Systém řízení bezpečnosti informací ve vybraném subjektu

Bc. Michaela Zelená

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Michaela Zelená**
Osobní číslo:	**L17138**
Studijní program:	**N3953 Bezpečnost společnosti**
Studijní obor:	**Bezpečnost společnosti**
Forma studia:	**prezenční**

Téma práce: **Systém řízení bezpečnosti informací vybraného subjektu**

Zásady pro vypracování:

1. **Zpracujte literární rešerši vztahující se k dané problematice s důrazem na monografie a analytické materiály.**
2. **Proveďte analýzu úrovně zabezpečení zvolené oblasti systému řízení bezpečnosti informací vybraného subjektu.**
3. **Na základě předchozí analýzy navrhněte případná opatření ke zkvalitnění stávajícího stavu.**
4. **Sumarizujte získané výstupy diplomové práce.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

[2] GDPR v kostce: praktický průvodce povinnostmi pro podniky a spolky. V Praze: C.H. Beck, 2018. ISBN 978-80-7400-704-0.

[3] KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[4] KRÁL, Mojmír. Bezpečný internet: chraňte sebe i svůj počítač. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- 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 UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona 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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 15.5.2019

Jméno a příjmení studenta: Bc. Michaela Zelená

.....
podpis studenta

ABSTRAKT

Práce se zaměřuje na systém řízení bezpečnosti informací ve vybraném subjektu. Teoretická část vymezuje základní pojmy a představuje problematiku bezpečnostní politiky a samotného řízení bezpečnosti informací. V praktické části je nejprve provedena základní charakteristika subjektu pomocí řízeného rozhovoru. Následně je analyzována úroveň zabezpečení informací v rámci vybraného subjektu a to pomocí auditu bezpečnostních opatření. Pro další poznání je provedena SWOT analýza na které je založen další postup. V návaznosti na zjištěné skutečnosti jsou identifikována a klasifikována aktiva a hrozby. Analýza rizik je provedena pomocí nástroje RISKAN a na základě mapy rizik jsou navrhnuta vhodná opatření. Výstupem práce je vyhodnocený audit bezpečnostních opatření a také dokumentace aktiv, hrozeb a rizik, na základě kterých byla navržena opatření vztahující se k zaměstnancům. Navržen byl bezpečnostní manuál obsahující vhodnou heslovou politiku a také pravidla pro práci na pracovišti.

Klíčová slova: analýza rizik, audit, bezpečnost informací, heslová politika, systém řízení bezpečnosti informací

ABSTRACT

This thesis is focused on safety management systém in chosen subject. Theoretical part defines basics terms and introduces problematics of safety politics and management of security of information. The practical part realizes elementary subject characteristics while using structured interview. Then the level of security of information is analyzed in chosen subject using Information Security audit. To understand topic more the SWOT analysis was done which was chosen as right strategy for next approach. Following facts that were found, assets and threats were identified and classified. Risk analysis is done using RISKAN tool, appropriate steps are suggested based on map of risks. The outlet of this thesis is information Security Audit, and documentation of assets, threats, risks, based on these was safety of human resources was suggested. Also the safety manual with proper passwords and essential safe procedures was suggested.

Keywords: Audit, Information Security, ISMS, Password Policy, Risk Analysis

Ráda bych poděkovala svému vedoucímu práce Ing. Petru Svobodovi za jeho cenný čas při vedení mé diplomové práce. Dále děkuji Ing. Jiřímu Dokulilovi, za jeho odborné rady a aktivní pomoc při odborných korekcích textu. Rovněž děkuji vybranému subjektu, za spolupráci a aktivní přístup.

V neposlední řadě významný dík patří také mé rodině a nejbližšímu okolí za podporu v průběhu celého studia a při zpracování této práce nevyjímaje.

Motto:

„Základem kvality je obyčejná poctivost.“

Ing. Jiří Chaloupka/Moravia

OBSAH

ÚVOD

Data jsou v dnešní době nepostradatelnou součástí všech procesů. Jejich prostřednictvím, můžeme definovat vše kolem nás. Mít správná data, ve správné kvalitě, v pravý čas pro nás může znamenat velkou výhodu. Ztráta dat však může vést k přesnému opaku, který může být až likvidační. V našem zájmu tedy jednoznačně je řádná péče o množství, kvalitu, celistvost, ale především bezpečnost. Pokud nebudou data splňovat tyto požadavky, nebudou ani informace spolehlivé a jednoznačné. To může vést až ke ztrátě důvěry v celou organizaci.

Informační systémy a informační technologie tvoří pro běžného uživatele již naprosto nepřehlednou změť vzájemně propojených prvků, které se snaží suverénně ovládat alespoň v omezeném rozsahu. Čím jsou však tyto systémy složitější a zpracovávané informace důvěrnější, roste nezbytnost zpracovávat přehledné dokumentace, které nám pomohou vše přehledně řídit – zavedení systému řízení bezpečnosti informací.

Cílem této práce je analýza úrovně zabezpečení informací v rámci vybraného subjektu (který z důvodu citlivosti zveřejňovaných údajů nebude konkrétně jmenován). V návaznosti na zjištěné skutečnosti budou navrhnuta opatření, která by tuto úroveň zabezpečení měla zvýšit.

Teoretická část se věnuje zejména problematice bezpečnosti informací a dále se pak zaměřuje na legislativní a normativní rámec, který je nezbytným podkladem pro tuto práci.

Praktická část nejprve prezentuje základní charakteristiky subjektu pomocí řízeného rozhovoru. Následně analyzuje úroveň zabezpečení informací v rámci vybraného subjektu a to pomocí auditu bezpečnostních opatření. Pro další poznání byla provedena SWOT analýza jejímž výstupem byla vhodná strategie pro další postup. V návaznosti na zjištěné skutečnosti byla identifikována a klasifikována aktiva a hrozby. Pro analýzu rizik byl vybrán nástroj RISKAN, výstupem je mapa rizik, na niž navazují vhodná opatření.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY

Tato kapitola osvětluje základní pojmy, které budou dále v práci užívány. Jedná se především o pojmy z oblasti kybernetické bezpečnosti. Pojmy jsou zejména definovány pomocí výkladového slovníku kybernetické bezpečnosti. [1]

- **Aktivní hrozba** je jakákoli hrozba úmyslné změny stavu systému zpracování dat nebo počítačové sítě. Tato hrozba by následně měla za následek úpravu zpráv, vložení falešných zpráv, vydávání se za někoho jiného nebo odmítnutí služby. [2]
- **Best practice** neboli příklad dobré praxe je osvědčený, efektivní postup či metoda, kterou lze využít k dosažení prozatím nejlepšího výsledku. Takovýto postup se vytříbí opakováním dané činnosti nejlépe mezi odborníky na danou problematiku. [1]
- **Bezpečnost informací** (dále jen „IFOSEC“) představuje oblast uplatnění obecných bezpečnostních opatření a postupů sloužících jak k ochraně informací před jejich ztrátou nebo kompromitací., případně k jejich zjištění a přijetí nápravných opatření k zachování dostupnosti informací a schopnosti s nimi dále pracovat v rozsahu, které umožňují opatření. Tato opatření zahrnují bezpečnost počítačů, přenosu, emisí a šifrovací bezpečnost, odhalování ohrožení nejrůznějších forem a možná preventivní činnost. [3]
- **Bezpečnostní politikou** se na úrovni organizace myslí zejména základní dokument, který vymezuje strukturu bezpečnostního rizika, definuje odpovědnost za ochranu informací v organizaci, a uvádí, jaké jsou úrovně ochrany informací. Na úrovni systému se poté jedná o soubor pravidel a praktik, které specifikují nebo regulují, jak systém nebo organizace poskytuje bezpečnostní služby, aby ochránil citlivé nebo kritické zdroje systému. [4]
- **Bezpečnostní incident** znamená porušení nebo možnou bezprostřední hrozbu porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu informační a komunikační technologie. [5]
- **Bluetooth** je bezdrátový komunikační standard, který slouží ke spárování zařízení, mezi které řadíme mobilní telefony, notebooky a kapesní počítače. Má větší dosah než zastaralý infračervený přenos. [2]
- **Botnet** je síť infikovaných počítačů, jejichž výkon se sčítá. Jedná se tedy o obrovský výpočetní výkon, který spravuje pouze jeden útočník. Jedná se o nezákonnou činnost ve velkém měřítku. [1]

- **Data** lze charakterizovat jako fakta, měření, obraz, zvuk, video, avšak v kontextu sledovaného procesu nebo situace. Mohou být rovněž chápána jako vstup či výstup počítačového programu. [6]
- **Informace** je znakovým projevem, který má smysl pro komunikátory i pro příjemce. Mohou to být uspořádaná, organizovaná, shrnutá a interpretovaná data. [1], [6]
- **Informační systém** je funkčním celkem, který má na starosti cílevědomé a systematické hromadění, zpracování, uchování a zpřístupňování informací a dat. Zastřešuje datové a informační zdroje, nosiče, hardwarové, softwarové a pracovní prostředky, technologie a postupy, související normy a pracovníky. [1]
- **Internet věcí** z anglického Internet of Things (dále jen „IoT“) je tvořen sítí fyzických předmětů – mobilních i pevně instalovaných, které jsou vybaveny pro komunikaci, monitorování, senzory nebo interakci s okolním prostředím. [7]
- **Nepopiratelnost** je schopností dokázat, že se stala událost nebo činnost, v rámci které známe dotčené subjekty, které ji vyvolaly. [1]
- **Slovníkový útok** je postup, při kterém jsou zjišťována hesla. Využívá se programu, který zkouší všechna slova ve slovníku. Rychlost postupu se odvíjí od velikosti slovníku a obětí se zpravidla stává osoba, která používá jednoduchá hesla. [1]
- **Šifrování** je kryptografická transformace dat, tedy nauka o metodách utajovaného smyslu zpráv převodem do podoby, která je srozumitelná pouze při speciálních znalostech. [8]
- **Operační technologie** (dále jen „OT“) jsou tvořeny hardwarem a softwarem, který detekuje změnu prostřednictvím přímého monitorování, případně řízení fyzických zařízení, procesů nebo událostí v podniku. [9]
- **Pseudonymizací** se rozumí proces, při kterém je kryta identita. Účelem je možnost shromažďovat další údaje týkající se stejného jednotlivce, aniž by bylo nutné znát jeho totožnost. Příkladem jsou údaje, které jsou kódovány pomocí klíče, kterým může být jméno, datum narození nebo adresa, jenž jsou uloženy odděleně. [3]
- **WiFi** je zkratkou pro wireless technology. Jedná se o bezdrátovou technologii, kdy jsou data roznášena „vzduchem“. Využívá se zejména tam, kde není možná instalace klasické kabelové sítě. K vytvoření je nezbytný vysílač a vhodně umístěné navazující přístupové body, které společně přenáší data. [1]

2 BEZPEČNOSTNÍ POLITIKA

Kapitola pojednává o základní charakteristice bezpečnostní politiky, zachycuje její důležitost a nutnost pro zabezpečení a ochranu dat. Dále představuje nejdůležitější právní předpisy.

2.1 Základní charakteristika bezpečnostní politiky

Bezpečnostní politika určuje souhrn požadavků, potřeb, směrnic, předpisů a zásad, které jsou definovány pro zabezpečení všech prvků informačního systému (dále jen „IS“), a to na všech úrovních přístupu tak jak budou odpovídat požadavkům a schopnostem organizace. De facto přesně stanovuje postup, který se bude plnit, pokud dojde k úniku informací a je tedy jasným argumentem proti možnému narušení důvěryhodnosti organizace, která by mohla vypadat jako nedostatečně zabezpečená. Pokud nebudujeme informační bezpečnost, nemůžeme očekávat, že vztahy s klienty či obchodními partnery budou důvěryhodné. [4],[5]

Informace jsou v podstatě aktiva a mají pro organizaci svou hodnotu. Je tedy třeba tyto aktiva chránit. Informační bezpečnost je zaměřena na velké spektrum hrozeb a zajišťuje kontinuitu činností organizace, přičemž buduje důvěryhodnost, minimalizuje obchodní ztráty a maximalizuje návratnost investic. [5], [8]

Je tedy třeba vytvořit základní dokument, který bude bezpečnostní politiku řešit. Tento dokument musí být závazný pro celou společnost a musí být schválen managementem. Průřezem je třeba definovat východiska pro všechny aktivity společnosti, a to nejen současné i budoucí aktivity, které se dotýkají informační bezpečnosti. Hlavním účelem však je definovat nejdůležitější cíle, které je třeba chránit a k nim vytvořit postup, jak je zabezpečovat společně s odpovědnými osobami, jež budou mít jasně vymezené pravomoci a odpovědnosti. V případě, kdy je bezpečnostní politika již vytvořena, je třeba rozpracovat zásady v oblasti informační bezpečnosti. [4], [5]

Obr. 1 Schéma dokumentu bezpečnostní politiky v organizaci. Zdroj: [vlastní]

Hlavní oblasti a principy IS se rozpracovávají velice podrobně. Tvoří se tzv. bezpečnostní standardy tedy závazné interní dokumenty společnosti. Zásadou je, že tyto standardy z bezpečnostní politiky vychází a, nesmí být s ní v rozporu. Bezpečnostní politika IS je relativně neměnný dokument. Bezpečnostní standardy se naopak v průběhu času mění. [4], [5]

Implementace se zpravidla provádí formou projektů, které je třeba realizovat tak, aby se bezpečnostní politika IS spolu s bezpečnostními standardy uvedla do praxe. Je tedy třeba popsat, jak ji konkrétně implementovat. Materiály pro zpracování by měly být dostupné již při tvorbě bezpečnostní politiky IS, což je také nejvhodnější čas tvorby. Je třeba, aby byly dodrženy parametry mezi, které patří následující: [4]

- Popis cíle a účelu.
- Priorita řešení.
- Popis výstupů.
- Popis projektových etap.
- Provázanost mezi projekty uvnitř organizace.
- Předpoklady a možná rizika.
- Odhad ceny a časové náročnosti. [4]

Významnou a často objevovanou chybou při tvorbě bývá, že je politika postavena na velkém množství kompromisů. Politika pak neumožní některé problémy řešit nebo nedokáže detekovat reálnou hrozbu. Jako další nešvarem se objevuje nereálnost politiky, tedy její vysoké nároky, které nelze naplnit. Pokud se chceme tomuto vyvarovat, je vhodné vytvořit přechodné období a implementovat postupně. Zaměstnanci si poté snadněji zvyknou na možné změny. [4]

Negativní vliv má také nepřiměřený rozsah politiky. V případě jejího přehnaně obšírného zpracování by hrozilo, že bude problém seznámit se podrobně se všemi body a schvalovací proces se tím zpomalí. Rovněž je třeba dbát na dostatečnou informovanost zaměstnanců a nekritické přejímání vzorů jiných politik. [4]

Je třeba také stanovit předběžný harmonogram, kde bude zřejmá návaznost jednotlivých projektů. V některých případech může být vhodný i souběh řešení projektů. [4]

Po vzniku bezpečnostní politiky by měla být oficiálně přijata a poté přichází čas seznámit s její podobou celou organizaci. Při schvalování nelze zapomenout na stanovení četností aktualizace dokumentu, ke které by nemělo docházet častěji než za dva roky. To však pouze v případě, kdy nedojde ke zjištění závažných pochybení, které by při současném stavu vedly k významnému nebezpečí. Odpovědnou osobou za přezkoumání a aktualizaci je zpravidla vlastník dané problematiky. Cílem je zlepšení řízení bezpečnosti informaci, ale také zpětná vazba tedy hlášení bezpečnostních incidentů. Zapracovat by se měly také změny legislativní povahy. [4], [5]

Všichni zaměstnanci musí být s tímto dokumentem srozuměni, a to alespoň s částmi, které souvisí s výkonem pracovní funkce v organizaci. Je dobré, rozčlenit zaměstnance do skupin podle shodnosti nebo alespoň podobnosti pracovních úkonů za účelem efektivnějšího školení. Školení je jednou z nejdůležitějších částí implementace. Pokud zaměstnanci dostatečně neporozumí postupům, které z politiky plynou, nebude nikdy dosaženo očekávaného efektu. [4], [5]

2.2 Bezpečnostní politika v právních předpisech

Základním právním dokumentem na území České republiky (dále jen „ČR“) je zákon č. 181/2014 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů, který vymezuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické

bezpečnosti. Specifikuje systém zajištění kybernetické bezpečnosti, základní pojmy, definuje stav kybernetického nebezpečí a také vymezuje možnost kontroly, nápravných opatření a přestupků v řešené oblasti. Nevztahuje se však na informační a komunikační systémy, které nakládají s utajovanými informacemi. Ty jsou upraveny zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů. [10], [11]

Ke zmíněnému zákonu o kybernetické bezpečnosti je třeba doplnit také prováděcí vyhlášku č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti bezpečnosti tedy tzv. vyhláška o kybernetické bezpečnosti. Nedílnou součástí v oblasti kybernetické bezpečnosti je také vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. [12], [13]

Důležitou mezinárodní normou, která aktuálně výrazně ovlivňuje legislativní prostředí je norma známá jako Nařízení Evropského parlamentu a Rady Evropské unie (dále jen „EU“) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu údajů - General Data Protection Regulation (GDPR) a o zrušení směrnice 95/46/ES., která z velké části nahrazuje stávající zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. Její součástí, zůstane pouze úprava aspektů týkajících se Úřadu pro ochranu osobních údajů jako je například jeho ustanovení či organizace a také některé dílčí záležitosti nutné k dotvoření celkového rámce ochrany osobních údajů. Tato nová mezinárodní norma je vzhledem ke své důležitosti podrobněji rozebrána v následující podkapitole. [2], [14], [15]

Nezbytná část zmíněné problematiky je také upravena v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Jedná se zejména o předem stanovené zásady pro klasifikaci informací jako informací utajovaných, dále podmínky pro přístup k nim a další požadavky na ochranu. Definuje také zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy. [16]

Na výše uvedenou problematiku navazuje zákon č. 101/2000 Sb., o ochraně osobních údajů, který má za úkol chránit každého před neoprávněným zasahováním do soukromí. Upravuje i práva a povinnosti při zpracování osobních údajů a také podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států. Zákon také zřizuje Úřad pro ochranu osobních údajů,

který je dozorovým úřadem pro oblast ochrany osobních údajů. Význam této oblasti vyplývá z mezinárodních smluv, které jsou součástí právního řádu. [17]

2.3 GDPR

Obecné nařízení o ochraně osobních údajů mění právní úpravu této problematiky pro všechny státy Evropské unie, ke kterým se přidává i Island, Norsko či Lichtenštejnsko. Tím se zaručuje jednotný Evropský postup a univerzální použitelnost. [2], [15]

Toto nařízení zakládá povinnosti, organizacím, které osobní údaje zpracovávají. Označuje je souhrnným pojmem „správce osobních údajů“, a to ať už se jedná o údaje vlastní nebo převzatá za účelem zpracování. Toto nařízení se tedy vztahuje i na dozorové úřady jako je Úřad pro ochranu osobních údajů. Nevztahuje se však na činnost fyzických osob a orgány, které vyšetřují, odhalují či stíhají za trestné činy, výkon trestu nebo provádějí preventivní činnost. Bylo však přesto nutné novelizovat zákon č. 273/2008 Sb., o Policii České republiky. [2], [14]

Nově je třeba brát na vědomí.:

- Povaha.
- Rozsah.
- Kontext.
- Účel zpracování.
- Možný dopad na práva a svobody fyzických osob.
- Zabezpečení dat. [2], [14]

Organizaci nyní musí zvážit jaká je míra ohrožení práv a svobod fyzických osob tzv. „subjekt údajů“ při bezpečnostním incidentu. Na základě toho totiž záleží na správci osobních údajů, zda tento incident ohlásí či nikoli. [2], [14]

Zavedl se také tzv. „správce“. Správcem se rozumí subjekt, který specifikuje účely a prostředky zpracování osobních údajů a za zpracování primárně odpovídá. Může jím být jakýkoli subjekt, tedy i fyzická osoba. Správce si může najmout zpracovatele, který pro něj bude provádět požadované operace s údaji. Tyto operace jsou výslovně definovány (omezeny) při pověření zpracovatele správcem. Oba subjekty mohou být jakékoli právní formy. [2][14]

Nařízení se zakládá na zásadách, mezi které patří.:

- **Zákonnost, korektnost a transparentnost,** kde správce musí zpracovávat osobní údaje na základě právního důvodu, a to naprosto transparentně vůči subjektu údajů.
- **Omezení účelu,** pro který budou osobní údaje shromažďovány, tedy je třeba existence legitimního právního důvodu. [2][14]
- **Minimalizace údajů,** které musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou shromažďovány a následně zpracovávány.
- **Přesnost** osobních údajů.
- **Omezení uložení,** tedy znemožnění hromadění údajů a ukládání údajů po dobu delší nežli je to pro zpracování nebo splnění legitimního důvodu nutné.
- **Integrita a důvěrnost,** čímž se rozumí technické a organizační zabezpečení osobních údajů. [2], [14]

Jako důkaz splnění těchto zásad je třeba vypracovat záznamy o činnostech zpracování a také kodexy a osvědčení. [2], [14]

Nejsou však stanoveny podmínky šifrování ani pseudonymizace při zpracování osobních údajů. Jsou brány jako bezpečnostní prvek, který zmírní následky úniku údajů, proto nabádá k jejich používání, ale neukládá je povinně. Může se jednat o rozhodující faktor v případě oznámení úniku, kdy v případě použití prvku nebude nutné oznámení učinit. Klíčové je zvážení a posouzení situace. [2], [14]

Zřídil se také tzv. „pověřenec“, který poskytuje informace a poradenství správci či zpracovateli, včetně zaměstnanců, kteří s údaji nakládají. Pověřenec také monitoruje soulad interních a dalších norem s normou mezinárodní. Na vyžádání může posuzovat vliv na ochranu osobních údajů a spolupráci s Úřadem pro ochranu osobních údajů. Jako osoba musí disponovat profesními kvalitami a odbornou znalostí práva. Dalšími nutnými předpoklady jsou praxe v oblasti ochrany osobních údajů a dostatečná znalost GDPR. [2], [14]

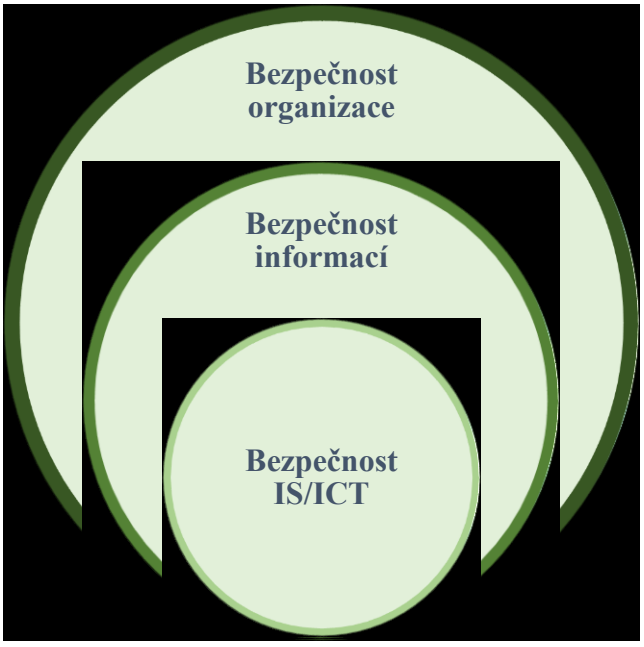
3 BEZPEČNOST INFORMACÍ

Kapitola se skládá ze základní charakteristiky problematiky bezpečnosti informací a představuje základy řízení bezpečnosti informací, které mají základ v metodikách, jenž jsou v rámci kapitoly rovněž představeny. Dále je zde rozveden i systém řízení bezpečnosti informací, kde jsou nastíněny základní náležitosti pro implementaci takového systému a příslušné technické normy, které tuto oblast zastřešují. [18]

Bezpečnost informací je především ochranou důvěrnosti, integrity a dostupnosti informací. Lze do ní ale zahrnout také další atributy - například autenticitu, odpovědnost, nepopiratelnost a spolehlivost. [1], [18]

Jedná se zejména o uplatnění obecných bezpečnostních opatření a postupů, které chrání informace před ztrátou či nežádoucí změnou, jako je nedůvěryhodnost nebo celistvost, potažmo před dalšími jevy, mezi které patří ztráta autentičnosti nebo odpovědnosti. Pokud je takový stav zjištěn, je nezbytné postupovat podle předem stanovených pravidel, podle nichž je stav napraven. V rámci práce s údaji je také nezbytný rozsah oprávnění přiděleným osobám, které mají s informacemi nakládat. [1]

V rámci této problematiky je třeba porozumět jednotlivým stupňům bezpečnosti uvnitř organizace. Pro tyto potřeby bylo vytvořeno schéma na obrázku 2, které zachycuje jednotlivé úrovně bezpečnosti.



Obr. 2 Vztah úrovní bezpečnosti v organizaci. Zdroj:[vlastní]

Každá úroveň má za úkol chránit jen určitou část aktiv. V rámci bezpečnosti IS/ICT jsou chráněna pouze aktiva, která jsou součástí informačního systému firmy, založeného na informačních a komunikačních technologiích. Chápeme ji tedy jako úzkou oblast řízení bezpečnosti. [18]

Na tomto úseku se však jedná zejména o „nehmatatelná“ data, která jsou interpretována jako informace a služby. Samozřejmě jsou součástí i hmotná aktiva jako je technické vybavení, to však může mít mnohem nižší hodnotu než informace uložené v nich. Mezi nehmotná aktiva můžeme zařadit pracovní postupy využívané v organizaci, data organizací vytvořené nebo převzatá, která jsou nezbytná pro vlastní provoz či programové vybavení - operačními systémy počínaje a programy nezbytným pro provoz počítačové sítě konče. Neopomenutelnou skupinou jsou také služby, mezi které lze zařadit zajištění základních služeb jako je osvětlení, topení či klimatizace. Tato nejužší část však může sloužit jako brána do celkové bezpečnosti organizace. Může být vstupní bránou pro narušení vyšších částí bezpečnosti. [18]

3.1 Řízení informatiky v organizacích

Pro funkce a procesy, při kterých jsou automaticky zpracovávána data v organizacích, se využívá mnoha různých termínů, jako:

- informatika,
- informační technologie,
- informační a komunikační technologie,
- informační systémy,
- informační management,
- IT Governance apod. [18]

V rámci všech těchto činností jde zejména o sběr, třídění, ukládání, zpracování a prezentaci dat, informací a znalostí jednotlivců a organizací, které jsou podpořeny informačními systémy, jejichž podstat je v informačních a komunikačních technologiích. Lze je rozlišovat na základě aspektů a prvků procesu, kterým je na ně kladen důraz z pohledu řízení informatiky. [18]

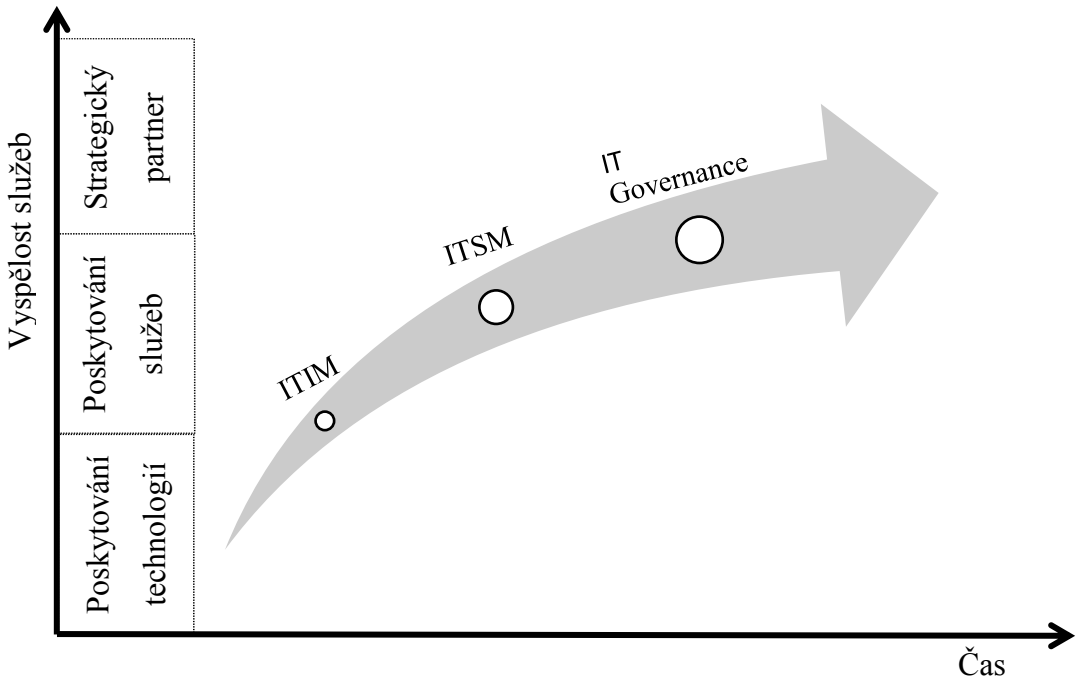
Čím více roste význam a závislost procesů v organizaci na informačních technologiích, tím je nezbytnější vyšší úroveň řízení. Hlavním úkolem informačních technologií je produkovat informace pro okolí organizace. A pokud jsou informace vycházející ze systému spolehlivé

a průkazné, vytváří také důvěru v organizaci, tedy celkový obraz o organizaci. Z tohoto důvodu je nezbytné, aby se na řízení těchto procesů účastnily všechny osoby působící v organizaci a to samozřejmě od nejvyššího vedení. Management musí být jako celek schopen reagovat na krizové situace, případně by těmto situacím měl umět předcházet. [18]

Nyní je hojně využívanou koncepcí řízení tzv. IT Governance (tzv. Správa a řízení). V podstatě se jedná o souhrn politik a interních kontrol, které pomáhají organizaci řídit. Nezbytná je v této částí transparentnost rizik a ochrana hodnot vlastníků. Cílem je sjednocení informační strategie organizace s její celkovou strategií za předpokladu, že jsou zaručeny přidané hodnoty díky informačním technologiím a současnému řízení rizik. Ruku v ruce s tímto souvisí aplikace moderních technologií. [18]

Nejobvyklejším rizikem při implementaci informačních technologií je ohrožení bezpečnosti informačních systémů a dat. Pro eliminaci takového rizika je, vhodná koncepce IT Governance problematika řízení bezpečnosti informací. Spolu s touto koncepcí je také využíváno IT Service Managementu (dále jen „ITSM“), který je zaměřen na nižší úroveň řízení informatiky, přičemž hlavním úkolem je poskytování kvalitních služeb v rámci informačních technologií. Základem je postup, který je v souladu s principy a praktikami pro návrh, dodávku a správu služeb IT ve smluvené kvalitě, jež bude schopna podporovat nejdůležitější aktivity zákazníka. [18]

IT Governance a ITSM mají mnoho společného, disponují však i specifiky. IT Governance má širší rozsah zájmu. Je součástí strategického řízení organizace, zato ITSM se zaměřuje spíše na taktickou a operativní rovinu. Lze se také setkat s problematikou IT Infrastructure Management, která se vyznačuje stylem řízení, zaměřeným na kapacitu a dostupnost zdrojů IT. V rámci této části jde tedy zejména o poskytnutí vhodných technologií, na jejichž základě se tvoří výše zmíněné koncepce. Pro větší přehlednost byl vytvořen graf v obrázku 3, který zobrazuje návaznost jednotlivých celků. [18]



Obr. 3 Cesta k IT Governance. Zdroj: [18]

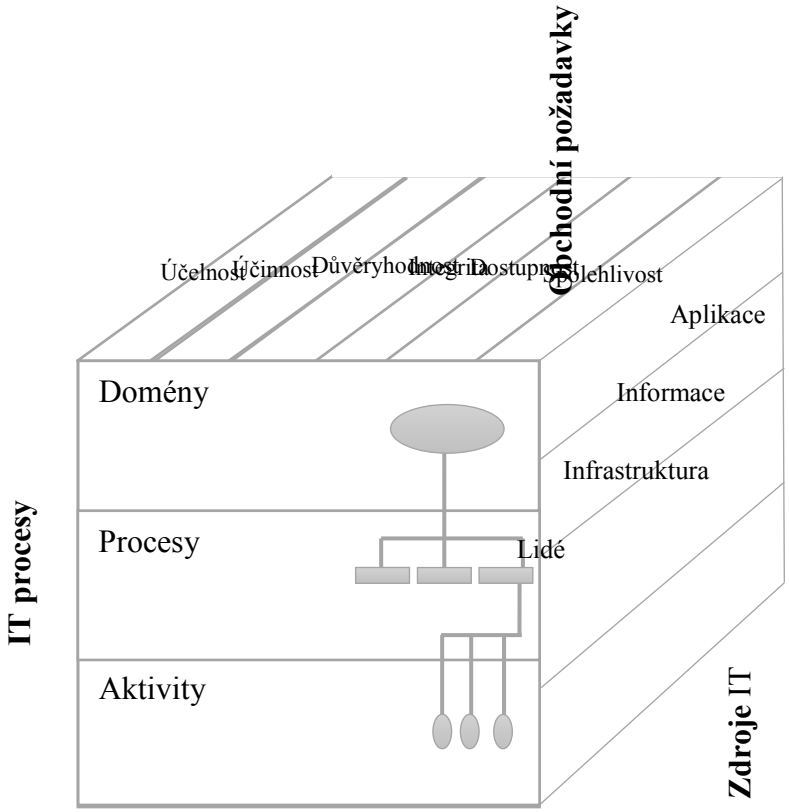
3.2 Metodiky

Pro výše zmíněné koncepce řízení informatiky je nutná podpora formou standardů. Ty se nejčastěji objevují ve formě metodik. Nejznámějšími metodikami jsou celosvětově známé metodiky Control Objektives for Information and Related Technology (dále jen „COBIT“) a Information Technology Infrastucture Library (dále jen „ITIL“). Ty se zabývají nejen oblastí řízení bezpečnosti, ale také aspekty řízení informatiky organizací. [18]

3.2.1 COBIT

Tato metodika je souborem všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, které mají za cíl získat maximum užitku z informačních technologií. Je základním nástrojem IT Governance, který vytvořila organizace Information Systems Audit and Control Foundation (dále jen „ISACA“) v roce 1996. Cílem metodiky je naplnění strategických cílů organizace za užití dostupných zdrojů minimalizací rizik. [18], [19], [20]

Celá metodika vychází z cílů organizace (strategických požadavků), ze zdrojů informačních technologií a z procesů. Pro přehlednost je tvořena tzv. COBIT kostka, který je znázorněna na obrázku 4. [18], [20]



Obr. 4 Kostka COBIT [18]

Podstatou jsou zdroje informatiky, které je nezbytné řídit procesně tak, aby se dosáhlo vytyčených cílů informatiky, které jsou dále v souladu se strategickými požadavky. Na obrázku 4 vidíme vzájemné vazby procesů IT, jako jsou domény, procesy, cíle kontrol a aktivity společně se zdroji informatiky, mezi které patří aplikace, infrastruktura a lidé. Požadavky na informační kritéria jsou efektivnost, výkonnost, důvěrnost, integrita, dostupnost, shoda a hodnověrnost. [18], [20]

3.2.2 ITIL

Tato metodika je tvořena souborem knih, které popisují způsob procesního řízení služeb včetně infrastruktury IT, které jsou jejím prostřednictvím poskytovány. Jde o jednotný postup tvořený „best practice“ pro oblast řízení služeb IT a souvisejících procesů. ITIL považuje samotnou informatiku za poskytovatele služeb a předpokládá, že by se měl přeměnit na „obchodní“ celek, který poskytne třetím stranám informatické služby. Mezi hlavní body této metodiky jsou zařazeny: [18]

- plánování,
- vytváření,
- modifikace,

- dodávka,
- správa,
- analýza,
- použití služeb IT. [18]

Základními znaky metodiky ITIL jsou v první řadě procesní výstupy, které jednoznačně cílí na řízení informatiky a informatické služby. V rámci metodiky ITIL mají procesy přidělen svůj cíl a vlastníka. Dále jsou předem stanoveny vstupy, výstupy a aktivity, které jsou definovány s využitím nástrojů procesní dokumentace. Taková dokumentace bývá tvořena procesními diagramy, RACI diagramy, procedurami a pracovními instrukcemi. Osobám v organizaci jsou jasně stanoveny role s předem přiřazenými zdroji. [18]

Důvodem popularity této metodiky je především užití best practice, díky kterému se otevírá prostor pro dostatečnou volnost, neboť jsou v hojné míře implementovány zkušenosti lidí znalých danou problematiku. Navíc pomocí této metodiky lze dosáhnout na požadovanou kvalitu IT služeb a vytváří prostor pro rozvoj svých ICT systémů. [18], [19]

V rámci této metody je také respektována individualita, protože metodiku tvoří návod, co by se mělo dělat, nikoliv jak to udělat. Zavádění je tedy čistě subjektivním postupem. Vychází se však z modelu, který je označován jako Service-Profit Chain Model vyobrazující ziskovosti služeb. Je využíváno zvýšení zaměstnanecké produktivity k větší spokojenosti zákazníků. V celé metodice je striktně užitá jednotná terminologie, což pozitivně ovlivňuje její srozumitelnost a nečiní problémy v komunikaci. [18]

Nyní je nejaktuálnější verzí ITIL V3, kde je zaveden proces Information Security Management (dále jen „ISM“) jako součást návrhu služeb. Tento proces má za úkol zaručit důvěryhodnost, integritu a dostupnost aktiv, informací, dat a služeb IT organizace. Klíčovým úkolem je spojení bezpečnosti informací s celkovou bezpečností organizace tak, aby se pokryly zájmy všech, kteří jsou závislí na informacích a informačních systémech. Hlavní částí je řízení rizik současně s bezpečnostními riziky. Tato část významně ovlivňuje životní cyklus služby IT. [18], [19]

3.2.3 Vztah ITIL a COBIT

Obě metodiky jsou vzájemně plně kompatibilní. COBIT však jasně definuje, jak sloučit podnikovou strategii s hlavními principy COBIT. ITIL je zejména dobrou praxí a představuje spíše doporučení skrze jasné definice a správu procesů v organizaci. [19]

Je zacílen především na taktickou a operativní úroveň řízení, zatímco COBIT je spíše nástrojem pro strategické – vrcholové řízení v rámci problematiky IT Governance. Je v ní tedy obsažena i problematika řízení lidských zdrojů a IT projektů. Silnou stránkou je jeho využitelnost pro audit shody mezi IT strategií a byznys strategií. ITIL spíše poukazuje jak vytvářet služby a jak implementovat jednotlivé procesy na operativní a taktické úrovni řízení. Na nejzákladnější rozdíly v metodikách přehledně poukazuje tabulka 1. [19]

Tab. 1 Vztah ITIL a COBIT

Kritérium	COBIT	ITIL
Cílová skupina uživatelů	Vrcholový management, auditoři	ICT manažeři, pracovníci zajišťující IT služby
Zaměření	Kontrola procesů a činností	Vykonávání každodenních činností IT služeb
Klíčové otázky	Co by se mělo dělat?	Jak vykonávat IT?
Cílová oblast	Celá informatika organizace	IT oddělení
Velikost organizace	Velká organizace (korporace)	Všechny typy organizací
Náročnost implementace	Vysoká	Nízká

Zdroj: [18]

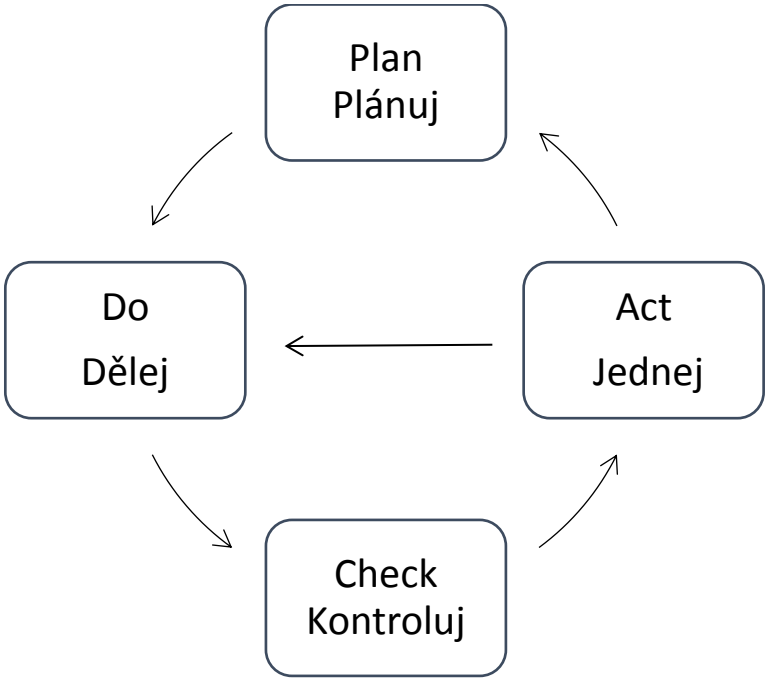
3.3 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informaci (dále jen „SBŘI“) pochází z anglického Information Security Management System (dále jen „ISMS“) a rozumíme pod ním tzv. bezpečnost informačního systému, do které řadíme ochranu veškerých informací, jež jsou přenášeny, zpracovávány a uchovávány v rámci informačního systému (dále jen „IS“). Nezbytným parametrem každé informace je: [18]

- důvěrnost,
- dostupnost,
- integrita. [18]

Zajištění těchto podmínek ze strany vlastníka informace má zásadní vliv na udržení konkurenceschopnosti, ziskovosti, právní shodě a dobrém jménu organizace. [21]

Implementace ISMS nemá pouze jeden předem daný postup. Existují různé doporučené principy jak dosáhnout cíle. Vhodným řešením je Plan, Do, Check, Act (dále jen „PDCA“), kterým rozumíme postup – plánuj, dělej, kontroluj a jednej. Tento cyklus je také znám pod názvem Demingův cyklus nebo Shewhartův cyklus. Je nezbytné zajistit, aby byl systém schopný aktivně reagovat na vývoj organizace. Koncept takového modelu je vyobrazen na obrázku 5. [18], [21]



Obr. 5 Princip Demingova PDCA modelu. Zdroj: [18]

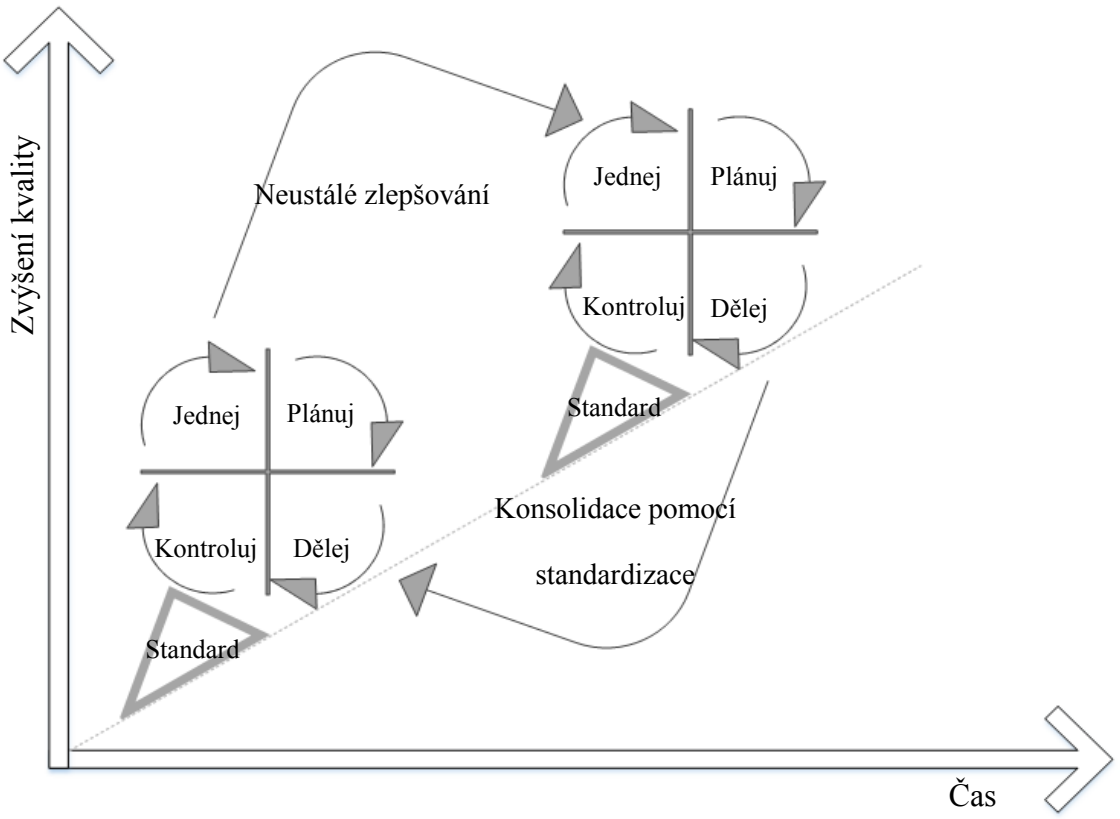
V rámci plánování je třeba definovat cíle komponent integrovaného systému řízení (dále jen „IMS“), rozvinutí strategie realizace komponent a ukazatelů pro měření účinnosti. Je nezbytné provést vstupní analýzu rizik. Následuje fáze „dělej“, kde je nezbytné implementovat komponenty IMS do systému řízení organizace, což v další fázi kontrolujeme. To obnáší nastavení počátečních hodnot ukazatelů pro provoz komponent, na jejichž základě budeme monitorovat a porovnávat stanovené hodnoty s hodnotami naměřenými pro vyhodnocení návrhu. Při postupu do fáze „jednej“ jsou projednány návrhy na změny v komponentách IMS a na základě výsledků vyhodnocování a příprava realizace změn se dále jedná o tzv. systémovou zpětnou vazbu, která je ihned propojena s fází „dělej“. [18], [19], [22]

Samotné ISMS je cyklem, který se skládá ze 4 celků:

- ustanovení ISMS,
- zavádění a provoz ISMS,

- monitorování a přezkoumání ISMS,
- údržba a zlepšování. [18]

Tyto celky podrobně upravují normy ISO/IEC 27001 a ISO/IEC 270002. Představují požadavky, které musí být v rámci implementace a provozu dodržovány. Tyto požadavky jsou v souladu s PDCA tak aby společně tvořily smysluplný celek. Vliv standardizace na zvyšování kvality můžeme názorně vidět na obrázku 6. [18]



Obr. 6 PDCA – vliv standardizace. Zdroj: [vlastní]

3.3.1 Ustanovení ISMS

V rámci ustanovení ISMS je třeba vymezit rozsah a ustanovit meze, kterých se řízení bezpečnosti dotýká. Základem je jasné manažerské zadání, kde jsou ohodnocena rizika, která jsou následně ošetřena bezpečnostními opatřeními. Komplexní řízení rizik je nedílnou a kritickou součástí každého systému řízení bezpečnosti informací. [18], [23]

Analýza pracuje s odhady možných dopadů, které mohou být více či méně přesné. Vše se odvíjí od přesnosti vstupních informací a úrovně dynamiky řízení rizik. Výstupem z této části je zpráva o hodnocení rizik, kde je zdokumentován celý postup jejich řízení. Mimo jiné je vhodné vytvoření registru rizik, který přehledně mapuje rizika společně s opatřeními pro

jejich ošetření a také jejich provázanost s jednotlivými složkami systému, ze kterých vyplývají. [18]

Nezbytnou součástí je také „Prohlášení o aplikovatelnosti“, by mělo být v souladu s normou ISO/IEC 270001. Jde o dokument obsahující cíle a popis jednotlivých bezpečnostních opatření, která byla pro daný ISMS vytvořena za účelem ošetření existujících bezpečnostních rizik. [18], [24]

Součástí ustanovení ISMS je také odsouhlasení tzv. „Prohlášení o politice ISMS“, což v podstatě znamená závazek vedení podniku, že bude podporovat informační bezpečnost. [18]

3.3.2 Zavádění a provoz ISMS

Při zavádění a provozu ISMS jsou účelně a systematicky prosazována vybraná bezpečnostní opatření, která jsou implementována do běžného chodu organizace. Nezbytné je především připravení dílčích částí, ve kterých jsou jasně definovány termíny, odpovědné osoby apod. Důležité je zdokumentovat vše v „Příručce bezpečnosti informací“. Tato příručka by měla sloužit k osvětlení bezpečnostních principů všem uživatelům a manažerům. [18], [23]

V návaznosti na vytvořenou příručku bezpečnosti informací je také nezbytné poukázat na nezbytnost neustálého prohlubování bezpečnostního povědomí pracovníků organizace, kteří musí být schopni dodržovat bezpečnostní principy a pravidla tak aby nedocházelo k bezpečnostním incidentům. Rovněž by měly znít příčiny bezpečnostních incidentů a skutečné potenciální následky. Lidský faktor je vždy nejslabším článkem systému ISMS a to zejména pro jeho nepředvídatelné projevy. [18]

Nezbytné je také vytvoření plánu zvládání rizik, ve kterém jsou popsány všechny potřebné činnosti ISMS pro řízení bezpečnostních rizik. Dále jsou stanoveny cíle a priority zmíněných činností, omezující okolnosti a nepostradatelné zdroje personálního, technického či znalostního charakteru. Opět je nutné stanovit odpovědné osoby za jednotlivé plánované činnosti. [18]

Pro prosazení efektivního řízení je nezbytné měřit účinnost aplikovaných bezpečnostních opatření. Nutné je tedy definovat a soustavně sledovat relevantní údaje o reálném fungování systému řízení bezpečnosti. Jen na takovém základu lze provádět důležitá rozhodnutí. [18]

V rámci procesu zavedení ISMS je nezbytné provádět všechny činnosti podle dohodnutých pravidel. Důležité je však neustále shromažďovat podklady pro další celek, který navazuje – pro monitorování. Je tedy podstatné vytvořit pravidla pro tvorbu, schvalování, distribuci

a aktualizaci dokumentace řízení bezpečnosti. Součástí je vedení záznamů, tedy dokumentů, v kterých jsou zapisovány dosažené výsledky nebo důkazy o provedených činnostech a další informace, které souvisí se systémem řízení kvality. [18]

3.3.3 Monitorování a přezkoumání ISMS

Celý proces je dále monitorován a přezkoumáván. Nezbytné je rovněž zajištění zpětné vazby, kam patří i hodnocení úspěšných a nedostatečných stránek řízení bezpečnosti informací. [18], [23]

Při provádění kontrol všemi osobami, které mají stanovenou jakoukoli odpovědnost na fungování ISMS je nutné, aby docházelo k aktivnímu plnění stanovených úkolů. Na toto plnění musí být dohlíženo. Součástí kontrol musí být detekování chyb, úspěšné i neúspěšné pokusy o narušení bezpečnosti a také schopnost sledovat bezpečnostní události tak, aby bylo možno včas rozpoznat bezpečnostní incident. [18]

Součástí monitoringu jsou také interní audity ISMS v rámci kterých se zjišťuje kritický a nezaujatý pohled na fungování ISMS. Požadavky takového auditu jsou stanoveny v normě ISO/IEC 27001. [18]

Dále je také nutné průběžně vyhodnocovat podněty a připomínky k ISMS, které slouží pro objektivní a účinné přezkoumání ISMS vedením organizace. Toto přezkoumání by se mělo konat nejméně jednou za rok. V rámci přezkoumání bývá vyhodnocována vhodnost, přiměřenost a efektivnost předmětu přezkoumání pro dosažení stanovených cílů. [18]

3.3.4 Údržba a zlepšování ISMS

Při údržbě a zlepšování se systém soustavně zkvalitňuje. Na základě předchozího kroku mělo by docházet k odstraňování zjištěných slabin a nedostatků. To je však v praxi velice náročné. De facto takové systémy vůbec neexistuj, a proto je nezbytné vycházet z předchozího celku, který vytvoří dostatečnou zpětnou vazbu. Získané podněty mohou organizaci pomoci k efektivnímu fungování ISMS – dochází k odhalování nedostatků, přičemž u zmíněných nedostatků jsou hledány příčiny k dalšímu řešení. Nezbytným aspektem zlepšování je také motivace pracovníků v rámci prováděných činností ISMS tak, aby využívali svých zkušeností a otevřeně navrhovali inovativní řešení stávajícího stavu v rámci ISMS. [18], [23]

Při odstraňování nedostatků v ISMS existují dvě formy opatření a to nápravná a preventivní. V rámci nápravných je podstatou řešení nedostatků ISMS. V podstatě reagujeme na vzniklý

projev nedostatku. V rámci preventivního opatření předcházíme vzniku nedostatku, avšak už máme indicie, které poukazují na možný vznik. Při volbě opatření je důležité zamezit opakování nedostatku, tedy pokrýt jeho příčiny. Je nezbytné tyto činnosti dokumentovat a přezkoumávat jejich účinnost. [18]

3.4 Technické normy v souvislosti s bezpečností informací

Nejdůležitějšími technickými normami, které se týkají oblasti bezpečnosti informací, jsou jednoznačně normy International Organization for Standardization (dále jen „ISO“) 27000. ISO 27000 definuje pojmy a terminologický slovník pro všechny ostatní normy z této série. Uplatnění nacházejí v organizacích všech kategorií i velikostí. [24], [25], [26]

Významnou normou pro potřeby této práce je však Česká technická norma (dále jen „ČSN“) ISO/IEC 27001, jež poskytuje požadavky na ustavení, implementaci, udržení a neustálé zlepšování systému řízení bezpečnosti informací. Je určena pro použití interními i externími stranami a pro zhodnocení odolnosti organizace vůči možným bezpečnostním incidentům. Jedná se o normu mezinárodní. [27]

Podstatné ukotvení problematiky řeší také ČSN ISO/IEC 27002, která poskytuje organizaci pokyny, jak implementovat obecně přijatá opatření bezpečnosti informací. Je rovněž určena pro řízení bezpečnosti informací ve vztahu k rizikům v bezpečnostním prostředí. Ukazuje možnosti zabezpečení pomocí vhodných opatření, včetně politik, procesů, postupů, organizačních struktur a softwarových i hardwarových funkcí. [28]

Pro pokrytí široké problematiky byly vydány i normy se vzestupným číslováním pro specifické celky. Například norma ISO/IEC 27006, která uvádí požadavky na akreditaci orgánů provádějících certifikaci systémů řízení bezpečnosti informací. Stanovuje podmínky pro udělování certifikací ISMS, podle nichž musí postupovat certifikační orgány, které služby spojené s touto problematikou poskytují. [18]

Oblast risk managementu zase pokrývá norma ISO/IEC 27005:2011 Řízení rizik bezpečnosti informací, jenž obsahuje rozsáhlé katalogy hrozeb a zranitelností. [18], [24], [29]

V oblasti měření pro řízení bezpečnosti informací byla vydána norma ISO/IEC 27004 upřesňující pravidla a způsoby využití nástrojů pro sledování účinnosti zavedení a prosazení ISMS. [18]

4 CÍLE A POUŽITÉ METODY

Cílem této práce je analýza úrovně zabezpečení informací v rámci vybraného subjektu (který z důvodu citlivosti zveřejňovaných údajů nebude konkrétně jmenován). V návaznosti na zjištěné informace navrhnout vhodná opatření. S ohledem na rozsah tématu se práce omezuje pouze na rozpracování bezpečnostního manuálu pro zaměstnance a souhrn doporučení v rámci navržených opatření proti nejpalčivějším rizikům.

Jeden z prvních sběrů informací o vybraném subjektu byl proveden pomocí řízeného rozhovoru společně s metodou check list, který byl vytvořen Národním úřadem pro kybernetickou bezpečnost. Jedná se o dokument, obsahující 16 stran otázek, cílených na ověření bezpečnostních opatření, která jsou již zavedena. V podstatě nám vymezí nechráněné úseky, které bude nezbytné ošetřit. Pro svou rozsáhlost je zařazen jako příloha této práce. Jako nejvhodnější typ řízeného rozhovoru byl pro potřeby této práce identifikován nestandardizovaný rozhovor, který je výrazně pružnější. Byly připraveny okruhy otázek, které byly zodpovězeny předem vymezeným okruhem osob. V rámci dotazování nebylo nutné držet se přesně stanoveného pořadí. Základním výzkumným problémem tohoto rozhovoru bylo, zda zabezpečení dat bude u subjektu veřejné správy dostatečné.

Dále byla provedena analýza vnitřního a vnějšího prostředí, k čemuž byla použita SWOT analýza. Tato metoda analyzuje základní oblasti vývoje každého subjektu, tedy silné a slabé stránky a také příležitosti a hrozby. Jedná se o univerzální analytickou techniku užívanou pro situační analýzu v rámci strategického řízení. [30]

V rámci identifikace aktiv byla základním vstupním podkladem zejména norma ISO/IEC 27005. Výzkumný tým pro tyto účely plnil starosta, místostarosta a IT technik subjektu. Rozdělena byla na primární a podpůrná, jejichž vzájemné vztahy byly vyznačeny v matici.

Klasifikace aktiv probíhala pomocí metody What-If Analysis. Jedná se o jednoduchou analytickou techniku hledající možné dopady ve vybraných situacích. Je založena na otázce „co když“ čímž pomáhá definování oblasti a cílů zájmů. Výsledná hodnota rizika byla stanovena na základě součtového algoritmu. V dalším kroku byly identifikovány hrozby včetně vyobrazení jejich propojení s aktivy. Hrozby byly také kvantifikovány na základě úsudku hodnotitelů. Pro všechna hodnocení byly jasně definovány hodnotící metriky.

Analýza rizik byla vyhotovena pomocí nástroje RISKAN – kalkulátoru pro tvorbu analýzy rizik. Hodnocena byla všechna primární aktiva, ale v rámci podpůrných aktiv pouze skupina

pracovníci. Rozhodnuto tak bylo na základě výstupů z předchozích analýz, jako byl audit a SWOT analýza. Zmíněné kategorie vykazovaly neuspokojivý vztah. Zbytek podpůrných aktiv již nebyl tolik významný, anebo příslušel do příliš technického oboru, pro který je vyžadována vyšší odbornost. Neanalyzovaná rizika jsou však připravena k ohodnocení v nástroji Excel, ve kterém celé hodnocení probíhalo. V neposlední řadě byl namodelován proces hlášení bezpečnostního incidentu za účelem podrobného přiblížení dané problematiky.

II. PRAKTICKÁ ČÁST

5 CHARAKTERISTIKA VYBRANÉHO SUBJEKTU

Vybraný subjekt si z důvodu, že při svojí činnosti pracuje s množstvím citlivých údajů, nepřál být zveřejněn. Jedná se o obecní úřad v obci se zhruba 1 500 obyvateli. V obci se nachází pošta, základní škola a zdravotnické zařízení, dále disponuje i vlastním sborem dobrovolných hasičů vybaveným na vysoké úrovni. V obci však nesídlí policie. Mezi další instituce a organizace působící na území dané obce lze zařadit farnost, sběrný dvůr a stravovací zařízení. [31]

5.1 Vymezení pracovních pozic

Na obecním úřadu pracuje 20 zaměstnanců v samostatné působnosti. Úřad však vykonává i přenesenou působnost, kterou vykonávají 4 zaměstnanci a to na úseku matričním, na evidenci obyvatel a na stavebním úřadu. Zastupitelstvo obce tvoří 15 členů a radu obce 5 členů. Bližší specifikace je uvedena v kapitole identifikace aktiv v tabulce 9. [31]

5.2 Sběr, zpracování a uchování dat

V první řadě subjekt zpracovává tzv. prvotní data, mezi která lze zařadit skutečnosti, číslice, hodnoty a další prvky, ze kterých se během procesu třídění, sumarizace, průměrování a testování stanou informace. Tyto informace musí být srozumitelné, jasné a snadno interpretovatelné. [32]

V rámci subjektu jsou data shromažďována různými způsoby, přičemž volba metody závisí zpravidla na časových možnostech subjektu, na dostupnosti těchto informací a na jejích parametrech. Subjekt shromažďuje informace zejména v rámci výkonu přenesené a samostatné působnosti. [32]

Nejužívanější metodou je rozhovor. Je sice jednou z nejpomalejších, ale v rámci výkonu samostatné působnosti jako je zasedání zastupitelstva nebo rady obce je toto řešení nezbytné. Výhodou tohoto sběru dat je rozšíření o další otázky nad rámec plánu. V rámci rozhovoru lze dojít do hlubších detailů a lépe definovat a specifikovat danou informaci. U takové informace je velká záruka přesnosti a lépe se tak předchází nedorozuměním. [32]

Častou metodou sběru informací je také dotazník, který je již řadu let běžnou součástí výkonu přenesené působnosti. K takovému sběru informací dochází hlavně na úseku přenesené působnosti, tedy na matričním úřadu a stavebním úřadu. Využitím této metody dochází

k úspoře času i financí. Problémem může být pouze sestavení takového dotazníku, který bude splňovat požadované parametry, mezi které řadíme jednoznačnost, stručnost a srozumitelnost. [32]

5.3 ŘÍZENÝ ROZHOVOR

Při získávání prvotních informací bylo využito metody řízeného rozhovoru, která je blíže specifikována v kapitole 4. V první části je nezbytné vymezit problém, tedy zda jsou v rámci vybraného subjektu implementovány normy ISO/IEC 27 001. Mezi respondenty byl z logického hlediska zařazen IT technik a starosta obce. Pro snadnější průběh rozhovoru byly předem připravené otázky zaslány již týden předem, aby se subjekt mohl připravit. Otázky byly předloženy písemně a autorka práce byla připravena jejich okruh rozšířit, případně je jednotlivě osvětlit. Tento řízený rozhovor je přílohou I této práce.

6 AUDIT BEZPEČNOSTNÍCH OPATŘENÍ

V rámci této kapitoly je shrnuto vyhodnocení auditu bezpečnostních opatření provedeného podle zákona o kybernetické bezpečnosti. Tento audit byl proveden podle předem vytvořeného check listu, který byl sestaven Národním úřadem pro kybernetickou bezpečnost. Náležitosti nástroje check list a jeho princip je vymezeny v kapitole Cíle a použité metody.

Vzhledem k rozsáhlosti tohoto nástroje je jeho vyplněná forma součástí této práce jako příloha 1. V rámci kapitoly jsou pouze shrnuty výsledky a z nich vyplývající další postup. Cílem tohoto šetření bylo získání vhodných bezpečnostních opatření, které jsou nezbytné ke splnění požadavků o kybernetické bezpečnosti a prováděcího právního předpisu vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

Vyplnění tohoto dokumentu probíhalo v součinnosti s vybraným subjektem. Zejména se jednalo o místostarostu, starostu a IT technika subjektu. Ověření tezí bylo prováděno zakřížkováním jedné ze 4 odpovědí. Tedy N – nezavedeno, P – v procesu zavádění, Z – zavedeno a NA – neaplikovatelné. V rámci každé teze je také vyznačeno, jakého subjektu se daná teze dotýká. Pomocí tohoto nástroje totiž mohou být hodnoceny jak informační a komunikační systémy kritické infrastruktury, tak rovněž správci významných informačních systémů. Autor se však domnívá, že použití tohoto nástroje je vhodné pro kohokoli, kdo si chce ověřit připravenost svého podniku či jiného subjektu ze své vlastní iniciativy. Nástroj je za účelem přehlednosti členěn podobně jako již zmíněná vyhláška, proto i následující výstupy z něj budou členěny stejně v rámci dvou základních podkapitol, které tvoří organizační patření a technická opatření. Každá kapitola poukáže na vyplývající opatření, která bude nezbytné implementovat.

6.1 Organizační opatření

V rámci bezpečnostních opatření se nejprve zaměříme na organizační opatření v rámci systému řízení bezpečnosti informací. V této oblasti vyplynul z dotazníku absolutně nevyhovující stav. Problémem je, že subjekt sice zajišťuje svou bezpečnost pomocí nejrůznějších organizačních opatření, ta však nejsou nijak dokumentována a řízena. Není zde vytvořena bezpečnostní politika a není implementována žádná část ISMS. Na základě tohoto je nezbytné stanovit rozsah ISMS a zavést proces řízení rizik. Nejsou rovněž nijak řízena aktiva a nejsou

známa rizika. Vybraný subjekt má sice povědomí o svých aktivech, ty však nejsou nijak identifikována a sepsána v žádné dokumentaci. Nejsou tedy ani nijak hodnocena a subjekt může hůře vytvářet vhodné bezpečnostní prostředí. Nezbytné bude také řešení problematiky aktiv a vyplývajících rizik, případně vhodná analýza rizik. Nutné je však dodat, že si subjekt uvědomuje rozsah důležitosti osobních údajů a také svých právních povinností a dalších závazků. Také velice dobře chápe dopady, které by byly spojeny s narušením důvěrnosti, integrity a dostupnosti dat a s tím už se dá velice dobře operovat.

Navzdory chybějící zásadní část dokumentace ISMS jsou díky velikosti subjektu a zásahům schopného a zkušeného IT technika hrozby ošetřeny velice dobře. Jako jedno ze slabších míst se jeví komunikační síť subjektu, v rámci které může dojít ke zneužití nebo modifikaci údajů. Nejslabším článkem takového systému jsou však vždy lidé. Jejich nevyzpytatelnost a další vlastnosti je nezbytné řešit. Bohužel nebylo možné provést šetření jejich základních znalostí. Proto se mi jeví jako nezbytné alespoň zavést monitorování činností uživatelů systému, protože se v současné době zakládá vše na přílišné důvěře vůči uživatelům, která dle mého názoru není na místě.

Z hlediska posouzení zranitelnosti vidím nedostatečné ošetření rizik. Stejně tak postup při identifikaci a odhalení negativních bezpečnostních jevů nelze považovat za akceptovatelný. Subjekt vykazuje přehnanou důvěru v antivirový program. Dle mého názoru by však bylo vhodné zavést širší spektrum ochrany. Obzvláště za předpokladu, že zde neexistuje žádný monitoring a také nezávislá kontrola s výjimkou IT technika. Subjekt však začal uvažovat o vyšším zabezpečení vůči uživatelům, zavedením přísnějších pravidel při užívání flash disků a podobně.

Bezpečnostní politika není podložena žádnou dokumentací. Neexistuje klasifikace aktiv, další části jsou však v procesu implementace. Je nutno podotknout, že je velice solidně řízena záloha a obnova dat. Dále jsou ošetřeny také vztahy s dodavateli a fyzická bezpečnost. Hlavní ochranou před škodlivým kódem je antivirový program ESET END point, zatímco v rámci serveru subjekt používá ESET File Security for Microsoft Windows Server. Kryptografické ochrany pozorovaný subjekt nevyužívá, po dokončení zavádění serveru je však v plánu kryptovat zálohy.

Neuspokojivá je zejména organizační bezpečnost. Nejsou jasně definované bezpečnostní role. Vše je delegováno především na jednoho člověka – externího IT technika, který spravuje celý systém. Zaměstnanci jsou sice školeni, ale to jen na začátku pracovního poměru

(kromě zaměstnanců, kteří vykonávají přenesenou působnost - ti jsou školeni poměrně často, ale nejčastěji v problematice softwarového vybavení, které je nezbytné pro výkon jejich pracovní pozice) a poté již neprobíhá žádná kontrola dodržování vymezených pravidel. Školení je navíc prováděno externí firmou, která řeší zejména obecná pravidla a nedokáže konkrétně postihnout potřeby subjektu. Na základě těchto skutečností lze předpokládat (protože je to obecně známým faktem), že dodržování pravidel postupem času klesá.

Bezpečnost lidských zdrojů se opírá právě o výše zmíněnou problematiku školení. Je vhodné mít stanovený plán rozvoje bezpečnostního povědomí, který doposud neexistuje.

Jak už bylo výše zmíněno, řízení provozu a komunikace v rámci zvládání kybernetických bezpečnostních událostí je řízeno, jen není dokumentováno. Při reakci a řešení bezpečnostních incidentů je hodně spoléháno na kooperaci s pověřencem GDPR. V součinnosti s ním by se bezpečnostní incident šetřil a také ohlašoval. Subjekt také při zavádění opatření pro implementaci změn v rámci GDPR nechal provést šetření, ze kterého vyplynula opatření, jež zabezpečila splnění normy. Na základě toho byli zaměstnanci proškoleni. Nutné však stále zůstává, aby byl subjekt schopný takový incident identifikovat. Na dobré cestě je však problematika výměny a předávání informací, kde si subjekt uvědomuje hodnotu aktiv, které tímto prostorem protékají, a je v procesu zvýšení jejich zabezpečení. Je také řízen postup pro restart a obnovu chodu systému po selhání. Jen by bylo vhodné zaučit i někoho dalšího, protože je tato oblast řízena pouze IT technikem. V případě, kdy by nebyl dostupný, není tato situace ošetřena.

Bezpečné chování uživatelů je v první řadě řízeno v rámci přístupu k informačnímu systému. Každý uživatel má přiřazený jednoznačný identifikátor. Jeho přidělování je omezeno a rovněž tak i jeho odebírání.

V subjektu je řízen již přístup do systému a také bezpečné chování uživatelů. Jsou přijata opatření pro zajištění ochrany údajů a uživatelé využívají hesla pro zabezpečení přístupu. Je také samostatně řízen přístup k aplikacím, kdy je přidělen samostatný identifikátor. Oprávnění jsou omezena přidělováním administrátorských práv. Ověřování bývá rovněž identita uživatelů. Přestože subjekt využívá mobilních zařízení pro práci jen výjimečně (vyjma telefonování), bylo by vhodné zavést bezpečnostní opatření pro používání mobilních zařízení. Tato opatření by měla mimo jiné obsahovat zásady, jak aktualizovat takové zařízení, poučení o instalacích bezpečných aplikací a podobně. Zejména z důvodu, že je využíváno operačního

systému Android. Navíc není nijak omezeno instalování aplikací a uživatelé nejsou proškoleni.

V rámci akvizice, vývoje a údržby je důležité říci, že si subjekt stanovuje požadavky na změny informačního systému. Další částí je řízení kontinuity činností, které je podloženo důsledným zálohováním.

Samotný audit prováděn v subjektu není. Vhodné by bylo provádět jej 1x ročně. Přesto (a zejména protože se jedná o subjekt veřejné správy) splňuje právní předpisy, které se na něj vztahují. Jen je nezbytné zvýšit úroveň dokumentace.

6.2 Technická opatření

Prvním článkem technických opatření je samozřejmě fyzická bezpečnost, která je v subjektu řešena. Lze konstatovat, že zabezpečení subjektu má solidní základ, který je v současné době po stránce zlepšování v progresu. Drobné nevyhovující části by měly být v blízké době napraveny.

V subjektu zatím neexistují kryptografické prostředky, jejichž použití je do budoucna plánováno pro zálohovaná data. Zatím však nejsou využívány pro ochranu vnitřní komunikační sítě ani pro její segmentaci.

Pozitivní je využívání nástroje pro ověřování identity uživatelů. Jedná se o autorizaci heslem, kde je nastavena minimální délka hesla 8 znaků. Dále bylo umožněno zvolit si hesla dle vlastního uvážení ve zmíněném rozsahu. Ten kdo si jej nestanovil sám, tomu bylo přiděleno a obsahovalo nejméně jedno velké a malé písmeno, číslici i speciální znak. IT technik využívá na důležité prvky jako server, switch, router a podobně silná hesla delší než 15 znaků obsahující velké a malé písmeno, číslici i speciální znak. Přesto že subjekt má zájem měnit každých sto dnů přístupová hesla, tak jak ukládá zákon, je zde stále negativní odezva na zapamatování hesla vzhledem k uvedeným nárokům (i těch hesel užívaných pro přístup do dalších softwarových částí v rámci výkonu pracovního poměru). Přístupová oprávnění jsou v tomto případě v pořádku, existuje tu však možnost rozšířit tuto část o nástroj pro řízení přístupových oprávnění, který rovnou zaznamenává použití přístupových oprávnění, což je vhodné pro následné vyhodnocování rizik.

Existuje také nástroj pro ochranu před škodlivým kódem a to antivirový program, který byl již blíže specifikován.

V závislosti na této práci je zaváděn nástroj pro sběr informací a provozních bezpečnostních činností – zejména jde o typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, nebo identifikaci původce, místa činnosti a úspěšnosti nebo neúspěšnosti činnosti.

Subjekt má plně zaveden nástroj pro detekci kybernetických bezpečnostních událostí. Je využíván v rámci vnitřní komunikační sítě a rovněž na serveru. Důležité však je, aby s ním uměli správně nakládat uživatelé – zaměstnanci. O aplikační bezpečnost se průběžně stará externí firma, která spravuje jednotlivé části systému na základě smluvního závazku. Je tu však možnost zvážit penetrační testy. Kryptografické prostředky jsou v subjektu společně s nástrojem pro zajišťování úrovně dostupnosti v řešení. Je však nezbytné oddělit záložní disk od serveru, což je obsaženo i v řešení.

7 ANALÝZA VNITŘNÍHO A VNĚJŠÍHO PROSTŘEDÍ

Pro další postup je nezbytné poznat vnitřní a vnější prostředí pro použití vhodné strategie, která by napomohla dosáhnutí cílů subjektu. Pro tyto účely je využito SWOT analýzy. Výsledná strategie určí další postup, jakým se bude práce ubírat.

Pro orientaci uveďme, že vnitřním prostředím se rozumí prostředí, kde může systém ovlivňovat sám sebe. Vnější prostředí je naopak prostředí, kde systém sám sebe ovlivňovat nemůže, jde tedy o vlivy vnějšího původu. [30]

V závěrečné fázi jsou tyto jednotlivé části opatřeny vahami důležitosti. Tím chápeme, jaká je spokojenost s danou silnou nebo slabou stránkou. U silných stránek a příležitostí je použita kladná stupnice od 1 do 5 s tím, že 5 znamená nejvyšší spokojenost a 1 nejnižší spokojenost. U slabých stránek a hrozeb je použita záporná stupnice od -1 jako nejnižší nespokojenost až -5 jako nejvyšší nespokojenost. Druhým přiřazovaným číslem je bodové hodnocení jednotlivých složek SWOT analýzy. Pro všechny skupiny je stanoven součet vah roven 1. Čím je číslo vyšší, tím je větší důležitost položky v dané kategorii a naopak. Výstupy ze SWOT analýzy jsou sumarizovány v závěru kapitoly. [30]

Tab. 2 SWOT analýza subjektu

	SWOT analýza	
Vnitřní prostředí	**Silné stránky**	**Slabé stránky**
	Subjekt veřejné správy	Nedostatečná dokumentace aktiv
	Malá organizační struktura	Nedostatečné školení zaměstnanců
	Dobré technické vybavení	Vysoká důvěra v technologie
	Proaktivní management	Absence řízení rizik
	Potenciál zaměstnanců	Špatné delegování odpovědnosti
Vnější prostředí	**Příležitosti**	**Hrozby**
	Pravidelné školení zaměstnanců	Nevhodný přístup zaměstnanců
	Zavedení řízení informačních rizik	Bagatelizace možných rizik
	Větší rozvržení odpovědnosti	Nerealizování navržených opatření
	Aktivní podpora managementu v oblasti ISMS	Ztráta integrity, dostupnosti a důvěrnosti informací
	Proaktivní přístup zaměstnanců	Finanční ztráty

Zdroj: [31], [33]

Silnou stránkou subjektu je jeho forma. Jeho činnosti jsou jasně vymezeny zákonem a lze je snadno identifikovat a následně s nimi pracovat. Výhodou je jeho autoritativní pozice, díky níž je velký zájem na zachování dobrého jména subjektu. Menší velikost organizace a pružná organizační struktura také přispívá k snazší implementaci změn. Na dobré úrovni je také technické vybavení zajišťující ochranu informací z tohoto pohledu. Proaktivní management se navíc nebrání změnám a podporuje zavedení řízení bezpečnostních rizik informací v plném rozsahu. To je nezbytným předpokladem pro úspěšné a kontinuální zlepšování stavu.

Také díky činnostem, které subjekt vykonává, je zde vysoký potenciál zaměstnanců chápajících nezbytnost nově zavedených opatření. Tito zaměstnanci jsou v rámci výkonu své činnosti zvyklí na standardizované postupy, při nichž přichází do kontaktu s velkým množstvím citlivých údajů, které spravují ve svých počítačích. Stačí tedy aktualizovat tyto postupy o bezpečnostní návyky.

Slabou stránkou je zejména organizační část v oblasti dokumentace aktiv, která naprosto schází. Samotný lidský faktor je největším rizikem a v tomto případě neošetřeným. Problematická je také vysoká důvěra v technologie zastiňující možná rizika plynoucí z této oblasti. Nevhodně je také řešena odpovědnost za některá aktiva technického charakteru. Zpravidla jsou delegována pouze na IT technika, který se tímto stává v podstatě nepostradatelným.

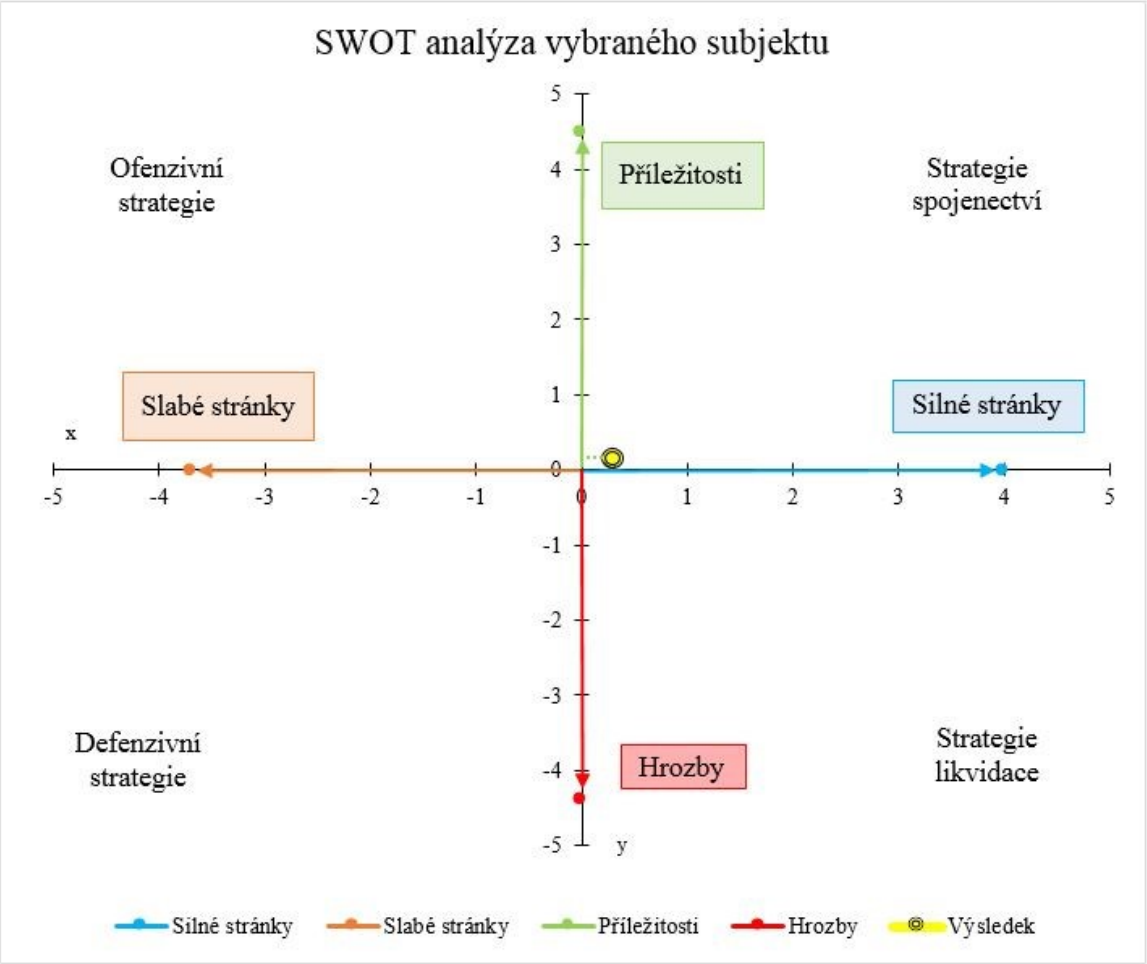
Velké příležitosti jsou však spatřovány v možnosti pravidelného školení zaměstnanců, které je nezbytné pro bezpečnější řízení informací v subjektu a to společně s doposud chybějícím kompletním zavedením řízení informačních rizik. Tento postup má společně s proaktivním přístupem zaměstnanců vysoký potenciál úspěšnosti projektu. Vhodnou možností je širší rozvržení odpovědností mezi více osob v rámci technických aktiv, kde je v současnosti na pozici místostarosty osoba, která má velké předpoklady k převzetí části odpovědnosti.

Největší hrozbou je ztráta integrity, dostupnosti a důvěrnosti, která může velice poškodit dobré jméno subjektu a mít nedozírné dopady na obyvatelstvo. S tímto problémem korespondují i finanční ztráty. Tyto hrozby plynou zejména z nevhodného přístupu zaměstnanců zaujímající klíčový prvek k zabezpečení informací. Neméně významnou hrozbou je bagatelizace rizik. To může mít v budoucnu nedozírné následky. Ohrožením bezpečnosti může být také nerealizování opatření, která vyplynou z plánované analýzy.

Tab. 3 SWOT analýza vybraného subjektu – složky s vahami a hodnocením

Typ	Složka	Váha	Hodnocení	Součin	Součet
Silné stránky	Subjekt veřejné správy	3	0,15	0,45	4
	Malá organizační struktura	3	0,15	0,45	
	Dobré technické vybavení	4	0,20	0,80	
	Proaktivní management	5	0,30	1,50	
	Potenciál zaměstnanců	4	0,20	0,80	
Slabé stránky	Nedostatečná dokumentace aktiv	-3	0,20	-0,60	-3,7
	Nedostatečné školení zaměst-nanců	-5	0,30	-1,50	
	Vysoká důvěra v technologie	-3	0,20	-0,60	
	Absence řízení rizik	-4	0,20	-0,80	
	Špatné delegování odpovědnosti	-2	0,10	-0,20	
Příležitosti	Pravidelné školení zaměstnanců	5	0,30	1,50	4,5
	Zavedení řízení informačních ri-zik	5	0,30	1,50	
	Větší rozvržení odpovědností	3	0,10	0,30	
	Aktivní podpora managementu v oblasti řízení rizik	4	0,20	0,80	
	Proaktivní přístup zaměstnanců	4	0,10	0,40	
Hrozby	Nevhodný přístup zaměstnanců	-4	0,10	-0,40	-4,4
	Bagatelizace možných rizik	-5	0,30	-1,50	
	Nerealizování navržených opat-ření	-4	0,20	-0,80	
	Ztráta integrity, dostupnosti a dů-věrnosti informací	-5	0,30	-1,50	
	Finanční ztráty	-2	0,10	-0,20	
Součet za vnitřní prostředí		**0,3**			
Součet za vnější prostředí		**0,1**			

Zdroj: [vlastní]



Obr. 7 Graf SWOT analýza. Zdroj: [vlastní]

Vhodnou strategií pro vybraný subjekt je strategie spojenectví, která využívá silných stránek pro získání výhody. Vhodným řešením, vyplývajícím z této analýzy je tedy zavedení řízení informačních rizik zakládající se na aktivní podpoře managementu. Bude tedy provedena analýza rizik pro vhodná opatření. Jedním z opatření bude patrně plán školení zaměstnanců a nové rozvržení odpovědností za aktiva. V návaznosti bude vhodné vytvořit i podpůrný materiál sloužící k udržení zavedených opatření k zvýšení bezpečnosti informací.

8 AKTIVA SUBJEKTU

Tato kapitola identifikuje aktiva subjektu, která doposud nebyla mapována. Na základě předchozích analýz bylo označeno za vhodné tato aktiva identifikovat a dále je klasifikovat pro analýzu rizik subjektu. Aktiva jsou hodnotou, kterou je nezbytné chránit. Spolu s aktivem bude vymezen i jeho vlastník, který za aktivum odpovídá.

Pro identifikaci aktiv je vhodné využít seznamu, v normě ČSN ISO/IEC 27005, příloha B. Ta vymezuje 2 skupiny aktiv:

- primární, které charakterizuje jako informace, obchodní procesy a činnosti, jenž v případě ztráty, změny nebo dalších negativních vlivů zásadně ovlivní fungování organizace,
- podpůrná - zahrnující hardware, software, sítě, pracovníky, lokality i samotnou organizaci, které jsou nezbytné pro funkci aktiv primárních. [29]

Podpůrná aktiva mohou být v rámci analýzy rizik označována také jako sekundární. K důkladnějšímu mapování bude mimo identifikaci již zmíněných skupin aktiv vymezena také závislost mezi nimi. Jednotlivá aktiva jsou dekomponována a agregována podle svého druhu do skupin. [34]

8.1 Identifikace primárních aktiv

Primární aktiva vymezuje příloha B normy ČSN ISO/IEC 27005 jako obchodní procesy, činnosti a informace. Jedná se tedy zejména o hlavní procesy, které vykonávají vedoucí pracovníci, odborníci v oblasti IS a uživatelé. Pro svůj rozsah je tato identifikace zaměřena především na klíčové prvky. Pro přehlednost lze rozčlenit primární aktiva do dvou skupin – procesy a informace, které budou blíže specifikovány. Zbývající procesy a informace, které nebudou identifikovány jako citlivé, nebudou dále klasifikovány. Při jejich narušení totiž bude organizace moci své poslání nadále plnit. [29]

8.1.1 Procesy a činnosti

V rámci obchodních procesů (případně dílčích procesů) a činnosti lze vymezit tyto procesy, které jsou charakteristické následujícími znaky:

- jejich ztráta nebo omezení jsou pro organizaci překážkami, aby plnila své poslání,

- obsahují tajné procesy nebo procesy zahrnující patentované, případně jinak chráněné technologie,
- jejich změna, může ovlivnit plnění poslání organizace,
- jsou nezbytné pro plnění smluvních, právních nebo regulačních opatření. [29]

Hlavními primárními aktivy v rámci tohoto subjektu je výkon samostatné a přenesené působnosti. Blíže jsou uvedena v tabulce 4.

Tab. 4 Primární aktiva – procesy a činnosti

Přenesená působnost	
ID číslo	**Stavební úřad**
1.	Správa územně plánovacích informací
2.	Vydávání územního rozhodnutí
3.	Vydávání stavebního povolení
4.	Souhlas s provedením stavby
5.	Vydání kolaudačního rozhodnutí
6.	Kolaudační souhlasy
7.	Souhlas s užíváním staveb
8.	Rozhodnutí o povolení předčasného užívání stavby
9.	Povolení zkušebního provozu staveb
10.	Povoluje odstranění stavby
11.	Řízení o odstranění staveb bez příslušného povolení
12.	Rozhoduje o nezbytných stavebních úpravách
13.	Vynucuje zabezpečovací práce a opatření při havarijních situacích staveb
14.	Provádí kontrolní prohlídky staveb a státní dozory
15.	Provádí sankční řízení
16.	Provádí záznamy staveb do informačního systému územní identifikace (dále jen „ISUI“)
17.	Provádí kontroly staveb
18.	Kompletuje a archivuje dokumentace staveb pro stavby v rámci své působnosti
ID číslo	**Matriční úřad**
19.	Vedení knihy narození, manželství, úmrtí
20.	Vydávání matričních dokladů
21.	Vydávání opisů matričních dokladů
22.	Potvrzení údajů zapsaných v matričních knihách
23.	Vede sbírky listin
24.	Vydává osvědčení pro církevní sňatek, dluhopisy matričních dokladů pro tuzemsko
25.	Vydává osvědčení pro matriční doklady pro cizinu
26.	Vydává osvědčení o právní způsobilosti k uzavření manželství
27.	Provádí zápisy pro zvláštní matriku
28.	Rozhoduje o povolení změny jména a příjmení
29.	Provádí ověřování listin, podpisů a výpisů z rejstříku trestů

30.	Podílí se na přípravě vítání občánků, jubilejních svateb a setkání rodáků
31.	Vede evidenci osob přihlášených k trvalému pobytu
32.	Vede evidenci odhlášených, narozených a zemřelých osob
33.	Eviduje počet sňatků a počet rozvodů
34.	Vydává potvrzení o změně místa trvalého pobytu
35.	Podílí se ne přípravě voleb (kontrola seznamů voličů a změn, tisk volební vyhlášky)
36.	Vystavuje na žádost výpisy z informačního systému Czech POINT
37.	Provádí elektronickou konverzi dokumentů
38.	Vybírá a odvádí správní poplatky na úseku matriky, vidimace a legalizace a služby Czech POINT
39.	Evidují a uzavírají se zde nájemní smlouvy na hřbitovní místa
40.	Výběr poplatků za nájem hrobových míst
Samostatná působnost	
ID číslo	**Zastupitelstvo obce**
41.	Schvalování programu rozvoje obce
42.	Schvalování rozpočtu obce a závěrečný účet obce
43.	Zřizování a rušení příspěvkových organizací, organizačních složek obce a její zřizovací listiny
44.	Rozhoduje o založení nebo zrušení právnických osob a veškeré dokumentace
45.	Vydává obecně závazné vyhlášky obce
46.	Rozhoduje o vyhlášení místního referenda
47.	Navrhuje změny katastrálních území uvnitř obce
48.	Schvaluje dohody o změně hranic obce a o slučování obce
49.	Zřizuje a ruší výbory
50.	Volí z řad členů zastupitelstva obce starostu, místostarosty a další členy rady obce; odvolává je z funkce
51.	Stanovuje počet členů rady obce (i počet dlouhodobě uvolněných členů)
52.	Zřizuje a zrušuje výbory; volí jejich předsedy a další členy, které i může odvolávat
53.	Stanovuje výši odměn neuvolněným členům zastupitelstva
54.	Rozhoduje o spolupráci s jinými obcemi a formě spolupráce
55.	Rozhoduje o zřízení a názvech částí obce, názvech ulic a dalších veřejných prostranství
56.	Uděluje a odnímá čestné občanství obce a ceny obce
57.	Stanovuje zásady o poskytování cestovních náhrad členům zastupitelstva obce
58.	Rozhoduje o peněžitých plněních poskytovaným fyzickým osobám (dále jen „FO“), kteří vykonávají funkci členů výborů
ID číslo	**Rada obce**
59.	Zabezpečuje hospodaření obce podle schváleného rozpočtu
60.	Vydává nařízení obce
61.	Stanovuje rozdělení pravomocí v obecním úřadu
62.	Rozhoduje o počtu zaměstnanců obecního úřadu
63.	Ukládá pokuty ve věcech samostatné působnosti obce
64.	Rozhodování o uzavírání nájemních smluv
65.	Stanovuje pravidla pro záležitosti petic

66.	Schvaluje účetní závěrku obce
ID číslo	**Kancelář starosty (starosta, místostarosta, administrativa)**
67.	Informování veřejnosti o činnosti obce
68.	Svolání a řízení zasedání zastupitelstva obce a rady obce
69.	Podepisování právních předpisů obce, usnesení zastupitelstva a rady obce a také zápisy z jednání obce a rady obce
70.	Odpovídá za včasné objednání přezkoumání hospodaření obce za uplynulý kalendářní rok
71.	Uzavírá a ukončuje pracovní poměr se zaměstnanci obce a stanovuje jejich plat
72.	Zabezpečuje výkon přenesené působnosti obce
73.	Formální vyhotovování veškerých dokumentů a zápisů z jednání
ID číslo	**Ekonomický úsek**
74.	Zajišťuje evidenci psů
75.	Vyřizuje fakturace
76.	Zajišťuje účetnictví
77.	Zajišťuje evidenci majetku obce
78.	Evidence v rámci rozpočtu obce
ID číslo	**Správa IT**
79.	Správa technických zařízení obce (HW a síť)
80.	Externí správa specializovaných SW
81.	Správa záloh obce

Zdroj: [35], [36], [37], [38], [39]

8.1.2 Informace

Primární informace jsou charakteristické tím, že obsahují:

- existenčně důležité informace pro plnění poslání nebo činností organizace,
- osobní údaje, jak je lze konkrétně definovat ve smyslu národní legislativy v rámci soukromí
- strategické informace nezbytné pro splnění cílů organizace,
- velice nákladné informace, jejichž nakládání a zpracování vyžaduje hodně času, anebo je nezbytně nákladný jejich přesnosti.

V rámci vybraného subjektu se nakládá s informacemi, které jsou zpracovány v tabulce 5. [29]

Tab. 5 Primární aktiva – informace

Lidské zdroje		**ID číslo**
Osobní údaje o zaměstnancích	osobní číslo	82.
	kontaktní informace	83.
	pracovní zařazení	84.
	výše mzdy	85.
	výsledky hodnocení	86.
Databáze pracovního zařazení	seznam pracovních pozic	87.
	popis pracovních pozic	88.
Motivační systém	bonusy	89.
	zaměstnanecké výhody	90.
	systém hodnocení	91.
Finanční řízení		**ID číslo**
účetní doklady		92.
pracovní výkazy		93.
rozvaha		94.
platební styk		95.
rozpočet obce		96.
Zařízení		**ID číslo**
plány budovy		97.
umístění čidel, spínačů		98.
soupis majetku		99.
odpisy		100.
IT		**ID číslo**
Typologie HW vybavení		101.
Síťová struktura	nastavení	102.
	dokumentace	103.
	hesla	104.
Systémy	nastavení	105.
	dokumentace	106.
	hesla	107.
Databáze	nastavení,	108.
	dokumentace	109.
	hesla	110.
Osobní údaje občanů		**ID číslo**
veřejné údaje katastru nemovitostí		111.
Neveřejné údaje o občanech	sankce	112.
	rodná čísla	113.
	výpisy z Veřejných rejstříků	114.
	datum narození	115.
Citlivé osobní údaje	o národnosti	116.

Citlivé osobní údaje	výpis z katastru nemovitostí	117.
	bodové hodnocení řidiče	118.
	výpis z insolvenčního rejstříku	119.
	matriční záznamy	120.
Dokumentace		**ID číslo**
smlouvy s dodavateli		121.
projektové dokumentace		122.
záznamy z jednání zastupitelstva a rady obce		123.
archiv		124.

Zdroj: [29]

8.2 Identifikace podpůrných aktiv

Podpůrná aktiva vymezuje norma ČSN ISO/IEC 27005 přílohy B jako:

- hardware,
- software,
- sítě,
- pracovníci,
- lokalita,
- organizace. [29]

8.2.1 Hardware

Hardware sestává z částí, které jsou přehledně sestaveny v následující tabulce 6, která přehledně zaznamenává i konkrétní aktiva. Tyto informace byly zjištěny na základě pozorování a konzultace s IT technikem vybraného subjektu. V tabulce jsou uvedeny pouze vybrané položky, které byly identifikovány ve vybraném subjektu.

Tab. 6 Podpůrná aktiva - Hardware

Typ aktiva	Konkrétní zařízení	Vlastník	ID číslo
Zařízení pro zpracování dat (aktivní)	paměťové médium – paměťová karta	IT technik	1.
	paměťové médium - pevný disk	IT technik	2.
	paměťové médium – flash disk	IT technik	3.
	paměťové jednotky – zálohovací zařízení	IT technik	4.
	notebook	IT technik	5.

Typ aktiva	Konkrétní zařízení	Vlastník	ID číslo
Přenosná zařízení	mobilní telefon	starosta, administrativní pracovnice, matrikářka, referent stavebního úřadu, radní, místostarosta	6.
Pevná zařízení	server poštovní	3. strana	7.
	server veřejný web	3. strana	8.
	počítač jako pracovní stanice	zaměstnanci	9.
	pevné telefon	IT technik	10.
Procesní periférie	tiskárna	v nájmu externě	11.
	scanner kódů konverze dokumentů (2D kód)	matrika	12.
	vyjímatelná disková jednotka (jen v serveru)	IT technik	13.
	počítačová klávesnice a myš	každý	14.
	monitor	zaměstnanci	15.
	reproduktor	zaměstnanci	16.
	aktivní síťové prvky	IT technik	17.
	datové rozvaděče	IT technik	18.
	WiFi zařízení	IT technik	19.
	FireWall	IT technik	20.
	kroucená dvojlinka	IT technik	21.
	optický kabel	IT technik	22.
Elektronické nosiče	USB flash disk	IT technik	23.
	vyjímatelný pevný disk	IT technik	24.
	paměťový klíč	zaměstnanci	25.
Ostatní nosiče	papír	administrativní pracovnice	26.

Zdroj: [31]

8.2.2 Software

Software je složen ze všech programů, které jsou využívány k provozu hardwaru pro zpracování dat. Tato aktiva jsou přehledně zpracována do tabulky 7.

Tab. 7 Podpůrná aktiva - software

Typ aktiva	Konkrétní zařízení	Vlastník	ID číslo
Operační systém	desktop – Microsoft Windows	IT technik	27.
	mobilní zařízení – Android	Místostarosta	28.
	server – Microsoft Windows	IT technik	29.
Software pro služby, údržbu nebo správu	doplňuje služby OS – firmware	IT technik	30.
	BIOS	IT technik	31.
Softwarové balíky nebo standardní software	software pro zasílání elektronických zpráv – outlook	IT technik	32.
	software pro webové servery	3. strana	33.
	MS Office 2013 - 2019	IT technik	34.
	antivirový SW ESET	IT technik	35.
	zálohovací SW - Microsoft	IT technik	36.
	zálohovací SW (server)- Cobian	IT technik	37.
Standardní podnikové aplikace	ekonomická agenda - Gordic	externě	38.
Specifické podnikové aplikace	VITA software – stavební úřad	externě	39.

Zdroj: [31]

8.2.3 Sítě

Sítě se skládají z telekomunikačních zařízení, jejichž účelem je propojení několika fyzicky vzdálených počítačů nebo prvků informačního systému. Tyto prvky, které jsou součástí vybraného subjektu, byly shromážděny v tabulce 8.

Tab. 8 Podpůrná aktiva - sítě

Typ aktiva	Konkrétní zařízení	Vlastník	ID číslo
Médium a podpory	veřejná telefonní síť	IT technik	40.
	Ethernet	IT technik	41.
	VDSL	IT technik	42.
	WiFi 802.11	IT technik	43.
	FireWire	IT technik	44.
	síťový most	IT technik	45.

Pasivní nebo aktivní přenos	směrovač	IT technik	46.
	rozbočovač	IT technik	47.
	přepínač	IT technik	48.
	automatická telefonní ústředna	IT technik	49.
Komunikační rozhraní	adaptér Ethernetu	IT technik	50.

Zdroj: [31]

8.2.4 Pracovníci

Pracovníci jsou skupinami osob, které přicházejí do kontaktu s informačním systémem. Tyto osoby jsou přehledně vykresleny v tabulce 9.

Tab. 9 Podpůrná aktiva - pracovníci

Druh pracovníka	Pracovní zařazení	ID číslo
Ti, co rozhodují	kancelář starosty	51.
	zastupitelstvo obce	52.
	rada obce	53.
Uživatelé	matrikářka	54.
	administrativní pracovnice	55.
	ekonomka	56.
	vedoucí stavebního úřadu	57.
	referenti stavebního úřadu	58.
	starosta	59.
	místostarosta	60.
	pokladna	61.
Pracovníci provozu, obsluhy	technik IT (externí)	62.
	smluvní strana pro SW Gordic	63.
	spisová služba	64.
	smluvní strana pro SW VITA	65.
	správa veřejných registrů	66.

Zdroj: [31]

8.2.5 Lokalita

Lokalita vymezuje všechna místa obsažená zcela nebo z části v rozsahu objektu a dále zachycuje fyzické prostředky, které jsou nezbytné pro provoz. Jednou z částí je vnější prostředí v rámci, kterého nelze uplatňovat bezpečnostní prostředky organizace. Jedná se o domovy pracovníků, například v případě práce mimo pracoviště. To však vykonává pouze ekonomický úsek, který má umožněn vzdálený přístup. Vše je shrnuto v tabulce 10.

Tab. 10 Podpůrná aktiva - lokalita

Typ aktiva	Konkrétní zařízení	Vlastník	ID číslo
Vnější prostředí	vzdálený přístup ekonomického úseku	ekonomka (účetní)	67.
	vzdálený přístup technika IT	IT technik – smluvně ošetřeno	68.
	vzdálený přístup 3. strany – správa softwaru	externě	69.
	internet	externě	70.
Areál	budova obecního úřadu	všichni	71.
Zóna	kanceláře	zaměstnanci	72.
	patra	zaměstnanci	73.
Nezbytné služby	výkon přenesené působnosti	matrika, stavební úřad	74.
	výkon samostatné působnosti	zastupitelstvo, rada, kancelář starosty, administrativní pracovnice, ekonomický úsek	75.
Komunikace	telefonní linka	zaměstnanci	76.
Vybavení	rozvody vody	zastupitelstvo	77.
	elektrické rozvody	zastupitelstvo	78.
	topení	zastupitelstvo	79.

Zdroj: [31]

8.2.6 Organizace

V rámci organizace lze popsat tzv. organizační rámec, ve kterém jsou v rámci struktury pracovníků přiděleny úkoly a postupy kontrolující tyto struktury. Pro přehlednost jsou vymezeny v následující tabulce 11 úseky organizace a příslušné pracovní pozice.

Tab. 11 Podpůrná aktiva - organizace

Úsek organizace	Pracovní pozice	ID číslo
Kancelář starosty	starosta obce	80.
	místostarosta	81.
	administrativní pracovnice	82.
Ekonomický úsek	účetní	83.
Zastupitelstvo obce	zastupitelé (15)	84.
Rada obce	radní (15)	85.
Matriční úřad	matrikářka	86.
Stavební úřad	vedoucí úřadu	87.
	referent	88.
Správa IT	IT technik	89.
	externí správa specializovaného SW	90.

Zdroj: [31]

8.2.7 Projektová činnost

V rámci subjektu se v současné době realizuje projekt zateplení obecního úřadu společně s výměnou technologie v kotelně a také výměna oken. Ve stejném rozsahu se realizuje projekt v rámci mateřské školy. Dalším projektem je vybudování hřiště u základní školy. Vše je zadáváno prostřednictvím externího pracovníka.

8.2.8 Subdodavatelé – dodavatelé - výrobci

Jednán se především o organizace, které vykonávají smluvenou službu pro subjekt, a celý tento proces je zastřešen smluvně. Tito subdodavatelé jsou uvedeni v tabulce 12.

Tab. 12 Podpůrná aktiva – subdodavatelé/dodavatelé/výrobci

Typ aktiva	Konkrétní zařízení	Vlastník	ID číslo
subdodavatelé/ dodavatelé/výrobci	správa areálu	technické služby	91.
	školení řidičů	kancelář starosty	92.
	školení bezpečnosti	kancelář starosty	93.
	školení zdravovědy	kancelář starosty	94.
	tisk (papíry + tonery)	externě	95.
	zmocněnec GDPR	externě	96.
	správa SW VITA	externě	97.
	správa SW Gordic	externě	98.
	správa IT	externě	99.
	zpracování projektů	externě	100.

Zdroj: [31]

8.3 Vazby mezi primárními a podpůrnými aktivy

Pro přehlednost byly vztahy mezi primárními a podpůrnými aktivy zaznačeny do přehledné tabulky 13. Tabulka obsahuje matici, kde jsou v horním řádku zastoupena podpůrná aktiva a v levém sloupci primární aktiva. Pokud existuje vzájemný vztah mezi aktivy, je zaznačen křížkem a zelenou barvou.

Tab. 13 Vztahy primárních a podpůrných aktiv

Název primárního aktiva	ID čísla	Podpůrná aktiva (IS systémy a aplikace a fyzické uložení) kde se primární aktivum nachází																												
		HW - zařízení pro zpracování dat	HW - přenosná zařízení	HW - pevná zařízení	HW - procesní periférie	HW - elektronické nosiče	HW - ostatní nosiče	SW - operační systém	SW - služby, údržba nebo správa	SW balíky nebo standardní SW	SW - standardní podnikové aplikace	SW - Specifické podnikové aplikace	NET - médium a podpory	NET - Pasivní nebo aktivní přenos	NET - komunikační rozhraní	HR - ti co rozhodují	HR - uživatelé	HR - pracovníci provozu, obsluhy	SPC - vnější prostředí	SPC - areál	SPC - zóna	SPC - nezbytné služby	SPC - komunikace	SPC - vybavení	ORG - kancelář starosty	ORG - ekonomický úsek	ORG - zastupitelstvo obce	ORG - rada obce	ORG - matriční úřad	ORG - stavební úřad	ORG - správa IT	Subdodavatelé, dodavatelé, výrobci
Činnosti a procesy - stavební úřad	1-18	x	x	x	x	x	x	x	x	x		x	x	x	x		x	x	x	x	x	x	x	x		x				x	x	x
Činnosti a procesy - matriční úřad	19-40	x	x	x	x	x	x	x	x	x			x	x	x		x	x	x	x	x	x	x	x					x		x	x
Činnosti a procesy - zastupitelstva obce	41-48	x		x	x	x	x	x	x	x			x	x	x	x	x		x	x	x	x	x	x	x		x				x	x
Činnosti a procesy - rada obce	59-73	x	x	x	x	x	x	x	x	x			x	x	x	x	x		x	x	x	x	x	x				x			x	x
Činnost a procesy - kancelář starosty	67-73	x	x	x	x	x	x	x	x	x			x	x	x	x	x		x	x	x	x	x	x	x						x	x
Činnost a procesy - ekonomického	74-78	x		x	x	x	x	x	x	x	x		x	x	x		x	x	x	x	x	x	x	x		x		x		x	x	x
Činnosti a procesy - správa IT	79-81	x		x	x	x		x	x	x			x	x	x		x	x	x	x	x	x	x	x							x	x
Informace z oblasti lidských zdrojů	82-91	x		x	x		x	x	x	x	x					x	x		x	x	x	x			x	x	x	x			x	x
Informace v oblasti finančního řízení	92-96	x		x	x		x	x	x	x	x	x					x	x	x	x	x	x			x	x	x	x		x	x	x
Informace v oblasti zařízení	97-100			x	x		x	x	x	x	x					x	x		x	x	x	x			x		x	x				x
Informace v oblasti IT	101-110	x		x	x			x	x	x			x	x	x		x	x	x	x	x	x									x	x
Osobní údaje občanů	111-120	x		x	x		x	x	x	x		x	x	x	x		x	x	x	x	x	x				x	x	x	x	x	x	x
Dokumentace	121-124				x		x			x						x	x		x	x	x	x		x	x	x	x	x				x

Zdroj: [31], [33]

8.4 Kvantifikace aktiv

V rámci hodnocení aktiv je nezbytné vymezit nejprve vhodnou škálu zakládající se na kritériích pro přidělení určité hodnoty této škály každému aktivu. Pro účely této práce bude využito kvalitativního hodnocení na škále dle tabulky 14.

Kritéria jsou redukovány na společný základ. Jejich výběr probíhá na základě vhodnosti pro vybraný subjekt. Vyplývají však z následků jako je ztráta důvěrnosti, integrity, dostupnosti, nepopiratelnosti, odpovědnosti nebo spolehlivosti aktiv. Mezi kritéria je zařazeno:

Tab. 14 Metrika pro hodnocení aktiv

Stupeň	1	2	3	4
Výše dopadu	nízká	střední	vysoká	kritická
Popis dopadu	malé škody	vážné škody	velmi vážné škody	přežití je ohroženo
Finanční ztráta	0,5%	5-10%	10-30%	30% a více
Porušení legislativy	drobné porušení – řešeno napomenutím	porušení – vyšetřování a udělena pokuta	závažné porušení – vyšetřování, soudní proces a udělena pokuta	velmi závažné porušení – soudní proces, subjektu hrozí zánik
Porušení spojené s osobními údaji	porušení práv v řádech jednotek osoby	porušení práv v řádech desítek až stovek osob	porušení práv v řádech tisíců osob	porušení práv v řádech desetitisíců a více
Neschopnost plnit právní závazky	nemá zásadní vliv	krátkodobá neschopnost	dlouhodobá neschopnost	likvidační neschopnost
Zhoršení výkonu činnosti subjektu	několik dnů	několik týdnů	několik měsíců	trvalá
Neschopnost poskytování služby	několik dnů	několik týdnů	několik měsíců	trvalá
Ztráta důvěry ve vnitřní IS	nemá zásadní vliv	drobná ztráta důvěry	značná ztráta důvěry	naprostá ztráta důvěry
Ztráta důvěry	nemá zásadní vliv	drobná ztráta důvěry	značná ztráta důvěry	naprostá ztráta důvěry

Zdroj: [23], [34]

Pro účely práce jsou klasifikována pouze primární aktiva a to zejména pro rozsáhlost problematiky. Jednotlivá aktiva jsou reprezentována jen svým ID. K hodnocení je využito metody What-If specifikované v kapitole 4. Každé primární aktivum je hodnoceno tak, že si hodnotitel položí otázku „Co se stane, když u aktiva bude narušena důvěrnost (CNF)/integrita (INT)/dostupnost (AVL)?“ a přiřadí hodnotu z metriky. Klasifikovaná aktiva jsou shrnuta v tabulce 15. Pro přehlednost jsou jednotlivé hranice označeny barevně. Nízká bíle, střední zeleně, vysoká žlutě a kritická červeně. Hodnota aktiva je vypočítána podle tzv. součtového algoritmu. Principem je součet dán jednoduchým vzorcem: [34], [40]

$$TAV = \frac{CNF+INT+AVL}{3} \quad (1)$$

TAV – Celková hodnota aktiva

Tab. 15 Klasifikace primárních aktiv

ID	CNF	INT	AVL	TAV	ID	CNF	INT	AVL	TAV
1.	3	2	1	2	63.	2	2	2	2,0
2.	3	2	1	2	64.	1	1	1	1,0
3.	3	2	1	2	65.	2	2	2	2,0
4.	3	2	1	2	66.	3	3	3	3,0
5.	3	2	1	2	67.	3	3	3	3,0
6.	3	2	1	2	68.	2	2	2	2,0
7.	3	2	1	2	69.	3	3	3	3,0
8.	2	2	1	1,7	70.	3	2	2	2,3
9.	2	2	1	1,7	71.	3	3	1	2,3
10.	3	2	1	2	72.	3	3	2	2,7
11.	3	2	1	2	73.	2	3	3	2,7
12.	2	2	1	1,7	74.	1	1	1	1,0
13.	3	2	1	2	75.	3	3	3	3,0
14.	3	2	1	2	76.	3	3	3	3,0
15.	2	2	1	1,7	77.	3	3	2	2,7
16.	3	3	2	2,7	78.	3	3	3	3,0
17.	2	2	1	1,7	79.	3	3	4	3,3
18.	2	3	1	2	80.	3	3	3	3,0
19.	3	3	1	2,3	81.	3	3	3	3,0
20.	3	2	1	2	82.	2	3	3	2,7
21.	3	2	1	2	83.	2	3	3	2,7
22.	2	2	1	1,7	84.	1	2	1	1,3
23.	3	3	2	2,7	85.	2	2	3	2,3
24.	2	2	1	1,7	86.	1	1	1	1,0
25.	2	2	1	1,7	87.	1	1	1	1,0
26.	3	2	1	2	88.	1	1	1	1,0
27.	3	2	1	2	89.	1	1	1	1,0
28.	2	1	1	1,3	90.	1	1	1	1,0
29.	3	3	1	2,3	91.	1	1	1	1,0
30.	1	1	1	1	92.	3	3	3	3,0
31.	2	2	1	1,7	93.	2	2	2	2,0
32.	2	2	1	1,7	94.	3	3	3	3,0
33.	1	1	1	1	95.	3	3	3	3,0
34.	3	2	1	2	96.	4	4	4	4,0
35.	2	2	2	2	97.	3	1	1	1,7
36.	3	3	1	2,3	98.	1	1	3	1,7
37.	2	3	1	2	99.	1	1	1	1,0

ID	CNF	INT	AVL	TAV	ID	CNF	INT	AVL	TAV
38.	1	1	1	1	100.	2	2	2	2,0
39.	1	1	1	1	101.	3	2	1	2,0
40.	1	1	1	1	102.	3	3	3	3,0
41.	3	3	1	2,3	103.	2	2	2	2,0
42.	3	3	3	3	104.	3	3	3	3,0
43.	3	3	2	2,7	105.	3	3	3	3,0
44.	2	2	1	1,7	106.	2	2	2	2,0
45.	3	3	3	3	107.	3	3	3	3,0
46.	3	3	1	2,3	108.	3	3	3	3,0
47.	2	3	2	2,3	109.	1	1	1	1,0
48.	3	3	2	2,7	110.	3	3	3	3,0
49.	2	2	2	2	111.	3	3	1	2,3
50.	3	3	2	2,7	112.	4	4	3	3,7
51.	2	2	2	2	113.	4	4	3	3,7
52.	3	3	2	2,7	114.	4	3	3	3,3
53.	2	2	2	2	115.	4	4	3	3,7
54.	3	2	2	2,3	116.	4	4	3	3,7
55.	3	2	1	2	117.	3	4	3	3,3
56.	1	1	1	1	118.	3	3	3	3,0
57.	1	1	1	1	119.	4	4	3	3,7
58.	2	2	1	1,7	120.	4	4	3	3,7
59.	3	3	3	3	121.	2	3	2	2,3
60.	3	3	3	3	122.	3	3	3	3,0
61.	3	3	2	2,7	123.	3	3	2	2,7
62.	3	3	2	2,7	124.	3	3	3	3,0

Zdroj:[31], [34], [40]

Nejhodnotnější aktiva lze pozorovat v oblasti osobních údajů občanů, které jsou velice citlivé povahy. Bezpečnostní opatření by se měly rozhodně této oblasti dotýkat. Seznam aktiv by měl být alespoň jednou ročně aktualizován.

Následující tabulka 16 vyhodnocuje podpůrná aktiva na stejném principu jako předešlá klasifikace primárních aktiv.

Tab. 16 Klasifikace podpůrných aktiv

ID	CNF	INT	AVL	TAV	ID	CNF	INT	AVL	TAV
1.	1	1	1	1,0	51.	1	1	1	1,0
2.	3	3	3	3,0	52.	1	1	1	1,0

ID	CNF	INT	AVL	TAV	ID	CNF	INT	AVL	TAV
3.	1	1	1	1,0	53.	1	1	1	1,0
4.	3	4	4	3,7	54.	2	1	2	1,7
5.	1	1	1	1,0	55.	1	1	1	1,0
6.	2	3	1	2,0	56	2	3	1	2,0
7.	3	2	4	3,0	57.	1	1	1	1,0
8.	2	2	2	2,0	58.	1	1	2	1,3
9.	4	3	4	3,7	59.	1	1	1	1,0
10.	1	1	1	1,0	60.	1	1	1	1,0
11.	2	1	1	1,3	61.	2	1	2	1,7
12.	1	1	1	1,0	62.	2	1	3	2,0
13.	3	1	3	2,3	63.	2	1	3	2,0
14.	2	1	1	1,3	64.	3	2	2	2,3
15.	1	1	1	1,0	65.	2	1	3	2,0
16.	1	1	1	1,0	66.	4	3	3	3,3
17.	2	2	3	2,3	67.	4	3	1	2,7
18.	2	1	2	1,7	68.	4	3	3	3,3
19.	2	2	3	2,3	69.	4	3	3	3,3
20.	3	1	1	1,7	70.	3	2	3	2,7
21.	1	1	1	1,0	71.	3	3	1	2,3
22.	2	1	3	2,0	72.	3	3	3	3,0
23.	2	2	3	2,3	73.	2	2	3	2,3
24.	2	2	3	2,3	74.	3	2	3	2,7
25.	1	1	1	1,0	75.	3	2	1	2,0
26.	1	1	1	1,0	76.	1	1	1	1,0
27.	3	2	4	3,0	77.		2	3	1,7
28.	3	2	2	2,3	78.	1	2	3	2,0
29.	3	2	4	3,0	79.	1	1	1	1,0
30.	3	2	3	2,7	80.	1	1	1	1,0
31.	3	2	3	2,7	81.	1	1	1	1,0
32.	3	2	2	2,3	82.	1	2	1	1,3
33.	1	1	1	1,0	83.	3	3	3	3,0
34.	2	2	2	2,0	84.	1	1	1	1,0
35.	3	4	4	3,7	85.	1	1	1	1,0
36.	3	2	4	3,0	86.	3	2	3	2,7
37.	3	2	4	3,0	87.	2	1	1	1,3
38.	3	2	3	2,7	88.	2	2	1	1,7
39.	3	2	3	2,7	89.	3	3	3	3,0
40.	1	1	1	1,0	90.	3	3	3	3,0

ID	CNF	INT	AVL	TAV	ID	CNF	INT	AVL	TAV
41.	3	3	1	2,3	91.	1	2	2	1,7
42.	3	3	3	3,0	92.	1	1	1	1,0
43.	3	3	2	2,7	93.	1	1	1	1,0
44.	2	2	1	1,7	94.	1	1	1	1,0
45.	3	3	3	3,0	95.	1	1	2	1,3
46.	3	3	1	2,3	96.	1	1	2	1,3
47.	2	3	2	2,3	97.	2	2	2	2,0
48.	3	3	2	2,7	98.	2	2	2	2,0
49.	2	2	2	2,0	99.	3	3	3	3,0
50.	3	3	2	2,7	100.	1	1	1	1,0

Zdroj:[31], [34], [40]

Nejhodnotnějším aktivy jsou zejména hardware a síťové prvky ve vybraném subjektu. Neopomenutelnou skupinou vysoce klasifikovaných aktiv jsou také zaměstnanci ať už na pozicích uživatelů nebo pozici provozovatelů, či třetí straně. Jedná se o významná aktiva, jejichž narušení může vést k významným škodám.

9 HROZBY PRO VYBRANÝ SUBJEKT

Hrozbou je náhodná nebo úmyslně vyvolaná událost, která může mít negativní dopad na důvěrnost, integritu a dostupnost aktiv. V této části jsou identifikovány hrozby včetně jejich původu a uvedení, na jaká aktiva působí. Následně jsou hodnoceny pro poznání nejnebezpečnějších z nich. [34]

9.1 Identifikace hrozeb

Identifikovány jsou pouze hrozby vhodné pro další analýzu. Jedná se o konvenční hrozby působící na IS. Každé identifikované hrozbě je přiřazeno pro přehlednost ID číslo. Další 3 sloupce jsou atributy bezpečnosti – důvěrnost, integrita a dostupnost (v tabulce jako CNF, INT, AVL). Pokud hrozba ohrožuje jednu z těchto kategorií, je označena křížkem. Poslední 3 sloupce označují původce hrozby a to zda byla způsobena úmyslně, neúmyslně nebo přírodně (v tabulce jako DLB, ACC, ENV). Pokud se v tabulce 17 jedná o původce dané hrozby, je rovněž označen křížkem.

Tab. 17 Identifikace hrozeb pro vybraný subjekt

ID hrozby	Hrozba	CNF	INT	AVL	DLB	ACC	ENV
1.	Blesk			x			x
2.	Požár		x	x	x	x	x
3.	Voda		x	x	x	x	x
4.	Prach			x			x
5.	Nepřípustná teplota			x	x	x	x
6.	Elektrostatický výboj			x			x
7.	Přerušení dodávek elektřiny			x	x	x	x
8.	Přerušení dodávek vody				x	x	x
9.	Nedostatek personálu			x	x	x	
10.	Chyba administrátora	x	x	x	x	x	
11.	Chyba uživatele	x	x	x	x	x	
12.	Průmyslová havárie v okolí			x		x	
13.	Demonstrace v okolí			x		x	
14.	Kyberterorismus	x	x	x	x		

ID hrozby	Hrozba	CNF	INT	AVL	DLB	ACC	ENV
15.	Terorismus			x	x		
16.	Odposlech	x			x		
17.	Krádež a vandalismus	x	x	x	x		
18.	Falšování identity	x	x	x	x		
19.	Neautorizovaný přístup k médiím	x	x	x	x		
20.	Neautorizovaný přístup do IS	x	x	x	x		
21.	Použití neautorizovaného SW		x	x	x		
22.	Použití škodlivého SW	x	x	x	x		
23.	Infiltrace komunikace		x		x		
24.	Přesměrování zpráv	x	x	x	x	x	
25.	Zneužití zdrojů			x	x		
26.	Přetížení zdrojů		x	x	x	x	
27.	Selhání záložních zdrojů		x	x	x	x	
28.	Selhání HW	x	x	x	x	x	
29.	Selhání SW	x	x	x	x	x	
30.	Selhání sítě		x	x	x	x	
31.	Selhání média		x	x	x	x	
32.	Selhání veřejné sítě		x	x	x	x	
33.	Selhání tiskového zařízení			x	x	x	

Zdroj: [31], [34]

Následující tabulka 18 propojuje jednotlivé hrozby se skupinami aktiv. Vychází se z objektové dekompozice aktiv. Není to tedy specifikace pro jednotlivá aktiva, ale pro celé skupiny, v rámci kterých byla identifikována. Pro přehlednost bylo využito následujících zkratek:

- síť – NET,
- data – DTA,
- personál – STF,
- prostor – SPC.

Tab. 18 Propojení hrozeb s aktivy ve vybraném subjektu

ID hrozby	Hrozba	HW	SW	NET	MED	DTA	STF	SPC
1.	Blesk	x		x				x
2.	Požár	x		x	x			x
3.	Voda	x		x	x		x	
4.	Prach	x			x			
5.	Nepřípustná teplota	x			x			
6.	Elektrostatický výboj	x		x	x	x		
7.	Přerušení dodávek elektřiny	x		x		x		
8.	Přerušení dodávek vody	x						
9.	Nedostatek personálu						x	
10.	Chyba administrátora	x	x	x	x	x		
11.	Chyba uživatele	x	x	x	x	x		
12.	Průmyslová havárie v okolí						x	
13.	Demonstrace v okolí						x	
14.	Kyberterorismus		x	x		x		
15.	Terorismus	x		x	x		x	x
16.	Odposlech			x				
17.	Krádež a vandalismus	x	x		x	x		
18.	Falšování identity						x	
19.	Neautorizovaný přístup k médiím				x	x		
20.	Neautorizovaný přístup do IS		x			x		
21.	Použití neautorizovaného SW							
22.	Použití škodlivého SW		x	x		x		
23.	Infiltrace komunikace							
24.	Přesměrování zpráv							
25.	Zneužití zdrojů							
26.	Přetížení zdrojů		x	x				

ID hrozby	Hrozba	HW	SW	NET	MED	DTA	STF	SPC
27.	Selhání záložních zdrojů	x						
28.	Selhání HW	x						
29.	Selhání SW		x					
30.	Selhání sítě			x				
31.	Selhání média				x			
32.	Selhání veřejné sítě			x				
33.	Selhání tiskového zařízení	x						

Zdroj: [31], [34]

9.2 Kvantifikace hrozeb

Pro kvantifikaci hrozeb neexistuje žádný algoritmus. Založena je na úsudku hodnotitelů. Vycházelo se zejména ze srovnání dostupných zkušeností subjektu a také z rešeršní činnosti, v rámci které byly vyhledávány dostupné příklady obdobných subjektů. Zahrnuta byla zejména lokalita, velikost, firemní kultura, předmět činnosti a zavedené procesy. Hodnocení je shrnuto v tabulce 19. K hodnocení bylo využito stupnice, kde: [34]

- 1 – nízká hrozba,
- 2 – střední hrozba,
- 3 – vysoká hrozba,
- 4 – kritická hrozba.

Tab. 19 Kvantifikace hrozeb

ID hrozby	Hrozba	Hodnota hrozby
1.	Blesk	2
2.	Požár	3
3.	Voda	1
4.	Prach	1
5.	Nepřípustná teplota	1
6.	Elektrostatický výboj	2
7.	Přerušení dodávek elektřiny	3
8.	Přerušení dodávek vody	3

ID hrozby	Hrozba	Hodnota hrozby
9.	Nedostatek personálu	1
10.	Chyba administrátora	2
11.	Chyba uživatele	3
12.	Průmyslová havárie v okolí	1
13.	Demonstrace v okolí	1
14.	Kyberterorismus	2
15.	Terorismus	1
16.	Odposlech	2
17.	Krádež a vandalismus	2
18.	Falšování identity	3
19.	Neautorizovaný přístup k médiím	1
20.	Neautorizovaný přístup do IS	1
21.	Použití neautorizovaného SW	1
22.	Použití škodlivého SW	1
23.	Infiltrace komunikace	2
24.	Přesměrování zpráv	1
25.	Zneužití zdrojů	2
26.	Přetížení zdrojů	2
27.	Selhání záložních zdrojů	1
28.	Selhání HW	2
29.	Selhání SW	3
30.	Selhání sítě	2
31.	Selhání média	2
32.	Selhání veřejné sítě	2
33.	Selhání tiskového zařízení	1

Zdroj: [31], [33], [34]

10 ANALÝZA RIZIK VE VYBRANÉM SUBJEKTU

Účelem této kapitoly je vyčíslení rizik ve vybraném subjektu pomocí detailní analýzy rizik systému IT obsahující identifikaci rizik a odhad jejich velikosti. Dotýká se však jen primárních aktiv a části podpůrných. Důvodem je, že primární aktiva byla propojena se sekundárními a je snadno dohledatelná paralela mezi jednotlivými částmi systému. V návaznosti na výstupy byla navržena vhodná opatření snižující, případně eliminující riziko. Tímto způsobem bylo ve vybraném subjektu zavedeno řízení rizik. Analytický tým tvořili zpracovatel práce společně s vrcholovým managementem subjektu a IT technikem. Jako podklady posloužila již identifikovaná aktiva a identifikované hrozby z předchozích kapitol práce.

Analýza rizik byla vyhotovena pomocí nástroje RISKAN. Nejprve byly v prostředí aplikace RISKAN vytvořeny seznamy aktiv a hrozeb, dále byly vytvořeny vhodné číselníky pro hodnocení aktiv, hrozeb a zranitelností. Současně se vymezily hranice pro jednotlivé stupně rizika. V návaznosti se ohodnotily jednotlivé zranitelnosti ve vztahu hrozba – aktivum a na základě toho bylo vypočítáno riziko pro předem vymezený okruh aktiv. Vymezený okruh aktiv je zdůvodněn v kapitole 4.

10.1 Vyhodnocení zranitelností

Pro provedení analýzy rizik bylo nezbytné vyhodnocení zranitelností na základě vztahu hrozba – riziko. Pro hodnocení bylo využito této metriky, kde:

- 1 – nízká zranitelnost aktiva,
- 2 – střední zranitelnost aktiva,
- 3 – vysoká zranitelnost aktiva,
- 4 – kritická zranitelnost aktiva.

Na základě metriky se v prostředí MS Excel vyhodnotily jednotlivé zranitelnosti v rámci vymezených hranic a předem stanovené hloubky analýzy rizik. Pro stanovení hodnot byla brána v potaz implementovaná opatření pro snížení rizika, identifikovaná v rámci řízeného rozhovoru a také provedeného auditu bezpečnostních opatření. Hodnocení je shrnuto na obrázku 8.

Riskan RIZIKOVÝ KALKULÁTOR / T-SOFT		Aktiva	AKTIVA - CELKEM	Primární aktiva	Procesy a činnosti	Stavební úřad	Matriční úřad	Zastupitelstvo obce	Rada obce	Kancelář starosty	Ekonomický úsek	Správa IT	Informace	Lidské zdroje	Finanční řízení	Zařízení	IT	Osobní údaje občanů	Dokumentace	Podpůrná aktiva	Hardware	Software	Sítě	Pracovníci	Lokalita	Organizace	Subdodavatelé
				PA	PČ	SÚ	MÚ	ZO	RO	KS	EÚ	SIT	INF	HR	FŘ	ZZ	IT	OÚO	DOK	SA	HW	SW	NET	STF	SPC	ORG	SUB
		Hodnoty aktiv	4	4	3	3	3	3	3	3	3	3	4	3	4	2	3	4	3	4	4	4	3	3	3	3	3
			kritická	kritická	vysoká	vysoká	vysoká	vysoká	vysoká	vysoká	vysoká	vysoká	kritická	vysoká	kritická	střední	vysoká	kritická	vysoká	kritická	kritická	kritická	kritická	vysoká	vysoká	vysoká	vysoká	vysoká
Hrozby		Pravděpodobnost																									
HROZBY - CELKEM		3	oce pravděpodo	4	4	4	4	4	2	2	3	4	4	4	4	4	4	4	4	4	4	4	0	0	0	4	0	0	0
1	Blesk	2	pravděpodobná	3	3	2	2	2	1	1	1	2	2	3	2	3	2	2	2	2	2	2	0	0	0	2	0	0	0
2	Požár	3	oce pravděpodo	4	4	3	3	3	1	2	3	2	2	4	3	3	4	3	3	4	3	0	0	0	3	0	0	0	0
3	Voda	1	epravděpodobn	4	4	3	1	3	1	2	3	2	2	4	3	2	4	2	2	4	3	0	0	0	3	0	0	0	0
4	Prach	1	epravděpodobn	3	3	2	2	2	1	2	2	2	2	3	3	3	2	2	2	1	1	0	0	0	1	0	0	0	0
5	Nepřípustná teplota	1	epravděpodobn	3	3	2	2	2	1	2	1	2	2	3	3	3	2	2	2	1	1	0	0	0	1	0	0	0	0
6	Elektrostatický výboj	2	pravděpodobná	4	4	3	3	2	2	2	2	2	2	4	3	3	4	2	3	2	1	0	0	0	1	0	0	0	0
7	Přerušení dodávek elektřiny	3	oce pravděpodo	4	4	3	2	3	2	2	2	2	2	4	3	3	4	2	2	2	1	0	0	0	1	0	0	0	0
8	Přerušení dodávek vody	3	oce pravděpodo	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	0	0	0	2	0	0	0	0
9	Nedostatek personálu	1	epravděpodobn	4	4	4	2	3	2	2	2	2	4	2	1	2	1	1	1	1	2	0	0	0	2	0	0	0	0
10	Chyba administrátora	2	pravděpodobná	4	4	3	3	3	1	1	1	3	2	4	4	4	4	3	3	1	4	0	0	0	4	0	0	0	0
11	Chyba uživatele	3	oce pravděpodo	4	4	4	4	4	2	2	2	4	1	4	4	4	4	4	4	3	2	0	0	0	2	0	0	0	0
12	Průmyslová havárie v okolí	1	epravděpodobn	3	2	2	1	1	2	2	1	2	1	2	2	2	2	1	1	2	3	0	0	0	3	0	0	0	0
13	Demonstrace v okolí	1	epravděpodobn	4	2	2	2	2	2	2	2	2	1	2	2	2	2	1	1	2	4	0	0	0	4	0	0	0	0
14	Kyberterorismus	2	pravděpodobná	4	3	3	3	3	1	1	1	3	3	3	3	3	3	3	3	1	4	0	0	0	4	0	0	0	0
15	Terorismus	1	epravděpodobn	3	2	2	2	1	2	2	2	1	1	2	1	2	1	1	1	1	3	0	0	0	3	0	0	0	0
16	Odposlech	2	pravděpodobná	4	3	3	2	3	1	2	2	3	1	3	3	3	1	3	3	2	4	0	0	0	4	0	0	0	0
17	Krádež a vandalismus	2	pravděpodobná	3	3	3	2	2	1	1	1	3	1	3	3	3	3	1	3	3	2	0	0	0	2	0	0	0	0
18	Falšování identity	3	oce pravděpodo	4	4	3	3	3	1	1	1	3	2	4	4	4	4	3	3	1	3	0	0	0	3	0	0	0	0
19	Neautorizovaný přístup k médiím	1	epravděpodobn	4	4	4	2	3	1	2	2	3	4	4	4	3	4	3	3	2	4	0	0	0	4	0	0	0	0
20	Neautorizovaný přístup do IS	1	epravděpodobn	4	4	4	3	3	1	2	2	4	1	4	4	4	4	3	3	1	4	0	0	0	4	0	0	0	0
21	Použití neautorizovaného SW	1	epravděpodobn	3	3	3	2	2	1	2	2	2	3	3	3	1	3	2	2	1	1	0	0	0	1	0	0	0	0
22	Použití škodlivého SW	1	epravděpodobn	3	3	2	2	2	1	1	1	1	2	3	3	3	3	2	2	1	1	0	0	0	1	0	0	0	0
23	Infiltrace komunikace	2	pravděpodobná	3	3	3	2	3	1	1	2	3	3	3	3	2	2	1	3	1	1	0	0	0	1	0	0	0	0
24	Přesměrování zpráv	1	epravděpodobn	2	2	2	2	1	1	1	1	2	2	2	2	1	1	1	2	1	2	0	0	0	2	0	0	0	0
25	Zneužití zdrojů	2	pravděpodobná	3	3	3	2	2	1	1	2	2	3	3	3	3	3	1	1	2	3	0	0	0	3	0	0	0	0
26	Přetížení zdrojů	2	pravděpodobná	4	4	4	1	2	1	1	1	1	4	1	1	1	1	1	1	1	3	0	0	0	3	0	0	0	0
27	Selhání záložních zdrojů	1	epravděpodobn	4	4	4	1	2	1	1	1	2	4	4	3	3	4	1	3	1	4	0	0	0	4	0	0	0	0
28	Selhání HW	2	pravděpodobná	3	3	2	2	2	1	1	2	2	2	3	3	2	3	2	2	1	3	0	0	0	3	0	0	0	0
29	Selhání SW	3	oce pravděpodo	3	3	2	2	2	1	1	2	2	2	3	3	3	3	2	2	1	3	0	0	0	3	0	0	0	0
30	Selhání sítě	2	pravděpodobná	3	3	2	2	2	1	1	2	2	1	3	3	3	2	2	2	1	3	0	0	0	3	0	0	0	0
31	Selhání média	2	pravděpodobná	3	3	2	2	2	1	1	2	2	2	3	3	3	2	2	2	1	3	0	0	0	3	0	0	0	0
32	Selhání veřejné sítě	2	pravděpodobná	3	3	2	2	2	1	1	2	2	2	3	3	3	2	2	2	1	3	0	0	0	3	0	0	0	0
33	Selhání tiskového zařízení	1	epravděpodobn	3	3	3	3	1	1	1	2	2	1	3	3	2	3	1	1	3	3	0	0	0	3	0	0	0	0

Obr. 8 Vyhodnocení zranitelností ve vybraném subjektu. Zdroj: [31], [33]

10.2 Vyhodnocení analýzy rizik

V návaznosti na vyhodnocení zranitelnosti byl proveden v MS Excel výpočet hodnoty rizika a to na základě vzorce:

$$R = A * H * Z \qquad (2)$$

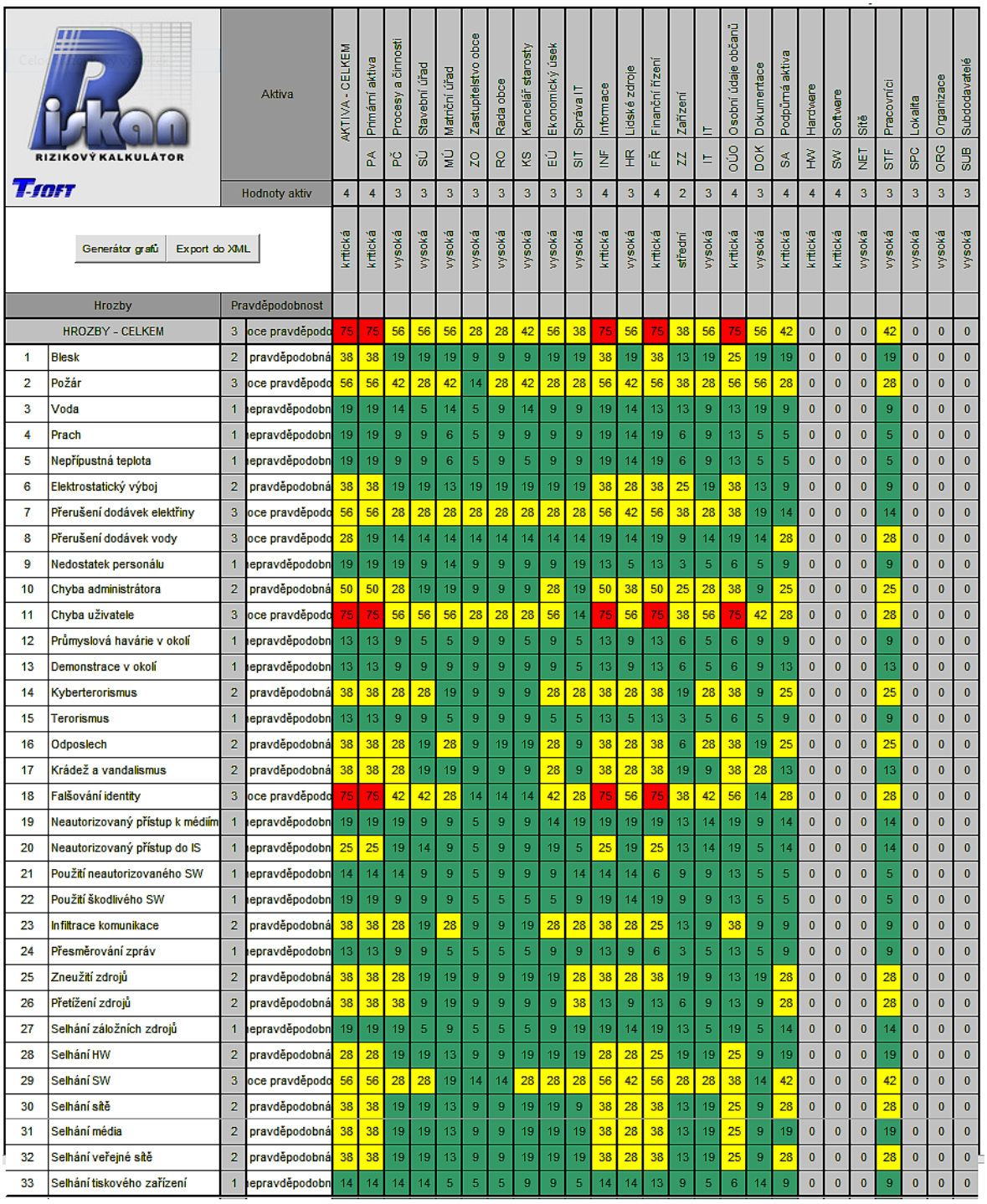
kde:

- R – výsledné riziko
- A – hodnota aktiva
- H – pravděpodobnost uplatnění hrozby
- Z – zranitelnost skupiny aktiv

Na základě výše uvedené hodnoty výsledného rizika je stanoveno barevné označení výsledných hodnot v předem stanovených hranicích, kde maximem bylo 100. Hranice byly stanoveny:

- nízké riziko v rozmezí 0 – 19 (zelená barva),
- střední riziko v rozmezí 20 – 19 (žlutá barva),
- vysoké riziko v rozmezí 70 – 100 (červená barva).

Pro další účely, jako je dopracování analýzy rizik v rámci zbylých podpůrných aktiv, či studia hodnot jednotlivých aktiv byl zvolen MS Excel. Výsledná matice je zachycena na obrázku 9.



Hrozby		Pravděpodobnost	AKTIVA - CELKEM	Přímání aktiva	Procesy a činnosti	Stavební úřad	Matriční úřad	Zastupitelstvo obce	Rada obce	Kancelář starosty	Ekonomický úsek	Správa IT	Informace	Lidské zdroje	Finanční řízení	Zařízení	IT	Osobní údaje občanů	Dokumentace	Podpůrná aktiva	Hardware	Software	Sítě	Pracovníci	Lokalita	Organizace	Subdodavatelé
			PA	PČ	SÚ	MÚ	ZO	RO	KS	EÚ	SIT	INF	HR	FŘ	ZZ	IT	OÚO	DOK	SA	HW	SW	NET	STF	SPC	ORG	SUB
	Hodnoty aktiv		4	4	3	3	3	3	3	3	3	3	4	3	4	2	3	4	3	4	4	4	3	3	3	3	3
	Generátor grafů / Export do XML		kritická	kritická	vysoká	vysoká	vysoká	vysoká	vysoká	vysoká	vysoká	vysoká	kritická	vysoká	kritická	střední	vysoká	kritická	vysoká	kritická	kritická	kritická	vysoká	vysoká	vysoká	vysoká	vysoká
	HROZBY - CELKEM	3	oce pravděpodo	75	75	56	56	56	28	28	42	56	38	75	56	75	38	56	75	56	42	0	0	0	42	0	0	0
1	Blesk	2	pravděpodobná	38	38	19	19	19	9	9	9	19	19	38	19	38	13	19	25	19	19	0	0	0	19	0	0	0
2	Požár	3	oce pravděpodo	56	56	42	28	42	14	28	42	28	28	56	42	56	38	28	56	56	28	0	0	0	28	0	0	0
3	Voda	1	epravděpodobn	19	19	14	5	14	5	9	14	9	9	19	14	13	13	9	13	19	9	0	0	0	9	0	0	0
4	Prach	1	epravděpodobn	19	19	9	9	6	5	9	9	9	9	19	14	19	6	9	13	5	5	0	0	0	5	0	0	0
5	Nepřípustná teplota	1	epravděpodobn	19	19	9	9	6	5	9	5	9	9	19	14	19	6	9	13	5	5	0	0	0	5	0	0	0
6	Elektrostatický výboj	2	pravděpodobná	38	38	19	19	13	19	19	19	19	19	38	28	38	25	19	38	13	9	0	0	0	9	0	0	0
7	Přerušení dodávek elektřiny	3	oce pravděpodo	56	56	28	28	28	28	28	28	28	28	56	42	56	38	28	38	19	14	0	0	0	14	0	0	0
8	Přerušení dodávek vody	3	oce pravděpodo	28	19	14	14	14	14	14	14	14	14	19	14	19	9	14	19	14	28	0	0	0	28	0	0	0
9	Nedostatek personálu	1	epravděpodobn	19	19	19	9	14	9	9	9	9	19	13	5	13	3	5	6	5	9	0	0	0	9	0	0	0
10	Chyba administrátora	2	pravděpodobná	50	50	28	19	19	9	9	9	28	19	50	38	50	25	28	38	9	25	0	0	0	25	0	0	0
11	Chyba uživatele	3	oce pravděpodo	75	75	56	56	56	28	28	28	56	14	75	56	75	38	56	75	42	28	0	0	0	28	0	0	0
12	Průmyslová havárie v okolí	1	epravděpodobn	13	13	9	5	5	9	9	5	9	5	13	9	13	6	5	6	9	9	0	0	0	9	0	0	0
13	Demonstrace v okolí	1	epravděpodobn	13	13	9	9	9	9	9	9	9	5	13	9	13	6	5	6	9	13	0	0	0	13	0	0	0
14	Kyberterorismus	2	pravděpodobná	38	38	28	28	19	9	9	9	28	28	38	28	38	19	28	38	9	25	0	0	0	25	0	0	0
15	Terorismus	1	epravděpodobn	13	13	9	9	5	9	9	9	5	5	13	5	13	3	5	6	5	9	0	0	0	9	0	0	0
16	Odposlech	2	pravděpodobná	38	38	28	19	28	9	19	19	28	9	38	28	38	6	28	38	19	25	0	0	0	25	0	0	0
17	Krádež a vandalismus	2	pravděpodobná	38	38	28	19	19	9	9	9	28	9	38	28	38	19	9	38	28	13	0	0	0	13	0	0	0
18	Falšování identity	3	oce pravděpodo	75	75	42	42	28	14	14	14	42	28	75	56	75	38	42	56	14	28	0	0	0	28	0	0	0
19	Neautorizovaný přístup k médiím	1	epravděpodobn	19	19	19	9	9	5	9	9	14	19	19	19	19	13	14	19	9	14	0	0	0	14	0	0	0
20	Neautorizovaný přístup do IS	1	epravděpodobn	25	25	19	14	9	5	9	9	19	5	25	19	25	13	14	19	5	14	0	0	0	14	0	0	0
21	Použití neautorizovaného SW	1	epravděpodobn	14	14	14	9	9	5	9	9	9	14	14	14	6	9	9	13	5	5	0	0	0	5	0	0	0
22	Použití škodlivého SW	1	epravděpodobn	19	19	9	9	9	5	5	5	5	9	19	14	19	9	9	13	5	5	0	0	0	5	0	0	0
23	Infiltrace komunikace	2	pravděpodobná	38	38	28	19	28	9	9	19	28	28	38	28	25	13	9	38	9	9	0	0	0	9	0	0	0
24	Přesměrování zpráv	1	epravděpodobn	13	13	9	9	5	5	5	5	9	9	13	9	6	3	5	13	5	9	0	0	0	9	0	0	0
25	Zneužití zdrojů	2	pravděpodobná	38	38	28	19	19	9	9	19	19	28	38	28	38	19	9	13	19	28	0	0	0	28	0	0	0
26	Přetížení zdrojů	2	pravděpodobná	38	38	38	9	19	9	9	9	9	38	13	9	13	6	9	13	9	28	0	0	0	28	0	0	0
27	Selhání záložních zdrojů	1	epravděpodobn	19	19	19	5	9	5	5	5	9	19	19	14	19	13	5	19	5	14	0	0	0	14	0	0	0
28	Selhání HW	2	pravděpodobná	28	28	19	19	13	9	9	19	19	19	28	28	25	19	19	25	9	19	0	0	0	19	0	0	0
29	Selhání SW	3	oce pravděpodo	56	56	28	28	19	14	14	28	28	28	56	42	56	28	28	38	14	42	0	0	0	42	0	0	0
30	Selhání sítě	2	pravděpodobná	38	38	19	19	13	9	9	19	19	9	38	28	38	13	19	25	9	28	0	0	0	28	0	0	0
31	Selhání média	2	pravděpodobná	38	38	19	19	13	9	9	19	19	19	38	28	38	13	19	25	9	19	0	0	0	19	0	0	0
32	Selhání veřejné sítě	2	pravděpodobná	38	38	19	19	13	9	9	19	19	19	38	28	38	13	19	25	9	28	0	0	0	28	0	0	0
33	Selhání tiskového zařízení	1	epravděpodobn	14	14	14	14	5	5	5	9	9	5	14	14	13	9	5	6	14	9	0	0	0	9	0	0	0

Obr. 9 Výsledná matice rizik ve vybraném subjektu. Zdroje: [31], [33]

Na obrázku lze pozorovat, že nejrizikovější skupinou jsou především zaměstnanci – uživatelé IS, u kterých je vysoké riziko chyby. Hlavním důvodem je nedostatečné školení. Problémem může být také nedostatečná heslová politika poskytující prostor pro neautorizovaný vstup do systému pod falešnou identitou jednoho ze zaměstnanců. Středně vysoké riziko představuje pro subjekt požár, který je standardně jednou z klasických hrozeb pro veřejnou správu. V návaznosti na tuto analýzu práce představuje vhodná opatření.

11 VYBRANÁ OPATŘENÍ PRO SUBJEKT

Kapitola shrnuje vhodná opatření vyplývající z předchozích analýz v rámci subjektu. Členěna je na organizační opatření a technická opatření. Práce se však zaměřuje především na organizační z důvodu rozsahu a složitosti dané problematiky.

11.1 Návrh organizačních opatření

Mezi nezbytná opatření bylo prioritně zařazeno zavedení plánu školení zaměstnanců v rámci bezpečnosti informací s jasně stanovenou periodicitou. Obsahem by mělo být vždy připomenutí významu ochrany informací. Každý zaměstnanec by si měl také uvědomovat, s jakými aktivy v rámci výkonu své činnosti nakládá a také jaká odpovědnost z toho plyne. Odpovědnost by však měla být rovnoměrně rozložena mezi zaměstnance. Zaměstnanci by také měli být motivováni k dodržování nastavených pravidel organizace.

Zaměstnanci by měli být schopno rozpoznávat bezpečnostní incidenty, zachovat chladnou hlavu a postupovat podle vymezených kroků vedoucích až k hlášení o bezpečnostním incidentu.

Mezi prioritní prvky patří zavedení silné heslové politiky zajišťující přístup pouze autorizované osobě. Nezbytné je nekompromisní vyžadování dodržování zavedené strategie.

Jasně by měla být vymezena i pravidla pro opouštění pracoviště, tedy naplňování zásady prázdného stolu a monitoru. A to i v případě, kdy se nenachází v místnosti další osoba.

Vhodným opatřením je také zavedení klasifikace informací, se kterými je v rámci výkonu činnosti nakládáno. Jednotlivé kategorie informací, by měly mít jasně vymezena pravidla ochrany.

Důležitá je také implementace uživatelského pravidla pro užívání mobilních zařízení, které nebylo doposud nijak řešeno. Dále provést školení o správné aktualizaci operačního systému a vysvětlit rizika instalací různých aplikací, případně je zakázat s náležitým zdůvodněním.

Zavedením manuálu pro uživatele, by se daly shrnout pokyny definující bezpečný postup uživatelů na pracovišti. Zahrnoval by běžné úkony prováděné bezpečným způsobem. Při jejich zavedení jako rutinních by se mohlo snížit riziko vzniku bezpečnostního incidentu.

Neustále by mělo být také upomínáno na nezbytnost hlášení bezpečnostních incidentů. Pokud zaměstnanec takový jev rozpozná, měl by automaticky postupovat podle definovaných pravidel, která jsou nastavena v součinnosti se zmocněncem GDPR.

11.2 Návrh technických opatření

V rámci technických opatření je vhodné zavedení monitorování uživatelů například instalací aplikací pro sledování uživatelů. Vhodnými nástroji může být například:

- Manic Time,
- Activity Monitor (placená verze). [41]

Manic Time je software pro zaznamenávání událostí o používání počítače v rámci celé společnosti. Mapuje strávený čas nad jednotlivými úkoly a k jakým aplikacím je v průběhu pracovní doby přistupováno. Shromážděné informace nejsou sdíleny se třetí stranou, ale pouze uložena v počítači. Využívána jsou pouze lokální uložiště a funguje i bez přístupu k internetu. [42]

Activity Monitor je program pro sledování aktivit na vybraném počítači v reálném čase. Skládá se ze serverové části a klientské části. Serverová část může být instalována na kterýkoli počítač. Klientská část je sledovacím SW, který je instalován na všech zájmových počítačích, které chceme sledovat. Sledování uživatelů je bezpečné a nenápadné. Sledovat zařízení lze pouze pod uživatelským jménem a heslem. SW je navíc zcela neviditelný a ani ve správci úloh nejsou vidět žádné procesy. Lze pořizovat i snímky z plochy vzdáleného počítače a také prohlížení historie prohlížení webových stránek. [41]

Dalším vhodným opatřením je vymezení nebo úplné zakázání vybraných webových stránek, jako jsou sociální sítě, vlastní emailová korespondence a podobně. Případně tuto problematiku lze jednoduše řešit na základě firewallu.

Vhodné se jeví také zakázání používání flash disků, případně zákaz portů. Flash disky jsou obvykle nositeli škodlivých SW, které mohou být velkým rizikem. Společně s tím bylo diskutováno zamknutí či zaplombování skříně pro zamezení připojování vlastních zařízení nebo zasahování do hlavních částí HW.

V neposlední řadě je také vhodné oddělení záložního disku od serveru, jelikož stávající řešení je značně nebezpečné. V případě poškození serveru by mohlo dojít i k poškození disků. Navíc je v současné době zařízení zbytečně zahříváno. Zálohy by měly být taky pro lepší ochranu kryptovány.

12 BEZPEČNOSTNÍ MANUÁL

Kapitola shrnuje řešení vybraných navržených opatření pro subjekt. Na základě předchozích analýz vyplynulo jako nezbytné opatření v rámci heslové politiky. Na autorizaci uživatele je postaven přístup do celkového systému. Proto je nutností implementovat vhodnou heslovou politiku vyhovující současným trendům.

12.1 Aktualizace analýzy rizik

Vytvořením dokumentací v rámci analýzy rizik není vhodné vnímat tuto problematiku jako vyřešenou. Je nezbytné, tuto analýzu rizik aktualizovat. Vhodným nástrojem, s přívětivým prostředím, hodnotím nástroj RAMSES, který je založený na metodice RAC RAMSES vycházející z normy ISO/IEC 27005. Lze vytvořit dotazníky hrozeb a zranitelností, hodnocení rizik a na ně předem vytipovaná opatření. Vytváří logický koncept postupu analýzy na webovém rozhraní s povolením přístupu neomezeného počtu uživatelů, které mohou zadávat parametry pro vyhodnocení hrozeb a zranitelností, které odrazí jasný obraz stavu rizik v subjektu. [43]

Nástroj je designován vhodněji, než program RISKAN. Je přímo zaměřen na provozování či implementaci ISMS. Využívá v průběhu hodnocení stromu událostí, kdy je možné důsledněji hodnotit důsledky propojení jednotlivých aktiv v různých procesech. Bude však nezbytné drobně upravit segmentaci aktiv. RAMSES poskytuje velice hodnotné grafické i písemné dokumentace zachycující problematiku z mnoha úhlů pohledu. [43]

12.2 Heslová politika

Již audit bezpečnostních opatření vyhodnotil jako vhodné opatření vytvoření nové heslové politiky. Je nezbytné uvědomit si, že heslo je vstupním prvkem, jehož odolnost je každým rokem snižována zvyšováním výpočetního výkonu počítačů. U mnohých organizací zamrzla hesla na parametrech 6 znaků a minimálně jedné číslice a to je dnes již výrazně nedostačující. Obzvláště pokud se užije celé slovo a číslice se umístí na konec. Přitom v dnešní době už není problémem prolomit heslo o 8 znacích i se speciálními znaky a číslicemi. [44], [45]

Ze statistických údajů vyplývá, že 70 % uživatelů používá uniklá hesla pro další služby minimálně rok a dalších 40 % více než 3 roky. V 87 % uživatelé modifikují pouze koncovou část hesla a 11 % pouze začáteční část. Vývoj prolamování hesel hrubou silou jde velice

rychle vpřed, jak dokumentuje tabulka 20, ve které je porovnána doba prolomení v roce 2016 a 2019. [46], [47]

Tab. 20 referuje o době prolomení hesla hrubou silou na vybraných zařízeních v roce 2016 a 2019

Parametry	Rok 2016	Rok 2019		
	notebook*	PC	grafické karty	superpočítač, cloud
6 znaků, pouze malá nebo velká písmena, číslice	1 minuta	31 minut	19 sekund	0,019 sekund
8 znaků, pouze malá nebo velká písmena, číslice	1 den	28 dnů	7 hodin	24 sekund
8 znaků, malá i velká písmena, číslice	2 měsíce	6 let	22 dní	31 minut
8 znaků, malá i velká písmena, číslice, speciální znak (32)**	5 let	45 let	165 dní	4 hodiny
9 znaků, malá i velká písmena, číslice	11 let	několik století	4 roky	1,3 dne
9 znaků, malá i velká písmena, číslice, speciální znak (32)	45 let	několik století	36 let	13 dní
10 znaků, malá i velká písmena, číslice	65 let	několik století	několik století	82 dní
10 znaků, malá i velká písmena, číslice, speciální znak (32)	4 240 let	několik století	několik století	3 roky

* Střední doba odhalení. Zdroj: [44], [46]

** 32 různých speciálních znaků (např.: +, -, @, !).

Jak tabulka naznačuje, dnes už není zcela vyhovující používat parametry hesla v prvních 3 řádcích tabulky. Vhodné heslo by nemělo:

- využívat celé slovo,
- mít méně než 8 znaků,
- užívat jen malé nebo velké písmeno v kombinaci s číslem.

Pro tvorbu dostatečného hesla dle vlastních parametrů lze využít generátory náhodných hesel, které jsou běžně dostupné online. Další možností je dvoufázové ověření nebo DiceWare Passphrase (jednoznačná fráze o 25 až 64 znacích i s využitím mezer, která nahrazuje heslo).

Další alternativou je využití serveru pro správu hesel, jakým je například KeePass - Password Safe, který je nejvyužívanějším systémem správy hesel na světě. Jedná se o databázi hesel běžící na vlastních serverech, kde je možno přistupovat ke správě hesel pod jedním hlavním heslem. Jen se jedná o placený produkt. Existuje však i neplacená verze – Keepass verze 2.41, která se dá se používat i lokálně. [48], [49]

Možné je tedy nastavit vhodnou heslovou politiku, která bude komfortní pro zaměstnance a nebude překážkou ji dodržovat. Na základě předešlých informací doporučuji využití následujících parametrů:

- 9 znaků,
- malá i velká písmena,
- číslice,
- využití speciálního znaku
- unikátní,
- obměňované 1x za 3 měsíce.

Doporučuji subjektu využití jedné z následujících metod. Volila bych spíše volnější přístup. Nastínila bych tyto možnosti zaměstnancům a nechala každého vybrat takovou metodu, která mu bude vyhovovat nejlépe. Přeci jen to bude on, kdo si heslo bude muset pamatovat. Následující hesla vypadají v konečné fázi možná velice děsivě a nezapamatovatelně. Důležitá je však právě vybraná cesta, jakou si daný jedinec heslo vytvoří. Stačí si pak následně pamatovat pomůcku a heslo je schopný dáti znovu dohromady.

L33t

Tato metoda se zakládá na tzv. l33t žargon, kdy se nahradí písmena číslicemi nebo speciálními znaky. To může být pro dobré zapamatování na základě grafické podobnosti znaků, tedy například A-@, E – 3, O – 0, I - ! a podobně. Výsledné heslo se pak vytvoří tak, že vezmeme desetiznakové slovo jako například „znamenitě“ přetvoříme na „zn@M3n!tě“. Nebo „zapamatuj“ můžeme upravit na „zA?am4tuj“.

Říkanka

Vybereme si nějakou snadno zapamatovatelnou říkanku. Například „dá do toho čtyři rány a už je hotovo“. V prvním kroku nahradíme slova na číslice a ze zbylých slov ponecháme

jen první písmena. Vznikne nám tedy „ddt4rahbh“. Teď můžeme na základě předchozí metody doplnit speciální znak a alespoň jeden velký znak. To už zcela pocitově. Pro mne by bylo výsledné heslo nejspíše „dDt4r@ubjh“.

Nebo takto „Čtyři stáli u postýlky, pátý těšil: „Neplakej“. Dle prvního kroku převedeme na základní tvar - 4sup5t“n“. V tomto případě stačí doplnit jen velké písmeno a výsledné heslo může znít následovně 4sup5t“N“.

V rámci této metody pak stačí zapamatovat si danou říkanku a šifrování už by mělo vycházet z citu vlastníka hesla tak, aby byl schopen vybavit si pomocí mnemotechnické pomůcky – říkanky samotné heslo.

Kombinace

Vymyslíme si vhodné slovo, které nesouvisí s mazlíčkem ani rodinou. Spíše něco více nespojitelné s Vaší osobou. Je dnes až směšně zjistit jméno Vašeho psa, které je sdíleno na sociálních sítích Vašimi dětmi. Proto vezmeme například slovo „sojka“ a rok 1945. Poté proložíme slovo tímto rokem a vznikne nám „s1o9j4k5a“. Následně stačí doplnit speciální znak a jedno velké písmeno. Výsledkem může být „s1o9J4k5@“

12.3 Bezpečné chování na pracovišti

Pro základní nastavení bezpečnosti na pracovišti je nezbytné respektovat následující bezpečnostní zásady jako vlastní bezpečnostní „desatero“:

1. Nesdělovat své heslo do IS třetím osobám ani nástěnce.
2. Nikdy neposílat přihlašovací jména a hesla emailem.
3. Neotevírat a neodpovídat na podezřelé e-maily.
4. Respektovat nastavenou heslovou politiku.
5. Vlastní data pravidelně zálohovat.
6. Dodržovat zásadu prázdného stolu a monitoru.
7. Nepřipojovat žádná zařízení k PC.
8. Provádět jen pracovní úkony na PC. (ne sociální sítě, soukromá korespondence, atd.)
9. Jakékoli nestandardní chování PC okamžitě hlásit.
10. Řídit se výše zmíněným.

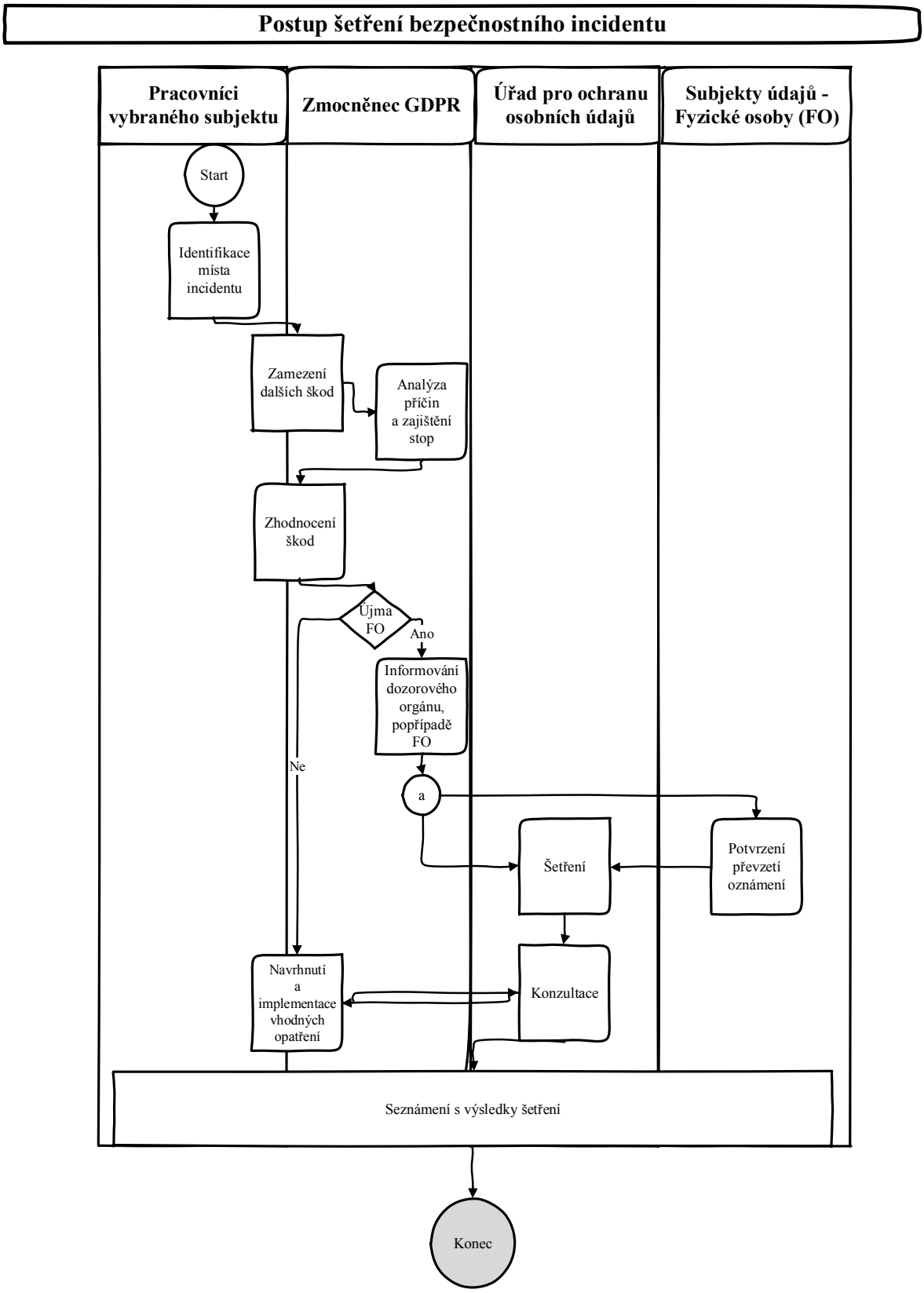
Zásada prázdného stolu a prázdné obrazovky v rámci nejen papírových dokumentů, ale i pro přenosová média. Zvláštní ohled by měl být brán hlavně na citlivé nebo kritické informace. Pro tato významná aktiva by měl být vyhrazen zvláštní uzamykatelný prostor.

12.4 Zvládání bezpečnostních incidentů

Bezpečnostní incident se může projevit jako:

- ztráta služby, zařízení nebo vybavení,
- chyby fungování nebo přetížení systému,
- porušení opatření fyzické bezpečnosti,
- lidské chyby, porušení právních předpisů,
- nesoulad s pokyny,
- porušení přístupu,
- pokus o narušení nebo útok na bezpečnost.

Pokud je jakákoli z výše jmenovaných událostí zaznamenána, je nezbytné ji okamžitě hlásit. Postup je možný podle následujícího modelu vyobrazeného na obrázku 10.



Obr. 10 Model procesu šetření bezpečnostního incidentu. Zdroj: [vlastní]

13 SHRNUTÍ

Vybraný subjekt má zvoleného IT technika s dlouholetou praxí, který zabezpečuje veškerou technickou datovou ochranu. Tato správa je na dobré úrovni, nebyla však nijak dokumentována. Scházela také dokumentace aktiv subjektu a také řízení rizik. Z toho plynou možné bezpečnostní mezery odhalené auditem bezpečnostních opatření. Jednalo se především o nedostatečné školení zaměstnanců. Lidský faktor, je však největší hrozbou systému.

Je také přehnaně spoléháno na antivirový program, který však neřeší všechny rizika narušující bezpečnost informací uvnitř systému. Subjekt se však nebrání zavedení řízení bezpečnosti informaci.

Problematické také je, že za velké množství technických aktiv odpovídá pouze jeden člověk a to IT technik. Znalosti v této oblasti má také místostarosta obce, který bohužel nebyl zcela seznámen se zavedenými postupy. V případě vzniku bezpečnostního incidentu se v rámci obnovy plnohodnotně počítá s řešením pouze ze strany IT technika a zmocněnce GDPR. Tento nedostatek bude nezbytné odstranit pomocí rozvržení a větší zainteresování zaměstnanců do řešení bezpečnostních incidentů.

Vytvořena byla dokumentace aktiv, hrozeb a zranitelností systému, na jejichž základě byla provedena analýza rizik vymezující nejpalčivější rizika. V návaznosti byla vymezena opatření na ošetření rizika a některá opatření blíže rozpracována. Jednalo se především o bezpečnostní manuál pro implementaci vhodné heslové politiky a také bezpečnostních doporučení pro práci na pracovišti. Namodelován byl také proces pro případ zjištění bezpečnostního incidentu.

Obecně lze říci, že subjekt se považuje za malý prvek, na který pravděpodobně nebude veden útok, a spoléhá na zodpovědnost svých zaměstnanců. Je však nezbytné pochopit, že je to stále subjekt, který nakládá s velkým množstvím citlivých osobních údajů, jež je nezbytné chránit.

ZÁVĚR

Diplomová práce si kladla za cíl posouzení stavu bezpečnosti informací ve vybraném subjektu. V první části seznamovala s problematikou bezpečnosti informací, a také právním a normativním ukotvením v České republice. Zásadní pozornost byla věnována zejména problematice ISMS.

Následně práce objasnila základní charakteristiky vybraného subjektu a to i prostřednictvím řízeného rozhovoru. V rámci rozšíření povědomí o stavu ISMS v rámci subjektu, byl proveden audit bezpečnostních opatření, který vymezil základní problematické okruhy. Pro lepší volbu strategie postupu byla provedena SWOT analýza, která identifikovala silné, slabé stránky subjektu, ale také příležitosti a hrozby. Na základě vytyčených cílů byla provedena analýza rizik, pro kterou bylo nezbytné identifikovat, klasifikovat a vzájemně vztáhnout aktiva a hrozby. Dále bylo postupováno s použitím nástroje RISKAN. Vymezeny byly zranitelnosti v souvislosti aktivum – hrozba. Toto hodnocení však proběhlo v rámci zvolených hranic a hloubky analýzy rizik omezené pouze na primární aktiva a v rámci podpůrných aktiv na personál. Z předchozích kroků byla vytvořena mapa rizik zobrazující největší rizika, která byla následně ošetřena vhodnými opatřeními.

Hlavním výstupem práce jsou dokumentace aktiv, hrozeb a rizik. V návaznosti byla vytvořena také vhodná opatření navržená především v organizačním rámci. A to s ohledem na rozsah a technickou složitost opatření technických. Konkrétně se jednalo o vytvoření bezpečnostního manuálu pro zaměstnance, jehož součástí je vymezení optimální heslové politiky a vhodných pracovních návyků v pracovním prostředí. Namodelován byl také postup při šetření bezpečnostního systému, pro snazší pochopení celého procesu.

Cíl diplomové práce si dovoluji, s přihlédnutím k výše zmíněným výstupům, považovat za splněný.

SEZNAM POUŽITÉ LITERATURY

[1] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2013. ISBN 978-80-7251-397-0.

[2] NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017, 304 s. Právo pro praxi. ISBN 978-80-271-0668-4.

[3] *GDPR - Obecné nařízení o ochraně osobních údajů prakticky: Pseudonymizace osobních údajů* [online]. 2018 [cit. 2018-04-02]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/pseudonymizace-osobnich-udaju/

[4] JAŠEK, Roman a David MALANÍK. FAKULTA APLIKOVANÉ INFORMATIKY. *BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 137 s. ISBN 978-80-7454-312-8.

[5] DRASTICH, Martin. Systém managementu bezpečnosti informací. Praha: Grada, 2011, 128 s. Průvodce (Grada). ISBN 978-80-247-4251-9.

[6] HRONEK, Jiří. KATEDRA INFORMATIKY, UNIVERZITA PALACKÉHO. *Informační systémy*. Olomouc, 2007, 165 s. Dostupné také z: http://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

[7] Top 10 technologií pro digitální veřejnou správu. *Computerworld: from IDG* [online]. International Data Group, 2016, 15. 07. 2016 [cit. 2019-01-16]. Dostupné z: https://computerworld.cz/analyzy-a-studie/top-10-technologii-pro-digitalni-verejnou-spravu-53201

[8] ČSN ISO/IEC TR 13335-1 Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security

[9] GARTNER. *IT glossary* [online]. [cit. 2019-04-15]. Dostupné z: https://www.gartner.com/it-glossary/operational-technology-ot/

[10] ČESKO. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ve znění pozdějších předpisů.

[11] ČESKO. Zákon č. 412/2005 Sb., ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů.

[12] ČESKO. Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních a o kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

[13] ČESKO. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.

[14] EVROPSKÁ UNIE. Nařízení Evropského parlamentu a Rady EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Obecné nařízení o ochraně osobních údajů – General Data Protection Regulation – GDPR).

[15] ČESKO. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

[16] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

[17] ČESKO. Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

[18] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[19] MATULA, Jan. *Informační management: normy, frameworky a nejlepší praxe v řízení služeb IT (ITSM)*. V Opavě: Slezská univerzita, Filozoficko-přírodovědecká fakulta v Opavě, Ústav bohemistiky a knihovnictví, 2017, 118 s. ISBN 978-80-7510-264-5.

[20] ISACA. *COBIT 5: A business framework for the Governance and Management of Enterprise IT*. United States of America: ISACA, 2012, 94 s. ISBN 978-1-60420-237-3.

[21] ISMS - Seriál o řízení bezpečnosti. *GiTy: Bezpečnost v kostce* [online]. [cit. 2019-01-16]. Dostupné z: http://www.chrantesidata.cz/cs/art/472-isms-serial-o-rizeni-bezpecnosti#start

[22] JOHNSON, Carinne N. The benefits of PDCA: Use this cycle for continual proces improvement. *Best Of Back to Basics, Leden 2016 edition* [online]. [cit. 2019-03-15]. Dostupné z: http://asq.org/quality-progress/2002/05/problem -solving/the-benefits-of-pdca.html

[23] VANĚK, Zdeněk. DCIT. *ISMS – systém řízení bezpečnosti informací: řešení požadavků zákona o kybernetické bezpečnosti*. Praha, 2015.

[24] HUMPHREYS, Edward. *Implementing the iso/iec 27001 isms standard, second edition*. 2nd ed. Boston: Artech House, 2016. ISBN 9781608079308.

[25] *Risk Analysis Consultants: Řada norem ISO/IEC 27000* [online]. 2017 [cit. 2018-04-02]. Dostupné z: http://www.iso27000.cz

[26] ČSN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017. 36 s. Třídící znak 369790

[27] ČSN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací - Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 28 s. Třídící znak 36 9797

[28] ČSN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 76 s. Třídící znak 36 9798

[29] ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. 62 s. Třídící znak 36 9790

[30] Konzultace a poznámky ze seminářů předmětu „Analýza rizik II.“ s Ing. Slavomírou Vargovou, PhD.

[31] Informace od managementu vybraného subjektu.

[32] PALMER, S., WEAVER, M., *Úloha informací v manažerském rozhodování,* Václav Dolanský, Praha: Grada, 2000. ISBN 80-7169-940-3

[33] Řízený rozhovor se starostou, místostarostou a IT technikem vybraného obecního úřadu.

[34] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.

[35] ČESKO. Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon).

[36] ČESKO. Zákon č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů.

[37] ČESKO. Vyhláška ministerstva vnitra č. 207/2001 Sb., k provedení zákona č. 301/2000 Sb., o matrikách, jménu a příjmení a o změně některých souvisejících zákonů.

[38] ČESKO. Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných čísel a o změně některých zákonů v souladu s Instrukcí, kterou vydalo Ministerstvo vnitra.

[39] ČESKO. Zákon č. 128/2000 Sb., Zákon o obcích (obecní zřízení)

[40] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[41] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

[42] *ManicTime* [online]. 2019 [cit. 2019-04-24]. Dostupné z: https://www.manictime.com

[43] Risk Analysis Consultants. *RAC RAMSES: Řízení bezpečnosti informací organizace.* [online]. 2019 [cit. 2019-04-24]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/Ramses

[44] Za jak dlouho hacker prolomí vaše heslo?. In: *Digitální sebeobrana: Školení bezpečnosti pro neajťáky* [online]. 2018, 18. 12. 2018 [cit. 2019-03-30]. Dostupné z: https://www.zaskolit.cz/za-jak-dlouho-hacker-prolomi-vase-heslo/

[45] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

[46] SMEJKAL, Radek. ETNETERA GROUP. *Entetera: Statistika hesel, vytváření slovníků, optimalizace lámání hesel* [online]. 2018 [cit. 2019-04-24]. Dostupné z: https://www.etnetera.cz/blog/statistika-hesel-vytvareni-slovniku-optimalizace-lamani-hesel

[47] PLECHÁČEK, Petr a Daniel KOBRLE. Analýza: Heslová politika, základ bezpečného IT. *CIO Business World* [online]. 2016, 29. 4. 2016, 2 [cit. 2019-03-30]. Dostupné z: https://issuu.com/eyceskarepublika/docs/8_9_analyza

[48] PLEASANT SOLUTIONS, *Pleasant Password Server* [online]. Canada: Copyright © 2019 Pleasant Solutions. All rights reserved, 2019 [cit. 2019-03-30]. Dostupné z: https://pleasantsolutions.com/passwordserver/

[49] REICH, Dominik. *KeePass Password Safe: What is KeePass?* [online]. 2019 [cit. 2019-04-21]. Dostupné z: https://keepass.info

[50] RYBÁKOVÁ. Národní úřad pro kybernetickou bezpečnost. *Pomůcka k auditu bezpečnostních opatření podle zákona o kybernetické bezpečnosti*. 2.1. 32 s. Dostupné také z: https://www.govcert.cz/download/kii-vis/container-nodeid-580/vkbchecklistfinalv21rev.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACC	Accidental threat – náhodná hrozba.
AVL	Availability - dostupnost.
CNF	Confidentiality - důvěrnost.
COBIT	Control Objektives for Information and Related Technology.
ČR	Česká republika.
DLB	Deliberate threat – úmyslná hrozba.
EU	Evropská unie.
ENV	Environmental threat – přírodní hrozba.
GDPR	General Data Protection Regulation.
HW	Hardware.
INFOSEC	Bezpečnost informací.
INT	Integrita.
IS	Informační systém.
ISACA	Information Systems Audit and Control Foundation.
ISM	Information Security Management.
ISMS	Systém řízení bezpečnosti informaci - Information Security Management System.
ISUI	Informační systému územní identifikace.
IoT	Internet of Things – Internet věcí.
ITIL	Information Technology Infrastucture Library.
ITSM	IT Systém Management.
KII	Kritická informační infrastruktura.
OHD	Object hierarchy decomposition – objektově hierarchická dekompozice.
OT	Operační technologie.
PDCA	Plan, Do, Check, Act – plánuj, dělej, kontroluj, jednej.

SŘBI	Systém řízení bezpečnosti informaci.
SW	Software
VIS	Významný informační systém.
VKB	Vyhláška o kybernetické bezpečnosti.
WiFi	Wireless Fidelity.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ŘÍZENÝ ROZHOVOR

Obecné otázky v rámci normy ISO/IEC 27 001

- *Využívají se mobilní zařízení pro práci na dálku?*

  Využívá se jen mobilní telefony, které nemají nastavené účty pro příjem emailové pošty. Výjimkou je místostarosta obce.

- *Jaká zařízení jsou využívána k práci z domova, popřípadě jsou využívána k práci v zaměstnání?*

  Vzdálený přístup do sítě využívá pouze správce sítě, účetní pro správu účetních agend.

- *Jak je zabezpečen princip oddělení povinností od vlastních zájmů?*

  Není zabezpečen. Zaměstnancům není nijak technicky bráněno v přístupu na jakékoli webové stránky. Mohou i do vlastní emailové pošty. Nemohou však instalovat programy.

- *Existují bezpečnostní opatření pro práci na těchto zařízeních?*

  Využívá se uživatelských účtů. Každý zaměstnanec se přihlašuje na vlastním PC do svého účtu, který má jen omezené pole působnosti.

- *Jsou prověřováni budoucí zaměstnanci a jsou využívány doložky ke smlouvám?*

  Ano, ale nejsou přijímáni na základě parametrů počítačové bezpečnosti nebo rozsáhlejší gramotnosti. Subjekt hodnotí pro výběr vhodného kandidáta jiná kritéria. Tato oblast se dá vyřešit po nástupu do pracovního poměru proškolením.

- *Je využito smluvního vztahu pro odpovědnost k organizaci? (Smlouva o mlčenlivosti)*

  Ano, každý zaměstnanec má podepsanou smlouvu o mlčenlivosti, je mu znám rozsah a možné následky plynoucí z porušení.

- *Jsou prováděny školení o bezpečnosti informací?*

  Bylo provedeno v rámci zavádění GDPR. Zaměstnanci byli také školeni externí firmou.

- *Jak často školíte zaměstnance v rámci bezpečnosti dat?*

  Od posledního školení (v rámci GDPR) nebylo provedeno. V rámci SW pro výkon přenesené působnosti jsou školení prováděna nezávisle na subjektu. Zajišťuje je stát.

- *Je prováděna zpětná vazba na to, zda bylo školení přínosné?*

  Pouze zaměstnanci mezi sebou, nikoli centrálně.

- *Účastní se školení zaměstnanců i správce sítě?*

  Ano, při školení stavebního úřadu.

- *Řídíte aktiva v rámci organizace?*

  Nejsou ani identifikována. Jsou schopni je však identifikovat, ale nevedou ji nijak dokumentovaná. Jsou uchovávána na HW počítače a ukládány na server, který se nachází v budově. Data jsou zálohována zrcadlově a jednou měsíčně je provedena záloha na externí disk.

- *Byla provedena klasifikace informací, se kterými se zde nakládá?*

  Ano, provedl ji zmocněnec GDPR v rámci vstupní analýzy. A to pro zjištění kritických míst, která byla v rozporu s GDPR. Jinak nejsou.

- *Jak je předcházeno neoprávněném vyřazení, modifikaci, odstranění nebo zničení informací na médiích?*

  Zálohou dat.

- *Jak je řízen přístup k informacím?*

  Uživatelskými účty, přístup do agend jen dle pracovního zařazení. Jednotlivé SW mají také svá hesla. Je oddělena samospráva od výkonu přenesené působnosti. Důležité je, že data jsou ukládána na vlastní server se zálohou. Jedná se především o data o občanech obce, vedení hřbitova nebo komunální poplatky. Další část je přenesená působnost a to zejména v rámci matriky (check-point a další veřejné registry, do kterých se přistupuje pod předem stanovenými rolemi, které opravňují uživatele ke konkrétním úkolům. Tak však může docházet k nesouladu informací ve veřejných a samosprávných registrech. Přenesená působnost má vlastní zákonnou úpravu a využívá vlastní SW.

- *Jaké vybavení je použito k přístupu k informacím?*

  PC, 2 notebooky, mobily s operačním systémem android.

- *Kdo má přístup k sítím a síťovým službám?*

  Správce sítě, zaměstnanci.

- *Je dodržen princip oddělení sítí?*

  Ano, dle přidělených práv.

- *Jak je zabezpečen postup při přenosu informací?*

  Plánuje se zavedení flash disků, které chrání PIN a data na nich jsou kryptována. Zatím sem tam využívají vlastní flash disky. Tomu je možno zabránit zákazem portů. To by však pravděpodobně způsobilo komplikace při řešení problémů administrátorem. Také pro externí správce při aktualizacích SW.

- *Jak je zabezpečen přenos informací při činnosti organizace a také externím stranám?*

  V rámci spisové služby je zabezpečeno elektronickým podpisem. K tomu je využito tokenu, kde se zadává čtyřmístný PIN. V případě, že není zadán 10x správně, disk se okamžitě naformátuje.

  Problematický je email, který je propojen s webem v rámci kterého chodí velké množství spamů. To už je však v řešení.

- *Jsou registrováni uživatelé, kteří přistupují k informacím?*

  Ano, dle přidělených práv.

- *Jsou přidělena přístupová práva uživatelům?*

  Ano.

- *Využíváte systému správy hesel?*

  Ano, budou se i každé 3 měsíce obměňovat.

- *Využíváte IoT? Pokud ano jaká?*

  Prozatím ne, ale uvažuje se nad koupí televize nebo projektoru.

- *Používáte kryptografická opatření?*

  Prozatím ne.

- *Jak probíhá elektronické předávání zpráv?*

  Zejména ISDS, tedy již zmíněný elektronický podpis a pak email, který je zabezpečován externě mailovým serverem.

- *Je implementována ochrana proti malwaru?*

  Ano, pomocí antivirového programu ESET end point. Jsou prováděny pravidelné testy PC a také jsou pravidelně aktualizovány. Upozorňuje i na nebezpečné přílohy v rámci emailové korespondence. Pro ochranu serveru se využívá ESET file security.

- *Zajišťujete integritu provozu systému?*

  Zajišťuje ji administrátor.

- *Provádíte audit informačních systémů?*

  Ne.

- *Provádíte testování bezpečnosti?*

  Ne.

- *Jak je zajištěna bezpečnost informací v dodavatelských vztazích?*

  Ošetřena smluvně se subjektem Gordic v rámci ekonomické agendy, matriky a evidence obyvatel. Druhým subjektem je Vita SW pro stavební úřad.

- *Jak jsou řízeny incidenty bezpečnosti informací?*

  Vše je směrováno na zmocněnce GDPR.

- *Je vytvořena odpovědnost za bezpečnostní incidenty?*

  Dle pracovního zařazení na konkrétního zaměstnance.

- *Jak je zabezpečeno hlášení bezpečnostních incidentů?*

  Ve spolupráci se zmocněncem GDPR, u kterého si úřad vyžádá formulář pro hlášení.

- *Jak jsou posouzeny takové úniky informací a kdo je posuzuje?*

  Ve spolupráci se zmocněncem GDPR, kterému se budou hlásit všechny dostupné informace, a zmocněnec bude posuzovat situaci.

- *Je stanoven postup pro bezpečnostní incidenty?*

  Vyřizoval by zmocněnec.

- *Jak se ponaučíte ze vzniklého incidentu?*

  Nechají si navrhnout zmocněncem.

- *Máte vytvořenou politiku bezpečnosti informací?*

  Jen zaměstnanci si při školení externí firmou poznačili informace, které byly přijaty za vlastní.

Technický a organizační okruh otázek

- *Jaké využíváte operační systémy (dále jen „OS“)?*

  Server používá Windows 2016 standard, PC Windows 10 a Windows XP v rámci notebooku pro rozhlas.

- *Jak často aktualizujete OS?*

  Automaticky se aktualizuje každé úterý. Dále se kontrolují namátkově. Server se aktualizuje vzdáleně cca 1x za 14 dní.

- *Kdo má fyzický přístup k serveru? Disponují uklízečky generálním klíčem?*

  Jen správce IT disponuje přístupem.

- *Jsou data uložená na serveru šifrovaná?*

  Nejsou, protože běží na firebird.

- *Jak je zabezpečena WiFi?*

  Je zabezpečena pomocí WPA2.

- *Co máte za Access point?*

  TP link 841n, ale je plánován UniFi.

- *Jak jej aktualizujete?*

  Aktualizuje se dle možností. Naposledy před 14 dny. Kódy se mění zřídka.

- *Jaké využíváte služební telefony?*

  Všichni mají telefony s OS Android. Jedná se o vedoucího stavebního úřadu, matrikářka, starosta, místostarosta a administrativní pracovnice.

- *Mohou zaměstnanci volně instalovat aplikace?*

  Ano, není nijak omezeno.

- *Proběhlo nějaké školení jak s takovým „chytrým telefonem“ zacházet?*

  Ne.

- *Aktualizuje se nějak hromadně OS ve služebních telefonech?*

  To má na starosti místostarosta obce. Zaměstnanci jsou poučení, aby v případě nutnosti řešili problémy přímo s ním.

- *Tiskárna je vždy součástí kanceláře nebo i někde volně stojí na chodbě?*

  Jedna je centrální síťová v kanceláři administrativy. Další je pokladní (lokální) pro tisk svých dokladů. Poté účetní má pro svoje doklady. Matriční úřad má svou. Stavební svou centrální. Poslední je v rámci vyřizování spisové služby na obálky.

- *Je tisk spuštěn automaticky nebo až po zadání hesla na tiskárně? Případně jinak?*

  Tisk není pod heslem, ale je možné implementovat. Je však omezen tisk na černobílý.

- *Jaký je využíván internetový prohlížeč*

  Mají k dispozici explorer na klasické nástroje při výkon přenesené působnosti. Zbytek v rámci výkonu samostatné působnosti využívá firefox a google chrome.

- *Jak je řešen firmware? SW/HW forma?*

  Jedná se o Fujitsu update, který je automaticky spouštěn, ale kontrolován technikem a hlídá si aktualizace BIOSu. Aktualizuje se SW ne HW.

- *Jak je zajištěn fyzický přístup k PC? Je více PC v jedné kanceláři? Jsou prostory průchozí?*

  Každé pracoviště má vlastní PC a rovněž v každé kanceláři je jedno PC. Kanceláře jsou v rámci 1 podlaží průchozí všechny.

- *Jak je nastaveno bootování? Není možné spustit portable systém z flash disku/CD/DVD třeba Kali Linux/Kubunu nebo jinou distribuci?*

  Není zaheslováno. Využívá jej technik pro spuštění z hard disku.

- *Jak je zabezpečena PC bedna?*

  Není zabezpečena, má k ní však přístup jen zaměstnanec a IT technik. Je možné zajistit ji plombou.

- *Jak je zajištěna implementace zákona o kybernetické bezpečnosti v rámci úseků, kde je vykonávána práce s významnými informačními systémy?*

  Začíná být řešena v rámci této práce. Byla a je řešena v rámci školení.

- *Využíváte nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí? Sledujete logy?*

  Ne, nebyly realizovány žádné útoky, proto subjekt neviděl důvod zavádět.

- *Jsou uživatelům po ukončení pracovního poměru odebrána všechna přidělená přístupová oprávnění?*

  Ano, kompletně se vše mění i login v rámci Czech point.

- *Jsou prováděny kontroly záloh?*

  Ano, neustále.

- *Je zaveden postup pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů?*

  Je zaveden postup při výpadku elektrické energie – nahozením záložního zdroje, který je schopný nahradit zdroj po dobu 2-3h IT technikem manuálně. Síťové disky jsou nové.

- *Lze rozpoznat na serveru, kdo provedl jakou změnu?*

  Jen technik a zaměstnanci v rámci svých databází. V rámci vlastních loginů to poté může sledovat spisovka a pak také vlastní část externích dodavatelů SW.

- *Jsou dostupné údaje, kdo se kdy přihlásil k počítači?*

  Je to vidět v systému v rámci správce událostí.

- *Jak dlouho by trvalo obnovení dat ze zálohy v případě bezpečnostního incidentu?*

  Když by nebyly napadeny síťové disky, tak jen nainstalování a pak obnova. To by mělo zabrat chvíli. Důležitý je však rozsah incidentu (ransomware). Také je plánováno oddělení záloh od serveru.

- *Jsou provedena opatření pro odstranění nebo blokování přenášených dat, která neodpovídají požadavkům na ochranu integrity komunikační sítě?*

  Nejsou.

- *Jsou využívány nástroje pro ochranu integrity vnitřní komunikační sítě, která zajistí její segmentaci?*

  Částečně zavedeno v rámci poštovního serveru TPweb – proti spamu. Úřad nikoli, jen centrálně přes poskytovatele internetu. Nejsou si však jisti co vše filtrují.

- *Jsou nastaveny požadavky na hesla jako minimální délka osm znaků?*

  Ano, zejména na server, switch, router, VDSL modem, jsou silná hesla a je stanovena heslová politika. Do PC je požadována délka 8 znaků.

- *Je požadována složitost hesla tak, že musí obsahovat tři z následujících požadavků?*

  1) nejméně jedno velké písmeno

  2) nejméně jedno malé písmeno

  3) nejméně jednu číslici

  4) nejméně jeden speciální znak

  Některé splňují (zejména ty, které přidělil správce). Zbytek si volil vlastní a ne všechny splňují tyto parametry.

- *Využívá administrátor heslo delší než 15 znaků?*

  Ano.

- *Vedou se záznamy o změnách přístupu – komu kdy kdo přidělil účet nebo u něj v podstatě cokoli měnil?*

  Ne. Je však vše členěno a tam lze dohledat. Matrika vlastní, síťová pokladna vlastní agendu a stavební úřad také.

- *Vedou se záznamy o tom, že se někdo pokoušel neúspěšně přihlásit?*

  Nevedou, protože subjekt nepředpokládá, že se tak děje.

PŘÍLOHA P II: AUDIT BEZPEČNOSTNÍCH OPATŘENÍ - ORGANIZAČNÍ OPATŘENÍ

Tab. 21 Audit bezpečnostních opatření - Systém řízení bezpečnosti informací

KII	VIS			N	P	Z	NA
X		odst. 1 a)	Je stanoven rozsah ISMS.	X			
X	X	odst. 1 b) odst. 2 a)	Je zaveden proces řízení rizik.	X			
X	X	odst. 1 c) odst. 2 b)	Jsou vytvořeny, schváleny a zavedeny bezpečnostní politiky v oblasti ISMS, zavedena příslušná bezpečnostní opatření.	X			
X		odst. 1 d)	Zaveden proces monitorování účinnosti bezpečnostních opatření.	X			
X		odst. 1 e)	Zaveden proces vyhodnocování vhodnosti a účinnosti bezpečnostní politiky.	X			
X		odst. 1 f)	Audit kybernetické bezpečnosti je prováděn nejméně 1-krát ročně.	X			
X		odst. 1 g)	Zajištěno vyhodnocení účinnosti ISMS, které obsahuje hodnocení stavu ISMS včetně revize hodnocení rizik, posouzeny výsledky provedených kontrol a auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně 1-krát ročně.	X			
X		odst. 1 h)	Je prováděna aktualizace ISMS a související dokumentace na základě zjištění auditů kybernetické bezpečnosti, výsledků hodnocení účinnosti ISMS a v souvislosti s prováděnými změnami.	X			
X		odst. 1 i)	Řízen provoz a zdroje ISMS, zaznamenávány činnosti spojené s ISMS a souvisejícím řízením rizik.	X			
	X	odst. 2 c)	Prováděna aktualizace zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí, a to nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami.	X			

Zdroj: [31], [33], [50]

Tab. 22 Audit bezpečnostních opatření - Řízení rizik

KII	VIS			N	P	Z	NA
X	X	odst. 1, 2 a)	Stanoveny metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik.	X			
X	X	odst. 1, 2 b)	Prováděna identifikace a hodnocení důležitosti aktiv, která patří do rozsahu ISMS, podle § 8 (Řízení aktiv) minimálně v rozsahu přílohy č. 1 k VKB a výstupy zapracuje do zprávy o hodnocení aktiv a rizik.	X			
X	X	odst. 1, 2 c)	Prováděna identifikace rizik, při kterých jsou zohledňovány hrozby a zranitelnosti, posuzovány možné dopady na aktiva, hodnotí tato rizika minimálně v rozsahu podle přílohy č. 2 k VKB. Jsou určena a schválena přijatelná rizika a je zpracována zpráva o hodnocení aktiv a rizik.	X			
X	X	odst. 1, 2 d)	Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováváno prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření.	X			
X	X	odst. 1, 2 e)	Je zpracovaný a zavedený plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik, určení osoby odpovědné za prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.	X			
X	X	odst. 1, 2 f)	Bez zbytečného odkladu jsou zohledňována reaktivní a ochranná opatření vydaná NBÚ v hodnocení rizik a v případě, že hodnocení rizik aktualizované o nové zranitelnosti spojené s realizací reaktivního nebo ochranného opatření překročí stanovená kritéria pro přijatelnost rizik, jsou doplněny plány zvládání rizik.	X			
X	X	odst. 3	Řízení rizik je zajištěno jinými způsoby (než jak je stanoveno v odstavci 1 a 2) a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň řízení rizik.	X			
		Zváženy hrozby, související s/se:					
X	X	odst. 4 a)	porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany uživatelů a administrátorů.			X	
X	X	odst. 4 b)	poškozením nebo selháním technického anebo programového vybavení.			X	
X	X	odst. 4 c)	zneužití identity fyzické osoby.			X	
X	X	odst. 4 d)	užíváním programového vybavení v rozporu s licenčními podmínkami.			X	
X	X	odst. 4 e)	kybernetickým útokem z komunikační sítě.	X			
X	X	odst. 4 f)	škodlivým kódem (například viry, spyware, trojské koně).		X		
X	X	odst. 4 g)	nedostatky při poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.			X	
X	X	odst. 4 h)	narušením fyzické bezpečnosti.			X	
X	X	odst. 4 i)	přerušením poskytování služeb elektronických komunikací nebo dodávek elektrické energie.			X	
X	X	odst. 4 j)	zneužitím nebo neoprávněnou modifikací údajů.	X			
X	X	odst. 4 k)	trvale působícími hrozbami.		X		
X	X	odst. 4 l)	odcizením nebo poškozením aktiva.		X		
X		odst. 6 a)	Porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany administrátorů kritické informační infrastruktury.				X

Zdroj: [31], [33], [50]

Tab. 23 Audit bezpečnostních opatření - Bezpečnostní politika

KII	VIS			N	P	Z	NA
		Stanovena bezpečnostní politika v oblastech:					
X	X	odst. 1 a) odst. 2 a)	Systém řízení bezpečnosti informací.	X			
X	X	odst. 1 b) odst. 2 b)	Organizační bezpečnost. (*Organizační bezpečnost (VKB § 6)*)		X		
X		odst. 1 c)	Řízení vztahů s dodavateli. (*Stanovení bezpečnostních požadavků pro dodavatele (VKB § 7)*)				X
	X	odst. 2 c)	Řízení dodavatelů. (*Stanovení bezpečnostních požadavků pro dodavatele (VKB § 7)*)			X	
X	X	odst. 1 d) odst. 2 d)	Klasifikace aktiv.	X			
X	X	odst. 1 e) odst. 2 e)	Bezpečnost lidských zdrojů.		X		
X	X	odst. 1 f) odst. 2 f)	Řízení provozu a komunikací.		X		
X	X	odst. 1 g) odst. 2 g)	Řízení přístupu.			X	
X	X	odst. 1 h) odst. 2 h)	Bezpečné chování uživatelů.				X
X	X	odst. 1 i) odst. 2 i)	Zálohování a obnova.			X	
X		odst. 1 j)	Bezpečné předávání a výměna informací.		X		
X		odst. 1 k)	Řízení technických zranitelností.			X	
X		odst. 1 l)	Bezpečné používání mobilních zařízení.		X		
X	X	odst. 1 m) odst. 2 j)	Poskytování a nabývání licencí programového vybavení a informací.			X	
X		odst. 1 n)	Dlouhodobé ukládání a archivace informací.			X	
X	X	odst. 1 o) odst. 2 k)	Ochrana osobních údajů.			X	
X		odst. 1 p)	Fyzická bezpečnost.			X	
X		odst. 1 q)	Bezpečnost komunikační sítě.		X		
X	X	odst. 1 r) odst. 2 m)	Ochrana před škodlivým kódem.		X		
X	X	odst. 1 s) odst. 2 n)	Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.		X		
X		odst. 1 t)	Využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.	X			

Zdroj: [31], [33], [50]

Tab. 24 Audit bezpečnostních opatření – Organizační bezpečnost

KII	VIS			N	P	Z	NA
X	X	odst. 1	Zavedena organizace řízení bezpečnosti informací (dále jen „organizační bezpečnost“), v rámci které je určen výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související s informačním systémem kritické informační infrastruktury, komunikačním systémem kritické informační infrastruktury nebo významným informačním systémem.	X			
X		odst. 2 a)	Určena bezpečnostní role: manažer kybernetické bezpečnosti.				X
X		odst. 2 b)	Určena bezpečnostní role: architekt kybernetické bezpečnosti.				X
X		odst. 2 c)	Určena bezpečnostní role: auditor kybernetické bezpečnosti.				X
X		odst. 2 d)	Určena bezpečnostní role: garant aktiva (podle § 2 písmene m).				X
	X	odst. 3	Bezpečnostní role jsou určeny přiměřeně podle odstavce 2.	X			
X	X	odst. 7	Určen výbor pro řízení kybernetické bezpečnosti.	X			
X	X	odst. 8	Je zajištěno odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí podle *Bezpečnost lidských* zdrojů odst. 1 písm. b).		X		

Zdroj: [31], [33], [50]

Tab. 25 Audit bezpečnostních opatření - Stanovení bezpečnostních požadavků pro dodavatele

KII	VIS			N	P	Z	NA
X	X	odst. 1	Jsou stanovena pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své dodavatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS. Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti IS nebo KS KII a VIS dokumentován písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.			X	
X		odst. 2 a)	U dodavatelů uvedených v odstavci 1 je před uzavřením smlouvy prováděno hodnocení rizik (podle přílohy č. 2 k VKB), která jsou spojena s podstatnými dodávkami.				X
X		odst. 2 b)	U dodavatelů uvedených v odstavci 1 uzavírá smlouvu o úrovni služeb, která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.				X
X		odst. 2 c)	U dodavatelů uvedených v odstavci 1 provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a zjištěné nedostatky odstraňuje nebo po dohodě s dodavatelem zajistí jejich odstranění.				X

Zdroj: [31], [33], [50]

Tab. 26 Audit bezpečnostních opatření – Řízení aktiv

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Jsou identifikována a evidována primární aktiva.	X			
X	X	odst. 1 b)	Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za primární aktiva.	X			
X	X	odst. 1 c)	Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a tato aktiva jsou zařazena do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k VKB.	X			
		Při hodnocení důležitosti primárních aktiv je posouzeno především:					
X	X	odst. 2 a)	Rozsah a důležitost osobních údajů nebo obchodního tajemství.		X		
X	X	odst. 2 b)	Rozsah dotčených právních povinností nebo jiných závazků.		X		
X	X	odst. 2 c)	Rozsah narušení vnitřních řídících a kontrolních činností.		X		
X	X	odst. 2 d)	Poškození veřejných, obchodních nebo ekonomických zájmů.		X		
X	X	odst. 2 e)	Možné finanční ztráty.		X		
X	X	odst. 2 f)	Rozsah narušení běžných činností orgánu a osoby.		X		
X	X	odst. 2 g)	Dopady spojené s narušením důvěrnosti, integrity a dostupnosti.		X		
X	X	odst. 2 h)	Dopady na zachování dobrého jména nebo ochranu dobré pověsti.		X		
X		odst. 3 a)	Jsou identifikována a evidována podpůrná aktiva.				X
X		odst. 3 b)	Jsou určeni garanti aktiv, kteří jsou odpovědní za podpůrná aktiva.				X
X		odst. 3 c)	Jsou určeny vazby mezi primárními a podpůrnými aktivy a hodnoceny důsledky závislostí mezi primárními a podpůrnými aktivy.				X
		Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že:					
X	X	odst. 4 a) 1.	Jsou určeny způsoby rozlišování jednotlivých úrovní aktiv.	X			
X	X	odst. 4 a) 2.	Jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv.	X			
X	X	odst. 4 a) 3.	Jsou stanoveny přípustné způsoby používání aktiv.	X			
X	X	odst. 4 b)	Jsou zavedena pravidla ochrany odpovídající úrovni aktiv.	X			
X	X	odst. 4 c)	Jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.	X			

Zdroj: [31], [33], [50]

Tab. 27 Audit bezpečnostních opatření – Bezpečnost lidských zdrojů

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.	X			
X	X	odst. 1 b)	V souladu s plánem rozvoje bezpečnostního povědomí je zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.				X
X	X	odst. 1 c)	Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.	X			
X	X	odst. 1 d)	Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.			X	
X	X	odst. 2	O školení podle odstavce 1 jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.			X	
X		odst. 3 a)	Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.		X		
X		odst. 3 b)	Je hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.	X			
X		odst. 3 c)	Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.			X	
X		odst. 3 d)	Zajištěna změna přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.			X	

Zdroj: [31], [33], [50]

Tab. 28 Audit bezpečnostních opatření - Řízení provozu a komunikací

KII	VIS			N	P	Z	NA
X	X	odst. 1	Pomocí technických nástrojů uvedených v § 21 až 23 jsou detekovány kybernetické bezpečnostní události, pravidelně vyhodnocovány získané informace a na zjištěné nedostatky reagováno v souladu s: *Zvládání kybernetických bezpečnostních událostí a incidentů (VKB § 13)*.			X	
X	X	odst. 2	Zajištěn bezpečný provoz informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému. Za tímto účelem jsou stanoveny provozní pravidla a postupy.		X		
X	X	odst. 4	Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh.			X	
		Provozní pravidla a postupy orgánu a osoby obsahují:					
X		odst. 3 a)	Práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů.	X			
X		odst. 3 b)	Postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů.		X		
X		odst. 3 c)	Postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech.	X			
X		odst. 3 d)	Spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží.			X	
X		odst. 3 e)	Postupy řízení a schvalování provozních změn.			X	
X		odst. 3 f)	Postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.	X			
X		odst. 5 a)	Je zajištěno oddělení vývojového, testovacího a produkčního prostředí.				X
X		Jsou řešena reaktivní opatření vydaná NBÚ tím, že orgán a osoba:					
X		odst. 5 b) 1.	Posuzuje očekávané dopady reaktivního opatření na informační systém kritické informační infrastruktury nebo komunikační systém kritické informační infrastruktury a na zavedená bezpečnostní opatření, vyhodnocuje možné negativní účinky a bez zbytečného odkladu je oznamuje NBÚ.	Pověřenec GDPR			
X		odst. 5 b) 2.	Stanovuje způsob rychlého provedení reaktivního opatření, který minimalizuje možné negativní účinky, a určuje časový plán jeho provedení.	Pověřenec GDPR			
X		odst. 6 a)	Je zajištěna bezpečnost a integrita komunikačních sítí a bezpečnost komunikačních služeb podle *Nástroj pro ochranu integrity komunikačních sítí (VKB § 17)*.			X	
X		odst. 6 b)	Jsou určeny pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi.	X			
X		odst. 6 c)	Výměna a předávání informací je prováděna na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla jsou dokumentována.			X	
X		odst. 6 d)	S ohledem na klasifikaci aktiv je prováděna výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.			X	

Zdroj: [31], [33], [50]

Tab. 29 Audit bezpečnostních opatření - Řízení přístupu a bezpečné chování uživatelů

KII	VIS			N	P	Z	NA
X	X	odst. 1	Na základě provozních a bezpečnostních potřeb je řízen přístup k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a významnému informačnímu systému a každému uživateli je přiřazen jednoznačný identifikátor.			X	
X	X	odst. 2	Jsou přijata opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů a administrátorů informačního systému kritické informační struktury, komunikačního systému kritické informační infrastruktury a významného informačního systému podle *Nástroj* pro ověřování identity uživatelů (VKB § 18) a *Nástroj pro řízení přístupových oprávnění (VKB § 19)*, a která brání ve zneužití těchto údajů neoprávněnou osobou.			X	
X		odst. 3 a)	Přistupujícím aplikacím je přidělen samostatný identifikátor.			X	
X		odst. 3 b)	Je omezeno přidělování administrátorských oprávnění.			X	
X		odst. 3 c)	Přidělování a odebírání přístupových oprávnění je prováděno v souladu s politikou řízení přístupu.		X		
X		odst. 3 d)	Je prováděno pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích.			X	
X		odst. 3 e)	Je využíván nástroj pro ověřování identity uživatelů podle *Nástroj* pro ověřování identity uživatelů (VKB § 18) a nástroj pro řízení přístupových oprávnění podle *Nástroj pro řízení přístupových oprávnění (VKB § 19)*.			X	
X		odst. 3 f)	Jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje.	X			

Zdroj: [31], [33], [50]

Tab. 30 Audit bezpečnostních opatření - Akvizice, vývoj a údržba

KII	VIS			N	P	Z	NA
X	X	odst. 1	Jsou stanoveny bezpečnostní požadavky na změny informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.		X		
X		odst. 2 a)	Jsou identifikována, hodnocena a řízena rizika související s akvizicí, vývojem a údržbou informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury; pro postupy hodnocení a řízení rizik se metodiky podle *Řízení rizik* (VKB § 4) odst. 1 písm. a) použijí obdobně.				X
X		odst. 2 b)	Je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat.				X
X		odst. 2 c)	Je prováděno bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu.				X

Zdroj: [31], [33], [50]

Tab. 31 Audit bezpečnostních opatření - Zvládání kybernetických bezpečnostních událostí a incidentů

KII	VIS			N	P	Z	NA
X	X	a)	Jsou přijata nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí u informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních jsou vedeny záznamy.				
X	X	b)	Je připraveno prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle *Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů (VKB § 21)*, *Nástroj pro detekci kybernetických bezpečnostních událostí (VKB §* 22), *Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (VKB § 23)*, je prováděno jejich vyhodnocení a jsou identifikovány kybernetické bezpečnostní incidenty.				
X	X	c)	Je prováděna klasifikace kybernetických bezpečnostních incidentů, přijímáno opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, prováděno hlášení kybernetického bezpečnostního incidentu podle § 32 a zajištěn sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.				
X	X	d)	Jsou prošetřeny a určeny příčiny kybernetického bezpečnostního incidentu, vyhodnocena účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení jsou stanovena nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.				
X	X	e)	Zvládání kybernetických bezpečnostních incidentů je dokumentováno.				

Zdroj: [31], [33], [50]

Tab. 32 Audit bezpečnostních opatření - Řízení kontinuity činností

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Jsou stanoveny práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role.	X			
		Jsou stanoveny cíle řízení kontinuity činností formou určení:					
X	X	odst. 1 b) 1.	Minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.			X	
X	X	odst. 1 b) 2.	Doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.			X	
X	X	odst. 1 b) 3.	Doby obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu.				
X	X	odst. 1 c)	Je stanovena strategie řízení kontinuity činností, která obsahuje naplnění cílů podle písmene b).		X		
X		odst. 2 a)	Jsou vyhodnocovány a dokumentovány možné dopady kybernetických bezpečnostních incidentů a posouzena možná rizika související s ohrožením kontinuity činností.	X			
X		odst. 2 b)	Jsou stanoveny, aktualizovány a pravidelně testovány plány kontinuity činností informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.				X
X		odst. 2 c)	Jsou realizována opatření pro zvýšení odolnosti informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickému bezpečnostnímu incidentu a je využíván nástroj pro zajišťování úrovně dostupnosti podle *Nástroj pro zajišťování úrovně dostupnosti (VKB § 26)*.		X		
		Jsou stanoveny a aktualizovány postupy pro provedení opatření vydaných NBÚ podle § 13 a 14 ZKB, ve kterých je zohledněno:					
X		odst. 2 d) 1.	Výsledky hodnocení rizik provedení opatření.				X
X		odst. 2 d) 2.	Stav dotčených bezpečnostních opatření.				X
X		odst. 2 d) 3.	Vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury				X

Tab. 33 Audit bezpečnostních opatření - Kontrola a audit kybernetické bezpečnosti Zdroj: [31], [33], [50]

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Je posouzen soulad bezpečnostních opatření s obecně závaznými právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky vztahujícími se k informačnímu systému kritické informační infrastruktury, komunikačnímu systému kritické informační infrastruktury a VIS a určena opatření pro jeho prosazování.			X	
X	X	odst. 1 b)	Jsou prováděny a dokumentovány pravidelné kontroly dodržování bezpečnostní politiky a výsledky těchto kontrol jsou zohledněny v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.	X			
X		odst. 2	Je zajištěno provedení auditu kybernetické bezpečnosti osobou s odbornou kvalifikací podle § 6 odst. 6 VKB (auditor kybernetické bezpečnosti), která hodnotí správnost a účinnost zavedených bezpečnostních opatření.	X			
X		odst. 3	Pro IS nebo KS KII je prováděna kontrola zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocování a je reagováno na zjištěné zranitelnosti.				X

Zdroj: [31], [33], [50]

PŘÍLOHA P III: AUDIT BEZPEČNOSTNÍCH OPATŘENÍ - TECHNICKÁ OPATŘENÍ

Tab. 34 Audit bezpečnostních opatření – Fyzická bezpečnost

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Jsou přijata nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.			X	
X	X	odst. 1 b)	Jsou přijata nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.			X	
X	X	odst. 1 c)	Je předcházeno poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytování služeb informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.		X		
X		odst. 2 a)	Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany na úrovni objektů.			X	
X		odst. 2 b)	Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury.	X			

Zdroj: [31], [33], [50]

Tab. 35 Audit bezpečnostních opatření - Nástroj pro ochranu integrity komunikačních sítí

KII	VIS			N	P	Z	NA
		Pro ochranu integrity rozhraní vnější komunikační sítě, která není pod správou orgánu nebo osoby, a vnitřní komunikační sítě, která je pod správou orgánu nebo osoby, je zavedeno(a):					
X	X	odst. 1 a)	Řízení bezpečného přístupu mezi vnější a vnitřní sítí.			X	
X	X	odst. 1 b)	Segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí.			X	
X	X	odst. 1 c)	Použití kryptografických prostředků (*Kryptografické prostředky* (VKB § 25)) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií.	X			
X	X	odst. 1 d)	Opatření pro odstranění nebo blokování přenášených dat, která neodpovídají požadavkům na ochranu integrity komunikační sítě.		X		
X		odst. 2	Jsou využívány nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.	X			

Zdroj: [31], [33], [50]

Tab. 36 Audit bezpečnostních opatření – Nástroj pro ověřování identity uživatelů

KII	VIS			N	P	Z	NA
X	X	odst. 1	Jsou používány nástroje pro ověření identity uživatelů a administrátorů informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.			X	
		Nástroj pro ověřování identity uživatelů, který používá autentizaci pouze heslem, zajišťuje:					
X	X	odst. 3 a)	Minimální délku hesla osm znaků.			X	
X	X	odst. 3 b)	Minimální složitost hesla tak, že heslo bude obsahovat alespoň tři z následujících čtyř požadavků: 1. nejméně jedno velké písmeno, 2. nejméně jedno malé písmeno, 3. nejméně jednu číslici nebo 4. nejméně jeden speciální znak, který není uveden v bodech 1 až 3.		X		
X	X	odst. 3 c)	Maximální dobu pro povinnou výměnu hesla nepřesahující sto dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.		X		
X	X	odst. 5	**Nástroj pro ověřování identity uživatelů je zajištěn jinými způsoby, než jaké jsou stanoveny v odstavcích 3 až 5, a orgán a osoba doložil(a), že použitá opatření zajišťují stejnou nebo vyšší úroveň odolnosti hesla.**	X			
		Je používán nástroj pro ověřování identity, který:					
X		odst. 4 a) 1.	Zamezuje opětovnému používání dříve používaných hesel a neumožní více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin.	X			
X		odst. 4 a) 2.	Provádí opětovné ověření identity po určené době nečinnosti.			X	
X		odst. 4 b)	Využívá nástroj pro ověřování identity administrátorů. V případě, že tento nástroj využívá autentizaci heslem, zajistí prosazení minimální délky hesla patnáct znaků při dodržení požadavků podle odstavce 3 písm. b) a c).			X	

Zdroj: [31], [33], [50]

Tab. 37 Audit bezpečnostních opatření - Nástroj pro řízení přístupových oprávnění

KII	VIS			N	P	Z	NA
X	X	Je používán nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění:					
X	X	odst. 1 a)	Pro přístup k jednotlivým aplikacím a datům.			X	
X	X	odst. 1 b)	Pro čtení dat, pro zápis dat a pro změnu oprávnění.			X	
X		odst. 2	Je používán nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik.	X			

Zdroj: [31], [33], [50]

Tab. 38 Audit bezpečnostních opatření - Nástroj pro ochranu před škodlivým kódem

KII	VIS			N	P	Z	NA
		Pro řízení rizik spojených s působením škodlivého kódu je používán nástroj pro ochranu informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému před škodlivým kódem, který zajistí ověření a stálou kontrolu:					
X	X	odst. 1 a)	Komunikace mezi vnitřní sítí a vnější sítí.			X	
X	X	odst. 1 b)	Serverů a sdílených datových úložišť.			X	
X	X	odst. 1 c)	Pracovních stanic.			X	
X	X		Je prováděna pravidelná aktualizace nástroje pro ochranu před škodlivým kódem, jeho definic a signatur.			X	

Zdroj: [31], [33], [50]

Tab. 39 Audit bezpečnostních opatření - Nástroj pro zaznamenávání činností uživatelů a administrátorů

KII	VIS			N	P	Z	NA
X	X	Je používán nástroj pro zaznamenávání činností informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému, který zajišťuje:					
X	X	odst. 1 a)	Sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti.		X		
X	X	odst. 1 b)	Ochranu získaných informací před neoprávněným čtením nebo změnou.			X	
X	X	Pomocí nástroje pro zaznamenávání činnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému je zaznamenáváno(y):					
X	X	odst. 2 a)	Přihlášení a odhlášení uživatelů a administrátorů.			X	
X	X	odst. 2 b)	Činnosti provedené administrátory.			X	
X	X	odst. 2 c)	Činnosti vedoucí ke změně přístupových oprávnění.	X			
X	X	odst. 2 d)	Neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů.	X			
X	X	odst. 2 e)	Zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému.			X	
X	X	odst. 2 f)	Automatická varovná nebo chybová hlášení technických aktiv.			X	
X	X	odst. 2 g)	Přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností.	X			
X	X	odst. 2 h)	Použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.	X			
X	X	odst. 4	Nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.			X	
X		odst. 3	Záznamy činností zaznamenané podle odst. 2 jsou uchovávány nejméně po dobu tří měsíců.	X			

Zdroj: [31], [33], [50]

Tab. 40 Audit bezpečnostních opatření - Nástroj pro detekci kybernetických bezpečnostních událostí

KII	VIS			N	P	Z	NA
X	X	odst. 1	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.			X	
		Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí ověření, kontrolu a případně zablokování komunikace:					
X		odst. 2 a)	V rámci vnitřní komunikační sítě.			X	
X		odst. 2 b)	Serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.			X	

Zdroj: [31], [33], [50]

Tab. 41 Audit bezpečnostních opatření - Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

KII	VIS			N	P	Z	NA
		Je používán nástroj pro sběr a průběžné vyhodnocování kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajišťuje:					
X		odst. 1 a)	Integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí z informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.				X
X		odst. 1 b)	Poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech v informačním systému kritické informační infrastruktury nebo komunikačním systému kritické informační infrastruktury.				X
X		odst. 1 c)	Nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.				X
X		odst. 2 a)	Je zajištěna pravidelná aktualizace nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování.				X
X		odst. 2 b)	Zajištěno využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury.				X

Tab. 42 Audit bezpečnostních opatření – Aplikační bezpečnost

Zdroj: [31], [33], [50]

KII	VIS			N	P	Z	NA
X	X	odst. 1	Jsou prováděny bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.		X		
X		odst. 2 a)	Je zajištěna trvalá ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.		X		
X		odst. 2 b)	Je zajištěna trvalá ochrana transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.		X		

Zdroj: [31], [33], [50]

Tab. 43 Audit bezpečnostních opatření - Kryptografické prostředky

KII	VIS			N	P	Z	NA
X	X	Pro používání kryptografické ochrany je(jsou) stanovena:					
X	X	odst. 1 a) 1.	Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.		X		
X	X	odst. 1 a) 2.	Pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat.	X			
X	X	odst. 1 b)	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik jsou používány kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti.		X		
X		odst. 2 a)	Pro používání kryptografických prostředků je stanoven systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů.		X		
X		odst. 2 b)	Jsou používány odolné kryptografické algoritmy a kryptografické klíče; v případě nesouladu s minimálními požadavky na kryptografické algoritmy uvedenými v příloze č. 3 k této vyhlášce řídí rizika spojená s tímto nesouladem.		X		

Zdroj: [31], [33], [50]

Tab. 44 Audit bezpečnostních opatření - Nástroj pro zajišťování úrovně dostupnosti

KII	VIS			N	P	Z	NA
X	X	odst. 1	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik je používán nástroj pro zajišťování úrovně dostupnosti informací.	X			
X		Je používán nástroj pro zajišťování úrovně dostupnosti informací, který zajišťuje:					
X		odst. 2 a)	Dostupnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury pro splnění cílů řízení kontinuity činností.			X	
X		odst. 2 b)	Odolnost informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost.				X
X		odst. 2 c)	Zálohování důležitých technických aktiv informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury 1. využitím redundance v návrhu řešení a 2. zajištěním náhradních technických aktiv v určeném čase.			X	

Zdroj: [31], [33], [50]