Kybernetická bezpečnost v prostředí škol

Bc. Anna Prokešová

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Anna Prokešová**
Osobní číslo:	**L20684**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Rizikové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Kybernetická bezpečnost v prostředí škol**

Zásady pro vypracování

1. Zpracujte literární rešerši zkoumané oblasti z domácích a zahraničních zdrojů.
2. Analyzujte současný stav zkoumané oblasti ve vybrané škole.
3. Navrhněte opatření ke zlepšení současného stavu.
4. Vytvořte interní bezpečnostní dokument reflektující zkoumanou problematiku.

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

Seznam doporučené literatury:

1. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů: podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Čeněk Aleš, 2019. ISBN 978-80-7380-765-8.
2. EVANS, Lester. *Cybersecurity: what you need to know about computer and cyber security, social engineering, the internet of things + an esential guide to ethical hacking for beginners.* USA: Lester Evans, 2019. ISBN 9781794647237.
3. DOUCEK, Petr. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional publishing, 2020. ISBN 978-80-88260-39-4.

Další odborná literatura dle doporučení vedoucího diplomové práce.

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

Datum zadání diplomové práce: **1. prosince 2021**
Termín odevzdání diplomové práce: **6. května 2022**

L.S.

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

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

V Uherském Hradišti dne 1. prosince 2021

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 Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 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 na 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: 6.5.2022

Jméno a příjmení studenta: Bc. Anna Prokešová

.....
podpis studenta

ABSTRAKT

Tato diplomová práce se z teoretického hlediska zabývá oblastí kybernetické bezpečnosti – její rešerší, terminologií, principy, potencionálními útoky a konkrétními opatřeními. Dále se práce zaměřuje na řešení této problematiky ve školství. Podrobněji se zabývá systémem řízení bezpečnosti informací, jedním z opatření kybernetické bezpečnosti, které vychází z norem řady ISO/IEC 27 000. Práce podle těchto norem charakterizuje vybrané školské zařízení, zpracovává analýzu rizik a navrhuje opatření ke zlepšení současného stavu. Aplikační část práce se zabývá zpracováním interního dokumentu zaměřeného na implementaci opatření kybernetické bezpečnosti a bezpečnosti informací vedoucí ke zlepšení stavu ve vybraném subjektu.

Klíčová slova: Analýza rizik, FMEA, Ishikawa diagram, Kybernetická bezpečnost, Školské zařízení

ABSTRACT

From a theoretical point of view, this diploma thesis deals with the area of cyber security - its research, terminology, principles, potential attacks and specific measures. Furthermore, the work focuses on solving this problem in education. It deals in more detail with the information security management system, one of the cyber security measures, which is based on the ISO / IEC 27 000 series of standards. The application part of the thesis deals with the elaboration of an internal document focused on the implementation of cyber security and information security measures leading to the improvement of the situation in the selected entity.

Keywords: Cyber Security, FMEA, Ishikawa diagram, School Facilities, Risk Analysis

Ráda bych poděkovala vedoucímu mé diplomové práce panu Ing. Petru Svobodovi, Ph.D. za jeho čas věnovaný vedení mé práce a za poskytnutí cenných rad při jejím zpracovávání. Děkuji rovněž Základní a mateřské škole Novosedly nad Nežárkou a paní ředitelce za aktivní spolupráci při konzultacích a poskytnutí informací.

V neposlední řadě bych ráda poděkovala mé rodině a přátelům, kteří při mně stáli po celou dobu mého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

„Jakýkoliv systém je tak bezpečný, jak bezpečný je jeho nejslabší článek.“

(Bašta a Kolouch, 2019)

OBSAH

ÚVOD

V posledních letech dochází k obrovské transformaci a vývoji v oblasti digitalizace. S každým rokem stoupá počet zařízení připojených do online prostředí. S trendem prolínání fyzického a digitálního světa dochází k nárůstu kybernetických hrozeb. Tlak na schopnost odolávat kybernetickému nebezpečí dnes čelí jednotlivci i soukromé a veřejné organizace různých velikostí. Uživatelé i subjekty ukládají do svých zařízení a elektronických platforem spoustu osobních informací, které se stávají terčem hackerů. Hodnota informací na černém trhu se zvyšuje spolu s vývojem informačních a komunikačních technologií.

Tlaku na implementaci bezpečnostních opatření čelí právě i ředitelé organizací, kteří jsou odpovědní za celý systém, který vedou. Některé subjekty mají své odborné bezpečnostní manažery, některé organizace na ně však svou strukturou nebo finančními prostředky nedosáhnou. V takových případech spadá většinou náplň bezpečnostního manažera do role samotných ředitelů. Příkladem této situace mohou být školská zařízení, kde musejí být ředitelé v rámci své funkce i bezpečnostními manažery. Tato diplomová práce upozorňuje na problematiku bezpečnosti ve školách se zaměřením na odvětví kybernetické bezpečnosti.

Práce v teorii charakterizuje oblast kybernetické bezpečnosti. Postupuje od obecného ke konkrétnímu – představuje literární rešerši, základní terminologii, definuje její principy, pojednává o kybernetických útocích a představuje základní opatření z nichž se detailněji zaměřuje na systém řízení bezpečnosti informací a fyzickou bezpečnost objektu a zařízení.

V praktické části diplomová práce popisuje vybrané školské zařízení s důrazem na řadu norem ISO/IEC 27 000. Dále provádí identifikaci rizikových oblastí pomocí Ishikawa diagramu s následnou analýzou rizik současného stavu za pomoci FMEA a obsahuje navržená opatření k jeho zlepšení.

V aplikační části je stanoven interní dokument, který reflektuje problematiku kybernetické bezpečnosti a systému řízení bezpečnosti informací (ISMS) v subjektu. Tento dokument je určen vedení organizace pro implementaci opatření ke zlepšení stavu v této oblasti nikoli ke striktnímu zavedení normy ISO/IEC 27 000. Protože interní dokument je určen do rukou vedení organizace a zřizovatele, je v přílohové části problematika doplněna o brožuru určenou všem zaměstnancům subjektu. To podtrhuje rozšíření povědomí o této problematice do celé systémové struktury.

CÍLE A METODY ZPRACOVÁNÍ DIPLOMOVÉ PRÁCE

Hlavní cíl diplomové práce:

- Návrh opatření na zlepšení současného stavu kybernetické bezpečnosti Základní školy a mateřské školy Novosedly nad Nežárkou.

Dílčí cíle diplomové práce:

- Rešerše současného stavu zkoumané oblasti.
- Analýza současného stavu kybernetické bezpečnosti vybraného vzdělávacího zařízení.
- Vytvoření interního bezpečnostního dokumentu pro potřeby vedení vybraného vzdělávacího zařízení.
- Vytvoření příručky pro potřeby zvýšení povědomí všech zaměstnanců v oblasti kybernetické bezpečnosti vybraného vzdělávacího zařízení.

Použité metody:

- Rešerše – byla využita v teoretické části práce k představení problematiky pomocí legislativy, norem a odborných literárních českých i zahraničních zdrojů a základní terminologie.
- Popis – byl využit při zpracování teoretické části, ve které se zaobírá problematikou kybernetické bezpečnosti a ISMS.
- Dotazování – bylo využito v rámci ústních rozhovorů s paní ředitelkou vybrané školy vedoucích k podrobné charakteristice subjektu podle norem ISO/IEC 27 000.
- Dedukce – byla využita při identifikaci rizikových oblastí vyplývajících z charakteristiky organizace.
- Analýza – byla využita k analýze současného stavu subjektu v oblasti řešené problematiky. Analýza byla provedená pomocí identifikační metody rizik Ishikawa diagram a kvantitativní metody FMEA.
- Syntéza – byla využita při vyhodnocení Ishikawa diagramu a FMEA.
- Indukce – byla využita v rámci vytváření závěru, který byl subjektivním vyhodnocením řešené problematiky autora této diplomové práce.

I. TEORETICKÁ ČÁST

1 REŠERŠE

Výchozím bodem pro zpracování diplomové práce byla rešerše. Následující podkapitola 1.1 představuje základní prameny, ze kterých práce čerpá anebo přímo souvisejí s daným tématem. V rámci rešerše byly zkoumány dvě oblasti, které práce propojuje – kybernetická bezpečnost a prostředí školních zařízení jakožto státních institucí. Podkapitola 1.2 dále uvádí čtenáře do tématu představením terminologie potřebné k jeho porozumění.

1.1 Legislativní dokumenty a jiné literární zdroje

Hlavní zdroje sloužící pro zpracování této práce a pro uchopení tématu, jsou zde logicky seřazeny od zákonů, vyhlášek, norem, přes národních strategii, zprávu o stavu kybernetické bezpečnosti, až po další odborné literární prameny.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Úkolem zákona o kybernetické bezpečnosti je upravovat práva, povinnosti a kompetence osob a veřejných orgánů v rámci problematiky kybernetické bezpečnosti. Zákon dále zahrnuje i předpisy EU a vychází také z norem řady ISO/IEC 27 000. Cílem tohoto zákona je stanovení minimální úrovně opatření a zlepšení detekce incidentů.

Podle Smejkala je hlavním cílem zákonu o kybernetické bezpečnosti ochrana infrastruktury, kde by v případě narušení kybernetické bezpečnosti nebo informačních systémů došlo k poškození či ohrožení zájmů státu. (ČESKO, 2014; Smejkal, Sokol a Kodl, 2019)

Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon implementuje a navazuje na předpisy Evropské unie a upravuje práva a povinnosti při zpracování osobních údajů v návaznosti na práva osob o ochraně soukromí. General Data Protection Regulation (GDPR) je právní rámec pro ochranu osobních údajů, který úzce souvisí s kybernetickou bezpečností, avšak není prvotně cílen do oblasti ICT. Hlavním cílem GDPR je ochrana práv proti neoprávněnému užívání dat subjektů. V rámci kybernetické bezpečnosti se za osobní údaje mohou považovat následující: jméno a příjmení, rodné číslo, lokační údaje, síťové identifikátory (jako je IP adresa, identifikátory cookies), elektronická komunikace, přístupové údaje a další. (Bašta a Kolouch, 2019; ČESKO, 2019)

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších zákonů

Zákon ustanovuje školám a školským zařízením, s výjimkou mateřských škol, povinnost uchovávat dokumenty a umožnit výběr archiválií. Dále ukládá povinnost státního oblastního archivu pro kontrolu výkonu spisové služby u škol. Definuje dokumenty, které se vždy předkládají k výběru za archiválie. (ČESKO, 2004)

Vyhláška č. 364/2005 Sb., o vedení dokumentace škol a školských zařízení a školní matriky a o předávání údajů z dokumentace škol a školských zařízení a ze školní matriky (vyhláška o dokumentaci škol a školských zařízení), ve znění pozdějších předpisů

Vyhláška definuje rozsah a vedení matriky a stanovuje pravidla pro předávání informací z dokumentace škol a školských zařízení. (ČESKO, 2005)

Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozu informačního systému datových schránek, ve znění pozdějších předpisů

Vyhláška stanovuje pravidla pro přístupové údaje do datové schránky, definuje bezpečnostní zásady pro přístup do schránky, maximální velikosti datových zpráv, jejich dobu uložení a formuluje elektronické prostředky pro přihlášení do schránky jako kryptografické. (ČESKO, 2009)

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (o kybernetické bezpečnosti)

Zpracovává obsah a strukturu bezpečnostní dokumentace vybraných subjektů i směrnici EU. Dále udává bezpečnostní opatření, hodnocení kybernetických bezpečnostních incidentů, reakci na incidenty, způsob likvidace dat apod. (Smejkal, Sokol a Kodl, 2019)

ŘADA ISO/IEC 27000 Informační technologie – Systém řízení bezpečnosti informací

Řada mezinárodních norem zaměřených na systém řízení bezpečnosti informací v rámci informačních technologií. Jedná se o dobrovolný a univerzální nástroj pro všechny typy organizací, který lze implementovat, ale nemusí projít certifikací. Podle těchto norem by měl být jakýkoliv subjekt schopen implementovat ISMS do své struktury. Konkrétní příklady norem vztahující se k řešené problematice:

- ČSN ISO/IEC 27 000 Informační technologie – Bezpečnostní techniky – Systémy managementu informací (Přehled a slovník),
- ČSN ISO/IEC 27 001 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací (Požadavky),
- ČSN ISO/IEC 27 002 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací (Soubor postupů pro ISMS),
- ČSN ISO/IEC 27 003 Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací,
- ČSN ISO/IEC 27 005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. (Ondrák, Sedlák a Mazálek, 2013; Smejkal, Sokol a Kodl, 2019)

Národní strategie kybernetické bezpečnosti ČR 2021-2025

Jedná se o základní bezpečnostní dokument České republiky, který se týká problematiky kybernetické bezpečnosti. Je zaměřený hlavně na oblasti bezpečnostních složek státu a veřejné správy. Může však sloužit i ostatním subjektům a osobám při jejich pohybu v kyberprostoru.

Mezi svými cíli strategie udává posílení zabezpečení v infrastruktuře, potírání kybernetické kriminality, posílení efektivity při mezinárodní spolupráci, systém vzdělávání v oblasti nebo také spolupráci mezi soukromou a veřejnou sférou. (Národní úřad pro kybernetickou bezpečnost, 2020)

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020

Zpráva upozorňuje na informace týkající se kybernetické bezpečnosti za rok 2020, který byl zlomový událostmi ve světě i v České republice. NÚKIB upozorňuje na zvyšující se počty kybernetických útoků, na nedostatek odborníků i na probíhající vzdělávání v oblasti. (Národní úřad pro kybernetickou bezpečnost, 2021)

Bezpečnost informačních systémů: podle zákona o kybernetické bezpečnosti

Významným literárním zdrojem je Bezpečnost informačních systémů od kolektivu autorů. Publikace se zabývá problematikou v širším slova smyslu – od legislativních předpisů, přes normy až po doporučené postupy řešení bezpečnostních incidentů. (Smejkal, Sokol a Kodl, 2019)

Problematika ISMS v manažerské informatice

Dílo prezentuje management informační bezpečnosti jako velmi potřebný. Charakterizuje základní pojmy a normy řešené oblasti. Poskytuje i základ pro implementaci ISMS do struktury organizace. (Ondrák, Sedlák a Mazálek, 2013)

Řízení kybernetické bezpečnosti a bezpečnosti informací

Svazek zabývající se kybernetickou bezpečností a bezpečností informací zkoumá problematiku podle současných trendů a v rámci mezinárodních standardů. Publikace si klade za cíl poskytnout ucelený přehled. (Doucek, 2020)

1.2 Terminologie

Práce zde definuje termíny v kontextu kybernetické bezpečnosti, které jsou pro danou oblast stěžejní. Terminologie je pro lepší přehlednost uspořádána abecedně.

Aktivum

Jako aktivum je chápán veškerý hmotný i nehmotný majetek subjektu, jehož hodnota se může snížit vlivem působení hrozby. (Ministerstvo vnitra České republiky, 2016)

Analýza rizik

Činnosti vedoucí k pochopení charakteru rizika a k jeho ohodnocení. Dále zahrnuje scénáře hrozeb s cílem posouzení zranitelnosti a dopadu. Dále poskytuje základ pro rozhodování o riziku, jeho ošetřování a monitoring. (Ministerstvo vnitra České republiky, 2016)

Bezpečnost

Jako bezpečnost lze obecně chápat stav, kdy je systém schopný odolat hrozbám, které proti němu negativně působí, tak aby byl zachován. Je tak vyjádřena míra jeho stability. (Ministerstvo vnitra České republiky, 2016)

Bezpečnostní hrozba

Hrozba, která má za následek vložení nepravdivých zpráv nebo jejich obměnu nebo vydávaní se za jinou osobu nebo subjekt. Tedy hrozba úmyslně narušující systém dat nebo počítačovou síť.

Hrozbou lze v rámci kybernetické bezpečnosti také chápat nežádoucí událost, která poškozuje systém i jeho aktiva. Tedy například zničení, kompromitaci systému nebo aktiv, změnu dat nebo dostupnost. (Ministerstvo vnitra České republiky, 2016)

Bezpečnost organizace

Znamená ochranu aktiv a ochranu přístupů do objektu. Součástí bezpečnosti organizace je i bezpečnost informací a IS/ICT. Bezpečnost informací zahrnuje zásady práce s různými druhy informací, v digitální i tištěné podobě a dále i jejich zpracování, archivaci, likvidaci apod. Bezpečnost IS/ICT pak chrání pouze aktiva v digitální podobě, která jsou součástí informačního systému. (Doucek, 2020)

Bezpečnostní incident

Jedná se o bezpečnostní událost, u které hrozí pravděpodobnost poškození činností a funkce organizace. V rámci kybernetiky se může jednat o narušení bezpečnosti služeb nebo informací v systémech anebo o narušení integrity sítí elektronických komunikací. (Sedlák a Konečný, 2021)

Bezpečnostní politika

V rámci organizace je bezpečnostní politika základním dokumentem, který charakterizuje bezpečnostní riziko a stanovuje odpovědnost za ochranu a její úroveň. V celém systému se pak jedná o souhrn cílů, pravidel a postupů, které specifikují ochranu aktiv. (Jirásek, Novák a Požár, 2013)

Bezpečnostní událost

Situace nebo stav systému, počítačové sítě nebo služby, který je identifikovatelný a který naznačuje možné narušení bezpečnosti nebo selhání bezpečnostních opatření. V rámci kybernetiky se pak může jednat o narušení bezpečnosti informací v IS, služeb anebo integrity elektronických komunikací. (Sedlák a Konečný, 2021)

Bezpečnostní zranitelnost IT

Zranitelností v rámci kybernetické bezpečnosti lze chápat neúmyslnou vadu nebo chybu, která může být potencionálně zneužita útočníkem. (Ministerstvo vnitra České republiky, 2016)

Fyzická bezpečnost

Fyzickou bezpečnostní lze chápat režim opatření technického a organizačního charakteru, který zabraňuje nepovolenému konání. (Ministerstvo vnitra České republiky, 2016)

Kybernetická bezpečnost

Souhrn opatření, které slouží k odhalení, identifikaci, analýze a redukci hrozeb v kybernetickém prostoru. Dále také jako soubor technických, organizačních, vzdělávacích i právních prostředků vedoucí k ochraně kybernetického prostoru. (Ministerstvo vnitra České republiky, 2016)

Kybernetická hygiena

Termín je důležitý zejména pro budoucí vývoj v rámci kybernetické bezpečnosti. Klade si za cíl budování bezpečnostního povědomí na všech úrovních. V současné době je již jedním z pilířů kybernetické bezpečnosti. Jejím cílem je zmírnění kybernetických rizik na všech úrovních. Zahrnuje obecná opatření jako je ochrana fyzického perimetru, síťová ochrana, ochrana zařízení, cloudu a další. (Sedlák a Konečný, 2021)

Kybernetický prostor

Prostředí tvořené informačními systémy, sítěmi elektronických komunikací a službami, které umožňují vznik, zpracovávání a sdílení informací. (Jirásek, Novák a Požár, 2013)

Řízení rizik

Řízením rizik lze chápat koordinování činností potřebných k řízení a kontrole subjektu se zřetelem na všechna rizika. (Ondrák, Sedlák a Mazálek, 2013)

Systém řízení bezpečnosti informací

Jedná se o řízení bezpečnosti informací, které zahrnuje určení rozsahu a odpovědností řízení. Dále prosazuje bezpečnostní opatření, zajišťuje zpětnou vazbu a hodnocení a následné neustálé zlepšování. Princip systému řízení bezpečnosti informací je založen na Demingově modelu, se kterým se můžeme setkat i pod pojmem PDCA model/cyklus. (Ondrák, Sedlák a Mazálek, 2013)

Uživatel

Uživatelem je každá osoba, která využívá informační službu, například za účelem zjišťování a sdílení informací. (Jirásek, Novák a Požár, 2013)

1.3 Dílčí závěr kapitoly

Zákon o kybernetické bezpečnosti není závazný pro všechny instituce a občany České republiky. Stanovení orgánů, na které se zákon vztahuje, závisí na jejich charakteristikách a

kritériích. Zákon cílí na zajišťování triády CIA. Normy na rozdíl od zákona a vyhlášky nejsou pro dané subjekty závazné. Implementace norem a jejich dodržování je pro subjekty dobrovolné. Normy však tvoří základ firmám a organizacím, které se dobrovolně chtějí věnovat zabezpečení v rámci ISMS a kybernetické bezpečnosti a poskytují základní principy pro řešení této problematiky. (FAQ, b.r.)

Hlavním dokumentem pro zpracování diplomové práce je právě řada norem ISO/IEC 27 000. Tyto normy slouží jako základ pro zpracování praktické části této práce, jejím cílem však není normu striktně zavést, nýbrž nastavit interní bezpečnostní politiku subjektu v této oblasti.

Pro řešenou problematiku je relevantní i Zpráva o stavu kybernetické bezpečnosti v České republice za rok 2020. Zpráva reflektuje současné trendy v dané oblasti, popisuje reálná fakta a upozorňuje na rizika. V době psaní této diplomové práce není dostupná zpráva za rok 2021.

2 KYBERNETICKÁ BEZPEČNOST

Pojem kybernetická bezpečnost je komplexní termín, pro který neexistuje jedna konkrétní obecně užívaná definice. Kybernetická bezpečnost nabývá na významu ve všech úrovních, ať už se jedná o soukromou firemní sféru, firemní nebo sféru národních politik. Pohybujeme se v řadách osob z veřejnosti, které využívají prvky ICT každý den. Od firmy, které stojí na činnostech jedinců až po národní bezpečnost, pro jejíž ochranu je třeba chránit mimo jiné i kyberprostor. Je třeba si uvědomit, že kybernetická bezpečnost se však netýká pouze kyberprostoru, ale i dalších důležitých souvislostí, jako například fyzických opatření, která přímo souvisí s objekty a zařízeními. V rámci aplikace kybernetické bezpečnosti jsou využívány principy, které se též nazývají triádou kybernetické bezpečnosti. Jedná se o:

- CIA,
- prvky kybernetické bezpečnosti,
- životní cyklus kybernetické bezpečnosti. (Bašta a Kolouch, 2019)

2.1 Principy kybernetické bezpečnosti

Po spojení těchto tří principů aplikování kybernetické bezpečnosti hovoříme o efektivním využívání lidí, technologií a procesů k prevenci, detekci a reakci na kybernetické útoky a další hrozby, které by mohly narušit triádu CIA. (Pačka, 2019)

2.1.1 Triáda CIA

Triáda CIA je jedna z nejznámějších a nejvyužívanějších triád kybernetické bezpečnosti. Skládá se ze tří následujících principů, které se vzájemně prolínají:

- C – confidentiality – důvěrnost,
- I – integrity – celistvost,
- A – availability – dostupnost. (Šulc, 2019)

Důvěrnost

Důvěrnost definuje přístup k datům a informacím pouze subjektům k tomu autorizovaným. K tomuto členění se využívá klasifikace informací, které si určí sama organizace. Tuto klasifikaci je pak možné prolínat celým procesem zvládání kybernetické bezpečnosti. Ke klasifikaci informací je možné přihlížet s ohledem na jejich hodnotu, legislativní požadavky nebo citlivost. Příkladem klasifikace informací využívaném v komerční sféře je dělení:

- chráněné,
- interní,
- citlivé,
- veřejné. (Bašta a Kolouch, 2019)

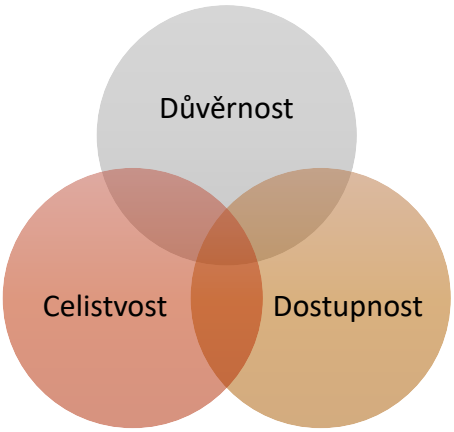
Dostupnost

Dostupnost garantuje přístup k informacím a datům v systémech v případě potřeby. V případě zničení nebo vymazání informací se zde jedná o narušení dostupnosti. (Bašta a Kolouch, 2019)

Celistvost neboli integrita

Integrita dat zajišťuje nemožnost zásahu do obsahu informací, dat a systémů neoprávněnou osobou. V souvislosti s touto problematikou se v rámci narušení bezpečnosti v informační bezpečnosti jedná o narušení integrity. V případě narušení integrity nemusí dojít k odhalení případně k němu dojde až po uplynutí delší časové doby. (Bašta a Kolouch, 2019)

Pro představení principů triády CIA je jejich prolínání graficky zpracováno na následujícím Obrázku 1 Propojení principů triády CIA. Při implementaci těchto tří oblastí se prostor, kde se vzájemně prolínají vymezuje jako kybernetická bezpečnost. (Bašta a Kolouch, 2019)



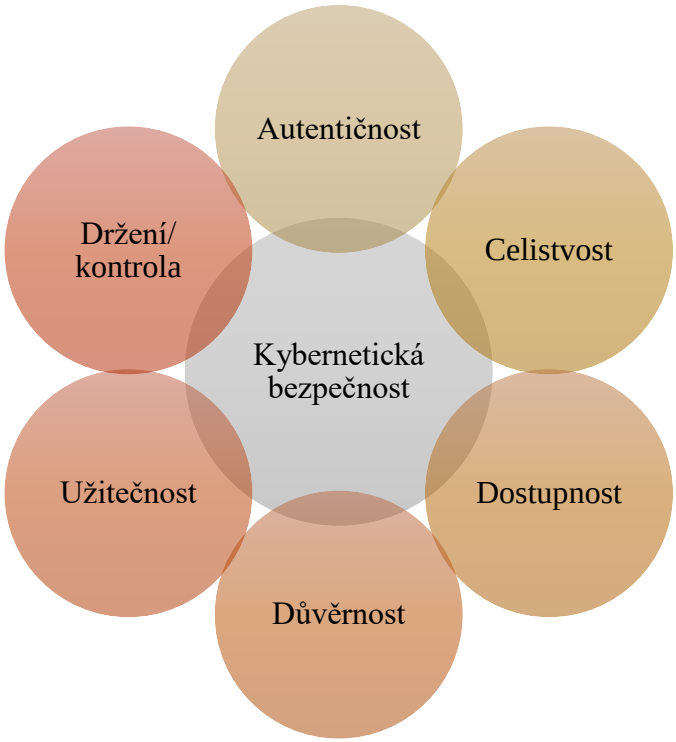
Obrázek 1 Propojení principů triády CIA (vlastní zpracování)

V současném vývoji však není dostačující využívat pouze tyto tři principy. Z tohoto důvodu některé literatury poukazují na využívání Parkerian hexad, což je rozšířená triáda CIA o tři další prvky:

- P/C – possession/control – držení nebo kontrola,
- A – authenticity – autentičnost,

- U – utility – užitečnost. (Marks, 2019)

Rozšířená triáda CIA je graficky zpracována na následujícím Obrázku 2 Parkerian hexad.



Obrázek 2 Parkerian hexad (vlastní zpracování)

Triáda CIA se vztahuje primárně k datům a informacím, které jsou prvky ICT zpracovávány, přenášeny a ukládány. Tato užší koncepce je tak chápána v rámci informační bezpečnosti, která se zaměřuje právě na ochranu informací, ale není zde podstatný jejich nosič. Jedná se tak o média v elektronické, papírové či jiné podobě. (Bašta a Kolouch, 2019)

2.1.2 Prvky kybernetické bezpečnosti

Interakce následujících tří prvků dohromady umožňuje tvořit kybernetickou bezpečnost:

- lidé,
- technologie,
- procesy. (Šulc, 2019)

Lidé

V rámci jakékoliv bezpečnosti jsou lidé klíčovým, ale zároveň často nejslabším prvkem. V případě kybernetické bezpečnosti je jejich role ještě umocněna, protože doba využívání ICT je ještě relativně krátká. Přesto je již náš život bez moderních technologií nemyslitelný.

Dynamika hardwaru a softwaru je obrovská, a proto je důležité, aby si lidé osvojili alespoň základní interakce v kyberprostoru. Stěžejní je:

- pochopení základů kybernetické bezpečnosti,
- porozumění funkcí ICT,
- posuzování využívaných aplikací,
- získávání gramotnosti v oblasti kybernetické bezpečnosti. (Bašta a Kolouch, 2019)

Na lidi podle jejich vzájemného působení s kybernetickou bezpečností lze nahlížet takto:

- tvůrci kybernetické bezpečnosti – tj. osoby prosazující a implementující principy a prvky kybernetické bezpečnosti ve vztahu k jednotlivci nebo k organizaci,
- příjemci základních pravidel a principů kybernetické bezpečnosti – tj. osoby implementující principy kybernetické bezpečnosti,
- subjekty, které jsou třeba chránit v rámci kybernetické bezpečnosti,
- subjekty, které je třeba vzdělávat v oblasti kybernetické bezpečnosti,
- rizika a hrozby v rámci fungování kybernetické bezpečnosti. (Bašta a Kolouch, 2019)

Technologie

Technologie jsou prostředkem, kterým se lidé neboli uživatelé připojují do online prostoru. V rámci technologií se hovoří o:

- koncových technologiích, zařízení pro uživatele (např. mobil, počítač, notebook),
- infrastruktuře sítě (např. Wi-Fi),
- službách (servery, aplikace),
- bezpečnostních prvcích (firewall),
- prvcích určených k monitoringu, analýze, autorizaci apod. (Bašta a Kolouch, 2019)

Procesy

Procesy jsou činnosti, které umožňují, aby lidé mohli pracovat s technologiemi. Může se jednat o identifikaci a dělení aktiv, řízení rizik, autorizaci, správu uživatelů, údržbu systémů, realizaci opatření, audit kybernetické bezpečnosti, školení, detekce incidentů apod. Procesy

jsou realizovány při všech druzích životních cyklů dat, informací, ICT, … (Bašta a Kolouch, 2019)

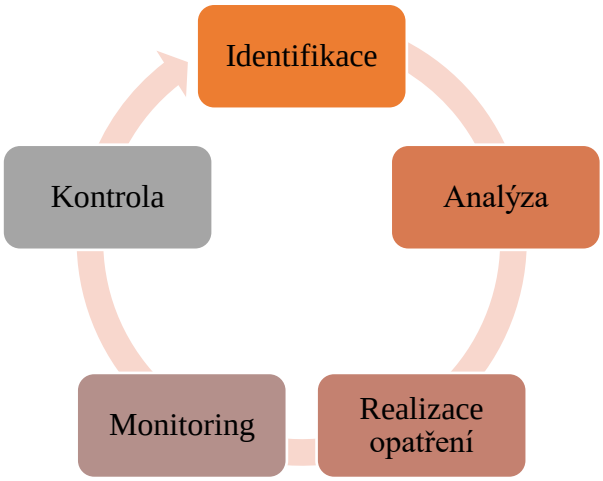
2.1.3 Životní cyklus kybernetické bezpečnosti

Při aplikaci kybernetické bezpečnosti je nutné uplatňovat triádu CIA i další dílčí prvky, kterými jsou:

- prevence,
- detekce,
- reakce.

Životním cyklem kybernetické bezpečnosti je koloběh, ve kterém neexistuje stacionární bod. Zavádění a udržování procesů kybernetické bezpečnosti lze přirovnat k cyklu analýzy rizik. Ten je však nutné v průběhu doplňovat o další podpůrné procesy. (Bašta a Kolouch, 2019)

Pro názornost je tento proces zobrazen na následujícím Obrázku 3 Analýza rizik.



Obrázek 3 Analýza rizik (vlastní zpracování podle (Bašta a Kolouch, 2019))

2.2 Kybernetické hrozby

Hrozbou může být cokoli, co je schopno narušení normálního stavu pomocí negativního působení. Hrozby lze podle různých hledisek nejčastěji klasifikovat následovně podle:

- zdroje hrozby,
- zdroje působení hrozby,
- cíle hrozby,
- motivace útočníka,

- typu hrozby. (Bašta a Kolouch, 2019)

Zdroje hrozby

Mezi zdroje hrozby lze zařadit:

- způsobené člověkem,
- technickou závadou,
- tzv. vyšší mocí.

U hrozeb ze strany člověka se lze zaměřit na iniciaci, jež vedla k zavinění, zda byla hrozba vedena úmyslně anebo neúmyslně. Úmyslnými hrozbami jsou kybernetické útoky, zcizení nebo smazání informací a dat anebo fyzické poškození. Z nedbalosti pak mohou vniknout hrozby v podobě fyzického poškození, neznalost interních postupů, a v důsledku toho poškození dat nebo systému, omylem smazaná data apod. Technickou závadou rozumíme chybu v zařízení. Vyšší mocí jsou myšlené přírodní události, požáry nebo výpadky elektrické energie. (Bašta a Kolouch, 2019)

Zdroje působení

Podle zdroje působení rozlišujeme hrozby vnitřní a vnější, tedy uvnitř nebo vně organizace. (Bašta a Kolouch, 2019)

Cíle hrozby

Hrozba může cílit na triádu CIA nebo na prvky kybernetické bezpečnosti. V rámci triády CIA se jedná o útok na důvěrnost dat, celistvost anebo jejich dostupnost. Při útoku na prvky kybernetické bezpečnosti se může jednat o lidi, technologie nebo procesy. Útoky na lidi probíhají nejen v reálném světě, ale i v kyberprostoru prostřednictvím kybernetických útoků. V případě technologií se typicky může jednat o hrozby působící na hardware, síť, software, uložená data a databáze. (Bašta a Kolouch, 2019)

Motivace

Motivací se zabýváme v případě, jeli hrozba způsobena člověkem úmyslně. Toto zkoumání je důležité pro vytvoření preventivních opatření v případě budoucího působení. U motivace lze sledovat hrozby za účelem:

- konkurenční výhody,
- finančního prospěchu,

- dokázání svých znalostí,
- odplaty. (Bašta a Kolouch, 2019)

Typ hrozby

Příklady typů hrozeb jsou mimo jiné sociální inženýrství, botnet, malware, ransomware, spam, podvodné nabídky, phishing, pharming, hacking, šíření závadného obsahu, kyberterorismus a další. (Bašta a Kolouch, 2019)

2.3 Kybernetické útoky

Kybernetickým útokem lze podle jedné z definic chápat jednání jedné osoby či skupiny osob využívající komunikační a informační technologie k útoku na jiné technologie a jejich infrastrukturu s cílem narušit jejich dostupnost, celistvost anebo integritu. Kybernetický útok je sled událostí, které se dělí na dvě základní stádia:

- neautorizovaný přístup,
- zneužití.

V rámci neautorizovaného přístupu se jedná o činnosti spojené s průzkumem napadeného prostoru, stanovení postupu útoku a aktivace útoku. Ve stádiu zneužití se útok přizpůsobuje prostředí, ustanovuje komunikační kanál pro řízení útoku a útočí. (Sedlák a Konečný, 2021; Bašta a Kolouch, 2019)

Spam

Spam je jakákoli hromadná nevyžádaná elektronická komunikace. Nejčastější podobou spamu je e-mail, SMS zprávy nebo zpráva na sociálních médiích. Masivně byl spam šířen okolo roku 2000. Tehdy tvořil většinu elektronické komunikace. Následkem bylo vytvoření spam filtrů. Jedná se o nástroj, který je dnes součástí antivirů, schránky e-mailu, popřípadě i sociálních sítí. Spam filtr dokáže pomocí algoritmů a statistik prověřit příchozí poštu a filtrovat ji. (Nejčastější pojmy v oboru IT zabezpečení, b.r.)

2.3.1 Malware

Malware je škodlivý kód, tedy škodlivý software, který byl vytvořený se špatným záměrem, a který může mít mnoho podob. Může se jednat o trojské koně, ransomware, viry, červy apod. Nejvíce zranitelný je samotný uživatel, který může být obětí phishingu, podvodných

e-mailů atp. Prevencí jsou aktualizace, tvorba záloh a obezřetnost v kyberprostoru. (Nejčastější pojmy v oboru IT zabezpečení, b.r.; Sedlák a Konečný, 2021)

Adware

Adwarem se rozumí software, který podporuje reklamu v podobě například vyskakovacího okna, webové stránky anebo reklam překrývajících část obrazovky. Jedná se o druh malwaru, který sleduje online pohyb uživatele, aby mohl cílit obsah reklam. Většinou se jedná o neškodný software, jeho odkazování však může vést i na podvodné stránky šířící malware. V některých případech dokáže adware měnit i nastavení domovské obrazovky v prohlížeči. (Adware, 2022)

Spyware

Spyware je špehovací software, který se neoprávněně nainstaluje do počítače uživatele. Jeho úkolem je sbírat informace o uživateli a odesílat je útočníkovi. Data poté využívá k reklamním účelům anebo útokům. Odhalení spywaru není snadné, většinou se vyznačuje tím, že zpomaluje internet a je odhalitelný v seznamu procesů. (Spyware, 2022)

Ransomware

Jedná se o škodlivý malware se schopností šifrování uživatelských dat, souborů, složek i celých zařízení, ta se pak stávají nedostupná. Ve většině případů pak hacker, který vlastní šifrovací klíč, požaduje výkupné. Existuje však více forem ransomwaru, ne vždy musí šifrovat. V některých případech může dojít pouze k uzamčení zařízení, aby se znemožnilo jeho použití. Existují i falešné ransomwary, které pouze klamou, že data byla zašifrována, nebo že zařízení bude uzamčeno. Ve skutečnosti útočník spoléhá pouze na zranitelnost oběti. Do systému se soubor může dostat stažením dat nebo díky nevhodnému zabezpečení. Nejčastěji se ransomware dostane do počítače za pomoci phishingového emailu nebo prostřednictvím sociálního inženýrství.

Oběťmi ransomwaru bývají organizace, které drží databáze informací a mají nevhodné nebo žádné bezpečnostní standardy Příkladem mohou být vzdělávací instituce nebo malé podniky. Dalšími cíli útoku mohou být subjekty závislé na svých datech, jako jsou nemocnice a velké korporace. (Sedlák a Konečný, 2021; Ransomware - definice a jak se úspěšně bránit, 2020)

2.3.2 Útoky

Sociální inženýrství

Sociální inženýrství v rámci svých útoků využívá vrozenou důvěru osob k získání přístupu jejich osobních dat. Existuje šest principů přesvědčování:

- Princip vzájemnosti – spočívá ve vštípení myšlenky, že když někomu poskytnete laskavost, měl by se odvděčit.
- Princip důslednosti – spočívá v lidské víře v dobré příběhy, které se lidem líbí a působí na ně.
- Princip sociálního důkazu – je široce používán v marketingu a působí na psychiku lidí.
- Princip autority – autority často dělají náročná rozhodnutí, která upoutávají pozornost ostatních. Pro osoby je však často jednodušší podřídit se lídrům a zbavit se odpovědností za svá rozhodnutí.
- Princip zalíbení – je opět hojně využíván v oboru reklamy, kdy jsou pro větší úspěch používány například modelky, které se vizuálně i projevově líbí. Pro lidi je pak lákavější produkt koupit.
- Princip nedostatku – myšlenka spočívající v tom, že lidé často ztrácejí pozornost, když mají omezený čas pro svá rozhodnutí. Tento princip je také využíván v marketingu v podobě dočasných slev.

Všechny tyto principy jsou běžně používané komerčními společnostmi, které se snaží své služby a produkty prodat. V současné době jsou principy využívané i hackery, kteří se snaží „hacknout“ lidskou mysl. Lidé mají nastavené chování. Jsme však nastaveni i pomoci a sdílet. Problém pak nastává při držení a sdílení citlivých informací, kdy je těžké rozlišit mezi veřejnými a soukromými údaji. (Evans, 2019)

Phishing

Pod pojmem phishing se skrývají útoky s cílem krádeže uživatelských dat, jako jsou přihlašovací údaje včetně hesel a platební údaje. Nejčastěji se k tomuto typu útoků využívají e-mailové služby. Jedná se o zkreslování odkazů, skrze které se po otevření útočník dostane k osobním informacím. (Sedlák a Konečný, 2021; Evans, 2019)

Pharming

Pharming je podvodná technika, jejíž cílem je krádež osobních údajů osob. Princip spočívá v napadení systému, který převádí jména domén na IP adresy a zase zpět, tzv. DNS (Domain Name System). Po napadení se prostřednictvím útoku přepisují IP adresy, které uživatele přesměrují na falešné stránky. Rozhraní těchto stránek může vypadat úplně stejně a útok je tím pádem jen těžko rozeznatelný. (Pharming, 2016; Co je DNS, 2016)

Denial of Service (dále DoS) a Distributed Denial of Service (dále DDoS)

DoS je druh kybernetického útoku, který má za cíl zablokování služby pro uživatele přetížením systému. Nejedná se tedy o útok, prostřednictvím kterého by útočník získal osobní data. Dochází k zahlcení systému uživatele, kvůli velkému množství požadavků, které jsou na něj vysílané. Systém není schopný zpracovávat takové množství požadavků a tím dojde k jeho zahlcení a nefunkčnosti. Pokud k útoku nedochází pouze z jednoho počítače, ale z více zdrojů najednou, hovoříme o DDoS útoku. (Šťastný, 2020)

Kapitola uvádí pouze některé druhy kybernetických útoků, které jsou v souvislosti s tématem a jsou v současné době nejvíce využívané v této oblasti. Údaje vycházejí ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2020 a dalších zdrojů.

2.4 Opatření kybernetické bezpečnosti

Ochranná opaření kybernetické bezpečnosti definuje zákon o kybernetické bezpečnosti. Subjekty splňující kritéria tohoto zákona jsou povinné tato opatření zavádět a zpracovávat k nim navazující bezpečnostní dokumentaci. Pro ostatní subjekty nejsou povinné, ale mohou je v rámci své bezpečnosti zavést dobrovolně a v jakémkoli rozsahu. Konkretizována jsou pak opatření ve vyhlášce o kybernetické bezpečnosti, která navazuje na normy řady ISO/IEC 27 000. (Bašta a Kolouch, 2019; ČESKO, 2014)

Bezpečnostní opatření jsou rozdělena na organizační a technická.

Organizační opatření zahrnují:

- systém řízení bezpečnosti informací,
- řízení rizik,
- bezpečnostní politiku,
- řízení aktiv,

- bezpečnost lidských zdrojů,
- řízení přístupu,
- zvládání bezpečnostních událostí a další. (Bašta a Kolouch, 2019)

Technická opatření zahrnují:

- řešení fyzické bezpečnosti,
- nástroje pro ochranu identity uživatelů,
- nástroje pro řízení přístupů,
- kryptografické prostředky apod. (Bašta a Kolouch, 2019)

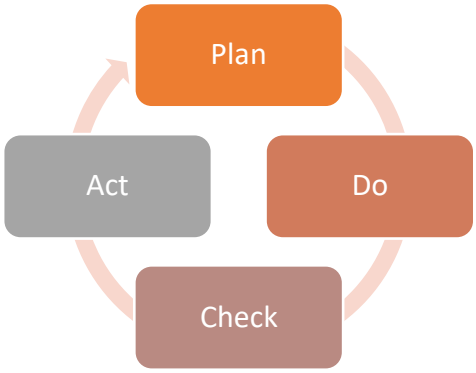
2.5 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (dále ISMS) je jedním z organizačních opatření kybernetické bezpečnosti. Jedná se o soubor pravidel části systému řízení, založených na procesu řízení rizik, jehož cílem je zachování důvěrnosti, dostupnosti a integrity dat. ISMS je součástí řízení, tedy managementu organizace, a může být aplikovaný na celý jeho systém nebo pouze část. ISMS lze zavádět v malých, středních i velkých podnicích a jeho interpretace se liší podle jednotlivých cílů a ambicí systému. Pro pomoc při zavádění ISMS v subjektu mají pomoci normy ISO/IEC 27 000, které jsou přizpůsobitelné jakémukoli typu organizace od průmyslových podniků, až po státní organizace. (Bašta a Kolouch, 2019)

ISMS je založený na komplexním přístupu v rámci celého cyklu. Jeho řízení je založené na Demingově cyklu, známém také jako PDCA cyklus. Jedná se o základní manažerský princip postupného zlepšování kvality prvků systému, a to díky opakovaným činnostem:

- plan – plánuj,
- do – dělej,
- check – kontroluj,
- act – jednej. (Bašta a Kolouch, 2019)

Tyto opakující se činnosti jsou graficky zobrazeny na následujícím Obrázku 4 Model PDCA cyklu.



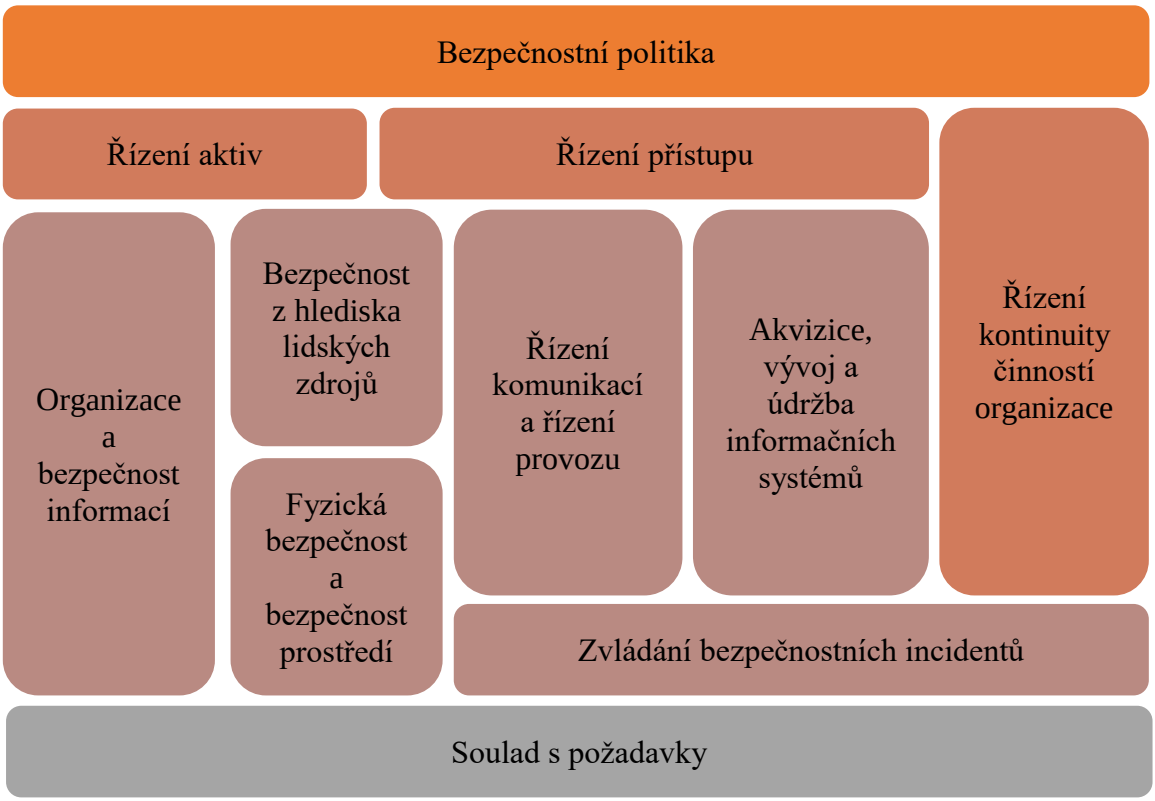
Obrázek 4 Model PDCA cyklu (vlastní zpracování)

PDCA cyklus lze využít při aplikaci a zavádění všech procesů ISMS. V normě ISO/IEC 27 001 jsou pak jeho fáze aplikace popsány detailněji:

- plánuj – obsahem je ustanovení cílů a politiky ISMS související s řízením rizik,
- dělej – jedná se o zavádění a používání ustanoveného ISMS,
- kontroluj – posuzování ISMS vůči stanoveným cílům a praktickým zkušenostem,
- jednej – spočívá v přijímání nápravných, preventivních a zlepšujících opatření. (Bašta a Kolouch, 2019)

V rámci normy ISO/IEC 27 001 je kladen důraz na pochopení požadavků ISMS, potřebu tvorby bezpečnostní politiky, implementaci a využívání opatření ISMS, dále monitorování a neustálé zlepšování. Zavedením ISMS nelze zajistit bezpečnost aktiv, ale lze snížit riziko zásahu do aktiv na přijatelnou úroveň. Nejslabším článkem bezpečnosti informací je člověk. (Bašta a Kolouch, 2019)

V rámci realizace procesů bezpečnostních opatření kybernetické bezpečnosti doporučuje norma ISO/IEC 27 002 jejich zařazení do 11 oblastí. Tyto oblasti jsou znázorněny na Obrázku 5 Oblasti bezpečnosti informací. (Doucek, 2020)



Obrázek 5 Oblasti bezpečnosti informací (Doucek, 2020)

Obsah jednotlivých oblastí:

- Bezpečnostní politika – v této oblasti je důležité stanovení cílů a jejich rozsahu, dále pravidel a principů a také definování pravomocí a odpovědností.
- Řízení aktiv – v organizaci je třeba zavést seznam aktiv, ke kterým je daný vlastník odpovědný za dané aktivum a nastavení přiměřené ochrany každému z nich.
- Organizace bezpečnosti informací – je potřeba stanovit strukturu bezpečnosti informací v rámci interních procesů a postupů a dále ve vztahu k externím dodavatelům anebo jiným organizacím. Dále je prioritou této oblasti dodržování stanovených pravidel skrze celou strukturu.
- Bezpečnost z hlediska lidských zdrojů – definování pravidel pro ochranu informací u zaměstnanců a udržování jisté míry ochrany.
- Fyzická bezpečnost a bezpečnost prostředí – jedná se o zabezpečení oblasti, která chrání subjekt jako celek a bezpečnost zařízení, které je zaměřené na jednotlivé prvky.

- Řízení komunikace a řízení provozu – jedná se o zajišťování ochrany systémů. Tato oblast se dělí do deseti skupin opatření zaměřených například na snížení rizika úmyslného zneužití systému apod.
- Řízení přístupu – pravidla pro přístup k zařízením a jejich využívání nebo k přístupu k informacím. Důležitým bodem této oblasti je napojování pravidel řízení přístupu na pracovní pozice, a ne pouze na fyzické osoby.
- Akvizice, vývoj a údržba informačních systémů – prosazování neustálého zlepšování nastaveného systému a jeho aktualizace. Tato oblast je vázána na aktuální trendy a modernizaci v oblasti řešené problematiky.
- Zvládání bezpečnostních incidentů – definování pravidel při detekci bezpečnostního incidentu jak pro uživatele, tak pro vedoucí a odborné pracovníky.
- Řízení kontinuity činností organizace – nápravná opatření po bezpečnostním incidentu a zavádění postupů prevence.
- Soulad s požadavky – naplnění požadavků z výchozí dokumentace. (Doucek, 2020)

Mezi přínosy zavedení ISMS v organizaci patří zvýšení konkurenceschopnosti, posílení organizační struktury subjektů, snížení rizik v oblasti práce s daty a informacemi, jako je jejich únik, nedostupnost anebo ztráta. Další výhody spočívají v úspoře nákladů při řešení případných incidentů a nákladů spojených s výpadkem systémů organizace a další. (Doucek, 2020)

2.6 Řešení fyzické bezpečnosti

Fyzická bezpečnost je zaměřena na ochranu aktiv subjektu s cílem zamezení přístupu nepovolaných osob, a nakonec zamezení úniku dat a informací. Základním článkem v procesu plánování je stanovení fyzického bezpečnostního perimetru, jeho hranice a definování potřebných prostředků na jeho ochranu. Tyto prostředky slouží k zamezování neoprávněného vstupu, poškození, nepovoleným zásahům a k zajištění vnější ochrany objektu, tedy budovy. Jedním ze základních principů fyzické bezpečnosti je vymezení vícestupňové ochrany. Stupně pak představují oblasti a hranice, které by musel narušitel překonat ve snaze narušení bezpečnosti. (Lukáš, 2015; Bašta a Kolouch, 2019)

Stupně ochrany jsou:

- Perimetrická ochrana – její součástí je uplatňování bezpečnostních opatření po obvodu pozemku subjektu a v prostoru mezi ním a jeho hranicí. Perimetrem je katastrální hranice subjektu vymezena dále bariérou. Cílem je zpomalení či odhalení pachatele a prvky aplikované v tomto stupni ochrany by měly být klimaticky odolné.
- Plášťová ochrana – realizuje se na plášti subjektu, konkrétně budovy, kterou tvoří stěny, dveře, okna a zámky. Dále popřípadě kamerové systémy, detektory, mříže a další prvky. Cílem tohoto stupně ochrany je znemožnění průchodu pachatele, jeho odhalení nebo zastrašení. Tyto prvky se aplikují zvenku budovy a opět musí splňovat určitou klimatickou odolnost.
- Prostorová ochrana – je realizována v prostorách budovy, konkrétními prvky jsou dveře, zámky, kontroly vstupu, kamerové systémy, poplachové zabezpečovací a tísňové systémy (dále PZTS) anebo detektory. Cílem tohoto stupně ochrany je zpoždění anebo odhalení narušitele.
- Předmětová ochrana – slouží jako ochrana cenných předmětů nebo zařízení. Mohou ji tvořit prvky typu kamerových systémů, PZTS, vitríny apod. (Benešová, 2019; Lukáš, 2015)

2.7 Dílčí závěr kapitoly

Kybernetickou bezpečnost umožňují tvořit lidé, technologie a procesy. Jedním ze základních principů je triáda CIA, která je zaměřená převážně na informace a data. Ta jsou ale zpracovávána, přenášena a ukládána zařízeními. Pro adekvátní nastavení ISMS je nutné nastavení hranic ochrany, identifikace aktiv primárních i podpůrných a identifikace procesů organizace. Životní cyklus kybernetické bezpečnosti je nikdy nekončícím procesem, který lze přirovnat k analýze rizik. Pro efektivní zavedení kybernetické bezpečnosti do provozu organizace se tudíž nesmí jednat o jednorázovou aktivu. Hrozby v podobě kybernetických útoků jsou díky vývoji moderních technologií na vzestupu a je třeba se na ně připravit v podobě preventivních opatření jak organizačních, tak technických.

3 KYBERNETICKÁ BEZPEČNOST VE ŠKOLÁCH

I díky pandemii Covid-19 došlo k velkému digitálnímu pokroku a transformaci. Ještě v roce 2017 bylo k internetu připojeno asi 27 miliard zařízení, do roku 2030 se odhaduje nárůst online zařízení až na 125 miliard. Digitální svět se začal stále více prolínat s tím fyzickým a tím se samozřejmě vyvíjejí i nová nebezpečí. Touto rostoucí tendencí kyberprostoru dochází i k odpovídajícímu nárůstu kybernetických útoků. Mezi hlavní odvětví zasažené kybernetickými hrozbami patří podle směrnice EU následující:

- veřejná správa/vláda – 198 nahlášených incidentů,
- poskytovatelé digitálních služeb – 152 nahlášených incidentů,
- široká veřejnost – 151 nahlášených incidentů,
- zdravotnictví – 143 nahlášených incidentů,
- finanční a bankovní sektor – 97 nahlášených incidentů. (Cybersecurity: main and emerging threats in 2021 (infographic), 2022)

Pozorování provedla Agentura Evropské unie pro kybernetickou bezpečnost (dále jen ENISA) v období od dubna 2020 do července 2021. Podle společnosti ENISA lze identifikovat devět hlavních skupin hrozeb kybernetické bezpečnosti:

- ransomware,
- cryptojacking (útočníci využívají zařízení uživatele k těžbě kryptoměny),
- hrozby proti datům,
- malware,
- šíření dezinformací,
- lidské chyby a chybné nastavení systému,
- útoky proti integritě a dostupnosti dat,
- e-mailové hrozby,
- hrozby v dodavatelských vztazích.

Podle zprávy z agenturního výzkumu se 76 % občanů EU domnívá, že se stanou obětí kybernetického útoku a že čelí vzrůstajícímu tlaku tohoto rizika. (Cybersecurity: main and emerging threats in 2021 (infographic), 2022)

3.1 Kybernetická bezpečnost v zahraničí

Společnost Check Point Research ve svém globálním výzkumu, prováděném v roce 2021, zkoumala nárůst kybernetických útoků cílených na organizace v prvním a druhém pololetí. V červenci byly nejvíce postižené země podle týdenních průměrných počtů útoků na organizace:

- Indie – 5 196 s 22% nárůstem oproti prvnímu pololetí,
- Itálie – 5 016 se 70% nárůstem,
- Izrael – 4 011 s nárůstem 51 %,
- Austrálie – 3 934 a s nárůstem o 17 %.

Dále následovaly Turecko, Portugalsko, Španělsko, Polsko, Mexiko, Singapore, Velká Británie a další. Společnost dále uvádí, že ve více než 50 % zemí je vzdělávací odvětví nejvíce postiženou oblastí a v 94 % z nich bylo odvětví vzdělávání mezi třemi nejpostiženějšími sektory. Z toho Velká Británie zaznamenala největší procentuální nárůst kybernetických útoků oproti jiným zemím. Některé servery dokonce uvádějí procento nárůstu o 142 %. (Education Sector Experienced Highest Volume of Cyber Attacks in July, 2018)

Zprávy o kybernetických útocích na vzdělávací sektor jsou v poslední době ve Velké Británii častým jevem. Již v roce 2017 došlo k úniku dat milionů uživatelů ze vzdělávací platformy. Mezi oběťmi byli učitelé, žáci a rodiče. V roce 2018 pak došlo k nabourání bezpečnostních kamer ve třech školách v anglickém Blackpoolu, jejichž obsah byl přenášen na americké webové stránce. Velký nárůst těchto útoků zaznamenali od podzimu roku 2020. Údajně byla útokem postižena až pětina vzdělávacích zařízení od základních škol, přes střední a vysoké školy, až po univerzity. Podle pojišťovny pro vzdělávací zařízení byly nejčastější formou útoku malware a phishing. Nejvíce jsou těmito útoky v zemi postiženy soukromé školy, které utrpí na pověsti. Často jsou útoky cílené na ztrátu nebo zcizení dat v oblasti vzdělávacích podkladů, finančních záznamů a tehdy s testováním v souvislosti s pandemií COVID-19. (Alert: Further ransomware attacks on the UK education sector by cyber criminals, 2022; Cyber attacks are one of the biggest threats that schools face, experts warn, 2019)

Útoky na vzdělávací systém zažívají i Spojené státy americké, které také čelí neustálému zvyšování počtu kybernetických útoků v této oblasti. Jen od roku 2016 bylo nahlášeno více než 1 200 kybernetických bezpečnostních incidentů na školy po celé zemi. Nejčastěji byly

tyto útoky prováděny formou ransomwaru, DDoS útoků a phishingů. Jen za rok 2020, kdy stoupal tlak na využívání technologií z důvodu pandemie, bylo hlášeno více než 400 incidentů. Zprávy dále uvádějí, že útoky mají velký dopad na výuku dětí a studentů, školní rozpočty, ochranu citlivých dat rodičů, žáků, studentů a učitelů a elektronickou komunikaci. Důvody jsou podle amerických odborníků obdobné. Školy vlastní databáze velkého množství různých dat, v poslední době mnohem více spoléhají školy na technologie, které mnohdy neumí zabezpečit nebo na jejich ochranu nemají dostatečné finanční prostředky. V lednu 2022 došlo k útoku ransomwaru, který ochromil webové stránky zhruba 5 000 škol. Problémem se v USA začínají zabývat i političtí představitelé. V roce 2021 bylo představeno minimálně 170 zákonů o kybernetické bezpečnosti. V říjnu 2021 prezident USA Joe Biden podepsal jeden ze zákonů o kybernetické bezpečnosti, který nařizuje vydání doporučení pro pomoc školským zařízením. (Cyber attacks are one of the biggest threats that schools face, experts warn, 2019; Klein, 2022; Klein, 2022)

3.2 Kybernetická bezpečnost v České republice

I v České republice byly zaznamenány kybernetické útoky na vzdělávací zařízení. Vzhledem k uchovávání citlivých informací ve školách, jako jsou záznamy dětí a studentů, zaměstnanců škol a rodičů, bychom si měli klást otázku, jak dobře jsou tyto informace zabezpečené. Nejčastějšími typy útoků vedených proti školám jsou malware a phishing, které spoléhají na malé znalosti uživatele. Školy navíc často nedisponují dostatečnou ochranou svého vybavení. Problémem, podle výzkumu společnosti Eset, je nedostatek financí školských zařízení na zajištění adekvátní bezpečnosti. Až jedna pětina z nich nemá dostatečné finance na IT specialistu a ochranu dat. Společnost do svého výzkumu zapojila 540 základních a středních škol. Z nich 43 % najímá externího odborníka, 34 % má interní pracovníky IT a ve zbylých procentech škol se o problematiku stará vyučující informatiky. Školy nespadají pod kybernetický zákon, a tak nelze určit počty vedených kybernetických útoků v celém vzdělávacím sektoru, protože nemají za povinnost je hlásit a mnohdy ani nemusejí vědět, že se staly obětí takového útoku. Národní úřad pro kybernetickou bezpečnost se snaží menším organizacím pomoci vydáváním manuálů a doporučení, a to právě v důsledku narůstajícího tlaku na využívání technologií za pandemie. (Magdoňová, 2019; Kresa, 2018)

Výroční zpráva NÚKIB uvádí, že se vzdělávací instituce stávají mnohem častěji cílem kybernetických útoků. Nejčastější formou útoku bývá ransomware. S tímto druhem útoku se

například potýkala Vysoká škola ekonomická v Praze a Univerzita Palackého v Olomouci. Masarykova Univerzita v Brně naopak zachytila nový typ malwaru, který cílil na uživatele phishingovou kampaní. Nejčastějším prostředkem byl podvodný e-mail. (Národní úřad pro kybernetickou bezpečnost, 2021)

3.3 Dílčí závěr kapitoly

Ve všech zemích kvůli pandemii COVID-19, transformaci digitalizace, a tudíž propojování online světa s tím fyzickým, vzrůstá počet kybernetických útoků. Některé země čelí nárůstu o desítky procent. Vzdělávací systém je ve spoustě zemí na prvních příčkách v počtu útoků. Útočníci často vidí učitele a rodiče dětí, žáků a studentů jako snadný cíl, protože nebývají vhodně vybaveni, aby dokázali kybernetickým útokům a často nedisponují ani znalostmi z této oblasti. Na černém webu jsou však citlivé údaje, shromažďované ve školském sektoru lukrativní. Na uvedených příkladech z různých zemí i České republiky lze pozorovat podobné charakteristiky. Oblast vzdělávání je v oblasti bezpečnosti finančně, odborně i legislativně podhodnocena.

II. PRAKTICKÁ ČÁST

4 CHARAKTERISTIKA VYBRANÉHO SUBJEKTU

Praktická část diplomové práce se zabývá charakteristikou vybraného subjektu podle řady norem ISO/IEC 27 000. Dále zahrnuje metodu identifikace rizik, analýzu rizik, jejich vyhodnocení a návrhy opatření na zlepšení současného stavu. Výsledkem praktické části je pak vytvoření interního bezpečnostního dokumentu, který je zaměřený na systém řízení bezpečnosti informací a kybernetickou bezpečnost, včetně vztahu k fyzické bezpečnosti objektu.

Diplomová práce pojednává o malotřídní škole Základní škola a mateřská škola Novosedly nad Nežárkou. Jedná se o trojtřídní školu s oddělením mateřské školy, školní družinou a se školní jídelnou a kuchyní. Řídícím subjektu je ředitel školy jakožto statutární orgán s rozhodovacím právem. Zřizovatelem subjektu je obec.

Škola se nachází v obci Novosedly nad Nežárkou, která náleží ORP Třeboň v jižních Čechách. Obec se skládá ze třech částí, a to Novosedly nad Nežárkou, Kolence a Mláka. Celkový počet obyvatel je cca 681.

Obrázek 6 Lokalizace obce (google.com/maps, b. r.)

Obrázek 7 Poloha školy (vlastní, 2021)

Obsah činnosti subjektu je dán zřizovací listinou příspěvkové organizace obce, podle které se objekt musí řídit: „*Tato příspěvková organizace poskytuje základní vzdělání, zabezpečuje rozumovou výchovu ve smyslu vědeckého poznání a v souladu se zásadami vlastenectví, humanity a demokracie a poskytuje mravní, estetickou, pracovní, zdravotní, tělesnou výchovu a ekologickou výchovu žáků. Umožňuje též náboženskou výchovu. Připravuje žáky pro další studium a praxi. Její činnost je vymezena příslušnými ustanoveními zákona č. 29/1984 Sb., o soustavě základních škol, středních škol a vyšších odborných škol (školský zákon), v platném znění, a prováděcími předpisy (zejména vyhláška MŠMT č. 291/1991 Sb., o základní škole, v platném znění).*“

O správu majetku školy se dělí dva subjekty – zřizovatel a správce školy. Zřizovatelem je starosta obce, protože pozemek i budovu samotnou vlastní obec. Další odpovědnou osobou je správce objektu, tedy ředitel školy, který má majetek ve výpůjčce. Tuto odpovědnost má danou zřizovací listinou: *„Příspěvkové organizaci se předává do správy k vlastnímu hospodářskému využití dále uvedený majetek ve vlastnictví zřizovatele, jehož celková účetní hodnota činí 5 435 769,41 Kč.“*

Umístění a topologie objektu

Škola má dlouholetou kořeny. Jedná se o více než 100 let starou budovu s rozsáhlou zahradou. Pozemek je lokalizovaný na rovině naproti obecnímu úřadu, který je vzdálen asi 100 m. Subjekt tvoří dvou patrová budova, je částečně podsklepená, s půdní vestavbou a včetně obecního bytu, který nemá vlastní samostatný vchod. Mezi přízemím a prvním patrem se v budově nachází kamenné schodiště.

Obrázek 8 Zobrazení školy (google.com/maps, b. r.)

V přízemí školy se nachází obecní byt, školní družina, sociální zařízení včetně technické místnosti, šatna pro základní školu, tělocvična a školní jídelna s kuchyní. V prvním patře se nachází tři kmenové třídy základní školy, sociální zařízení, sklad/archiv, ředitelna a oddělení mateřské školy.

Pozemek je obehnaný laťkovým plotem a na zahradu se lze dostat dvěma vraty, která se nezamykají. Do budovy vedou tři vstupy, a to hlavní vchod, který je zabezpečený, dále zadní vchod, který vede na pozemek školy (zahradu) a je vedený jako evakuační a boční vstup vedoucí ze školní kuchyně skrze rampu rovněž na pozemek školy. Z pozemku školy je také boční přístup do sklepa a zadní přístup do garáže soužící obecním zaměstnancům.

Pro komplexní charakteristiku a následnou identifikaci rizik je nutné uvést, že škola byla v minulosti dvakrát vykradena. V prvním případě šlo o případ ze série krádeží hotovosti malotřídních škol v malých obcích. Jednalo se o období, kdy školy vybíraly peníze na školní výlety. Zloději byli dopadeni. Jako opatření zavedl subjekt platby ze stran rodičů primárně převodem na účet školy. Platby v hotovosti tak již nejsou v subjektu běžné.

Ve druhém případě šlo o krádež dvou křovinořezů, které byly obecním majetkem a byly uloženy v garáži, kterou využívají obecní zaměstnanci. V tomto případě se pachatele nepodařilo dopadnout.

Tyto události podtrhují význam chybějících prvků poplachových zabezpečovacích a tísňových systémů (dále PZTS).

Zaměstnanci a žáci

V současné době působí na škole 15 zaměstnanců, které lze rozdělit na dvě skupiny:

- pedagogičtí zaměstnanci,
- nepedagogičtí zaměstnanci.

Pedagogickými zaměstnanci se rozumí učitelky a učitelé oddělení mateřské a základní školy a vychovatele školní družiny. V rámci pedagogů je výhodou školy 100 % aprobovanost učitelů a personální rozvoj dalšího vzdělávání všech pracovníků.

Nepedagogickými zaměstnanci se rozumí provozní a ostatní pracovníci školy. Jsou zde zahrnuty následující pracovní pozice: školnice, kuchařka, vedoucí ŠJ, pomocná síla ŠJ a topič.

Přehled počtu zaměstnanců v jednotlivých skupinách je uveden v následující Tabulce 1 Přehled počtu zaměstnanců.

Tabulka 1 Přehled počtu zaměstnanců

DRUH ZAMĚSTNANCŮ	POČET
Pedagogičtí zaměstnanci	10
Nepedagogičtí zaměstnanci	5
Celkem	**15**

Počty žáků jsou v jednotlivých odděleních kapacitně omezeny, tyto limity jsou uvedeny v Tabulce 2 Maximální kapacity.

Tabulka 2 Maximální kapacity

ODDĚLENÍ	MAXIMÁLNÍ KAPACITA
Mateřská škola	24 (25 na povolení zřizovatele)
Základní škola	44
Školní družina	44
Školní jídelna	70

Školu v současné době navštěvuje 65 žáků. Čísla jsou uvedena včetně přijímaných dětí uprchlíků vzhledem k událostem ve světě. Přehled počtu žáků uvádí Tabulka 3 Přehled počtu žáků.

Tabulka 3 Přehled počtu žáků

ŽÁCI	POČET
Žáci v MŠ	25
Žáci v ZŠ	40
Celkem	**65**

Během aktivní doby subjektu se na pozemku a v budově může pohybovat okolo 80 osob.

Řízení komunikace subjektu

Komunikaci v rámci subjektu lze rozdělit na následující skupiny:

- komunikace mezi zaměstnanci,
- komunikace s rodiči (odpovědnými zástupci dětí a žáků) a lidmi mimo organizaci.

Komunikace mezi zaměstnanci školy může probíhat skrze server, který jsou všichni povinni sledovat prostřednictvím virtual private network (VPN). V rámci online komunikace lze zaměstnance kontaktovat skrze MS Teams a školní e-mail. Dalšími možnostmi komunikace jsou papírové dokumenty, osobní konfrontace a porady, které se dělí na porady pedagogické a porady provozní. Na pedagogické porady nemají nepedagogičtí pracovníci přístup, protože se zde jedná s osobními údaji dětí a žáků.

Komunikace s rodiči (zákonnými zástupci dětí a žáků) může probíhat online formou skrze MS Teams, e-mail nebo webové stránky. Dalšími možnostmi jsou papírové dokumenty anebo osobní konzultace. Škola nemá online systém pro zjednodušení správy školní agendy, kterým je například informační systém Bakaláři.

Komunikačními kanály pro komunikaci s dalšími osobami jsou telefon, e-mail, datová schránka, papírová dokumentace a osobní schůzky.

4.1 Popis subjektu podle řady norem ISO/IEC 27 000

Tato podkapitola poskytuje detailnější popis subjektu podle částí norem řady 27 000. V obsahu jsou části a jednotlivé odstavce číslovány podle normy ČSN/ISO 27000. V dílčím závěru kapitoly jsou následně uvedená rizika vyplývající z celkové charakteristiky subjektu.

A.5 Politiky bezpečnosti informací

Škola v současné době nedisponuje nastavením politiky bezpečnosti informací, proto je cílem této práce zavést interní dokument dostupný vedení subjektu a vytvoření příručky pro zaměstnance. Školní prostředí soustřeďuje citlivé informace o zaměstnancích a dětech a žácích včetně jejich zákonných zástupců. Proto je důležité nastavení ochrany informací jakožto jedním z opatření kybernetické bezpečnosti.

A.6 Organizace bezpečnosti informací

Oblast organizace bezpečnosti informací je rozdělena na 2 obsahové části:

- interní organizace,

- mobilní zařízení a práce na dálku.

Obě tyto oblasti jsou charakterizovány v následujících odstavcích.

A.6.1 Interní organizace

Cílem této části je rámec pro ustanovení řízení bezpečnosti informací.

A.6.1.1. Role a odpovědnosti bezpečnosti informací

Odpovědnost za bezpečnost subjektu má ředitel školy, dá se tedy nazvat manažerem bezpečnosti. Tato role zahrnuje i odpovědnost za bezpečnost informací. Ředitel odpovídá za organizaci i své zaměstnance. Podle těchto odpovědností ho lze definovat i jako manažera bezpečnosti, což zahrnuje i management bezpečnosti informací. Odpovědnost za objekt má zřizovatel.

Zaměstnanci jsou různě podle své náplně práce pověřování nad správou některých aktiv, za která v průběhu pracovního vztahu odpovídají. Úrovně oprávnění přístupu k informacím jsou stanoveny v pracovních smlouvách zaměstnanců, dále i v nařízeních, vyhláškách a pokynech.

Soubor aktiv není subjektem veden, tento seznam bude proto zahrnut do interního dokumentu v aplikační části práce.

A.6.1.2 Princip oddělení povinností

V subjektu dochází ke třem případům konfliktních rolí a jejich působnost:

- ředitel školy je zároveň učitelem 1,
- zřizovatel je zároveň topičem a má i přístup do všech prostor,
- školnice má ve své náplni práce více typů činností – úklid, správa objektu, správa nad fotodokumentací, skartace a další.

Subjekt má zavedené kroky, které mají předcházet zneužití postavení. Ředitel školy má podpisový vzor společně s vychovatelkou, aby se zamezilo zneužití státních financí. Školnice má ve své pracovní smlouvě podepsanou doložku o mlčenlivosti.

A.6.1.3 Kontakt s příslušnými orgány a autoritami

Ředitel má v případě potřeby možnost kontaktování různých autorit, a to podle druhu potencionálního bezpečnostního incidentu. V případě drobných incidentů provádí ředitel

šetření sám a ukládá kázeňská/kárná opatření v rámci zákoníku práce. V případě závažnějšího incidentu má ředitel následující možnosti kontaktování autorit:

- kontakt se zřizovatelem,
- kontakt s pověřencem GDPR,
- kontakt s právníkem (škola má právní ochranu),
- kontakt s policií.

Incidenty, kdy je za potřebí hasičského záchranného sboru, pohotovostních služeb, dodavatelů elektřiny apod. kontaktuje stanovená požární hlídka podle evakuačního plánu/ poplachové směrnice.

A.6.1.4 Kontakt se zájmovými skupinami

Škola má ve svém okruhu široké spektrum zájmových skupin. K nejčastějšímu kontaktu dochází v rámci následujících skupin:

- pověřenec GDPR – zasílá a aktualizuje informace týkající se např. nakládání s dokumentací,
- kontakt v rámci MŠMT – telefonní linky pro ředitele škol, statistiky apod.,
- kontakt v rámci Asociace ředitelů základních škol,
- kontakt v rámci školení, která jsou akreditovaná MŠMT a další.

V souvislosti s kybernetickou bezpečností a bezpečností informací má škola možnost sledovat aktuality na webových stránkách Národního úřadu pro kybernetickou bezpečnost a v případě bezpečnostního incidentu jej kontaktovat.

A.6.1.5 Bezpečnost informací v řízení projektů

Projekty ve školách mohou nabývat různého rámce – projekty mezi školami, dotační programy pro školy, projekty ve spolupráci s organizacemi, spolupráce s MŠMT a další. V rámci těchto projektů se nejčastěji řeší problematika GDPR v souvislosti s pořizováním fotodokumentace.

A.6.2 Mobilní zařízení a práce na dálku

Ředitel školy i většina zaměstnanců školy má ke své činnosti pracovní notebook. Subjekt nemá nastavená žádná pravidla pro jeho správu, ochranu a použití.

A.7 Bezpečnost lidských zdrojů

Oblast bezpečnosti lidských zdrojů je rozdělena na dobu před vznikem a během pracovního vztahu.

A.7.1. Před vznikem pracovního vztahu

Cílem této části je ochrana při přijímání nových zaměstnanců.

A.7.1.1 Prověřování

Při vybírání nových zaměstnanců jsou vyžadovány výpisy z rejstříků trestů a reference z minulých prací. Poté si ředitel provádí vlastní reference.

A.7.2.2 Podmínky pracovního vztahu

Vybraní noví zaměstnanci musí podstoupit zdravotní prohlídku a školení BOZP. Zaměstnanci jsou poučeni o náplních své práce a svých rolích v zařazení v rámci organizace a jsou povinni podle toho jednat. Součástí pracovní smlouvy je doložka o mlčenlivosti.

A.7.2. Během pracovního vztahu

Cílem pracovního vztahu je dodržování stanovených pravidel, jeho náplně a rolí.

A.7.2.1 Odpovědnosti vedení organizace

Vedení, tedy ředitel školy, je povinen neprodleně informovat zaměstnance o změnách týkajících se jejich pracovního vztahu nebo změny v řízení a struktury organizace. Ředitel je povinen kontrolovat plnění pracovních povinností.

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

V současné době ve škole neprobíhá školení nebo jiné vzdělávání v souvislosti s kybernetickou bezpečností anebo s bezpečností informací.

A.7.2.3 Disciplinární řízení

V případě drobných bezpečnostních incidentů ukládá ředitel kázeňská/kárná opatření v rámci zákoníku práce. V případě závažnějšího incidentu má ředitel možnost kontaktovat příslušné autority.

A.8 Řízení aktiv

Cílem řízení aktiv je stanovení odpovědností za aktiva, stanovení pravidel o jejich nakládání a definování klasifikace informací, ...

A.8.1 Odpovědnost za aktiva

Odpovědnost za aktiva cílí na ochranu před jejich poničením nebo ztrátou.

A.8.1.1/A.8.1.2 Seznam aktiv a vlastnictví aktiv

Náplní je identifikace aktiv subjektu, definování odpovědností za ně a případně stanovení činností vedoucích k jejich ochraně. V současném stavu není komplexní seznam aktiv v subjektu veden. Jejich seznam je proto zpracován v aplikační části práce v návrhu interního bezpečnostního dokumentu.

A.8.1.3 Přípustné použití aktiv

Subjekt nemá nastavena pravidla pro použití aktiv.

A.8.1.4 Navrácení aktiv

Zaměstnanci jsou povinni navrátit aktiva, která jim byla zapůjčena. Organizace vede evidenci navrácených aktiv v dlouhodobém vypůjčení. Subjekt neřeší navrácení vypůjčených aktiv krátkodobého držení, tím se rozumí například papírová dokumentace, která však může obsahovat citlivé údaje.

A.8.2. Klasifikace informací

Informace by měly mít odpovídající stupeň ochrany v návaznosti na jejich důležitost.

A.8.2.1. Klasifikace informací

V organizaci lze rozdělit informace podle přístupu k nim následovně:

- s přístupem pouze ředitele školy (případně zřizovatele),
- s přístupem pedagogických zaměstnanců,
- s přístupem všech zaměstnanců.

Všichni zaměstnanci mají ve smlouvách podepsanou doložku o mlčenlivosti.

A.8.2.2. Označování informací

V současné době využívá ředitel školy vlastního barevného označování papírové dokumentace, kde:

- červené šanony obsahují matriku školy,
- černé šanony obsahují účetnictví,
- zelené šanony obsahují další dokumenty.

A.8.2.3 Manipulace s aktivy

Zaměstnanci jsou povinni manipulovat pouze s takovými aktivy, které využívají a potřebují k činnostem v rámci své pracovní náplně. Tuto skutečnost je těžké kontrolovat, protože z důvodu nedostatku prostor je ředitelna včetně jejího obsahu sdílena s dalšími zaměstnanci.

A.9 Řízení přístupu

Cílem řízení přístupu je omezení přístupu k informacím a vybavení pro zpracování informací.

A.9.1 Požadavky organizace na řízení přístupu

Cílem by mělo být definování politiky řízení přístupu.

A.9.1.1 Politika řízení přístupu

V souvislosti s informacemi a daty převážně v papírové podobě, a které jsou uloženy v archivu/skladu a v ředitelně, není omezen přístup pro zaměstnance. Obě místnosti jsou více účelové. V ředitelně se nachází server a je zde umístěna tiskárna s kopírkou, ke které mají zaměstnanci neomezený přístup. Přístup není podmíněn žádným přihlášením.

Co se týče počítačového vybavení mají zaměstnanci vlastní notebook nebo přidělen stolní počítač. V těchto zařízeních si sami určují míru zabezpečení a dohlížejí na bezpečnost zařízení i přístup k němu pro jiné osoby. Správu/údržbu nad těmito zařízeními provádí externí IT pracovník na základě požadavků uživatelů (zaměstnanců).

V rámci serveru funguje v objektu pro zaměstnance VPN (virtual private network), ke které se mohou připojit. Toto připojení je funkční pouze v objektu nikoli na dálku.

K počítačovému vybavení učeben mají přístup žáci pod dohledem učitele. K přístupu k těmto zařízením slouží pro žáky univerzální přístupové jméno a heslo.

Řízení přístupu jednotlivých místností je dáno podle hmotné odpovědnosti vyplývající z pracovní smlouvy. Klíče pro přístup jsou soustředěny v ředitelně. Klíče, které nejsou sdíleny více zaměstnanci nosí dotyční zaměstnanci u sebe.

A.10 Kryptografie

Cílem je zamezení zneužití a únik citlivých informací.

A.10.1 Kryptografická opatření

Slouží k ochraně dat a informací.

A.10.1.1 Politika pro použití kryptografických opatření

V ředitelně je umístěn server, který využívá již zmíněnou VPN, která šifruje online připojení. Dalším opatřením je využití elektronického podpisu ředitele školy pomocí tokenu. Na zasílání citlivých dokumentů je využívána datová schránka. A v neposlední řadě využívá ředitel školy v mzdové a personální oblasti (dále PaM) šifrování dokumentů v příloze e-mailů.

A.11 Fyzická bezpečnost a bezpečnost prostředí

V rámci ochrany dat a informací včetně zařízení, které je zpracovávají a uchovávají je, je fyzická bezpečnost nedílnou součástí jejich ochrany.

A.11.1 Bezpečné oblasti

Cílem této části je předcházení neautorizovaného fyzického přístupu, poškození a zásahů do informací a vybavení pro zpracování informací organizace.

11.1.1 Fyzický bezpečnostní perimetr

Tato část navazuje na stručnou charakteristiku objektu na začátku kapitoly. Pozemek je v jeho přední části zabezpečený laťkovým plotem, který již není ve vyhovujícím stavu. Součástí plotu jsou dvoje vrata vedoucí na pozemek, ty se na popud zřizovatele nezamykají z důvodu přítomnosti načiní pro obecní zaměstnance v garáži objektu. Ze stran pozemek sousedí s jinými pozemky a v zadní částí jsou louky a pole.

Hlavní vstup do budovy je zabezpečený acces control systémem (dále ACS). Kromě zvukového přenosu, slouží systém i k obrazovému přenosu podle kterého lze vpouštět osoby do objektu. K přístupu ACS je možné využít i aplikaci v mobilním telefonu. Tuto funkci zaměstnanci subjektu v současné době nevyužívají. Další dva vchody nejsou kromě možnosti zamykání nijak zabezpečeny.

Okna subjektu nedisponují žádným zabezpečením. Objekt nedisponuje prvky poplachového zabezpečovacího a tísňového systému (dále PZTS). Po škole jsou rozmístěny ruční hasicí zařízení podle zprávy o PO. Na střeše budovy se nachází hromosvod, anténa na internet a elektrická rotační siréna.

11.1.2 Fyzické kontroly vstupu

V subjektu není prováděn záznam či monitoring všech přístupů a výstupů do a z budovy např. ve formě čipů anebo karet. Všechny dveře do budovy jsou na klíče a pouze hlavní

vchod disponuje zvýšeným zabezpečením. ACS je obsluhován během provozu školy školní družinou (za oddělení ZŠ) a mateřskou školou, jejichž zaměstnanci jsou během provozu odpovědné za pohyb dalších anebo nepovolaných osob v budově. Zadní vchod je vedený jako evakuační a během činnosti školy musí být odemčen. Z obou stran je na dveřní kliku, není tedy zabezpečen proti vstupu nepovolané osoby v době činnosti školy. Boční vchod dostupný skrze rampu je během činnosti uzamčen, jeho účelem je zásobování kuchyně.

Doprovody dětí chodících do mateřské školy doprovázejí děti až do oddělení školky, které se nachází v prvním patře. Tyto doprovody se tak pohybují v celém prostoru budovy. Žáci chodící do základní školy vstupují do budovy bez doprovodu, případně jejich doprovody mají přístup v přízemí ke školní družině a šatně základní školy.

Další osoby vstupující do objektu musejí podléhat souhlasu ředitele školy. Může se jednat například o osoby provádějící kontrolu subjektu, ty se mohou po objektu pohybovat pouze se souhlasem ředitele školy a s jeho doprovodem. Doprovodem může případně ředitel školy určit odpovědného zaměstnance.

Přístupová práva se mění v souladu s pracovními smlouvami zaměstnanců a povinnostmi z ní vyplývající.

Obrázek 9 Access control systém (vlastní, 2022)

11.1.3 Zabezpečení kanceláří, místností a vybavení

Všechny místnosti v budově jsou na klíč. Neexistuje univerzální klíč. Přístup do všech místností má ředitel, školnice a zřizovatel. Klíče potřebné pro ostatní zaměstnance se nacházejí v ředitelně, někteří zaměstnanci mají kopie potřebných klíčů.

Ústřední místností subjektu je ředitelna, která obsahuje počítačové vybavení, server, administrativu ředitele a další převážně papírovou dokumentaci. Místnost disponuje tiskárnou s kopírkou, která je sdílená většinou zaměstnanců. Server subjektu je chráněn RACK skříní, obsahuje zároveň virtual private network (VPN), zálohy a náhradní zdroj napájení (UPS). Pohled do ředitelny je umožněn na Obrázku 10 Ředitelna školy. Ředitelna slouží i jako zázemí pro další zaměstnance, převážně učitelky ZŠ a školnici. Dokumentace ředitele je uložena v kancelářských skříních na univerzální klíč. Další dokumentace je pak uložena ve skladu/archivu. Do této místnosti je klíč uložený v ředitelně a během činnosti školy bývá odemčen, jelikož slouží i jako šatna pro zaměstnance a nachází se zde prostor pro občerstvení zaměstnanců (lednice a varná konvice).

Počítačově jsou vybaveny i všechny učebny, oddělení mateřské školy, školní družina a zaměstnanci mají také své pracovní notebooky.

Obrázek 10 Ředitelna (vlastní, 2021)

11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí

Před nepovolaným vniknutím cizí osoby chrání subjekt oplocení pozemku s umístěnými dvěma vraty a ACS umístěný na hlavních dveřích budovy. Budova nedisponuje prvky PZTS. Její patra jsou spojena pouze jedním schodištěm, chybí tedy úniková evakuační trasa. V budově školy se nachází ruční hasící zařízení rozmístěné podle zprávy o požární ochraně.

Objekt není umístěn v povodňovém území. Škola disponuje rotační sirénou, která by měla být podle revize funkční, ale nebyla odzkoušena po neznámou dobu.

Subjekt nakládá s jednou nebezpečnou látkou, konkrétně se jedná o oplachovač myčky, se kterým je nakládáno v prostředí kuchyně. Nádoba této látky je označena výstražnými symboly, je k ní vypracován bezpečnostní list a manipuluje s ní pouze jedna vyškolená osoba, kterou je školnice. Prázdný obal je svážen při svozu nebezpečného odpadu.

11.1.6 Oblasti pro nakládku a vykládku

Pro vykládku a nakládku zboží především potravinářského charakteru slouží boční vchod skrze rampu u kuchyně. Dveře jsou na klíč a převzetí zboží zajišťuje kuchařka anebo školnice. Odpad včetně nádoby od nebezpečné látky je vynášen vchodem ze sklepa a odvážen od hranic pozemku. Osoby zajišťující odvoz či přívoz materiálu nemají přístup do objektu, pouze na jeho pozemek, nemají přístup k vybavení zpracovávající informace, ani s ním nepřicházejí do kontaktu.

A.11.2 Zařízení.

Cílem obsahu o zařízení je předcházení ztrátě, krádeži nebo kompromitaci aktiv.

11.2.1 Umístění zařízení a jeho ochrana.

V přízemí je školní kuchyně vybavena kuchyňským náčiním značné finanční hodnoty. Do kuchyně jsou orientovány dva vstupy, jeden venkovní z rampy a druhý vnitřní z chodby. Klíče vlastní kuchařka, školnice, ředitelka a zřizovatel. Ve stejném patře ŠD obsahuje počítačové vybavení včetně tiskárny, dveře jsou zabezpečeny na klíč. Ten vlastní ředitelka, zřizovatel, školnice a družinářka.

Většina klíčového vybavení se však nachází v prvním patře, není tedy dostupné zrakem zvenku a veřejnost k němu nemá přístup. Podstatné vybavení se nachází v ředitelně školy, kde se jedná o server a zálohy, tiskárnu s kopírkou, počítač ředitele školy s dokovací stanicí a při činnosti školy i notebooky zaměstnanců. Ředitelna je po otevření dostupná všem zaměstnancům, přístup není nijak kontrolován. Klíč k ředitelně vlastní ředitelka a učitelky základní školy.

Učebny základní školy disponují počítačovým vybavením a dvě z nich i interaktivní tabulí. Klíče od jednotlivých učeben jsou uložené v ředitelně školy.

Počítačové vybavení obsahuje i oddělení mateřské školy, včetně interaktivní tabule a notebooků zaměstnanců. Oddělení je na klíč, který vlastní vedoucí MŠ, učitelky MŠ, a je umístěný i v ředitelně.

11.2.2 Podpůrné služby.

Subjekt není nijak chráněn před výpadkem elektrické energie, telekomunikace, vody a plynu. Pakliže dojde k výpadku některého z uvedených napájení dochází k omezení funkce objektu. V případě výpadku dodávek vody fungují místní dobrovolní hasiči, kteří mohou zabezpečit náhradní mobilní zdroj pitné vody. V případě výpadku elektrické energie je umístěn v RACK u serveru náhradní napájecí zdroj, který by zajistil řádné ukončení procesů spuštěných na hlavním počítači ředitele školy. Objekt nedisponuje nouzovým osvětlením ani komunikací. Budova má následující nouzové vypínače a ventily:

- hlavní uzávěr vody,
- hlavní uzávěr plynu,
- hlavní vypínač rozvodů.

11.2.3 Bezpečnost kabelových rozvodů.

Kabeláž není chráněna před odposloucháváním anebo rušením. Přívod elektřiny do budovy je v zemi. Kabely nejsou odděleny. Mimo zdi jsou kabely chráněny plastovými lištami. Přístup ke kabelovým systémům není nijak chráněn. V rámci technické prohlídky probíhají kontroly zařízení připojených ke kabelům.

11.2.4 Údržba zařízení.

V rámci detekce a signalizace závad probíhají v objektu pravidelné kontroly. Časové intervaly kontrol jsou dány zákony a vyhláškami. Jsou prováděny následující revize:

- revize budovy (např. včetně revize hromosvodu) – každých 5 let,
- plynu – 1 ročně,
- revize malých a přenosných elektrospotřebičů – 1 ročně,
- velká elektro revize – 1 ročně,
- PO (především kontrola hasících zařízení) – 1 ročně,
- tělocvičny a hřiště – 1 ročně,
- tabulí – jednou za 3 až 5 let,

- pravidelná prohlídka závad a provedení oprav – kontroluje a provádí školnice podle potřeby.

Údržba dalších zařízení (např. velký mixér ve školní kuchyni apod.) je prováděna podle potřeby, provádějí externí pracovníci.

Údržbu počítačového vybavení provádí externí IT zaměstnanec v případě potřeby.

11.2.5 Přemístění aktiv.

Každý zaměstnanec má svůj pracovní notebook, se kterým může pracovat i mimo objekt. Kromě ředitele školy nepracují většinou zaměstnanci s citlivými údaji, a hlavním účelem je příprava na výuku. Ředitel školy, pracující s důležitými daty může svůj notebook odebírat z dokovací stanice hlavního počítače a pracovat s ním i mimo objekt.

V rámci papírové dokumentace je zakázáno vynášení mimo prostory objektu. Výjimku tvoří pouze skutečnost kontroly probíhající mimo prostory objektu, na kterou se podklady musejí dovést. Dále je přemisťováno účetnictví kvůli přemístění k externímu zaměstnanci.

11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace.

Bezpečnost přenosného počítačového vybavení zaměstnanců je zajištěna přístupovými údaji, které nejsou sdílené. Hranice fyzické bezpečnosti si nastavují zaměstnanci sami. Bezpečnost papírové dokumentace není zajištěna, ředitel si sám nastaví její hranice.

11.2.7 Bezpečná likvidace nebo opakované použití zařízení.

Likvidace paměťových médií v subjektu zatím neproběhla. Užitá paměťová média se nacházejí v archivu školy. Ředitel školy používá elektronický podpis pomocí tokenu a jeho likvidace zatím nebyla potřeba.

11.2.8 Uživatelská zařízení bez obsluhy.

Ochranou aktuálně nepoužívaných zařízení je automatické přecházení do režimu spánku, tzn. blokovacího mechanismu a pro opětovný vstup vyžaduje přístupové údaje. Zaměstnanci mají své vlastní přístupové údaje. Počítače v učebnách jsou nastavené na univerzální přístupové údaje.

11.2.9 Zásada prázdného stolu a prázdné obrazovky.

Dokumenty s citlivými údaji by neměli zůstat bez dozoru na odkládací ploše. Tuto skutečnost nelze v současné době nijak kontrolovat.

Počítače jsou v nepřítomnosti zaměstnanců odhlášené.

A.15 Dodavatelské vztahy

Cílem je ochránit citlivá data a informace vstupující do dodavatelských vztahů.

Škola jako organizace spolupracuje s celou řadou dodavatelů mnoha oblastí. Z hlediska druhu zboží, služeb či jiných činností je můžeme dělit do následujících kategorií:

- správce informačních technologií,
- zpracování účetnictví a platů,
- právní pomoc,
- pojistka,
- služby bank,
- dodavatelé energií,
- revizní služby (revize budovy, plynu, elektro revize, revize požární ochrany, tělocvičny, hřiště, tabulí apod.),
- telekomunikační služby,
- pracovně lékařské služby (smlouva s lékařem ohledně pracovních prohlídek),
- dodavatelé potravin do školní kuchyně,
- dodavatelé učebních pomůcek a úklidového materiálu,
- odpady (smlouva s obcí, zbytky jídla – firma z Českých Budějovic).

V případě že dodavatelé nakládají s citlivými daty subjektu, je ve smlouvě stanovena doložka o mlčenlivosti. K takové skutečnosti dochází například u smluvního vztahu mezi subjektem a externím IT zaměstnancem anebo externí firmou zpracovávající účetnictví a platy.

4.2 Dílčí závěr kapitoly

Z charakteristiky objektu a řízení subjektu lze definovat rizikové oblasti, přičemž je podstatné zaměřit se na fyzický parametr. V rámci fyzické bezpečnosti nedochází k pravidelnému zabezpečování vrat vedoucích na pozemek, oplocení není ve vyhovujícím stavu, respektive nebylo by těžkou překážkou pro případného pachatele, zadní dveře a boční dveře jsou na klíč, s tím že i na jejich vnější straně je umístěná dveřní klika. Obecní byt situovaný v objektu nemá vlastní vchod, a tudíž mají nájemci přístup do prostor školy. Škola

se potýká s nedostatkem prostor a v důsledku toho musí být ředitelna obsahující klíčová aktiva sdílena více zaměstnanci. Kancelářské skříně se vyrábějí s univerzálním klíčem a neposkytují tak potřebnou ochranu důležité papírové dokumentaci. V subjektu neprobíhá řádná klasifikace informací a její důsledné označování. Ve škole není prováděno školení pro zaměstnance z oblasti kybernetické bezpečnosti ani bezpečnosti informací. Tato rizika a další jsou předmětem analýzy rizik obsažené v následující kapitole 5.

5 ANALÝZA RIZIK

Před samotnou analýzou rizik byla k identifikaci rizik zvolena metoda Ishikawův diagram. Diagram zobrazuje možné příčiny chyb a vad v řízení bezpečnosti vzdělávacího zařízení. Následně graficky a přehledně zaznamená rizikové faktory do skupin.

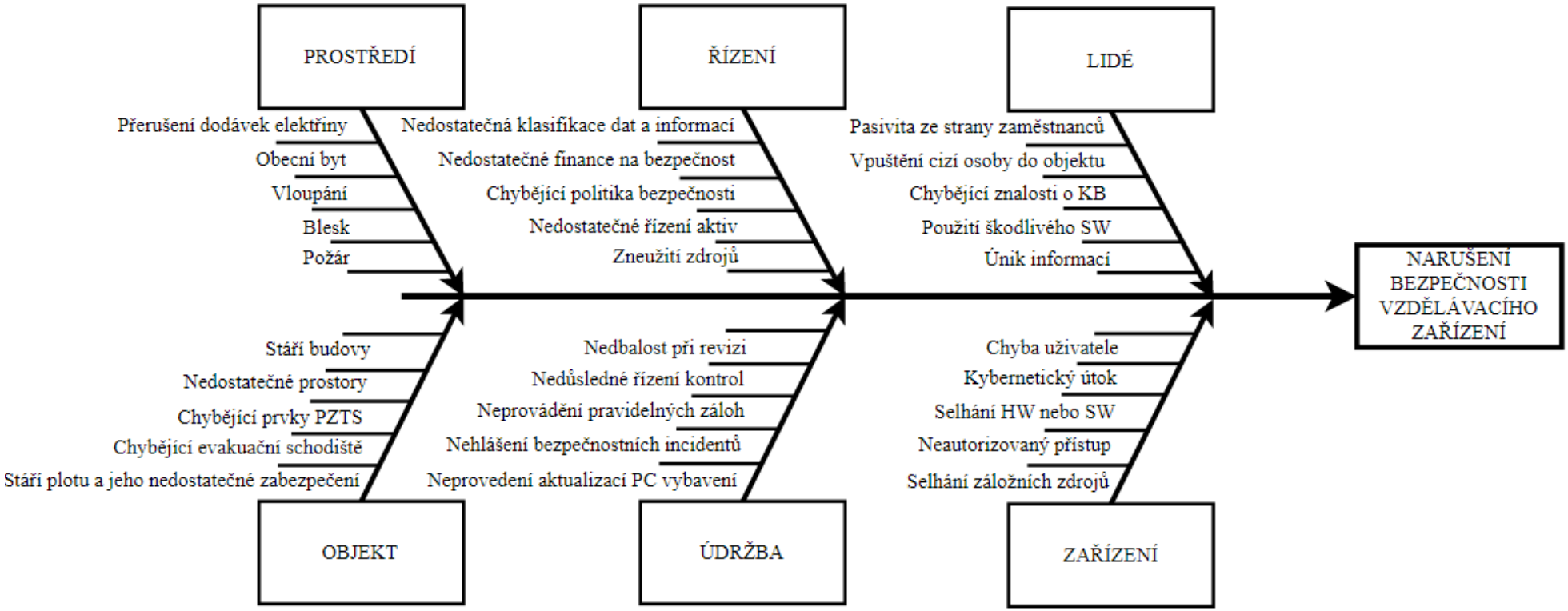
Pro samotnou analýzu rizik byla vybrána FMEA. Právě FMEA je v souvislosti s ISMS využívána v praxi. Jedná se o formulář kvantitativně analyzující současný stav, který ihned definuje konkrétní opatření a následně dochází k nové kvantifikaci rizika po případném zavedení opatření.

5.1 Ishikawa diagram

K identifikaci rizik došlo v rámci rozhovorů vedených s ředitelkou školy. Poznatky z těchto konzultací byly zaznamenány do diagramu, tzv. „rybí kosti“. Diagram byl rozdělen na následujících 6 oblastí:

- prostředí,
- řízení,
- lidé,
- objekt,
- údržba,
- zařízení.

V každé větvi bylo hledáno 5 rizik (příčin), které by mohly vést k následku – narušení bezpečnosti vzdělávacího zařízení. Výsledek je graficky zobrazen na následujícím Obrázku 11 Ishikawa diagram.



Obrázek 11 Ishikawa diagram (vlastní zpracování)

Shrnutí Ishikawa diagramu:

V oblasti prostředí bylo identifikováno přerušení dodávek elektrické energie, které může vést ke ztrátě dat. Obecní byt byl identifikován jako riziko, protože nájemníci sdílejí se školou vstupní prostory. Ke vloupání a krádeži došlo v objektu již dvakrát, a proto je důležité toto riziko do analýzy také zahrnout. Požár a blesk jsou obecná rizika, jejichž důsledky také mohou vést k narušení bezpečnosti zařízení.

V oblasti řízení neboli vedení může být rizikem nedostatečná klasifikace informací, která nevede k dodržování pravidel stanovených stupněm zařazení zaměstnance. Dále nedostatečné finance na řízení bezpečnosti, nedefinovaná politika bezpečnosti, absence řízení aktiv a možné zneužití zdrojů. Všechny tyto faktory mohou ovlivnit integritu, dostupnost a celistvost dat.

V oblasti lidé je rizikové pasivní chování zaměstnanců, kteří nejsou ochotni se podílet na činnostech a procesech organizace. Lidé jsou nejslabším článkem, proto jejich chování může vést k chybě, která může být příčinou vpuštění cizí osoby do objektu, úniku informací nebo infikování PC malwarem. V subjektu neprobíhá školení zaměstnanců v oblasti kybernetické bezpečnosti a bezpečnosti informací, proto mohou být zaměstnanci snadným cílem pachatele.

Objektem školy je 100 let stará budova, ve které neproběhla žádná rozsáhlá rekonstrukce týkající se například elektrických rozvodů a kabelů. Jejich narušení nebo poškození může vést k ohrožení zařízení a ztrátě dat. Škola se potýká i s problematikou fyzického zabezpečení objektu. Nejsou zde instalovány žádné prvky PZTS a vrata vedoucí na pozemek se nezamykají, takže netvoří žádnou mechanickou překážku pro pachatele. A v neposlední řadě je důležité zmínit nedostatečné prostory. Ředitelna je sdílena více zaměstnanci, to může představovat riziko. Budově dále chybí evakuační schodiště.

Při údržbě může dojít k nedbalosti v rámci revizí, kontrol a zálohování dat. Riziko by mohl představovat i nenahlášený bezpečnostní incident, který se podcení a vyústí právě v narušení bezpečnosti.

Při práci se zařízeními a v online prostředí může dojít k chybě uživatele, kybernetickému útoku. V rámci problematiky týkající se zařízení může dále nastat selhání HW nebo SW, může dojít k neautorizovanému přístupu anebo selhání záložních zdrojů.

5.2 FMEA

Metoda analýzy rizik FMEA je zpracována pomocí formuláře, který je rozdělený na dvě hlavní části:

- analýzu současného stavu a hodnocení,
- návrhy opatření s hodnocením po případné realizaci opatření.

Jedná se o kvantitativní metodu, která pracuje s výpočtem rizikového čísla (RPN) pomocí kritérií závažnosti, výskytu a odhalení chyby. Stupnice jednotlivých kritérií jsou stanoveny v následujících tabulkách. Následuje Tabulka 4 Kritéria závažnosti chyby.

Tabulka 4 Kritéria závažnosti chyby

KRITÉRIUM ZÁVAŽNOSTI CHYBY (Z)		OHODNOCENÍ
Zanedbatelná	Chyba nevede ke znatelnému problému, důsledku.	1
Nízká	Chyba vede ke snadno řešitelným problémům vstupujících do chodů školního zařízení.	2-3
Střední	Chyba vyžadující pozornost a řešení problému.	4-6
Vysoká	Chyba ohrožující funkčnost a bezpečnost školního zařízení a vyžaduje řešení ze strany vedení.	7-8
Velmi vysoká	Chyba ovlivňující bezpečnost vzdělávacího zařízení a vyžaduje zapojení zájmových skupin.	9-10

Následuje Tabulka 5 Kritéria výskytu chyby.

Tabulka 5 Kritéria výskytu chyby

KRITÉRIUM VÝSKYTU CHYBY (V)		OHODNOCENÍ
Velmi nízká	Zanedbatelná pravděpodobnost výskytu chyby.	1
Nízká	Nepravděpodobný výskyt chyby.	2-3
Střední	Průměrná pravděpodobnost výskytu chyby.	4-6
Vysoká	Vysoká pravděpodobnost výskytu chyby.	7-8
Velmi vysoká	Velmi vysoká pravděpodobnost výskytu chyby.	9-10

Následuje Tabulka 6 Kritéria odhalení chyby.

Tabulka 6 Kritéria odhalení chyby

KRITÉRIUM ODHALENÍ CHYBY (O)		OHODNOCENÍ
Velmi vysoká	Snadno odhalitelná chyba.	1
Vysoká	Odhalitelná chyba ředitelem, zaměstnancem.	2-3
Střední	Odhalitelná chyba při údržbě systému anebo provozu školního zařízení externím IT zaměstnancem nebo jiným odborníkem.	4-6
Nízká	Chyba odhalitelná pouze v případě kontroly, revize.	7-8
Velmi nízká	Těžko odhalitelná chyba.	9-10

FMEA výsledným výpočtem rizikového čísla (RPN) určuje míru rizika. Výpočtem se rozumí součin jednotlivých kritérií:

$$\mathbf{RPN = Z \times V \times O.}$$

Míra rizika včetně rozsahu byla stanovena v následující Tabulce 7 Klasifikace RPN.

Tabulka 7 Klasifikace RPN

KLASIFIKACE RPN	
Nízké riziko	0-200
Střední riziko	201-600
Vysoké riziko	601-1000

Zpracovaný formulář FMEA je uveden v rámci následující Tabulky 8 Formulář FMEA.

Tabulka 8 Formulář FMEA

OBJEKT: ZŠ A MŠ NOVOSEDLY NAD NEŽÁRKOU										**ČÍSLO: 1**					
ODPOVĚDNOST ZA VYPRACOVÁNÍ: BC. PROKEŠOVÁ ANNA										**ROK: 2022**					
FMEA – ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Prvek	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (preventiv-ní opatření)**	**Řízení procesu vedoucí k odhalení chyby**	**Odhalení (O)**	**RPN**	**Doporučená opatření**	**Odpovědnost**	**Závažnost (Z)**	**Výskyt (V)**	**Odhalení (O)**	**RPN**
Živelní a fyzikální hrozby	Požár	Poškození anebo ztráta aktiv	10	Nedbalost na pracovišti, úmyslné založení, zkrat el. sítě	5	Hasicí přístroje, požární směrnice	3členná požární hlídka dle požární směrnice	2	100	Prvky PZTS – hlásiče požáru, detektory kouře a teploty	Zřizovatel	10	5	1	50
	Výpadek el. energie	Ztráta dat Poškození zařízení	9	Meteorologi-cká situace (bouřka, vichřice, sníh), elektromagn etické impulsy (EMP)	8	UPS, pravidelné zálohování	Žádné	8	576	Instalace motor-generátoru, systém těsnění – elektromagn etické stínění	Zřizovatel	9	8	3	216

OBJEKT: ZŠ A MŠ NOVOSEDLY NAD NEŽÁRKOU										**ČÍSLO: 1**					
ODPOVĚDNOST ZA VYPRACOVÁNÍ: BC. PROKEŠOVÁ ANNA										**ROK: 2022**					
FMEA – ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Prvek	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (preventiv-ní opatření)**	**Řízení procesu vedoucí k odhalení chyby**	**Odhalení (O)**	**RPN**	**Doporučená opatření**	**Odpovědnost**	**Závažnost (Z)**	**Výskyt (V)**	**Odhalení (O)**	**RPN**
Technolog. hrozby	Zkratování el. sítě/zařízení v el. síti	Poškození HW	10	Přepětí v síti, poškození izolace přívodních nebo vnitřních vodičů/staré rozvody, jističe	7	Jističe, pravidelné elektro revize 1x ročně, zálohy, UPS, hasící zařízení	Nařízení vlády č. 101/2005 Sb. o podrob. požadav. na pracoviště a pracovní prostředí	5	350	Modernizace jističů a kabelových rozvodů, prvky PZTS	Zřizovatel	10	4	3	120
		Ztráta dat													
		Požár													
		Porušení kabelových rozvodů													
	Selhání HW nebo SW	Nefunkčnost PC	8	Životnost komponent, přehřátí serveru, použití škodlivého SW	7	Zálohování dat	Údržba zařízení IT pracovní-kem	6	336	Chladící zařízení serveru, pravidelná údržba, školení o KB	Externí IT pracovník	8	3	3	72
		Nedostupnost dat													
		Selhání záložních zdrojů													

OBJEKT: ZŠ A MŠ NOVOSEDLY NAD NEŽÁRKOU										**ČÍSLO: 1**					
ODPOVĚDNOST ZA VYPRACOVÁNÍ: BC. PROKEŠOVÁ ANNA										**ROK: 2022**					
FMEA – ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Prvek	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (preventiv-ní opatření)**	**Řízení procesu vedoucí k odhalení chyby**	**Odhalení (O)**	**RPN**	**Doporučená opatření**	**Odpovědnost**	**Závažnost (Z)**	**Výskyt (V)**	**Odhalení (O)**	**RPN**
Technolog. hrozby	Únik plynu	Požár Zdravotní nebezpečí	10	Stáří budovy (zastaralé vedení plynu a uzávěr), nedbalost	3	Žádné	Revize plynu 1x ročně	7	210	Detektor úniku plynu	Zřizovatel	10	3	1	30
	Absence prvků PZTS	Narušení bezpečnosti	9	Nízký rozpočet na bezpečnost	10	Hasící přístroje, hlídka PO, mecha-nické zábranné prostředky	Žádné	8	720	Instalace prvků PZTS, využití dotací	Zřizovatel	1	3	1	3

OBJEKT: ZŠ A MŠ NOVOSEDLY NAD NEŽÁRKOU										ČÍSLO: 1					
ODPOVĚDNOST ZA VYPRACOVÁNÍ: BC. PROKEŠOVÁ ANNA										ROK: 2022					
FMEA – ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ			
Prvek	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (preventiv-ní opatření)**	**Řízení procesu vedoucí k odhalení chyby**	**Odhalení (O)**	**RPN**	**Doporučená opatření**	**Odpovědnost**	**Závažnost (Z)**	**Výskyt (V)**	**Odhalení (O)**	**RPN**
Hrozby způsobené uživatelem při používání aktiv	Neautorizovaný přístup	Infikování PC škodlivým SW, ztráta/únik dat a informací	9	Neškolený anebo pasivní uživatel, neoprávněná osoba, víceúčelová ředitelna, obecní byt	9	Antivirový program ESET	Žádné	10	810	Spouštění antivirového testu programu ESET, školení kybernetické bezpečnosti,	Zaměstnanci	9	4	8	288
	Instalace neoriginálního SW														
	Chyba uživatele														
	Neoprávněná manipulace s daty	Infikování PC škodlivým SW, ztráta/únik dat a informací	10		8	Žádné	Žádné	10	800	Vhodná klasifikace dat a zabezpečení	Ředitel školy	10	6	7	420
	Neprovádění aktualizací SW									Školení o KB	Externí IT zaměstnanec, zaměstnanci				

OBJEKT: ZŠ A MŠ NOVOSEDLY NAD NEŽÁRKOU										**ČÍSLO: 1**					
ODPOVĚDNOST ZA VYPRACOVÁNÍ: BC. PROKEŠOVÁ ANNA										**ROK: 2022**					
FMEA – ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Prvek	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (preventiv-ní opatření)**	**Řízení procesu vedoucí k odhalení chyby**	**Odhalení (O)**	**RPN**	**Doporučená opatření**	**Odpovědnost**	**Závažnost (Z)**	**Výskyt (V)**	**Odhalení (O)**	**RPN**
Hrozby způsobené uživatelem při používání aktiv	Porušení zásady čistého stolu/obrazovky		5		9	Uzamčení zařízení při nečinnosti	Žádné	9	405	Vytvoření prostor pro samostatnou ředitelnu, nastavení přístupu	Ředitel školy	5	2	6	60
	Nenahlášení bezpečnostního incidentu	Narušení bezpečnosti zařízení	6	Pasivita zaměstnanců / nedbalost	3	Žádné	Žádné	9	162	Vedení evidence bezpeč-nostních incidentů	Ředitel školy	6	1	7	42
Úmyslně způsobené hrozby	Narušení fyzické bezpečnosti objektu	Zcizení anebo poškození zařízení Ztráta financí Únik anebo poškození dat	9	Neoprávně-né vniknutí do objektu, loupež, absence prvků PZTS	8	Plot, dveře se zámkem, ACS u hlavních dveří	Žádné	10	720	Prvky PZTS – detektory, kontrola vstupu – např. čipy, prvky VDS	Zřizovatel	9	8	1	72

OBJEKT: ZŠ A MŠ NOVOSEDLY NAD NEŽÁRKOU										**ČÍSLO: 1**					
ODPOVĚDNOST ZA VYPRACOVÁNÍ: BC. PROKEŠOVÁ ANNA										**ROK: 2022**					
FMEA – ANALÝZA SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Prvek	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (preventiv-ní opatření)**	**Řízení procesu vedoucí k odhalení chyby**	**Odhalení (O)**	**RPN**	**Doporučená opatření**	**Odpovědnost**	**Závažnost (Z)**	**Výskyt (V)**	**Odhalení (O)**	**RPN**
Úmyslně způsobené hrozby	Kybernetický útok	Ztráta/ únik dat Zašifrování dat Napadení elektronického bankovnictví	10	Kyberne-tický útok	9	Antivirový program ESET, údržba IT zařízení externím pracov-níkem	Nastavení firewallu	9	810	Školení zaměstnanců v oblasti kybernetické bezpečnosti	Ředitel školy, zaměstnanec	10	9	5	450

Vyhodnocení FMEA:

Nejrizikovějšími oblastmi jsou podle výpočtů RPN hrozby způsobené uživatelem, úmyslně způsobené hrozby včetně související hrozby nedostatečného fyzického zabezpečení:

- Kybernetický útok – jde o úmyslnou hrozbu, kterou nelze ve velké míře ovlivnit, znalostmi zaměstnanců o kybernetické bezpečnosti však lze eliminovat potencionální následky útoku. Proto je doporučené zavedení školení o KB pro zaměstnance školy a z důvodu šíření povědomí byla pro ně vytvořena příručka vztahující se k dané problematice umístěná v přílohové části práce.
- Hrozby způsobené uživatelem – neautorizovanému přístupu a neoprávněné manipulaci s daty lze předejít zavedením klasifikace dat a informací. Instalaci neoriginálního SW a chybě uživatele lze předejít školením a zvyšováním povědomí o kybernetické bezpečnosti. Těmto hrozbám lze předcházet rozvíjením znalostí o dané problematice. Toho je dosaženo v praktické části vytvořením interního dokumentu pro potřeby vedení a následně příručky dostupné pro všechny zaměstnance.
- Rizika spojená s fyzickou bezpečností – hrozby v této oblasti lze minimalizovat instalací prvků PZTS. Fyzická bezpečnost je důležitá pro ochranu zařízení a dalších aktiv. Proto jsou prvky na ochranu fyzického perimetru mimo jiné blíže rozebrány v následující kapitole 6 Návrh opatření.

6 NÁVRH OPATŘENÍ

Hlavním návrhem na zlepšení současného stavu je zavedení bezpečnostní dokumentace, která upraví zásady a pravidla pro dodržování bezpečnostních principů v subjektu, a která jsou zaměřená na systém řízení bezpečnosti informací. V rámci subjektu je důležitý komplexní přístup k bezpečnosti včetně ochrany fyzického perimetru.

Návrhy opatření se dále primárně zaměřují na ochranu zařízení s čímž souvisí právě i ochrana objektu před neoprávněným vniknutím cizí osoby. Aby bylo dosaženo určité úrovně zabezpečení je nutné začít od základních drobných návrhů ke zlepšení současného stavu. K ochraně subjektu patří i plot vedoucí po přední straně pozemku, který již není ve vyhovujícím stavu, proto by měl být rekonstruován a spolu s tím by měla být zabezpečena i dvoje vrata, která jsou jeho součástí a doposud se nezamykají. Další možnou stavební úpravou je doporučení vytvoření samostatného vchodu pro obecní byt, tak aby jeho obyvatelé nesdílely vstupní prostory školy.

Dalším opatřením souvisejícím s ochranou dat a informací včetně zařízení by bylo osamostatnění prostor ředitelny. Jejíž součástí by byl i archiv citlivých dat v papírové podobě. Toto opatření by však představovalo zrušení zázemí pro učitelky oddělení ZŠ. Jinou variantou je definování přístupu do místnosti. V případě provádění činností ředitele školy by nemuseli mít zaměstnanci do místnosti přístup. Tento způsob opatření je začleněný do příručky pro zaměstnance.

Důležitým opatřením pro bezpečný pohyb v kyberprostoru je zavedení povinného školení o kybernetické bezpečnosti. Taková školení jsou vytvořená Národním úřadem pro kybernetickou bezpečnost a zdarma dostupná na jejich webových stránkách.

Prvky PZTS

S přihlédnutím ke skutečnostem, že subjekt byl již dvakrát v minulosti vykraden, je důležité implementovat prvky PZTS, které by byly schopné zachytit vniknutí nepovolané osoby do prostředí subjektu. Základem při implementaci prvků PZTS je instalace ústředny, ve které dochází ke spojení všech prvků PZTS. Ústředna bývá napojena i na mobilní aplikaci, ve které lze ovládat všechny prvky. Ústřednu je vhodné instalovat do míst, kam nemá přístup veřejnost. Z tohoto důvodu je doporučeno instalovat ústřednu do prostor ředitelny, jakožto centra školy.

V rámci plášťové ochrany je doporučená instalace magnetických kontaktů. Tyto kontakty jsou vhodné implementovat na okna a dveře suterénu a přízemí. Toto určení vychází z pravidla, že terén je brán jako nultý bod a od něj prahové a parapetové úrovně do 2,5 metrů jsou rizikové. Následující Obrázek 12 Magnetický kontakt zobrazuje povrchový samolepící magnetický kontakt, který je vhodný například i na umístění plechových dveří, které vedou zvenku do sklepních prostor.

Obrázek 12 Magnetický kontakt (VAR-TEC FM-102 - 0701-046, 2022)

Zezadu budovy jsou zadní („zahradní“) dveře, které v době činnosti subjektu musejí být odemčené, protože jsou stanoveny jako evakuační. Základním opatřením by mohla být instalace dveřní koule místo kliky zvenčí dveří. Konkrétnějším opatřením pro zvýšení bezpečnosti by bylo zavedení čipů a tím i vymezení práv přístupu. Otevírání dveří na čip by bylo vhodné na přední hlavní dveře k doplnění ACS, zadní dveře, ale i na boční dveře vedoucí do školní jídelny s omezeným přístupem. Příkladem může být pořízení přístupového systému. Systém obsahuje řídící jednotku, stěnové čtečky, čtečku pro zadávání nových čipů do systému, software a hardwarový klíč. Pořízení takového systému však může pro subjekt představovat vyšší finanční zatížený. Výhodou tohoto systému je řízení vstupu do objektu. Příklad přístupové jednotky je zobrazen na Obrázku 13 Přístupový systém MPS.

Obrázek 13 Přístupový systém MPS (Přístupový systém MPS, 2022)

Jedním ze základních prvků pro vnitřní detekci je instalace pohybových PIR – detektorů pohybu. V rámci subjektu je vhodná instalace těchto detektorů prostorové ochrany i v kombinaci s detektorem tříštění skla plášťové ochrany. A to z důvodu velkého množství oken a dveří se skleněnými plochami. Kombinovaný detektor je zobrazen na Obrázku 14 Detektor pohybu osob a rozbití skla.

Obrázek 14 Detektor pohybu osob a rozbití skla (JA-120PB Sběrnicový detektor pohybu osob a rozbití skla - Jablotron, b.r.)

Prvky VDS

Problematika kamerového systému je složitá a musí se brát v potaz hodně faktorů. Je třeba myslet na náklady spojené s pořízením systému, jeho instalací a údržbou. Dále je nutné myslet na právní dokumentaci týkající se GDPR tedy ochrany osobních údajů, označení snímaných prostor, stanovení pravidel pro využívání systému a archivaci sbíraných dat. V rámci subjektu by mohla fungovat jedna otočná IP kamera umístěna v přízemí. IP kamery mají tu výhodu, že mohou sloužit samostatně, jsou napojeny do sítě, zaznamenávají i audio a záznam odesílají do uložiště. Problematika instalace kamer byla zkonzultována s odborníkem na instalaci kamerových systémů Bc. Dušanem Kučeříkem. Právě uložiště bývá problematickou částí kamerových systémů, protože při vlastnictví kamer s kvalitnějším obrazem zabírá záznam velkou kapacitu, což může být pro subjekt finančně nákladné. Jako náhradní a jednodušší řešení lze využít kamery s méně kvalitním obrazem, ale při potencionálním dokazování bezpečnostního incidentu nebudou nekvalitní záběry relevantní. Po zmíněné konzultaci se instalace kamerového systému prozatím subjektu nedoporučuje.

Plán případné instalace prvků PZTS je součástí interního bezpečnostního dokumentu.

7 NÁVRH BEZPEČNOSTNÍ DOKUMENTACE

Tato kapitola se zabývá vytvořením interního bezpečnostního dokumentu pro vybrané školské zařízení ke zvýšení kybernetické bezpečnosti a zabezpečení ISMS. Bezpečnostní dokument je soubor doporučení a obecných pravidel, jeho struktura vychází z norem řady ISO/IEC 27 000 a cílem je vytvoření bezpečnostní politiky se zaměřením na řešenou problematiku a dlouhodobé zlepšování této oblasti. Dokument necílí na striktní zavedení uvedené normy a její následnou certifikaci, ale pouze na zavedení principů z ní vycházejících.

Interní dokument je určený do rukou vedení školy a zřizovatele. Z důvodu výsledků analýzy rizik FMEA však byla do přílohové části přidána příručka pro všechny zaměstnance k šíření povědomí o této problematice a k implementaci určitých zásad a pravidel skrze celou organizaci.

Při zpracovávání bylo využito i Minimálního bezpečnostního standardu verze 1.0, vydaného NÚKIB pro organizace nespadající pod zákon o kybernetické bezpečnosti.

Tabulka 9 Hlavička bezpečnostního dokumentu

ZÁKLADNÍ ŠKOLA A MATEŘSKÁ ŠKOLA NOVOSEDLY NAD NEŽÁRKOU Novosedly nad Nežárkou 112, 378 17, skola@zsnovosedlynn.cz	
Interní bezpečnostní dokument v oblasti kybernetické bezpečnosti a ISMS	
Vypracoval: Bc. Anna Prokešová	
Schválil:	
Platnost od: projednání	Platnost do: odvolání

Východiska a cíle dokumentu

Dokument vychází z mezinárodních norem řady ISO/IEC 27 000, jejichž implementace je pro organizace dobrovolná, nicméně vzhledem k modernizaci i v oblasti školství dochází k potřebám ochrany aktiv oblasti informační i kybernetické více než kdy dřív. Dokument normu striktně nezavádí ani není podkladem k certifikaci. Dalším východiskem je Minimální bezpečnostní standard verze 1.0 Národního úřadu pro kybernetickou bezpečnost (dále jen NÚKIB).

Dokument nastavuje základní pravidla bezpečnostní politiky školy a stanovuje efektivní systém ke zvýšení nejen kybernetické bezpečnosti, ale i bezpečnosti organizační a ISMS. Cílem je vytvoření interních pravidel pro vedení školy a její zaměstnance k bezpečnému fungování celé organizace nejen na administrativní a organizační úrovni.

Základní předpoklady

Osoba odpovědná za bezpečnost školy je ředitel, který je zároveň administrátorem SW. Ředitel školy dbá na řízení kybernetické bezpečnosti a na její rozvoj. Na odpovědnosti za kybernetickou bezpečnost se dále podílí externí IT zaměstnanec, který je odpovědný za údržbu, stav a bezpečnost zařízení. Případné nedostatky anebo incidenty ihned komunikuje s ředitelem školy.

Řízení lidských zdrojů

Pro všechny zaměstnance školy je nařízeno absolvování on-line kurzů „*Dávej kyber*“ a „*Bezpečně v kyber*“. Tyto kurzy jsou volně dostupné na stránkách NÚKIB na následujícím odkaze:

https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/verejnost/.

Své absolvování kurzů zaměstnanci doloží vystaveným certifikátem s jejich jménem, které odešlou do rukou ředitele školy.

Zaměstnanci dále musejí být seznámení s bezpečnostními pravidly vyplývajícími z tohoto dokumentu formou školení. Jejich rozsah stanový ředitel školy. Zároveň je třeba školení periodicky opakovat. Četnost opakování stanový ředitel školy.

Zaměstnanci jsou povinni oznamovat případné bezpečnostní incidenty řediteli školy, případně i externímu zaměstnanci IT, kteří následně situaci vyhodnotí a stanoví další postup.

Při vybírání nových zaměstnanců jsou vyžadovány výpisy z rejstříků trestů, dále reference z minulých praxí. Povinnost absolvování kurzů kybernetické bezpečnosti se vztahuje i na nové zaměstnance, kteří se školení podrobí co nejdříve po nástupu do zaměstnání. Zaměstnanci dále podstupují i zdravotní prohlídky a školení BOZP.

Součástí pracovní smlouvy je doložka o mlčenlivosti.

Zaměstnanci jsou poučeni o náplních své práce a svých rolích v zařazení v rámci organizace a jednají v souladu s tím. Zaměstnanci jednají v souladu s tímto pokynem a dalšími směrnicemi a pokyny vydanými ředitelem školy.

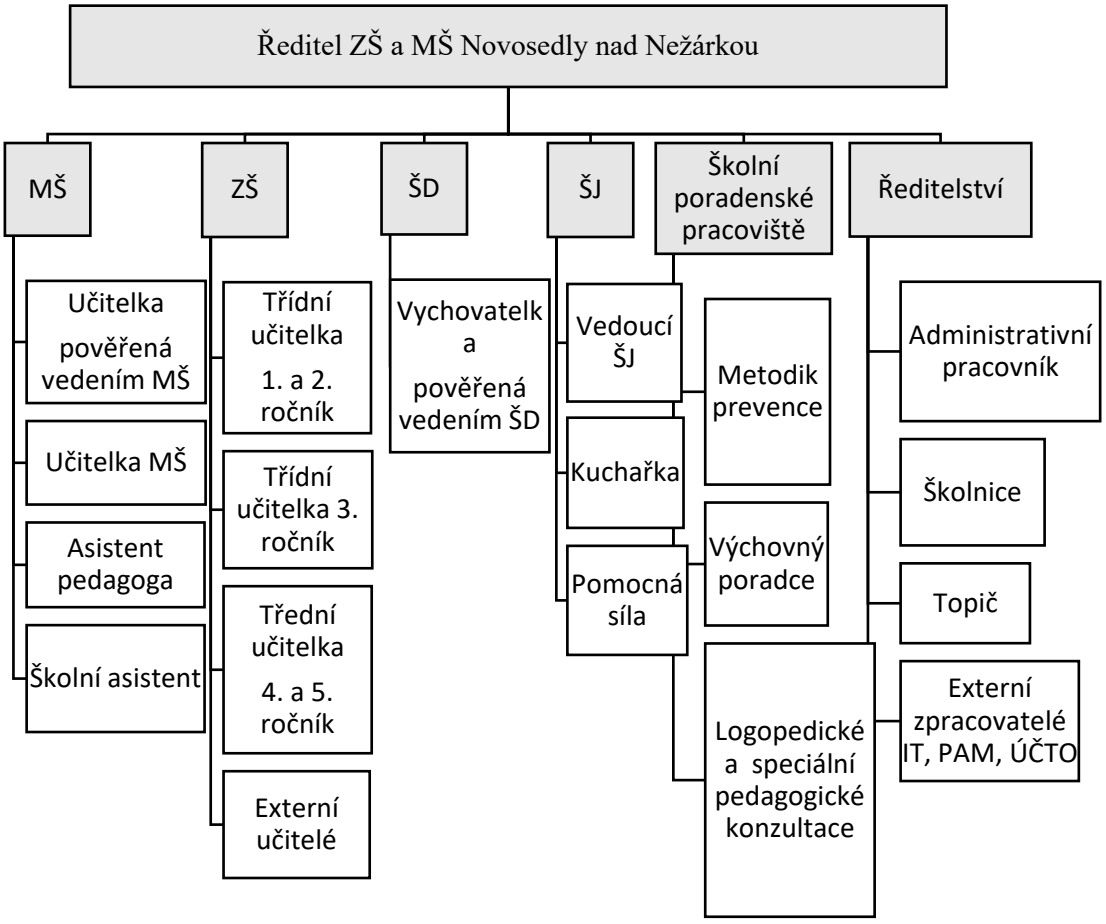
Řízení dodavatelů

Škola disponuje širokou sítí externích dodavatelů z různých oborů. Pro zachování bezpečnosti informací je důležité zohlednit ve smlouvách u dodavatelů, kde je relevantní zachování důvěrnosti, integrity a dostupnosti dat, doložku o mlčenlivosti.

Externí zpracovatelé IT, PaM a ÚČTO mají ve smlouvě doložku o mlčenlivosti., která má cílit na ochranu interních informací subjektu. Ve smlouvě s nimi jsou uvedené i informace o způsobu předávání dat mezi smluvními stranami. Externí zpracovatelé mají za povinnost podle smlouvy neprodleně upozornit subjekt v případě narušení bezpečnosti na jejich straně.

Organizační struktura

Na následujícím Obrázku 15 je definována organizační struktura školy.



Obrázek 15 Organizační struktura (vlastní)

Řízení aktiv

Aktivem se rozumí vše, co má pro organizaci hodnotu. Aktiva musejí být chráněna, proto je důležitá jejich identifikace a následný proces řízení. Aktiva školy jsou přehledně rozdělena do tabulek. Jsou rozlišena aktiva primární a podpůrná.

Jako primární aktiva byly určeny činnosti, procesy a informace, které jsou zásadní pro chod organizace. Jsou to aktiva vztahující se k činnostem souvisejících s citlivými daty a jejichž ztráta anebo omezení by znamenala narušení chodu subjektu. Jejich seznam je sestaven v následující Tabulce 10 Primární aktiva – činnosti a procesy.

Tabulka 10 Primární aktiva – činnosti a procesy

ŘEDITEL ŠKOLY (STATUTÁRNÍ ZASTOUPENÍ)
Vedení pedagogické dokumentace
Vedení ekonomické dokumentace
Vedení personální dokumentace
Vedení mzdové dokumentace
Vedení bezpečnostní dokumentace (BOZP a PO apod.)
Plánování, čerpání a vyhodnocování rozpočtu
Zúčtování se státním rozpočtem
Správa a vedení bankovních účtů subjektu
Platba faktur
Správa majetku
Inventarizace ZŠ
Řízení oddělení MŠ
Řízení oddělení ZŠ
Řízení oddělení ŠD
Řízení oddělení ŠJ
Vydávání vysvědčení
Správa datové schránky

Správa elektronických systémů
Správa smluvních vztahů
Komunikace a správa dokumentace zdravotních pojišťoven
Komunikace a správa Okresní správy sociálního zabezpečení
Plánování oprav
Vlastnictví podpisových práv
Vedení poradenského pracoviště
Provádění činnosti výchovného poradce
UČITEL 2
Provádění činnosti v oblasti prevence
UČITEL 3
Vedení pokladny
Správa nad pokladní hotovostí
VEDOUCÍ UČITELKA MŠ
Inventarizace MŠ
Vedení matriky MŠ v papírové podobě
VEDOUCÍ ŠJ
Inventarizace ŠJ
Správa softwaru VIS Plzeň
Správa SIPA v rámci stravného
Vlastnictví podpisových práv
ŠKOLNICE
Správa předávání klíčů
Správa fotodokumentace
Správa webových stránek

EXTERNÍ FIRMY
Zpracování účetnictví
Zpracování PAM a platy
EXTERNÍ IT ZAMĚSTNANEC
Správa zařízení včetně serveru a SW
Správa záloh

Mezi primární aktiva byly zařazeny i informace, se kterými se nakládá v rámci definovaných činností. Jedná se o citlivé údaje, které je potřeba adekvátně chránit.

Tabulka 11 Primární aktiva – informace

LIDSKÉ ZDROJE	
Osobní údaje zaměstnanců	Jméno a příjmení
	Rodné číslo
	Kontaktní informace
	Pracovní zařazení
	Lékařské údaje
	Výše platů
	Osobní ohodnocení
DĚTI, ŽÁCI A RODIČE	
Osobní a neveřejné údaje	Jméno a příjmení
	Rodné číslo dětí a žáků
	Datum narození
	Kontaktní informace
	Záznamy z matriky
	Hodnocení
Citlivé osobní údaje	Lékařské zprávy

OBJEKT	
Revize	
Soupis majetku	
Odpisy	
Plány	
IT ZAŘÍZENÍ	
HW vybavení	
Nastavení	
Hesla	
FINANCE	
Kniha faktur	
Pokladna	
Rozvaha	
Výpisy z účtu	
Rozpočet	
Účetnictví	
PAM	
DOKUMENTACE	
Ředitelství	Smlouvy s dodavateli
	Smlouvy s externími zaměstnanci
	Záznamy z jednání zastupitelstva
	Záznamy komunikace se zřizovatelem

Ředitelství	Dokumentace správních řízení
	Dokumentace pedagogická
	Dokumentace ekonomická
	Dokumentace mzdová
	Dokumentace personální
	Bezpečností dokumentace
Oddělení ZŠ	Archiv ZŠ
	Kroniky ZŠ
	Žákovské knížky
	Třídní knihy
	Fotodokumentace ZŠ
Oddělení MŠ	Fotodokumentace MŠ
	Kronika MŠ
	Archiv MŠ
	Matrika MŠ – papírová podoba
Oddělení ŠD	Dokumentace účastníků družiny
	Školní knihovna

Mezi podpůrná aktiva lze zařadit hardware, software, zaměstnance, prostředí a objekt. Podpůrná aktiva jsou definována v následující Tabulce 12 Podpůrná aktiva.

Tabulka 12 Podpůrná aktiva

DRUH AKTIVA	AKTIVUM	ODPOVĚDNOST/VLASTNÍK
ŘEDITELSTVÍ		
Pevné zařízení	Dokovací stanice	Ředitel školy/škola
	RACK: server, zálohy a náhradní napájecí zdroj	Ředitel školy/škola
	Tiskárna + kopírka	Ředitel školy/škola
	Telefon – pevná linka	Ředitel školy/škola
Přenosná zařízení	Notebook	Ředitel školy/škola
	Skartovačka	Ředitel školy/škola
Elektronické nosiče	USB token – elektronický podpis	Ředitel školy/škola
	USB flash disk	Ředitel školy/škola
	Externí disk	Ředitel školy/škola
Procesní periferie	Monitor	Ředitel školy/škola
	Reproduktor	Ředitel školy/škola
	PC klávesnice a myš	Ředitel školy/škola
	WiFi zařízení	Ředitel školy/škola
Operační systém	Microsoft Windows	Externí IT zaměstnanec/škola
SW a online databáze a systémy	Antivirový SW ESET	Externí IT zaměstnanec/škola
	E-mail školy	Ředitel školy/škola
	Datové schránky	Ředitel školy/škola
	Elektronické bankovnictví 1	Ředitel školy/škola
	Elektronické bankovnictví 2	Ředitel školy/škola

SW a online databáze a systémy	Matrika školy – elektronická podoba	Ředitel školy/škola
	Teams administrátor	Ředitel školy/škola
	Webové stránky	Ředitel školy/škola
	MŠMT UIV výkazy – internetová stránka	Ředitel školy/škola
	ČSÚ přístup	Ředitel školy/škola
	PAM přístup	Ředitel školy/škola
	Inventarizace ZŠ	Ředitel školy/škola
Aktiva v papírové podobě	Matrika školy v papírové podobě	Ředitel školy/škola
	Kniha faktur	Ředitel školy/škola
Ostatní	Razítka organizace	Ředitel školy/škola
ODDĚLENÍ ZŠ		
Pevná zařízení	Interaktivní tabule + dataprojektor	Učitelka 1/škola
	Interaktivní tabule + dataprojektor	Učitelka 2/škola
	Školní PC 6x	Učitelka 1/škola
	Školní PC 6x	Učitelka 2/škola
	Školní PC 3x	Učitelka 3/škola
Přenosná zařízení	Notebook	Učitelka 1/škola
	Notebook	Učitelka 2/škola
	Notebook	Učitelka 3/škola
	Notebook	Školnice/škola
Elektronické nosiče	USB flash disk	Učitelka 1/škola
	USB flash disk	Učitelka 2/škola
	USB flash disk	Učitelka 3/škola

	Externí disk	Školnice/škola
Online aplikace	E-mail zaměstnance	Učitelka 1/škola
	E-mail zaměstnance	Učitelka 2/škola
	E-mail zaměstnance	Učitelka 3/škola
	E-mail zaměstnance	Školnice/škola
	Platforma Teams	Učitelka 1/škola
	Platforma Teams	Učitelka 2/škola
	Platforma Teams	Učitelka 3/škola
ODDĚLENÍ MŠ		
Pevná zařízení	Interaktivní tabule + dataprojektor	Vedoucí MŠ/škola
	Tiskárna	Vedoucí MŠ/škola
Přenosná zařízení	Notebook	Vedoucí MŠ/škola
	Notebook	Učitelka MŠ/škola
Online aplikace	E-mail zaměstnance	Vedoucí MŠ/škola
	E-mail zaměstnance	Učitelka MŠ/škola
	E-mail zaměstnance	Asistent pedagoga/škola
ODDĚLENÍ ŠD		
Pevná zařízení	Stolní PC	Vychovatelka/škola
	Tiskárna	Vychovatelka/škola
ODDĚLENÍ ŠJ		
Přenosná zařízení	Notebook	Vedoucí ŠJ/škola
SW	SW VIS Plzeň	Vedoucí ŠJ/škola
PROSTŘEDÍ		
Areál	Školní budova	Obec

Vybavení	Internet	Ředitel školy
	Telefonní linka	Ředitel školy
	Rozvod vody	Obec
	Elektrické rozvody	Obec
	Topení	Obec

Řízení vstupu a klíčová politika

Řízení vstupu do objektu je definováno v následující Tabulce 13 Řízení vstupu. Jsou zde definovány jednotlivé vstupy a jejich určení.

Tabulka 13 Řízení vstupu

VSTUP DO BUDOVY	URČENÍ	TECHNICKÉ ZABEZPEČENÍ	PERSONÁLNÍ ZABEZPEČENÍ
Přední (hlavní) vchod	Zaměstnanci školy, žáci, obyvatelé obecního bytu, cizí osoby (doprovody, kontroly)	Access control system	Pedagogický a nepedagogický dohled
Zadní (zahradní) vchod	Zaměstnanci školy, žáci v rámci činnosti školy, obyvatelé obecního bytu	Zámek	Pedagogický a nepedagogický dohled
Boční vchod (rampa)	Nepedagogičtí zaměstnanci	Zámek	Nepedagogický dohled

Seznam klíčů včetně jejich přidělování je veden ředitelem školy. Zaměstnanci školy jsou povinni zamykat budovu školy a jimi určené prostory jako jsou učebny, oddělení mateřské školy, jídelna s kuchyní a ředitelna. Zaměstnancům je zakázáno vytvářet duplikáty klíčů nebo je svěřovat neoprávněným osobám. V případě ztráty je potřeba nahlásit tuto skutečnost řediteli školy.

Zaměstnanci jsou povinni zavírat okna v budově, aby se zamezilo nepovolenému vniknutí do budovy nebo k poničení zařízení.

V případě narušení fyzické bezpečnosti nahlásí tuto skutečnost ředitel zřizovateli a případně dalším orgánům podle potřeby.

Ochrana zařízení

Zařízení je umístěno mimo pohled z vnějšího prostředí. Klíčové zařízení je situováno v ředitelně školy, kde je zamezen přístup veřejnosti.

Klasifikace informací

Ve škole lze klasifikovat informace do třech kategorií:

- vyhrazené, slouží k přístupu všem zaměstnancům,
- důvěrné, slouží k přístupu pouze pedagogickým zaměstnancům,
- tajné, slouží k přístupu pouze vedení, v tomto případě pouze pro ředitele školy.

K tomuto klasifikování vedlo dělení zaměstnanců ve škole. Vyhrazený přístup mají všichni zaměstnanci školy, i v tomto stupni je podmínkou doložka o mlčenlivosti.

Informace lze pro přehlednost označovat barevně:

- vyhrazené – není potřeba označovat,
- důvěrné – zelené označovaní informací pro pedagogické pracovníky,
- tajné – červené označení pro přístup vyhrazený řediteli školy.

Doporučení a odpovědnosti pro uživatele

Pro zaměstnance školy jsou doporučené následující principy pro zachování kybernetické bezpečnosti:

- manipulace s aktivy pouze podle svého pracovního zařazení,
- oddělení soukromých a pracovních zařízení a účtů,
- využívat silná hesla a neukládat si je do prohlížeče,
- zařízení musí být chráněno heslem,
- do zařízení se nesmí připojovat cizí paměťová média,
- aktualizovat SW a antivirový program,

- využívat pracovní komunikaci skrze pracovní platformy (školní e-mail a MS Teams),
- využívat pouze důvěryhodné a oficiální webové adresy a odkazy,
- do svých zařízení stahovat pouze originální a důvěryhodné aplikace,
- dodržovat zásadu prázdného stolu a prázdné obrazovky,
- k zařízení by měl být omezen přístup dalších osob,
- osobně si definovat pravidla ochrany soukromí,
- upozorňovat zaměstnavatele, popřípadě externího IT zaměstnance o podezřelých bezpečnostních incidentech.

Heslová politika

Heslo je vstupním prvkem do systémů, které obsahují důležité informace, proto by jeho tvorba neměla být podceňována. Pro zaměstnance jsou doporučeny následující parametry, co by mělo heslo obsahovat:

- malá i velká písmena,
- čísla,
- alespoň jeden speciální znak,
- a jeho délka by měla být alespoň 9 znaků.

Důležité je samozřejmě i pravidelné obměňování hesla. Heslo by rovněž nemělo být v různých přístupech shodné.

Komunikace

Komunikace zaměstnanců školy je povolena pouze skrze pracovní email. V rámci mobilní komunikace lze komunikovat skrze pracovní telefonní linku. Další komunikace vedení školy probíhá skrze datové schránky.

Detekce incidentů

Důležité je i zvládání bezpečnostních incidentů. Podstatou je povinnost jejich hlášení v případě zaznamenání jakékoli odchylky od běžného stavu. Tato odchylka se může projevit jako:

- narušení fyzické bezpečnosti,
- nefunkčnost služby nebo zařízení,

- lidská chyba,
- chyby ve funkčnosti systému,
- ztráta dat a informací.

Ředitel školy je povinen šetřit nahlášený bezpečnostní incident. Šetření může probíhat za pomoci externího IT zaměstnance nebo GDPR zmocněnce, případně dalších autorit.

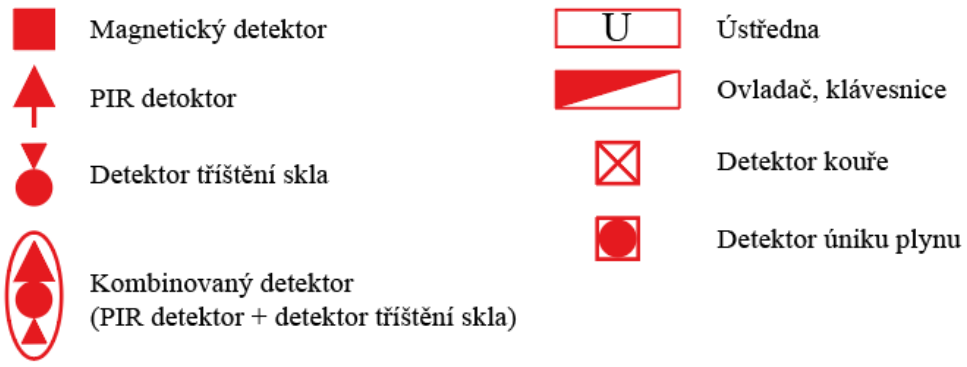
Plán zavádění opatření

V návaznosti na doporučená opatření vyplývající z analýzy rizik je v rámci interního bezpečnostního dokumentu zpracován plán zavádění opatření. Účelem není kalkulovat cenu, ale pouze navrhnout možný proces implementace a rozmístění prvků PZTS do objektu. K tomuto účelu bylo využito technických výkresů školy a obecných značení prvků PZTS.

Potřebné kroky k případné implementaci prvků PZTS:

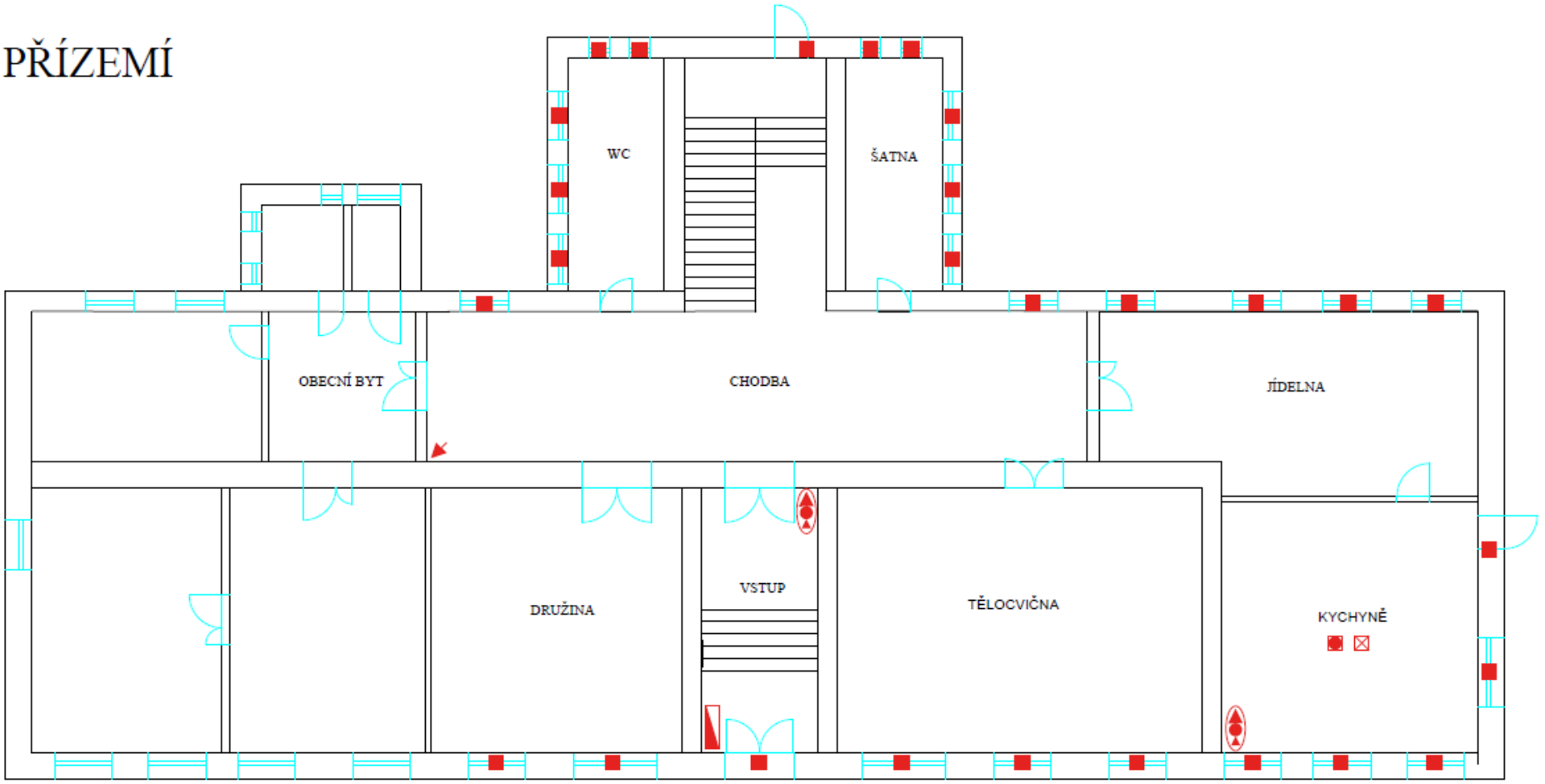
- bezpečnostní posouzení objektu,
- zhotovení projektu k nabídce a jeho posouzení,
- uzavření smlouvy o dodávce,
- montáž, aktivace a nastavení systému,
- testování systému,
- zaškolení obsluhy a předání díla včetně dokumentace.

Značení a vysvětlivky jsou uvedeny níže na Obrázku 16 Značení prvků PZTS ve výkresech.

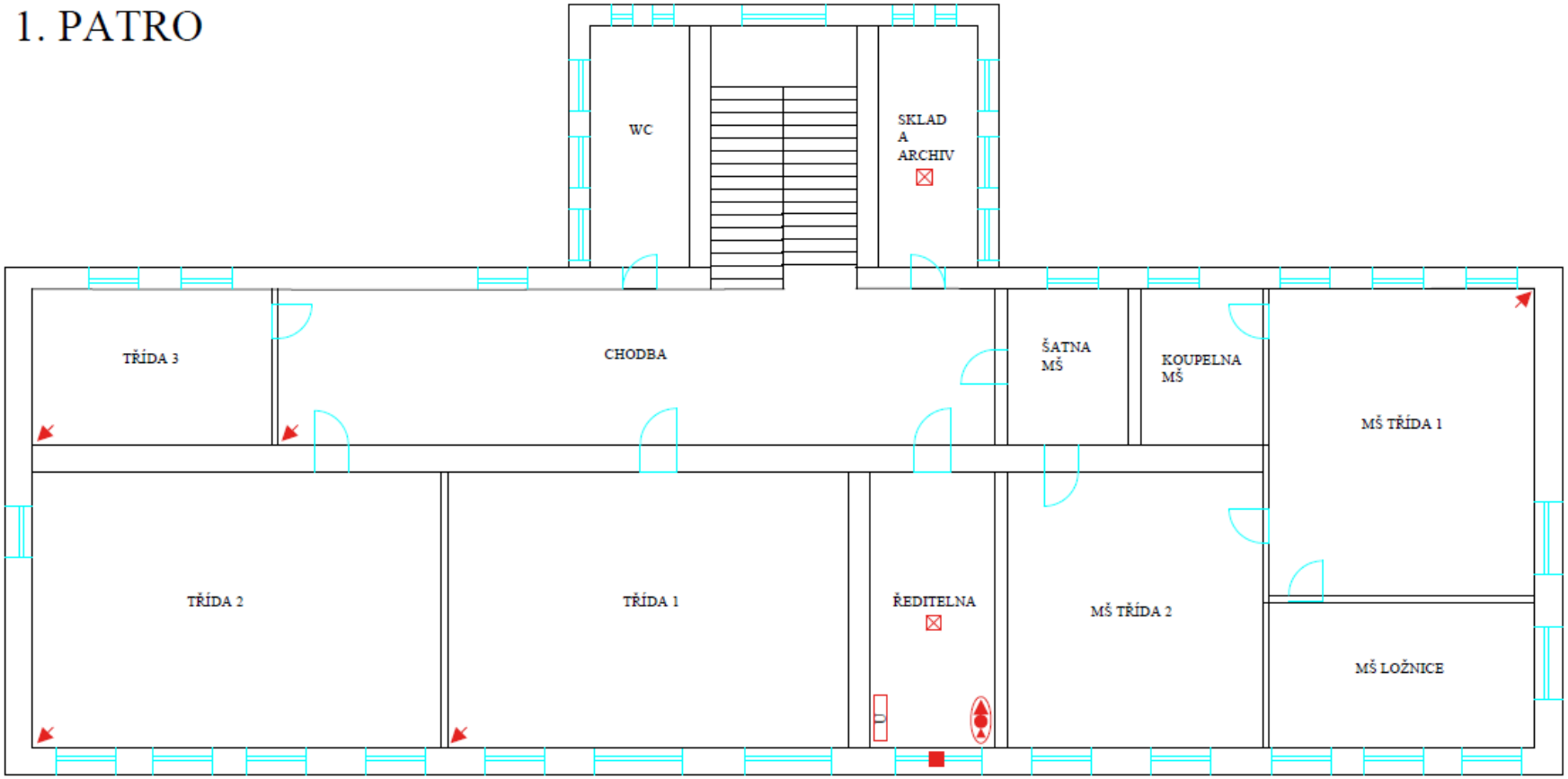


Obrázek 16 Značení prvků PZTS ve výkresech (vlastní)

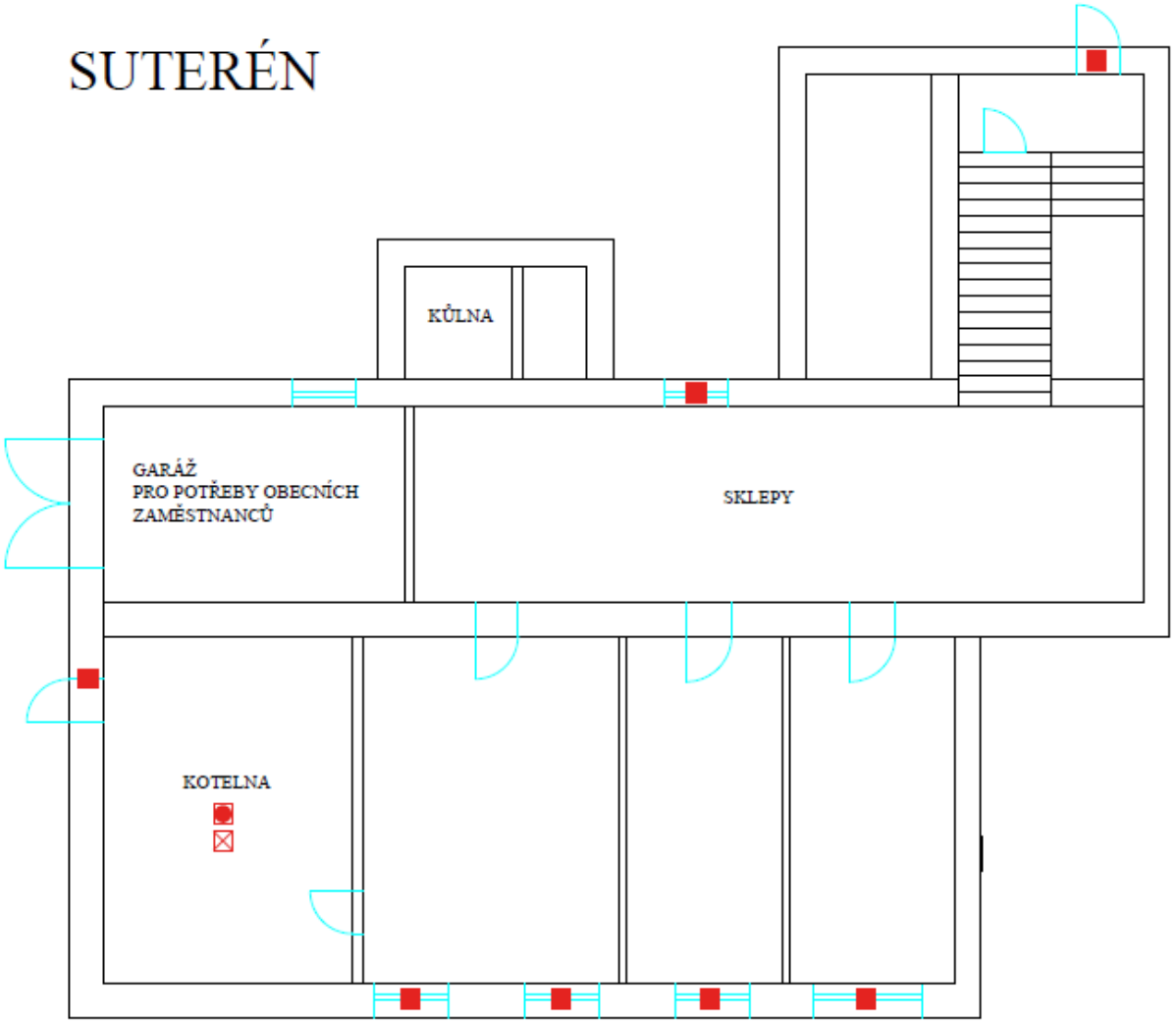
Následují výkresy přízemí, 1. patra a suterénu, do kterých bylo navrhnuto implementování jednotlivých prvků.



Obrázek 17 Rozmístění prvků PZTS v přízemí (vlastní)



Obrázek 18 Rozmístění prvků PZTS v 1. patře (vlasní)



Obrázek 19 Rozmístění prvků PZTS v suterénu (vlastní)

- Doporučené umístění ústředny je v ředitelně, protože je páteřní místností celé budovy. A také proto, aby ústředna nebyla přístupná cizím osobám v objektu.
- Naopak ovládání (klávesnice) systému je umístěné blízko vstupu, aby bylo blízko dveřím.
- Magnetické detektory byly navrženy tak, aby nedocházelo k jejich ovlivnění z okolí, například nedocházelo k nežádoucímu drnčení. Měly by být nastaveny tak, aby detekovaly vniknutí celého těla osoby. Jsou umístěny za předpokladu, že terén je nultým bodem a prahová a parapetová riziková výška je 2,5 metru, proto jsou umístěny převážně v suterénu a v přízemí objektu. V prvním patře je pak magnetický detektor umístěný v ředitelně z důvodu jejího strategického postavení.
- PIR detektory byly navrženy tak aby nebyly osvícené přímým slunečním světlem, aby nebyly rušeny prouděním vzduchu nebo nedošlo k jejich zastínění. Jsou umístěny v suterénu a v přízemí. V 1. patře jsou umístěny v místnostech s důležitými aktivy.
- Detektory tříštění skla nejsou umístěny v prostorech automaticky generovaných zvuků, například vyzvánění telefonu, v jejich aktivním stavu. A jsou v kombinaci s PIR detektory pohybu.
- Detektory kouře jsou umístěny na stropě více než 0,5 m od stěn a 0,6 m od rohů. Jsou umístěny v kuchyni, kotelně, ředitelně a archivu/skladu.
- Detektory plynu jsou umístěné v kuchyni a v kotelně v místech, kde by mohlo potencionálně dojít k úniku. Jsou umístěné v blízkosti stropu, protože se v objektu využívá zemní plyn, který je lehčí než vzduch.

Prvky PZTS se zároveň kumulují v ředitelně, protože se jedná o páteřní místnost celého objektu, které tedy musí být zabezpečeno.

Udržování a kontrola

Udržování bezpečnostní dokumentace, ISMS a kybernetické bezpečnosti by měl být nepřetržitý proces, ke kterému lze využít PDCA cyklus. K vyhodnocení problematiky by mělo dojít jedenkrát ročně, případně častěji v případě potřeby. Dále k nastavení a zavedení potřebných opatření.

Kontrolní činnost

V rámci kontrolní činnosti je tímto dokumentem ustanoven počet kontrol na 1krát ročně, v případě potřeby vícekrát. Odpovědnou osobou za kontrolu stavu bezpečnostní politiky a její dodržování je ředitel školy. Kontroluje stav, aktuálnost a dodržování tohoto dokumentu z praktického hlediska.

Řízení změn

V rámci efektivního a funkčního řízení systému je důležité zaznamenávat změny týkající se pozitivních i negativních změn. Aby se minimalizovala možnost hrozby narušení bezpečnosti je třeba každou změnu zaznamenat a případně opatření implementovat v tomto bezpečnostním dokumentu.

Prohlášení o aplikovatelnosti

Vedení školy prohlašuje, že na základě zpracování bezpečnostního dokumentu má zájem na řízení bezpečnosti organizace. Dokument obsahuje zabezpečení fyzického parametru, politiku řízení aktiv, klasifikaci informací, možné způsoby aplikace opatření k zabezpečení subjektu a další data důležitá k efektivnímu řízení bezpečnosti subjektu. Dokument doplňuje příručka kybernetické bezpečnosti dostupná pro všechny zaměstnance a uvedená v příloze.

Ředitel školy vyjádřil souhlas s prohlášením o aplikovatelnosti, tento souhlas je stvrzený podpisem a dokument spolu s ním je uvedený v příloze.

ZÁVĚR

Diplomová práce představovala teoretická východiska oblasti kybernetické bezpečnosti. Zaměřovala se i na konkrétní bezpečnostní opatření v souvislosti s ISMS a fyzickou bezpečností. V teoretické části byly v neposlední řadě uvedené údaje o aktuálním vývoji problematiky kybernetické bezpečnosti ve vzdělávacím sektoru v České republice a v zahraničí. Nejpostiženějšími zeměmi jsou Indie, Itálie, Austrálie, Velká Británie i USA. Práce byla zpracována v rámci aktuálního tématu šíření kybernetických hrozeb ve školním prostředí.

Hlavní cíl práce byl naplněn v kapitole 6, která se věnovala navržení opatření na rizika vycházející z analýzy rizik. Opatření byla navržena s přihlédnutím k převážně k fyzickému parametru, který je základem pro úspěšné řízení bezpečnosti subjektu.

První dílčí cíl v podobě rešerše současného stavu řešené problematiky, v zahraničí i v České republice, byl naplněn v teoretické části práce.

Druhým dílčím cílem byla stanovena analýza současného stavu kybernetické bezpečnosti v subjektu. K naplnění cíle došlo za pomoci nástroje pro identifikaci rizik Ishikawův diagram a kvantitativní analýzy FMEA v kapitole 5.

Třetím dílčím cílem bylo zpracování interního bezpečnostního dokumentu, který reflektuje řešenou problematiku. Dokument je určený do rukou ředitele školy a zřizovatele. Tento cíl byl naplněn v kapitole 7.

A v neposlední řadě bylo dílčím cílem stanoveno zpracování příručky určené pro všechny zaměstnance školy. Ta si klade za cíl posílit povědomí o dané problematice mezi zaměstnanci. Tento cíl byl naplněn v přílohové části, kde je příručka zobrazena.

Nejrizikovějšími faktory podle výsledků analýzy rizik jsou: kybernetický útok, neautorizovaný přístup, instalace neoriginálního SW, chyba uživatele, neoprávněná manipulace s daty, neprovádění aktualizací a narušení fyzické bezpečnosti v souvislosti s absencí prvků PZTS.

Nejdůležitějšími návrhy na opatření bylo stanoveno: potřeba školení zaměstnanců a zvyšování povědomí o kybernetické bezpečnosti, instalace prvků PZTS ke zvýšení fyzické bezpečnosti vedoucí k ochraně aktiv a v neposlední řadě vytvoření interního bezpečnostního dokumentu ke stanovení bezpečnostní politiky organizace.

Interní bezpečnostní dokument se zaměřuje na bezpečnost řízení lidských zdrojů, řízení aktiv včetně identifikace a stanovení vlastnictví aktiv a odpovědností za ně, řízení vstupu, klasifikaci informací, doporučení pro uživatele, detekci incidentů a plán zavádění navržených opatření.

Byly zahájeny konzultace o navržených opatřeních s ředitelkou školy a se zřizovatelem. V současné době tak probíhají jednání o implementaci těchto návrhů.

Cíle diplomové práce, s přihlédnutím k výše uvedeným závěrům, lze považovat za splněné.

SEZNAM POUŽITÉ LITERATURY

Adware, 2022. *ESSET* [online]. Praha: ESET software spol. s r.o. [cit. 2022-05-05]. Dostupné z: https://www.eset.com/cz/adware/

Alert: Further ransomware attacks on the UK education sector by cyber criminals, 2022. *National Cyber Security Centre* [online]. NCSC [cit. 2022-04-21]. Dostupné z: https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector

BAŠTA, Pavel a Jan KOLOUCH, 2019. *CyberSecurity*. První. Praha: CZ.NIC. ISBN 978-80-88168-31-7.

BENEŠOVÁ, Kristýna, 2019. *Systém řízení bezpečnosti informací vybraného subjektu*. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

Co je DNS, 2016. *Správa sítě: slovník pojmů* [online]. Praha: Aira GROUP [cit. 2022-04-20]. Dostupné z: https://www.sprava-site.eu/dns/

Cyber attacks are one of the biggest threats that schools face, experts warn, 2019. *Schools improvement* [online]. London: Schools Improvement [cit. 2022-04-21]. Dostupné z: https://schoolsimprovement.net/cyber-attacks-are-one-of-the-biggest-threats-that-schools-face-experts-warn/

Cybersecurity: main and emerging threats in 2021 (infographic), 2022. *Evropský parlament: Zprávy* [online]. [cit. 2022-04-21]. Dostupné z: https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic

ČESKO, 2004. Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2004-499

ČESKO, 2005. Vyhláška č. 364/2005 Sb., o vedení dokumentace škol a školských zařízení a školní matriky a o předávání údajů z dokumentace škol a školských zařízení a ze školní matriky (vyhláška o dokumentaci škol a školských zařízení). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-364

ČESKO, 2009. Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2009-194

ČESKO, 2014. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO, 2019. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

DOUCEK, Petr, 2020. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. První. Praha: Professional publishing. ISBN 978-80-88260-39-4.

Education Sector Experienced Highest Volume of Cyber Attacks in July, 2018. *CXOTToday.com: Technology News, Business Technology News, Information Technology News, Tech News India* [online]. Trivone Digital Services Pvt Ltd [cit. 2022-04-21]. Dostupné z: https://www.cxotoday.com/press-release/education-sector-experienced-highest-volume-of-cyber-attacks-in-july/

EVANS, Lester, 2019. *Cybersecurity: What You Need To Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners*. 1. USA: Lightning Source Inc. ISBN 97811794647237.

FAQ: Zákon o kybernetické bezpečnosti, b.r. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2022-04-20]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/#otazka2

Alert: Further ransomware attacks on the UK education sector by cyber criminals, 2022. *National Cyber Security Centre* [online]. NCSC [cit. 2022-04-21]. Dostupné z: https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector

BAŠTA, Pavel a Jan KOLOUCH, 2019. *CyberSecurity*. První. Praha: CZ.NIC. ISBN 978-80-88168-31-7.

BENEŠOVÁ, Kristýna, 2019. *Systém řízení bezpečnosti informací vybraného subjektu*. Diplomová práce. Univerzita Tomáše Bati ve Zlíně.

Co je DNS, 2016. *Správa sítě: slovník pojmů* [online]. Praha: Aira GROUP [cit. 2022-04-20]. Dostupné z: https://www.sprava-site.eu/dns/

Cyber attacks are one of the biggest threats that schools face, experts warn, 2019. *Schools improvement* [online]. London: Schools Improvement [cit. 2022-04-21]. Dostupné z: https://schoolsimprovement.net/cyber-attacks-are-one-of-the-biggest-threats-that-schools-face-experts-warn/

Cybersecurity: main and emerging threats in 2021 (infographic), 2022. *Evropský parlament: Zprávy* [online]. [cit. 2022-04-21]. Dostupné z: https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic

ČESKO, 2004. Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2004-499

ČESKO, 2005. Vyhláška č. 364/2005 Sb., o vedení dokumentace škol a školských zařízení a školní matriky a o předávání údajů z dokumentace škol a školských zařízení a ze školní matriky (vyhláška o dokumentaci škol a školských zařízení). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-364

ČESKO, 2009. Vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2009-194

ČESKO, 2014. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO, 2019. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

DOUCEK, Petr, 2020. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. První. Praha: Professional publishing. ISBN 978-80-88260-39-4.

Education Sector Experienced Highest Volume of Cyber Attacks in July, 2018. *CXOTToday.com: Technology News, Business Technology News, Information Technology News, Tech News India* [online]. Trivone Digital Services Pvt Ltd [cit. 2022-04-21]. Dostupné z: https://www.cxotoday.com/press-release/education-sector-experienced-highest-volume-of-cyber-attacks-in-july/

EVANS, Lester, 2019. *Cybersecurity: What You Need To Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners*. 1. USA: Lightning Source Inc. ISBN 97811794647237.

FAQ: Zákon o kybernetické bezpečnosti, b.r. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2022-04-20]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/#otazka2

IP kamera: Dahua Imou Dome Lite 4MP IPC-D42 (IPC-D42-IMOU) bílá, 2022. *DATART* [online]. Zlín: HP TRONIC Zlín, spol. s r.o. [cit. 2022-04-27]. Dostupné z: https://www.datart.cz/imou-ip-kamera-dome-lite-4mp-ipc-d42-pv280165.html?gclid=Cj0KCQjw06OTBhC_ARIsAAU1yOULwxGb2pRwJmsZyl9qkPAJ5GT1Iq8yrDK3EpeBiQCw4S5lQLHnDiIaAvy8EALw_wcB#moreDescription

JA-120PB Sběrnicový detektor pohybu osob a rozbití skla - Jablotron, b.r. *JABLOSHOP: velkoobchod a maloobchod* [online]. Praha: TELMO, a.s. [cit. 2022-04-27]. Dostupné z: https://www.jabloshop.cz/ja-120pb-sbernicovy-detektor-pohybu-osob-a-rozbiti-skla

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2013. *Výkladový slovník Kybernetické bezpečnosti: Cyber Security Glossary*. Praha. Dostupné také z: https://afcea.cz/wp-content/uploads/2015/03/Slovnik_Final_screen_v2_0.pdf

KLEIN, Alyson, 2022. Cyber Attacks on Schools: Who, What, Why and Now What?. *Government technology* [online]. California: e.Republic [cit. 2022-04-21]. Dostupné z: https://www.govtech.com/education/k-12/cyber-attacks-on-schools-who-what-why-and-now-what

KRESA, Dan, 2018. 3 výzvy kybernetické bezpečnosti ve vzdělávacím sektoru. *KYBEZ* [online]. Jihlava: GORDIC [cit. 2022-04-21]. Dostupné z: https://www.kybez.cz/3-vyzvy-kyberneticke-bezpecnosti-ve-vzdelavacim-sektoru/

LUKÁŠ, Luděk, 2015. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-05-7.

MAGDOŇOVÁ, Jana, 2019. Obrana českých škol proti hackerům? Pětina z nich si podle průzkumu nemůže dovolit IT specialistu. *IROZHLAS* [online]. Praha [cit. 2022-04-21]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/hackerske-utoky-na-skoly-it-specialista_1912071621_ada

MARKS, Paul, 2019. Cybersecurity and the Parkerian Hexad. *Staffhost Europe* [online]. [cit. 2022-04-19]. Dostupné z: https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2016. *TERMINOLOGICKÝ SLOVNÍK POJMŮ Z OBLASTI KRIZOVÉHO ŘÍZENÍ, OCHRANY OBYVATELSTVA, ENVIRONMENTÁLNÍ BEZPEČNOSTI A PLÁNOVÁNÍ OBRANY STÁTU*. Praha. Dostupné také z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU BEZPEČNOST, 2020. *NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY*. Praha. Dostupné také z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU BEZPEČNOST, 2021. *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2020*. Praha, 39 s. Dostupné také z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

Nejčastější pojmy v oboru IT zabezpečení: Malware, b.r. *ESSET* [online]. Praha [cit. 2022-04-19]. Dostupné z: https://www.eset.com/cz/malware/

Nejčastější pojmy v oboru IT zabezpečení: Spam, b.r. *ESSET* [online]. Praha [cit. 2022-04-19]. Dostupné z: https://www.eset.com/cz/spam/#co-je-spam-filter

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK, 2013. *PROBLEMATIKA ISMS V MANAŽERSKÉ INFORMATICE*. První. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM, s. r. o. ISBN 978-80-7204-872-4.

PAČKA, Roman, 2019. *CSIRT: v přední linii boje proti kybernetickým hrozbám*. Brno: Centrum pro studium demokracie a kultury. Politologická řada. ISBN 9788073254735.

Pharming, 2016. *Správa sítě: slovník pojmů* [online]. Praha: Aira GROUP [cit. 2022-04-20]. Dostupné z: https://www.sprava-site.eu/pharming/

Přístupový systém MPS, 2022. *Klíčové centrum* [online]. Plzeň [cit. 2022-04-27]. Dostupné z: https://www.klicovecentrum.cz/produkt/mps-pristupovy-system/

Ransomware - definice a jak se úspěšně bránit, 2020. *Uloz to a sdilej* [online]. Praha [cit. 2022-04-20]. Dostupné z: https://www.uloztoasdilej.cz/ransomware-definice-a-jak-se-uspesne-branit/#Typy_ransomwaru

SEDLÁK, Petr a Martin KONEČNÝ, 2021. *KYBERNETICKÁ (NE)BEZPEČNOST: Problematika bezpečnosti v kyberprostoru*. První. Brno: AKADEMICKÉ NAKLADATELSTVÍ CERM, s. r. o. ISBN 978-80-7623-068-2.

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

Spyware, 2022. *ESSET* [online]. Praha: ESET software spol. s r.o. [cit. 2022-05-05]. Dostupné z: https://www.eset.com/cz/spyware/

ŠŤASTNÝ, Jakub, 2020. Trestní postih DoS/DDoS útoků. *Epravo.cz* [online]. Praha [cit. 2022-04-20]. Dostupné z: https://www.epravo.cz/top/clanky/trestni-postih-dosddos-utoku-110941.html

ŠULC, Vladimír, 2019. *Kybernetická bezpečnost*. První. Praha: Vydavatelství a nakladatelství Aleš Čeněk, s. r. o. ISBN 978-80-7380-737-5.

VAR-TEC FM-102 - 0701-046: povrchový, samolepící magnetický kontakt, 2vodič, bílý, 2022. *ABALARM: Smart electronics systems* [online]. Most: PrestaShop [cit. 2022-04-27]. Dostupné z: https://www.abalarm.cz/ishop/cs/magneticke-kontakty/609-fm-102-bila-povrchovy-samolepici-2vodic--8595584600439.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control System
CIA	Confidentiality, Integrity, Availability
ČSN	Česká technická norma
ČŠÚ	Český statistický úřad
DDoS	Distributed Denial of Service
DoS	Denial of Service
EU	Evropská unie
GDPR	General Data Protection Regulation
HW	Hardware
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IS	Informační systém
ISMS	Information Security Management Systém
ISO	International Organization for Standardization
IT	Information technology
KARS	Kvalitativní analýza rizik s použitím jejich souvztažností
KB	Kybernetická bezpečnost
MS	Microsoft
MŠ	Mateřská škola
MŠMT	Ministerstvo školství, mládeže a tělovýchovy
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSSZ	Okresní správa sociálního zabezpečení
PaM	Personalistika a mzdové účetnictví
PDCA	Plan, Do, Check, Act
PO	Požární ochrana

PZTS	Poplachový zabezpečovací a tísňový systém
SMS	Short Message Service
SW	Software
ŠD	Školní družina
ŠJ	Školní jídelna
ŠPZ	Školní poradenské zařízení
UPS	Uninterruptible Power Supply/Source
USA	United States of America
ÚIV	Úřad pro informace ve vzdělávání
VDS	Video dohledový systém
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
ZŠ	Základní škola

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I PŘÍRUČKA PRO ZAMĚSTNANCE ŠKOLY

PŘÍLOHA P II VYJÁDŘENÍ SOUHLASU S PROHLÁŠENÍM O APLIKOVATELNOSTI

Základní škola a mateřská škola Novosedly nad Nežárkou

Prohlášení o aplikovatelnosti

Vedení školy prohlašuje, že na základě zpracování interního bezpečnostního dokumentu má zájem na řízení bezpečnosti organizace. Dokumentace obsahuje zabezpečení fyzického parametru, politiku řízení aktiv, klasifikaci informací, možné způsoby aplikace opatření k zabezpečení subjektu a další data důležitá k efektivnímu řízení bezpečnosti subjektu.

Základní škola a mateřská škola
Novosedly nad Nežárkou
Novosedly nad Nežárkou 112, 378 17
tel.: 384 791 199 IČO: 709 85 120

ředitel školy

5. 5. 2022