VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

ZAVEDENÍ BEZPEČNOSTNÍCH OPATŘENÍ DLE ISMS PRO ZÁKLADNÍ ŠKOLU

IMPLEMENTING OF SECURITY MEASURES ACCORDING TO ISMS FOR ELEMENTARY SCHOOL

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Marek Pexa

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Marek Pexa**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2018/19

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Zavedení bezpečnostních opatření dle ISMS pro základní školu

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza současného stavu
Vlastní návrh řešení a přínos návrhu řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem diplomové práce je zavedení bezpečnostních opatření dle ISMS na dané základní škole.

Základní literární prameny:

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Požadavky, Praha: Český normalizační institut, 2006.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnostiinformací - Soubor postupů, Praha: Český normalizační institut, 2008.

DOUCEK Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práce se zabývá zavedením bezpečnostních opatření pro základní školu. Práce je rozdělena na tři hlavní části. V první části diplomové práce jsou zpracovány základní teoretické pojmy z oblasti informační bezpečnosti a legislativní náležitosti potřebné pro pochopení dané problematiky. Druhá část diplomové práce popisuje stávající stav na základní škole. Poslední praktická část obsahuje samotný návrh bezpečnostních opatření a doporučení.

Abstract

The diploma thesis deals with introduction of security measures for primary and elementary school. The thesis is devided into three main parts. The first part deals with basic theoretical concepts of information security and legislative elements needed for understanding the issue. The second part desrcibes the current state for primary and elementary school. The last practical part includes proposal of security measures and recommendations.

Klíčová slova

informační a kybernetická bezpečnost, ISO/IEC 27000, budování bezpečnostního povědomí, aktivum, ISMS

Key words

information and cyber security, ISO/IEC 27000, security awareness education, asset, ISMS

Bibliografická citace

PEXA, Marek. *Zavedení bezpečnostních opatření dle ISMS pro základní školu* [online]. Brno, 2019 [cit. 2019-05-09]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119780. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 12. května 2019

.....

podpis autora

Poděkování

Tímto způsobem bych chtěl poděkovat vedoucímu mé bakalářské práce panu Ing. Petru Sedlákovi a panu Ing. Viktoru Ondrákovi, Ph.D. za konstruktivní připomínky k práci, odborné rady a cenné informace, které mi pomohly k vypracování diplomové práce. Dále bych chtěl poděkovat vedení základní školy za poskytnutí potřebných materiálů a jejich vstřícnému jednání.

OBSAH

ÚVOD

V dnešní době si ani nedokážeme představit život bez informační techniky. Ať se jedná o mobilní telefony, tablety, notebooky, stolní počítače. S informačními technologiemi se setkáme téměř všude. S tím, jak se nároky uživatelů stupňují, vyvíjí se i informační technologie. Tím rostou i možná rizika. Jednou z nejcennějších věcí jak pro běžného uživatele, tak pro velké společnosti jsou data a informace. S tímto úzce souvisí pojem informační bezpečnost. Bohužel informační bezpečnost je u mnoha firem, společností a organizací velmi podceňována a není ji přikládána téměř žádná váha. Je velmi důležité se informační bezpečnosti věnovat a dbát na její dodržování. S informační bezpečností by se měli setkat uživatelé již na základní škole. Měla by být vytvořena metodika a postupy, jak žáky vzdělávat. Tento proces by měl dále pokračovat i na střední škole. Poté i v zaměstnání. Je to jeden z kroků, jak zamezit informační negramotnosti uživatelů. V organizacích by měli být pravidelně školeni uživatelé, kteří se dostávají s informačními aktivy do styku. Školení by měli probíhat pravidelně. A to především z toho důvodu, že lidský faktor bývá často příčinou problému a posléze ztráty firmy. Ať se již jedná o ztrátu dat, informací či finanční. Z toho důvodu je nutné bezpečnostní povědomí neustále budovat.

K této problematice patří i budování fyzické bezpečnosti a obzvláště, když se jedná o veřejnou budovu, kterou žáci pravidelně navštěvují. Jako odstrašující příklad můžeme uvést útok ženy na základní škole, kde byl po útoku usmrcen jeden z žáků. Je tedy důležité chránit jak aktiva organizace, tak i zdraví jejich zaměstnanců a žáků. Dle mého názoru je fyzická bezpečnost v rámci ČR na školách dost zanedbávána. I když by bezpečnost měla být prioritou zřizovatele, potažmo vedení.

Diplomová práce je rozdělena do několik částí. V úvodu jsou objasněny základní teoretické východiska nutné pro pochopení dané problematiky, kterou se diplomová práce zabývá. Druhá část práce je věnována analýze současného stavu na dané základní škole. Závěrečná třetí část práce je věnována samotnému návrhu řešení. V této části jsem vycházel z provedených analýz, které byly provedeny v předcházející kapitole. Veškerá

opatření jsou definována dle norem ČSN ISO/IES 27000:2017, 27001:2017, 27002:2017. V závěru práce je ekonomické zhodnocení a časový harmonogram.

1 CÍL A METODIKA PRÁCE

Hlavním cílem diplomové práce je provést analýzu současného stavu a analyzovat informační bezpečnost na základní škole. Na základě provedených analýz jsou vybraná jednotlivá bezpečnostní opatření, která budou zaváděna v souladu s ISMS. V práci nebude zaváděn systém řízení bezpečnosti informací v plném rozsahu. Pouze vybraných částí, které budou zavedeny v první etapě.

Diplomová práce je rozdělena na tři hlavní části. V první jsou vypracovaná teoretická východiska a vysvětleny základní pojmy a definice, které se týkají daného tématu. Druhá část popisuje analýzu současného stavu organizace, součástí jsou i provedené analýzy (asistované zhodnocení). Návrhová část obsahuje návrh vybraných bezpečnostních opatření, ekonomické zhodnocení a časový harmonogram. Práce končí závěrem, kde jsou shrnuty veškeré poznatky.

2 TEORETICKÁ VÝCHODISKA

V úvodní kapitole diplomové práce budou zpracovány teoretická východiska, z kterých budu vycházet v průběhu celé práce. Kapitola je rozdělena do několika částí. Budou zde vysvětleny základní teoretické postupy a pojmy.

2.1 Informační systém

V poslední době je tento výraz často používán. Ale neexistuje žádná jedinečná, ustálená ani všeobecně přijatelná definice tohoto pojmu. Pod tímto pojmem si můžeme představit účelově uspořádanou množinu prvků a vazeb mezi nimi, které mají definované cílové chování. IS můžeme definovat jako: „*soubor technických, lidských organizačních prostředků a metod, který efektivně poskytuje oprávněným uživatelům definované informační služby v definované kvalitě*“ (1, 4).

2.1.1 Složky informačního systému

Složky informačního systému společně s jednotlivými vazbami určují chování informačního systému, jeho parametry, kvalitu služeb a jeho bezpečnost.

Hardware – pod tímto pojmem si můžeme představit technické prostředky hmotného charakteru. Kvalita je ovlivněna poruchovostí informačního systému. Je jedním z faktorů, který určuje kvalitu poskytovaných služeb (dostupnost, rychlost) (4).

Software – jde o technické prostředky nehmotného charakteru. Obsahují algoritmy. Podílí se na chování informačního systému (4).

Údaje – jsou uloženy v informačním systému. Mohou být v podobě dat, informací nebo znalostí (4).

Lidský faktor – lidé mají za úkol zabezpečit obsluhu, údržbu a užívání informačního systému (4).

2.1.2 Uživatelé a jejich oprávnění

Cílem informačního systému je, poskytování informačních služeb pouze jednoznačně definovaným uživatelům. Systém tedy musí umět jednoznačně rozpoznat uživatele. Uživateli poskytovat pouze informace, pro které je oprávněn. Pod pojmem uživatel si můžeme představit člověka či jiný informační systém (4).

Autentizace – jedná se o ověření identity daného subjektu. Zjišťujeme, zda je daný subjekt ten, za který se vydává (4).

Autorizace – povolení přístupu k úkonu nebo operaci. Autorizace navazuje na proces autentizace (4).

2.1.3 Kvalita služeb

Kvalitu poskytovaných služeb bychom měli definovat již ve fázi projektování IS. Hlavní ukazatele kvality informačních služeb:

- správnost informací,
- úplnost,
- forma prezentace,
- míra dostupnosti.
- včasnost poskytnutí informace,
- rychlost odezvy (4).

2.2 Bezpečnost informačního systému

Pojem bezpečnost obecně chápeme, jako ochranu objektu či věci před zničením, poškozením, ztrátou nebo zcizením. Informační bezpečnost tedy můžeme chápat jako ochranu informačního systému před poškozením, ztrátou, zničením nebo zcizením (4).

2.2.1 Základní atributy bezpečnosti IS

Informační systémy jsou určeny k uspokojování potřeb (informačních) pro oprávněné uživatele. Můžeme definovat tři atributy, které je zapotřebí u informačního systému zabezpečit:

- Důvěrnost (confidentiality),
- Integrita (integrity),
- Dostupnost (availability) (4).

Pojem informační bezpečnost tedy můžeme definovat jako systém ochrany důvěrnosti, integrity a dostupnosti informací v informačním systému (4).

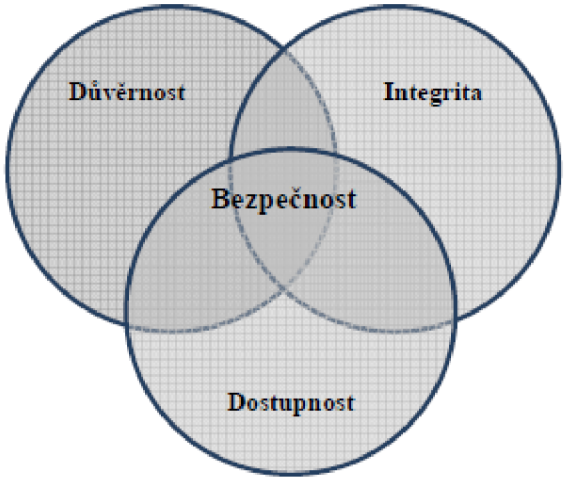
Důvěrnost (Confidentiality) – stav, kdy jsou informace poskytnuty jen oprávněným uživatelům. V případě, že se informace dostanou k neoprávněným uživatelům, jde o narušení důvěrnosti. Důležité je, aby byly informace srozumitelné pro všechny uživatelé a vhodně je klasifikovat (určit stupeň důvěrnosti) (4).

Integrita (Integrity) – můžeme ji definovat jako stav, kdy jsou všechny informace správné a úplné. V případě, že dojde k narušení integrity, mohou selhat některé prvky systému (hardware, software, uživatel) (4).

Dostupnost (Availability) – dostupnost můžeme chápat jako stav, kdy jsou informační služby poskytnuty oprávněným uživatelům v definované podobě a v okamžiku jejich potřeby (4).

2.2.2 Vazba mezi atributy

V případě, že dojde k narušení informačního systému, může dojít k finančním ztrátám, poškození dobrého jména organizace a v některých případech k ohrožení života a zdraví lidí. Proto je důležité informační systém před narušením chránit, a to v průběhu celého životního cyklu IS. Vždy musíme brát v potaz, jak informační systém chránit. Přehnaná snaha chránit jeden atribut může vést k ohrožení ostatních atributů, což je nežádoucí (4).



Obrázek č. 1: Vazba mezi atributy (Zdroj: 4, s. 6)

2.2.3 Narušení informační bezpečnosti

Na informační aktiva mohou působit vlivy, jak z okolí tak i zevnitř informačního sytému. V případě, že tyto vlivy naruší struktury, vlastnosti a vazby aktiva jedná se o hrozby. V případě, že tyto hrozby naruší bezpečnost IS, mluvíme o bezpečnostních hrozbách.

Aktivum (Asset) – aktivem chápeme cokoliv, co má pro informační systém cenu. Je to veškerý hmotný a nehmotný majetek (1, 2, 3).

Hrozba (Treat) – pokud na informační aktiva působí vlivy z okolí či zevnitř informačního systému a mohou způsobit nežádoucí změny ve struktuře aktiva, vlastnostech a vazbách mluvíme o možné hrozbě (4).

Zranitelnost (Vulnerability) – jedná se o slabé místo aktiva nebo systému (HW prostředek, aplikace, služba), na které mohou působit hrozby a tím aktivum narušit (1, 4).

Opatření (Countremeasure) – napomáhá ke snížení pravděpodobnosti vzniku hrozeb, snižuje zranitelnost aktiv a snižuje dopad na organizaci (4).

Riziko (Risk) – jedná se o kombinaci hrozby a zranitelnosti. Je to tedy pravděpodobnost, že bezpečnostní hrozba přeroste v bezpečnostní incident (1, 2).

Bezpečnostní událost (Information security event.) – v případě, že hrozba realizuje své působení na zranitelné místo aktiva, jedná se o bezpečnostní událost. Je to tedy aktivita, která působí na zranitelné místo aktiva (2).

Bezpečnostní incident (Information security incident) – jde o narušení důvěrnosti, integrity nebo dostupnosti. Jako příklad můžeme například uvést neoprávněné otevření dveří do datového centra (4).

Úroveň rizika – vynásobením rizika vzniku incidentu a možným dopadem incidentu získáme úroveň rizika. To nám charakterizuje nebezpečnost hrozby pro organizaci (4).

2.3 Informační aktiva

Pokud je aktivum součástí informačního systému nebo má vazbu na informační systém, mluvíme o informačním aktivu. Může se jednat o HW, SW, data, uživatele. Patří sem i nehmotná aktiva, jako je například pověst společnosti.

2.3.1 Analýza aktiv

V případě, že se jedná o rozsáhlý a složitý systém, obsahuje velké množství aktiv. Aktiva jsou v různě formě a podobě. Proto je jejich analýzu velmi obtížné provádět. Je vhodné pro analýzu aktiv složit tým odborníků pro všechny oblasti ICT. Analýzy by měla mít strukturu projektu (cíl, tým, časový plán, dokumentace, metodika,…).

Fáze analýzy aktiv:

- zadat a definovat cíle,
- sestavit tým,
- dekompozice systému
- identifikace aktiv a jejich vlastníků,
- rozdělení aktiv
- klasifikace a ohodnocení (4).

2.4 Řízení rizik (Risk management)

V dnešní době si pod pojmem riziko můžeme představit nebezpečí vzniku škody, poškození, ztráty či zničení. Pro definici pojmu riziko neexistuje žádná obecně uznávaná definice. Můžeme ho definovat různě:

- *„pravděpodobnost či možnost vzniku ztráty, obecně nezdaru*,
- *variabilita možných výsledků nebo nejistota jejich dosažení*,

- *odchýlení skutečných a očekávaných výsledků*,
- *pravděpodobnost jakéhokoliv výsledku ošidného od výsledku očekávaného*,
- *situace, kdy kvantitativní rozsah určitého jevu podléhá jistému rozdělení pravděpodobnosti*,
- *nebezpečí negativní odchylky od cíle*,
- *nebezpečí chybného rozhodnutí*,
- *možnost vzniku ztrát nebo zisku*,
- *neurčitost spojená s vývojem hodnoty aktiva*,
- *střední hodnota ztrátové funkce*,
- možnost, že specifická hrozba využije specifickou zranitelnost systému,
- kombinace pravděpodobnosti události a jejího následku“ (9, str. 90).

Bezpečnostní riziko (Risk)

Tento pojem můžeme pochopit, jako pravděpodobnost vzniku bezpečnostního incidentu. Můžeme ho definovat v rozsahu <1;0>, kdy 1 představuje jistotu rizika a 0 žádné riziko (4).

Řízení rizik (Risk management)

Jedná se o deterministický a systematický řízený proces, který by měl v organizaci přispět k tomu, aby:

- byla provedena identifikace bezpečnostních rizik informačních systémů
- byly posouzeny rizika z pohledu jejich důsledků na aktiva, informační systémy,
- bylo stanovení priorit při ošetření rizik,
- byly nastaveny priority a činnosti, které povedou ke snížení rizika,
- byla sledována účinnost ošetření rizik (4).

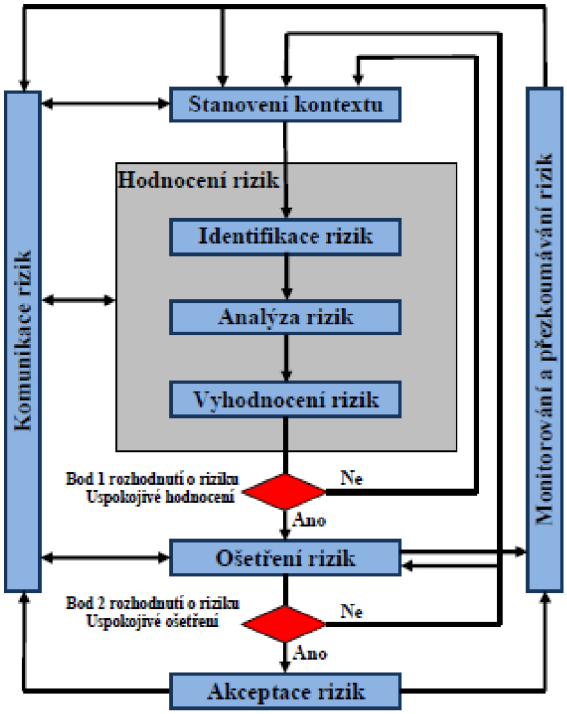
Implementaci řízení rizik můžeme aplikovat s ohledem na velikost, strukturu organizace, počtu informačních systému na organizaci (4).

2.4.1 Proces řízení rizik

Proces řízení rizik informační bezpečnosti se skládá z těchto činností:

- stanovení kontextu,
- identifikace rizik,
- analýza rizik,
- vyhodnocení rizik,
- ošetření rizik,
- akceptace rizik,
- monitorování a přezkoumání rizik,
- komunikace rizik (4)

Celý proces řízení rizik můžeme demonstrovat na schématu, který ukazuje jednotlivé návaznosti činností. Můžeme si všimnout cyklické návaznosti celého procesu řízení. V úvodu celého procesu si stanovíme kontext řízení rizik, dále pokračujeme hodnocením rizik. Dalším krokem je ošetření rizika, popřípadě jeho akceptace. Proces je ukončen přezkoumáním rizik (4).



Obrázek č. 2: Schéma procesu řízení rizik (Zdroj: 4, s. 32)

Stanovení kontextu

Kontext řízení rizik informační bezpečnosti zahrnuje:

- „*stanovení základních kritérií pro řízení rizik bezpečnosti informací*,
- *definici rozsahu a hranic*,
- *stanovení organizační struktury pro řízení rizik*“ (4, str. 33).

Abychom stanovili kontext správně, je důležité určit konkrétní účel řízení rizik informační bezpečnosti (4).

Stanoven základních kritérií

Určení metrik, postupů, metod a rozhodovacích kritérií, které jsou použity při jednotlivých činnostech řízení rizik (4).

Specifikace přístupu k řízení rizik – organizace vyjádří prioritu ohledně řízení rizik a jeho podpoře, zhodnocení dostupných zdrojů, definování komunikace, stanovení dokumentů a způsob předávání informací (4).

Kritéria hodnocení rizik – jsou stanoveny metody, které budou požity při analýze rizik, klasifikační schémata a postupy (4).

Kritéria dopadu – na základě stupně škod nebo ztrát stanovíme klasifikaci dopadů (4).

Kritéria akceptace rizik – na základě bezpečností politiky, cílech a záměrech společnosti klasifikujeme, které riziko je pro společnost akceptovatelné (4).

2.4.2 Stanovení rozsahu a hranic

Jako první krok by měla organizace stanovit a pevně definovat rozsah a hranice pro řízení rizik informační bezpečnosti. Mimo to by měly být stanoveny i vnější hranice. Ty nám pomáhají k oddělení zkoumání rizik vnější a vnitřní bezpečnostní hrozby (4).

2.4.3 Stanovení organizační struktury

Vedení společnosti jasně stanoví organizační strukturu. Jsou jasně ustanoveny zodpovědné osoby, definovány odpovědnosti, stanoveny vztahy mezi organizací a systémem řízení rizik, ustanovení pravomocí (4).

2.5 Analýza rizik

První krok při snížení rizik je jejich analýza. Jedná se o proces definování hrozeb, pravděpodobnosti jejich vzniku a dopadu na aktiva. Abychom analýzu rizik mohli provést, jsou pro nás důležité informace, které získáme na základě analýzy aktiv, z analýzy incidentů a analýzy hrozeb (4, 9).

Když chceme, zjisti bezpečnostní riziko incidentu, musíme si uvědomit, časovou posloupnost výskytu incidentu. Bezpečnostní hrozba může vyvolat bezpečnostní událost a ta s nějakou pravděpodobností může způsobit bezpečnostní incident (4).

Pravděpodobnost, že se vyskytne hrozba, je závislé na mnoha proměnných. Těmi mohou být – čas, významnost informačního systému, cena informací, geografická poloho, charakter organizace (4).

Pravděpodobnost, že hrozba vyvolá bezpečnostní událost, závisí na struktuře informačního systému, charakteru hrozby, intenzitě a podobě hrozby (4).

Pravděpodobnost, že bezpečnostní událost způsobí bezpečnostní incident, závisí na rychlosti reakce na projevy bezpečnostní událost a na konkrétní realizaci aktiva (4).

Matematický výpočet bezpečnostního rizika

V případě, že chceme matematicky přesně vypočítat bezpečnostní riziko incidentu, musíme u všech bezpečnostních incidentů, které identifikujeme, všech možných událostí a všech hrozeb určit dílčí rizika. Výsledné bezpečnostní riziko u každého incidentu je součet všech dílčích rizik (4).

Matematický vztah pro výpočet bezpečnostního incidentu rizika:

$$R_i = \sum_{i=1}^{n} Pui_i * \left(\sum_{j=1}^{m_i} Phu_{ij} * Ph_{ij} \right)$$

kde:

- R_i – „*bezpečnostní riziko možného bezpečnostního incidentu*,
- Pui_i - *pravděpodobnost, že i-tá událost způsobí bezpečnostní incident*,
- Phu_{ij} – *pravděpodobnost, že j-tá hrozba vyvolá i-tou bezpečnostní událost*,
- Ph_{ij} – *pravděpodobnost výskytu j-té hrozby i-té události*,
- n - *počet možných bezpečnostních událostí, které mohou vyvolat daný bezpečnostní incident*,
- m_i – *počet hrozeb, které mohou způsobit i-tou bezpečnostní událost*“ (4, str. 35).

2.5.1 Metody pro analýzu rizik

Pro analýzu rizik se v praxi využívají dvě skupiny klasifikačních schémat:

- Kvalitativní analýza,
- Kvantitativní analýza (4)

Kvalitativní analýza

K ohodnocení se používá slovní spojení – nízké, střední, vysoké riziko vzniku bezpečnostního incidentu. Odhadujeme pravděpodobnost, že při působení konkrétní hrozby nastane konkrétní bezpečnostní incident. Analýza je založena na subjektivních pocitech hodnotitelů. Vhodné je tuto analýzu nahradit analýzou kvantitativní (4).

Součástí kvalitativní analýzy je nutné vhodně zvolit hodnotící kritérium. Mohou být stanovena různá klasifikační kritéria pro různé typy aktiv, skupiny hrozeb a incidentů (4).

Nejčastěji se kvalitativní analýzy používá:

- jako první stupeň analýzy rizik, který následuje analýzou kvantitativní,
- pokud je tento druh analýzy postačující pro rozhodnutí,
- pokud zdroje pro analýzu nejsou dostatečné (4).

Kvantitativní analýza

Jako klasifikační kritérium je použita stupnice s číselným ohodnocením. Rozdílem oproti kvalitativní analýze je, že není prováděn odhad rizika vzniku incidentu odborným odhadem, ale jsou odhadována jednotlivá dílčí rizika. Je použit předem definovaný algoritmus, který odhady transformuje na výslednou hodnotu rizika (4).

Data jsou čerpány z předcházejících provedených analýz aktiv, incidentů a hrozeb. Dále také na základě praktických zkušeností z reálného provozu zkoumaného informačního systému. Nevýhodou této analýzy je, že vyžaduje velké množství kvalitních informací. V případě, že nebudou pro tuto analýzu kvalitní podklady, může vykazovat horší výsledky, než analýza kvalitativní (4).

2.6 Činnosti analýzy rizik

2.6.1 Posouzení následků

Prvním krokem analýzy rizik by mělo být posouzení následků incidentu. Ohodnotíme tedy reálný dopad na společnost. Následky posuzujeme zvlášť pro všechny atributy informační bezpečnosti. Vstupem pro analýzu jsou výstupy analýzy incidentů, analýzy hrozeb a analýzy aktiv. Výstupem činnosti je doplnění seznamu možných incidentů o ohodnocení následků bezpečnostních incidentů zohledněný o aktiva a kritéria dopadu (4).

2.6.2 Určení pravděpodobnosti incidentu

Činnost by nám měla ukázat pravděpodobnost vzniku bezpečnostních incidentů. Vstupem činnosti jsou výstupy z analýzy incidentů, analýzy hrozeb a analýzy aktiv. Důležitým vstupem je i seznam všech existujících nebo plánovaných bezpečnostních opatření, jejich specifikace, účinnost a uplatnění (4).

Příklad klasifikačního schématu:

Klasifikační stupeň	Pravděpodobnost incidentu
1	Nepravděpodobný
2	Málo pravděpodobný
3	Středně pravděpodobný
4	Vysoce pravděpodobný
5	Téměř jistý

Obrázek č. 3: Klasifikační schéma pro určení pravděpodobnosti vzniku incidentu (Zdroj:4, s. 38)

Výstupem je kvalitativní či kvantitativní ohodnocení pravděpodobnosti výskytu jednotlivých incidentů a doplnění do seznamu možných incidentů (4).

2.6.3 Určení úrovně rizik

Někdy se v praxi můžeme setkat tím, že mohou nastat incidenty s vysokou pravděpodobností, ale s minimálním dopadem (např. nefunkční myš u PC). Avšak někdy se můžeme v organizaci setkat s naprostou opačnou situací. Pro objektivní stanovení priorit nasazování bezpečnostních opatření musíme vyjádřit nebezpečnost jednou hodnotou. Je zavedena veličina, která se nazývá úroveň rizika. Vypočtena jako součin pravděpodobnosti vzniku bezpečnostního incidentu a následku incidentu. Tuto veličinu můžeme ohodnotit kvalitativně či kvantitativně (4).

Kvalitativní ohodnocení

		Pravděpodobnost výskytu incidentu				
		Velmi nízká	Nízká	Střední	Vysoká	Velmi vysoká
Dopad	Velmi nízký	Nízké riziko 0	Nízké riziko 1	Nízké riziko 2	Střední riziko 3	Střední riziko 4
	Nízký	Nízké riziko 1	Nízké riziko 2	Střední riziko 3	Střední riziko 4	Střední riziko 5
	Střední	Nízké riziko 2	Střední riziko 3	Střední riziko 4	Střední riziko 5	Vysoké riziko 6
	Vysoký	Střední riziko 3	Střední riziko 4	Střední riziko 5	Vysoké riziko 6	Vysoké riziko 7
	Velmi vysoký	Střední riziko 4	Střední riziko 5	Vysoké riziko 6	Vysoké riziko 7	Vysoké riziko 8

Obrázek č. 4: Přiřazení úrovně rizika (Zdroj: 4, s. 39)

Výstupem je kvalitativní či kvantitativní ohodnocení pravděpodobnosti úrovně rizika jednotlivých incidentů a doplnění do seznamu možných incidentů (4).

2.6.4 Vyhodnocení rizik

Dochází k vyhodnocení nebezpečností jednotlivých bezpečnostních incidentů a jejich seřazení dle úrovně rizik. Účelem jejich seřazení je určení priorit v ochraně bezpečnosti informačního systému. Dále slouží také k porovnání s kritériem hodnocení rizik a kritériem pro akceptaci rizik (4).

Výstupem je seznam možných incidentů, kterým je udělena priorita dle kritérií hodnocení rizik (4).

2.6.5 Ošetření rizik

Úkolem ošetření rizik je návrh opatření, které vedou ke snížení, podstoupení, vyhnutí se, nebo sdílení rizik. Vstupem pro tuto činnost jsou výstupy z analýzy incidentů, ohodnocení úrovně rizik a vyhodnocení rizik. Důležitým vstupem je i seznam všech bezpečnostních opatření, jejich specifikace, účinnost, uplatnění a stav použít (4).

Rizika můžeme ošetřit těmito způsoby:

- modifikace rizik,
- podstoupení rizik,
- vyhnutí se riziku.
- sdílení rizik (4).

2.7 Bezpečnostní opatření

Pod tímto pojmem si lze představit prostředky, které slouží pro modifikaci bezpečnostní rizik. Snižují tedy úroveň rizika hrozeb. Úroveň rizika je závislá na pravděpodobnosti výskytu hrozby, pravděpodobnosti, s jakou hrozba způsobí incident a na dopadu incidentu na organizaci (4).

Bezpečnostní opatření můžeme směrovat na tyto aspekty:

snížení nebo odstranění pravděpodobnosti výskytu hrozby – školení uživatelů, zvýšení technické složitosti opatření proti provedení útoku (4).

snížení nebo odstranění zranitelnosti aktiva – implementace firewallu napomáhá k méně zranitelnému připojení (4).

snížení nebo vyloučení dopadu na organizaci – datové zálohování, plány obnovy snižují dopad ztráty dat na akceptovatelnou míru. Pro řešení incidentů se zavádí systém auditních záznamů (4).

V praxi se často vyžívá použití několika opatření, které jsou zaměřena na jeden či více aspektů. Důležité je zvážit na jaká opatření se zaměřit. Většinou však existuje více opatření s různými zaměřeními. Na základě analýzy rizik poté vybereme jedno, nebo více opatření (4).

2.7.1 Rozdělení opatření

Na základě toho, který faktor informační bezpečnosti může hrozba ovlivnit a na tom, jaký může mít daná hrozba dopad, směřujeme k některému z cílů:

prevence – „*úplná eliminace bezpečnostní hrozby*,

minimalizace – *snížení úrovně rizika hrozby*,

detekce – včasné zjištění incidentu,

obnova – *uvedení aktiv do původního stavu před bezpečnostním incidentem*“ (4).

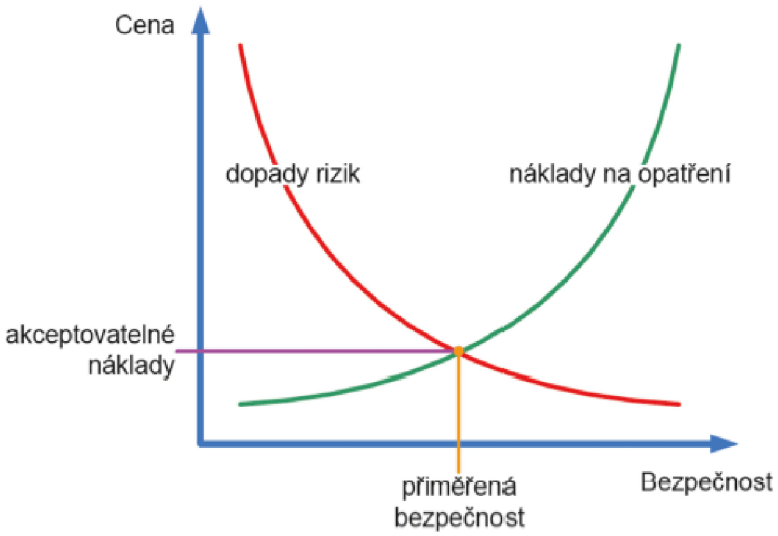
Se zvyšujícím stupněm účelu opatření se snižuje úroveň rizika. Avšak náklady na tyto opatření se zvyšují. Opět je dobré vycházet z analýzy rizik, analýzy nákladů a výnosů (4).

Typy opatření:

- fyzické,
- technické,
- administrativní,
- řídící.

2.7.2 Přiměřená bezpečnost

U návrhu bezpečnostních opatření musíme sledovat přiměřenost nákladů. Vynaložené úsilí a investice do bezpečnosti informačního systému by měly odpovídat hodnotě aktiv a míře možných rizik. Pro lepší představu si danou problematiku můžeme znázornit na následujícím obrázku (1, 4).



Obrázek č. 5: Graf přiměřené bezpečnosti (Zdroj: 4, s. 54)

2.8 Možnost řízení informační bezpečnosti

K efektivní ochraně musíme použít ucelený proces řízení. Nedílnou součástí celkového systému řízení organizace je Information Security Management System – ISMS. Tento systém má za úkol prosazovat informační bezpečnost v organizaci v těchto oblastech:

- „*řízení rizik souvisejících s informační bezpečností*,
- *organizační zajištění informační bezpečnosti*,
- *zavedení a prosazování bezpečnostní politiky a plánu zvládání rizik zajišťujících*,
- *důvěrnost, integritu a dostupnost informačních aktiv*,
- *správa informačních aktiv*,
- *bezpečnost lidských zdrojů*“,

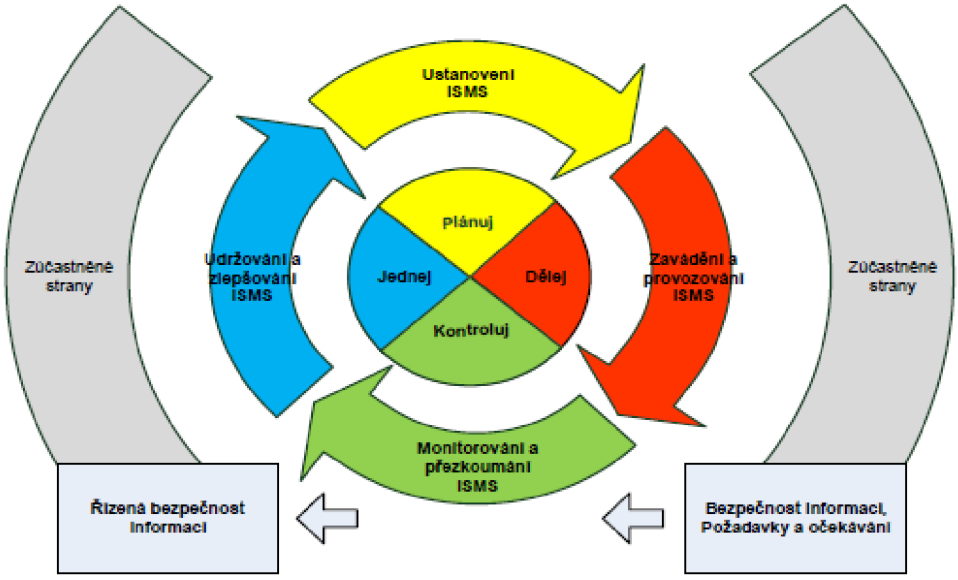
- *fyzická a areálová bezpečnost*,
- *řízení komunikací a provozu informačních systémů*,
- *řízení přístupu k informačním aktivům*,
- *pořizování, vývoj a údržba informačních systémů*,
- *reakce na bezpečnostní hrozby a bezpečnostní incidenty*,
- *zachování kontinuity činnosti organizace*,
- *dosahování souladu s právními a smluvními závazky*“ (4, str. 56).

2.9 Demingův model (PDCA cyklus)

Demingův model nebo také nazývaný PDCA cyklus je metoda postupného zlepšování kvality (výrobků, služeb, procesů, aplikací a dat). Princip této metody spočívá v opakování čtyř základních činností:

- **Plan** (plánuj – ustavení ISMS) – fáze, kdy dochází k ustavení politiky ISMS, cílů, procesů a postupů, které souvisí s managementem rizik a zlepšováním bezpečnosti, aby byly v souladu s celkovou politikou organizace,
- **Do** (dělej – zavádění a provozování ISMS) – realizace plánu. Zahrnuje testování a implementaci. Zavádíme a následně využíváme politiky ISMS,
- **Check** (kontroluj – monitorování a přezkoumání ISMS) – Ověření a porovnání výsledků oproti původnímu plánu,
- **Act** (jednej – udržování a zlepšování ISMS) – plošná implementace a zavedení do praxe. Součástí jsou i změny a úpravy (1, 3).

Součástí tohoto modelu je i dokumentace, která přesně definuje a dokumentuje každou jeho etapu. Jednotlivé procesy je třeba identifikovat, popsat a dokumentovat, řídit se na základě dokumentace a poté optimalizovat jejich průběh (1).



Obrázek č. 6: Životní cyklus ISMS (Zdroj: 4, s. 58)

2.10 Knihovna ITIL

ITIL – Information Technology Infrastructure Library je mezinárodně uznávaný standard. Je rámec, nikoliv metodika. Zajišťuje dodávku kvalitních IT služeb za přiměřené náklady, které vychází z těch nejlepších znalostí. Knihovna je rozdělena do několika částí. Tyto části se zaměřují na specifické řízení IT služeb, které odpovídá klíčovým procesům v IT oddělení. ITIL není normou, je to rámec obsahující doporučení a osvědčené postupy (Best Practices) (1, 4).

ITSM (IT Service Management) – souhrn dodávky IT služeb (IT Service Delivery) a Podpora IT služeb (IT Service Support) (1).

ITIL obsahuje a popisuje:

Definování procesů potřebných pro zajištění ITMS:

- „*stanovení cílů, vstupů, výstupů a aktivit každého procesu*,
- *stanovení rolí a jejich odpovědností v daném procesu*,
- *způsob měření kvality poskytovaných IT služeb a účinnost ITSM procesů*,
- *vzájemné vazby mezi jednotlivými procesy*,
- *postupy auditu a zásady reportingu pro každý proces*“ (1, str. 28).

Zásady pro implementaci procesů ITSM:

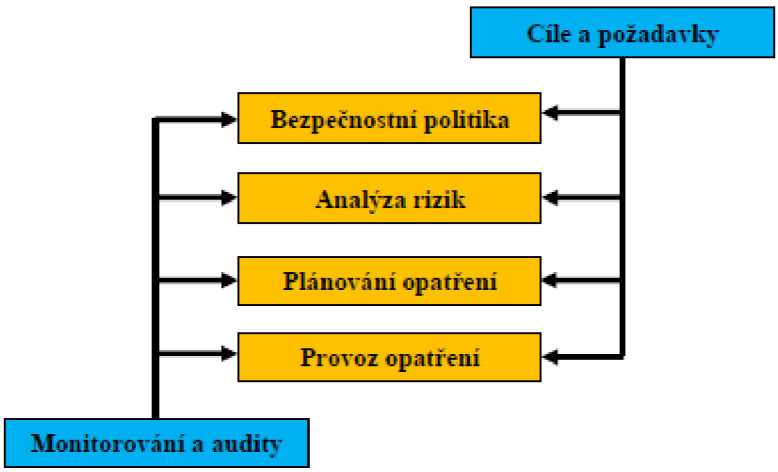
- „*přínosy každého procesu*,
- *Critical Success Factors, možné problémy a vhodná opatření*,
- *náklady na implementaci a následný provoz*,
- *zásady pro řízení podpůrné ICT infrastruktury*,
- *zásady bezpečnosti ICT infrastruktury*“ (1, str. 28).

ITIL neřeší:

- „*konkrétní podobu organizační struktury*,
- *způsob obsazení rolí konkrétními pracovními pozicemi (pouze dává doporučení, které role by měly nebo neměly být kumulovány u jedné konkrétní osoby)*,
- *podobu a obsah pracovních procedur (pracovních postupů) → neexistují žádné dva podniky, které by měly procesy ITSM podle ITIL naimplementovány naprosto stejným způsobem* ,

- *projektovou metodiku implementace ITSM (pouze dává doporučení, aby byla použita metodika PRINCE2 a s ohledem na tuto metodiku doporučuje v některých případech rámec některých kroků)*“ (1, str. 29).

Základní procesy řízení dle definice ITIL:



Obrázek č. 7: Procesy řízení bezpečnosti ITIL (Zdroj: 4, s. 64)

2.11 COBIT

Mezinárodně uznávaný rámec vytvořený asociací ISACA. Slouží pro správu a řízení ICT. Jde o soubor všeobecných praktik řízení informačních a komunikačních technologií. Cílem je propojení principů obecného řízení organizace s pravidly, které se uplatňují v prostředí IT. Rámec COBIT vychází z nejlepších zkušeností (1, 4).

Snahou metodiky je strukturovat složité systémy řízení ICT, aby struktura byla srozumitelná. Tato metodika je primárně určena top manažerům k posuzování ICT a pro provádění auditů systému řízení ICT (4).

2.12 ISMS (Information Security Management System)

Definice ISMS dle normy:

„*Information Security Management System je součástí řízení organizace, založená na přístupu k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací*“ (1).

Jedná se o dokumentovatelný systém řízení a správy informačních aktiv. Cílem je, abychom eliminovali jejich ztrátu nebo poškození. Určíme si, která aktiva mají být chráněná. Tyto aktiva si zvolíme a řídíme možná rizika. Dále zavedeme opatření s požadovanou úrovní záruk. ISMS můžeme zavádět pro společnost, informační systéme nebo jeho část nebo jen pro organizační složku společnosti (1).

Okruhy ISMS:

- „*IT bezpečnost,*
- *Komunikační bezpečnost,*
- *Personální bezpečnost,*
- *Administrativní bezpečnost,*
- *Fyzická bezpečnost,*
- *Dokumentace,*
- *Bezpečnostní funkce a mechanizmy*“ (1).

2.12.1 Etapy zavádění ISMS

Cílem zavedení ISMS je efektivní a systematické nastavení bezpečnostní opatření. Zavádění systému řízení bezpečnosti informací (ISMS) se skládá z několika kroků (1).

Kroky zavedení ISMS:

První krok

Prvním krokem je získání souhlasu vedení společnosti, abychom mohli systém nasadit. Tento souhlas je požadován normou. Zavádění ISMS probíhá od shora dolů. V případě, že vedení souhlasí, zavazuje se tím, že bude zavádění ISMS podporovat (1).

Druhý krok

V tomto kroku identifikujeme aktiva a jejich hodnotu. Je zde vyhotovena analýzy rizik, dle zvolené metodiky. Aktiva ohodnotíme z hlediska dostupnosti, důvěrnosti a integrity.

Třetí krok

Po vyhotovení analýze rizik navazuje dokument označený jako Návrh opatření. Hledáme kritická místa, zjišťujeme bezpečnostní potřeby a určujeme priority. Na základě nich vybereme vhodná opatření, které rizika vhodně a dostatečně eliminují (1).

Další variantou, jak můžeme na případná rizika reagovat, je akceptace rizik. Tento způsob se využívá v případě, že opatření by bylo extrémně finančně nákladné a míra rizika nízká. Normou je dále nařízeno, že společnost musí vytvořit dokument, který se nazývá Prohlášení o aplikovatelnosti. Tento dokument popisuje cíle opatření a jednotlivá bezpečnostní opatření. Důležité je doložit, jaké části ISMS jsou již zavedené (1).

Čtvrtý krok

Tento krok je z hlediska zavádění ISMS nepovinný. ISMS stačí pouze implementovat, není potřeba jej certifikovat. Samotná certifikace se skládá ze dvou částí. První část obsahuje certifikaci povinné dokumentace. V druhé části se kontroluje praktické zavádění ISMS (1).

2.12.2 Povinná dokumentace ISMS

V dokumentaci musí být obsažena všechna rozhodnutí vedení organizace. Činnosti musí být identifikovatelné a dohledatelné v záznamech. Všechny činnosti musejí být zaznamenány (1).

Rozsah a hranice ISMS

Jedná se o dokument, který popisuje části systému, které jsou určeny k implementaci. Jsou zde definovány hranice a rozsah ISMS.

Politika ISMS

Dokument, který určuje společnost připravenou a odpovědnou k prosazení cílů při zavádění ISMS.

2.13 Normalizační instituce

Normalizační instituce se zabývají standardizační činností i standardizací bezpečnosti IT na různých úrovních (1).

2.13.1 Pojmy

Standard – jde o dokumentovatelnou úmluvu, která obsahuje technické specifikace nebo jiná přesně stanovená kritéria. Ty se následně používají jako pravidla nebo směrnice (1).

Norma – je určité doporučení pro daný standard či řešení (1).

2.14 Normy řady 27000

Normy řady 27000 se týkají oblasti informační bezpečnosti. Můžeme se setkat s velkou řadou norem, avšak v diplomové práci budou uvedeny jen vybrané, které se týkají dané problematiky. Na základně diplomové práce je dobré se seznámit a znát tyto normy:

ČSN ISO/IEC 27000: Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti – Přehled a slovník.

Mezinárodní norma zabývající se systémem řízení informací a definuje související termíny. Použité termíny a definice v této normě se týkají definic obecně použitých norem v ISMS (1).

ČSN ISO/IEC 27001: Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti – Požadavky

Norma nám poskytuje doporučení, jak aplikovat bezpečnostní opatření (ISO/IEC 27002), v rámci procesu ustavení, provozu, údržby a zlepšování systému managementu bezpečnosti informací. Norma prosazuje procesní přístup k řešení ISMS. Je zde zaveden Demingův model (PDCA cyklus) – Plánuj, Dělej, Kontroluj, Jednej (1).

Hlavní část normy pojednává o požadavcích na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci. Dále jsou zde

specifikovány požadavky na výběr a zavedení bezpečnostních opatření, které chrání informační aktiva. Norma ve svých přílohách dále obsahuje cíle a opatření (1).

ČSN ISO/IEC 27002: Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti – Soubor postupů

Jde o sbírku norem, která obsahuje nejlepší opatření, bezpečnostních praktik a postupů. Norma obsahuje 35 cílů opatření, které chrání informační aktiva z pohledu důvěrnosti, dostupnosti a integrity. Norma dále popisuje nejlepší praktiky, které vedou k zajištění informační bezpečnosti. Není jasně specifikováno normou, která opatření by měly být aplikována, toto rozhodnutí je ponecháno na organizaci. Vhodná opatření jsou vybrána na základě analýzy rizik. Implementace je závislá na konkrétní situaci organizace. Norma je tedy široce aplikovatelná a uživatelům umožňuje značnou flexibilitu. Na základě normy pak můžeme rychle a snadno určit stav bezpečnosti informací a současně vytvořit východiska pro zlepšení (1, 5).

ČSN ISO/IEC 27003: Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací

Norma obsahuje doporučení pro ustanovení a implementaci ISMS v souladu s normou ISO/IEC 27000. Norma je obecně použitelná pro všechny typy organizací, které zavádějí ISMS. Je zde vysvětlen proces návrhu a implementace. Proces plánování je normou popsán pěti etapách (1).

ČSN ISO/IEC 27004: Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření

Doporučení pro vývoj a používání metrik. Měří účinnost zavedení ISMS a účinnost opatření. Jsou zde zahrnuty procesy rozvoje metrik a měření, analýza dat a hlášení výsledků měření. Přílohy normy obsahují příklady konceptů měření pro určitá opatření či procesy ISMS (1).

ČSN ISO/IEC 27005: Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací

Obsahem normy je doporučení pro řízení rizik bezpečnosti informací s ohledem na požadavky ISMS. Norma nenabízí konkrétní metodiku pro řízení rizik bezpečnosti informací. Organizace si sama volí, jaký způsob si k řízení rizik zvolí. Je určena pro manažery a odpovědné pracovníky, kteří jsou zodpovědní za řízení rizik. Může být aplikovatelná na všechny typy organizací, které chtějí řídit rizika (1, 5).

ČSN ISO/IEC 27006: Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

Jsou zde specifikovány požadavky a doporučení pro orgány, které provádějí audit a certifikaci ISMS. Norma je určena k procesu akreditace certifikačních orgánů, které poskytují certifikaci ISMS (1).

2.15 Kybernetická vyhláška

Vyhláška č. 82/2018 Sb.

„*Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*“ (6).

Vyhláška je stanovena Národním úřadem pro kybernetickou a informační bezpečnost.

Vyhláška upravuje:

- „*strukturu a obsah bezpečnostní dokumentace*,
- *obsah a rozsah bezpečnostních opatření*,
- *typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů*,
- *náležitosti a způsob hlášení kybernetického bezpečnostního incidentu*,
- *náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,*
- *vzor oznámení kontaktních údajů a jeho formu,*
- *způsob likvidace dat, provozních údajů, informací a jejich kopií“* (7).

První část – Úvodní ustanovení

Vymezení pojmů a úpravy (systém řízení bezpečnosti, aktivum, riziko a řízení rizika, hrozba, zranitelnost, bezpečnostní politika, atd.) (7).

Druhá část – Bezpečnostní opatření

- Organizační opatření – HLAVA 1,
- Technické opatření – HLAVA 2,
- Bezpečnostní politika a bezpečnostní dokumentace – HLAVA 3 (7).

Třetí část – Kybernetický bezpečnostní incident

„*Typy, kategorie, forma a náležitosti*“ (7).

Čtvrtá část – Reaktivní opatření a kontaktní údaje

„*Typy, kategorie, forma a náležitosti*“ (7).

Pátá část - Účinnost

Součástí kybernetické vyhlášky jsou také přílohy, které obsahuji stupnici pro hodnocení rizik, zranitelnost a hrozby, likvidaci dat, obsah bezpečnostní politiky a bezpečnostní dokumentaci, formuláře hlášení a oznámení (7).

3 ANALÝZA SOUČASNÉHO STAVU

V této části kapitoly popíši danou vybranou základní školu. Úvodní část kapitoly popisuje základní informace o základní škole, jako je organizační struktura, procesy, informační systém, role a odpovědnosti. Dále bude zhodnocen současný stav z pohledu bezpečnosti a provedena analýza bezpečnosti. Bude zde zhodnocena současná síťová infrastruktura, technické a programové vybavení. V závěru bude provedeno celkové zhodnocení zjištěných poznatků a informací.

3.1 Popis organizace

Základní škola si nepřála být jmenována. V diplomové práci tedy nebude uveden název ani možné identifikující znaky, které by mohly základní školu identifikovat.

Škola se nachází v Jihomoravském kraji. Základní škola je příspěvkovou organizací, jejíž zřizovatelem je Statutární město Brno. Celková kapacita školy je 18 tříd a 8 odborných učeben. Školu navštěvuje přibližně 400 žáků z celkové maximální kapacity 540.

3.2 Popis budovy

Základní škola byla uvedena do provozu v roce 1985. Je situována v oblasti sídliště poblíž centra Brna. Škola má tři podlaží – suterén, 1. patro, 2, patro. Ve všech podlažích se nacházejí místnosti, které jsou školou využívány (školní třídy, specializované učebny, školní jídelna, tělocvična, kabinety, kanceláře, školní družina). Součástí pozemku je i školní dvůr.

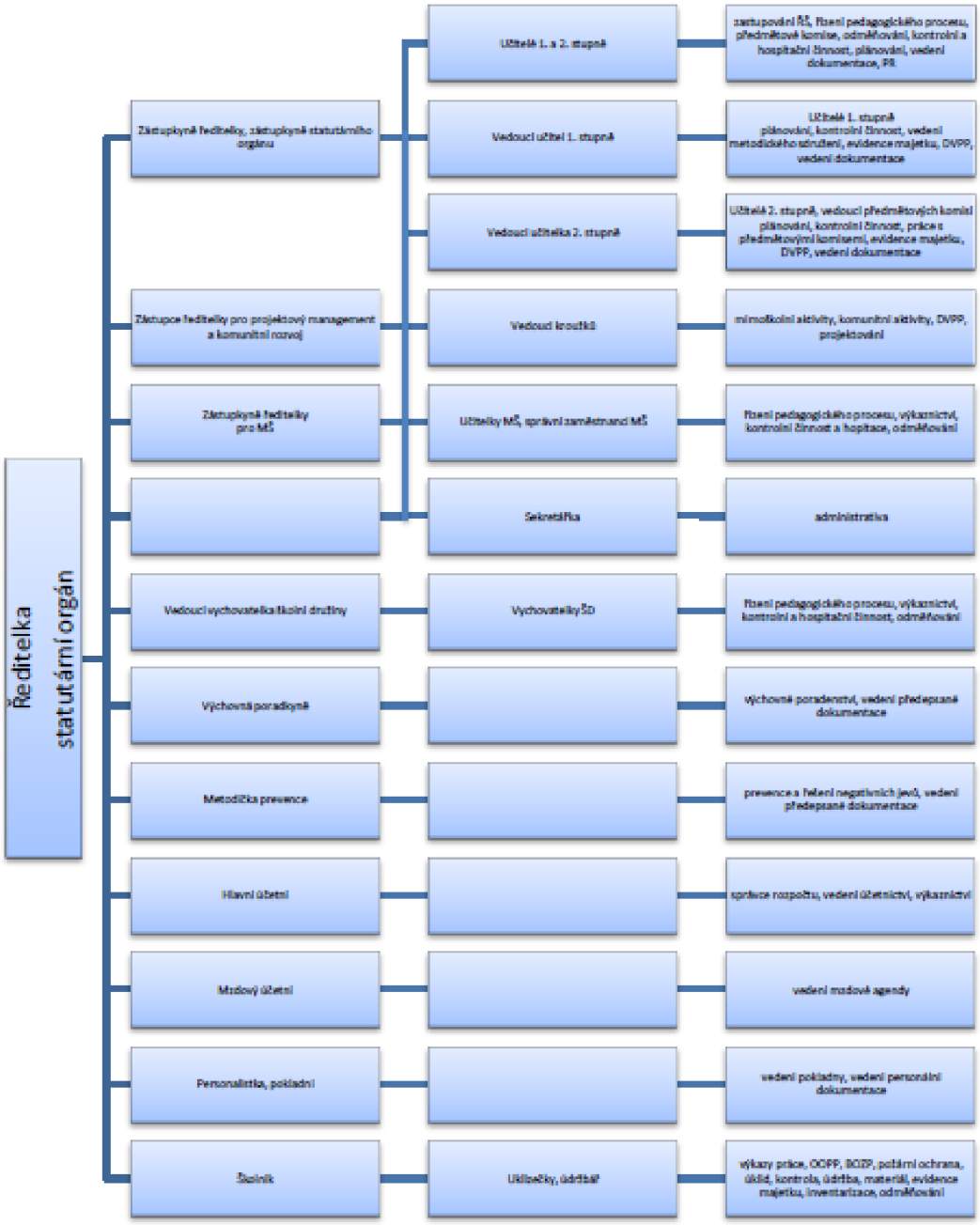
Pozemek školy je ohraničen oplocením. K dispozici jsou dva vchody. Hlavní vchod je využíván studenty. Vchod je zabezpečen dveřmi s mechanickým zámkem. Tento vchod také využívají návštěvníci školy. Druhý vchod je umístěn na druhé straně budovy. Je přístupný přes školní dvůr. Tento vchod využívají pouze zaměstnanci školy.

3.3 Organizační struktura

Ve vedení základní školy je ředitelka potažmo statutární orgán. Pod ní jsou v organizační struktuře:

- zástupkyně ředitelky, zástupkyně statutárního orgánu,
- zástupce ředitelky pro projektový management a komunitní rozvoj,
- zástupkyně ředitelky pro MŠ,
- vedoucí vychovatelka školní družiny,
- výchovná poradkyně,
- metodička prevence,
- hlavní účetní,
- mzdový účetní,
- personalistika, pokladní,
- školní.

Tito zaměstnanci mají pod sebou v organizační struktuře ostatní zaměstnance školy. Těmi jsou učitelé 1. a 2. stupně, vedoucí učitel 1. stupně, vedoucí učitelka 2. stupně, vedoucí kroužků, učitelky MŠ, sekretářka, vychovatelky školní družiny, uklízečky. V současné době je ve škole 45 zaměstnanců. Mimo tyto zaměstnance školy zde také působí externí zaměstnanci. Mezi tyto zaměstnance patří i IT pracovník, který spolupracuje s vedením školy na technickém zabezpečení a stará se o plynulý a bezpečný chod sítě.



Obrázek č. 8: Organizační struktura (Zdroj: vlastní zpracování)

3.4 Odpovědnost

Vedení základní školy (ředitelka a odpovědné osoby), by měli zavést systém řízení bezpečnosti informací. Měly by být stanoveny role a odpovědnosti konkrétním osobám. V současné době není zavedeno.

3.5 Popis místností

V této kapitole budou popsány důležité místnosti z pohledu informační bezpečnosti. Bude se jednat o popis serverovny, počítačové učebny a odborných učeben.

3.5.1 Serverovna

Serverovna se nachází v prvním patře školy, v místnosti vedle ředitelny. Místnost je zabezpečena vstupními dveřmi a mechanickým zámkem. Klíčem od této místnosti disponuje ředitel školy a zástupce, který je současně i správcem školní sítě.

Jak je patrné z obrázku. Jedná se o běžnou místnost, která není klimatizována. Je zde nainstalován větrák, který napomáhá k odvětrávání. V místnosti se nachází server HP Proliant. Ten je virtualizovaný pomocí virtualizačního SW ESXi VMware 5.5.0 na několik logických serverů. Dále se v místnosti nachází diskové pole Synology DS712+, MikroTik, UPS zařízení, switch, který není managementovaný, Unifi kontroler a elektronický zabezpečovací systém (EZS).

Server, který se ve serverovně nachází, je zde již delší dobu. Disponuje operačním systémem Windows Server 2012. Na serveru běží DHCP a DNS, mimo to zde není spuštěna žádná další služba. Firewall je na serveru spuštěný v rámci jeho operačního systému. Data jsou ukládána na diskovém poli Synology. Data jsou na diskové pole ukládána pomocí metody RAID 1 (data jsou ukládány na síťový disk, který je rozdělen na dva disky v poli konfigurovaném jako RAID 1). Veškerá data jsou několikrát ročně

zálohována na externí disky, které jsou po zálohování odpojeny a uloženy u školního správce sítě v uzamčené skříně.

Jak je patrné z obrázku v serverovně se nachází i telefonní ústředna. O její provoz se stará externí společnost. Telefonní ústředna není součástí řešení diplomové práce.

Obrázek č. 9: Serverovna (Zdroj: vlastní zpracování)

3.5.2 Počítačová učebna

Počítačová učebna se nachází v prvním patře školy. Nachází se zde 20 stolních počítačů, které jsou určeny pro studenty ke studijním účelům. V počítačové učebně je umístěn rack, kde jsou umístěny dva managementované switche. Na počítačích je nainstalován operační systém Windows 7, dále jsou zde grafické programy – Zoner Callisto, sada kancelářských programů MS Office 2016 Standard

Žáci se nedisponují přihlašovacími údaji k počítačům, které jsou umístěny v počítačové učebně. Po zapnutí počítače se žákům zpřístupní pracovní plocha na daném počítači. Pedagogové se k počítačům přihlašují pod svým heslem, které jim bylo přiděleno školním správcem sítě. Hesla k počítačům a bezdrátové sítě jsou odlišné.

Počítače jsou chráněny antivirovým programem Defender. Na některých zařízeních je nainstalován Avast.

3.5.3 Učebny pro běžnou výuku

V učebnách, kde probíhá klasická výuka, jsou dataprojektory. Každý vyučující disponuje svým školním notebookem, na kterém je nainstalován operační systém Windows 7. V nedávně době byly zakoupeny nové notebooky, které disponují operačním systémem Windows 10. Všechna zařízení jsou chráněna antivirovým programem Windows Defender, na některých zařízeních je nainstalován Avast.

3.5.4 Kanceláře

V ředitelně a kancelářích jsou zaměstnanci (ředitelka, zástupce, sekretářka) využívány stolní počítače. Nainstalován je zde operační systém Windows 7. Sada kancelářských programů MS Office Standard 2016. Stejně jako na všech zařízeních jsou nainstalovány antivirové programy Defender a Avast.

3.6 Popis ICT infrastruktury

3.6.1 Hardware

Jak bylo zmíněno v předcházející kapitole. Škola disponuje stolními počítači, notebooky, dataprojektory, stanicí typu server, switchi, přístupovými body.

Server

Technické specifikace:

HP Proliant ML 310c Gen 8 v2 - CPU 3,3392 GHz

Intel Xcon – CPU E3 – 1240 v3 – CPU 3,4 GHz; RAM 16GB

Diskové pole

Synology DS712

- Operační paměť: 1 GB,
- Procesor: CPU 1,8 GHz,
- Rozhraní: 3x USB 2.0,
- Rozhraní: SATA,
- Síťové protokoly: CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, VPN,
- Konfigurace: DiskStation Manager, webové management rozhraní (10).

MikroTik

MikroTik RB 1100AHx2

- Operační paměť: 2048 MB,
- Procesor: PowerPC P2020 dual core 1066MHz,
- Rozhraní: RJ-45 (13 portů),
- Podpora IPv6: ano (11).

3.7 Komunikační a síťová infrastruktura

Datová síť je realizována pomocí kabelů UTP kategorie 5e. Jejich maximální přenosová rychlost je 1000 MBit/s. Kabelové trasy jsou vedeny pomocí lišt nebo v podhledech. Kabely jsou realizovány z bezhalogenových materiálů (LSOH), z důvodu vysokého výskytu osob v budově. Kabeláž neobsahuje žádné bezpečnostní prvky nultého, ani prvního stupně.

Struktura sítě

V přízemí školní budovy se nachází v podhledu v datovém rozvaděči modem. Z něj jsou kabelovými trasami vedeny kabely do prvního patra budovy, kde se nachází MikroTik. Na MikroTiku není nainstalováno DHCP ani DNS, pouze firewall. Odtud jsou vedeny rozvody do jednotlivých přístupových bodů ve škole. Celkem se zde nachází 9 přístupových bodů (Ubiquiti – Long Range). Ty jsou rozmístěny tak, aby byl pokryt požadovaný prostor. Na přístupových bodech je aktivován automatický roaming, který umožňuje „přebírat“ připojené uživatelé, kteří se pohybují po budově. Přístupové body jsou řízené pomocí zařízení Ubiquiti UniFi Controller.

Rozdělení uživatelských skupin

Školní bezdrátová síť je rozdělena do dvou skupin:

Škola 2019 – Tato bezdrátová síť je určena pro žáky školy v počítačové učebně. Slouží studentům k výuce v případě, že využívají svůj vlastní notebook. V současné době žáci nemají možnost se k bezdrátové síti připojit, jelikož jsou generována nová hesla.

ICTkouch – Sít určená pro všechny zaměstnance školy. Ti se do školní sítě přihlašují pod společným heslem.

Radius server nebo jiný způsob autentizace zatím není na škole nasazen. Do budoucna je v plánu vybudovat studentskou bezdrátovou síť, která bude oddělena od infrastruktury. V současné době není možné vytvořit VLAN. A to především z důvodu použitých aktivních prvků, které nejsou managementované a nemají možnost VLAN.

3.8 Software

Na základní škole je studenty využíván balíček kancelářských MS Office 2016 Standard a Zoner Callisto. Vyučující využívají především školní systém Bakaláři.

3.8.1 Informační systém

Základní škola využívá pro řízení agendy informační systém Bakaláři. Tento informační systém bude detailně popsán v následující kapitole. Interní komunikace mezi zaměstnanci školy je realizována pomocí MS Outlook. Každý pedagogický a výchovný zaměstnanec má ve svém kabinetu telefon. Telefonní síť není v kompetenci externího IT pracovníka ani správce školní sítě. V diplomové práci nebude tato problematika dále řešena.

Informační systém Bakaláři

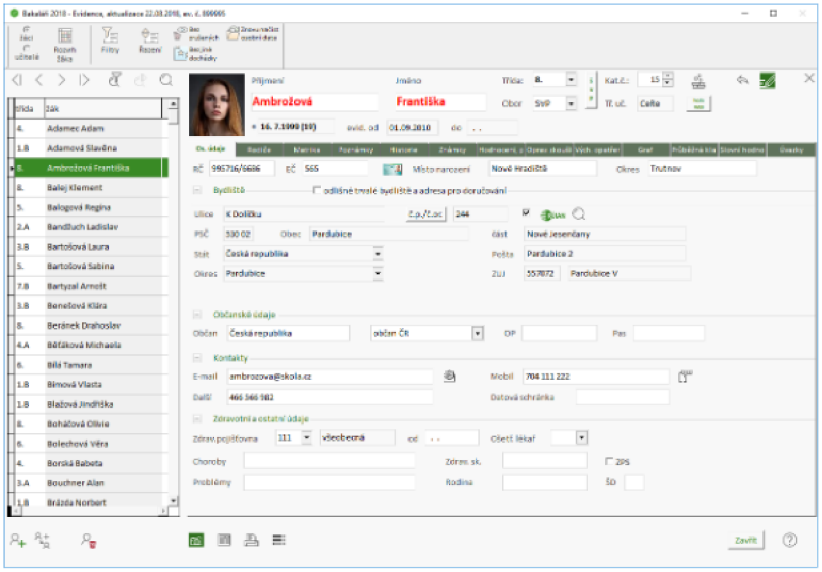
Základní škola využívá pro svůj chod informační systém Bakaláři. Ten napomáhá zvládat organizaci, každodenní administrativu a napomáhá ke komunikaci mezi školou a rodinou. Provoz je uzpůsoben na míru dané základní škole. V současné době je nasazena aktuální verze programu – Bakaláři 2019.

Popis informačního systému

Informační systém Bakaláři obsahuje řadu modulů a doplňkových funkcí, které napomáhají škole ulehčit agendu. Program je určen nejen pro management školy, ale i jednotlivé pracovníky, rodiče a žáky.

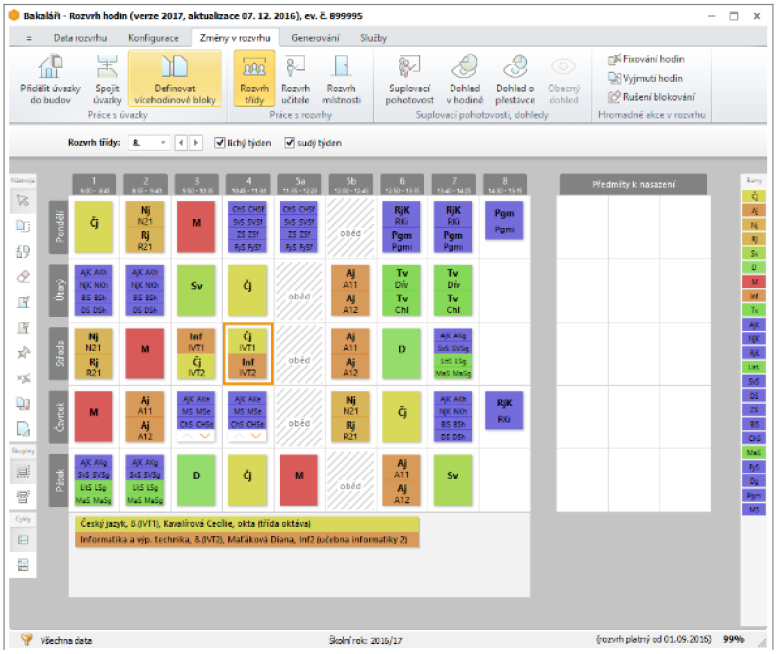
Informační systém nabízí širokou škálu doplňkových modulů. Základní školy využívá pro svůj chod tyto moduly:

Evidence žáků a zaměstnanců, školní matrika – jsou zde obsaženy osobní údaje žáků, průběžná klasifikace.



Obrázek č. 10: Informační systém Bakaláři (Zdroj: 12)

Rozvrh – program, který napomáhá řešit možné kolize ve výuce, vyhledává možné přesuny a výměny vyučujících hodin.



Obrázek č. 11: Informační systém Bakaláři - Rozvrh (Zdroj: 13)

V současné době je software Bakaláři 2019 uložen na SQL serveru na cloudu poskytovatele. Server je umístěn v datovém centru s veškerými bezpečnostními prvky.

3.9 Směrnice ICT

Na základní škole není sepsána interní směrnice pro ICT. Žáci školy jsou seznámení s řády učebny a následně podepisují souhlas, že byli ponaučeni a s pravidly souhlasí.

3.10 Zaznamenávání provozu na síti

Síťový provoz je zaznamenáván do logů na řadiči. Data jsou ukládána na SD kartu. Řadič je umístěn v technické místnosti, která je zabezpečena mechanickým zámkem.

3.11 Bezpečnostní stav organizace

V této kapitole bude popsán současný bezpečnostní stav základní školy. Celá kapitola bude rozdělena do několika podkapitol, které budou analyzovat jednotlivé bezpečnostní oblasti.

3.11.1 Objektová bezpečnost

Objektová bezpečnost základní školy je řešena pomocí kontrolovaného přístupu do budovy, alarmového systému a videotelefonem (v případě, že je hlavní vchod uzavřen), který je umístěn u hlavního vchodu budovy. Celý areál školy je oplocen. Klíče od vchodu do budovy mají všichni pedagogičtí pracovníci školy a provozní úsek. Žáci do školy vstupují hlavním vchodem, který je před začátkem vyučování odemčen. Školní areál disponuje dvorem, kde jsou zřízena parkovací místa. Školní dvůr je zabezpečen příjezdovou bránou. Která je uzamčena a je otevřena pouze na vyžádání. Klíčem od této brány disponují zaměstnanci školy.

Obrázek č. 12: Zvonek s kamerou umístěný u hlavního vchodu do školy (Zdroj: vlastní zpracování)

Všechny místnosti a učebny školy jsou opatřeny dveřmi s mechanickým zámkem. Klíče od těchto místností mají pedagogičtí zaměstnanci a provozní úsek. Zaměstnanci jsou poté povinni po skončení pracovní doby tyto místnosti opět uzamknout a zabezpečit.

3.12 Bezpečnostní analýza

V této části kapitoly se zaměřím na zhodnocení bezpečnostních opatření na základní škole. Analýzu provedu na základě „Pomůcky k auditu bezpečnostních opatření podle vyhlášky o kybernetické a informační bezpečnosti č. 82/2018 Sb. Jedná se o podpůrný materiál Národního úřadu pro kybernetickou bezpečnost (NÚKIB). Analýzu jsem provedl kompletně, avšak pro účely diplomové práce jsem vybral pouze konkrétní části, které se vztahují k dané problematice. Celé asistované zhodnocení je obsaženo v příloze diplomové práce.

Šablona, podle které byla analýzy zpracována:

Požadavek	
Stav	
Komentář	

Stav je definován třemi stavy:

Aplikováno
Částečně aplikováno
Neplikováno
Nerelevantní

Systém řízení bezpečnosti informací (ISMS):

Požadavek	Stanovení rozsahu ISMS
Stav	Nezavedeno
Komentář	

Požadavek	Jsou vytvořeny, schváleny a zavedeny bezpečnostní politiky v oblasti ISMS, zavedena příslušná bezpečnostní opatření
Stav	Nezavedeno
Komentář	

Požadavek	Zaveden proces vyhodnocování vhodnosti bezpečnostních opatření.
Stav	Nezavedeno
Komentář	

Požadavek	Audit kybernetické bezpečnosti
Stav	Nezavedeno
Komentář	

Požadavek	Řízení provozu a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti spojené se systémem řízení bezpečnosti a řízením rizik
Stav	Nezvedeno
Komentář	

3.12.1 Shrnutí asistovaného zhodnocení

Jak bylo zmíněno na začátku kapitoly, asistované zhodnocení bylo v organizace provedeno v plném rozsahu, ale pro účely a rozsah diplomové práce byly vybrány jen relevantní informace, které se shodují s předmětem řešení diplomové práce.

Z celkové analýzy vyplývá, že organizace splňuje 18 požadavků (15%), částečně aplikováno je 29 požadavků (24%) a 74 požadavků není aplikováno (61%). Na obrázku (Obr. 12) je znázorněný koláčový graf, který celou analýzu zobrazuje i z grafického hlediska.

Obrázek č. 13: Grafické zhodnocení analýzy (Zdroj: vlastní zpracování)

3.13 Souhrn asistovaného zhodnocení k opatřením ISMS

Na základě provedené analýzy byla sestavena tabulka, která mapuje jednotlivá opatření ISMS. Je zde obsažen souhrn informací, které daná organizace splňuje či nikoliv. Opatření jsou převzata z normy ČSN ISO/IEC 27001. K jednotlivým opatřením je přiřazen stav - aplikováno, částečně aplikováno (v práci jen částečně), neaplikováno, nerelevantní. V práci bude uvedena pouze část souhrnného zhodnocení. Kompletní zhodnocení je v příloze.

Tabulka č. 1: Souhrnná analýza opatření ISMS (vlastní zpracování dle: 3)

A.5	**Politiky a bezpečnosti informací**	
A.5.1	Směřování bezpečnosti informací vedením organizace	
A.5.1.1	Politiky pro bezpečnost informací	Neaplikováno
A.5.1.2	Přezkoumání politik pro bezpečnost informací	Neaplikováno
A.6	**Organizace bezpečnosti informací**	
A.6.1	**Interní organizace**	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	Neaplikováno
A.6.1.2	Princip oddělení povinností	Neaplikováno
A.6.1.3	Kontakt s příslušnými orgány a autoritami	Neaplikováno
A.6.1.4	Kontakt se zájmovými skupinami	Neaplikováno
A.6.1.5	Bezpečnost informací v řízení projektů	Neaplikováno
A.6.2	**Mobilní zařízení a práce na dálku**	
A.6.2.1	Politika mobilních zařízení	Neaplikováno
A.6.2.2	Práce na dálku	Neaplikováno
A.7	**Bezpečnost lidských zdrojů**	
A.7.1	**Před vznikem pracovního vztahu**	
A.7.1.1	Prověřování	Částečně
A.7.1.2	Podmínky pracovního vztahu	Aplikováno

3.14 Požadavky organizace

Hlavním požadavkem vedení organizace je zvýšení bezpečnostního povědomí. A to především z důvodu využívání ICT technologií ve vyšší míře, než tomu bylo doposud. Dalším důvodem je především možnost potencionálních incidentů na škole. Dalšími kroky, které chce vedení zavést je:

- zaměstnanci budou dodržovat základní pravidla informační bezpečnosti,
- pravidelné proškolování pověřených osob,
- zaměstnanci školy by měli lépe zacházet s aktivy organizace,
- každý zaměstnanec by měl znát své povinnosti a odpovědnosti,
- zaměstnanci by měli znát pravidla bezpečného používání informačních a komunikačních technologií,
- zaměstnanci by měli být seznámeni s následky nedodržení informační bezpečnosti,
- zabezpečení stolní počítačů a notebooku,
- oddělení síťového provozu.

Dalšími požadavky vedení školy je minimální časová náročnost zavedení opatření a dodržení rozpočtu 120 000 Kč.

3.15 Souhrn analýzy současného stavu

Na základě provedené analýzy současného stavu v dané základní škole jsem zhodnotil současný stav, procesy, odpovědnosti, síťovou infrastrukturu, fyzické i objektové zabezpečení, hardwarové i softwarové vybavení, směrnice, data, informační systém. V současné době se ve škole nachází hned několik slabých míst, které je potřeba změnit, aby byla zajištěna celková informační bezpečnost. Jedním z kroků je rozdělení školní sítě do VLAN. K tomu bude zapotřebí, aby škola zainvestovala do odpovídajících hardwarových síťových prvků. Dalším krokem je zabezpečení školních počítačů jednotným antivirovým programem. Měli by být dále jasně stanoveny odpovědné osoby za dané úkoly. Tato odpovědné osoby by měli být více vzdělávány a proškolovány v dané problematice. Této problematice se budu věnovat v následující kapitole, kde budou navrženy návrhy na opatření.

4 VLASTNÍ NÁVRH ŘEŠENÍ

Tato kapitola bude pojednávat o samotném návrhu řešení, který povede ke zlepšení stávajícího stavu na dané základní škole. Při návrhu je vycházeno z provedené analýzy současného stavu, norem a směrnic.

Kapitola je rozdělena do několika částí. V úvodu kapitoly je vymezen rozsah a hranice práce, dále ohodnotím a identifikuji aktiva. Následně bude provedena analýza rizik, jejich zhodnocení a návrhy pro snížení dopadu rizik.

4.1 Rozsah a hranice

Základní škola neplánuje v současné době zavádět systém řízení bezpečnosti informací (ISMS) ani žádat o certifikaci. Hlavním cílem je vybudování bezpečnostního povědomí, zavedení bezpečnostních opatření a předcházení potencionálním rizikům. Dalším krokem je zavedení jednotného antivirového programu pro všechny stanice na dané škole.

4.2 Analýza rizik

Aby mohla být realizována analýza rizik, musí být nejdříve identifikována a ohodnocena aktiva. Jedná se o ty aktiva, kterých se mohou případná rizika týkat. Analýzu rizik začnu nejdříve tím, že ohodnotím aktiva, vyhodnotím hrozby a zranitelnost. Výstupem je vyhodnocení rizik.

4.2.1 Identifikace a hodnocení aktiv

V prvním kroku je potřeba aktiva identifikovat. Aktiva jsem rozdělil o čtyř základních skupin:

- informační aktiva,
- hardwarová aktiva,
- softwarová aktiva,
- služby.

Identifikace aktiv probíhala společně s pověřenou osobou.

Klasifikace aktiv

Pro vyhodnocení aktiv využiji klasifikační schéma (viz Tabulka 1).

Tabulka č. 2: Klasifikační schéma (Zdroj: vlastní zpracování)

Klasifikační stupeň	Klasifikační kritérium	Riziko pro organizaci
1	Žádný dopad na organizaci	Bezvýznmné
2	Zanendbatelný dopad na organizaci	Akceptovatelné
3	Potíže či finanční ztráty	Nízké
4	Vážné potíže či podstatné finanční ztráty	Nežádoucí
5	Existenční potíže	Nepřijatelné

Tuto kvalifikaci je nutné provést zvlášť pro všechny tři atributy (integrita, důvěrnost, dostupnost). Hodnotu aktiva jsem vypočítal na základě vzorce:

$$Hodnota\ aktiva = \frac{Důvěrnost + Integrita + Dostupnost}{3}$$

Tabulka č. 3: Identifikace a ohodnocení aktiv (Zdroj: vlastní zpracování)

Skupina aktiv	Aktivum	Dustupnost	Důvěrnost	Integrita	Hodnota
Informační aktiva	Data o zaměstnancích	2	3	3	3
	Data o studentech	3	4	4	4
	Zálohování dat	5	5	5	5
	Administrativní data	2	3	2	2
Hardwarová aktiva	Stolní počítače	2	3	2	2
	Notebooky	3	3	3	3
	Mobilní zařízení	2	3	3	3
	Tiskárny	2	1	1	1
	Server	3	4	3	3
	Aktivní síťové prvky	4	5	4	4
	Pasivní síťové prvky	4	5	4	4
	Diskové pole	5	5	5	5
	Firewall	3	4	3	3
Softwarová aktiva	Informační systém - Bakaláři	4	5	5	5
	Operační systém	4	3	3	3
	Účetní SW	3	4	4	4
Služby	Internetové připojení	3	3	4	3
	Elektronická pošta	4	4	4	4
	Webové stránky	4	3	2	3
	Zálohování	4	5	4	4

Z tabulky je patrné, že aktiva s největší hodnotou pro organizaci jsou data o zaměstnancích a studentech, interní dat, data uložená na server, zálohování, aktivní a pasivní prvky sítě, firewall.

4.2.2 Identifikace hrozeb

V dalším kroku je zapotřebí stanovit hrozby, které mohou na danou organizaci působit a určit pravděpodobnosti jejich výskytu. Jednotlivým hrozbám je přiřazena pravděpodobnost výskytu a příklad zranitelnosti.

Pravděpodobnost a vznik hrozby je znázorněn na klasifikačním schématu (viz Tabulka 4):

Tabulka č. 4: Klasifikační schéma (Zdroj: vlastní zpracování)

Klasifikace pravděpodobnosti	Ohodnocení
Velmi nízká pravděpodobnost	1
Nízká pravděpodobnost	2
Střední pravděpodobnost	3
Vysoká pravděpodobnost	4
Velmi vysoká pravděpodobnost	5

V další tabulce jsou uvedeny a identifikovány hrozby, které se mohou, vyskytnou dle normy ČSN ISO/IEC 27005 (viz Tabulka 4). V tabulce jsou ohodnoceny i zranitelnosti, analogicky, jako u předcházející tabulky (Tabulka 3).

Tabulka č. 5: Identifikace hrozeb a jejích pravděpodobnost (Zdroj: vlastní zpracování)

Kategorie hrozby	Typ hrozby	Ohodnocení
Fyzické poškození	Požár	2
	Poškození vodou	2
	Zničení zařízení nebo médií	3
Přírodní události	Meterologický jev	1
	Povodeň	1
Ztráta základních služeb	Selhání klimatizace nebo dodávky vody	2
	Přerušení dodávky elektřiny	3
	Selhání telekomunikačního zařízení	3
Ohrožení informací	Vzdálená špionáž	1
	Odposlech	1
	Krádež médií nebo dokumentů	3
	Krádež zařízení	3
	Vyzrazení	4
	Falšování pomocí aplikačního vybavení	3
Technické selhání	Selhání zařízení	4
	Chybové fungování zařízení	3
	Přetížení informačního systému	2
	Chyba údržby	3
Neoprávněné činnosti	Neoprávněné použití zařízení	3
	Podvodné kopírování aplikačního programového vybavení	1
	Poškození dat	2
	Nezákonné zpracování dat	1
Ohrožení funčknosti	Chyba v používání	3
	Zneužití oprávnění	4
	Falšování práv	2
	Odepření činností	3
	Nedostatek personálu	4

4.2.3 Matice zranitelnosti

Pomocí matice zranitelnosti můžeme vyjádřit pravděpodobnost hrozby v závislosti na hodnotě aktiva. Pro vyhodnocení je, využito klasifikační schéma viz Tabulka 5. V příloze je uvedena celá matice zranitelnosti. V práci je jen uvedena její část pro informační aktiva.

Tabulka č. 6: Klasifikační schéma zranitelnosti (Zdroj: vlastní zpracování)

Kritérium pro zranitelnosti	Ohodnocení
Velmi nízká	1
Nízká	2
Střední	3
Vysoká	4
Velmi vysoká	5

Tabulka č. 7: Matice zranitelnosti (Zdroj: vlastní zpracování)

ZRANITELNOST [V]		Informační aktiva				
		AKTIVUM	Data o zaměstnancích	Data o studentech	Zálohování dat	Administrativní data
		A	3	4	5	2
HROZBA	T					
Požár	2					
Poškození vodou	2					
Zničení zařízení nebo médií	3					
Meterologický jev	1					
Povodeň	1					
Selhání klimatizace nebo dodávky vody	2					
Přerušení dodávky elektřiny	3		4	4	4	3
Selhání telekomunikačního zařízení	3		4	4	4	3
Vzdálená špionáž	1		4	4	4	3
Odposlech	1					
Krádež médií nebo dokumentů	3		3	4	1	2
Krádež zařízení	3					
Vyzrazení	4		3	3	3	3
Falšování pomocí aplikačního vybavení	3		2	3	3	2
Selhání zařízení	4					
Chybové fungování zařízení	3					
Přetížení informačního systému	2		4	4	2	2
Chyba údržby	3					
Neoprávněné použití zařízení	3					
Podvodné kopírování aplikačního programového vybavení	1					
Poškození dat	2		3	3	3	3
Nezákonné zpracování dat	1		3	3	3	3
Chyba v používání	3		3	3	3	2
Zneužití oprávnění	4		3	3	3	3
Falšování práv	2		3	3	2	2
Odepření činností	3					
Nedostatek personálu	4					

4.2.4 Matice úrovně rizik

Pro určení úrovně rizika R využijeme tří parametrovou metodu. Jak je, již z názvu patrné metoda je složena ze tří parametrů:

- A – hodnota aktiva
- T – pravděpodobnost hrozby
- V – zranitelnost aktiva

Po vynásobení všech tří parametrů získáme úroveň rizika.

Vzorec pro určení úrovně rizika:

$$R = A * T * V$$

Úroveň rizika klasifikujeme pomocí klasifikačního schématu úrovně rizika:

Tabulka č. 8: Klasifikační schéma úrovně rizika (Zdroj: vlastní zpracování)

Klasifikační kritérium úrovně rizika	**Ohodnocení**
Bezvýznamné riziko	0-10
Akceptovatelné riziko	11-20
Nízké riziko	21-30
Nežádoucí riziko	31-60
Nepřijatelné riziko	61-125

Příklad výpočtu úrovně rizika:

Přerušení dodávky elektřiny [T] - 3

Data o zaměstnancích [A] – 3

Zranitelnost aktiva [Z] – 4

Dosazení do vzorce:

$R = A * T * V = 3 * 3 * 4 = \underline{\underline{36}}$

V práci bude znázorněna část matice úrovně rizik pro informační aktiva. Celá matice bude v plném rozsahu v příloze.

Tabulka č. 9: Matice úrovně rizik (Zdroj: vlastní zpracování)

ZRANITELNOST [V]		AKTIVUM	Data o zaměstnancích	Data o studentech	Zálohování dat	Administrativní data
		A	3	4	5	2
HROZBA	**T**					
Požár	2					
Poškození vodou	2					
Zničení zařízení nebo médií	3					
Meterologický jev	1					
Povodeň	1					
Selhání klimatizace nebo dodávky vody	2					
Přerušení dodávky elektřiny	3		36	48	60	18
Selhání telekomunikačního zařízení	3		36	48	60	18
Vzdálená špionáž	1		4	16	20	6
Odposlech	1					
Krádež médií nebo dokumentů	3		27	48	5	12
Krádež zařízení	3					
Vyzrazení	4		36	48	60	24
Falšování pomocí aplikačního vybavení	3		18	36	45	12
Selhání zařízení	4					
Chybové fungování zařízení	3					
Přetížení informačního systému	2		24	32	20	8
Chyba údržby	3					
Neoprávněné použití zařízení	3					
Podvodné kopírování aplikačního programového vybavení	1					
Poškození dat	2		18	24	30	12
Nezákonné zpracování dat	1		9	12	15	6
Chyba v používání	3		27	36	45	12
Zneužití oprávnění	4		36	48	60	24
Falšování práv	2		18	24	20	8
Odepření činností	3					
Nedostatek personálu	4					

4.2.5 Zhodnocení

V následující tabulce budou uvedeny rizika, která jsou pro organizaci nepřijatelná a rizika, která se tomuto stavu přibližují.

Tabulka č. 10: Nepřijatelné a nežádoucí rizika (Zdroj: vlastní zpracování)

HROZBA	Úroveň rizika	Aktivum
Zneužití oprávnění	64	IS - Bakaláři
Zneužití oprávnění	64	Účetní SW
Přerušení dodávky elektřiny	60	Zálohování dat
Selhání telekomunikačního zařízení	60	Zálohování dat
Vyzrazení	60	Zálohování dat
Zneužití oprávnění	60	Zálohování dat
Chyba v používání	60	Diskové pole

Na základě provedené analýzy vyplývá, že největším rizikem je zneužití oprávnění. Jedná se především o IS – Bakaláři, který obsahuje citlivá data o všech studentech školy. A je téměř nepostradatelný pro každodenní chod školy. V tomto případě se jedná o lidský faktor, kterému se nejde téměř vyhnout, a setkáme se s ním téměř všude. Jak je patrné data jsou pro základní školu velice cenná, což je vidět i z provedené analýzy. Data jsou uložena z velké části především na serveru a u poskytovatele IS. Můžeme tedy říci, že bezpečnost je mnohem vyšší, než kdyby byl server uložen přímo ve škole.

Tento fakt úzce souvisí s internetovým připojením. Jelikož je nutné se k potřebným datům připojovat vzdáleně. Je tedy patrné, že internetové připojení je pro chod školy také dost důležité.

Dále je velké riziko v zneužití oprávnění účetního SW. Při samotném zneužití může základní škole vzniknout velká škoda. K zneužití oprávnění může dojít buď úmyslně, nebo náhodně.

Je podstatné zmínit i další rizika, které mají hodnotu 60 a považujeme je za nepřijatelná rizika. Mezi tyto rizika patří přerušení dodávky elektřiny, selhání telekomunikačního zařízení, vyzrazení, zneužití oprávnění a chyba v používání.

4.3 Výběr bezpečnostních opatření

Na základě provedené analýzy dle normy ČSN ISO/IEC 27001 a požadavků vedení školy byly vybrány bezpečnostní opatření. Ty budou uvedeny v následující tabulce.

Tabulka č. 11: Vybraná bezpečnostní opatření – První etapa (Zdroj: vlastní zpracování)

A.5	**Politiky a bezpečnosti informací**
A.5.1	Směřování bezpečnosti informací vedením organizace
A.5.1.1	Politiky pro bezpečnost informací
A.5.1.2	Přezkoumání politik pro bezpečnost informací
A.6	**Organizace bezpečnosti informací**
A.6.1	**Interní organizace**
A.6.1.1	Role a odpovědnosti bezpečnosti informací
A.6.1.2	Princip oddělení povinností
A.6.1.3	Kontakt s příslušnými orgány a autoritami
A.6.1.4	Kontakt se zájmovými skupinami
A.6.1.5	Bezpečnost informací v řízení projektů
A.6.2	**Mobilní zařízení a práce na dálku**
A.6.2.1	Politika mobilních zařízení
A.6.2.2	Práce na dálku
A.8	**Řízení aktiv**
A.8.1	**Odpovědnost za aktiva**
A.8.1.3	Přípustné použití aktiv
A.8.2	**Klasifikace informací**
A.8.2.1	Klasifikace informací
A.8.2.2	Označování informací
A.8.2.3	Manipulace s aktivy
A.8.3	**Manipulace s médii**
A.8.3.1	Správa výměnných médií
A.8.3.2	Likvidace médií
A.8.3.3	Přeprava fyzických médií
A.10	**Kryptografie**
A.10.1	**Kryptografická opatření**
A.10.1.1	Politika pro použití kryptografických opatření
A.10.1.2	Správa klíčů
A.11	**Fyzická bezpečnost a bezpečnost prostředí**
A.11.1	**Bezpečné oblasti**
A.11.1.1	Fyzický bezpečnostní perimetr
A.11.1.5	Práce v zabezpečených oblastech

Dále bych chtěl podotknout, že v práci bude řešena pouze první etapa zavedení bezpečnostních opatření. Vedení školy se rozhodlo zavádět bezpečnostní opatření ve dvou etapách. První bude probíhat v průběhu tohoto roku. Druhá etapa bude zavedena v průběhu roku 2020 a 2021.

4.4 Návrh zavedení bezpečnostních opatření

V této části práce bude řešeno samotné zavádění bezpečnostních opatření, které jsou v souladu s normou ČSN ISO/IEC 27002:2017. Některá opatření jsou upravena a přizpůsobena potřebám základní školy. Budou zavedena patření, které nejsou v organizaci aplikováno nebo aplikována jen částečně.

4.4.1 A.5 - Politiky bezpečnosti informací

A.5.1 - Pokyny managementu organizace k bezpečnosti informací

Cíl: „*Poskytnout pokyny a podporu ze strany managementu pro bezpečnost informací v souladu s požadavky podnikatelské činnosti organizace a příslušnými zákony a předpisy*“ (14, s. 10).

A.5.1.1 Politiky pro bezpečnost informací

Opatření: Měly by být definovány bezpečnostní opatření, které budou schváleny vedením školy. Všichni zaměstnanci školy budou s bezpečnostními politikami seznámeni. Budou jasně definovány a rozděleny odpovědnosti a pravomoci, které jsou spojeny s bezpečnostními politikami. V zájmu vedení školy by mělo být neustále zlepšování bezpečnosti informací.

Časová náročnost:

- Vytvoření bezpečnostních politik pro základní školu: 40 hodin.
- Seznámení zaměstnanců s bezpečnostními politikami: 15 hodin.

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Opatření: Pravidelně přezkoumání politik bezpečnostních opatření, nebo v případě významných změn. Tím je zajištěna vhodnost, přiměřenost a efektivnost.
K přezkoumání politik bude docházet jednou ročně. V případě jakýchkoliv změn je nutný souhlas vedení školy. Veškeré provedené změny budou evidovány.

Časová náročnost:

Přezkoumání bezpečnostních politik: 20 hodin.

4.4.2 A.6 – Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: „*Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace*“ (14, s.11)

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Opatření: Měli by být zavedeny odpovědnosti za bezpečnost informací, které by měly být jasně definovány a přiděleny v souladu s bezpečností politikou základní školy.

Stanovit manažera bezpečnosti, který ponese odpovědnost za implementaci a rozvoj bezpečnosti. Své povinnosti může delegovat (odpovědná osoba je stále jen jedna). Aktivům se přidělí vlastník, který za dané aktivum ponese odpovědnost.

Časová náročnost:

Definování rolí a odpovědností: 10 hodin.

A.6.1.2 Princip oddělení povinností

Opatření: V organizaci by měly být odděleny povinnosti a oblasti působnosti, aby bylo zamezeno neoprávněným nebo neúmyslným změnám nebo zneužití aktiv organizace. V případě, že povinnosti nebude možné oddělit, by měli být činnosti monitorovány (činnosti prováděné s aktivem). Měl by být vytvořen dokument, který bude jasně popisovat a definovat kdo má jaká práva, povinnosti a odpovědnosti.

Časová náročnost:

Rozdělení rolí, odpovědností, práv, povinností: 6 hodin.

A.6.1.3 Kontakt s příslušnými orgány a autoritami

Opatření: Opatření je z části aplikováno. Je využíváno spojení s vyššími správními orgány, které umožňují konzultace s odborníky. Měly by být zavedeny a jasně definovány postupy, které budou určovat kým, a kdy by měly být autority kontaktovány.

Časová náročnost:

Zavedení postupů: 3 hodin.

A.6.1.4 Kontakt se zájmovými skupinami

Toto opatření se úzce vztahuje k opatření A.6.1.3. Není tedy nutné jej zavádět.

A.6.1.5 Bezpečnost informací v řízení projektů

Opatření: Bezpečnost informací by měla být řešena a začleněna do metod řízení projektů. Tím nalezneme a identifikujeme rizika bezpečnosti informací a můžeme je minimalizovat.

Používané metody při řízení projektů by měly vyžadovat:

a) zahrnout cíle bezpečnosti informací do projektových cílů,
b) pro identifikaci nezbytných opatření by se měly posuzovat rizika bezpečnosti informací v rané fázi projektu,
c) bezpečnost informací by měla být součástí všech fází použité projektové metodiky (14, str. 13).

Veškeré dopady bezpečnosti informací by měly být pravidelně řešeny a přezkoumány.

Časová náročnost:

Zavedení bezpečnosti informací do řízení projektů, vytvoření pravidel a návodů: 7 hodin.

A.6.2 Mobilní zařízení a práce na dálku

Cíl: „*Zajistit bezpečnost práce na dálku a bezpečnost použití mobilních zařízení*“ (14, str. 13).

A.6.2.1 Politika mobilních zařízení

Opatření: Vytvořit a zavést politiky pro používání mobilních zařízení tak, aby nebyly kompromitovány informace týkající se činností organizace. Při používání mobilních zařízeních na veřejných místech by si měli dát uživatelé obzvlášť pozor. Mobilní zařízení by neměly zůstávat bez dozoru. Měla by se na ně uplatnit ochrana před neoprávněným přístupem, vyzrazením informací, instalací softwaru, omezení připojení k informačním službám, ochrana před malwarem. Každé mobilní zařízení by mělo mít nastaveno zálohování dat a možnost vymazání obsahu a možnost zařízení na dálku zablokovat v případě jeho odcizení.

Časová náročnost:

Vytvoření politiky pro mobilní zařízení: 6 hodin.

A.6.2.2 Práce na dálku

Opatření: K ochraně informací, ke kterým je přistupováno na dálku by měla být vytvořena a zavedena politika a podpůrné bezpečnostní opatření. Politiky by měly definovat podmínky a omezení pro používání práce na dálku. Měl by být kladen důraz na zabezpečení komunikace, s přihlédnutím vzdáleného přístupu k interním systémům organizace, citlivosti informací a interního systému, které budou přenášeny přes komunikační linky. Důležitým krokem je zavedení malwaru proti různým typům útoků.

Časová náročnost:

Vytvoření politik pro řízení a práci na dálku: 5 hodin.

4.4.3 A.8 Řízení aktiv

A.8.1 Odpovědnosti za aktiva

Cíl: „*Identifikovat aktiva organizace a definovat odpovědnosti za přiměřenou ochranu*“ (14, str. 19).

A.8.1.3 Přípustné použití aktiv

Opatření: Měly by být ustanovena práva pro přípustné používání informací a aktiv spojených s informacemi a vybavením pro zpracování informací. Zaměstnanci i uživatelé z externích stran, mající přístup k aktivům organizace by měli být uvědomeni o požadavcích bezpečnosti informací na aktiva organizace spojené s informacemi a vybavením pro zpracování informací a zdroji. Jednotlivci nesou odpovědnosti za použití jakýchkoliv zdrojů pro zpracování informací.

Časová náročnost:

Vytvoření pravidel pro přípustné použití aktiv: 4 hodin.

A.8.2 Klasifikace informací

Cíl: „*Zajistit, aby informace získala odpovídající úroveň ochrany v souladu s jejím významem pro organizaci*“ (14, str. 21).

A.8.2.1 Klasifikace informací

Opatření: Informace by měly být klasifikovány a to z hlediska právních požadavků, hodnoty, kritičnosti a citlivosti ve vztahu k neoprávněnému vyzrazení či modifikaci. Mohou být klasifikovaná i jiná aktiva, než informace. Vlastnící informačních aktiv by měli být zodpovědní za jejich klasifikaci. Na základě důvěrnosti, integrity a dostupnosti je ohodnocena úroveň ochrany. Klasifikace poskytuje lidem, kteří se zabývají informacemi, stručnou indikaci, jak s informacemi zacházet a chránit je. Některé informace mohou přestat být citlivé nebo kritické po určité době (například informace, které byly zveřejněny). Při vytváření klasifikace musíme brát v potaz škodu, která nastane při zveřejnění informací či prozrazení.

Příklad klasifikačního schématu:

a) prozrazení či únik informací nezpůsobuje žádné škody,
b) prozrazení či únik informací způsobí menší nepříjemnosti nebo menší provozní potíže,
c) prozrazení či únik informací má významný krátkodobý dopad na provozní činnosti nebo taktické cíle,
d) prozrazení či únik informací má vážný dopad na dlouhodobé strategické cíle nebo vystavuje riziku pokračování organizace v činnosti (14).

Časová náročnost:

Klasifikace informací: 17 hodin.

A.8.2.2 Označování informací

Opatření: Označení informací je dalším krokem po jejich klasifikaci. Je potřeba veškeré informace správně označit. Ať už se jedná o papírové či elektronické dokumenty. Označení musí být snadno rozeznatelné. Na základě označení informací je s nimi posléze

zacházeno. Zaměstnanci by měli být seznámeni se způsobem označení informací a jak s takto označenými informacemi zacházet.

Časová náročnost:

Vytvoření postupů pro označování informací: 7 hodin.

A.8.2.3 Manipulace s aktivy

Pro zacházení s aktivy by měly být zavedeny a vyvinuty postupy, které jsou v souladu se schématem klasifikace informací přijatým organizací. Měly by být vytvořeny postupy pro zacházení, zpracování, ukládání a předávání informací v souladu s jejich klasifikací. Klasifikační schémata se mohou v různých organizacích lišit.

Měly by být v úvahu vzaty následující položky:

a) omezení přístupu podporující požadavky na ochranu na každé úrovni klasifikace,
b) udržování formálního záznamu o oprávněných příjemcích aktiv,
c) ochrana dočasných nebo trvalých kopií informace na úrovni odpovídající ochraně původní informace,
d) skladování IT aktiv v souladu se specifikacemi výrobce,
e) zřetelné označení všech kopií médií pro upoutání pozornosti oprávněného příjemce (14, str. 22).

Časová náročnost:

Vytvoření postupů pro manipulaci s aktivy: 5 hodin.

A.8.3 Manipulace s médii

Cíl: „*Zabránit neoprávněnému prozrazení, modifikaci, odstranění nebo zničení informací uložených na médiu*“ (14, str. 22)

A.8.3.1 Správa výměnných medií

Opatření: Měly by být zavedeny postupy, které jsou v souladu se schématem klasifikace přijatých organizací. Pro ukládání důvěrných dat na média se využívá šifrování. Média, která se v organizaci již nepoužívají, by měly být zničena a to nejlépe neobnovitelným způsobem. Média by měla být uložena v bezpečném prostředí v souladu, který specifikuje výrobce. V případě degradace dat by měly být data přenesena na nová média, než se stanou nečitelnými. Veškeré média musí být evidována.

Časová náročnost:

Vytvoření postupů pro práci a správu výměnných médií: 4 hodin.

A.8.3.2 Likvidace médií

Opatření: V případě, že média již nejsou zapotřebí, měly by být zlikvidovány dle formálních postupů, aby se minimalizovalo riziko úniku důvěrných informací. Média, která obsahují citlivé data, by měly být likvidována destruktivním způsobem (spálením, zkratováním, vymazáním údajů), aby nemohla být použita jinou aplikací.

Časová náročnost:

Vytvoření postupů pro likvidaci médií: 3 hodin.

A.8.3.3 Přeprava fyzických médií

Opatření: Média, která obsahují informace, by měla být během přepravy chráněna před neoprávněným přístupem, zneužitím nebo poškozením. Pro přepravu médií by měla být zvolená spolehlivá přeprava popřípadě zvolena spolehlivá kurýrní služba (autorizovaná). Média by měla být chráněna šifrováním před neoprávněným přístupem.

Časová náročnost:

Vytvoření postupů pro přepravu fyzických médií: 2 hodin.

4.4.4 A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: „*Zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity a/nebo integrity informací*“ (14, str. 31).

A.10.1.1 Politika použití kryptografických opatření

Opatření: Vypracovat a realizovat politiky použití kryptografických opatření na ochranu informací. Každá informace nemusí vyžadovat stejnou úroveň zabezpečení. V případě, kdy informace opouští perimetr organizace, je nutné využít kryptografické opatření (šifrování). Součástí politiky by mělo být i definování správy klíčů a metody zašifrované informace v případě ztráty.

Časová náročnost:

Vytvoření postupů pro použití kryptografických opatření: 5 hodin.

A.10.1.2 Správa klíčů

Opatření: Politika kryptografických opatření vyžaduje správu klíčů. Součástí politiky je správa kryptografických klíčů během celého životního cyklu a to včetně generování, ukládání, archivace, distribuce, vyřazení a zničené klíče. Veškeré kryptografické klíče by měly být chráněny před modifikací a ztrátou. Zařízení, sloužící ke generování, ukládání a archivaci klíčů by mělo mít fyzickou ochranu. Je důležité, aby fungovaly algoritmy pro dešifrování informací, v případě, že dojde k modifikaci nebo ztrátě.

Časová náročnost:

Vytvoření postupů pro použití kryptografických opatření: 5 hodin.

4.4.5 A.11 Fyzická bezpečnost a bezpečnostní opatření

A.11.1 Zabezpečené oblasti

Cíl: „*Zabránit neoprávněnému fyzickému přístupu, poškození a narušování informací a vybavení pro zpracování informací organizace*“ (14, str. 33).

A.11.1.1 Fyzický bezpečnostní perimetr

Opatření: Měly by být určeny bezpečnostní perimetry, a ty by měly být použity k ochraně oblastí, které obsahují buď citlivé, nebo kritické informace a vybavení pro zpracování informací. Některé bezpečnostní perimetry jsou již z části aplikovány. Vedení organizace by však mělo zvážit jejich rozšíření. Měly by být zváženy následující pokyny a ve vhodných případech implementovány pro fyzické bezpečnostní perimetry:

a) definování bezpečnostních perimetrů a umístění a síla každého perimetru by měla záviset na bezpečnostních požadavcích aktiv v rámci perimetru a na výsledcích posuzování rizik,
b) zavedení vhodných systémů detekce průniku, které budou naistalovány dle regionálních či mezinárodních norem a pravidelně testovány. Oblasti, které nejsou využívané, by měly být permanentně zabezpečeny alarmem,
c) vybavení pro zpracování informací spravované organizací by mělo být fyzicky odděleno od vybavení spravovaného externími firmami.

Časová náročnost:

Vytvoření postupů pro použití kryptografických opatření: 6 hodin.

A.11.1.5 Práce v zabezpečených oblastech

Opatření: V organizaci by měly být navrženy a zavedeny postupy pro práci v zabezpečených oblastech. Některé z těchto postupů již zavedeny jsou, ale vedení organizace by mělo uvažovat o jejich rozšíření. Měla by být zvážena následující opatření:

a) mělo by se vyvarovat práci bez dohledu,
b) prázdné fyzické oblasti by měli být pravidelně přezkoumávány,

Opatření se týkají jak zaměstnanců, tak i externích stran, kteří v zabezpečené oblasti pracují.

Časová náročnost:

Vytvoření postupů pro použití kryptografických opatření: 4 hodin.

4.5 Budování bezpečnostního povědomí

Budování bezpečnostního povědomí je nikdy nekončící proces. Je velmi důležité, aby se všichni zaměstnanci neustále vzdělávali a tím budovali bezpečnostní povědomí SAE (Security Awareness Education). Norma NIST SP 800-50 (Building an Information Technology Security Awareness and Training Program) se věnuje budování bezpečnostního povědomí. Bezpečnostní povědomí není závislé na zavedení bezpečnostních opatření. Jde o kontinuální proces, kdy jsou uživatelé rozděleni do skupin a vzděláváni na několika úrovních, dle potřeb organizace. Na budování bezpečnostní povědomí můžeme nahlížet z různých pohledů:

- úroveň vzdělání (školení, povědomí, certifikace, osobní a profesní rozvoj),
- funkčního dělení vazeb na ICT,
- skupiny uživatelů, dle (začátečník, středně pokročilý, pokročilý).

Základem pro budování bezpečnostního povědomí je plán. Ten se skládá z několika prvků:

Role a odpovědnosti – Jsou určeny role a odpovědnosti. Je stanovena odpovědná osoba (manažer kybernetické bezpečnosti - CIO). Odpovědnou osobou za budování bezpečnostního povědomí bude ředitelka školy. Jako zastupující osoba bude určen zástupce ředitelky, starající se o chod IT ve škole. Ředitelka školy bude dohlížet na plnění plánu a průběžně ho upravovat tak, aby bylo dosaženo co nejvyšší efektivity.

Stanovení cílů - jsou stanoveny cíle pro jednotlivé úrovně vzdělání. Pro každou úroveň je stanoven cíl, který se musí dosáhnout.

Rozdělení uživatelů do skupin

- běžný zaměstnanec – uživatel/zaměstnanec, který má pouze základní znalosti o ICT,
- pokročilý zaměstnanec – uživatel/zaměstnanec má pokročilé znalosti ICT. Většinou se jedná o vedoucí pracovníky jednotlivých oddělení,
- specialista – podílí se na zvyšování bezpečnosti informací ve společnosti, potažmo organizaci (ředitelka školy, zástupce ředitelky, pověřená osoba).

Srovnávací rámec

Tabulka č. 12: Srovnávací rámec (Zdroj: 15)

Srovnávací rámec			
	Povědomí	**Školení**	**Vzdělání**
Atribut	„Co“	„Jak“	„Proč“
Úroveň	Informativní	Znalostní	Pochopení
Cíl vzdělání	Zapamatování a rozpoznání	Dovednost, zdatnost	Plné porozumění
Cílová skupina	Běžný uživatel, Pokročilý uživatel, Specialista	Pokročilý uživatel, Specialista	Specialista
Vzdělávací metoda	Výuková videa, Bezpečnostní brožury, Prospekty, Praktické ukázky	Případové studie, Praktické ukázky	Semináře, Diskuze, Studium, Výzkum
Způsob testování vzdělání	Test - ANO/NE, Otevřené otázky	Praktické řešení problémů (případová studie)	Esej
Časová náročnost	Krátkodobá	Střednědobá	Dlouhodobá

V dalším kroku jsou ověřeny vstupní znalosti uživatelů a posléze jsou uživatele rozděleni do skupin. Na základě těchto skupin můžeme lépe specifikovat cíle a rozsah bezpečnostního vzdělávání.

Je nutné:

- určení cílů,
- vytvořit školící a vzdělávací materiály pro jednotlivé skupiny,
- definovat a určit problematiku, která bude náplní jednotlivých školení a kurzů,
- vetvoření metodiky pro nasazení jednotlivých aspektů programu,
- vyhotovení dokumentace, zpětná vazba, průběh výuky,
- vyhodnocení a aktualizace výukových materiálů,
- určení četnosti opakování vzdělání, aktualizace materiálů,
- kalkulace a vyhodnocení výsledků.

4.5.1 Návrh zavedení bezpečnostního povědomí na základní škole

Na základní škole se nachází mnoho zaměstnanců a uživatelů, kteří mají různé znalosti a vztah k ICT. Z tohoto důvodu by bylo vhodné, aby uživatele byli kategorizování. KE každé skupině uživatelů by se přistupovalo jinak a školení by bylo přizpůsobeno jednotlivým skupinám. Vzdělávání uživatelů bychom mohli rozdělit do tří skupin:

Manažer kybernetické bezpečnosti – Osoby v této skupině by měli velice dobře porozumět dané problematice. Dokázat odpovědět na otázky co, jak a proč. Měli by mít možnost se účastnit přednášek a seminářů vztahujících se k dané problematice. Výstupem je získání certifikace. Jde o dlouhodobý proces vzdělávání.

Vzdělávání zaměstnanců – Zaměstnanci školy, především učitelé by měli danou problematiku znát. Je vhodné, aby zaměstnanci jednou ročně absolvovali školení

informační bezpečnosti. Školením by měli určitě projít zaměstnanci školy, kteří přichází do styku s informačními technologiemi.

Vzdělávání studentů – Žáci by měli mít alespoň minimální povědomí o dané problematice. Možnost jak zvýšit bezpečnostní povědomí u žáku jsou video ukázky, videokurzy, letáky, přednášky odborníku, praktické ukázky. Ověřit znalosti studentů je možné ověřit například pomocí testu Ano/Ne.

Je důležití přizpůsobit obsah a formu vzdělávacího programu a to především z toho důvodu, že základní školu navštěvují děti ve věku 6 až 15 let.

4.6 Postup zavedení první etapy

Jak již bylo zmíněno v předcházející kapitole, v práci bude řešena pouze první etapa zavedení bezpečnostních opatření. Vedením organizace byly vybrány bezpečnostní opatření, které jsou pro základní školu v současné době nejdůležitější. Velkým rizikem může být útok hackera, aby získal citlivé údaje, které jsou obsaženy v systému školy. Z tohoto důvodu je vhodné zavést bezpečnostní opatření označené jako **A.10 Kryptografie**. Součástí tohoto opatření je vytvoření politik pro šifrování dat. Toto bezpečnostní opatření by mělo zamezit, aby se útočník dostal k neoprávněným datům a nedošlo k jejich vyzrazení.

Významnou roli pro snížení rizik, které jsou v práci uvedeny napomůže zavedení bezpečnostních opatření **A.11** , které se týká fyzické bezpečnosti a bezpečnosti prostředí. Dalším opatřením, které se týká zavedení první etapy je **A.8 Řízení aktiv**. Opatření identifikují aktiva a zajišťují jejich ochranu. Dále klasifikují informace a označují informace. Udávají jak s aktivy manipulovat. Popisují i manipulace s médii (správa, likvidace a přeprava médií).

Jako další skupina bezpečnostní opatření, které budou zavedeny jsou **A.5 Politiky a bezpečnosti informací** a **A.6 Organizace bezpečnosti informací**. V tomto případě nejspíše nepůjde opatření definovat najednou, ale postupným zaváděním a zlepšováním, jelikož zavedení bezpečnostní politiky je poměrně složitý proces. Je důležité reagovat na nově vzniklé hrozby. Součástí zavedení opatření **A.6** je definování rolí a odpovědností, práce na dálku a mobilní zařízení.

Důvodem, proč budou zaváděny bezpečnostní opatření na etapy, je ten, aby byla co nejméně narušena školní výuka a také nedostatek lidských zdrojů. Zavedení první etapy by mělo být realizováno do konce roku 2019. Časová náročnost a harmonogram zavedení opatření bude zpracován v následující kapitole.

4.7 Ekonomické zhodnocení a časový harmonogram

Vedení základní školy se rozhodlo zavádět bezpečností opatření ve dvou etapách. A to především z důvodu nízkého rozpočtu a nedostatku lidských zdrojů. Náklady spojené se zaváděním bezpečnostních opatření se týkají pouze pracovních hodin zaměstnanců, kteří budou tyto opatření zavádět. Jsou dvě možnosti, jak bezpečnostní opatření ve škole zavést. První z nich je ta, že se o zavedení ISMS bude starat externí pracovník, který již na škole působí. Tady však vzniká problém, jelikož by se nemohl věnovat pouze zavádění bezpečnostních opatření pro danou školu, ale i jiným zakázkám. Druhou variantou je, že si škola pro zavedení těchto opatření najme certifikovanou firmu.

Tabulka č. 13: Porovnání mzdy pracovníků (Zdroj: vlastní zpracování)

Zavedení bezpečnostních opatření	Hodinová mzda [Kč/h]
Externí pracovník	500
Firma	1000

Jak je vidět z předcházející tabulky, v případě, že se o zavedení bezpečnostních opatření bude starat externí zaměstnanec, který na škole již působí, náklady na zavedení se sníží zhruba o polovinu. Avšak se nebude moci plně věnovat pouze této zakázce. Tudíž celkový čas na zavedení bezpečnostních opatření bude přibližně o polovinu delší, než při zavádění opatření certifikovanou firmou. V diplomové práci pro kalkulaci bude řešena první varianty, kdy opatření bude zavádět externí pracovník.

Tabulka č. 14: Odhadované časové a finanční náklady pro zavedení první etapy (Zdroj: vlastní zpracování)

Opatření	Časová náročnost [h]		Náklady [Kč]	
	Zavedení	Ročně	Zavedení	Ročně
A.5.1.1	19	2	9500	1000
A.5.1.2	5	6	2500	3000
A.5	**24**	**8**	**12000**	**4000**
A.6.1.1	11	1	5500	500
A.6.1.2	3	1	1500	500
A.6.1.3	2	1	1000	500
A.6.1.4	2	1	1000	500
A.6.1.5	3	1	1500	500
A.6.2.1	6	1	3000	500
A.6.2.2	3	1	1500	500
A.6	**30**	**7**	**15000**	**3500**
A.8.1.3	3	1	1500	500
A.8.2.1	9	2	4500	1000
A.8.2.2	3	1	1500	500
A.8.2.3	2	1	1000	500
A.8.3.1	4	1	2000	500
A.8.3.2	2	1	1000	500
A.8.3.3	2	1	1000	500
A.8	**25**	**8**	**12500**	**4000**
A.10.1.1	4	1	2000	500
A.10.1.2	6	2	3000	1000
A.10	**10**	**3**	5000	1500
A.11.1.1	4	1	2000	500
A.11.1.5	3	1	1500	500
A.11	**7**	**2**	**3500**	**1000**
Celkem	**96**	**28**	**48000**	**14000**

Tabulka 14 popisuje odhadovanou časovou náročnost s odhadovanými náklady. Je zde započítána mzda 500 Kč/h pro zaměstnance, který ve škole již externě působí. V případě, že by se škola rozhodla zvolit pro zavedení bezpečnostních opatření externí certifikovanou firmu, byla by výše hodinové mzdy minimálně 1000 Kč/h.

Jak je z tabulky patrné odhadovaná doba trvání pro zavedení bezpečnostních opatření činí 96 hodin. Opakující se roční činnosti pak činní 28 hodin.

Celkové odhadované náklady na první etapu zavedení bezpečnostních opatření činí 48 000 Kč. Jedná se pouze o orientační odhad a v průběhu zavádění opatření se může měnit. Je také nutné započítat roční náklady, které slouží k revizi, průběžného zlepšování a udržování opatření. Tyto náklady budou přibližně 14 000 Kč. Vedením školy byl pro zavedení první etapy odsouhlasen rozpočet 90 000 Kč. A to především z důvodu rezerv a neočekávaných nákladu spojené se zavedením bezpečnostních opatření.

Časový harmonogram pro zavedení první etapy

Časová náročnost zavedení jednotlivých bezpečnostních opatření je znázorněna v tabulce 14. V následující tabulce jsou časy trvání zobrazeny graficky

Tabulka č. 15: Časový harmonogram první etapy (Zdroj: vlastní zpracování)

Opatření	Název	1.Týden	2. Týden	3. Týden	4. Týden	5. Týden	6. Týden	7. Týden	8. Týden	9. Týden	10.Týden
A.10	Kryptografie										
A.11	Fyzická bezpečnost a bezpečnost prostředí										
A.8	Řízení aktiv										
A.5	Politiky bezpečnosti informací										
A.6	Organizace bezpečnosti informací										

4.8 Přínosy práce

K hlavním přínosům diplomové práce patří zvýšení informační bezpečnosti na dané základní škole. Na základě provedených analýz má vedení možnost vidět slabá místa, rizika a jejich dopady. V případě, že bude ISMS zavedeno v celém rozsahu, může škola usilovat a certifikaci.

Řízení informační bezpečnosti je nekončící proces a je tedy nutné ho neustále zlepšovat a udržovat. Je důležité zavedené postupy, opatření, politiky neustále přezkoumávat.

Práce může vedení školy poskytnout základní metodiku při zavádění části ISMS. Pokud bude v budoucnu rozhodnuto a zavedení celého ISMS, je možné navázat na tuto práci a navrhnout a zavést zbývající opatření. Velkým ekonomickým přínosem je i to, že škola nebude muset vynaložit finanční prostředky pro zpracování projektu na zavedení bezpečnostních opatření. Práce především využije externí IT pracovník působící na škole.

Dle mého názoru bude největším přínosem zavedení první etapy bezpečnostních opatření na takové úrovni, že se podle ní budou řídit všichni zaměstnanci školy i žáci.

ZÁVĚR

Cílem diplomové práce bylo vytvořit návrh bezpečnostních opatření, které jsou v souladu s ISMS. Návrh bezpečnostních opatření byl vytvořen na základě provedených analýz (analýza současného stavu, asistované zhodnocení, požadavky organizace, analýza rizik). Opěrným bodem, podle kterých jsem se řídil, jsou normy ČSN ISO/IEC řady 27000:2017 a kybernetická vyhláška. Diplomová práce je zpracována pro základní školu, která si nepřála být jmenována, proto není v práci uveden její název.

Práce je rozdělena do tří hlavních kapitol. První kapitola popisuje teoretická východiska, pojmy a definice, které jsou potřebné k pochopení dané problematiky.

Druhá část práce je zaměřena na analýzu současného stavu. Jsou zde uvedeny základní informace o základní škole, popis současného stavu. Velkou část této kapitoly tvoří analýzy. Konkrétně pak analýza asistovaného zhodnocení. Jedná se o pomůcku k auditu bezpečnostních opatření. Dále je zde souhrn asistovaného zhodnocení, který vypovídá o tom, jaké bezpečnostní opatření jsou aplikovány, částečně aplikovány nebo neaplikovány. K této analýze byla využita norma ČSN ISO/IEC 27001:2017. V samotném závěru druhé části je pak celkové shrnutí asistovaného zhodnocení a požadavky vedení organizace.

Třetí část práce obsahuje samotný návrh řešení. V úvodu jsou definovány hranice a rozsah práce. Dále následuje analýza rizik. Z této analýzy se pak vychází při samotném návrhu jednotlivých bezpečnostních opatření. Součástí analýzy je i matice zranitelnosti a matice úrovně rizik. Bezpečnostní opatření, které jsou navržena, vychází z normy ČSN ISO/IEC 27001:2017 a normy ČSN ISO/IEC 27002:2017. V práci je popsáno pouze zavedení první etapy bezpečnostních opatření, které by mělo být realizováno v průběhu tohoto roku. V závěru práce je ekonomické zhodnocení, časový harmonogram a popsány přínosy diplomové práce. Můžu tedy říci, že hlavní cíle diplomové práce byly splněny.

Důležité je, aby se vedení neustále věnovalo zlepšování bezpečnostního povědomí všech zaměstnanců i žáků školy. Jelikož systém řízení informační bezpečnosti je nikdy nekončící proces je potřeba ho neustále udržovat a zlepšovat.

SEZNAM POUŽITÝCH ZDROJŮ

(1) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

(2) ONRÁK, V. *Bezpečnost IS/IT* (přednášky). Brno: VUT, 2018.

(3) ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

(4) ONRÁK, V. *Management informační bezpečnosti* (skripta). Brno: VUT, 2013.

(5) ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

(6) Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) ze dne 21. května 2018.

(7) SEDLÁK, P. Kybernetická vyhláška – č.82/2018 Sb. (přednáška). Brno: VUT,2018.

(8) SEDLÁK, P. *Management informační bezpečnosti* (přednáška). Brno: VUT,2018.

(9) POŽÁR, Josef. *Manažerská informatika*. Plzeň: Aleš Čeněk, 2010, 357 s. : il., grafy, tab. ISBN 978-80-7380-276-9.

(10) SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s.: portréty, grafy, tab. ISBN 978-80-247-4644-9

(11) *Tsbohemia: Synology DS712+ Disc Station* [online]. [cit. 2019-03-03]. Dostupné z: https://www.tsbohemia.cz/synology-ds712-disc-station-_d137196.html

(12) *Tsbohemia: Mikrotik RB1100AHX2* [online]. [cit. 2019-03-03]. Dostupné z: https://www.tsbohemia.cz

(13) *Bakalari: Bakaláři – mezi školou a rodinou* [online]. [cit. 2019-03-03]. Dostupné z: https://www.bakalari.cz/Static/evidence

(14) *Bakalari: Bakaláři – mezi školou a rodinou* [online]. [cit. 2019-03-03]. Dostupné z: https://www.bakalari.cz/Static/rozvrh

(15) Building an Information Technology Security Awareness and Training Program. *Citadel-information.com* [online]. b.r. [cit. 2019-04-05]. Dostupné z: http://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-50-building-information-security-awareness-program-2003.pdf

(16) ČSN ISO/IEC 27002. *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. 2. vydání Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

COBIT – Standard pro správné postupy řízení informačních technologií

ČSN – Česká technická norma

GDPR – General Data Protection Regulation

HW – Hardware

ICT – Information and Communication Technology

IEC – Mezinárodní úřad pro elektrotechniku

IS – Informační systém

ISMS – Systém řízení bezpečnosti informací

ISO – Mezinárodní organizace pro normalizaci

IT – Informační technologie

ITIL – Knihovna infrastruktury informačních technologií

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

PDCA – Demingův cyklus (Plánuj, dělej, kontroluj, jednej)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha č. 1: Asistované zhodnocení

Řízení aktiv:

Požadavek	Identifikace a evidence aktiva
Stav	Částečně aplikováno
Komentář	

Požadavek	Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za primární aktiva
Stav	Částečně aplikováno
Komentář	

Požadavek	Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a tato aktiva jsou zařazena do jednotlivých úrovní.
Stav	Částečně aplikováno
Komentář	Chybí rozřazení aktiv.

Požadavek	Při hodnocení důležitosti primárních aktiv je posouzeno především: - Rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství, - Rozsah dotčených právních povinností nebo jiných závazků, - Rozsah narušení vnitřních řídicích a kontrolních činností, - Poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty, - Dopady na poskytování důležitých služeb, - Rozsah narušení běžných činností, - Dopady na zachování dobrého jména nebo ochranu dobré pověsti, - Dopady na bezpečnost a zdraví osob, - Dopady na mezinárodní vztahy, - Dopady na uživatele informačního a komunikačního systému.
Stav	Částečně zavedeno
Komentář	Jsou zavedeny pouze některé body z výše uvedeného seznamu.

Požadavek	Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že: - jsou určeny způsoby rozlišování jednotlivých úrovní aktiv, - jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv, - jsou stanoveny přípustné způsoby používání aktiv, - jsou zavedena pravidla ochrany odpovídající úrovni aktiv, - jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv.
Stav	Nezavedeno
Komentář	

Řízení rizik:

Požadavek	Stanoveny metodiky pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik.
Stav	Nezavedeno
Komentář	

Požadavek	Provedení hodnocení rizik v pravidelných intervalech a při významných změnách.
Stav	Nezavedeno
Komentář	

Požadavek	Při hodnocení rizik zohlednění relevantní hrozby a zranitelnosti a posouzení možných dopadů na aktiva.
Stav	Nezavedeno
Komentář	

Požadavek	Je prováděno hodnocení rizik v pravidelných intervalech a při významných změnách.
Stav	Nezavedeno
Komentář	

Požadavek	Jsou zpracovávány zprávy o hodnocení aktiv.
Stav	Nezavedeno
Komentář	

Požadavek	Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováno prohlášení o aplikovatelnosti, které obsahuje přehled bezpečnostních opatření.
Stav	Nezavedeno
Komentář	

Požadavek	Je zavedený a zpracovaný plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání jednotlivých rizik, určení osoby zajišťující prosazování bezpečnostních opatření pro zvládání rizik, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení, popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a způsob realizace bezpečnostních opatření.
Stav	Nezavedeno
Komentář	

Organizační bezpečnost

Požadavek	Zajištění dostupnosti zdrojů potřebných pro systém řízení bezpečnosti informací.
Stav	Neaplikováno
Komentář	

Požadavek	Informování zaměstnanců o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky se všemi dotčenými stranami.
Stav	Neaplikováno
Komentář	

Požadavek	Zajištění podpory k dosažení zamýšlených výstupů systému řízení bezpečnosti informací.
Stav	Neaplikováno
Komentář	

Požadavek	Vedení zaměstnanců k rozvíjení efektivity systému řízení bezpečnosti informací a podporování je při tomto rozvoji.
Stav	Neaplikováno
Komentář	

Požadavek	Prosazování neustálého zlepšování systému řízení bezpečnosti informací.
Stav	Neaplikováno
Komentář	

Požadavek	Je zajištěno stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role.
Stav	Neaplikováno
Komentář	

Požadavek	Zajištění zachování mlčenlivosti administrátorů a osob zastávajících bezpečnostní role.
Stav	Aplikováno
Komentář	Je součástí pracovní smlouvy.

Požadavek	Určení bezpečnostní role: manažer kybernetické bezpečnosti.
Stav	Neaplikováno
Komentář	

Požadavek	Určení bezpečnostní role: architekt kybernetické bezpečnosti-
Stav	Neaplikováno
Komentář	

Požadavek	Určení bezpečnostní role: garant aktiva a auditor kybernetické bezpečnosti.
Stav	Neaplikováno
Komentář	

Řízení dodavatelů

Požadavek	Stanovení pravidel pro dodavatele, které zohledňují požadavky systému řízení bezpečnosti.
Stav	Neaplikováno
Komentář	

Požadavek	Vedení evidence svých významných dodavatelů
Stav	Aplikováno
Komentář	Dodavatelé jsou evidovány v systému.

Požadavek	V souvislosti s řízením rizik spojených s významnými dodavateli je zajištěno, aby smlouvy uzavírané s významnými dodavateli obsahovaly relevantní oblasti.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba u významných dodavatelů provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany.
Stav	Neaplikováno
Komentář	

Bezpečnost lidských zdrojů

Požadavek	S ohledem na stav a potřeby systému řízení bezpečnosti informací je stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování.
Stav	Neaplikováno
Komentář	

Požadavek	Uživatelé, administrátoři, osoby zastávající bezpečnostní role a dodavatelé jsou poučení o jejich povinnostech a o bezpečnostní politice.
Stav	Neaplikováno
Komentář	

Požadavek	Teoretické i praktické školení uživatelů, administrátorů a osob zastávající bezpečnostní role.
Stav	Neaplikováno
Komentář	

Požadavek	Zajištění kontroly dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávající bezpečnostní role.
Stav	Částečně aplikováno
Komentář	

Požadavek	V případě ukončení smluvního vztahu s administrátory a osobami zastávajícím bezpečnostní role zajišťuje předání odpovědností.
Stav	Aplikováno
Komentář	

Požadavek	Je hodnocen plán účinnosti plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí.
Stav	Neaplikováno
Komentář	

Požadavek	Jsou určeny pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávající bezpečnostní role.
Stav	Částečně aplikováno
Komentář	

Řízení provozu a komunikací

Požadavek	Povinná osoba v rámci řízení provozu a komunikací zajišťuje bezpečný provoz informačního a komunikačního systému a stanoví provozní pravidla a postupy.
Stav	Částečně aplikováno
Komentář	Jsou stanovena některá provozní pravidla a postupy.

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role.
Stav	Částečně aplikováno
Komentář	Práva a povinnosti jsou stanovena pouze slovní formou. Nejsou uvedena do písemné podoby.

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů.
Stav	Částečně aplikováno
Komentář	

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Postupy pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech.
Stav	Neaplikováno
Komentář	

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Pravidla a postupy pro ochranu před škodlivým kódem.
Stav	Neaplikováno
Komentář	

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Řízení technických zranitelností.
Stav	Neaplikováno
Komentář	

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory.
Stav	Aplikováno
Komentář	

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Postupy řízení a schvalování provozních změn.
Stav	Aplikováno
Komentář	Dokumentováno

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.
Stav	Aplikováno
Komentář	

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu.
Stav	Neaplikováno
Komentář	

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Pravidla a postupy pro instalaci technických aktiv.
Stav	Aplikováno
Komentář	Zprostředkovává interní zaměstnanec. Dokumentováno.

Požadavek	Provozní pravidla a postupy orgánu a osoby zahrnují: Provádění pravidelného zálohování a kontroly použitelnosti provedených záloh a pravidla a postupy pro zajištění bezpečnosti síťových služeb.
Stav	Částečně aplikováno
Komentář	

Řízení přístupu

Požadavek	Povinná osoba dále v rámci řízení přístupu informačnímu a komunikačnímu systému: Řídi přístup na základě skupin a rolí.
Stav	Částečně aplikováno
Komentář	

Požadavek	Povinná osoba dále v rámci řízení přístupu informačnímu a komunikačnímu systému: Přidělí každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému přístupová práva a oprávnění a jedinečný identifikátor.
Stav	Aplikováno
Komentář	

Požadavek	Povinná osoba dále v rámci řízení přístupu informačnímu a komunikačnímu systému: Zavádí bezpečnostní opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba dále v rámci řízení přístupu informačnímu a komunikačnímu systému: Přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu.
Stav	Částečně aplikováno
Komentář	

Požadavek	Povinná osoba dále v rámci řízení přístupu informačnímu a komunikačnímu systému: Provádí pravidelné přezkoumání nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba dále v rámci řízení přístupu informačnímu a komunikačnímu systému: Zajistí odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba dále v rámci řízení přístupu informačnímu a komunikačnímu systému: Zajistí odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu a dokumentuje přidělování a odebírání přístupových oprávnění.
Stav	Částečně aplikováno
Komentář	

Požadavek	Povinná osoba dále v rámci řízení přístupu informačnímu a komunikačnímu systému: Dokumentuje přidělování a odebírání přístupových oprávnění.
Stav	Neaplikováno
Komentář	

Zvládání kybernetických bezpečnostních událostí a incidentů

Požadavek	Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů: Zavede proces detekce a vyhodnocování kybernetických bezpečnostních událostí a zvládání kybernetických bezpečnostních incidentů.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů: Přidělí odpovědnosti a stanoví postupy.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů: Vyhodnotí kybernetické bezpečnostní události a incidenty.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů: Definuje a aplikuje postupy pro identifikaci, sběr, získání a uchování věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů: Zajistí detekci kybernetických bezpečnostních událostí.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů: Zajistí, že uživatelé, administrátoři, osoby zastávající bezpečnostní role, další zaměstnanci a dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti.
Stav	Částečně aplikováno
Komentář	

Požadavek	Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů: Zajistí zvládání kybernetických bezpečnostních incidentů podle stanovených postupů.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba v rámci zvládání kybernetických bezpečnostních událostí a incidentů: Vede záznamy o kybernetických bezpečnostních incidentech a o jejich zvládání
Stav	Neaplikováno
Komentář	

Řízení kontinuity činností

Požadavek	Povinná osoba v rámci řízení kontinuity činností: Stanoví práva a povinnosti administrátorů a osob zastávajících bezpečnostní role.
Stav	Neaplikováno
Komentář	

Požadavek	Povinná osoba v rámci řízení kontinuity činností: Pomocí hodnocení rizik a analýzy dopadů vyhodnotí a dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika
Stav	Neaplikováno
Komentář	

Fyzická bezpečnost

Požadavek	Předchází se poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému.
Stav	Částečně aplikováno
Komentář	

Požadavek	Je stanoven fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému.
Stav	Aplikováno
Komentář	

Požadavek	U fyzického bezpečnostního perimetru jsou stanovena a přijata nezbytná opatření a uplatněny prostředky fyzické bezpečnosti: - k zamezení neoprávněnému vstupu, - k zamezení poškození a neoprávněným zásahům, - pro zajištění ochrany na úrovni objektů a v rámci objektů.
Stav	Částečně aplikováno
Komentář	

Bezpečnost komunikačních sítí

Požadavek	Je zajištěna segmentace komunikační sítě.
Stav	Neaplikováno
Komentář	

Požadavek	Je zajištěna komunikace v rámci komunikační sítě a perimetru komunikační sítě.
Stav	Částečně aplikováno
Komentář	

Požadavek	Pomocí kryptografie je zajištěna důvěrnost a integrita dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií,
Stav	Aplikováno
Komentář	

Požadavek	Nežádoucí komunikace je aktivně blokována.
Stav	Aplikováno
Komentář	Firewall

Požadavek	Je zajištěna segmentace sítě a řízení komunikace mezi jejími segmenty a je využíván nástroj, zajišťující ochranu integrity.
Stav	Částečně aplikováno
Komentář	

Správa a ověřování identit

Požadavek	Je používán nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému.
Stav	Aplikováno
Komentář	

Požadavek	Nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací zajišťuje: - ověření identity před zahájením aktivit v informačním a komunikačním systému, - řízení počtu možných neúspěšných pokusů o přihlášení, - odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití, - ukládání autentizačních údajů ve formě odolné proti offline útokům, - opětovné ověření identity po určené době nečinnosti, - dodržení důvěrnosti autentizačních údajů při obnově přístupu a centralizovanou správu identit.
Stav	Aplikováno
Komentář	

Požadavek	Pro ověření identity uživatelů, administrátorů a aplikací využívá autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů.
Stav	Neaplikováno
Komentář	

Požadavek	Nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, musí vynucovat tyto pravidla: - délka hesla alespoň 12 znaků u uživatelů a 17 znaků u administrátorů, -možnost zadat heslo o délce alespoň 64 znaků, - neomezující použití malých a velkých písmen, číslic a speciálních znaků, -možnost uživatelům změnit heslo, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut.
Stav	Částečně aplikováno
Komentář	

Požadavek	Nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, neumožňuje uživatelům a administrátorům: - zvolit si nejčastěji používaná hesla, - tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem, - opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel.
Stav	Neaplikováno
Komentář	

Řízení přístupových oprávnění

Požadavek	Povinná osoba používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění: - pro přístup k jednotlivým aktivům informačního a komunikačního systému a pro čtení dat, zápis dat a změnu oprávnění.
Stav	Aplikováno
Komentář	

Ochrana před škodlivým kódem

Požadavek	Je zajištěna nepřetržitá automatická ochrana: -koncových stanic.
Stav	Aplikováno
Komentář	Zajištěno antivirovým programem

Požadavek	Je zajištěna nepřetržitá automatická ochrana: -mobilních zařízení.
Stav	Neaplikováno
Komentář	

Požadavek	Je zajištěna nepřetržitá automatická ochrana: -serverů, -datových úložišť a výměnných datových nosičů.
Stav	Částečně aplikováno
Komentář	

Požadavek	Je zajištěna nepřetržitá automatická ochrana: -komunikační sítě a prvků komunikační sítě a obdobných zařízení.
Stav	Částečně aplikováno
Komentář	

Požadavek	Je prováděna pravidelná a účinná aktualizace nástroje pro ochranu před škodlivým kódem.
Stav	Částečně aplikováno
Komentář	Pouze u některých částí síťové infrastruktury

Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

Požadavek	Jsou zaznamenávány bezpečnostní a potřebné provozní události důležitých aktiv informačního a komunikačního systému.
Stav	Částečně aplikováno
Komentář	

Požadavek	Je prováděn sběr informací a bezpečnostních a provozních událostech. Zaznamenává se: -datum a čas, -typ činnosti, -identifikace technického aktiva, které činnost zaznamenalo, -jednoznačná identifikace účtu, pod kterým byla činnost provedena, -úspěšnost nebo neúspěšnost činností.
Stav	Neaplikováno
Komentář	

Požadavek	Je prováděn sběr informací pro ochranu před neoprávněným čtením a jakoukoliv změnou. Zaznamenává se: -přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů, -činnosti provedené administrátory, -úspěšné i neúspěšné manipulace s účty, oprávněními a právy, -neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, -činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému, -zahájení a ukončení činností technických aktiv, -kritické i chybové hlášení technických aktiv.
Stav	Neaplikováno
Komentář	

Požadavek	Synchronizace jednotného času technických aktiv je prováděna nejméně jednou za 24 hodin.
Stav	Neaplikováno
Komentář	

Požadavek	Záznamy o zaznamenaných událostech jsou uchovávány nejméně po dobu 12 měsíců.
Stav	Neaplikováno
Komentář	

Detekce kybernetických bezpečnostních událostí

Požadavek	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí: -ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi.
Stav	Neaplikováno
Komentář	

Požadavek	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí: - ověření a kontrolu přenášených dat na perimetru komunikační sítě.
Stav	Neaplikováno
Komentář	

Požadavek	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí: - blokování nežádoucí komunikace.
Stav	Neaplikováno
Komentář	

Aplikační bezpečnost

Požadavek	Jsou prováděny penetrační tesy informačního a komunikačního systému se zaměřením na důležitá aktiva a to před jejich uvedením do provozu.
Stav	Neaplikováno
Komentář	

Požadavek	Je zajištěna trvalá ochrana aplikací, informací a transakcí před neoprávněnou činností a popřením provedených činností.
Stav	Částečně aplikováno
Komentář	

Kryptografické prostředky

Požadavek	Jsou používány aktuální odolné kryptografické algoritmy a kryptografické klíče.
Stav	Neaplikováno
Komentář	

Požadavek	Je použit systém správy klíčů a certifikátů, který: - zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů, - umožní kontrolu a audit.
Stav	Aplikováno
Komentář	

Bezpečnostní politika a bezpečnostní dokumentace

Požadavek	Je stanovena bezpečnostní politika.
Stav	Neaplikováno
Komentář	

Požadavek	Bezpečnostní politika je pravidelně přezkoumávána a dokumentována.
Stav	Neaplikováno
Komentář	

Požadavek	Jsou identifikovány, hodnoceny a evidovány primární aktiva.
Stav	Neaplikováno
Komentář	

Požadavek	Aktiva jsou hodnoceny z hlediska důvěrnosti, integrity a dostupnosti.
Stav	Neaplikováno
Komentář	

Požadavek	Jsou určeny bezpečnostní role a jejich práva a povinnosti.
Stav	Částečně aplikováno
Komentář	

Požadavek	Politika řízení dodavatelů.
Stav	Neaplikováno
Komentář	

Požadavek	Politika bezpečnosti lidských zdrojů.
Stav	Neaplikováno
Komentář	

Požadavek	Bezpečnostní školení nových uživatelů.
Stav	Částečně aplikováno
Komentář	

Požadavek	Politika řízení přístupu.
Stav	Částečně aplikováno
Komentář	

Požadavek	Politika zálohování a dlouhodobého ukládání.
Stav	Částečně aplikováno
Komentář	

Požadavek	Politika bezpečného předávání a výměny informací
Stav	Neaplikováno
Komentář	

Požadavek	Politika řízení technických zranitelností.
Stav	Neaplikováno
Komentář	

Požadavek	Politika bezpečného používání mobilních zařízení.
Stav	Neaplikováno
Komentář	

Požadavek	Politika akvizice, vývoje a údržby.
Stav	Neaplikováno
Komentář	

Požadavek	Politika ochrany osobních údajů.
Stav	Aplikováno
Komentář	

Požadavek	Politika fyzické bezpečnosti.
Stav	Aplikováno
Komentář	

Požadavek	Politika bezpečnosti komunikační sítě.
Stav	Částečně aplikováno
Komentář	

Požadavek	Politika ochrany před škodlivým kódem
Stav	Neaplikováno
Komentář	

Požadavek	Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
Stav	Neaplikováno
Komentář	

Požadavek	Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.
Stav	Neaplikováno
Komentář	

Požadavek	Politika bezpečného používání kryptografické ochrany.
Stav	Neaplikováno
Komentář	

Požadavek	Politika řízení kontinuity činností.
Stav	Neaplikováno
Komentář	

Příloha č. 2: Souhrn asistovaného zhodnocení k opatřením ISMS

A.5	**Politiky a bezpečnosti informací**	
A.5.1	Směřování bezpečnosti informací vedením organizace	
A.5.1.1	Politiky pro bezpečnost informací	**Neaplikováno**
A.5.1.2	Přezkoumání politik pro bezpečnost informací	**Neaplikováno**
A.6	**Organizace bezpečnosti informací**	
A.6.1	**Interní organizace**	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	**Neaplikováno**
A.6.1.2	Princip oddělení povinností	**Neaplikováno**
A.6.1.3	Kontakt s příslušnými orgány a autoritami	**Neaplikováno**
A.6.1.4	Kontakt se zájmovými skupinami	**Neaplikováno**
A.6.1.5	Bezpečnost informací v řízení projektů	**Neaplikováno**
A.6.2	**Mobilní zařízení a práce na dálku**	
A.6.2.1	Politika mobilních zařízení	**Neaplikováno**
A.6.2.2	Práce na dálku	**Neaplikováno**
A.7	**Bezpečnost lidských zdrojů**	
A.7.1	**Před vznikem pracovního vztahu**	
A.7.1.1	Prověřování	**Částečně**
A.7.1.2	Podmínky pracovního vztahu	**Aplikováno**
A.7.2	**Během pracovního vztahu**	
A.7.2.1	Odpovědnosti vedení organizace	**Částečně**
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	**Neaplikováno**
A.7.2.3	Disciplinární řízení	**Částečně**
A.7.3	**Ukončení a změna pracovního vztahu**	
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	**Aplikováno**
A.8	**Řízení aktiv**	
A.8.1	**Odpovědnost za aktiva**	
A.8.1.1	Seznam aktiv	**Aplikováno**
A.8.1.2	Vlastnictví aktiv	**Aplikováno**
A.8.1.3	Přípustné použití aktiv	**Neaplikováno**
A.8.1.4	Navrácení aktiv	**Aplikováno**
A.8.2	**Klasifikace informací**	
A.8.2.1	Klasifikace informací	**Neaplikováno**
A.8.2.2	Označování informací	**Neaplikováno**
A.8.2.3	Manipulace s aktivy	**Neaplikováno**

A.8.3	**Manipulace s médii**	
A.8.3.1	Správa výměnných médií	**Neaplikováno**
A.8.3.2	Likvidace médií	**Neaplikováno**
A.8.3.3	Přeprava fyzických médií	**Neaplikováno**
A.9	**Řízení přístupu**	
A.9.1	**Požadavky organizace na řízení přístupu**	
A.9.1.1	Politika řízení přístupu	**Částečně**
A.9.1.2	Přístup k sítím a síťovým službám	**Částečně**
A.9.2	**Řízení přístupu uživatelů**	
A.9.2.1	Registrace a zrušení registrace uživatele	**Částečně**
A.9.2.2	Správa uživatelských přístupů	**Částečně**
A.9.2.3	Správa privilegovaných přístupových práv	**Částečně**
A.9.2.4	Správa tajných autentizačních informací uživatelů	**Částečně**
A.9.2.5	Přezkoumání přístupových práv uživatelů	**Aplikováno**
A.9.2.6	Odebrání nebo úprava přístupových práv	**Aplikováno**
A.9.3	**Odpovědnosti uživatelů**	
A.9.3.1	Používání tajných autentizačních informací	**Částečně**
A.9.4	**Řízení přístupu k systémům a aplikacím**	
A.9.4.1	Omezení přístupu k informacím	**Aplikováno**
A.9.4.2	Bezpečné postupy přihlášení	**Částečně**
A.9.4.3	Systém správy hesel	**Částečně**
A.9.4.4	Použití privilegovaných programových nástrojů	**Neaplikováno**
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	**Částečně**
A.10	**Kryptografie**	
A.10.1	**Kryptografická opatření**	
A.10.1.1	Politika pro použití kryptografických opatření	**Neaplikováno**
A.10.1.2	Správa klíčů	**Neaplikováno**
A.11	**Fyzická bezpečnost a bezpečnost prostředí**	
A.11.1	**Bezpečné oblasti**	
A.11.1.1	Fyzický bezpečnostní perimetr	**Částečně**
A.11.1.2	Fyzické kontroly vstupu	**Aplikováno**
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	**Aplikováno**
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	**Aplikováno**
A.11.1.5	Práce v bezpečných oblastech	**Neaplikováno**
A.11.1.6	Oblasti pro nakládku a vykládku	**Nerelevantní**
A.11.2	**Zařízeni**	
A.11.2.1	Umístění zařízení a jeho ochrana	**Částečně**
A.11.2.2	Podpůrné služby	**Neaplikováno**
A.11.2.3	Bezpečnost kabelových rozvodů	**Částečně**
A.11.2.4	Údržba zařízení	**Neaplikováno**
A.11.2.5	Přemístění aktiv	**Neaplikováno**
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	**Neaplikováno**
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	**Neaplikováno**
A.11.2.8	Uživatelská zařízení bez obsluhy	**Neaplikováno**
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	**Neaplikováno**

A.12	**Bezpečnost provozu**	
A.12.1	**Provozní postupy a odpovědnosti**	
A.12.1.1	Dokumentované provozní postupy	**Částečně**
A.12.1.2	Řízení změn	**Částečně**
A.12.1.3	Řízení kapacit	**Neaplikováno**
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	**Nerelevantní**
A.12.2	**Ochrana proti malwaru**	
A.12.2.1	Opatření proti malwaru	**Neaplikováno**
A.12.3	**Zálohování**	
A.12.3.1	Zálohování informací	**Částečně**
A.12.4	**Zaznamenávání formou logů a monitorování**	
A.12.4.1	Zaznamenávání událostí formou logů	**Částečně**
A.12.4.2	Ochrana logů	**Částečně**
A.12.4.3	Logy o činnosti administrátorů a operátorů	**Částečně**
A.12.4.4	Synchronizace hodin	**Neaplikováno**
A.12.5	**Správa provozního softwaru**	
A.12.5.1	Instalace softwaru na provozní systémy	**Částečně**
A.12.6	**Řízení technických zranitelností**	
A.12.6.1	Řízení technických zranitelností	**Neaplikováno**
A.12.6.2	Omezení instalace softwaru	**Částečně**
A.12.7	**Hlediska auditu informačních systémů**	
A.12.7.1	Opatřeni k auditu informačních systémů	**Částečně**
A.13	**Bezpečnost komunikací**	
A.13.1	**Správa bezpečnosti sítě**	
A.13.1.1	Opatření v sítích	**Aplikováno**
A.13.1.2	Bezpečnost síťových služeb	**Částečně**
A.13.1.3	Princip oddělení v sítích	**Částečně**
A.13.2	**Přenos informací**	
A.13.2.1	Politiky a postupy při přenosu informací	**Neaplikováno**
A.13.2.2	Dohody o přenosu informací	**Neaplikováno**
A.13.2.3	Elektronické předávání zpráv	**Částečně**
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	**Částečně**
A.14	**Akvizice, vývoj a údržba systémů**	**Nerelevantní**
A.15	**Dodavatelské vztahy**	
A.15.1	**Bezpečnost informací v dodavatelských vztazích**	
A.15.1.1	Politika bezpečnosti informaci pro dodavatelské vztahy	**Neaplikováno**
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	**Částečně**
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	**Neaplikováno**
A.15.2	**Řízení dodávek služeb dodavatelů**	
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	**Neaplikováno**
A.15.2.2	Řízení změn ve službách dodavatelů	**Neaplikováno**

A.16	**Řízení incidentů bezpečnosti informací**	
A.16.1	**Řízení incidentů bezpečnosti informací a zlepšování**	
A.16.1.1	Odpovědnosti a postupy	**Neaplikováno**
A.16.1.2	Hlášení událostí bezpečnosti informací	**Neaplikováno**
A.16.1.3	Hlášení slabých míst bezpečnosti informací	**Částečně**
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	**Neaplikováno**
A.16.1.5	Reakce na incidenty bezpečnosti informací	**Neaplikováno**
A.16.1.6	Ponaučeni z incidentů bezpečnosti informací	**Neaplikováno**
A.16.1.7	Shromažďování důkazů	**Neaplikováno**
A.17	**Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací**	
A.17.1	**Kontinuita bezpečnosti informací**	
A.17.1.1	Plánování kontinuity bezpečnosti informací	**Neaplikováno**
A.17.1.2	Implementace kontinuity bezpečnost informací	**Neaplikováno**
A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	**Neaplikováno**
A.17.2	**Redundance**	
A.17.2.1	Dostupnost vybavení pro zpracování informací	**Částečně**
A.18	**Soulad s požadavky**	
A.18.1	**Soulad s právními a smluvními požadavky**	
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	**Aplikováno**
A.18.1.2	Ochrana duševního vlastnictví	**Aplikováno**
A.18.1.3	Ochrana záznamů	**Aplikováno**
A.18.1.4	Soukromí a ochrana osobních údajů	**Aplikováno**
A.18.1.5	Regulace kryptografických opatření	**Neaplikováno**
A.18.2	**Přezkoumání bezpečnosti informací**	
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	**Neaplikováno**
A.18.2.2	Shoda s bezpečnostními politikami a normami	**Neaplikováno**
A.18.2.3	Přezkoumání technické shody	**Neaplikováno**

Příloha č. 3: Matice úrovně rizik

ZRANITELNOST [V]		AKTIVUM	Data o zaměstnancích	Data o studentech	Zálohování dat	Administrativní data	Stolní počítače	Notebooky	Mobilní zařízení	Tiskárny	Server	Aktivní síťové prvky	Pasivní síťové prvky	Diskové pole	Firewall	IS - Bakaláři	Operační systém	Účetní SW	Internetové připojení	Elektronická pošta	Webové stránky	Zálohování
		A	3	4	5	2	2	3	3	1	3	4	4	5	3	4	3	4	3	4	3	4
HROZBA	**T**																					
Požár	2						12	18	12	6	18	24	32	30	18				18			
Poškození vodou	2						12	18	18	4	12	16	8	20	12				12			
Zničení zařízení nebo médií	3						18	18	18	6	18	24	24	50	18				18			
Meterologický jev	1																					
Povodeň	1						8	9	9	4	12	16	16	20	12				12			
Selhání klimatizace nebo dodávky vody	2																					
Přerušení dodávky elektřiny	3		36	48	60	18	18	18	3	6	27	48	48	45	48				36	36	27	24
Selhání telekomunikačního zařízení	3		36	48	60	18	12	18	27	6	18	24	24									
Vzdálená špionáž	1		4	16	20	6	4	6	3	1	6	12	8	10	18	8		24				
Odposlech	1																		9	8	6	
Krádež médií nebo dokumentů	3		27	48	5	12																
Krádež zařízení	3						12	27	36	3	9	24	12	30	18							
Vyzrazení	4		36	48	60	24																
Falšování pomocí aplikačního vybavení	3		18	36	45	12										12	9	24				
Selhání zařízení	4						16	24	12	4	36	48	32	40	36							
Chybové fungování zařízení	3						12	18	18	3	27	36	24	30	27							
Přetížení informačního systému	2		24	32	20	8										32	12	16				
Chyba údržby	3						12	18	18	6	27	18	24	30	18	36	18	24				
Neoprávněné použití zařízení	3						12	27	18	3	18	36	36	30	18							
Podvodné kopírování aplikačního programového vybavení	1															8	6	12				
Poškození dat	2		18	24	30	12																
Nezákonné zpracování dat	1		9	12	15	6										8		16				
Chyba v používání	3		27	36	45	12	18	27	27	6	9	24	36	60	27				18	24	18	24
Zneužití oprávnění	4		36	48	60	24	24	48	36	8	24	48	32	40	36	64	36	64	36	32	12	
Falšování práv	2		18	24	20	8																
Odepření činností	3						12	18	18	3	27	36		30	27	36	18	24				
Nedostatek personálu	4																	32				

Příloha č. 4: Matice zranitelnosti

		Informační aktiva					Hardwarová aktiva									SW aktiva			Služby			
ZRANITELNOST [V]		AKTIVUM	Data o zaměstnancích	Data o studentech	Zálohování dat	Administrativní data	Stolní počítače	Notebooky	Mobilní zařízení	Tiskárny	Server	Aktivní síťové prvky	Pasivní síťové prvky	Diskové pole	Firewall	IS - Bakaláři	Operační systém	Účetní SW	Internetové připojení	Elektronická pošta	Webové stránky	Zálohování
		A	3	4	5	2	2	3	3	1	3	4	4	5	3	4	3	4	3	4	3	4
HROZBA	**T**																					
Požár	2						3	3	2	3	3	3	4	3	3				3			
Poškození vodou	2						3	3	3	2	2	2	1	2	2				2			
Zničení zařízení nebo médií	3						3	2	2	2	2	2	2	2	2				2			
Meterologický jev	1																					
Povodeň	1						4	3	3	4	4	4	4	4	4				4			
Selhání klimatizace nebo dodávky vody	2																					
Přerušení dodávky elektřiny	3		4	4	4	3	3	2	1	2	3	4	4	3	4				4	3	3	2
Selhání telekomunikačního zařízení	3		4	4	4	3	2	2	3	2	2	2	2									
Vzdálená špionáž	1		4	4	4	3	2	2	1	1	2	3	2	2	3	2		3				
Odposlech	1																		3	2	2	
Krádež médií nebo dokumentů	3		3	4	1	2																
Krádež zařízení	3						2	3	4	1	1	2	1	2	2							
Vyzrazení	4		3	3	3	3																
Falšování pomocí aplikačního vybavení	3		2	3	3	2										1	1	2				
Selhání zařízení	4						2	2	1	1	3	3	2	2	3							
Chybové fungování zařízení	3						2	2	2	1	3	3	2	2	3							
Přetížení informačního systému	2		4	4	2	2										4	2	2				
Chyba údržby	3						2	2	2	2	3	2	2	2	2	3	2	2				
Neoprávněné použití zařízení	3						2	3	2	1	2	3	3	2	2							
Podvodné kopírování aplikačního programového vybavení	1															2	2	3				
Poškození dat	2		3	3	3	3																
Nezákonné zpracování dat	1		3	3	3	3										2		4				
Chyba v používání	3		3	3	3	2	3	3	3	2	1	2	3	2	3				2	2	2	2
Zneužití oprávnění	4		3	3	3	3	3	4	3	2	2	3	2	2	3	4	3	4	3	2	1	
Falšování práv	2		3	3	2	2																
Odepření činností	3						2	2	2	1	3	3		2	3	3	2	2				
Nedostatek personálu	4																	2				

Příloha č. 5: Prohlášení o aplikovatelnosti první etapy

A.5 Politiky bezpečnosti opatření

Cíl: Vytvoření politik a podpory ze strany managementu pro bezpečnost informací, které jsou v souladu s požadavky organizace a příslušnými právními zákony a předpisy.

A.5.1.1 Politiky pro bezpečnost informací

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Vytvoření bezpečnostní politiky
- **Dokument:** Politika pro bezpečnost informací
- **Opatření:** Soubor politik pro bezpečnost informací musí být definován, schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním externím stranám.

A.5.1.2 Přezkoumání politik pro bezpečnost informací

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Přezkoumání politik, jejich přiměřenosti, vhodnosti a celkové efektivnosti zavedených bezpečnostních opatření. Přezkoumání se provádí v pravidelných cyklech. Nejdelší možná lhůta je 12 měsíců.
- **Dokument:** Záznam o přezkoumání politik pro bezpečnostní opatření
- **Opatření:** Pro zjištění neustálé vhodnosti, přiměřenosti a efektivnosti musí být politiky pro bezpečnost informací přezkoumávány v plánovaných intervalech vždy, když nastane významná změna.

A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Stanovit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.

A.6.1.1 Role a odpovědnosti bezpečnosti informací

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Určením vedení společnosti.
- **Dokument:** Pracovní smlouva, pracovní řád
- **Opatření:** Musí být definovány a přiděleny odpovědnosti v oblasti bezpečnosti informací.

A.6.1.2 Princip oddělení povinností

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Určením vedení společnosti (dokument určující role, odpovědnosti, pracovní pozice, odpovědnosti, práva).
- **Dokument:** Součástí bezpečnostních politik
- **Opatření:** Pro snížení příležitostí k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv organizace musí být zajištěno oddělení neslučitelných povinností a odpovědností

A.6.1.3 Kontakt s příslušnými orgány a autoritami

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Pravidelné aktualizování seznamu využívaných kontaktů.
- **Opatření:** Musí být udržovány přiměřené vztahy s příslušnými orgány a autoritami.

A.6.1.4 Kontakt se zájmovými skupinami

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Sledování novinek vztahující se ke kybernetické bezpečnosti (například webové stránky NÚKIB).
- **Opatření:** Musí být udržovány přiměřené vztahy s odbornými zájmovými skupinami nebo ostatními odbornými fóry na bezpečnost a profesními sdruženími.

A.6.1.5 Bezpečnost informací v řízení projektů

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Organizace se řídí dle norem a doporučení, které se týkají informační bezpečnosti.
- **Dokument:** Příručka ISMS
- **Opatření:** Bezpečnost informací musí být zohledněna v řízení projektů nezávisle na typu projektu.

A.6.2 Mobilní zařízení a práce na dálku

Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.

A.6.2.1 Politika mobilních zařízení

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Vytvoření manuálu obsahující politiky a práva pro uživatele mobilních zařízení.
- **Dokument:** Příručka ISMS
- **Opatření:** Musí být přijata politika a relevantní bezpečnostní opatření pro zvládání rizik spojených s používáním mobilních zařízení.

A.6.2.2 Práce na dálku

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Definování požadavků vztahující se k práci na dálku.
- **Dokument:** Příručka ISMS
- **Opatření:** Musí být implementována politika a relevantní bezpečnostní opatření na ochranu informací, která jsou přístupná, zpracovaná nebo ukládaná v místech pro práci na dálku.

A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.

A.8.1.3 Přípustné použití aktiv

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Dokument definující přípustné použití aktiv v organizaci.
- **Dokument:** Politika organizace
- **Opatření:** Musí být určena, dokumentována a implementována pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a vybavením pro zpracování informací.

A.8.2 Klasifikace informací

Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.

A.8.2.1 Klasifikace informací

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Dokumentace ISMS
- **Dokument:** Politika organizace
- **Opatření:** Informace musí být klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci.

A.8.2.2 Označování informací

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Dokumentace ISMS
- **Dokument:** Politika organizace
- **Opatření:** Pro označování informací musí být vytvořen a implementován vhodný soubor postupů, které budou v souladu se schématem klasifikace informací přijatým organizací.

A.8.2.3 Manipulace s aktivy

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Dokumentace ISMS
- **Dokument:** Politika organizace
- **Opatření:** Pro manipulaci s aktivy musí být vytvořeny a implementovány postupy v souladu se schématem klasifikace informací přijatých organizací.

A.8.3 Manipulace s médii

Cíl: Předcházet neoprávněnému vyzrazení, modifikací, odstranění nebo zničení informací uložených na médiích.

A.8.3.1 Správa výměnných médií

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Provozní řád organizace, Pracovní smlouva
- **Dokument:** Provozní řád
- **Opatření:** Musí být implementovány postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatých organizací.

A.8.3.2 Likvidace médií

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Média jsou destruktivně ničena, aby nemohla být znovu použita.
- **Dokument:** Provozní řád
- **Opatření:** Média, pokud nejsou dále upotřebitelná, musí být bezpečně zlikvidována v souladu s formalizovanými postupy.

A.8.3.3 Přeprava fyzických médií

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Jsou definovány postupy, jak média přepravovat
- **Dokument:** Provozní řád
- **Opatření:** Média obsahující informace musí být během přepravy chráněna proti neoprávněnému přístupu, zneužití nebo narušení.

A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajisti řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací.

A.10.1.1 Politika pro použití kryptografických opatření

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Vytvoření dokumentu obsahující pravidla a postupy pro kryptografii a šifrování.
- **Dokument:** Provozní řád
- **Opatření:** Musí být vytvořena a implementována politika pro užívání kryptografických opatření na ochranu informací.

A.10.1.2 Správa klíčů

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** dle nastavených pravidel (provozní řád organizace)
- **Dokument:** Provozní řád
- **Opatření:** Politika pro používání, ochranu a dobu existence kryptografických klíčů musí být vytvořena a implementována po celou dobu jejich životního cyklu.

A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Bezpečné oblasti

Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.

A.11.1.1 Fyzický bezpečnostní perimetr

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Provedení celkové revize a zlepšování slabých míst (bezpečnostní dveře, zámky, atd.).
- **Dokument:** Provozní řád
- **Opatření:** Bezpečnostní perimetry musí být definovány a používány k ochraně oblastí, které obsahují citlivé nebo kritické informace a vybavení pro zpracování informací.

A.11.1.2 Fyzické kontroly vstupu

- **Vyloučeno:** Ne
- **Způsob plnění požadavku:** Pomocí video zvonku sekretářka kontroluje a povoluje vstup osobám do budovy.
- **Dokument:** Provozní řád
- **Opatření:** Aby bylo zajištěno, že je přístup do bezpečných oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.