která slouží jako sídlo obecního úřadu.

Jak bylo uvedeno v teoretické části této práce, jednou ze základních a zároveň klíčových institucí obce je obecní úřad. Z pohledu kybernetické bezpečnosti se jedná o zásadní prvek, protože právě obecní úřad spravuje značné množství citlivých informací a prostředků, které mohou být potenciálně ohroženy kybernetickými útoky.

10.1 Popis budovy obecního úřadu

Jak již bylo v předchozích kapitolách zmíněno, obecní úřad představuje dominantní stavbu na náměstí obce. Jedná se o objekt prvorepublikové architektury, který byl původně vystavěn jako finanční instituce. Budova úřadu má obdélníkový půdorys s půlkruhovou přístavbou zasedací místnosti. Je tvořena částečně podsklepeným přízemím a dalšími třemi nadzemními podlažími, zastřešenými sedlovou střechou.

V roce 2001 prošla celá budova kompletní rekonstrukcí, především kvůli tomu, že obec získala status obce s rozšířenou působností (ORP), což vyžadovalo úpravu všech prostor pro výkon nezbytných administrativních agend. Budova obecního úřadu je zabezpečena pomocí poplachového zabezpečovacího a tísňového systému (PZTS), který je napojen na pult centralizované ochrany (PCO) soukromé bezpečnostní agentury. Stálý přístup do objektu mají pouze vybraní zaměstnanci: vedení obce, tj. starosta, místostarosta, tajemník, vedoucí odborů a někteří další zaměstnanci, například pracovníci úklidu, správce IT, krizový pracovník a správce budovy, který ráno budovu otevírá a deaktivuje (tzv. „dekóduje“) systém PZTS. Po skončení pracovní doby budovu zamykají a aktivují („kódují“) pracovníci úklidu. Ostatní zaměstnanci mají přístup pouze v době pracovní doby.

Budova má tři vstupy – hlavní vchod pro veřejnost a dva boční vchody. Jeden z nich je určen výhradně zaměstnancům a je zabezpečen elektronickým zámekem, druhý slouží jako evakuační a záložní východ a běžně se nepoužívá. U vstupu pro zaměstnance je vlevo za dveřmi umístěn docházkový modul typu WP-9S-1EM spolu s přístupovým modulem s klávesnicí pro ovládání systému PZTS. Od roku 2024 jsou hlavní vstup i vstup pro zaměstnance nepřetržitě monitorovány kamerovým systémem se záznamem. Celá budova obecního úřadu tvoří z pohledu zabezpečení (PZTS) jeden celek, a všechny oprávněné osoby tedy disponují stejnými přístupovými právy.

V samotné budově úřadu je celkem dvacet devět kanceláří, z nichž některé jsou vybaveny detektory pohybu. U kanceláří bez těchto detektorů jsou senzory umístěny na přilehlých chodbách. Okna v přízemních kancelářích jsou kromě detektorů pohybu chráněna také detektory otevření oken a detektory tříštění skel. Kancelář IT a archivy, nacházející se v suterénu budovy, jsou navíc zvenku zabezpečeny mřížemi.

10.2 Ostatní budovy obecního úřadu

Obecní úřad disponuje dalšími dvěma budovami, ve kterých se nachází detašovaná pracoviště jednotlivých odborových agend. Zřízení těchto detašovaných pracovišť bylo nutné s ohledem na kapacity hlavní budovy a s ohledem na potřebu výkonu všech agend, které jsou uloženy ORP v rámci přenesené působnosti.

Jednou z těchto budov je budova, kde se najdeme pracoviště Odboru životního prostředí, Odboru sociálního a Živnostenské oddělení. Jedná se o čtyřpatrovou budovu, která slouží nejen k úřednímu využití obce, ale i k účelům ostatních úřadů, jako je například Finanční úřad, jehož pracoviště zde sice bylo zrušeno, ovšem v období podání daňových zde sídlí jeho podatelna. Dále také ke komerčním účelům, například obchody umístěné v přízemí s vlastními oddělenými vstupy přímo z ulice. Obecní úřad zabírá celá dvě podlaží této budovy. Rovněž tyto prostory obecního úřadu jsou kompletně zabezpečeny PZTS s připojením na PCO soukromé bezpečnostní agentury. Budova je od roku 2024 monitorována kamerovým systémem se záznamem. Do prostor mají trvale přístup všichni zaměstnanci, kteří na těchto pracovištích pracují.

Druhou budovou je budova, kde se nachází městská policie (MP) a detašované pracoviště části Odboru přestupkového (OP). Jedná se o dvoupodlažní budovu, ve které se, mimo již uvedeného, nachází také ordinace soukromé lékařské praxe. Celá budova je kompletně zabezpečena PZTS s připojením na PCO soukromé bezpečnostní agentury a okna kanceláří v přízemní jsou navíc zabezpečena mřížemi. PZTS je zde třísektorové s rozdělením na MP, OP a ordinaci. Každý z těchto sektorů má vlastní přístupový kód a přístup do budovy je pro oprávněné osoby možný nepřetržitě. Tato budova je od roku 2024 rovněž monitorována kamerovým systémem se záznamem.

10.3 Zaměstnanci úřadu

V současné době je v pracovním poměru obce 88 zaměstnanců, které lze dělit na tři základní skupiny:

- Vedení obce
- Úředníci, výkon úkolů v přenesené působnosti obce
- Ostatní profese, výkon úkolů v samostatné působnosti obce

Úředníkem se podle zákona č. 312/2002 Sb., o úřednících územních samosprávných celků, konkrétně dle § 2 odst. 4, rozumí zaměstnanec územního samosprávného celku, který vykonává správní činnosti. Tento pracovník je zařazen do různých typů úřadů, například do obecního nebo městského úřadu, v případě statutárního města do magistrátu, či jeho územně členěné části, do úřadu městského obvodu, krajského úřadu, Magistrátu hlavního města Prahy nebo úřadu některé z městských částí Prahy.

Jedná se o výkon státní správy, kterou stát přenesl na výše uvedené samosprávní celky.

(Ministerstvo vnitra České republiky, 2025)

Zaměstnanci obce, kteří působí v rámci samostatné působnosti, vykonávají svou činnost ve prospěch samotné obce, a to tak, aby naplňovali její vlastní cíle nebo potřeby jejích obyvatel. Tato činnost může zahrnovat například správu obecního bytového fondu, zajištění dopravní obslužnosti, podporu zdravotnických služeb, školství nebo kulturních aktivit.

Rozsah toho, co obce mohou samostatně spravovat, je vymezena prostřednictvím zákona. Pokud má dojít k omezení těchto pravomocí, je možné tak učinit pouze změnou zákona.

Obce i kraje mají zároveň povinnost aktivně přispívat k rozvoji svého území. To zahrnuje vytváření vhodných podmínek pro poskytování potřebných služeb a snahu o naplňování potřeb místní komunity v co nejširším rozsahu.

(Frank Bold, 2017)

Tabulka 1 Zaměstnanci

Zaměstnanci	Počet
celkový počet zaměstnanců	88
vedení obce	3
úředníci	49
ostatní profese	27
strážníci MP	6
informatici	2 + 1 záloha (IT v důchodu)

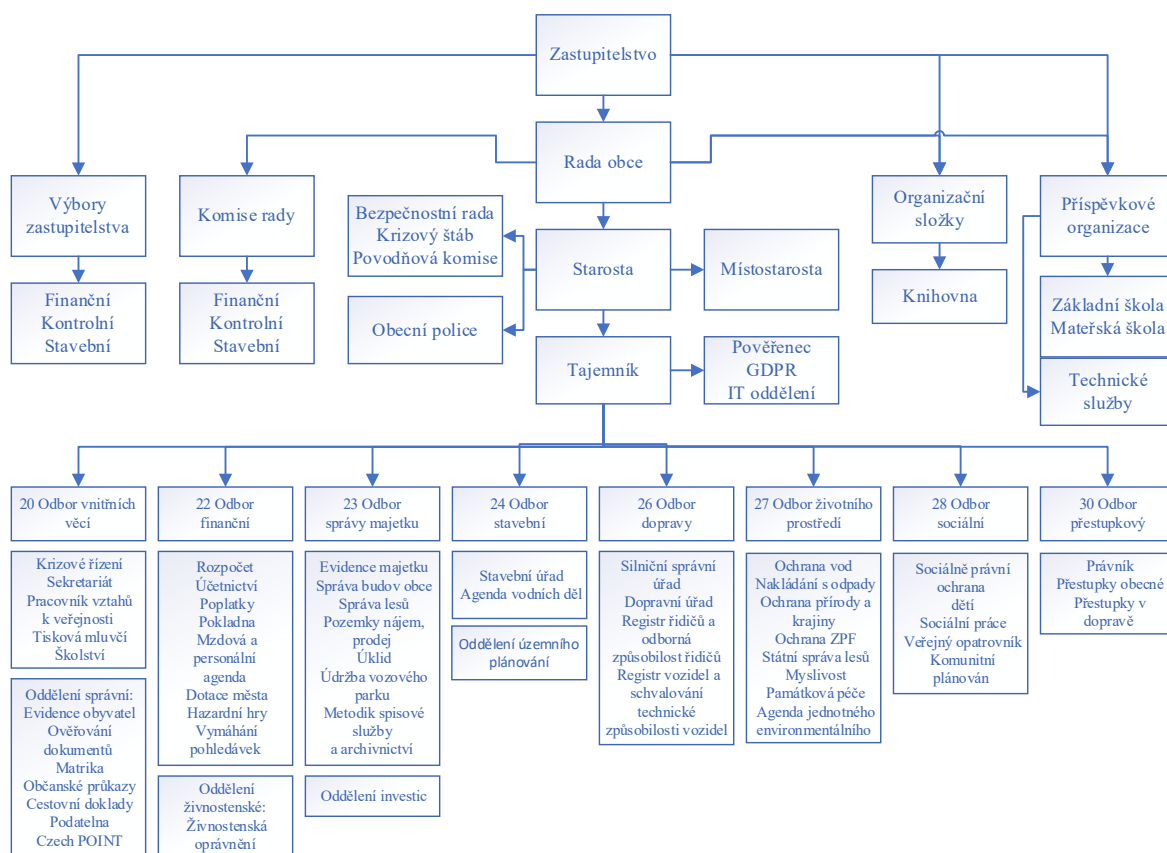
(zdroj: vlastní zpracování)

Tabulka 2 Struktura

Struktura	Počet
odbory	8
oddělení	4
orgány obce	9
výbory zastupitelstva	3
komise rady	4
příspěvkové organizace	6

(zdroj: vlastní zpracování)

10.4 Organizační struktura obce



Obrázek 7 Schéma organizační struktury obce

(zdroj: vlastní zpracování)

11 ANALYTICKO-METODOLOGICKÁ ČÁST

V předchozích kapitolách byl popsán územně samosprávný celek – obec s rozšířenou působností, které se tato diplomová práce stěžejně týká. V následujících kapitolách je provedena analýza rizik této zvolené obce, se zaměřením na informační bezpečnost, resp. kybernetickou bezpečnost.

11.1 Analytická část

Pro realizaci analýzy rizik týkajících se kybernetických hrozeb v obci byl vybrán standardizovaný postup v souladu s normami ČSN ISO 31000 a ČSN EN ISO/IEC 27005, které poskytují komplexní rámec pro systematické řízení rizik. Podle této normy je řízení rizik definováno jako kontinuální proces, který zahrnuje systematickou aplikaci politik, postupů a praxí při komunikaci, konzultaci, stanovování kontextu, identifikaci, analýze, hodnocení, zvládání, monitorování a přezkoumávání rizik. Bližší popis obou norem, i se zobrazenými schématy, je uveden v teoretické části této práce. Pro účely analýzy rizik v oblasti kybernetické bezpečnosti v rámci obce byly realizovány následující kroky.

11.1.1 Stanovení kontextu

V úvodní fázi byla stanovena oblast působnosti analýzy rizik, a to především z pohledu specifických potřeb obecního úřadu jako instituce zajišťující veřejnou správu a služby obyvatelům. Byla vymezena působnost v agendách, a na základě toho vymezení, byla selektována primární aktiva a na základě primárních aktiv jejich podpůrná aktiva.

11.1.2 Identifikace rizik

Na základě stanoveného kontextu byla provedena detailní identifikace potenciálních kybernetických hrozeb. Tato fáze zahrnovala shromažďování informací prostřednictvím analýzy legislativy a dokumentace informačních systémů. Identifikované hrozby byly kategorizovány a zaznamenány do přehledného registru rizik.

11.1.3 Analýza rizik

V této fázi byla provedena podrobná analýza pravděpodobnosti výskytu a dopadu identifikovaných hrozeb. Rizika byla hodnocena jak kvalitativně slovním hodnocením, tak kvantitativně bodováním na škále závažnosti a pravděpodobnosti. Získané údaje byly

následně využity k vytvoření matice rizik, která názorně zobrazuje nejvíce kritická rizika pro obec.

11.1.4 Hodnocení rizik

Na základě provedené analýzy byla posouzena rizika z hlediska přijatelnosti, tedy zda je nutné okamžitě přijmout opatření k jejich zmírnění či odstranění, nebo zda postačuje průběžný monitoring. Hodnocení rizik bylo provedeno ve spolupráci jak s IT pracovníky obce, tak s řadovými zaměstnanci a zahrnovalo diskusi a konsenzus nad prioritami dalšího postupu.

11.1.5 Zvládání rizik

Byla navržena konkrétní opatření vedoucí ke snížení nebo eliminaci kritických kybernetických rizik. Doporučení byla stanovena v souladu s platnou a aktuálně implementovanou legislativou a zahrnovala technická opatření (např. zlepšení fyzické bezpečnosti, modernizaci bezpečnostních technologií), organizační opatření (např. pravidelná školení zaměstnanců, systematické kontroly) a administrativní opatření (např. pravidelná aktualizace bezpečnostních politik).

11.1.6 Monitorování a přezkoumání

V závěrečné fázi analytické části bylo navrženo pravidelné monitorování a periodické přezkoumávání účinnosti zavedených opatření. Tento krok zajistí průběžné vyhodnocování aktuálnosti analýzy rizik a umožní pružně reagovat na případné změny v prostředí kybernetických hrozeb.

11.2 Metodologická část

Veškerá data, která budou použita k analýze rizik kybernetické bezpečnosti vybrané obce, budou získávána formou řízených rozhovorů s odpovědnými pracovníky, kterými jsou vedoucí pracovníci obce, IT zaměstnanci, pracovník krizového řízení, ale i s pracovníky znalými v dané oblasti. Zpracování dat proběhne formou vlastního zpracování a následné komparace s názory a tvrzeními, s již zmiňovanými pracovníky formou konzultací a dotazování.

K analýze rizik byla využita metoda maticového výpočtu, která je metodou základní a je často používána pro identifikaci, analýzu a hodnocení potenciálních rizik v systémech nebo procesech. V souvislosti s kybernetickými hrozbami spočívá analýza v systematickém posouzení jednotlivých informačních aktiv, kde se zkoumají možné způsoby dopadu (například zneužití dat, narušení integrity systémů, nedostupnost služeb) a jejich dopady na obecní úřad.

U každého identifikovaného selhání byla stanovena pravděpodobnost výskytu, míra závažnosti dopadu a schopnost systému detekovat danou hrozbu. Tyto parametry byly následně použity k výpočtu tzv. rizikového čísla (Risk Priority Number - RPN), které umožnilo stanovit priority při implementaci nápravných opatření. Výsledkem této analýzy je cílená prevence nejvýznamnějších kybernetických hrozeb a posílení odolnosti informačních systémů v obci.

Využití normy ČSN ISO 31000 spolu s metodou maticového výpočtu zajistilo systematický, transparentní a efektivní přístup k řízení rizik kybernetické bezpečnosti v řešeném územně samosprávném celku, což přispívá k posílení celkové odolnosti obce vůči kybernetickým útokům.

12 STANOVENÍ KONTEXTU

V rámci stanovení kontextu bylo nutné nejprve analyzovat stávající stav a dokumentaci obce, která se týká bezpečnosti informací a řízení kybernetických rizik. Ačkoli obec již v minulosti realizovala jedno hodnocení rizik v oblasti kybernetické bezpečnosti, toto hodnocení nebylo prováděno podle žádné zavedené metodiky nebo normy, a proto chyběl jasný popis a struktura celého procesu. Rovněž byla zpracována Organizační směrnice – Řízení informační bezpečnosti, ovšem ani tento dokument nesplňuje požadavky, které jsou v této oblasti legislativně požadovány. Jedná se spíše o dokument pracovního právního charakteru, který velmi zevrubně informuje všechny zaměstnance organizace, a spolupracující organizace, o problematice IT a zároveň jim ukládá povinnosti v této oblasti. Většina zaměstnanců nebyla se směrnicí přímo seznámena, nebo o její existenci ani neví.

V této diplomové práci byla využita vzorová metodika obsažená v podpůrných materiálech Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Konkrétně příloha č. 2 – metodika pro identifikaci a hodnocení aktiv a hodnocení rizik dle „Průvodce řízením aktiv a rizik, dle vyhlášky o kybernetické bezpečnosti“, která vychází z platné vyhlášky o kybernetické bezpečnosti a „Kybernetická bezpečnost obcí“. Tento dokument řeší způsoby, jak postupovat při plnění povinností podle nového zákona o kybernetické bezpečnosti a vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, která je právě relevantní pro obce s rozšířenou působností. Tato metodika je upravena pro specifické potřeby obce s rozšířenou působností, zejména pokud jde o terminologii garantů jednotlivých aktiv, nastavení akceptovatelné hranice rizika a formální náležitosti dokumentu.

Dle ustanovení návrhu nového zákona o kybernetické bezpečnosti má každá obec povinnost určit rozsah řízení kybernetické bezpečnosti. Toto vymezení lze chápat jako definování oblasti, která bude podléhat dalšímu systematickému řízení a zavádění příslušných bezpečnostních opatření. V rámci tohoto rozsahu je obec povinna nejen implementovat bezpečnostní opatření, ale rovněž sledovat a případně hlásit bezpečnostní incidenty, které by mohly mít významný dopad právě v definovaném rozsahu.

Obec v rámci stanovení rozsahu řízení kybernetické bezpečnosti identifikuje tzv. primární aktiva. Jedná se především o informace, které jsou zpracovávány, a služby, které jsou poskytovány v rámci regulované služby, typicky označované jako „Výkon svěřených

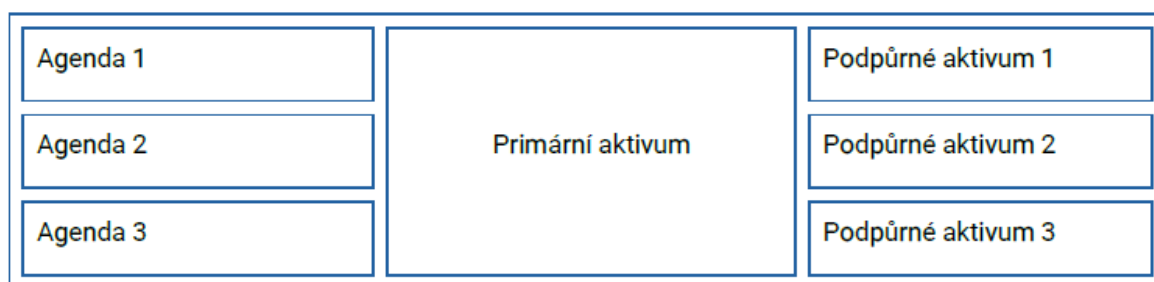
pravomocí“. Tím je zajištěno, že řízení kybernetické bezpečnosti se zaměřuje na oblasti, které mají přímý vztah k hlavní činnosti obce a k výkonu její veřejné správy.

Současně má obec možnost vymezit také oblasti, ve kterých bezpečnostní opatření záměrně zavádět nebude. Takový postup je přípustný zejména tehdy, pokud daná oblast není přímo spojena s regulovanou službou, tedy není nutná k zajištění výkonu svěřených pravomocí. Toto cílené vymezení umožňuje efektivnější a hospodárnější využití zdrojů obce při ochraně těch informačních aktiv, která mají zásadní význam pro plnění jejích základních funkcí a povinností.

Dále je nutno provést identifikaci podpůrných aktiv. Podpůrná aktiva představují zdroje potřebné k zajištění funkčnosti primárních aktiv, která se podílejí na výkonu regulované služby obce. Mezi typická podpůrná aktiva patří například zaměstnanci, externí dodavatelé služeb, technické vybavení (hardware, software), budovy a další prostory, ve kterých se primární aktiva nachází nebo kde dochází k výkonu příslušných agend.

Podpůrná aktiva se evidují ve vztahu k primárním aktivům, přičemž evidence nemusí být nutně vedena pro každou jednotlivou položku zvlášť. Z praktického hlediska je efektivní evidovat podpůrná aktiva po skupinách podle jejich typu či charakteru, zejména pokud jsou ve vztahu ke kybernetické bezpečnosti spravována obdobně. To znamená, že v počáteční fázi stanovování rozsahu kybernetické bezpečnosti není nezbytné evidovat například každý jednotlivý počítač, každého zaměstnance, či konkrétní soubory nebo programy, pokud se jejich zabezpečení a řízení rizik plánuje řešit stejným způsobem.

(zdroj: Kybernetická bezpečnost obcí, 2024)



Obrázek 8 Obecné schéma propojení aktiv

(zdroj: Kybernetická bezpečnost obcí, 2024)

13 POSOUZENÍ RIZIK

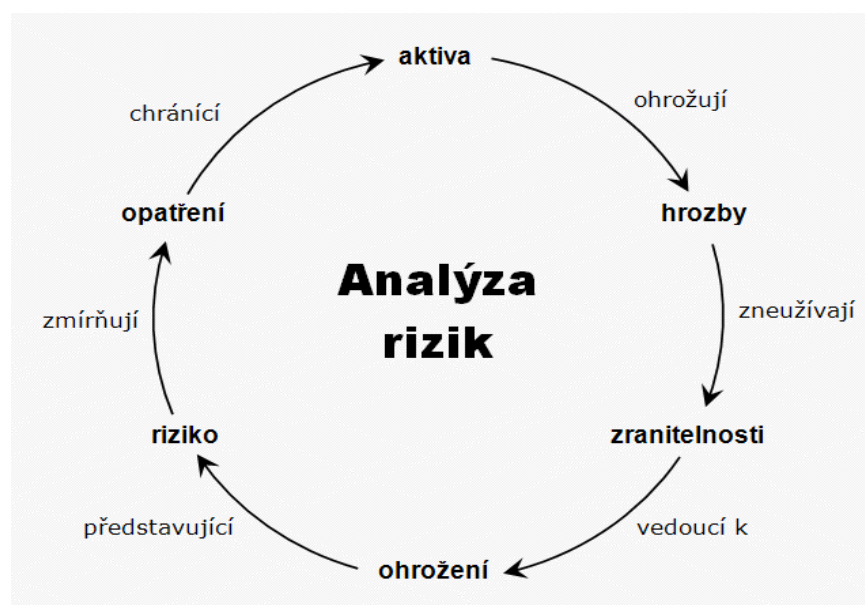
Smyslem procesu posuzování rizik je získat informace o existujících rizicích v rámci jasně definovaného kontextu. Celý proces posouzení rizik lze rozdělit do tří vzájemně navazujících kroků: identifikace rizik, analýza rizik a vyhodnocení jejich přijatelnosti. Prvním nezbytným krokem je identifikace rizik. Ta v teoretické rovině zahrnuje určení aktiv, jejich hodnocení a vhodné kategorizace, a dále také identifikaci relevantních hrozeb a jejich zdrojů. Tyto kroky slouží jako základ pro navazující analýzu rizik. (Ministerstvo životního prostředí, 2022)

13.1 Identifikace rizik

Identifikace rizik zahrnuje jednotlivé kroky, ve kterých jsou nejdříve stanoveny jak primární, tak podpůrná aktiva. Tento krok je velmi důležitý, neboť aktiva jsou to, co má pro jejich vlastníka cenu a co může být ohrožováno hrozbami.

V další fázi jsou zjištěny a pojmenovány hrozby, které představují možné ohrožení pro předmětná aktiva. Identifikace hrozeb probíhá dle scénáře útoků nebo incidentů, jež by mohly vést k ohrožení nebo ztrátě aktiv.

Po identifikaci aktiv a hrozeb následuje určení potenciálních zranitelností, tedy slabých míst nebo nedostatků, která by mohla být zneužita k narušení kybernetické bezpečnosti. Tyto zranitelnosti se mohou týkat jak technologických aspektů, tak organizačních procesů.



Obrázek 9 Schéma analýzy rizik

(zdroj: Čermák, 2010)

13.2 Aktiva

Jak bylo podrobněji popsáno v teoretické části, informační aktiva zahrnují veškerá data, informace a znalosti, které dotčený subjekt využívá ke svému provozu a rozhodovacím procesům. Představují pro organizaci hodnotu, protože umožňují efektivní fungování a řízení. Pokud by v případě dotčené obce došlo k jejich ztrátě, odcizení nebo zneužití, mohlo by to vážně narušit chod celé obce a omezit její schopnost plnit funkce, které jsou jí svěřeny nebo pro které je určena.

Dělení aktiv

Podle vyhlášky o kybernetické bezpečnosti jsou aktiva dělena na primární a podpůrná:

- Primární aktivum představuje informaci nebo službu, kterou zpracovává nebo poskytuje informační a komunikační systém.
- Podpůrné aktivum představuje technické aktivum, zaměstnance a dodavatele podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.

(NÚKIB, 2025)

13.2.1 Garant aktiva

Každé aktivum musí mít přiřazenu odpovědnou osobu, tzv. Garanta. Garant aktiva představuje bezpečnostní roli, která zahrnuje odpovědnost za rozvoj, správu, bezpečné používání a celkovou ochranu aktiva. Úkolem Garanta je dohlížet na to, aby aktivum splňovalo stanovené bezpečnostní požadavky a bylo využíváno odpovídajícím způsobem.

Garanty primárních aktiv obce jmenuje a odvolává tajemník obce, a to na základě návrhu předsedy Výboru. U podpůrných aktiv pak návrh na jmenování a odvolání Garantů předkládá Manažer KB ve spolupráci s Garantem příslušného primárního aktiva, přičemž rozhodnutí o jejich jmenování či odvolání přísluší předsedovi Výboru.

Každé primární i podpůrné aktivum v rámci obce musí mít vždy určeného konkrétního Garanta, který je za dané aktivum odpovědný. Zaměstnanci zastávající bezpečnostní role mohou některé konkrétní činnosti a povinnosti delegovat na jiného zaměstnance. Přesto však konečná odpovědnost a plnění bezpečnostní role zůstává vždy u osoby, která byla do této role oficiálně jmenována. Delegace povinností musí být vždy jasně stanovena a prokazatelně dokumentována. (Svaz měst a obcí České republiky, 2023)

V obci doposud nebyla zpracována systematická evidence primárních aktiv. Bylo proto nezbytné vytvořit jejich ucelený katalog včetně podrobného hodnocení tak, aby odpovídal požadavkům nové legislativy v oblasti strategie řízení rizik a odpovídající metodice. V předmětné obci rovněž doposud neexistuje Výbor pro kybernetickou bezpečnost, jehož předseda by mohl navrhnout Garant k jejich jmenování. Z výše uvedeného je patrné, že nemůžou být doposud jmenováni Garanti ani jednoho z aktiv a tato role přechází na vlastníka aktiv, resp. jejich statutární zástupce, kterými jsou v případě obecního úřadu tajemník a v případě obce starosta.

Po vytvoření tohoto katalogu vedení obce, doposud bez existence Výboru pro kybernetickou bezpečnost, byla tato primární aktiva konzultována, posuzována a upravována. Všechna aktiva byla následně zaznamenána v nově vytvořené evidenci, včetně jejich podrobného slovního popisu.

13.2.2 Identifikace primárních aktiv

Při určování informačních aktiv předmětné obce bylo postupováno v souladu s dokumentem „Kybernetická bezpečnost obcí“ (dále také jako „KBO“), který vydal NÚKIB v souvislosti s novým zákonem o kybernetické bezpečnosti a jeho dopadem na obce s rozšířenou působností. (Kybernetická bezpečnost obcí, 2024)

Registr práv a povinností

Obec při určování informačních aktiv vychází z Registru práv a povinností (dále také jako „RPP“) dostupného na stránkách Digitální a informační agentury. Jsou zde evidovány veškeré agendy, které vykonávají nejen obce všech kategorií, ale i ostatní orgány veřejné moci. (Digitální a informační agentura, 2025)

Konkrétní aktuální příklady agend se nachází v přehledu dostupném na Rozcestníku vygenerovaných agend. Každá agenda zde má uvedeny vlastní činnosti, role, služby veřejné správy a další podrobnější údaje. (Digitální a informační agentura, 2025)

Z RPP byla provedena analýza všech agend, které tento registr obsahuje. Následně byly vybrány agendy, které předmětná obec vykonává, nebo je k jejich výkonu věcně a místně příslušná. Jedná se tedy o agendy, kde je příslušná obec I. kategorie, obec II. druhé kategorie, obec III. kategorie a agendy, k nimž jsou příslušné všechny orgány veřejné moci. Vzhledem k tomu, že je předmětná obec obcí s rozšířenou působností, tedy obcí s nejrozsáhlejším výkonem veřejné správy, přísluší jí výkon 140 agend z RPP.

Sdružování souvisejících agend do primárních aktiv

Jak bylo uvedeno v předchozí kapitole, předmětné obci přísluší 140 agend z RPP. S takto velkým množstvím agend by se kybernetická bezpečnost řešila velmi špatně. V metodice NÚKIB KBO je doporučeno, že pro lepší práci se získanými daty je možné více agend sdružit do větších celků, které potom budou představovat primární aktiva. Podmínkou takového sdružování je, že agendy spolu musí souviset věcně, procesně, organizačně a technicky. Pro příklad lze uvést, že např. agendy, které řeší odbor dopravy budou sloučeny do jedné agendy s názvem Doprava. Tímto způsobem byly rozděleny i všechny agendy předmětné obce, a to do celkem deseti primárních aktiv. Bližší rozdělení, včetně názvů pod agend a jejich kódů, je uvedeno v následujících tabulkách.

Identifikovaná primární aktiva

Tabulka 3 Primární aktiva obec a orgány obce

Obec a orgány obce		
Kód	Název agendy dle RPP	Aktivum ID
A343	Obecní zřízení (zákon o obcích)	PRA1
A388	Veřejné rozpočty	
A420	Obecní policie	
A561	Podpora regionálního rozvoje	
A572	Zajištění dopravní obslužnosti veřejnými službami v přepravě cestujících	
A1097	Krajské zřízení (zákon o krajích)	
A5104	Pravidla rozpočtové odpovědnosti	
A8334	Vydávání Sbírky zákonů a mezinárodních smluv a tvorba právních předpisů	

(zdroj: vlastní zpracování)

Tabulka 4 Primární aktiva správní činnosti

Správní činnosti		
Kód	Název agendy dle RPP	Aktivum ID
A44	Stanovení stálých volebních okrsků	PRA2
A46	Uzavírání manželství a určování otcovství	

Správní činnosti		
Kód	Název agendy dle RPP	Aktivum ID
A102	Základní registr - registr osob	
A113	Registrace agend a orgánů veřejné moci pro výkon agendy	
A115	Evidence obyvatel a rodná čísla	
A117	Občanské průkazy	
A118	Cestovní doklady občanů České republiky	
A345	Czech POINT - kontaktní místo veřejné správy	
A414	Matriky	
A483	Rejstřík trestů	
A687	Sčítání lidu, domů a bytů	
A688	Státní statistická služba	
A926	Agenda zákona o poštovních službách	
A1023	Státní občanství České republiky	
A1061	Ochrana utajovaných informací a bezpečnostní způsobilost	
A1086	Zdravotní služby	
A1095	Místní referendum	
A1133	Volba prezidenta republiky	
A1153	Správní řád	
A1155	Vydávání Sbírky zákonů a Sbírky mezinárodních smluv	
A1183	Volby do Parlamentu České republiky	
A1261	Poskytování informací (zákon č. 106/1999 Sb.)	
A1263	Státní kontrola	
A1281	Volby do zastupitelstev obcí	
A1282	Volby do zastupitelstev krajů	
A1301	O úřednicích územních samosprávných celků	
A1342	Ověřování (vidimace a legalizace)	
A1601	Krajské referendum	
A1661	Kontrolní řád	
A1921	Odpovědnost za škodu při výkonu veřejné moci	
A1941	Střet zájmů	
A7884	Dlouhodobé řízení informačních systémů veřejné správy	
A8567	Sbírka právních předpisů územních samosprávných celků a některých správních úřadů	
A10044	Ochrana utajovaných informací v informačních a komunikačních systémech	
A13711	Ochrana oznamovatelů	
A14633	Registr zastupování	

(zdroj: vlastní zpracování)

Tabulka 5 Primární aktiva krizové řízení a ochrana obyvatelstva

Krizové řízení a ochrana obyvatelstva		
Kód	Název agendy dle RPP	Aktivum ID
A51	Státní pomoc po živelní či jiné pohromě	PRA3
A337	O integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpisů	
A338	Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů	
A341	Požární ochrana	
A721	Povodňová ochrana v ČR	
A819	Nouzové zásoby ropy a řešení stavu ropné nouze	
A820	Působnost SSHR	
A821	Hospodářská opatření pro krizové stavy	
A1045	Vodovody a kanalizace pro veřejnou potřebu	
A1382	Nakládání s geneticky modifikovanými organismy a genetickými produkty	
A1441	Zajišťování obrany České republiky	
A3905	Atomový zákon	

(zdroj: vlastní zpracování)

Tabulka 6 Primární aktiva majetek obce

Majetek obce		
Kód	Název agendy dle RPP	Aktivum ID
A32	Pohřebnictví	PRA4
A372	Knihovní zákon	
A549	Péče o válečné hroby	
A1343	Archivnictví	
A1741	Majetkové vyrovnání s církvemi a náboženskými společnostmi	
A2106	Zákon o podpoře sportu	
A4067	Evidence skutečných majitelů	
A9145	Spisová služba	

(zdroj: vlastní zpracování)

Tabulka 7 Primární aktiva doprava

Doprava		
Kód	Název agendy dle RPP	Aktivum ID
A43	Pojištění odpovědnosti z provozu vozidla	PRA5
A998	Agenda o podmínkách provozu vozidel na pozemních komunikacích	

Doprava		
Kód	Název agendy dle RPP	Aktivum ID
A1042	Silniční doprava	
A1046	Agenda řidičů	
A1381	Pozemní komunikace a silniční správní úřady	

(zdroj: vlastní zpracování)

Tabulka 8 Primární aktiva výstavba

Výstavba		
Kód	Název agendy dle RPP	Aktivum ID
A123	Územní identifikace	PRA6
A560	Geologické práce	
A565	Územní plánování a stavební řád	
A565	Stavební řád	
A567	Vyvlastnění	
A569	Agenda speciálního stavebního úřadu	
A1045	Vodovody a kanalizace pro veřejnou potřebu	
A1163	Podpora rozvoje bydlení	
A1181	Zeměměřictví	
A6186	Územní plánování	
A14172	Stavební řád	

(zdroj: vlastní zpracování)

Tabulka 9 Primární aktiva životní prostředí

Životní prostředí		
Kód	Název agendy dle RPP	Aktivum ID
A32	Pohřebnictví	PRA7
A434	Památková péče	
A471	Přírodní léčivé zdroje a zdroje přírodních minerálních vod	
A943	Myslivost	
A944	Činnosti dle zákona o zemědělství	
A946	Státní správa rybářství	
A951	Reprodukční materiál lesních dřevin	
A963	Ochrana přírody a krajiny	
A967	Státní správa lesů	
A1044	Veterinární zákon	
A1089	Zákon o ochraně a využití nerostného bohatství (horní zákon)	
A1107	Zákon o těžebních odpadech	
A1126	Ochrana ovzduší	

Životní prostředí		
Kód	Název agendy dle RPP	Aktivum ID
A1162	Zákon o vodách	
A1182	Ochrana zvířat proti týrání	
A1186	Odpadové hospodářství	
A1221	Náhrady škod způsobených zvláště chráněnými živočichy	
A1283	Ochrana zemědělského půdního fondu	
A1384	Posuzování vlivů záměrů a koncepcí na životní prostředí EIA	
A1385	Předcházení ekologické újmy a EMAS	
A1422	Poskytování informací o životním prostředí	
A8595	Zákon o odpadech	
A9067	Zákon o výrobcích s ukončenou životností	
A15211	Jednotné environmentální stanovisko	

(zdroj: vlastní zpracování)

Tabulka 10 Primární aktiva finanční agenda

Finanční agenda		
Kód	Název agendy dle RPP	Aktivum ID
A42	Místní poplatky	PRA8
A121	Živnostenské podnikání	
A394	Finanční kontrola	
A397	Cenová regulace a kontrola	
A401	Odškodnění - restituční řízení	
A404	Provozování loterií a jiných podobných her	
A405	Správní poplatky	
A761	Omezení nočního provozu zastaváren (ŽÚ)	
A1021	Daně spravované celními orgány	
A1083	Ochrana spotřebitele (ŽÚ)	
A1092	Volný pohyb služeb (ŽÚ)	
A1115	Nakládání s bezpečnostním materiálem (ŽÚ)	
A1341	Zdravotní pojištění (ŽÚ)	
A1386	Cestovní ruch (ŽÚ)	
A1681	Povinné značení lihu (ŽÚ)	
A3082	Školský zákon	
A3082	Regionální školství	
A4877	Provozování činností pojišťoven a zajišťoven (ŽÚ)	
A7385	Agenda zákona o realitním zprostředkování (ŽÚ)	

(zdroj: vlastní zpracování)

Tabulka 11 Primární aktiva sociální oblast

Sociální oblast		
Kód	Název agendy dle RPP	Aktivum ID
A530	Sociální služby	PRA9
A1029	Sociální zabezpečení	
A1148	Pomoc v hmotné nouzi	
A1185	Sociálně-právní ochrana dětí	

(zdroj: vlastní zpracování)

Tabulka 12 Primární aktiva přestupky

Přestupky		
Kód	Název agendy dle RPP	Aktivum ID
A432	Autorské právo	PRA10
A822	Ochranné známky	
A824	Patenty	
A825	Užitné vzory	
A826	Průmyslové vzory	
A827	Topografie polovodičových výrobků	
A1094	Rostlinolékařská péče	
A1143	Vojenská policie	
A1149	Přestupkový zákon	
A1401	Provozování dráhy a provozování drážní dopravy	
A1722	Správa spotřebních daní	
A3787	Zákon o odpovědnosti za přestupky a řízení o nich	
A3791	Vysoké školy	

(zdroj: vlastní zpracování)

13.2.3 Hodnocení primárních aktiv

Dle VKB se hodnocení aktiv provádí na základě posouzení významnosti aktiva v kontextu dopadu porušení důvěrnosti, integrity a dostupnosti (zkráceně CIA - Confidentiality, Integrity, Availability).

Všechna aktiva jsou ohodnocena podle možného dopadu při:

- narušení důvěrnosti (neoprávněné vyzrazení),
- narušení integrity (neoprávněná změna),
- narušení dostupnosti, kde je samostatně hodnocen dopad v případě:

- úplného zničení aktiva (dále označováno pouze jako „ztráta“) a
- dočasné nedostupnosti (doba je daná SLA, v případě neexistence SLA je hranice dočasné nedostupnosti max. 1 týden); dolní hranice dočasné nedostupnosti aktiva pro stanovení dopadu se volí podle povahy aktiva.

V rámci této metodiky se za odpovídající bezpečnostní opatření, která podporují zachování integrity a důvěrnosti, považují i prvky jako auditovatelnost (účtovatelnost) nebo neodmítnutelnost (možnost přiřadit operace konkrétním subjektům). Pokud tyto prvky chybí, je jejich absence vnímána jako zranitelnost systému. (Svaz měst a obcí České republiky, 2023)

Vždy se hodnotí nejzávažnější realistický scénář dopadu, který může být způsoben narušením důvěrnosti, integrity nebo dostupnosti. Pro každý uvedený aspekt se vybírá nejvyšší relevantní hodnota podle příslušné tabulky, a to i v případě, že narušení bezpečnosti způsobí více následků najednou (např. současně finanční ztrátu i porušení právních předpisů). Při stanovování hodnoty aktiv se neberou v úvahu již zavedená bezpečnostní opatření, jako například dostupnost zálohovaných dat v případě selhání diskového pole. Tato opatření jsou zohledněna až v následujících fázích analýzy. (Metodika analýzy rizik (DPIA), 2018)

Tabulka dopadů umožňuje kategorizovat a hodnotit závažnost kybernetických hrozeb podle jejich potenciálního vlivu na organizaci. Každá hrozba je přiřazena číselné hodnotě od 1 až do 4, které odpovídají slovním hodnotám Nízký, Střední, Vysoký a Kritický.

Tabulka 13 Základní stupnice dopadů

Číselná hodnota	Slovní hodnota
1	Nízký
2	Střední
3	Vysoký
4	Kritický

(zdroj: vlastní zpracování)

Bylo provedeno samotné hodnocení aktiv dle CIA. Hodnotící kritéria byla navržena s využitím podpůrných materiálů poskytovaných NÚKIB. Každá analýza byla upravena dle specifických potřeb obce. V tabulkách níže je uvedeno hodnocení aktiv dle CIA. (Svaz měst a obcí ČR, 2023)

Tabulka 14 Hodnocení důvěrnosti

Úroveň		Popis
1	Nízká	Aktivum lze běžně zpřístupnit veřejnosti nebo je určeno k publikaci. Případné narušení důvěrnosti nemá dopad na zájmy či chod obce.
2	Střední	Aktivum není určeno k veřejnému šíření a má pro obec významnou hodnotu. Jeho ochranu ale přímo nevyžaduje zákon ani konkrétní smluvní podmínky.
3	Vysoká	Aktivum je neveřejné a musí být chráněno na základě právních norem, předpisů nebo smluvních závazků.
4	Kritická	Aktivum je neveřejné a vyžaduje mimořádnou úroveň ochrany, která přesahuje požadavky stanovené pro „Vysokou“ úroveň.

(zdroj: vlastní zpracování dle vzoru Svaz měst a obcí ČR, 2023)

Tabulka 15 Hodnocení integrity

Úroveň		Popis
1	Nízká	Aktivum nepotřebuje zvláštní ochranu integrity. Pokud by došlo k narušení integrity, zájmy obce tím nejsou negativně ovlivněny.
2	Střední	U aktiva může být nutné zajistit ochranu jeho integrity. Její narušení by mohlo ovlivnit zájmy obce a způsobit méně významné škody na hlavních aktivech.
3	Vysoká	Aktivum je nutné chránit před narušením integrity. Porušení integrity by poškodilo zájmy obce a způsobilo by značné negativní důsledky na hlavních aktivech.
4	Kritická	Aktivum vyžaduje mimořádnou ochranu integrity. Porušení integrity by vedlo k závažnému poškození zájmů obce s bezprostředními a zásadními důsledky na hlavní aktiva.

(zdroj: vlastní zpracování dle vzoru Svaz měst a obcí ČR, 2023)

Tabulka 16 Hodnocení dostupnosti

Úroveň		Popis
1	Nízká	Výpadek aktiva není kritický; případná delší nedostupnost (přibližně do jednoho týdne) nebo ztráta, nemá významný vliv na chod obce.
2	Střední	Přerušení dostupnosti aktiva by nemělo trvat déle než jeden pracovní den. Delší výpadek by mohl ohrozit řádné fungování obce.
3	Vysoká	Výpadek dostupnosti aktiva je třeba řešit v rámci několika hodin. I krátkodobá nedostupnost způsobuje přímé ohrožení důležitých funkcí a zájmů obce.
4	Kritická	Výpadek dostupnosti aktiva je nepřijatelný. I velmi krátký výpadek (v řádu minut) znamená závažné ohrožení základních funkcí a zájmů obce.

(zdroj: vlastní zpracování dle vzoru Svaz měst a obcí ČR, 2023)

Každé aktivum bylo hodnoceno prostřednictvím strukturovaných rozhovorů s vybranými pracovníky obce, kteří poskytovali odpovědi na otázky týkající se potenciálních dopadů v případě realizace nejzávažnějších možných scénářů. Jednalo se o zaměstnance obce, kteří byli zpravidla dobře obeznámeni s jednotlivými aktivy a schopní posoudit reálné důsledky případných incidentů. Při tomto průzkumu bylo využito vodítko v podobě dopadové tabulky, která je uvedena v metodickém materiálu Národního úřadu pro kybernetickou a informační bezpečnost. Tato tabulka sloužila jako pomocný nástroj k objektivnějšímu stanovení závažnosti dopadů a ke sjednocení přístupu při hodnocení různých typů aktiv. Výsledkem bylo konzistentní a transparentní ohodnocení všech aktiv v souladu s doporučenou metodikou a zvolenou strategií obce. (NÚKIB, 2018)

Podle katalogů jednotlivých aktiv, které jsou sestaveny a uvedeny v předchozí kapitole, bylo přistoupeno k jejich detailnímu zhodnocení. Jak již bylo zmíněno, samotné hodnocení bylo realizováno s využitím tzv. zjednodušené dopadové tabulky, která je uvedena v příloze 3 dokumentu Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti (dále také jako „PŘA“). Dopadová tabulka slouží jako praktická pomůcka umožňující systematicky a přehledně identifikovat a posoudit možné následky různých typů bezpečnostních hrozeb či incidentů na konkrétní aktiva. Prostřednictvím této tabulky je možné nejen klasifikovat závažnost případných dopadů, ale také usnadnit porovnání rizik mezi jednotlivými aktivy a sjednotit metodický přístup při jejich vyhodnocení. Pro lepší přehlednost je v příloze této diplomové práce vložen vzor zjednodušené varianty této tabulky shrnující základní informace pro rychlou orientaci v tématu. (NÚKIB, 2022, b)

Dle metodiky uvedené ve zmíněné příloze 3, je možné oblasti určené k hodnocení seskupit do kategorií podle jejich vzájemné blízkosti a míry překryvu. Účelem takového rozdělení je zjednodušit a urychlit proces hodnocení, zejména v situacích, kdy hranice mezi jednotlivými oblastmi nejsou zcela zřetelné. Přitom však nesmí dojít ke zhoršení kvality hodnocení primárních aktiv, ani k vynechání některé z důležitých oblastí. Kategorizace může být u každého řešeného subjektu odlišná, proto je vždy nezbytné, aby byla dopadová tabulka upravena konkrétním podmínkám a potřebám daného subjektu. V případě řešené obce byly všechny oblasti rozděleny do pěti kategorií, stejně jako v návrhu uvedeného v modelovém příkladu, pouze byly nepatrně upraveny jednotlivé kategorie tak, aby co nejvíce odpovídaly konkrétním podmínkám řešené předmětné obce.

Kategorie osobních údajů (VKB § 4 písm. a))

V rámci této kategorie se posuzuje rozsah a důležitost:

- osobních údajů s dopadem na dotčený subjekt, tedy nositele osobních údajů,
- finanční dopad na dotčený subjekt, nositele osobních údajů,
- zvláštních kategorií osobních údajů (např. zdravotní stav, sexuální život a orientaci atd.)

Kategorie povinností obce (VKB § 4 písm. a), b))

V rámci této kategorie se posuzuje rozsah dotčených:

- výkonů právních povinností daných zákonem nebo jiným legislativním dokumentem,
- zachovávání mlčenlivosti,
- trestně-právních řízení či občansko-právních, (např. trestání za přestupky)
- jiných, např. smluvních závazků (veřejno-právní smlouvy atd.).

Kategorie chodu obce (VKB § 4 písm. c), f), j))

V rámci této kategorie se posuzuje rozsah:

- narušení řídicích činností obce,
- narušení kontrolních činností obce,
- narušení běžných činností, (výkon samostatné a přenesené působnosti)
- dopadů na interní uživatele IS.

Kategorie image obce (VKB § 4 písm. d), g), i))

V rámci této kategorie se posuzují:

- veřejné zájmy, zájmy občanů a jiných dotčených subjektů,
- strategické a ekonomické zájmy,
- možné ekonomické ztráty,
- zachování dobré pověsti obce.

Kategorie core obce (VKB § 4 písm. e), h))

V rámci této kategorie se posuzují dopady na:

- poskytování důležitých služeb, (např. sociální služby)
- bezpečnost a zdraví osob, (např. krizové stavy na území obce)
- zainteresované strany (jiné orgány veřejné správy).

(NÚKIB, 2022, b)

Tyto přizpůsobené kategorie dopadů byly použity pro sestavení jednotlivých jednoduchých dopadových tabulek, ze kterých bylo prováděno hodnocení jednotlivých primárních rizik řešené obce. Vypracované tabulky hodnocení primárních aktiv jsou zobrazeny následně.

Tabulka 17 Hodnocení primárního aktiva PRA 1 Obec a orgány obce

Název primárního aktiva:	PRA1 Obec a orgány obce																		
Gestor primárního aktiva:	pracovník KŘ																		
Garant primárního aktiva:	starosta																		
Datum hodnocení:	23.03.2025																		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	2																	
	Ztráta	3																	
	Důvěrnost	2																	
	Integrita	3																	
Oblasti dopadu	Dostupnost						Ztráta							Důvěrnost			Integrita		
	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	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)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
Kategorie osobních údajů	1	2	2	2	2	2	2	2	2	2	2	3	3	3	2	2	2	2	3
Kategorie povinností obce	1	1	1	2	2	2	1	1	1	1	3	3	3	3	1	1	2	2	3
Kategorie chodu obce	1	1	2	2	2	2	1	1	1	1	2	3	3	3	1	1	2	2	3
Kategorie image obce	2	2	2	2	2	2	1	1	1	1	2	2	3	3	2	2	2	2	2
Kategorie core obce	1	1	1	2	2	2	1	1	1	1	3	3	3	3	1	1	2	2	3

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 18 Hodnocení primárního aktiva PRA 2 Správní činnosti

Název primárního aktiva:	PRA2 Správní činnosti																		
Gestor primárního aktiva:	pracovník KŘ																		
Garant primárního aktiva:	tajemník																		
Datum hodnocení:	23.03.2025																		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	3																	
	Ztráta	4																	
	Důvěrnost	4																	
	Integrita	3																	
Oblasti dopadu	Dostupnost						Ztráta							Důvěrnost			Integrita		
	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	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)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
Kategorie osobních údajů	1	2	3	3	3	3	2	2	3	3	3	4	4	4	2	2	4	2	3
Kategorie povinností obce	1	2	2	2	2	3	1	1	2	2	3	4	4	3	1	1	3	2	3
Kategorie chodu obce	1	3	3	3	3	3	1	1	2	2	3	3	3	3	1	1	3	2	3
Kategorie image obce	2	2	2	2	2	3	1	1	1	2	2	3	3	3	2	2	3	2	2
Kategorie core obce	1	2	3	3	3	3	1	2	2	2	2	3	3	4	1	2	3	2	3

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 19 Hodnocení primárního aktiva PRA 3 Krizové řízení a ochrana obyvatelstva

Název primárního aktiva:	PRA3 Krizové řízení a ochrana obyvatelstva																		
Gestor primárního aktiva:	pracovník KŘ																		
Garant primárního aktiva:	tajemník																		
Datum hodnocení:	23.03.2025																		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	4																	
	Ztráta	4																	
	Důvěrnost	4																	
	Integrita	4																	
Oblasti dopadu	Dostupnost						Ztráta								Důvěrnost			Integrita	
	Nedostupnost 1 h						Ztráta dat od zálohy (15 min)										Prozrazení v rámci organizace		
	Nedostupnost 4 h						Ztráta dat od zálohy (1 h)										Prozrazení smluvním partnerům		
	Nedostupnost 8 h						Ztráta dat od zálohy (4 h)										Prozrazení vně organizaci		
	Nedostupnost 1 den						Ztráta dat od zálohy (8 h)												
	Nedostupnost 2 dny						Ztráta dat od zálohy (1 den)												
	Nedostupnost 1 týden						Ztráta dat od zálohy (2 dny)												
							Ztráta dat od zálohy (1 týden)												
							Úplná ztráta dat												
Kategorie osobních údajů	3	4	4	4	4	4	2	3	4	4	4	4	4	4	4	3	4	4	3
Kategorie povinností obce	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	3
Kategorie chodu obce	3	4	4	4	4	4	3	3	3	4	4	4	4	4	4	4	4	4	3
Kategorie image obce	2	3	3	3	3	3	3	3	3	3	3	3	3	3	4	3	2	3	2
Kategorie core obce	2	2	3	3	3	3	4	4	4	4	4	4	4	4	4	2	3	4	3

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 20 Hodnocení primárního aktiva PRA 4 Majetek obce

Název primárního aktiva:	PRA4 Majetek obce																		
Gestor primárního aktiva:	pracovník KŘ																		
Garant primárního aktiva:	starosta																		
Datum hodnocení:	23.03.2025																		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	2																	
	Ztráta	3																	
	Důvěrnost	2																	
	Integrita	3																	
Oblasti dopadu	Dostupnost						Ztráta								Důvěrnost			Integrita	
	Nedostupnost 1 h						Ztráta dat od zálohy (15 min)									Prozrazení v rámci organizace			
	Nedostupnost 4 h						Ztráta dat od zálohy (1 h)									Prozrazení smluvním partnerům			
	Nedostupnost 8 h						Ztráta dat od zálohy (4 h)									Prozrazení vně organizaci			
	Nedostupnost 1 den						Ztráta dat od zálohy (8 h)									Modifikace dat malého rozsahu			
	Nedostupnost 2 dny						Ztráta dat od zálohy (1 den)									Modifikace dat velkého rozsahu			
	Nedostupnost 1 týden						Ztráta dat od zálohy (2 dny)												
							Ztráta dat od zálohy (1 týden)												
							Úplná ztráta dat												
							Prozrazení v rámci organizace												
Kategorie osobních údajů	1	1	1	2	2	2	1	1	2	2	2	3	3	3	1	1	2	1	3
Kategorie povinností obce	1	1	1	1	2	2	1	1	2	2	2	2	2	3	1	1	2	1	3
Kategorie chodu obce	1	1	1	1	1	2	1	1	2	2	2	2	2	3	1	1	2	1	3
Kategorie image obce	1	1	1	1	1	1	1	1	1	1	1	2	2	3	1	1	2	1	2
Kategorie core obce	1	1	1	1	1	2	1	1	1	1	1	2	2	3	1	1	2	1	2

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 21 Hodnocení primárního aktiva PRA 5 Doprava

Název primárního aktiva:	PRA5 Doprava																		
Gestor primárního aktiva:	pracovník KŘ																		
Garant primárního aktiva:	tajemník																		
Datum hodnocení:	23.03.2025																		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	2																	
	Ztráta	3																	
	Důvěrnost	2																	
	Integrita	3																	
Oblasti dopadu	Dostupnost						Ztráta							Důvěrnost			Integrita		
	Nedostupnost 1 h						Ztráta dat od zálohy (15 min)								Prozrazení v rámci organizace			Modifikace dat malého rozsahu	
	Nedostupnost 4 h						Ztráta dat od zálohy (1 h)								Prozrazení smluvním partnerům			Modifikace dat velkého rozsahu	
	Nedostupnost 8 h						Ztráta dat od zálohy (4 h)								Prozrazení vně organizaci				
	Nedostupnost 1 den						Ztráta dat od zálohy (8 h)												
	Nedostupnost 2 dny						Ztráta dat od zálohy (1 den)												
	Nedostupnost 1 týden						Ztráta dat od zálohy (2 dny)												
							Ztráta dat od zálohy (1 týden)												
							Úplná ztráta dat												
Kategorie osobních údajů	1	1	1	2	2	2	1	1	2	2	2	2	2	3	1	2	2	2	3
Kategorie povinností obce	1	1	1	2	2	2	1	1	2	2	2	2	2	3	1	2	2	2	3
Kategorie chodu obce	1	1	2	2	2	2	1	1	2	2	2	2	2	3	1	1	2	2	3
Kategorie image obce	1	1	2	2	2	2	1	1	1	1	2	2	2	2	1	1	2	2	2
Kategorie core obce	1	1	1	2	2	2	1	1	1	1	2	2	2	2	1	2	2	2	3

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 22 Hodnocení primárního aktiva PRA 6 Výstavba

Název primárního aktiva:	PRA6 Výstavba																		
Gestor primárního aktiva:	pracovník KŘ																		
Garant primárního aktiva:	tajemník																		
Datum hodnocení:	23.03.2025																		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	3																	
	Ztráta	4																	
	Důvěrnost	2																	
	Integrita	3																	
Oblasti dopadu	Dostupnost						Ztráta							Důvěrnost			Integrita		
	Nedostupnost 1 h						Ztráta dat od zálohy (15 min)								Prozrazení v rámci organizace			Modifikace dat malého rozsahu	
	Nedostupnost 4 h						Ztráta dat od zálohy (1 h)								Prozrazení smluvním partnerům			Modifikace dat velkého rozsahu	
	Nedostupnost 8 h						Ztráta dat od zálohy (4 h)								Prozrazení vně organizaci				
	Nedostupnost 1 den						Ztráta dat od zálohy (8 h)												
	Nedostupnost 2 dny						Ztráta dat od zálohy (1 den)												
	Nedostupnost 1 týden						Ztráta dat od zálohy (2 dny)												
							Ztráta dat od zálohy (1 týden)												
							Úplná ztráta dat												
Kategorie osobních údajů	1	1	2	2	2	3	1	1	2	3	3	4	4	4	1	2	2	2	3
Kategorie povinností obce	1	1	2	2	2	3	1	1	2	2	3	3	4	4	1	2	2	2	3
Kategorie chodu obce	1	1	2	2	2	3	1	1	2	2	3	3	3	4	1	2	2	2	3
Kategorie image obce	1	1	2	2	2	2	1	1	2	2	2	2	3	3	1	2	2	2	3
Kategorie core obce	1	1	2	3	3	3	1	2	2	3	3	3	4	4	1	1	2	2	3

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 23 Hodnocení primárního aktiva PRA 7 Životní prostředí

Název primárního aktiva:	PRA7 Životní prostředí																			
Gestor primárního aktiva:	pracovník KŘ																			
Garant primárního aktiva:	tajemník																			
Datum hodnocení:	23.03.2025																			
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	3																		
	Ztráta	3																		
	Důvěrnost	2																		
	Integrita	3																		
Oblasti dopadu	Dostupnost						Ztráta								Důvěrnost			Integrita		
	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	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)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizací	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu	
Kategorie osobních údajů	1	1	1	2	3	3	1	1	2	2	3	3	3	3	1	2	2	2	3	
Kategorie povinností obce	1	1	1	2	2	3	1	1	2	2	2	2	2	3	1	2	2	2	3	
Kategorie chodu obce	1	1	2	2	3	3	1	1	2	2	2	3	3	3	1	1	2	2	3	
Kategorie image obce	1	1	2	2	2	2	1	1	1	1	2	2	2	2	1	1	2	2	2	
Kategorie core obce	1	1	1	2	2	3	1	1	1	1	2	2	2	3	1	2	2	2	3	

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 24 Hodnocení primárního aktiva PRA 8 Finanční agenda

Název primárního aktiva:	PRA8 Finanční agenda																		
Gestor primárního aktiva:	pracovník KŘ																		
Garant primárního aktiva:	tajemník																		
Datum hodnocení:	23.03.2025																		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	3																	
	Ztráta	4																	
	Důvěrnost	4																	
	Integrita	4																	
Oblasti dopadu	Dostupnost						Ztráta								Důvěrnost			Integrita	
	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	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)	Úplná ztráta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizací	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
Kategorie osobních údajů	2	3	3	3	3	3	2	3	3	3	4	4	4	4	3	4	4	3	4
Kategorie povinností obce	2	3	3	3	3	3	2	3	3	3	4	4	4	4	3	3	3	3	4
Kategorie chodu obce	2	2	3	3	3	3	2	3	3	3	4	4	4	4	3	3	3	3	4
Kategorie image obce	1	1	2	3	3	3	2	2	2	2	3	3	3	3	3	3	3	3	3
Kategorie core obce	2	2	3	3	3	3	2	2	3	3	4	4	4	4	3	3	4	3	4

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 25 Hodnocení primárního aktiva PRA 9 Sociální služby

Název primárního aktiva:	PRA9 Sociální služby																			
Gestor primárního aktiva:	pracovník KŘ																			
Garant primárního aktiva:	tajemník																			
Datum hodnocení:	23.03.2025																			
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	3																		
	Zrůta	3																		
	Důvěrnost	3																		
	Integrita	3																		
Oblasti dopadu	Dostupnost						Zrůta							Důvěrnost			Integrita			
	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	Zrůta dat od zálohy (15 min)	Zrůta dat od zálohy (1 h)	Zrůta dat od zálohy (4 h)	Zrůta dat od zálohy (8 h)	Zrůta dat od zálohy (1 den)	Zrůta dat od zálohy (2 dny)	Zrůta dat od zálohy (1 týden)	Úplná zřůta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu	
Kategorie osobních údajů	1	1	2	2	3	3	2	3	3	3	3	3	4	4	2	3	4	2	3	
Kategorie povinností obce	1	1	2	2	3	3	1	1	2	2	3	3	4	4	2	3	4	2	3	
Kategorie chodu obce	1	1	2	2	3	3	1	1	1	1	1	2	2	3	2	3	3	2	3	
Kategorie image obce	1	1	2	2	3	3	1	2	2	2	2	2	2	3	2	3	3	2	3	
Kategorie core obce	1	2	2	3	4	4	1	1	1	2	2	2	3	4	2	3	4	2	3	

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 26 Hodnocení primárního aktiva PRA 10 Přestupky

Název primárního aktiva:	PRA10 Přestupky																		
Gestor primárního aktiva:	pracovník KŘ																		
Garant primárního aktiva:	tajemník																		
Datum hodnocení:	23.03.2025																		
Výsledné hodnocení primárního aktiva (nejvyšší hodnoty jednotlivých atributů)	Dostupnost	3																	
	Zrůta	3																	
	Důvěrnost	3																	
	Integrita	3																	
Oblasti dopadu	Dostupnost						Zrůta							Důvěrnost			Integrita		
	Nedostupnost 1 h	Nedostupnost 4 h	Nedostupnost 8 h	Nedostupnost 1 den	Nedostupnost 2 dny	Nedostupnost 1 týden	Zrůta dat od zálohy (15 min)	Zrůta dat od zálohy (1 h)	Zrůta dat od zálohy (4 h)	Zrůta dat od zálohy (8 h)	Zrůta dat od zálohy (1 den)	Zrůta dat od zálohy (2 dny)	Zrůta dat od zálohy (1 týden)	Úplná zřůta dat	Prozrazení v rámci organizace	Prozrazení smluvním partnerům	Prozrazení vně organizaci	Modifikace dat malého rozsahu	Modifikace dat velkého rozsahu
Kategorie osobních údajů	1	1	1	2	2	3	1	2	2	2	3	3	3	3	1	1	3	2	3
Kategorie povinností obce	1	1	1	2	2	2	1	1	1	1	2	2	2	3	1	1	2	2	3
Kategorie chodu obce	1	1	1	2	2	2	1	1	1	1	2	2	2	2	1	1	2	2	3
Kategorie image obce	1	1	1	1	1	1	1	1	1	1	2	2	2	2	1	1	1	2	3
Kategorie core obce	1	1	1	2	2	2	1	1	1	1	2	2	2	2	1	1	3	2	3

(zdroj: vlastní zpracování dle vzoru PŘA)

Tabulka 27 Katalog primárních aktiv s ohodnocením dle CIA

KATALOG PRIMÁRNÍCH AKTIV												
ID	Primární aktiva	Specifikace	Kategorie	Gestor	Garant	Osobní údaj	Určený IS	ISMS	Dostupnost A	Ztráta L	Důvěrnost C	Integrita I
PRA1	Obec a orgány obce	Výkon samostatné působnosti obce	služba	pracovník KŘ	starosta	ano	ano	ano	2	3	2	3
PRA2	Správní činnosti	Výkon samostatné i přenesené působnosti obce	služba	pracovník KŘ	tajemník	ano	ano	ano	3	4	4	3
PRA3	Krizové řízení a ochrana obyv.	Výkon přenesené působnosti ve věcech KZ a OO	služba	pracovník KŘ	tajemník	ano	ano	ano	4	4	4	4
PRA4	Majetek obce	Správa a péče o majetek obce	služba	pracovník KŘ	starosta	ano	ano	ano	2	3	2	3
PRA5	Doprava	Výkon přenesené působnosti ve věcech dopravy	služba	pracovník KŘ	tajemník	ano	ano	ano	2	3	2	3
PRA6	Výstavba	Výkon přenesené působnosti ve věcech výstavby	služba	pracovník KŘ	tajemník	ano	ano	ano	3	4	2	3
PRA7	Životní prostředí	Výkon samostatné i přenesené působnosti v oblasti ŽP	služba	pracovník KŘ	tajemník	ano	ano	ano	3	3	2	3
PRA8	Finanční agenda	Výkon samostatné i přenesené působnosti v oblasti financí	služba	pracovník KŘ	tajemník	ano	ano	ano	3	4	4	4
PRA9	Sociální služby	Výkon samostatné i přenesené působnosti v sociální oblasti	služba	pracovník KŘ	tajemník	ano	ano	ano	4	4	4	3
PRA10	Přestupky	Výkon samostatné i přenesené působnosti v přestupkové oblasti	služba	pracovník KŘ	tajemník	ano	ano	ano	3	3	3	3

(zdroj: vlastní zpracování)

Primární aktiva obce byla hodnocena z pohledu základních principů bezpečnosti informací – dostupnosti A, ztráty L, důvěrnosti C a integrity I. Z provedené analýzy vyplývá, že nejkritičtějšími aktivy z hlediska všech čtyř složek jsou zejména „Krizové řízení a ochrana obyvatelstva“ (PRA3), „Finanční agenda“ (PRA8) a „Sociální služby“ (PRA9), která byla ohodnocena nejvyššími hodnotami 4 ve čtyřech a třech kategoriích CIA-L. Další kritickou kategorií je aktivum (PRA2) „Správní činnosti“, které dosáhlo nejvyšších hodnot 4 ve dvou kategoriích. Tato aktiva zahrnují vysokou důležitost pro funkci obce, jsou určena pro fungování společnosti, zajištění jejich základní a nezbytných potřeb a mají zásadní význam pro plynulý chod veřejné správy, a tedy i pro bezpečnostní a provozní stabilitu obce a jejich obyvatel.

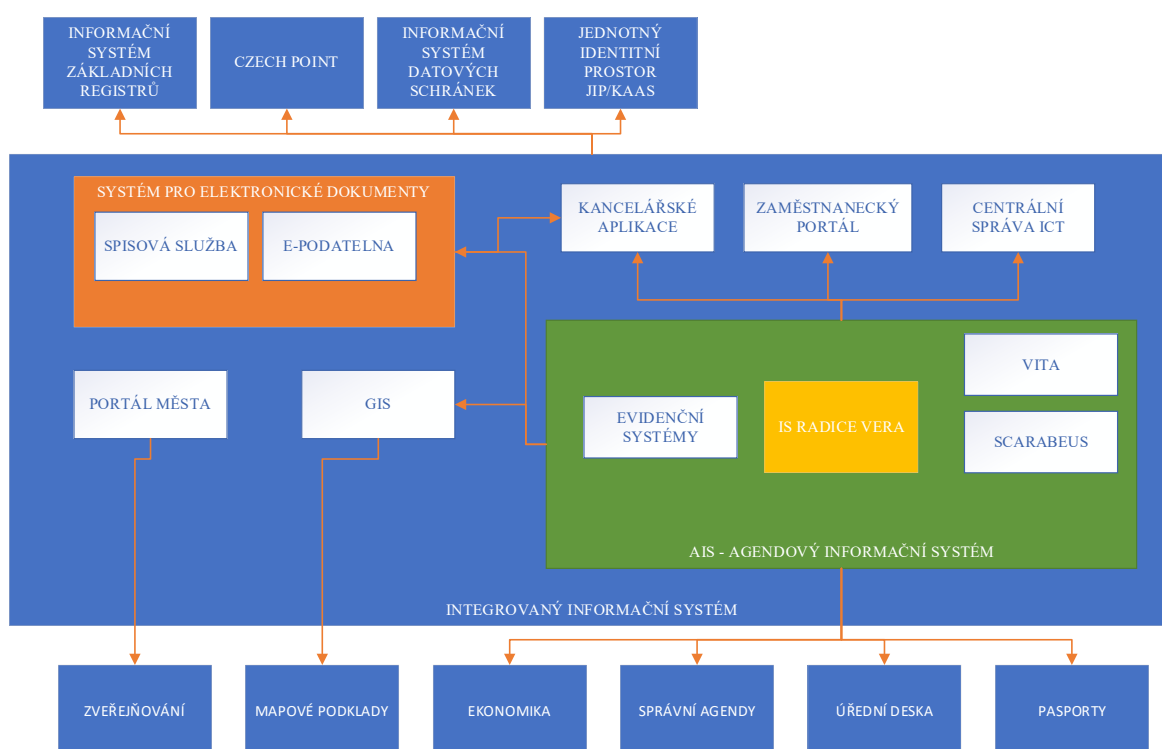
Naopak aktiva jako „Výstavba“ (PRA6), „Životní prostředí“ (PRA7) a „Doprava“ (PRA5) vykazují mírně nižší hodnoty, zejména v oblasti důvěrnosti, což odpovídá jejich menší citlivosti zpracovávaných dat, ale stále vyžadují pečlivé řízení dostupnosti a integrity údajů. Nejnižší hodnoty důvěrnosti 2 byly přiděleny u více aktiv, což odráží nižší citlivost informací, které jsou v těchto oblastech zpracovávány.

Hodnocení vychází z posouzení dopadu ztráty jednotlivých aspektů na činnost obce a je důležitým vstupem pro stanovení priorit při zavádění opatření.

13.2.4 Identifikace podpůrných aktiv

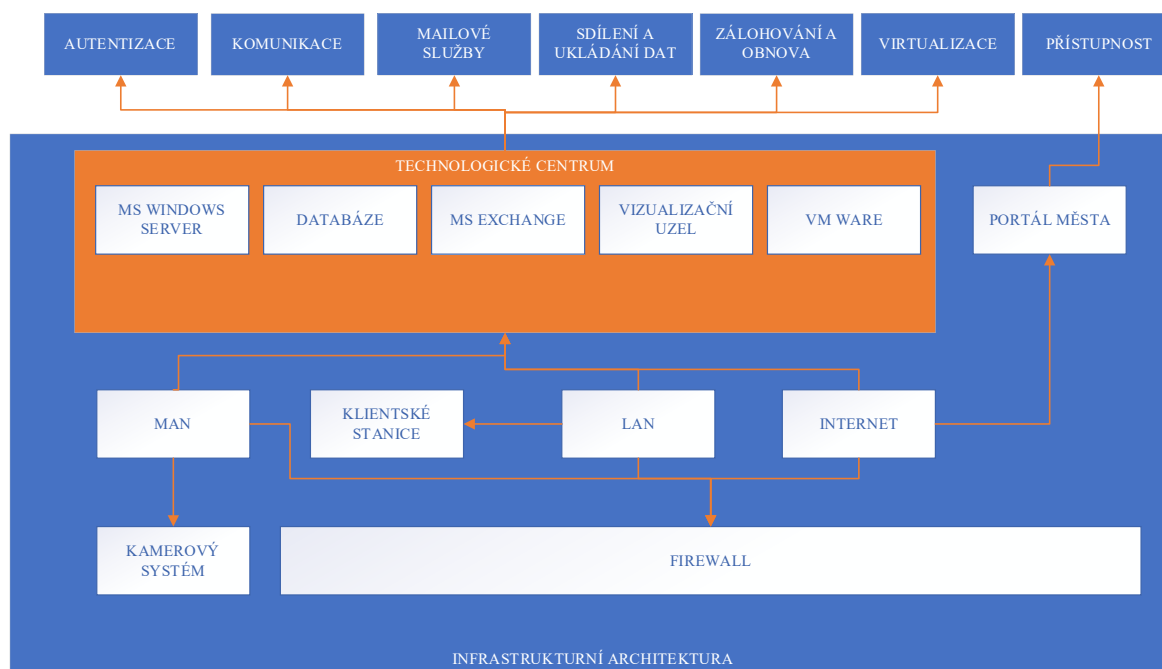
Podpůrná aktiva jsou přímo vázána na primární aktiva. Zabezpečují jejich funkčnost, podporu, dostupnost, ale i bezpečnost. Podpůrnými aktivy jsou například zaměstnanci, dodavatelé, hardware, software, budovy nebo jiné prostory, ve kterých jsou umístěna primární aktiva, tedy aktiva potřebná k zajištění výkonu jednotlivých agend obce. Podpůrná aktiva je vhodné evidovat vždy v návaznosti na primární aktiva, ke kterým se vztahují. Tato evidence může být prováděna i skupinově, a to podle typu aktiv. Při počátečním definování rozsahu systému řízení bezpečnosti není vždy nutné zaznamenávat každé jednotlivé podpůrné aktivum samostatně. Například není třeba evidovat každý konkrétní počítač, jednotlivého zaměstnance nebo aplikaci zvlášť, pokud je vůči nim plánováno uplatňování stejných nebo obdobných opatření.

Obec má poměrně velmi dobře zpracovanou technickou dokumentaci ke všem svým informačním systémům. Rovněž je dobře zdokumentována topologie aplikační i technologické infrastruktury. Pro lepší přehlednost byly zpracovány schémata obou zmíněných infrastruktur.



Obrázek 10 Stav aplikační vrstvy

(zdroj: vlastní zpracování dle podkladů obce)



Obrázek 11 Stav technologická vrstva

(zdroj: vlastní zpracování dle podkladů obce)

Podobně jako u primárních aktiv, je možné i podpůrná aktiva sdružovat do tzv. typových skupin, a to na základě jejich vzájemné souvislosti, ať už věcné, procesní, organizační nebo technické.

V případě předmětné obce byl zvolen postup, kdy byly určeny jednotlivé kategorie, následně skupiny a k nim byla přidružena, analýzou získaná, typová aktiva. Při identifikaci podpůrných aktiv bylo čerpáno z této dokumentace a následně byla doplněna aktiva z ostatních kategorií na základě rozhovorů s pracovníky IT. S pracovníky IT oddělení bylo rovněž provedeno ohodnocení jednotlivých podpůrných aktiv dle tabulky Váhy vlivu, jenž je součástí metodiky NUKIB - PŘA. K tomuto hodnocení bylo přistoupeno již při samotné identifikaci podpůrných aktiv pro lepší přehlednost. Kompletní tabula Váhy vlivu i s popisem hodnotících kritérií je uvedena v následující kapitole Hodnocení podpůrných aktiv. Pro hodnocení podpůrných aktiv byla použita hodnotící stupnice se čtyřmi úrovněmi 1 - 4, přičemž při určování hodnoty těchto aktiv byl zvažován nejhorší možný scénář bez ohledu na existující bezpečnostní opatření.

Tabulka 28 Identifikace podpůrných aktiv a jejich hodnocení dle váhy vlivu

Podpůrná aktiva PPA				Hodnocení PPA dle váhy vlivu			
Kategorie	Skupina	Typové aktivum	PPA ID				
Software (SW)	Systémový	OS MS Windows server	PPA 1	3	1	3	2
		OS Základní (Windows, macOS, Apple, Android)	PPA 2	2	2	1	3
		OS MS Exchange (pošta)	PPA 3	3	2	2	3
		Virtualizační SW	PPA 4	2	1	2	3
	Bezpečnostní	Antivir ESET NOD32	PPA 5	2	3	3	3
		Síťové DLP	PPA 6	2	3	3	3
	Aplikační	Kancelářský SW (MS Office, Adobe atd.)	PPA 7	2	1	2	3
		Radnice VERA (základní aplikace, ekonomika, spisy, pošta)	PPA 8	3	2	1	3
		Agendový SW (VITA, SCARABEUS atd.)	PPA 9	2	2	1	3
		Mzdy a docházka KVASAR PERM, Power Key 3.0	PPA 10	1	1	1	3
Hardware (HW)	Pracovní stanice	Stolní počítač, Terminál	PPA 11	1	3	2	3
	Mobilní zař.	Notebook, Mobilní telefon, Tablet	PPA 12	1	3	3	3
	Servery	Servery – fyzické i virtuální	PPA 13	3	2	2	3
	Datová úložiště	Diskové pole (RAID), NAS zařízení	PPA 14	2	3	2	3
	Ostatní	Tiskárny, skenery, platební terminál	PPA 15	1	1	1	2
		Výměnná média	PPA 16	2	3	3	3
		Docházkový terminál WP9S-1EM	PPA 17	1	1	2	2
Komunik. prostředky (KP)	Kom. sítě	Internetové připojení, MAN, KIVS	PPA 18	2	1	3	3
	Síťová zařízení	HW firewall	PPA 19	3	2	2	3
		LAN a SAN switche	PPA 20	3	2	2	3
		WiFi Access Point	PPA 21	2	2	2	2
		Strukturovaná kabeláž, rozvaděče, datové zásuvky	PPA 22	3	2	2	3
Objekty (OB)	Budovy OÚ	Kanceláře	PPA 23	3	3	3	3
		Serverovny	PPA 24	3	3	3	3
Lidské zdroje (LZ)		Vedení obce	PPA 25	2	3	4	3
		IT pracovníci	PPA 26	3	4	3	3
		Úředníci	PPA 27	1	1	3	3
		Ostatní zaměstnanci	PPA 28	1	1	2	2

(zdroj: vlastní zpracování)

13.2.5 Hodnocení podpůrných aktiv

Při hodnocení podpůrných aktiv je třeba zajistit maximální soulad s hodnocením primárních aktiv. Podobně jako u primárních aktiv je nutné i u podpůrných aktiv posoudit dopady případného narušení bezpečnosti informací, přičemž je třeba hodnotit minimálně dopady na důvěrnost, integritu a dostupnost informací. V rámci hodnocení dostupnosti je možné, stejně jako u hodnocení primárních aktiv, rozlišit mezi dočasnou nedostupností a trvalou ztrátou dat. Dle metodiky NÚKIB - PŘA se doporučuje použít hodnotící stupnici se čtyřmi

úrovněmi, přičemž při určování hodnoty aktiv by měl být zvažován nejhorší možný scénář bez ohledu na existující bezpečnostní opatření. Při tomto procesu je rovněž důležité vzít v potaz vzájemnou provázanost podpůrných a primárních aktiv.

Existuje několik možných způsobů, jak tuto provázanost hodnotit:

- Podpůrná aktiva dědí hodnoty primárních aktiv (nejméně přesné)
- Podpůrná aktiva jsou posuzována individuálně s ohledem na hodnotu primárních aktiv
- Podpůrná aktiva přebírají hodnoty primárních aktiv prostřednictvím vzorce

Pro hodnocení podpůrných aktiv byl zvolen postup, kdy jsou jednotlivá aktiva ohodnocena vahou vlivu předem daných podmínek a následně došlo výpočtu hodnoty aktiva podle daného vzorce.

Pro stanovení hodnot váhy vlivu byla použita tabulka uvedená v metodickém dokumentu NÚKIB - PŘA. Hodnoty váhy v rozmezí 1 - 4 byly ponechány, neboť pro dané hodnocení podpůrných aktiv jsou dostačující.

Tabulka 29 Váha vlivu (dále jako „VV“)

VÁHA Vlivu		
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.

(zdroj: vlastní zpracování dle vzoru PŘA)

Hodnota podpůrného aktiva byla vypočítána podle vzorce:

$$\text{HODNOTA PPA} = \text{HODNOTA VV} \times \text{HODNOTA PRA}$$

Pro lepší přehlednost a snadnější výpočet hodnot PPA, byla podle výše uvedeného vzorce vytvořena následující tabulka. Tabulka obsahuje jednotlivá identifikovaná primární aktiva PRA 1-10. Hodnoty byly převzaty z tabulky 27, Katalog primárních aktiv, vytvořené v kapitole 13.2.3., s ohodnocením dle CIA-L, tedy dostupnosti A, ztráty L, důvěrnosti C a integrity I. Jednotlivé hodnoty PRA byly vynásobeny vahou vlivu, která byla stanovena v

tabulce 28, Identifikace podpůrných aktiv a jejich hodnocení dle váhy vlivu. Výsledkem tohoto výpočtu je sloupec s uvedením maximálních hodnot podpůrných aktiv.

Tabulka 30 Hodnoty podpůrných aktiv, výpočet dle vzorce

Hodnoty podpůrných aktiv podle váhy vlivu			Maximální hodnota podpůrného aktiva	Primární aktiva																																										
				PRA1			PRA2			PRA3			PRA4			PRA5			PRA6			PRA7			PRA8			PRA9			PRA10															
				Služba			Služba			Služba			Služba			Služba			Služba			Služba			Služba			Služba			Služba															
				A	L	C	I	A	L	C	I	A	L	C	I	A	L	C	I	A	L	C	I	A	L	C	I	A	L	C	I	A	L	C	I	A	L	C	I							
Podpůrná aktiva	PPA1	OS Windows	12	4	12	8	6	3	6	6	9	4	9	6	12	4	12	8	6	3	6	6	6	3	6	6	9	4	6	6	9	3	6	6	9	4	12	8	12	4	12	6	9	3	9	6
	PPA2	OS Základní	8	8	4	12	4	6	2	9	6	8	3	9	8	8	4	12	4	6	2	9	4	6	2	9	6	8	2	9	6	6	2	9	6	8	4	12	8	8	4	9	6	6	3	9
	PPA3	OS Exchange	12	8	8	12	6	6	4	9	9	8	6	9	12	8	8	12	6	6	4	9	6	6	4	9	9	8	4	9	9	6	4	9	9	8	8	12	12	8	8	9	9	6	6	9
	PPA4	Vizuálizace	8	4	8	12	4	3	4	9	6	4	6	9	8	4	8	12	4	3	4	9	4	3	4	9	6	4	4	9	6	3	4	9	6	4	8	12	8	4	8	9	6	3	6	9
	PPA5	Antivir	8	12	12	12	4	9	6	9	6	12	9	9	8	12	12	12	4	9	6	9	4	9	6	9	6	12	6	9	6	9	6	9	6	12	12	12	8	12	12	9	6	9	9	9
	PPA6	Síťové TLP	8	12	12	12	4	9	6	9	6	12	9	9	8	12	12	12	4	9	6	9	4	9	6	9	6	12	6	9	6	9	6	9	6	12	12	12	8	12	12	9	6	9	9	9
	PPA7	Kancelářský	8	4	8	12	4	3	4	9	6	4	6	9	8	4	8	12	4	3	4	9	4	3	4	9	6	4	4	9	6	3	4	9	6	4	8	12	8	4	8	9	6	3	6	9
	PPA8	Rad. VERA	12	8	4	12	6	6	2	9	9	8	3	9	12	8	4	12	6	6	2	9	6	6	2	9	9	8	2	9	9	6	2	9	9	8	4	12	12	8	4	9	9	6	3	9
	PPA9	Agendový	8	8	4	12	4	6	2	9	6	8	3	9	8	8	4	12	4	6	2	9	4	6	2	9	6	8	2	9	6	6	2	9	6	8	4	12	8	8	4	9	6	6	3	9
	PPA10	Pers. KVAS.	4	4	4	12	2	3	2	9	3	4	3	9	4	4	4	12	2	3	2	9	2	3	2	9	3	4	2	9	3	3	2	9	3	4	4	12	4	4	9	3	6	3	3	9
	PPA11	Prac. st.	4	12	8	12	2	9	4	9	3	12	6	9	4	12	8	12	2	9	4	9	2	9	4	9	3	12	4	9	3	9	4	9	3	12	8	12	4	12	8	9	3	9	6	9
	PPA12	Mob. zař.	4	12	12	12	2	9	6	9	3	12	9	9	4	12	12	12	2	9	6	9	2	9	6	9	3	12	6	9	3	9	6	9	3	12	12	12	4	12	12	9	3	9	9	9
	PPA13	Fyz. serv.	12	8	8	12	6	6	4	9	9	8	6	9	12	8	8	12	6	6	4	9	6	6	4	9	9	8	4	9	9	6	4	9	9	8	8	12	12	8	8	9	9	6	6	9
	PPA14	Dat. úlož.	8	12	8	12	4	9	4	9	6	12	6	9	8	12	8	12	4	9	4	9	4	9	4	9	6	12	4	9	6	9	4	9	6	12	8	12	8	12	8	9	6	9	6	9
	PPA15	Tiskárny	4	4	4	8	2	3	2	6	3	4	3	6	4	4	4	8	2	3	2	6	2	3	2	6	3	4	2	6	3	3	2	6	3	4	4	8	4	4	6	3	3	3	6	
	PPA16	Výměn. m.	8	12	12	12	4	9	6	9	6	12	9	9	8	12	12	12	4	9	6	9	4	9	6	9	6	12	6	9	6	9	6	9	6	12	12	12	8	12	12	9	6	9	9	9
	PPA17	Docház. ter	4	4	8	8	2	3	4	6	3	4	6	6	4	4	8	8	2	3	4	6	2	3	4	6	3	4	4	6	3	3	4	6	3	4	8	8	4	4	8	6	3	3	6	
	PPA18	Int. přip.	8	4	12	12	4	3	6	9	6	4	9	9	8	4	12	12	4	3	6	9	4	3	6	9	6	4	6	9	6	3	6	9	6	4	12	12	8	4	12	9	6	3	9	9
	PPA19	HW fire	12	8	8	12	6	6	4	9	9	8	6	9	12	8	8	12	6	6	4	9	6	6	4	9	9	8	4	9	9	6	4	9	9	8	8	12	12	8	8	9	9	6	6	9
	PPA20	LAN SAN sw.	12	8	8	12	6	6	4	9	9	8	6	9	12	8	8	12	6	6	4	9	6	6	4	9	9	8	4	9	9	6	4	9	9	8	8	12	12	8	8	9	9	6	6	9
	PPA21	WIFI AP	8	8	8	8	4	6	4	6	6	8	6	6	8	8	8	8	4	6	4	6	4	6	4	6	6	8	4	6	6	6	4	6	6	8	8	8	8	8	8	6	6	6	6	6
	PPA22	Kabeláž	12	8	8	12	6	6	4	9	9	8	6	9	12	8	8	12	6	6	4	9	6	6	4	9	9	8	4	9	9	6	4	9	9	8	8	12	12	8	8	9	9	6	6	9
	PPA23	Kancelář	12	12	12	12	6	9	6	9	9	12	9	9	12	12	12	12	6	9	6	9	6	9	6	9	12	6	9	9	9	6	9	9	12	12	12	12	12	12	9	9	9	9	9	9
	PPA24	Serverovna	12	12	12	12	6	9	6	9	9	12	9	9	12	12	12	12	6	9	6	9	6	9	6	9	12	6	9	9	9	6	9	9	12	12	12	12	12	12	12	9	9	9	9	9
	PPA25	Vedení ob.	8	12	16	12	4	9	8	9	6	12	12	9	8	12	16	12	4	9	8	9	4	9	8	9	6	12	8	9	6	9	8	9	6	12	16	12	8	12	16	9	6	9	12	9
	PPA26	IT prac.	12	16	12	12	6	12	6	9	9	16	9	9	12	16	12	12	6	12	6	9	6	12	6	9	9	16	6	9	9	12	6	9	9	16	12	12	12	16	12	9	9	12	9	9
	PPA27	Úředníci	4	4	12	12	2	3	6	9	3	4	9	9	4	4	12	12	2	3	6	9	2	3	6	9	3	4	6	9	3	3	6	9	3	4	12	12	4	4	12	9	3	3	9	9
	PPA28	Ostatní zam.	4	4	8	8	2	3	4	6	3	4	6	6	4	4	8	8	2	3	4	6	2	3	4	6	3	4	4	6	3	3	4	6	3	4	8	8	4	4	8	6	3	3	6	

(zdroj: vlastní zpracování)

Výsledné hodnocení podpůrných aktiv je nyní v intervalu 1 – 16. Pro sjednocení hodnocení s primárními aktivy, kde je hodnocení těchto aktiv v intervalu 1 – 4, je nutno upravit hodnocení podpůrných aktiv rovněž do intervalu 1 – 4. K této úpravě slouží převodní tabulka, která byla vypracována dle vzoru metodiky NÚKIB.

Tabulka 31 Převodní tabulka hodnoty podpůrných aktiv

Výsledná hodnota podpůrného aktiv	
1 – 4	1
5 – 8	2
9 – 12	3
13 – 16	4

(zdroj: vlastní zpracování)

Tabulka 32 Výsledné hodnoty aktiv

Hodnoty aktiv po převodu do intervalu 1 - 4			Výsledné hodnoty aktiv			
			A	L	C	I
Podpůrná aktiva	PPA1	OS Windows	3	1	3	2
	PPA2	OS Základní	2	2	1	3
	PPA3	OS Exchange	3	2	2	3
	PPA4	Vizualizace	2	1	2	3
	PPA5	Antivír	2	3	3	3
	PPA6	Síťové TLP	2	3	3	3
	PPA7	Kancelářský	2	1	2	3
	PPA8	Rad. VERA	3	2	1	3
	PPA9	Stav. VITA	2	2	1	3
	PPA10	Pers. KVAS.	1	1	1	3
	PPA11	Prac. st.	1	3	2	3
	PPA12	Mob. zař.	1	3	3	3
	PPA13	Fyz. serv.	3	2	2	3
	PPA14	Dat. úlož.	2	3	2	3
	PPA15	Tiskárny	1	1	1	2
	PPA16	Výměn. m.	2	3	3	3
	PPA17	Docház. ter	1	1	2	2
	PPA18	Int. příp.	2	1	3	3
	PPA19	HW fire	3	2	2	3
	PPA20	LAN SAN sw.	3	2	2	3
	PPA21	WiFi AP	2	2	2	2
	PPA22	Kabeláž	3	2	2	3
	PPA23	Kancelář	3	3	3	3
	PPA24	Serverovna	3	3	3	3
	PPA25	Vedení ob.	2	3	4	3
	PPA26	IT prac.	3	4	3	3
	PPA27	Úředníci	1	1	3	3
	PPA28	Ostatní zam.	1	1	2	2

(zdroj: vlastní zpracování)

Výsledné hodnocení aktiv ukazuje, že nejvyšších stupňů bylo dosaženo v oblasti lidských zdrojů, konkrétně u vedení a obce a IT pracovníků. Druhou nevyšší hodnocenou kategorií jsou objekty, tedy kanceláře a serverovny.

14 ANALÝZA RIZIK

Další částí této práce v rámci posouzení rizik je jejich samotná analýza. K tomu, aby mohla být analýza rizik provedena, je nejdříve nutné identifikovat zranitelnosti a hrozby, které, na již v předchozích kapitolách identifikovaná a ohodnocená aktiva, působí a můžou vzájemně způsobit jejich ohrožení.

Analýza rizik byla provedena ve třech částech:

- Identifikace zranitelností
- Identifikace hrozeb
- Výpočet rizika

14.1 Identifikace zranitelností a jejich hodnocení

Zranitelnost je charakteristika nebo nedostatek aktiva, který jej činí citlivým na zneužití potenciálními hrozbami, což může vést k nežádoucím dopadům. Jinými slovy, jedná se o slabé místo, které zvyšuje pravděpodobnost, že aktivum bude poškozeno nebo zneužito konkrétní hrozbou.

Řešený subjekt musí dle § 5 odst. 1 písm. b) vyhlášky o kybernetické bezpečnosti (VKB) sestavit vlastní katalog zranitelností, který vychází zejména z kategorií uvedených v příloze č. 3 této vyhlášky. Tento katalog zranitelností může být následně přizpůsoben specifickým podmínkám a potřebám organizace, přičemž jednotlivé kategorie budou dále konkretizovány a rozšířeny o specifické zranitelnosti relevantní pro činnost, v daném případě obce. Při tvorbě katalogu zranitelností obce bylo zjištěno, že katalog uvedený v příloze č. 3 VKB není potřeba nikterak zvláště upravovat či doplňovat a z tohoto důvodu bylo vycházeno z katalogu vzorového.

Při tvorbě katalogu zranitelností byly definované zranitelnosti doplněny o kategorie aktiv, u kterých se tyto zranitelnosti mohou vyskytovat. Tohoto bylo později využito při určování hodnoty rizik, kdy budou vyřazeny zranitelnosti, které nemají souvztažnost s kategorií podpůrných aktiv. Vazby byly určovány principem položené otázky: Může daná zranitelnost působit na identifikované aktivum?

Tabulka 33 Katalog zranitelností

ID	Zranitelnost	Kategorie aktiv a vazby na zranitelnost				
		SW	HW	KP	OB	LZ
Z1	Nedostatečné provádění údržby informačních systémů	x	x	x		
Z2	Zastaralé informační systémy a technologie	x	x	x		
Z3	Nedostatečné zabezpečení vnějšího perimetru	x	x	x	x	
Z4	Nízká úroveň bezpečnostního povědomí uživatelů a administrátorů					x
Z5	Nevyhovující nebo nesprávné nastavení přístupových práv	x	x	x	x	x
Z6	Nedostatečné postupy pro identifikaci a řešení kybernetických bezpečnostních událostí a incidentů	x	x	x	x	x
Z7	Neefektivní monitorování aktivit uživatelů a administrátorů, neschopnost identifikovat nežádoucí chování	x	x	x		x
Z8	Nedostatečná specifikace bezpečnostních pravidel a rolí, nejasné určení odpovědnosti	x	x	x	x	x
Z9	Nedostatečná ochrana aktiv	x	x	x	x	x
Z10	Nevhodně navržená bezpečnostní architektura	x	x	x		
Z11	Nedostatečná míra nezávislé kontroly bezpečnostních opatření	x	x	x	x	
Z12	Neschopnost včasného odhalení chyb či pochybení zaměstnanců					x
Z13	Nedostatečný počet zaměstnanců s odpovídající odborností					x

(zdroj: vlastní zpracování)

Dalším krokem bylo vytvoření tabulky, která ohodnocuje jednotlivé zranitelnosti. K hodnocení bylo použito rozpětí na škále 1 až 4, kdy jsou tímto rozpětím ohodnocovány všechna výstupní data této práce, sloužící k analýze rizik. Jednotlivé hodnoty jsou rozděleny podle přijatých opatření v rámci kybernetické bezpečnosti a možnosti výskytu prolomení těchto bezpečnostních opatření. Jednotlivé četnosti výskytu jsou popsány v tabulce hodnotící zranitelnosti.

Tabulka 34 Hodnocení zranitelnosti

Hodnota	Úroveň zranitelnosti	Popis stavu bezpečnostních opatření
1	Nízká	Zranitelnost je zanedbatelná nebo velmi málo pravděpodobná. Obec aktivně využívá bezpečnostní opatření, která dokážou rychle detekovat vznikající zranitelnosti i případné pokusy o jejich zneužití.
2	Střední	Zranitelnost je málo až středně pravděpodobná. Zavedená bezpečnostní opatření jsou pravidelně ověřována, přesto jejich schopnost včasné detekce zranitelností nebo pokusů o jejich zneužití nemusí být vždy plně efektivní. Dosud však nebyly zaznamenány úspěšné pokusy o překonání těchto opatření.
3	Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření jsou sice implementována, avšak nejsou dostatečně komplexní, neřeší všechny potřebné oblasti nebo jejich efektivita není pravidelně ověřována. Existují známé případy částečně úspěšného překonání těchto opatření.
4	Kritická	Zranitelnost je velmi pravděpodobná až téměř jistá. Obec nemá odpovídající bezpečnostní opatření, případně jsou implementována nedostatečně a bez pravidelné kontroly jejich funkčnosti. Již byly zaznamenány úspěšné případy zneužití těchto zranitelností.

(zdroj: vlastní zpracování)

14.2 Identifikace a hodnocení hrozeb

Hrozbou se rozumí jakákoli událost nebo činnost, která může negativně ovlivnit kybernetickou bezpečnost obce a vést k poškození, ztrátě nebo ohrožení jejích aktiv. Hrozby lze klasifikovat podle povahy a původu na úmyslné, neúmyslné a přírodní, či způsobené vyšší mocí. Při tvorbě katalogu hrozeb obce bylo postupováno obdobně jako u katalogu zranitelností. Bylo použito katalogu uvedeného v příloze č. 3 VKB, který nebylo potřeba upravovat či doplňovat. Při tvorbě katalogu hrozeb byly definované hrozby doplněny o možné zasažené atributy CIA-L, u kterých se tyto hrozby mohou vyskytovat. Tohoto bylo později využito při určování hodnoty rizik, kdy budou vyřazeny hrozby, které nemají souvztažnost s kategorií příslušných aktiv.

Tabulka 35 Katalog hrozeb

ID	Hrozby	Atributy CIA-L a vazba na hrozby			
		A	L	C	I
H1	Porušení bezpečnostních pravidel, neoprávněné činnosti, zneužití práv uživatelů nebo administrátorů	x	x	x	x
H2	Technické nebo softwarové závady či selhání	x	x		x

ID	Hrozby	Atributy CIA-L a vazba na hrozby			
		A	L	C	I
H3	Zneužití či odcizení identity			x	x
H4	Používání softwaru v rozporu s licenčními pravidly	x	x		x
H5	Infekce škodlivým kódem (viry, spyware, trojské koně)	x	x	x	x
H6	Ohrožení fyzické bezpečnosti	x	x	x	x
H7	Výpadek elektronických komunikačních služeb nebo dodávek elektrické energie	x	x		x
H8	Neoprávněné použití či změna dat	x	x	x	x
H9	Ztráta, odcizení nebo poškození aktiv	x	x	x	
H10	Porušení smluvních povinností ze strany dodavatelů	x	x	x	x
H11	Chyby a omyly zaměstnanců	x	x	x	x
H12	Sabotáž nebo zneužití interních zdrojů	x	x	x	x
H13	Dlouhodobé přerušení důležitých služeb (komunikace, elektřina aj.)	x	x		
H14	Nedostatek kvalifikovaného personálu	x	x		
H15	Kybernetické útoky využívající sociální inženýrství nebo špionážní metody	x	x	x	x
H16	Zneužití přenosných datových médií			x	
H17	Útoky na elektronickou komunikaci (odposlechy, neoprávněné úpravy)			x	x

(zdroj: vlastní zpracován dle přílohy 2 PŘA)

Byla vytvořena tabulka, která ohodnocuje jednotlivé hrozby. Hodnocení probíhalo na základě konzultací s odpovědnými zaměstnanci obce. K ohodnocení bylo použito rozpětí na škále 1 až 4, přičemž jednotlivé hodnoty jsou rozděleny podle četnosti výskytu. Jednotlivé četnosti výskytu jsou popsány v tabulce hodnotící hrozby.

Tabulka 36 Hodnocení hrozeb

Hodnota	Pravděpodobnost výskytu hrozby	Odhadovaná četnost výskytu
1	Velmi nízká pravděpodobnost – výskyt je téměř vyloučen	Méně často než jednou za 3 roky
2	Nízká až střední pravděpodobnost – výskyt je možný	Přibližně jednou za 1 až 3 roky
3	Střední až vysoká pravděpodobnost – výskyt je pravděpodobný	Přibližně jednou za 1 měsíc až 1 rok
4	Vysoká až téměř jistá pravděpodobnost – výskyt je velmi častý	Častěji než jednou za měsíc

(zdroj: vlastní zpracován dle přílohy 2 PŘA)

14.3 Výpočet rizika

Výpočet rizika patří k základním procesům řízení informační bezpečnosti a jeho cílem je identifikovat a kvantifikovat potenciální ohrožení aktiv organizace. Standardně je při hodnocení rizika využíván vzorec, který zahrnuje tři základní proměnné: dopad, hrozbu a zranitelnost. V souladu s VKB je doporučována následující obecně platná funkce pro výpočet rizika:

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

Dopad je definován jako potenciální škoda, která by mohla vzniknout v důsledku narušení jednoho nebo více atributů informační bezpečnosti – důvěrnosti, integrity nebo dostupnosti. Výši dopadu určuje hodnota aktiv, jak je stanoveno v § 4 VKB, který rozlišuje primární aktiva, představující přímo hodnotné informace nebo systémy organizace, a podpůrná aktiva, která jsou nutná pro jejich ochranu a provoz. Hodnocení těchto aktiv umožňuje určit rozsah možných škod a tím i závažnost dopadu.

Hrozba vyjadřuje pravděpodobnost výskytu události nebo činnosti, která může způsobit poškození aktiva. Tato pravděpodobnost se stanovuje na základě historických údajů, statistických analýz nebo expertních odhadů.

Zranitelnost určuje, jak snadno je možné aktivum poškodit nebo zneužít, přičemž zahrnuje hodnocení existujících bezpečnostních opatření a jejich schopnost minimalizovat nebo eliminovat možnost zneužití zranitelnosti.

Výsledné hodnoty rizika, tzv. rizikové číslo RPN, slouží k prioritizaci bezpečnostních opatření a umožňují obci zaměřit se na kritické oblasti, jejichž zabezpečení je nezbytné pro efektivní řízení informační bezpečnosti a minimalizaci potenciálních škod.

Rizikové číslo (RPN) je většinou součin hodnot předem stanoveného významu, v tomto případě $RPN = D \times Z \times H$. Kritické hodnoty obvykle určuje řešitel (např. $RPN_{krit} = 64$).

Tabulka výpočtu hodnoty rizik byla sestavována postupně výběrem jednotlivých aktiv z katalogu aktiv, k nimž byla přiřazována příslušná zranitelnost uvedená v katalogu zranitelností. Poté byla určena hrozba, která tuto zranitelnost mohla využít. Tímto způsobem vznikala postupně jednotlivá spojení aktiv, jejich zranitelností a odpovídajících hrozeb. Vzhledem k velkému objemu možných kombinací, byly vybrány aktiva, zranitelnosti a

hrozby, které poskytují nejlepší podklad pro řešení rizik. Hodnocení rizik je dáno výčtem uvedeným v následující tabulce.

Tabulka 37 Hodnocení rizik a proces jejich zvládání

HODNOCENÍ RIZIK - R			PROCES ZVLÁDÁNÍ RIZIKA
1-16	nízká akceptace	R považováno za přijatelné – akceptovatelné	Garant, ve spolupráci s gestorem aktiva rozhodují o přijetí rizika a následně provádějí jeho sledování.
17-31	střední sledování	R sníženo méně náročnými opatřeními, v případě vyšší náročnosti je R akceptovatelné.	Pokud je zvolen přístup zvládání rizika formou akceptace, rozhodnutí přijímá garant společně s gestorem aktiva a probíhá sledování rizika. Pokud je zvolen přístup riziko snížit, navrhuje příslušná bezpečnostní opatření odpovědná osoba, ve spolupráci s gestorem.
32-47	vysoká redukce	R je dlouhodobě nepřijatelné, vytvoření postupu k redukci R	Garant společně s gestorem aktiva stanoví vhodný postup pro zvládnutí rizika. Pokud se rozhodnou riziko snížit, odpovědný pracovník navrhne ve spolupráci s garantem konkrétní bezpečnostní opatření, které je v co nejkratší době aplikováno.
48-64	kritická redukce	R je nepřijatelné a situaci je nutné řešit neprodleně redukcí R	Návrh na řešení identifikovaného rizika připravuje odpovědná osoba ve spolupráci s gestorem aktiva. Pokud se jako přístup zvolí snížení rizika, návrh konkrétních bezpečnostních opatření zpracovává odpovědná osoba. Návrh, včetně opatření, je následně předložen garantovi, který rozhodne o jeho schválení, případně určí jiný způsob řešení.

(zdroj: vlastní zpracování)

Výpočet rizikových čísel a jejich porovnání s kritickou hodnotou je dalším krokem této práce. Pro lepší přehlednost a pochopení, byla dle vzoru metodiky PŘA, vytvořena tabulka výpočtu hodnoty rizikového čísla RPN. Výpočet byl realizován podle výše uvedeného vzorce, tedy $\text{riziko} = \text{dopad} \times \text{hrozba} \times \text{zranitelnost}$. Tabulka obsahuje jednotlivá identifikovaná aktiva R 1 - 54. Hodnoty byly převzaty z tabulky 27, Katalog primárních aktiv, vytvořené v kapitole 13.2.3., s ohodnocením dle CIA-L, tedy dostupnosti A, ztráty L, důvěrnosti C a integrity I. Jednotlivé hodnoty PRA byly vynásobeny váhou vlivu, která byla stanovena v tabulce 28, Identifikace podpůrných aktiv a jejich hodnocení dle váhy vlivu. Výsledkem tohoto výpočtu je sloupec s uvedením maximálních hodnot podpůrných aktiv.

V následujících kontinuální tabulce jsou uvedeny výpočty rizikových čísel jednotlivých aktiv.

Tabulka 38 Hodnocení rizik

HODNOCENÍ RIZIK - VÝPOČET														
ID	Aktivum	Hodnota dopadu A	Hodnota dopadu L	Hodnota dopadu C	Hodnota dopadu I	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupnost	Hodnota rizika - ztráta	Hodnota rizika - důvěrnost	Hodnota rizika - integrita	Způsob zvládání rizika
R1	PPA 1 OS Windows server SW	3	1	3	2	Z1 Nedostatečné provádění údržby informačních systémů	2	H2 Technické nebo softwarové závady či selhání	3	18	6	18	12	Sledování
R2	PPA 1 OS Windows server SW	3	1	3	2	Z2 Zastaralé informační systémy a technologie	1	H2 Technické nebo softwarové závady či selhání	1	3	1	3	2	Akceptace
R3	PPA 1 OS Windows server SW	3	1	3	2	Z5 Nevyhovující nebo nesprávné nastavení přístupových práv	2	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	3	18	6	18	12	Sledování
R4	PPA 1 OS Windows server SW	3	1	3	2	Z8 Nedostatečná specifikace bezpečnostních pravidel a rolí	3	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	3	27	9	27	18	Sledování
R5	PPA 2 OS Základní SW	2	2	1	3	Z1 Nedostatečné provádění údržby informačních systémů	2	H2 Technické nebo softwarové závady či selhání	2	8	8	4	12	Akceptace
R6	PPA 2 OS Základní SW	2	2	1	3	Z2: Zastaralost aktiv	2	H2: Poškození nebo selhání technického nebo programového vybavení	3	12	12	6	18	Sledování
R7	PPA 2 OS Základní SW	2	2	1	3	Z5 Nevyhovující nebo nesprávné nastavení přístupových práv	2	H9 Ztráta, odcizení nebo poškození aktiv	3	12	12	6	18	Sledování
R8	PPA 2 OS Základní SW	2	2	1	3	Z7 Neefektivní monitorování aktivit uživatelů a administrátorů	3	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	4	24	24	12	36	Redukce

HODNOCENÍ RIZIK - VÝPOČET														
ID	Aktivum	Hodnota dopadu A	Hodnota dopadu L	Hodnota dopadu C	Hodnota dopadu I	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupnost	Hodnota rizika - ztráta	Hodnota rizika - důvěrnost	Hodnota rizika - integrita	Způsob zvládnání rizika
R9	PPA 3 OS Exchange SW	3	2	2	3	Z2: Zastaralost aktiv	2	H2: Poškození nebo selhání technického nebo programového vybavení	2	12	8	8	12	Akceptace
R10	PPA 3 OS Exchange SW	3	2	2	3	Z5 Nevyhovující nebo nesprávné nastavení přístupových práv	3	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	4	36	24	24	36	Redukce
R11	PPA 4 Vizualizace SW	2	1	2	3	Z1 Nedostatečné provádění údržby informačních systémů	2	H2: Poškození nebo selhání technického nebo programového vybavení	2	8	4	8	12	Akceptace
R12	PPA 5 Antivir SW	2	3	3	3	Z1 Nedostatečné provádění údržby informačních systémů	3	H8 Neoprávněné použití či změna dat	4	24	36	36	36	Redukce
R13	PPA 6 Síťové TLP SW	2	3	3	3	Z4 Nízká úroveň bezpečnostního povědomí uživatelů a administrátorů	2	H2: Poškození nebo selhání technického nebo programového vybavení	3	12	18	18	18	Sledování
R14	PPA 7 Kancelářský SW	2	1	2	3	Z2: Zastaralost aktiv	3	H2 Technické nebo softwarové závady či selhání	2	12	6	12	18	Sledování
R15	PPA 7 Kancelářský SW	2	1	2	3	Z4 Nízká úroveň bezpečnostního povědomí uživatelů a administrátorů	3	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	3	18	9	18	27	Sledování
R16	PPA 8 Rad. VERA SW	3	2	1	3	Z4 Nízká úroveň bezpečnostního povědomí uživatelů a administrátorů	3	H11 Chyby a omyly zaměstnanců	3	27	18	9	27	Sledování

HODNOCENÍ RIZIK - VÝPOČET														
ID	Aktivum	Hodnota dopadu A	Hodnota dopadu L	Hodnota dopadu C	Hodnota dopadu I	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupnost	Hodnota rizika - ztráta	Hodnota rizika - důvěrnost	Hodnota rizika - integrita	Způsob zvládání rizika
R17	PPA 8 Rad. VERA SW	3	2	1	3	Z5 Nevyhovující nebo nesprávné nastavení přístupových práv	3	H8 Neoprávněné použití či změna dat	4	36	24	12	36	Redukce
R18	PPA 8 Rad. VERA SW	3	2	1	3	Z7 Neefektivní monitorování aktivit uživatelů a administrátorů	3	H12 Sabotáž nebo zneužití interních zdrojů	3	27	18	9	27	Sledování
R19	PPA 9 Agendový SW	2	2	1	3	Z2 Zastaralé informační systémy a technologie	3	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	3	18	18	9	27	Sledování
R20	PPA 9 Agendový SW	2	2	1	3	Z7 Neefektivní monitorování aktivit uživatelů a administrátorů	3	H12 Sabotáž nebo zneužití interních zdrojů	4	24	24	12	36	Redukce
R21	PPA 10 Pers. KVAS. SW	1	1	1	3	Z1 Nedostatečné provádění údržby informačních systémů	2	H9 Ztráta, odcizení nebo poškození aktiv	2	4	4	4	12	Akceptace
R22	PPA 11 Pracovní stanice HW	1	3	2	3	Z2: Zastaralost aktiv	3	H2: Poškození nebo selhání technického nebo programového vybavení	3	9	27	18	27	Sledování
R23	PPA 11 Pracovní stanice HW	1	3	2	3	Z3 Nedostatečné zabezpečení vnějšího perimetru	4	H9 Ztráta, odcizení nebo poškození aktiv	4	16	48	32	48	Redukce
R24	PPA 12 Mobilní zařízení zař. HW	1	3	3	3	Z3 Nedostatečné zabezpečení vnějšího perimetru	2	H9 Ztráta, odcizení nebo poškození aktiv	3	6	18	18	18	Sledování

HODNOCENÍ RIZIK - VÝPOČET														
ID	Aktivum	Hodnota dopadu A	Hodnota dopadu L	Hodnota dopadu C	Hodnota dopadu I	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupnost	Hodnota rizika - ztráta	Hodnota rizika - důvěrnost	Hodnota rizika - integrita	Způsob zvládání rizika
R25	PPA 13 Servery HW	3	2	2	3	Z3 Nedostatečné zabezpečení vnějšího perimetru	4	H6 Ohrožení fyzické bezpečnosti	4	48	32	32	48	Redukce
R26	PPA 13 Servery HW	3	2	2	3	Z7 Neefektivní monitorování aktivit uživatelů a administrátorů	3	H8 Neoprávněné použití či změna dat	3	27	18	18	27	Sledování
R27	PPA 13 Servery HW	3	2	2	3	Z9 Nedostatečná ochrana aktiv	4	H9 Ztráta, odcizení nebo poškození aktiv	3	36	24	24	36	Redukce
R28	PPA 14 Datová úložiště HW	2	3	2	3	Z3 Nedostatečné zabezpečení vnějšího perimetru	3	H9 Ztráta, odcizení nebo poškození aktiv	4	24	36	24	36	Redukce
R29	PPA 14 Datová úložiště HW	2	3	2	3	Z4 Nízká úroveň bezpečnostního povědomí uživatelů a administrátorů	3	H2 Technické nebo softwarové závady či selhání	3	18	27	18	27	Sledování
R30	PPA 15 Tiskárny HW	1	1	1	3	Z9 Nedostatečná ochrana aktiv	2	H9 Ztráta, odcizení nebo poškození aktiv	2	4	4	4	12	Akceptace
R31	PPA 16 Výměnná média HW	2	3	3	3	Z6 Nedostatečné postupy pro identifikaci	3	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	4	24	36	36	36	Redukce
R32	PPA 16 Výměnná média HW	2	3	3	2	Z9 Nedostatečná ochrana aktiv	4	H16 Zneužití přenosných datových médií	4	32	48	48	32	Redukce

HODNOCENÍ RIZIK - VÝPOČET														
ID	Aktivum	Hodnota dopadu A	Hodnota dopadu L	Hodnota dopadu C	Hodnota dopadu I	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupnost	Hodnota rizika - ztráta	Hodnota rizika - důvěrnost	Hodnota rizika - integrita	Způsob zvládnutí rizika
R33	PPA 17 Docházkový terminál HW	1	1	2	2	Z9 Nedostatečná ochrana aktiv	2	H9 Ztráta, odcizení nebo poškození aktiv	2	4	4	8	8	Akceptace
R34	PPA 18 Internetové připojení	2	1	3	3	Z7 Neefektivní monitorování aktivit uživatelů a administrátorů	3	H5 Infekce škodlivým kódem (viry, spyware, trojské koně)	3	18	9	27	27	Sledování
R35	PPA 19 HW firewall	3	2	2	3	Z1 Nedostatečné provádění údržby informačních systémů	2	H13 Dlouhodobé přerušení důležitých služeb	3	18	12	12	18	Sledování
R36	PPA 19 HW firewall	3	2	2	3	Z2: Zastaralost aktiv	3	H15 Kybernetické útoky využívající sociální inž. nebo špiónážní metody	4	36	24	24	36	Redukce
R37	PPA 20 LAN SAN switch	3	2	2	3	Z1 Nedostatečné provádění údržby informačních systémů	2	H2 Technické nebo softwarové závady či selhání	4	24	16	16	24	Sledování
R38	PPA 20 LAN SAN switch	3	2	2	3	Z2: Zastaralost aktiv	3	H7 Výpadek el. komunikačních služeb nebo dodávek elektrické energie	3	27	18	18	27	Sledování
R39	PPA 21 WiFi AP	2	2	2	2	Z2: Zastaralost aktiv	3	H3 Zneužití či odcizení identity	3	18	18	18	18	Sledování
R40	PPA 22 Kabeláž	3	2	2	3	Z3 Nedostatečné zabezpečení vnějšího perimetru	4	H17 Útoky na elektronickou komunikaci	4	48	32	32	48	Redukce

HODNOCENÍ RIZIK - VÝPOČET														
ID	Aktivum	Hodnota dopadu A	Hodnota dopadu L	Hodnota dopadu C	Hodnota dopadu I	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupnost	Hodnota rizika - ztráta	Hodnota rizika - důvěrnost	Hodnota rizika - integrity	Způsob zvládání rizika
R41	PPA 22 Kabeláž	3	2	2	3	Z9 Nedostatečná ochrana aktiv	4	H8 Neoprávněné použití či změna dat	3	36	24	24	36	Redukce
R42	PPA 23 Kanceláře	3	3	3	3	Z3 Nedostatečné zabezpečení vnějšího perimetru	4	H6 Ohrožení fyzické bezpečnosti	4	48	48	48	48	Redukce
R43	PPA 23 Kanceláře	3	3	3	3	Z9 Nedostatečná ochrana aktiv	4	H9 Ztráta, odcizení nebo poškození aktiv	3	36	36	36	36	Redukce
R44	PPA 24 Serverovny	3	3	3	3	Z3 Nedostatečné zabezpečení vnějšího perimetru	4	H6 Ohrožení fyzické bezpečnosti	3	36	36	36	36	Redukce
R45	PPA 24 Serverovny	3	3	3	3	Z5 Nevyhovující nebo nesprávné nastavení přístupových práv	3	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	3	27	27	27	27	Sledování
R46	PPA 24 Serverovny	3	1	3	3	Z9 Nedostatečná ochrana aktiv	4	H9 Ztráta, odcizení nebo poškození aktiv	4	48	16	48	48	Redukce
R47	PPA 25 Vedení oborů	2	3	4	3	Z6 Nedostatečné postupy pro identifikaci	3	H12 Sabotáž nebo zneužití interních zdrojů	3	18	27	36	27	Redukce
R48	PPA 25 Vedení oborů	2	3	4	3	Z8 Nedostatečná specifikace bezpečnostních pravidel a rolí	2	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	3	12	18	24	18	Sledování

HODNOCENÍ RIZIK - VÝPOČET														
ID	Aktivum	Hodnota dopadu A	Hodnota dopadu L	Hodnota dopadu C	Hodnota dopadu I	Zranitelnost	Hodnota zranitelnosti	Hrozba	Hodnota hrozby	Hodnota rizika - dostupnost	Hodnota rizika - ztráta	Hodnota rizika - důvěrnost	Hodnota rizika - integrity	Způsob zvládnání rizika
R49	PPA 25 Vedení oborů	2	3	4	3	Z13 Nedostatečný počet zaměstnanců s odpovídající odborností	2	H14 Nedostatek kvalifikovaného personálu	2	8	12	16	12	Akceptace
R50	PPA 26 IT pracovníci	3	4	3	3	Z7 Neefektivní monitorování aktivit uživatelů a administrátorů	4	H12 Sabotáž nebo zneužití interních zdrojů	3	36	48	36	36	Redukce
R51	PPA 26 IT pracovníci	3	4	3	3	Z13 Nedostatečný počet zaměstnanců s odpovídající odborností	3	H13 Dlouhodobé přerušení důležitých služeb	4	36	48	36	36	Redukce
R52	PPA 27 Úředníci	1	1	3	3	Z4 Nízká úroveň bezpečnostního povědomí uživatelů a administrátorů	3	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	3	9	9	27	27	Sledování
R53	PPA 27 Úředníci	1	1	3	3	Z5 Nevyhovující nebo nesprávné nastavení přístupových práv	4	H8 Neoprávněné použití či změna dat	3	12	12	36	36	Redukce
R54	PPA 28 Ostatní zam.	1	1	2	2	Z4 Nízká úroveň bezpečnostního povědomí uživatelů a administrátorů	2	H1 Porušení bezpečnostních pravidel, neoprávněné činnosti	2	4	4	8	8	Akceptace

(zdroj: vlastní zpracování)

Výsledné vyhodnocení tabulky Hodnocení rizik – proběhne v následující kapitole, kde budou vyjmenována nejvíce ohrožená aktiva a rovněž je zde rozebráno, proč jsou tyto aktiva považována za nejrizikovější. Obsáhlejší část (přílohová) je věnována opatřením, proti zjištěným rizikům.

14.4 Vyhodnocení provedené analýzy

Na základě provedené analýzy rizik kybernetické bezpečnosti, která se opírala o hodnocení jednotlivých kategorií aktiv dle bezpečnostní triády CIA lze konstatovat následující výsledky. Informační aktiva, software, hardware, komunikační prostředky, lidské zdroje a objekty byly detailně posouzeny a bylo shledáno, že žádné aktivum nedosahuje kritických stupňů rizikové škály, ale zároveň byly nalezeny oblasti, kde je potřeba přijmout opatření k redukci rizik.

Nejvíce nedostatků bylo odhaleno v oblasti fyzické bezpečnosti objektů a ve správě lidských zdrojů. V oblasti lidských zdrojů byla zjištěna rizika spojená zejména s nedostatečným organizačním rozdělením funkcí a personálním obsazením. Především není zřízena funkce manažera kybernetické bezpečnosti, což je důležitá role v oblasti KB. To, že jsou nyní všechna aktiva vázána pouze na statutárního zástupce, tedy tajemníka a starostu, je naprosto nevyhovující. Každé aktivum by mělo být katalogizované a mělo by mít jiného garanta, např. vedoucí jednotlivých oborů. Není řešena zastupitelnost důležitých zaměstnanců. Tento stav je obdobný i u managementu obce. Tato situace vyžaduje realizaci systematických kroků a aktivit k zavedení stavu dle platné legislativy a metodik.

Další oblastí, kde je nutné přijetí opatření k redukci rizik, je oblast fyzické bezpečnosti. Všechny budovy obce jsou z hlediska možných hrozeb zabezpečeny velmi nedostatečně, a to zejména v době, kdy jsou tyto budovy otevřeny pro veřejnost. Pohyb těchto osob po vnitřním perimetru není nikterak kontrolován. Vstupní dveře do jednotlivých pater a stejně tak do kanceláří jsou volně přístupné a může se jimi kdokoliv volně pohybovat. Rovněž samotné dveře nemají žádnou bezpečnostní funkci a jsou lehce překonatelné i bez vynaložení větší námahy.

I přes relativně uspokojivé výsledky v hodnocení softwarových, hardwarových a komunikačních prostředků nelze tato aktiva považovat za bezproblémová a je třeba neustálé sledování, zda identifikovaná rizika nepřesáhnou mez, kdy bude potřeba přijmout opatření k redukci rizik. Lze doporučit jejich stálé monitorování, údržbu a aktualizace s cílem udržet požadovanou úroveň bezpečnosti.

Celkově lze shrnout, že nejvyšší prioritou by mělo být zavedení účinných opatření v oblasti fyzické bezpečnosti a řešení otázky lidského faktoru dle platné legislativy a současně metodik, které byly vytvořeny pro oblast veřejné správy.

15 NÁVRHOVÁ ČÁST

Tato část se zaměřuje na jednotlivá doporučení autora této diplomové práce. Návrhy byly zpracovány na základě informací získaných z předchozí analýzy rizika a na podkladu Opatření informační bezpečnosti, vycházejících z Přílohy A normy ČSN EN ISO/IEC 27001.

V odborných kruzích je uváděn fakt, že subjekty, které v současnosti plní podmínky pro držitele certifikace podle normy ČSN EN ISO/IEC 27001, plní z velké části zároveň podmínky opatření stanovené v právním předpisu NIS2. Rozdílem je to, že norma ČSN EN ISO/IEC 27001 je dobrovolná. Žádný subjekt k její implementaci není nucen a při jejím nedodržování nehrozí žádný postih. Zavedením tohoto systému však organizace chrání důvěrnost, integritu a dostupnost svých informačních aktiv a prokazuje tak svou schopnost efektivně řídit informační bezpečnost. Směrnice NIS2 je právním předpisem (zákonem), který rozšiřuje požadavky na kybernetickou bezpečnost v rámci EU. Je povinná pro vybrané sektory, mezi něž, po implementování do českého právního řádu, budou patřit i obce s rozšířenou působností, i když v režimu nižších povinností. Její implementace představuje právně normativní postup pro všechny organizace, které mají povinnost zvýšit svou odolnost vůči kybernetickým hrozbám. Je nutno podotknout, že subjektům, které spadají, nebo budou spadat, do působnosti směrnice NIS2, hrozí za nedodržování opatření dle tohoto právního předpisu sankce.

Céline Kivimäki uvádí, „*Pokud jste povinni dodržovat NIS2, ISO 27001 zůstává skvělým způsobem, jak využít osvědčené postupy a odpovědět na otázky, jak implementovat široce dané požadavky NIS2 pro vaši organizaci*“.

„*Celkově vzato, pokud vaše firma zpracovává citlivá data a nabízí také digitální služby, můžete dokonce zvážit implementaci obou frameworků. Kombinace norem ISO 27001 a NIS2 může poskytnout komplexní přístup, který zajistí bezpečnost dat a zároveň usnadní bezpečné poskytování digitálních služeb*“ (Kivimäki, 2024)

V následujících čtyřech kapitolách jsou popsána klíčová opatření, která byla vybrána na základě jejich nejvyšší důležitosti. Kompletní zpracování návrhových opatření je zařazeno do přílohy této práce. Struktura návrhové části odpovídá členění Přílohy A výše uvedené normy, včetně jednotlivých částí a odstavců, což umožňuje systematické a přehledné zpracování informací.

15.1 Organizační opatření

Organizační opatření v rámci normy ČSN EN ISO/IEC 27001 představují soubor bezpečnostních opatření zaměřených na řízení informační bezpečnosti z pohledu obce. Tato opatření zahrnují například vymezení odpovědností a rolí v oblasti bezpečnosti, řízení lidských zdrojů, pravidla pro přístup k informacím a řízení dodavatelských vztahů. Účelem je zajistit, aby byly zavedeny vhodné procesy a struktury podporující ochranu informací a minimalizaci rizik spojených s lidským faktorem i organizačními činnostmi.

V oblasti organizačních opatření bylo v rámci provedené analýzy zjištěno velké množství nedostatků. V politice informační bezpečnosti by vedení obce mělo konkretizovat a řádně zdokumentovat, jaké politiky budou v této oblasti uplatňovány, a dbát na to, aby byly uplatňovány i v praxi, nikoli jen formálně. V oblasti rolí a odpovědností musí každý zaměstnanec znát svou úlohu při ochraně informací – ať už jde o řadové úředníky, IT správce nebo vedení obce. K tomuto pověření zatím nedošlo, což je významný nedostatek. Odpovědnost za informační bezpečnost byla přenesena na všechny zaměstnance organizace, což není zcela vhodné řešení, neboť takto rozmělněná odpovědnost postrádá závaznost. Měl by být jmenován manažer kybernetické bezpečnosti, aby tato role nebyla svázána s vedením obce. Rovněž by měli být určeni garanti jednotlivých aktiv a jejich gestoři, jak to stanovuje metodika NÚKIB. Oddělení povinností není v obci jasně a prokazatelně zdokumentováno – tedy kdo má jaká práva a povinnosti v oblasti informační bezpečnosti. Nelze vyloučit, že je tato zásada porušována. Povinnosti by měly být jednoznačně zdokumentovány, pravidelně aktualizovány a kontrolovány. Katalog aktiv dosud nebyl zpracován a zdokumentován, jak vyžaduje metodika NÚKIB. Není tedy zřejmé, kdo je odpovědný za jednotlivá aktiva a jak jsou hodnocena z hlediska bezpečnosti.

Z výše uvedeného je patrné, že obec musí věnovat organizačním opatřením mnohem větší pozornost. Zavedením organizačních opatření lze výrazně zvýšit úroveň informační bezpečnosti a naplnit požadavky stanovené novou legislativou.

15.2 Opatření v oblasti lidských zdrojů

Opatření v oblasti lidských zdrojů se zaměřují na řízení bezpečnosti informací ve všech fázích pracovního poměru – před nástupem zaměstnance, během jeho pracovního poměru i po jeho ukončení. Cílem je zajistit, aby si zaměstnanci byli vědomi svých povinností v oblasti informační bezpečnosti, aby byli proškoleni, podepisovali závazky mlčenlivosti a jednali v souladu s bezpečnostními zásadami obce. Tato opatření pomáhají minimalizovat rizika spojená s lidským faktorem, který je často nejslabším článkem v oblasti kybernetické bezpečnosti.

V oblasti lidských zdrojů nebylo v rámci provedené analýzy zjištěno větší množství nedostatků, jako tomu bylo v kapitole věnované organizačním opatřením, která s touto oblastí úzce souvisí. Prověřování lidských zdrojů zahrnuje kontrolu a hodnocení všech zaměstnanců i externích spolupracovníků. V rámci opatření by měli být prověřováni i zaměstnanci během trvání pracovního poměru, nejen při jeho vzniku, jak je tomu doposud. V souvislosti s opatřením týkajícím se podávání zpráv o událostech informační bezpečnosti by bylo vhodné zajistit řádné poučení zaměstnanců o této povinnosti, neboť drtivá většina o ní ani neví – přestože je uvedena v organizační směrnici o kybernetické bezpečnosti obce. Možným řešením je například informační sdělení umístěné na monitoru.

15.3 Opatření fyzické bezpečnosti

Opatření fyzické bezpečnosti se zaměřují na ochranu fyzických prostor, zařízení a jiných aktiv před neoprávněným přístupem, poškozením nebo narušením. Patří sem například kontrola přístupu do budov, zabezpečení serveroven, dohledové systémy nebo řízení vstupu návštěv. Cílem těchto opatření je zajistit, aby kritická zařízení a informace byly chráněny i v reálném fyzickém prostoru, nejen v digitálním prostředí.

V této oblasti bylo zjištěno mnoho nedostatků, které by měly být řešeny přijetím vhodných opatření. Perimetrem fyzické bezpečnosti je prostor, který odděluje a chrání zájmová aktiva subjektu (např. počítač, síť nebo systém) před možným nebezpečím. Nejvýznamnější riziko v oblasti zabezpečení vzniká během pracovní doby, tedy v době, kdy je budova obce otevřena i pro veřejnost. Nebezpečí plyne zejména ze skutečnosti, že se kdokoli, bez jakékoli kontroly, může volně pohybovat téměř po celé budově obce. Uvnitř budovy jsou místnosti (kanceláře i serverovna) zabezpečeny naprosto nedostatečně – většinou pouze jednoduchými, často prosklenými dřevotřískovými dveřmi, které nepředstavují pro

případného útočníka žádnou překážku. Vhodným řešením by bylo zabezpečit vnitřní perimetr budovy tak, aby se nepovolané osoby nemohly bez kontroly pohybovat v citlivých prostorách. Jako efektivní se jeví uzavření jednotlivých pater budovy, kde by vstup byl možný pouze prostřednictvím elektronického zámku. Ten by umožnil vstup pouze zaměstnancům, případně jiným osobám výhradně za doprovodu zaměstnance. Tento systém byl s úspěchem zaveden na jiném úřadě vyššího územně samosprávného celku. Řešení tohoto opatření je velmi důležité, neboť byl nedávno zaznamenán neoprávněný vstup do jedné ze serveroven obce.

15.4 Technologická opatření

Technologická opatření představují soubor bezpečnostních mechanismů, které využívají technické prostředky k ochraně informací a systémů. Zahrnují například řízení přístupových práv, šifrování dat, bezpečnostní aktualizace, antivirovou ochranu, firewall, detekci narušení a zálohování. Cílem těchto opatření je minimalizovat technická rizika, zabránit neoprávněnému přístupu a zajistit dostupnost, integritu a důvěrnost informací v digitálním prostředí.

Technologická opatření spadají do oblasti, kde byly provedenou analýzou zjištěny nedostatky, které vyžadují řešení. Je nutné zavést opatření v oblasti omezení přístupu k informacím. V současné době neexistuje žádná databáze, ve které by bylo uvedeno, ke kterým informacím mají jednotliví zaměstnanci přístup. Pokud je zaměstnanci zřízen přístup k určitému typu informací, není po jeho přeřazení na jinou pracovní pozici tento přístup revidován ani upraven. Nelze tedy vyloučit, že někteří zaměstnanci mají přístup k informacím, ke kterým by již přístup mít neměli.

15.5 Shrnutí kapitoly

V předchozích kapitolách byla představena opatření vycházející z požadavků normy ČSN EN ISO/IEC 27001. Tato opatření byla zvolena jako nejvýznamnější na základě výsledků provedené analýzy, která tvoří hlavní část této diplomové práce. Cílem jejich uvedení bylo poukázat na stěžejní oblasti kybernetické bezpečnosti, které si v daném kontextu zaslouží zvýšenou pozornost. **Kompletní návrh opatření v souladu s výše uvedenou normou je zařazen v přílohách PI až PIV této práce.**

ZÁVĚR

Cílem této diplomové práce bylo analyzovat problematiku kybernetické bezpečnosti ve vybraném územně samosprávném celku, konkrétně v reálně existující obci s rozšířenou působností.

V úvodních kapitolách byla provedena literární rešerše odborných zdrojů zabývajících se danou tematikou, která autorovi poskytla teoretické východisko pro zpracování práce. Byly vymezeny a vysvětleny klíčové pojmy související s kybernetickou bezpečností. Pozornost byla věnována zejména pojmům jako kyberprostor, informační a kybernetická bezpečnost, informace a data, a dalším relevantním termínům. Součástí teoretické části bylo rovněž zhodnocení aktuálních kybernetických hrozeb, které nejčastěji cílí na subjekty veřejné správy. Dále byl vysvětlen princip tzv. CIA triády, která představuje základní rámec ochrany informací z hlediska důvěrnosti, integrity a dostupnosti. Tento koncept byl dále využit jako teoretické východisko pro hodnocení identifikovaných aktiv v praktické části práce, zejména v rámci analýzy rizik.

Významná část teoretického rámce byla věnována shrnutí platné legislativy, standardů a metodik souvisejících s oblastí kybernetické bezpečnosti a řízením rizik. Zohledněny byly jak národní, tak evropské právní předpisy, jejichž požadavky mají přímý dopad na fungování územních samospráv. Zvláštní důraz byl kladen na mezinárodní standardy ISO, především na rámec řízení rizik dle normy ČSN ISO 31000 a řízení informačních rizik podle normy ČSN EN ISO/IEC 27005. Důležitým podkladem pro praktickou část se stala metodika zaměřená na kybernetickou bezpečnost obcí, která umožnila systematický přístup k identifikaci aktiv, hrozeb a zranitelností a vytvořila základ pro provedení analýzy rizik.

Praktická část práce se soustředí na konkrétní podmínky analyzované obce. V jejím úvodu bylo detailně popsáno prostředí obce, včetně personální struktury a technického zázemí, se zaměřením na zabezpečení budov a prostor, zejména serveroven. Následně byla zpracována analýza rizik kybernetické bezpečnosti, která byla hlavním cílem této práce. Analýza byla rozdělena do tří navazujících částí: stanovení kontextu obce, posouzení rizik a jejich následné hodnocení. Ačkoli byly jednotlivé části zpracovány samostatně, jejich propojením vznikl ucelený pohled na stav kybernetické bezpečnosti obce.

Výsledky analýzy rizik ukázaly, že nejzávažnější rizika souvisejí s oblastí lidských zdrojů a fyzickým zabezpečením budov. V oblasti lidských zdrojů se jako problematické ukázalo

nedostatečně řešené rozdělení odpovědností v oblasti kybernetické bezpečnosti. V současnosti není stanoveno, jakým způsobem bude tato problematika řešena po účinnosti nového zákona o kybernetické bezpečnosti. V oblasti fyzického zabezpečení byla identifikována celá řada nedostatků, které ohrožují nejen kybernetickou bezpečnost, ale také bezpečnost osob. V minulosti již došlo k incidentům, jako je odcizení hardwarového vybavení a neoprávněný přístup do serverovny.

Na základě výsledků analýzy byla navržena konkrétní opatření vycházející z požadavků nové normy ČSN EN ISO/IEC 27001, která reflektuje směrnici NIS2. Mezi klíčová doporučení patří posílení fyzické ochrany obecních budov a zavedení přesně definovaných a dokumentovaných pravidel v oblasti personální odpovědnosti za kybernetickou bezpečnost.

Závěrem lze konstatovat, že analýza potvrdila výchozí hypotézu, že zkoumaná obec, obdobně jako většina obcí s rozšířenou působností, nepřistupuje ke kybernetické bezpečnosti s odpovídající vážností a není dostatečně připravena na implementaci nových legislativních požadavků vyplývajících ze směrnice NIS2. Autor doporučuje zvýšit důraz na oblast kybernetické bezpečnosti, pravidelně revidovat stávající opatření a jejich účinnost porovnávat s aktuálním stavem hrozeb, aby bylo zajištěno jejich efektivní a včasné uplatnění v praxi.

SEZNAM POUŽITÉ LITERATURY

ALKHALIL, Zainab; HEWAGE, Chaminda; NAWAF, Liqaa a KHAN, Imtiaz, 2021. *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*. Online. Frontiers in Computer Science. 2021-3-9, roč. 3. ISSN 2624-9898. Dostupné z: <https://doi.org/10.3389/fcomp.2021.563060>. [cit. 2025-04-03].

APTIENT LABS s.r.o., 2024. *Základy řízení rizik ve firmě*. Online. Dostupné z: <https://aptien.com/cs/kb/articles/risk-management>. [cit. 2025-04-04].

BURGESS, Jonah, 2022. *Modern DDoS Attacks and Defences - Survey*. arXiv preprint arXiv:2211.15404. Dostupné z: <https://arxiv.org/abs/2211.15404>. [cit. 2025-04-01].

CALDER, Alan, 2020. *Cyber security: essential principles to secure your organisation*. Ely, Cambridgeshire: IT Governance Publishing. ISBN 978-1-78778-210-5. Dostupné také z: <https://ebookcentral.proquest.com/lib/natl-ebooks/detail.action?docID=6176700>.

ČERMÁK, Miroslav, 2010. *Analýza rizik*. Online. In: Clever and Smart. 20. 05. 2010, 20.01.2013. Dostupné z: <https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/>. [cit. 2025-03-27].

ČESKO, 1993. *Ústavní zákon č. 1/1993 Sb., Ústava České republiky*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/1993-1>.

ČESKO, 2000. *Zákon č. 128/2000 Sb. o obcích*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2000-128>.

ČESKO, 2002. *Zákon č. 314/2002 Sb. o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2002-314>.

ČESKO, 2005. *Zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2005-412>.

ČESKO, 2010. *Nařízení vlády č. 432/2010 Sb., ve znění Nařízení vlády č. 315/2014 Sb., definuje kritéria pro určení prvků kritické infrastruktury v České republice*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2010-432>

ČESKO, 2014. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2014-181>.

ČESKO, 2017. *Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2017-437>.

ČESKO, 2018. *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2018-82>.

ČESKO, 2021. *Vyhláška č. 316/2021 Sb., o požadavcích pro zápis do katalogu cloud computingu*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2021-316>.

ČESKO, 2021. *Vyhláška č. 317/2014 Sb., o významných informačních systémech*. In: *Sbírka zákonů ČR*. Dostupné také z: <https://www.zakonyprolidi.cz/cs/2014-317>

ČSN EN ISO/IEC 27001, 2023. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Česká agentura pro standardizaci, 2023.

ČSN EN ISO/IEC 27005, 2022. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Česká agentura pro standardizaci, 2022.

ČSN ISO 31000, 2018. *Management rizik – Směrnice*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Česká agentura pro standardizaci, 2018.

DIGITÁLNÍ A INFORMAČNÍ AGENTURA, 2025. *Registr práv a povinností*. Online. Dostupné z: <https://www.szrcr.cz/cs/registr-prav-a-povinnosti>. [cit. 2025-03-22].

DIGITÁLNÍ A INFORMAČNÍ AGENTURA, 2025. *Rozcestník vygenerovaných agend*. Online. Dostupné z: <https://rpp-ais.egon.gov.cz/gen/agendy-detail/>. [cit. 2025-03-22].

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

DQS SLOVAKIA s.r.o., 2022. *Normy pro bezpečnost informací - přehled*. Online. Dostupné z: <https://www.dqsglobal.com/cs-cz/vzdelavani/blog/normy-pro-bezpecnost-informaci-prehled>. [cit. 2025-04-07].

EFFICHEM, s.r.o., 2021. *Integrita dat*. Online. Dostupné z: https://gcms.cz/labrulez-bucket-strapih3hsga3/Effichem_Integrita_dat_11849d3a3e/Effichem-Integrita-dat.pdf. [cit. 2025-04-03].

EU, 2016. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 16. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii, 2016. In: EU.

EU, 2019. Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií. 2019. In: EU.

EU, 2022. Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii. 2022. In: EU.

EU, 2024. Prováděcí nařízení Komise (EU) 2024/482 ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC). 2024. In: EU.

FORCEPOINT, 2024. *What is the CIA Triad?* Online. Forcepoint. Cyber Edu. Dostupné z: <https://www.forcepoint.com/cyber-edu/cia-triad>. [cit. 2025-04-03].

FRANK BOLD, 2017. *Samostatná a přenesená působnost*. Online. Frank Bold. Poradna. 11. 4. 2017, 12. 1. 2022. Dostupné z: <https://frankbold.org/poradna/fungovani-obci-a-uradu/cinnost-obce-a-kraje/cinnost-obce-a-kraje/rada/samostatna-a-prenesena-pusobnost>. [cit. 2025-03-16]

HARVARD BUSINESS SCHOOL, 2023. *What Is Risk Management & Why Is It Important?* Online. Dostupné z: https://online.hbs.edu/blog/post/risk-management?utm_source=chatgpt.com. [cit. 2025-04-06].

INFORMA TECHTARGET, 2024. *What is the CIA triad*. Online. Informa Techtarget. Dostupné z: <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>. [cit. 2025-04-03].

IT-slovník.cz, 2024. *Co je to Informace?* Online. Dostupné z: <https://it-slovník.cz/pojem/informace>. [cit. 2025-04-02].

KIVIMÄKI, Céline, 2024. *ISO 27001 and NIS2: Understanding their Connection*. Online. CYBERDAY Inc. NIS2 collection. 01.03.2024. Dostupné z: <https://www.cyberday.ai/blog/iso-27001-and-nis2-connection>. [cit. 2025-04-03].

KLEIN, Galit and ZWILLING, Moti, 2023. *The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home*. *Journal of Computer Information Systems*, 64(3), 408–422. <https://doi.org/10.1080/08874417.2023.2221200>. [cit. 2025-04-02].

KOLOUCH, Jan a BAŠTA, Pavel, 2019. *CyberSecurity*. 2019. Praha: CZ.NIC, z.s.p.o. ISBN 978-80-88168-34-8.

KSHETRI, Naresh, RAHMAN, Mir, Mehedi, SAYEED, Abu, Sayed, SULTANA, Irin, 2024. *Cryptoran: A Review on Cryptojacking and Ransomware Attacks W.R.T. Banking Industry—Threats, Challenges, & Problems*. *Journal of Information Security*, Vol.15 No.4, October 29, 2024, s. 523-528. Dostupné z: <https://www.scirp.org/reference/referencespapers?referenceid=3848405>. [cit. 2025-04-01]

Kybernetická bezpečnost obcí, 2024. Online. S. 12. Dostupné z: NÚKIB, https://portal.nukib.gov.cz/storage/uploads/2025/02/14/podpurny-material_kyberneticka-bezpecnost-obci_uid_6753022f5e89b_uid_67af075214cc3.pdf. [cit. 2025-03-22].

LEGISLATIVA s.r.o., 2022. *Kybernetický útok (kyberútok). Definice, typy, následky a prevence*. Online. 13.09.2022. Dostupné z: <https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok>. [cit. 2025-04-02].

Metodika analýzy rizik (DPIA), 2018. Online. S. 28. Dostupné z: Microsoft, https://download.microsoft.com/documents/cs-cz/Priloha-1_Metodika-analyzy-rizik_health.pdf. [cit. 2025-03-22].

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY ČR, 2024. *Data a informace*. Online. Ministerstvo školství, mládeže a tělovýchovy ČR. Pomáháme základním školám. 15.08.2024. Dostupné z: <https://digitalizace.rvp.cz/files/vystup-rvp-e-strana-1-8.pdf>. [cit. 2025-04-02].

MINISTERSTVO VNITRA ČR, 2025. *Pojmy úředník*. Online. Ministerstvo vnitra ČR. Dostupné z: <https://mv.gov.cz/odk2/soubor/stanovisko-k-bodu-programu-c-2-802894.aspx>. [cit. 2025-03-16].

MINISTERSTVO ŽIVOTNÍHO PROSTŘEDÍ ČR, 2022. *Perun*. Online. Ministerstvo životního prostředí ČR. Perun. 2022. Dostupné z: <https://www.perun-klima.cz/terms/managementRizik.html>. [cit. 2025-03-18].

MONGA, Sukhpreet, 2025. *Understand the Cyberspace Meaning: Definition, Importance & Key Concepts*. Online. Plutus Education. Understand the Cyberspace Meaning: Definition, Importance & Key Concepts. Dostupné z: <https://plutuseducation.com/blog/cyberspace-meaning/>. [cit. 2025-04-02].

NÚKIB, 2020. *Doporučení k používání protokolu TLP ke sdílení chráněných informací*. Online. NÚKIB. Doporučení. 03.07.2020. Dostupné z: <https://nukib.gov.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/>. [cit. 2025-04-06].

NÚKIB, 2022, a. *NÚKIB zveřejnil Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti*. Online. NÚKIB. Aktuality. 22.08.2022. Dostupné z: <https://nukib.gov.cz/cs/infoservis/aktuality/1868-nukib-zverejnil-pruvodce-rizenim-aktiv-a-rizik-dle-vyhlasky-o-kyberneticke-bezpecnosti/>. [cit. 2025-04-06].

NÚKIB, 2022, b. *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti*. Online. NÚKIB. Materiály k vyhlášce o kybernetické bezpečnosti. 18.08.2022. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/materialy-k-vyhlasce-o-kyberneticke-bezpecnosti/>. [cit. 2025-04-03].

NÚKIB, 2022, c. *Příloha 5 - Vzorová pravidla ochrany jednotlivých úrovní aktiv*. Online. NÚKIB. Materiály k vyhlášce o kybernetické bezpečnosti. 18.08.2022. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/materialy-k-vyhlasce-o-kyberneticke-bezpecnosti/>. [cit. 2025-04-03].

NÚKIB, 2024. *Legislativa*. Online. NÚKIB. Legislativa. 24.10.2024. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/>. [cit. 2025-04-04].

NÚKIB, 2024. *Kybernetická bezpečnost obcí*. Online. NÚKIB. Aktuality. 04.12.2024. Dostupné z: https://portal.nukib.gov.cz/storage/uploads/2025/02/14/podpurny-material_kyberneticka-bezpecnost-obci_uid_6753022f5e89b_uid_67af075214cc3.pdf. [cit. 2025-04-06].

NÚKIB, 2025. *NÚKIB v roce 2024 zaznamenal více kybernetických incidentů než v předchozích letech.* Online. NÚKIB. Aktuality. 31.01.2025. Dostupné z: https://nukib.gov.cz/cs/infoservis/aktuality/2215-nukib-v-roce-2024-zaznamenal-vice-kybernetickych-incidentu-nez-v-predchozich-letech/?utm_source=chatgpt.com. [cit. 2025-04-01].

NÚKIB, 2025. *Šéfuj kyber.* Online. NÚKIB, Osvěta. Dostupné z: <https://osveta.nukib.gov.cz/mod/page/view.php?id=4022>. [cit. 2025-03-27].

Q-COM s.r.o., 2019. *Základní normativní rámec ISMS.* Online. Q-COM s.r.o. Dostupné z: <https://www.qcom.cz/systemy-rizeni/isms/zakladni-normativni-ramec/>. [cit. 2025-04-01].

Security Risk Analysis for Information Asset, 2022. Online. Journal of System and Management Sciences. Roč. 2022, č. 12, s. 191-204. ISSN 1816-6075. Dostupné z: <https://doi.org/10.33168/JSMS.2022.0412>. [cit. 2025-04-01].

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru.* Vydání: první. Brno: CERM, akademické nakladatelství. ISBN 978-80-7623-068-2.

SMEJKAL, Vladimír, SOKOL, Tomáš a KODL, Jindřich, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* 2019. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-765-8.

STRUPCZEWSKI, Grzegorz, 2021. *Defining cyber risk: Safety Science.* Online. ISSN 0925-7535. Dostupné z: <https://doi.org/https://doi.org/10.1016/j.ssci.2020.105143>. [cit. 2025-04-02].

SVAZ MĚST A OBCÍ ČR, 2023. *Kybernetická a informační bezpečnost: Úvod do problematiky a metodický rámec.* Online. s. 16. Dostupné z: https://www.smocr.cz/shared/clanky/12991/P%C5%99%C3%ADloha_1_%C3%9Avod%20do%20problematiky%20a%20metodick%C3%BD%20r%C3%A1mec_Kybernetick%C3%A1%20a%20informa%C4%8Dn%C3%AD%20bezpe%C4%8Dnost.docx. [cit. 2025-03-22].

SVAZ MĚST A OBCÍ ČR, 2023. *Politiky organizačních a technických opatření kybernetické bezpečnosti.* Online. s. 75. Dostupné z: Svaz měst a obcí ČR, https://www.smocr.cz/shared/clanky/12991/P%C5%99%C3%ADloha_3_Politika%20orga

niza%C4%8Dn%C3%ADch%20a%20technick%C3%BDch%20opat%C5%99en%C3%A
D%20kybernetick%C3%A9%20bezpe%C4%8Dnosti_vzor.docx. [cit. 2025-03-22].

VANĚK, Jiří, 2023. *Co je to CIA triáda a k čemu tento koncept slouží*. Online. Jiří Vaněk –
Osobní blog. 23.07.2023, 05.12.2023. Dostupné z:
<https://blog.jirivanek.eu/cs/2023/07/23/co-je-to-cia-triada-a-k-cemu-tento-koncept-slouzi/>.
[cit. 2025-04-03].

SEZNAM OBRÁZKŮ

Obrázek 1 Triáda CIA	26
Obrázek 2 Traffic Light Protocol.....	29
Obrázek 3 Struktura norem řady ISO 27000	40
Obrázek 4 Proces řízení rizik dle normy ČSN ISO 31000.....	45
Obrázek 5 Proces řízení informačních rizik dle normy ČSN EN ISO/IEC 27005	46
Obrázek 6 Proces sledování a zlepšování řízení rizik	47
Obrázek 7 Schéma organizační struktury obce	55
Obrázek 8 Obecné schéma propojení aktiv	60
Obrázek 9 Schéma analýzy rizik	61
Obrázek 10 Stav aplikační vrstvy	81
Obrázek 11 Stav technologická vrstva	82

SEZNAM TABULEK

Tabulka 1 Zaměstnanci.....	54
Tabulka 2 Struktura.....	55
Tabulka 3 Primární aktiva obec a orgány obce.....	64
Tabulka 4 Primární aktiva správní činnosti.....	64
Tabulka 5 Primární aktiva krizové řízení a ochrana obyvatelstva	66
Tabulka 6 Primární aktiva majetek obce	66
Tabulka 7 Primární aktiva doprava	66
Tabulka 8 Primární aktiva výstavba.....	67
Tabulka 9 Primární aktiva životní prostředí	67
Tabulka 10 Primární aktiva finanční agenda	68
Tabulka 11 Primární aktiva sociální oblast	69
Tabulka 12 Primární aktiva přestupky	69
Tabulka 13 Základní stupnice dopadů.....	70
Tabulka 14 Hodnocení důvěrnosti	71
Tabulka 15 Hodnocení integrity	71
Tabulka 16 Hodnocení dostupnosti.....	71
Tabulka 17 Hodnocení primárního aktiva PRA 1 Obec a orgány obce	74
Tabulka 18 Hodnocení primárního aktiva PRA 2 Správní činnosti.....	74
Tabulka 19 Hodnocení primárního aktiva PRA 3 Krizové řízení a ochrana obyvatelstva .	75
Tabulka 20 Hodnocení primárního aktiva PRA 4 Majetek obce	75
Tabulka 21 Hodnocení primárního aktiva PRA 5 Doprava.....	76
Tabulka 22 Hodnocení primárního aktiva PRA 6 Výstavba	76
Tabulka 23 Hodnocení primárního aktiva PRA 7 Životní prostředí.....	77
Tabulka 24 Hodnocení primárního aktiva PRA 8 Finanční agenda	77
Tabulka 25 Hodnocení primárního aktiva PRA 9 Sociální služby	78
Tabulka 26 Hodnocení primárního aktiva PRA 10 Přestupky	78
Tabulka 27 Katalog primárních aktiv s ohodnocením dle CIA	79
Tabulka 28 Identifikace podpůrných aktiv a jejich hodnocení dle váhy vlivu	83
Tabulka 29 Váha vlivu (dále jako „VV“).....	84
Tabulka 30 Hodnoty podpůrných aktiv, výpočet dle vzorce	85
Tabulka 31 Převodní tabulka hodnoty podpůrných aktiv.....	85
Tabulka 32 Výsledné hodnoty aktiv.....	86
Tabulka 33 Katalog zranitelností	88
Tabulka 34 Hodnocení zranitelnosti	89

Tabulka 35 Katalog hrozeb	89
Tabulka 36 Hodnocení hrozeb.....	90
Tabulka 37 Hodnocení rizik a proces jejich zvládání	92
Tabulka 38 Hodnocení rizik	93

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CIA	Důvěrnost, integrita, dostupnost
ČSN	Česká státní norma
EIA	Posuzování vlivů na životní prostředí
EMAS	Systém ekologického řízení a auditu
EU	Evropská unie
EUCC	Evropský systém certifikace kybernetické bezpečnosti
FMEA	Analýza možného výskytu a vlivu vad
HA	Vysoká dostupnost
HW	Hardware
CHKO	Chráněná krajinná oblast
ICT	Informační a komunikační technologie
ID	Identifikace
IEC	Mezinárodní elektrotechnická komise
IS	Informační systém
ISO	Mezinárodní organizace pro normalizaci
ISMS	Systém řízení informační bezpečnosti
ISVS	Informační systém veřejné správy
IT	Informační technologie
KB	Kybernetická bezpečnost
KBO	Kybernetická bezpečnost obcí
KI	Kritická infrastruktura
KP	Komunikační připojení
LZ	Lidské zdroje
NBÚ	Národní bezpečnostní úřad
NIS	Směrnice EU o bezpečnosti sítí a informací

NIS2	Směrnice EU o bezpečnosti sítí a informací – nová
NÚKIB	Národní úřad pro kybernetickou bezpečnost
OB	Objekty
ORP	Obce s rozšířenou působností
OSPOD	Orgán sociálně právní ochrany dětí
PCO	Pult centralizované ochrany
PPA	Podpůrná aktiva
PRA	Primární aktiva
PŘA	Průvodce řízením aktiv
PZTS	Poplachový zabezpečovací a tísňový systém
ROB	Registr obyvatel
ROS	Registr hospodářských subjektů
RPN	Rizikové číslo
RPP	Registr práv a povinností
RÚIAN	Registr územní identity a adres nemovitostí
SLA	Smlouva mezi poskytovatelem a uživatelem služby
SW	Software
TLP	Traffic Light Protocol - slouží k určení míry důvěrnosti informací
VKB	Vyhláška o kybernetické bezpečnosti
VV	Váha vlivu
ŽU	Živnostenský úřad

SEZNAM PŘÍLOH

Příloha P I: Organizační opatření

Příloha P II: Opatření v oblasti lidských zdrojů

Příloha P III: Opatření fyzické bezpečnosti

Příloha P IV: Technologická opatření

PŘÍLOHA P I: ORGANIZAČNÍ OPATŘENÍ

A1 - 5. Organizační opatření

Organizační opatření zahrnují zpracování a zdokumentování pravidel, postupů a procesů, které pomáhají chránit citlivé informace organizace.

A1 - 5.1 Politika pro informační bezpečnost

Politika definuje zásady, odpovědnosti a postupy pro zabezpečení informačních systémů, ochranu osobních údajů občanů a minimalizaci rizik spojených s útoky. Vedení obce je odpovědné za implementaci, pravidelnou aktualizaci a zajištění, aby zaměstnanci byli s principy politik obeznamenáni, a hlavně, aby je aktivně dodržovali. Vedení obce se sice usneslo na tom, že bude podporovat stanovené cíle IB a že bezpečnostními politikami vyjadřuje svou strategii a závazek trvalého zajišťování, dodržování a zvyšování bezpečnosti informací jako nedílné součásti interních řídicích procesů, ovšem tato podpora a strategie není nikde konkretizována a dokumentována.

A1 - 5.2 Role a odpovědnosti a pravomoci organizace

Jasně vymezení rolí, odpovědností a pravomocí v oblasti kybernetické bezpečnosti je velmi důležité pro efektivní řízení rizik v organizaci. Každý zaměstnanec musí znát svou úlohu při ochraně informací, ať už jde o řadové úředníky, IT správce nebo vedení obce. IT oddělení nese odpovědnost za správu a zabezpečení informačních systémů po technické stránce, zatímco vedení obce zajišťuje strategickou podporu a dodržování bezpečnostních politik. Důležité je pověřit konkrétní osoby, či osob, dohledem nad implementací opatření proti kybernetickým hrozbám. K tomuto pověření zatím nedošlo, což je významný nedostatek. Odpovědnost za IB byla přenesena na všechny zaměstnance organizace, což není úplně nejvhodnější řešení, neboť takto rozmělněná odpovědnost není zavazující. Měl by být jmenován manažer kybernetické bezpečnosti, tak, aby tato role nebyla svázána s vedením obce. Rovněž by měli být jmenováni garanti jednotlivých aktiv a jejich gestoři.

A1 - 5.3 Oddělení povinností

V rámci kybernetické bezpečnosti je bezpečnostní princip, který zajišťuje, že žádná jednotlivá osoba nemá úplnou kontrolu nad celým kritickým procesem nebo systémem. Cílem je minimalizovat riziko zneužití pravomocí, chyb nebo podvodů tím, že se úkoly rozdělí mezi více osob nebo rolí. Je to důležitý princip pro organizace, které chtějí zajistit bezpečnost dat a systémů. V obci není zcela jasně jakkoliv zdokumentováno, kdo a jaká má

práva v této oblasti. Nelze tedy zcela vyloučit, že je tato zásada kontroly porušena. Povinnosti by měli být jasně zdokumentovány, aktualizovány a kontrolovány.

A1 - 5.4 Odpovědnost vedení

Management obce nese hlavní roli při zajištění ochrany dat, systémů a IT infrastruktury. Vedení obce by mělo nést odpovědnost za to, aby byla informační bezpečnost součástí strategie organizace. Bohužel je vnímána spíše jen jako technický problém, který je sice nutné řešit, ale bez další návaznosti.

A1 – 5.5 Kontakt s autoritami

Podstatou je spolupráce organizace s regulačními, dohledovými a bezpečnostními institucemi za účelem prevence, detekce a reakce na kybernetické hrozby, např. NÚKIB, CERT. Cílem kontaktu s autoritami je zajištění efektivní prevence a řešení kybernetických incidentů prostřednictvím koordinace s odpovědnými autoritami. Má být stanoveno a zdokumentováno kdo a kdy má kontaktovat orgány (policii, regulatorní orgány, orgány dohledu) a jak včas mají být zjištěné incidenty oznámeny. Toto však zatím není nikterak řešeno, a to jak po stránce legislativní, tak po stránce personální a technické.

A1 – 5.6. Kontakt se zvláštními zájmovými skupinami

Opatření, které se vztahuje ke spolupráci s organizacemi, komunitami a odbornými sdruženími, která se zabývají kybernetickou ochranou, výzkumem a výměnou informací o hrozbách, např. ISACA, FIRST, CSIRT/CERT a jiné týmy pro sdílení znalostí a zkušeností. Cílem je posílení obranyschopnosti organizace prostřednictvím sdílení informací, osvědčených postupů a nejnovějších trendů v kybernetické bezpečnosti. Obec zatím nenavázala členství se zvláštními zájmovými skupinami ani fóry. Rovněž toto opatření zatím není na obci nikterak řešeno.

A1 – 5.7 Zpravodajství o hrozbách

Threat Intelligence zahrnuje sběr, analýzu a využití informací o kybernetických hrozbách k ochraně organizace před útoky. Podstatou opatření je schopnost obce detekovat, předcházet a reagovat na kybernetické hrozby na základě aktuálních a relevantních informací. Obec by měla pravidelně sledovat aktuální zpravodajství o hrozbách. Tímto úkolem je vhodné pověřit určitou osobu, nejlépe manažera kybernetické bezpečnosti.

A1 – 5.8 Informační bezpečnost v řízení projektů

Principy informační bezpečnosti, a s nimi související opatření, musí být začleněny do celého životního cyklu všech projektů. Obec se řízením projektů zabývá jen okrajově a tuto oblast řeší spíše dodavatelsky, kdy je odpovědnost za informační bezpečnost v řízení projektů přenesena na dodavatele.

A1 – 5.9 Evidence informací a dalších souvisejících aktiv

Tímto opatřením je systematická identifikace, klasifikace a správa informačních aktiv a souvisejících technických i organizačních prostředků za účelem ochrany před kybernetickými hrozbami. Zpracováním přehledu o kritických informačních aktivech, může organizace minimalizovat bezpečnostní rizika. V organizační směrnici o řízení informační bezpečnosti, jsou v kapitole „Klasifikace dat“, data, se kterými obec pracuje, rozdělena a klasifikována do tří stupňů. Zabezpečení a ochranu dat jednotlivých stupňů zajišťují příslušní původci, uživatelé a správce IS. Podrobnější identifikace druhů dat, se kterými organizace pracuje, je přílohou předmětné směrnice. Není však zpracován a zdokumentován katalog aktiv, tak jak to vyžaduje metodika NÚKIB. Není tedy jasné, kdo je odpovědný za dané aktivum a jaké je jeho hodnocení z hlediska bezpečnosti.

A1 – 5.10 Přípustné používání informací a dalších souvisejících aktiv

Opatření definuje pravidla a zásady, které minimalizují rizika spojená se zneužitím, únikem nebo kompromitací dat. Jak bylo řečeno v předchozí kapitole, organizace má klasifikována data do tří stupňů. Ovšem není vůbec řešeno, kdo s jakými daty může pracovat, disponovat, nakládat, kdo a do jakých systémů má přístup atd. Zaměstnanci, ale ostatní zainteresovaní, by měli mít přístup pouze k těm informacím a systémům, které jsou nezbytné pro jejich práci. Každý zaměstnanec by měl být odpovědný za ta data, se kterými je oprávněn pracovat, a při práci s nimi je rovněž odpovědný za dodržování bezpečnostních pravidel. Toto samozřejmě platí obdobně i při používání souvisejících aktiv.

A1 – 5.11 Vrácení aktiv

Jedná se o proces, který v rámci řízení kybernetické bezpečnosti zajišťuje, že při ukončení pracovního poměru, změně pracovních povinností nebo při vyřazení technických prostředků nedojde k narušení informační bezpečnosti organizace. Tento proces se týká jak fyzických zařízení (např. notebooky, mobilní telefony, USB disky), tak digitálních aktiv (přístupové údaje, šifrovací klíče, software atd.). Opatření je řešeno ze strany zaměstnanců IT oddělení.

Aktiva jsou vydávána a navracena zpět těmto IT zaměstnancům. Proces vydávání a vracení aktiv však není nijak písemně zdokumentován a je založen spíše na důvěře.

A1 – 5.12 Klasifikace informací

Klasifikace informací slouží k určení citlivosti a hodnoty dat, a tím i k nastavení odpovídajících bezpečnostních opatření. Klasifikace probíhá podle tzv. triády CIA, tedy důvěrnosti, integrity a dostupnosti. Zodpovědně zpracovaná klasifikace informací pomáhá organizacím chránit důležité informace před neoprávněným přístupem, ztrátou nebo zneužitím. Obec má ve své směrnici o IB uvedeno, že bezpečnost informací znamená zajistit zachování CIA.

Zajištění důvěrnosti informací znamená, že informace je přístupná pouze těm uživatelům, kteří mají oprávnění k ní mít přístup.

Zajištění integrity informací spočívá v zajištění přesnosti a kompletnosti informací a metod jejich zpracování.

Zajištění dostupnosti informací znamená, že jsou informace a s nimi spojená informační aktiva uživatelům přístupná v době, kdy je potřebují.

Ovšem samotné opatření není nikterak blíže specifikováno. Zajištění důvěrnosti, integrity a dostupnosti je ve směrnici pouze uvedeno. Není zpracován a písemně zdokumentován postup pro zajištění požadovaných vlastností informační bezpečnosti CIA.

A1 – 5.13 Označování informací

Proces označování informací spočívá v jednoznačném označení dokumentů, dat, souborů a dalších informačních aktiv tak, aby bylo zřejmé, jak se má s nimi nakládat a kdo je oprávněn s nimi nakládat. Jak bylo popsáno v kapitole A1 – 5.9 obec má rozděleny informace podle jejich citlivosti do tří stupňů. Samotné informace jsou charakterizovány v příloze č. 3 směrnice o IB ve formě seznamu. Jejich zpracovatel „je“ informován o tom, že například informace, která zrovna zpracovává, jsou informace citlivé. V rámci opatření by tedy měl být zpracován i postup, jakým způsobem budou informace označeny.

A1 – 4.14 Předávání informací

Předávání informací, ale i jejich příjem, je nedílnou součástí každodenních procesů. Bezpečné předávání informací je velmi důležité nejen pro zachování důvěry a integrity dat, ale také pro ochranu citlivých informací před neoprávněným přístupem, ztrátou nebo zneužitím. Obec předává informace ve dvou základních úrovních. První je předávání na

úrovni zabezpečených registrů veřejné správy. Jedná se např. o registr obyvatel (ROB) registr osob (ROS) registr územní identifikace, adres a nemovitostí (RÚIAN). Druhá úroveň funguje na bázi předávání informací na žádost mezi odbory obce, na žádost jiných orgánů veřejné správy (např. policie, soud), předávání ze zákonné povinnosti (např. statistiky), na žádost v právním zájmu (účastník správního řízení) atd. V organizační směrnici o IB jsou v Příloze č. 1 – Pravidla bezpečného chování zaměstnanců v kapitole č. 2 - Pravidla pro bezpečnou práci s důvěrnými informacemi, stanovena pravidla, která jsou po zaměstnancích při nakládání s informacemi požadována a rovněž, které činnosti jsou zakázány. Bylo by vhodné upřesnit, co je považováno za důvěrné informace. Toto není nikde v organizační směrnici blíže specifikováno a je na zaměstnanci, aby zvážil, zda informace, se kterými pracuje a předává je, lze považovat za důvěrné či nikoli. Lze vycházet pouze z obecných definicí uvedených v dostupných zdrojích.

A1 5.15 - Řízení přístupu

Řízení přístupu v souvislosti s kybernetickou bezpečností obce znamená soubor pravidel, procesů a technologií, které určují, kdo, kdy a jak může přistupovat k informačním systémům a citlivým datům. Smyslem řízení přístupu je zajistit, že pouze oprávněné osoby mají přístup k relevantním informacím a systémům, čímž se minimalizuje riziko neoprávněného přístupu. V organizační směrnici o IB jsou v Příloze č. 1 – Pravidla bezpečného chování zaměstnanců v kapitole č. 3 - Pravidla pro fyzickou bezpečnost, jsou stanovena pravidla, která jsou po zaměstnancích ve vztahu k fyzické bezpečnosti požadována. Tato pravidla jsou poměrně dobře nastavena. Mělo by být však jasně stanoveno, kdo a jak často bude dodržování těchto pravidel kontrolovat.

A1 – 5.16 Management identit

Systém pro správu identit slouží ke sjednocení a řízení uživatelských účtů a přístupových oprávnění v rámci celého jejich životního cyklu z jednoho centrálního místa. Jeho úkolem je zajistit, aby přístup k informačním systémům a zdrojům měly pouze oprávněné osoby, a to ve správný čas, z oprávněných důvodů a s úplným dohledem nad těmito přístupy. Z hlediska bezpečnosti přispívá k ochraně důvěrnosti, integrity a dostupnosti dat. Správa tohoto systému probíhá prostřednictvím zásahů správce informačního systému.

A1 – 5.17 Autentizační informace

V prostředí obce představují autentizační informace soubor údajů a mechanismů sloužících k ověření identity uživatele při přístupu k informačním systémům a citlivým datům. Mezi

hlavní typy autentizačních informací patří např. hesla a přístupové údaje, digitální certifikáty, tokeny a čipové karty. V organizační směrnici o IB jsou v Příloze č. 1 – Pravidla bezpečného chování zaměstnanců v kapitole č. 4 - Pravidla pro přístupové kódy, jsou stanovena pravidla, která jsou po zaměstnancích ve vztahu k ochraně autentizačních informací požadována. Tato pravidla jsou stanovena velmi obecně a vztahují se víceméně na hesla a přístupové údaje. Pravidla by měla být více specifikována a rozšířena i na další používané autentizační informace, tedy na digitální certifikáty, klíče, tokeny a čipové karty.

A1 – 5.18 Přístupová práva

Přístupová práva určují, kdo, kdy, k jakým informacím či datům, a v jakém rozsahu může přistupovat v rámci informačních systémů a dat. Nastavení uživatelských přístupových práv v informačním systému musí být vždy omezeno na konkrétní část systému nebo na specifické datové a aplikační zdroje. Přístupová oprávnění jsou přiřazována jednotlivým zaměstnancům obce podle jejich potřeb, na jejich žádost se souhlasem vedoucího pracovníka, nebo přímo na žádost vedoucích pracovníků. Přidělená oprávnění je nutné řádně dokumentovat a pravidelně kontrolovat. Cílem těchto revizí je identifikovat neplatné přístupové účty, nesprávná oprávnění nebo změny ve vlastnostech systému. Kontrola přístupových práv by měla probíhat minimálně dvakrát ročně.

A1 – 5.19 Informační bezpečnost ve vztazích s dodavateli

Opatření zahrnuje ochranu citlivých dat a systémů při spolupráci s externími partnery, jako jsou IT služby, dodavatelé softwaru nebo provozovatelé infrastruktury. Důležité je uzavírání smluv s již implementovanými bezpečnostními požadavky, řízení přístupu dodavatelů k IT systémům a pravidelné audity jejich bezpečnostních opatření. Měli by být vybíráni pouze dodavatelé s prověřenou minulostí a také na základě odborných referencí. Výběr by měl probíhat vždy formou výběrového řízení, a to i u zakázek, u kterých by výběrové řízení nemuselo v souladu se zákonem proběhnout.

A1 – 5.20 Řešení informační bezpečnosti v dohodách s dodavateli

Řešení informační bezpečnosti v dohodách s dodavateli zahrnuje zakotvení bezpečnostních požadavků do smluv s externími partnery, aby byla chráněna citlivá data a IT systémy obce. Dohody by měly být uzavírány písemně a měly by obsahovat pravidla pro nakládání s daty, odpovědnost za bezpečnostní incidenty, omezení přístupových práv a povinnost dodržování platné legislativy. Každou dodávku IT služeb je nutné realizovat na základě uzavřené smlouvy, ve které již budou zaneseny bezpečnostní požadavky, za které dodavatel IT služeb

ručí. Je nutná pravidelná kontrola a audit dodržování těchto podmínek. Tímto se minimalizují rizika spojená s dodavatelskými vztahy.

A1 - 5.21 Management informační bezpečnosti v dodavatelském řetězci

Management, nebo také řízení, IT bezpečnosti v dodavatelském ve své podstatě znamená řízení a kontrolu bezpečnostních rizik spojených s externími dodavateli, kteří mají přístup k citlivým datům nebo IT systémům obce. Při tvorbě norem, legislativy nebo oborových doporučení pro řízení rizik v dodavatelských řetězcích, můžou být využity například normy ISO 28000 a další oborové normy.

A1 – 5.22 Monitorování, přezkoumávání a management změn dodavatelských služeb

Toto opatření obnáší průběžné kontinuální sledování a vyhodnocování bezpečnostních opatření dodavatelů s cílem zajistit ochranu IT systémů. Měli by být prováděny pravidelné přezkumy smluvních podmínek, audity bezpečnostních standardů a řízení změn v poskytovaných službách tak, aby odpovídaly aktuálním kybernetickým hrozbám a byly v souladu s platnou legislativou.

A1 – 5.23 Informační bezpečnost při používání cloudových služeb

Opatření zahrnuje ochranu citlivých dat a zajištění jejich dostupnosti, integrity a důvěrnosti při využívání externích cloudových platform. Cloudové služby, od datových úložišť až po sdílené aplikace a nástroje, nabízejí nepostradatelnou řadu výhod. Ovšem při jejich používání musí být zajištěna dostatečná bezpečnost takto zpracovávaných dat. V organizační směrnici o IB jsou v Příloze č. 2 – Cloudové služby, jsou stanovena pravidla, která zaměstnanci při používání těchto služeb musí dodržovat (např. šifrování), včetně povolených cloudových služeb. Rovněž jsou zde uvedeny cloudové služby, které jsou zakázány.

A1 – 5.24 Plánování a příprava managementu incidentů informační bezpečnosti

Smyslem je vytvoření strategie pro včasnou detekci, reakci a obnovu po bezpečnostních incidentech, jako jsou kybernetické útoky nebo úniky dat. Důležité je definování postupů, odpovědností a komunikačních kanálů, včetně školení zaměstnanců a pravidelného testování krizových scénářů. Dle směrnice o IB povinnosti spojené s řízením informační bezpečnosti, vykonává tajemník obce, který mj. přezkoumává bezpečnostní incidenty v organizaci. Není však stanoven bližší postup, jakým by mělo být toto opatření realizováno.

A1 – 5.25 Posuzování a rozhodování o událostech informační bezpečnosti

Podstatou je identifikace, analýza a klasifikace bezpečnostních událostí s cílem určit jejich závažnost a potřebnou reakci. Nejpodstatnější je rychlé vyhodnocení dopadu na systémy a data, koordinace odpovědných osob a případné eskalování incidentu podle stanovených postupů. V organizační směrnici o IB jsou v Příloze č. 1 – Pravidla bezpečného chování zaměstnanců v kapitole č. 0 - Úvodní ustanovení, je v odstavci č. 6 uvedeno následující Každý je povinen hlásit bezpečnostní incident správci IS. Bezpečnostní incident je událost, která může způsobit:

- narušení bezpečnosti informací v informačních systémech
- narušení bezpečnosti služeb a sítí elektronických komunikací
- únik důvěrných dat
- i jen podezření na bezpečnostní incident je incidentem!

Zaměstnanec má tedy povinnost hlásit bezpečnostní incident a je na správci IS aby posoudil závažnost tohoto incidentu a rozhodl o patřičných opatřeních. Je důležité, aby zaměstnanec byl s touto povinností obeznámen.

A1 – 5.26 Odezva na incidenty informační bezpečnosti

Jedná se koordinovaný dokumentovaný postup a soubor opatření k rychlému řešení bezpečnostních incidentů. Velmi důležité je okamžité zjištění a izolace hrozby, informování odpovědných osob, provedení analýzy a zavedení nápravných opatření pro minimalizaci škod. Jak bylo popsáno v předchozí kapitole A1 - 5.25, zaměstnanci musí hlásit všechny bezpečnostní incidenty správci IS. Měl by být písemně detailně popsán postup, jak se v dané situaci chovat a jaké jsou časové intervaly na provedení jednotlivých úkonů jak ze strany zaměstnance, tak ze strany správce IS.

A1 – 5.27 Poučení se z incidentů informační bezpečnosti

Opatření analyzuje a vyhodnocuje bezpečnostní incidenty. Úkolem je identifikace příčin a zavedení vhodných preventivních opatření. Důležité je dokumentovat průběh incidentu, zjistit slabá místa v bezpečnostních procesech a implementovat vylepšení, například úpravu politik, školení zaměstnanců nebo technická opatření.

A1 – 5.28 Shromažďování důkazů

Cílem je systematické získávání, uchovávání a analýza digitálních stop souvisejících s bezpečnostními incidenty. Podstatou opatření je zajistit integritu a důvěryhodnost důkazního materiálu pro interní vyšetřování nebo pro případné poskytnutí důkazního materiálu orgánům státní správy (např. police, soudy). Důkazy by měli být shromažďovány odpovědnými pracovníky. Tento postup je důležité zdokumentovat.

A1 – 5.29 Informační bezpečnost během narušení

Jedná se o vytvoření plánu, kterým se organizace řídí v době narušení informační bezpečnosti tak, aby byly udrženy informační služby na odpovídající běžné úrovni. Jedná se o vyhotovení krizového scénáře obce, který by měl obsahovat všechny možné druhy narušení a přijímaná opatření při těchto narušeních.

A1 – 5.30 Připravenost ICT na zajištění kontinuity činnosti organizace

Bezchybné fungování informačních a komunikačních technologií (ICT) je nezbytné pro zachování procesů organizace v kontextu digitalizace. Obec musí na základě kontinuity činnosti obce plánovat, zavádět, udržovat a testovat připravenost ICT.

A1 – 5.31 Zákonné, statutární, regulatorní a smluvní požadavky

Organizace by měla být zavázána plnit veškeré zákonné, statutární, regulatorní a smluvní požadavky v oblasti systému bezpečnosti informací. Plnění těchto požadavků by mělo být identifikováno, dokumentováno a pravidelně aktualizováno.

A1 – 5.32 Práva duševního vlastnictví

Opatření zahrnují ochranu autorských práv, patentů, obchodních značek a dalších nehmotných aktiv souvisejících s činností obce. Důležité je zajistit, aby obec legálně nakládala se softwarem, dokumenty a databázemi a zabránila neoprávněnému šíření chráněných materiálů. Vzhledem k tomu, že obec používá pouze software, který je pořizován legální cestou a z ověřených dodavatelských zdrojů, je toto opatření realizováno v souladu s předmětnou normou.

A1 – 5.33 Ochrana záznamů

Obec musí mít zabezpečeny úřední dokumenty, databáze a další informace proti neoprávněnému přístupu, ztrátě nebo zneužití. Důležité je dodržování legislativních požadavků na archivaci a skartaci, řízení přístupu k citlivým údajům a použití

bezpečnostních technologií, jako je šifrování nebo zálohování. Toto opatření je ze strany obce realizováno v několika úrovních. Ochrana záznamů je ošetřena v organizační směrnici o IB, konkrétně v kapitole č. 2. Dále je ošetřeno nakládání se záznamy ve spisovém a skartačním řádu obce a rovněž v platné legislativně, např. v zákoně o zpracování osobních údajů, tzv. GDPR.

A1 – 5.34 Soukromí a ochrana PII

Zkratku PII znamená v překladu osobně identifikovatelné informace (Personally Identifiable Information), v souvislosti s GDPR tedy osobní údaje. V kontextu informační bezpečnosti obce zahrnuje ochranu osobních údajů a soukromí občanů, ale i zaměstnanců a ostatních dotčených osob, před neoprávněným přístupem, zneužitím nebo únikem. Toto opatření je ze strany obce realizováno v několika úrovních stejně jako v předchozí kapitole A1 – 5.33.

A1 – 5.35 Nezávislé přezkoumání informační bezpečnosti

Opatření se vztahuje na audit nebo kontrolu bezpečnostních opatření, procesů a politik prováděnou externími nebo interními nezávislými subjekty. Cílem je identifikace slabých míst, ověření souladu s legislativními požadavky (např. GDPR) a doporučení ke zlepšení bezpečnostní strategie. Obec doposud nespádala do působnosti zákona o KB a proto se ni nevztahovalo ustanovení §7 ZoKB o povinných auditech. Tento bezpečnostní audit byl však na základě dobrovolnosti proveden nezávislou odbornou firmou v roce 2022.

A1 – 5.36 Dodržování politik, pravidel a norem pro informační bezpečnost

Všechny procesy, systémy a zaměstnanci obce by se měli řídit stanovenými bezpečnostními opatřeními, legislativními požadavky, a to jak interními dokumenty, tak i zákonnými předpisy. To zahrnuje dodržování stanovených politik informační bezpečnosti. Dodržování musí být pravidelně kontrolováno. Tyto kontroly by měli být zahrnuty do pravidelného plánu kontrol.

A1 – 5.37 Dokumentované provozní postupy

Jedná se jasně definované a písemně zaznamenané procesy pro práci s IT systémy, pro ochranu dat a řešení bezpečnostních incidentů. Tyto postupy zajišťují konzistentní a bezpečné nakládání s informacemi, minimalizují riziko lidské chyby. Tyto zdokumentované postupy by měli být zpřístupněny zaměstnancům dle jejich potřeby, ale hlavně by s nimi měli být aktivně seznamováni, např. na pravidelných školeních.

(zdroj: ČSN EN ISO/IEC 27001, 2023 a 27005, 2022)

PŘÍLOHA P II: OPATŘENÍ V OBLASTI LIDSKÝCH ZDROJŮ

A1 – 6.1 Prověřování

Prověřování lidských zdrojů zahrnuje kontrolu a hodnocení všech zaměstnanců i externích spolupracovníků. Hlavním smyslem tohoto procesu je snížit bezpečnostní rizika, a to nejen v oblasti informační bezpečnosti. Prověřování začíná ještě před samotným přijetím pracovníka, pokračuje při přidělování odpovídajících přístupových oprávnění a následným proškolením v oblasti informační bezpečnosti. Při přijímání nových zaměstnanců do příslušné obce se vyžaduje předložení výpisu z rejstříku trestů, a to i v případě pozic, u nichž to zákon explicitně nestanovuje. Dále musí kandidát doložit svůj životopis a poskytnout ověřitelné reference od předchozích zaměstnavatelů. Prověřování by mělo probíhat i v rámci zaměstnaneckého poměru, tedy nejen při začátku.

A1 – 6.2 Podmínky pracovního poměru

Opatření zahrnuje pravidla a závazky zaměstnanců, vztahující se k ochraně citlivých informací a dodržování pravidel IB. Tyto podmínky by měly být zakotveny v pracovních smlouvách, interních směrnících, ale i zákonné legislativě. Mohou obsahovat např. povinnosti týkající se mlčenlivosti, používání IT systémů. Noví zaměstnanci obce musí podstoupit vstupní školení, které zahrnuje online školení, ale i seznámení se s interními a legislativními předpisy. Zaměstnanci jsou proškoleni o svých povinnostech, tedy i o povinnostech v oblasti IB. U úřednických profesí je doložka mlčenlivosti zakotvena v zákoně o úřednících. U ostatních profesí je tato doložka součástí pracovní smlouvy.

A1 – 6.3 Povědomí, vzdělávání a školení o informační bezpečnosti

Zaměstnanci obce by měli soustavně zvyšovat znalosti a dovednosti v oblasti ochrany citlivých údajů a prevence kybernetických hrozeb. Pravidelná školení pomáhají zaměstnancům rozpoznat bezpečnostní rizika a správně reagovat na incidenty. Cílem je zajistit, aby všichni pracovníci rozuměli bezpečnostním politikám obce, dodržovali je a aktivně přispívali k informační bezpečnosti. Zaměstnanci vykonávající úřednické profese, mají dle zákona povinné školení. Územní samosprávný celek je povinen zajistit prohlubování kvalifikace a vypracovat plán vzdělávání, který obsahuje časový rozvrh prohlubování kvalifikace úředníka v rozsahu nejvýše 18 dní po dobu následujících tří let. Je však na úřednících, jakou oblast školení si zvolí. Nemusí se povinně vzdělávat v oblasti IT, což může být problém.

A1 – 6.4. Disciplinární řízení

Disciplinární řízení zahrnuje soubor opatření a sankcí za porušení bezpečnostních politik a pravidel při nakládání s citlivými informacemi nebo IT systémy. Jeho hlavním účelem je zajistit odpovědnost zaměstnanců za jejich jednání, a tím předcházet bezpečnostním incidentům způsobeným úmyslným počináním nebo nedbalostí. Disciplinární opatření mohou mít, podle závažnosti porušení či dopadu, podobu varování, finanční sankce nebo v závažných případech až ukončení pracovního poměru. Ve velmi závažných případech, může být porušení řešeno i v rovině trestně právní dle platné legislativy.

A1 – 6.5 Odpovědnost po ukončení pracovního poměru

Týká se ochrany důvěrných informací a dodržování bezpečnostních pravidel i po ukončení pracovního poměru zaměstnance obce. Týká se zejména závazku mlčenlivosti, vrácení přístupových prostředků (např. karet, tokenů) a zamezení neoprávněného přístupu k IT systémům. K navrácení aktiv a přístupových prostředků dochází ještě těsně před ukončením pracovního poměru. Zaměstnanci zařazení do obecního úřadu mají ze zákona povinnost zachovávat mlčenlivost ohledně informací, které získali při výkonu své práce, a které není možné v zájmu zaměstnavatele sdílet s dalšími osobami. Tato povinnost mlčenlivosti může být zrušena pouze rozhodnutím statutárního zástupce nebo jím pověřeného vedoucího pracovníka, pokud jiný právní předpis nestanoví něco jiného. Tato povinnost platí i po ukončení pracovního poměru.

A1 – 6.6 Dohody o důvěrnosti nebo mlčenlivosti

Jedná se o právně závazné dokumenty, které zavazují zaměstnance obce a externí spolupracovníky k ochraně citlivých informací a zabránění jejich neoprávněnému sdílení či zneužití. Tyto dohody stanovují povinnost mlčenlivosti jak během pracovního poměru, tak i po jeho ukončení, a mohou obsahovat i případné sankce za porušení. Vzhledem k tomu, že toto opatření řeší platné právní předpisy, nemusí být ze strany obce nikterak specificky řešeno. Co se týče externích spolupracovníků, jsou tyto povinnosti řešeny individuálně ve smluvních závazcích.

A1 – 6.7 Práce na dálku

Opatření zahrnuje pravidla pro bezpečné vykonávání pracovních povinností mimo kancelář např. služební cesty, práci v terénu, nebo z domova, tzv. home-office. V organizaci jsou stanovena pravidla, která stanovují, že při výkonu pracovních činností lze používat pouze aktiva poskytnutá zaměstnavatelem. Je-li tedy vykonávaná práce např. z domova, musí být

tato činnost povolena, a to pouze se zařízením, které je dodáno správcem IS obce, např. notebook. Dále je stanoveno, že síť, do níž je zařízení připojováno, musí být zabezpečena. Nelze se připojovat do nezabezpečené či neznámé sítě. Kontrolovat pracovní poštu lze i z osobního zařízení.

A1 – 6.8 Podávání zpráv o událostech informační bezpečnosti

Jedná se opatření, při kterém zaměstnanci hlásí bezpečnostní incidenty, podezřelé aktivity nebo narušení ochrany citlivých dat. Důležité je v této oblasti zavedení jasných postupů a komunikačních kanálů pro rychlé a důvěrné oznámení incidentů, což umožňuje jejich včasné vyhodnocení a minimalizaci dopadů. V organizační směrnici o IB je v příloze č. 1 – Pravidla bezpečného chování zaměstnanců, uvedeno v kapitole č. 0 – Úvodní ustanovení a vysvětlení pojmů, že každý je povinen hlásit bezpečnostní incident správci IS. Pro upřesnění je zde uveden telefonní kontakt na správce IS a emailová adresa. Bylo by vhodné uvedení čísla mobilního telefonu v případě, že by se správce IS nezdržoval v blízkosti pevné linky. Rovněž je nutná pravidelná edukace zaměstnanců o této povinnosti. Drtivá většina o této povinnosti neví. Možnosti je informační sdělení umístěné např. na monitoru.

(zdroj: ČSN EN ISO/IEC 27001, 2023 a 27005, 2022)

PŘÍLOHA P III: OPATŘENÍ FYZICKÉ BEZPEČNOSTI

A1 – 7.1 Perimetry fyzické bezpečnosti

Bezpečnostní perimetr je prostor, který odděluje a chrání zájmová aktiva subjektu (počítač, síť nebo systém) před možným nebezpečím. Fyzický bezpečnostní perimetr zahrnuje místnosti, budovu, prostory, části budovy. Ochrana perimetru např. zamčené dveře, brány, ploty, stěny, kamery atd. Zabezpečení fyzického perimetru lze rozdělit na dvě části, a to na pracovní dobu a mimopracovní dobu. Zabezpečení mimo pracovní dobu bylo popsáno v kapitole Popis budovy obecního úřadu a z pohledu bezpečnosti je na dobré úrovni. Ovšem zabezpečení v pracovní době, tedy v době, kdy je budova obce otevřena i pro veřejnost, je naprosto nedostačující. Nebezpečí plyne zejména ze skutečnosti, že se kdokoliv bez minimální kontroly, může volně pohybovat takřka po celé budově obce. Uvnitř budovy jsou naprosto nedostatečně zabezpečeny místnosti (kanceláře, ale i serverovna) pouze jednoduchými, v drtivé většině prosklenými, dřevotřískovými dveřmi, které nepřestávají pro případného útočníka žádnou překážku.

A1 – 7.2 Fyzický vstup

Fyzickým vstupem je rozuměn, např. přístup do budovy, do kanceláří, do místností s počítači, do serverovny, do kartoték atd., dále „zájmové prostory“. V současné době je v budově obce řízen přístup do zájmových prostor pomocí klasických klíčů a mechanických dveřních zámků. Klíče jsou přidělovány zaměstnancům dle kanceláře, ve které vykonávají pracovní činnost. Klíče pak umožňují zaměstnanci vstup pouze do jeho kanceláře a do příslušného patra, ve kterém se kancelář nachází. Klíčem nelze odemknout budovu obce ani jiné zájmové prostory. Vedení obce, určení zaměstnanci a také uklízečky mají přidělen tzv. univerzální klíč, se kterým je možné odemknout všechny zájmové prostory včetně budovy obce. Jediný elektronický přístup je umístěn na dveřích pro vstup zaměstnanců a je aktivován pomocí docházkového čipu. Z pohledu zabezpečení je tento systém zcela zastaralý a nejsou ním plněna daná opatření.

A1 – 7.3 Zabezpečení kanceláří, místností a vybavení

Zabezpečením zájmových prostor se rozumí ochrana fyzických prostor a zařízení před neoprávněným přístupem, krádeží nebo zneužitím. Jak bylo popsáno v kapitole A1 – 7.1 Perimetry fyzické bezpečnosti, zájmové prostory jsou na budovách obce chráněny nedostatečně, a to obzvlášť v pracovní době. Většina zájmových prostor má pouze dřevotřískové dveře s klasickým mechanickým zámkem bez bezpečnostního kování a s

klikami na obou stranách dveří. Dveře jsou navíc většinou prosklené s klasickým zalištováním, bez bezpečnostního skla. V kancelářích nejsou umístěny čidla PZTS. Okna jsou klasická, bez bezpečnostního skla a mříží. Bylo by vhodné zabezpečit alespoň jednotlivá patra, kdy by do těchto byl vstup možný např. na docházkový čip.

A1 – 7.4 Monitorování fyzické bezpečnosti

Monitorování fyzické bezpečnosti znamená nepřetržité sledování a kontrolu přístupu do budov, kanceláří a citlivých prostor za účelem ochrany informací, majetku ale i zaměstnanců. To zahrnuje využívání bezpečnostních kamer, elektronických přístupových systémů, alarmů atd. Ve všech budovách obce byly v roce 2024 instalovány kamery na obou vstupech do budovy, se záznamem tzv. 24/7. Žádné jiné monitorovací zařízení není v současné době nainstalováno. Neoprávněný vstup do zájmových prostor (např. serverovna) není nikterak monitorován.

A1 – 7.5 Ochrana před fyzickými a přírodními hrozbami

Opatření se vztahuje k minimalizaci rizik spojených s požáry, povodněmi, či jinými přírodními katastrofami. Žádná budova obce se nenachází v oblasti, kde by byla vyšší míra nebezpečí působení přírodních katastrof. V úvahu přichází snad jen úder bleskem či požár. Proti těmto hrozbám jsou budovy chráněny standardními prostředky. Zdroj elektrické energie je plně zálohován UPS.

A1 – 7.6 Práce v zabezpečených oblastech

Zabezpečená oblast je vymezený prostor uvnitř určitého objektu. Podle způsobu přístupu k utajovaným informacím se tyto oblasti člení na dvě kategorie. Třída I. zahrnuje prostory, kde již samotným vstupem dochází k přístupu k utajovaným informacím. Třída II. označuje prostory, kde vstup sám o sobě neznamena seznámení s utajovanými informacemi. V budovách obce se žádná zabezpečená oblast nevyskytuje, a proto není nutné přijímat žádná specifická opatření související s prací v těchto oblastech.

A1 – 7.7 Prázdný stůl, prázdná obrazovka

Opatření má za účel snížení rizika neoprávněného přístupu, ztráty a poškození informací na stolech, obrazovkách a dalších místech v kanceláři. V organizační směrnici o IB je v příloze č. 1 – Pravidla bezpečného chování zaměstnanců, je uvedeno v kapitole č. 3 – Pravidla pro fyzickou bezpečnost, že každý je povinen neponechávat IT vybavení, AAA média a papírové dokumenty s důvěrnými daty bez dozoru na veřejně dostupných místech - zásada prázdného

stolu vzhledem ke všemu, co lze fyzicky zneužít. Byla by vhodná kontrola dodržování tohoto opatření.

A1 – 7.8 Umístění a ochrana zařízení

Účelem umístění je fyzická a technická ochrana IT a kancelářského vybavení, aby se minimalizovalo riziko poškození přírodními hrozbami, neoprávněným přístupem, jiným poškozením nebo krádeží. Umístění a ochrana zařízení není v obci nikterak specificky řešena. Zařízení je umisťováno dle momentálních potřeb a dle dispozičních možností, např. napájení proudem, dostupnost sítě atd. Bylo by vhodné vytvořit pravidla dle tohoto opatření.

A1 – 7.9 Bezpečnost aktiv mimo prostory organizace

Jedná se o IT aktiva, která jsou používána mimo budovu obce, například při práci na dálku nebo služebních cestách. Opatření zahrnuje fyzické zabezpečení notebooků a mobilních zařízení a dodržování bezpečnostních zásad s cílem zabránit neoprávněnému přístupu, zneužití nebo krádeži informací. Aktiva, která jsou využívána k pracovním účelům mimo prostory obce, jsou jen v majetku organizace. Soukromá aktiva nelze k pracovním účelům využívat. Správce IS předá zaměstnanci aktivum, které je zabezpečeno s přihlédnutím k možným rizikům, která vyplývají z jeho použití. Zaměstnanec je poučen o bezpečnostních opatřeních při použití aktiva.

A1 – 7.10 Paměťová média

Mezi paměťová média se řadí např. paměťové karty, pevné disky, flash disky, ale i CD nebo DVD disky. Tato média slouží k ukládání, zálohování či přenosu virtuálních dat. Ve směrnici o IB je uvedeno pravidlo, že důvěrná data sdílet pouze přes schválená úložiště. Je zakázáno používat přenosná média (přenosné harddisky, flashdisky, CD/DVD) pro interní sdílení důvěrných dat. Pro externí sdílení, pro archivační účely a pro uložení dat do spisu je povoleno používat pouze přenosná média schválená pracovníky IT. Přenosná archivační média nesmí opustit prostory organizace. Vždy je nutné prověřit media vkládaná a připojovaná do PC/notebooku na přítomnost virů.

A1 – 7.11 Podpůrné služby

Podpůrné služby se týkají zejména infrastruktury, systémů a procesů, které podporují fungování informačních systémů organizace. Jedná se zejména o dodávky elektriny, telekomunikační služby atd. Obec má zálohovány dodávky elektrické energie pomocí

vlastního záložního zdroje UPC. Rovněž je možnost připojení generátoru poháněného spalovacím motorem.

A1 – 7.12 Bezpečnost kabelových rozvodů

Bezpečnost kabelových rozvodů je velmi důležitá pro ochranu informací, které jsou prostřednictvím těchto kabelů přenášeny. Kabeláž IT může být cílem odposlechu, manipulace nebo fyzického poškození s cílem znemožnění poskytování služeb. Kabeláž IT je v budovách obce vedena, v drtivé většině, v instalačních lištách tzv. pod omítkou. Jednotlivé výstupy jsou zakončeny zásuvkou typu RJ 45, která se nachází v blízkosti připojovaného aktiva. Na chodbách se ovšem nacházejí kabelové instalační šachty, které jsou zakryty pouze plastovým krytem, zajištěným pouze šroubky. Tyto šachty by měli být zabezpečeny proti neoprávněnému přístupu.

A1 – 7.13 Údržba zařízení

Údržba zařízení zahrnuje pravidelné servisní a bezpečnostní kontroly IT a kancelářského vybavení s cílem zajistit jeho spolehlivost kontinuitu poskytovaných služeb. Údržba zahrnuje revize, aktualizace softwaru a firmwaru, opravy hardwaru, kontrolu zabezpečení a bezpečné vyřazování nefunkčních a zastaralých zařízení. V obci probíhají periodické kontroly, které jsou naplánovány v souladu s interními předpisy nebo v souladu s platnou legislativou. Rovněž je stanoven plán na obnovu IT a kancelářského vybavení. Tato obměna probíhá rovněž periodicky nebo v případě potřeby výměny za nefunkční nebo poškozené zařízení. Bylo by vhodné zavést pravidelné kontroly aktualizací veškerého instalovaného software na jednotlivých pracovních stanicích.

A1 – 7.14 Bezpečná likvidace nebo opakované použití zařízení

Opatření má za cíl zabránění neoprávněnému přístupu k citlivým datům při vyřazování nebo znovupoužití IT a kancelářského vybavení. Toto obnáší bezchybné mazání dat ověřenými metodami, fyzickou likvidaci pevných disků a elektronických nosičů nebo jejich bezpečné přeformátování pro případné další použití. Bezpečná likvidace probíhá v obci prostřednictvím správce IT. Správce IT přebere od zaměstnance aktivum, které je určeno k likvidaci a toto zařízení bezpečně zlikviduje, nebo jej připraví k bezpečnému opakovanému použití, např. v jiné organizaci.

(zdroj: ČSN EN ISO/IEC 27001, 2023 a 27005, 2022)

PŘÍLOHA P IV: TECHNOLOGICKÁ OPATŘENÍ

A1 – 8.1 Koncová zařízení uživatele

Označují zařízení, která používají uživatelé k přístupu k sítím a datům, například počítače, notebooky, chytré telefony nebo tablety. Tato zařízení představují zranitelný bod bezpečnosti, protože mohou být cílem útoků, malware nebo neoprávněného přístupu. Všechna koncová zařízení opatřena antivirovou ochranou, řízením přístupu a pravidelnou aktualizací veškerého nainstalovaného software. K zabezpečení síťového provozu je nainstalován firewall. Měla by být naplánována pravidelná kontrola aktualizací a pravidelná údržba těchto zařízení pracovníky IT.

A1 – 8.2 Privilegovaná přístupová práva

Jedná se o práva, která uživatelům nebo systémům umožňují provádět kritické operace, jako je správa systémů, instalace softwaru nebo změna bezpečnostních nastavení. Přístupová práva jsou řízena způsobem, kdy běžní zaměstnanci mají omezená přístupová práva, nemůžou např. instalovat software, měnit způsob zabezpečení, měnit přístupová práva jiným zaměstnancům atd. Neomezená přístupová práva mají správci IT a vybraní zaměstnanci.

A1 – 8.3 Omezení přístupu k informacím

Opatření má za cíl řízení toho, kdo může přistupovat k citlivým datům a systémům. Chráněné informace by měli být dostupné pouze oprávněným osobám dle principu nejmenších oprávnění. Přístup k různým druhům informací je řízen dle pracovních potřeb jednotlivých zaměstnanců obce. Požadavek na přístup vznáší zaměstnanec, potažmo vedoucí odboru, a správce IS tento přístup umožní. Bohužel neexistuje žádná databáze, ve které by bylo uvedeno, ke kterým informacím mají jednotliví zaměstnanci umožněn přístup. Pokud je tedy zaměstnanci zřízen přístup k určitému druhu informací, po přeřazení na jinou pracovní pozici není upraven přístup k informacím.

A1 – 8.4 Přístup ke zdrojovému kódu

Přístup ke zdrojovému kódu znamená kontrolu nad tím, kdo může zobrazit, upravovat nebo spravovat zdrojový kód určitého softwaru. Neřízený přístup může vést k únikům, zneužití nebo vnesení škodlivého kódu. Přístup ke zdrojovému kódu software není nikterak řešen, a to jak po stránce pouhého čtení zdrojového kódu, tak ani po stránce zápisu nebo změny zdrojového kódu. Nicméně se jedná o tak specifické operace, které běžný zaměstnanec není

schopen provádět. Jiné osoby by musely mít přístup k software nebo hardware, čemuž by měla bránit jiná opatření.

A1 – 8.5 Bezpečná autentizace

Jedná se o proces ověřování identity uživatele nebo systému pomocí bezpečných metod, jako je více faktorová autentizace (MFA), biometrie nebo jednorázové kódy. Opatření má za cíl zabránit neoprávněnému přístupu k citlivým datům a systémům. K přístupu do všech programů a systémů je vyžadováno ověření pomocí hesla. Heslo k přístupu do sítě je povinně nutné obměňovat v daných časových intervalech. Do ostatních programů není tato pravidelná obměna vyžadována. Nejsou stanovena pravidla pro obsahovost hesla, což může být zásadní problém, neboť může být zaměstnancem udáváno heslo snadno prolomitelné. Více faktorová autentizace pak není aplikována takřka vůbec.

A1 – 8.6 Management kapacit

Účelem je plánování, monitorování a optimalizace výkonu IT systémů tak, aby byly schopny bezpečně zvládnout požadovanou zátěž. Opaření spočívá v předcházení výpadkům, přetížení nebo zranitelnostem vyplývajícím z nedostatečných zdrojů. Kapacity IT systémů jsou na pravidelně monitorovány a jsou rovněž plánována jejich pravidelná obměna, za novější zařízení s vyšší kapacitou. V případě zjištění neočekávaného přetížení IT systémů lze bez problémů tento nedostatek řešit, například výměnou za výkonnější aktivum.

A1 – 8.7 Ochrana před škodlivým softwarem

Ochrana před škodlivým softwarem zahrnuje opatření k detekci, prevenci a odstranění malware, jako jsou např. viry, trojské koně nebo ransomware. Toto opatření obnáší použití antivirových programů, firewallů, aktualizací softwaru. Na všech používaných IT zařízeních je instalován pravidelně aktualizovaný antivirový program od společnosti ESET. K ochraně sítě je instalován firewall a veškerý používaný software je pravidelně aktualizován. Nedostatek lze spatřovat v tom, že si zaměstnanec může antivirový program nekontrolovaně vypnout a nemusí reagovat na potřebné aktualizace.

A1 – 8.8 Management technických zranitelností

Opatření zahrnuje identifikaci, hodnocení a odstranění slabin v IT systémech, které by mohly být zneužity útočníky. Management technických zranitelností zahrnuje přesně zpracovaný seznam všech IT aktiv, jejich dodavatele, aktuální nasazení, odpovědnou osobu, a rovněž zahrnuje pravidelné skenování zranitelností, nasazování bezpečnostních záplat a aktualizací

softwaru s cílem minimalizovat riziko zranitelnosti. Tento management by měl být realizován, kdy by měl být zpracován a pravidelně aktualizován seznam všech aktiv.

A1 – 8.9 Management konfigurací

Řízení konfigurací zajišťuje dohled nad nastavením IT systémů tak, aby odpovídalo stanoveným bezpečnostním požadavkům. Jejím cílem je zajistit, že konfigurace zůstane konzistentní a nebude nechtěně nebo neoprávněně změněna, což by mohlo ohrozit stabilitu nebo bezpečnost systémového prostředí. Management konfigurací vyžaduje ustanovení, dokumentování a monitorování včetně přezkumu.

A1 – 8.10 Vymazání informací

Mazání informací spočívá v odstranění dat z informačních systémů, zařízení nebo jiných paměťových médií tehdy, když již nejsou nadále využívána. Tento proces musí být proveden tak, aby nebylo možné data následně obnovit nebo jakkoliv zneužít neoprávněnými osobami. Veškeré informace uložené v informačních systémech jsou spravovány správci IS. Tito správci jsou zodpovědní za toto opatření a provádějí vymazání těch informací, které již nejsou potřebné.

A1 – 8.11 Maskování dat

Maskování dat má za úkol omezit nechtěné vystavení citlivých údajů včetně PII v souladu s platnou legislativou (GDPR). Informace a data, která obsahují citlivé údaje, a při práci s nimi může dojít k jejich vystavení, jsou v souladu s platnou legislativou anonymizována. Jedná se na příklad o povinně zveřejňované informace podle zákona č. 106/1999 Sb. o svobodném přístupu k informacím. Citlivá data, se kterými je nutno nakládat, např. poskytnutí jiným orgánům státní správy, jsou povinně šifrována.

A1 – 8.12 Prevence úniku dat

Únikem dat je situace, kdy dojde k neoprávněnému zpřístupnění citlivých, důvěrných nebo osobních informací ze systémů nebo sítí daného subjektu nějaké neoprávněné osobě. Prevence úniku dat má těmto situacím předcházet. Prevence úniku dat v organizaci obsahuje velké množství úkolů, které je nutno dodržet. Jedná se například o identifikaci a klasifikaci dat za účel jejich ochrany, monitorování kanálů nebo karanténu dat obsahující citlivé údaje atd. Tato opatření by měla být v obci zavedena, jako prevence úniku dat.

A1 – 8.13 Zálohování informací

Jedná se o vytváření kopií dat za účelem jejich obnovy v případě ztráty, poškození nebo kybernetického útoku. Zálohy mohou být ukládány lokálně, na externích úložištích nebo v cloudu a měly by být chráněny před ztrátou, poškozením či kybernetickým útokem. Za tímto účelem musejí být zálohy pravidelně testovány. V obci je zaveden systém zálohování informací. Zálohování informací mají ve své gesci jak původci dat, tedy zaměstnanci, tak správci IT.

A1 – 8.14 Redundance vybavení pro zpracování informací

Redundance vybavení pro zpracování informací znamená použití záložních nebo duplicitních systémů, aby bylo zajištěno nepřetržité fungování IT infrastruktury při selhání hardwaru, softwaru nebo výpadku služeb. Typicky zahrnuje záložní servery, datová úložiště, síťové prvky a napájecí zdroje. Co se týče hardwarového vybavení, je redundance řešena způsobem, že většina zařízení je ihned k dispozici u správců IT. Tudíž je provedena okamžitá výměna vadného kusu za funkční. U softwarového vybavení je redundance řešena obdobným způsobem jako u hardwarového vybavení. Co se týče prvků sítě, tyto nejsou plně redundantní, obzvláště v případě kabelových rozvodů. Nicméně selhání těchto prvků je velmi nepravděpodobné, a proto je není třeba ani nikterak významně řešit.

A1 – 8.15 Zaznamenávání formou logů

Zaznamenávání formou logů znamená automatické ukládání událostí, akcí a přístupů v IT systémech za účelem monitorování a analýzy. Logy pomáhají identifikovat bezpečnostní incidenty, neoprávněné přístupy nebo systémové chyby. V obci prozatím není zavedeno komplexní řešení, které by shromažďovalo logy o událostech ze zařízení a aplikací na síti. Neexistuje tedy ani korelace se zpracovávanými daty v reálném čase.

A1 – 8.16 Monitorovací činnosti

Monitorovací činnosti zahrnují nepřetržité sledování a analýzu systémových událostí, síťového provozu a uživatelských aktivit za účelem detekce hrozeb a anomálií. Účelem je včasné odhalení a reakce na bezpečnostní incidenty. Monitorovací systém, který by byl nakonfigurován na základě stanovené základní linie tak, aby bylo možno identifikovat anomální chování, např. činnost spojenou se škodlivým softwarem, útoky, neobvyklé chování systému a jiné, není zaveden.

A1 – 8.17 Synchronizace hodin

Podstatou synchronizace hodin je udržování jednotného a přesného času na všech IT systémech v síti pomocí protokolů, jako je NTP (Network Time Protocol). Správná synchronizace je klíčová pro přesné logování událostí, analýzu bezpečnostních incidentů a správné fungování autentizačních a šifrovacích mechanismů. Synchronizace data a hodin je zavedena. Toto opatření je mj. nutné i pro konverzi formátů. Při převodu elektronického dokumentu, který byl doručen například ve formátu ZFO nebo EML, do papírové podoby je třeba zajistit, aby obsah tištěného dokumentu zcela odpovídal původnímu elektronickému originálu. Součástí tohoto procesu je také ověření shody obsahu obou verzí. V rámci této konverze je nezbytné doplnit systémové označení, tedy interní digitální podpis a časové razítko z agendového informačního systému (AIS), které slouží k prokázání autenticity a času provedení převodu.

A1 – 8.18 Používání privilegovaných obslužných programů

Privilegované obslužné programy mohou spouštět systémové nástroje s vyššími oprávněními, které umožňují správu, konfiguraci nebo diagnostiku IT systémů. Zneužití těchto programů může vést k narušení bezpečnosti, proto je důležité jejich řízení, omezení přístupu. Na obecním úřadu nejsou používány privilegované obslužné programy.

A1 – 8.19 Instalace softwaru na provozních systémech

Instalace softwaru na provozních systémech znamená nasazování aplikací (software), ale i aktualizací systému. Mělo by se jednat o kontrolovaný proces. Důležité je dodržování schválených postupů, omezení instalace pouze na důvěryhodný software a pravidelné aktualizace pro opravu zranitelností. Neoprávněná nebo neřízená instalace může vést k poškození provozního systému, nekompatibilitě nebo ohrožení stability systému. Z tohoto důvodu jsou k těmto úkonům oprávněni pouze správci IT. Ostatním zaměstnancům je tato činnost zakázána. Měla by být zavedena kontrola a dodržování tohoto opatření.

A1 – 8.20 Bezpečnost sítí

Bezpečnost sítí zahrnuje ochranu síťové infrastruktury před neoprávněným přístupem, útoky a zneužitím. Opatření lze realizovat za pomoci firewallů, šifrování, segmentace sítí, detekční a prevenční systémy a řízení přístupu. Na obecním úřadu je instalován firewall, který od sebe odděluje vnitřní a vnější prostředí, filtruje podezřelé aktivity, balancuje výkon a propouští pouze dovolené a schválené služby. Na přístupových bodech WiFi sítí je nastaveno šifrování WPA2. Nedostatečně je však řešena segmentace sítí, detekční a prevenční systémy.

A1 – 8.21 Bezpečnost síťových služeb

Bezpečnost síťových služeb zahrnuje identifikaci a zavedení bezpečnostních opatření nezbytných pro konkrétní služby, jako jsou bezpečnostní prvky, úrovně služeb a požadavky na služby. Organizace musí zajistit, aby poskytovatelé síťových služeb tato opatření implementovali. Obec vypsala výběrové řízení, ve které požadovala nabídku na vybudování hlasové a datové sítě včetně virtuální IP sítě s šifrováním pro potřeby hlasové a datové komunikace. Součástí poptávky byl i nový komunikační systém pro obec a její příspěvkové organizace. Nový systém byl realizován firmou STAND CZ spol. s r. o. Systém využívá pro telefonní a datovou konektivitu jednu přípojku internetu a telefonní sítě ISDN/VoIP v budově obecního úřadu.

A1 – 8.22 Oddělení sítí

Oddělení sítí (network segmentation) je bezpečnostní a výkonnostní strategie, která rozděluje skupiny informačních služeb, uživatele a informační systémy na menší, izolované části sítě. Je vhodné rozdělit jednotlivé broadcast domény na menší segmenty, nejlépe pomocí jednotlivých VLAN. Z bezpečnostního hlediska je rozdělení sítě na menší segmenty vhodné proto, že umožňuje efektivnější řízení přístupů do jednotlivých částí sítě a lepší kontrolu komunikace mezi těmito segmenty. Důležité je rovněž pravidelně sledovat, zda reálný síťový provoz odpovídá stanoveným bezpečnostním politikám.

A1 – 8.23 Filtrování webových stránek

Opatření má za cíl kontrolu a omezení přístupu zaměstnanců k určitým webovým stránkám na základě bezpečnostních politik organizace. Používá se k blokování škodlivých, nevhodných nebo neproduktivních webů pomocí firewallů, proxy serverů nebo specializovaných filtrů. Filtrování webových stránek, mimo stránek, které jsou všeobecně označovány za nebezpečné, prozatím není aplikováno.

A1 – 8.24 Používání kryptografie

Používání kryptografie obnáší šifrování dat a komunikace za účelem zajištění jejich důvěrnosti, integrity a autenticity CIA. V praxi se využívají metody jako symetrická a asymetrická kryptografie, digitální podpisy nebo hashovací funkce. Účelem je ochrana citlivých informací. V současné době je neautorizovanému čtení bráněno právy na síťových discích na úrovni filesystemu. Ve směrnici od IB je uvedeno, že na všech zařízeních, či datových médiích, která mají přístup nebo obsahují důvěrné informace, je nutno šifrovat data

na harddisku PC, na harddisku notebooku, přenosných harddiscích, flash discích, smartphonech a tabletech.

A1 – 8.25 Životní cyklus bezpečného vývoje

Podstata spočívá v začlenění bezpečnostních praktik do všech fází vývoje softwaru, od návrhu po nasazení a údržbu. Obsahuje kroky jako analýzu bezpečnostních požadavků, bezpečné programování, testování zranitelností a pravidelné aktualizace. Obec se nezabývá vývojem software.

A1 – 8.26 Požadavky na bezpečnost aplikací

Účelem opatření je, aby při vývoji či pořizování aplikací byly identifikovány a řešeny všechny požadavky na informační bezpečnost. Správce IT je odpovědný za definici a kontrolu bezpečnostních požadavků ve vývoji a údržbě systémů. Jeho úkolem je mj. definovat bezpečnostní požadavky na zajištění důvěrnosti, integrity a dostupnosti, definovat požadavky na ochranu dat od návrhu systému, až po ukončení jeho činnosti, zajišťovat postupy pro pořizování a úpravy software.

A1 – 8.27 Princip architektury a inženýrství bezpečnostních systémů

Podstatou je návrh bezpečnosti ve všech vrstvách architektury, tedy datové, aplikační a technologické. Principy mají být stanoveny, dokumentovány a uplatňovány při všech činnostech inženýrství informačních systémů. V současné době na obecním úřadu neexistuje navržená ani zdokumentovaný princip architektury bezpečného inženýrství. Vytváření architektury informačních systémů by bylo vhodné řešit dodavatelsky.

A1 – 8.28 Bezpečné programování

Jedná se o soubor principů a postupů zaměřených na prevenci bezpečnostních zranitelností při vývoji softwaru. Obec se nezabývá vývojem software.

A1 – 8.29 Testování bezpečnosti při vývoji a akceptaci

Podstatou je proces ověřování v rámci celého životního cyklu vývoje, zda software nebo systém splňuje bezpečnostní požadavky a je odolný vůči hrozbám a útokům. Obec se nezabývá vývojem software.

A1 – 8.30 Vývoj zajišťovaný externími zdroji

Vývoj softwaru externími zdroji znamená, že organizace outsourcuje (svěří) část nebo celý vývojový proces třetím stranám (externím firmám či offshore týmům). Obec se nezabývá vývojem software.

A1 – 8.31 Oddělení prostředí vývoje atestování a produkce

Oddělení jednotlivých prostředí je zásadním principem bezpečného a stabilního vývoje softwaru. Zajišťuje izolaci různých fází vývoje, minimalizuje rizika nasazení chybných změn do produkce. Obec se nezabývá vývojem software.

A1 – 8.32 Management změn

Cílem managementu změn je proces řízení, dokumentace a kontrolování změn v IT systémech, softwaru nebo infrastruktuře. Účelem je minimalizovat rizika, výpadky a negativní dopady na provoz organizace. Doposud není zpracována žádná dokumentace, která by management změn v oblasti IT upravovala. Změny se v této oblasti dějí zpravidla až v době, kdy je změna vyvolána potřebou, například používáním již nedostatečného nebo zastaralého vybavení. Další změny se dějí po změně legislativy, kdy je na takovou změnu organizace povinna reagovat, například změna archivačního systému, změna systému stavebního řízení atd. Změny v oblasti IT se ovšem mohou dít i ze strany vedení obce. Jedná se například o reakci na nabídky firem, které poskytují softwarové vybavení pro obecní úřady. Mnohdy dojde ke změně takového IT systému, který může mít i negativní dopad na chod organizace.

A1 – 8.33 Informace pro testování

Testování je součástí vývoje softwaru a zajišťuje, že aplikace splňuje funkční i bezpečnostní požadavky. Obec se nezabývá vývojem software.

A1 – 8.34 Ochrana informací během auditního testování

Auditní testování zahrnuje důkladnou kontrolu a ověřování bezpečnosti, výkonu a souladu systému s předpisy. Během tohoto procesu může docházet k manipulaci s citlivými informacemi, což vyžaduje přijetí opatření k zajištění jejich ochrany. Bezpečnostní audit IT proběhl naposledy v roce 2022. Auditní testování není nikterak plánováno. V případě, že by bylo opětovně prováděno auditní testování, bylo by toto testování naplánováno a odsouhlaseno testovací entitou a vedením obce.

(zdroj: ČSN EN ISO/IEC 27001, 2023 a 27005, 2022)