VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

BUDOVÁNÍ BEZPEČNOSTNÍHO POVĚDOMÍ NA ZÁKLADNÍ ŠKOLE

INCREASE OF SECURITY AWARENESS AT THE PRIMARY SCHOOL

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Jana Kolajova**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Jana Kolajova**
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:

Budování bezpečnostního povědomí na základní škole

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury

Cíle, kterých má být dosaženo:

Cílem diplomové práce je vypracovat vhodný plán vedoucí ke zvyšování bezpečnostního povědomí na základních školách. Tento plán je vypracován na míru pro konkrétní základní školu. Zavedení programu by mělo vést k větší informovanosti, čímž by mělo dojít k zajištění ochrany a zvýšení bezpečnosti všech osob.

Základní literární prameny:

ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK V., P. SEDLÁK a V. 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 problematikou budování bezpečnostního povědomí na základní škole. Práci lze rozdělit na tři hlavní části. V úvodní části jsou uvedeny základní pojmy z oblasti informační bezpečnosti a stručný popis legislativních náležitostí, které je třeba dodržet pro správný návrh programu. Ve druhé části je provedena analýza současné situace na vybrané základní škole, včetně zpracování analýzy SLEPT, Porterovy analýzy pěti sil, analýzy 7S a SWOT. V praktické části je představen návrh zavedení programu, který je plně uzpůsoben požadavkům a potřebám základní školy. V poslední části jsou zhodnoceny přínosy a nedostatky zavedeného řešení.

KLÍČOVÁ SLOVA

budování bezpečnostního povědomí, informační bezpečnost, kybernetická bezpečnost, informace, data, GDPR, ISMS

ABSTRACT

This diploma thesis is focused on the development of informational environment safety awareness at primary schools. The thesis consists of three main parts. The introduction explains the basic safety terms and briefly describe the legislative essentials necessary for this proposal. The second part consists of the analysis of the current situation at the school chosen for this research, including SLEPT analysis, Porter´s analysis, 7S analysis, and SWOT analysis. The practical part introduces the proposal of implementation of the program which is tailored to the requirements and needs of the primary school. The final part evaluates the pros and cons of the implemented solution.

KEY WORDS:

Development of security awareness, information security, cyber security, information, data, GDPR, ISMS

BIBLIOGRAFICKÁ CITACE

KOLAJOVÁ, Jana. Budování bezpečnostního povědomí na základní škole [online]. Brno, 2019 [cit. 2019-05-09]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119828. 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 zpracovala 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 9. května 2019

……

Bc. Jana Kolajová

PODĚKOVÁNÍ

Na tomto místě bych chtěla poděkovat panu Ing. Petru Sedlákovi, který mi byl oporou při psaní práce a uděloval mi cenné rady. Dále bych chtěla poděkovat vedení základní školy, školní psycholožce a učiteli CVT, kteří mi svými připomínkami a sdělenými informacemi pomohli práci zdárně dokončit. V neposlední řadě bych ráda poděkovala Ing. Jiřímu Rubášovi za veškerou podporu.

OBSAH

OBSAH 5

ÚVOD 10

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE 11

1 TEORETICKÁ VÝCHODISKA PRÁCE 12

1.1 Základní pojmy 12

1.2 Oblast analýzy rizik 15

1.3 Oblast GDPR 15

1.4 ISMS 16

1.4.1 Postupy zavádění ISMS 17

1.5 Normy a zákony 17

1.5.1 Normy řady 27000 18

1.5.2 NIST standardy 20

1.5.3 Kybernetický zákon č. 205/2017 Sb. 21

1.5.4 Vyhláška č. 316/2014 Sb. 21

1.6 Bezpečnost informací v akademickém prostředí 21

1.7 Přiměřená bezpečnost 22

1.8 Kybernetická bezpečnost v ČR 22

1.9 NÚKIB 23

1.10 Bezpečnostní týmy v ČR 24

1.11 Evropské nařízení GDPR 24

1.11.1 DPO 25

1.11.2 Správce – povinnosti, odpovědnost 26

1.11.3 Zpracovatel – povinnosti, odpovědnost 27

1.12 PDCA cyklus 27

1.13 Program SAE 28

1.13.1 Modely programu SAE 29
1.13.2 Fáze programu 30
1.13.3 Odpovědnosti v programu 32
1.14 Bezpečnost počítačové sítě 33
1.14.1 Cloud computing 34
1.15 Analýza rizik 35
1.16 SLEPT 36
1.17 Porterova analýza pěti sil 37
1.18 Analýza 7S 38
1.19 SWOT analýza 39
1.20 Lewinův model 40
1.21 PERT 41
2 ANALÝZA SOUČASNÉHO STAVU 42
2.1 Popis organizace 42
2.2 Organizační struktura 42
2.3 Vybavení školy 43
2.3.1 Hardware 43
2.3.2 Software 45
2.3.3 Fyzická bezpečnost objektu 45
2.4 Bezpečnost dat 46
2.5 Budování bezpečnostního povědomí SAE 46
2.6 SLEPT 47
2.7 Porterova analýza pěti sil 48
2.8 Analýza 7S 49
2.9 SWOT analýza 51
2.10 Zhodnocení analýzy 52

2.10.1 Informační systém školní jídelny ... 52
3 VLASTNÍ NÁVRHY ŘEŠENÍ ... 57
3.1 Cíl programu ... 57
3.2 Výstupy ... 57
3.3 Přínosy ... 58
3.4 Plán ... 58
3.5 Lewinův model ... 58
3.5.1 Analýza situace ... 58
3.5.2 Identifikace agenta změny ... 59
3.5.3 Identifikace intervenčních oblastí ... 61
3.5.4 Intervence ... 61
3.5.5 Verifikace ... 62
3.6 PERT ... 62
3.6.1 Seznam činností ... 62
3.6.2 Návaznost a odhad doby trvání činností v hodinách ... 63
3.6.3 Návaznost činností ... 64
3.6.4 Časová analýza ... 64
3.6.5 Síťový graf ... 65
3.7 Analýza rizik ... 67
3.7.1 Mapa rizik ... 68
3.7.2 Zhodnocení analýzy rizik ... 71
3.8 Rozsah programu ... 71
3.9 Role a odpovědnosti SAE ... 72
3.9.1 CISO ... 72
3.9.2 Ředitel školy ... 73
3.9.3 Učitelé ... 73

3.9.4 Ostatní uživatelé ... 73
3.10 Rozdělení uživatelů ... 73
3.11 Fáze programu ... 75
3.11.1 Povědomí ... 75
3.11.2 Školení ... 75
3.11.3 Vzdělávání ... 77
3.11.4 Profesní rozvoj ... 78
3.12 Povědomí – podpůrné a školící materiály ... 78
3.12.1 Bezpečnostní desatero ... 79
3.13 Bezpečnostní politika ... 80
3.13.1 Cíle bezpečnosti ... 81
3.13.2 Šíření působnosti a politiky bezpečnosti ... 81
3.13.3 Doprovodná dokumentace ... 84
3.14 Budování bezpečnostního povědomí u žáků ... 85
3.15 Post-implementační část ... 88
3.15.1 Dokumentace ... 88
3.15.2 Četnost opakování, aktualizace materiálů ... 88
3.16 Přínos návrhů řešení ... 89
4 ZÁVĚR ... 91
SEZNAM POUŽITÉ LITERATURY ... 92
SEZNAM TABULEK ... 96
SEZNAM OBRÁZKŮ ... 97

ÚVOD

V dnešní době moderních technologií a růstu komunikačních technologií je nutné změnit celkový pohled na bezpečnost. Lidé přichází do styku s technologiemi ve stále nižším věku, více než polovina dětí již ve školce. Dospívající se věnují internetu více, než povinnostem doma, případně přípravě do školy, a zaměstnanci jsou i okolím donuceni věnovat více času online, než tomu bylo dříve. Je třeba přizpůsobit se tomuto trendu a vytvořit opatření, která by v rámci školení pro všechny věkové kategorie byla akceptována.

Tato práce se zabývá budováním bezpečnostního povědomí na základní škole, z čehož vyplývá, že se věnuje dvěma rovinám. První z nich je školení pro zaměstnance školy. V současné době při nástupu do zaměstnání probíhá pouze školení BOZP (bezpečnost a ochrana zdraví při práci) a PO (požární ochrana), což je nedostatečné. Vzhledem k faktu, že každý pedagog denně pracuje s ICT a s osobními údaji svých žáků a jejich zákonných zástupců, je zapotřebí přidat ještě jedno školení, a to školení o informační bezpečnosti. Druhá rovina se týká žáků školy. Podle předpisů má probíhat jednou ročně hodinové školení pro každou třídu na škole vycházející z BOZP a PO, nicméně informace o tom, jak mají žáci zacházet s daty a při práci na internetu, chybí.

Při zavedení programu budou mít děti šanci rozvíjet technickou a informační bezpečnost již od útlého věku a zaměstnanci školy budou správně nakládat s daty, které jim byly svěřeny.

VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem této diplomové práce je vybudovat a zavést program vedoucí ke zvýšení bezpečnostního povědomí na základní škole. Program je uzpůsoben požadavkům a potřebám jedné konkrétní základní školy. Výsledkem práce by mělo být zajištění dostatečné informovanosti pracovníků a žáků školy, které následně povede k většímu zajištění ochrany a bezpečnosti uživatelů, včetně jejich okolí.

Aby bylo tohoto cíle dosaženo, je nutné definovat dílčí cíle, po jejichž splnění dojde k utvoření celku, a, při dodržení všech postupů, i ke správnému dosažení cíle. V první řadě je nutné uvést základní informace z oblasti informační a kybernetické bezpečnosti. K pochopení celkové problematiky budeme vyházet ze SAE a ISMS, které je nutné zmínit a rozepsat poznatky z dané oblasti. S tím souvisí popis norem, zákonů a různých nařízení, které se obsahu týkají.

Ve druhé řadě dojde k popisu současného stavu základní školy, kde bude zmíněna organizační struktura školy, kompetence a z nich vyplývající odpovědnosti. S analýzou současného stavu souvisí také analýza rizik spojených s projektem. Ty jsou analyzovány pomocí metod SLEPT, 7S, Porterovy analýzy, SWOT, PERT a Lewinova modelu.

Řešení diplomové práce vychází z metodiky NIST SP 800-50, která slouží jako podklad pro tvorbu projektu, a z programu SAE, který slouží k určení rolí a odpovědností. Dále k řešení patří stanovení jednotlivých cílů pro jednotlivé fáze, vytvoření podkladů pro fáze školení a finanční plán projektu.

1 TEORETICKÁ VÝCHODISKA PRÁCE

K pochopení praktické části je nutné vytvořit přehled základních pojmů týkajících se dané oblasti. Tato kapitola tedy obsahuje všechny potřebné znalosti, které jsou využity při vlastním návrhu řešení.

1.1 Základní pojmy

Audit (v kontextu informační bezpečnosti) – proces, který zajišťuje (dohromady s autentizací a identifikací) individuální odpovědnost uživatele (za danou činnost), jenž nakládá s osobními údaji. [1]

Autentizace – ověření pravosti identity. V praxi například přihlášení a odhlášení. Dělí se na autentizace - hesla, autentizace - tokeny, autentizace - biometriky.[2]

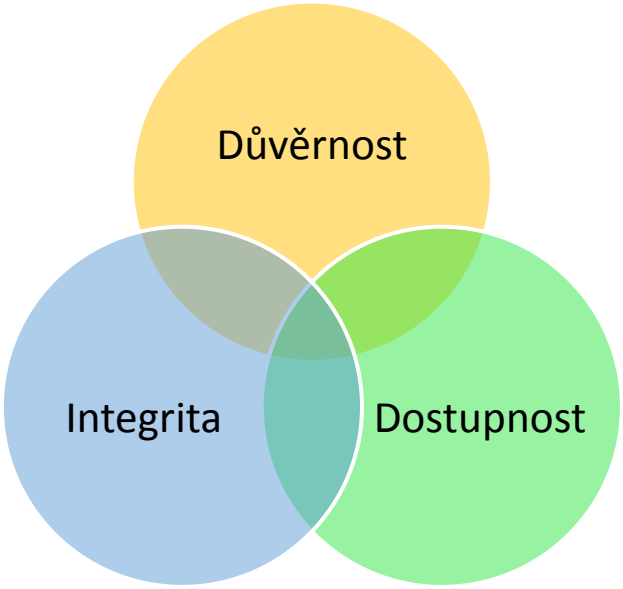
Autorizace – je získání oprávnění k nějaké akci, nebo k jejímu provedení. Z pravidla často navazuje na již dříve zmíněný proces autentizace. [2]

Bezpečnostní politika – právní dokument, který popisuje, jakým způsobem je řízena bezpečnost v organizaci. Jedná se o základní dokument pro zajištění informační bezpečnosti. Vychází z něj všechny standardy, směrnice a opatření ve firmě. Pro zaměstnance je závazná. [3]

Data – představují fakta, měření, obraz, zvuk, video, nejčastěji v kontextu sledovaného procesu nebo situace. Data jsou často vstupem či výstupem počítačového programu. V praxi lze připodobnit ke zprávě. Častou jsou chápány jako potencionální informace, která umožňuje komunikaci, zpracování nebo vyhodnocování. [2]

Dostupnost – v požadovaný okamžik je zajištěn přístup k informacím oprávněnému uživateli. [4]

Důvěrnost – zaručuje, že informace není dostupná nebo prozrazená neautorizovaným osobám, entitám nebo procesům. [4]



Obrázek č. 1: CIA triáda
(Zdroj: Vlastní zpracování dle č. 4)

Hoax – šíření poplašných, nebezpečných a často zbytečných řetězových zpráv. V dnešní době však předcházejí, nebo se snaží předejít tzv. hoaxům například stránky na kterých lze spolehlivě dohledat klamavou zprávu. Největším přítelem a zároveň nepřítelem jim však je rychlost, kterou se zprávy šíří mezi lidmi. [5]

Incident – jedná se o kybernetickou bezpečnostní událost, která představuje narušení bezpečnosti informací v IS, případně narušení bezpečnosti služeb a sítí elektronických komunikací. [6]

Informace – v nejobecnějším slova smyslu je informace chápána jako údaj o reálném prostředí, o jeho stavu a procesech v něm probíhajících. Tvoří také protiklad šumu. Jedná se o kódovaná data, se kterými je možné pracovat pomocí technických zařízení. Informace snižují neurčitost. [2]

Informační bezpečnost – ochrana informací ve všech formách a během celého životního cyklu. Jedná se o ochranu před narušením integrity, důvěrnosti či dostupnosti informace. [4]

Informační systém – soubor technických prostředků (HW, SW) a dat, který je určen ke sběru, zpracování, užití, uložení a sdílení. [2]

Integrita – zajištění úplnosti a správnosti dodávaných informací. [4]

Kritická infrastruktura – dle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), se jedná o prvek nebo systém prvků, jehož narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. [2]

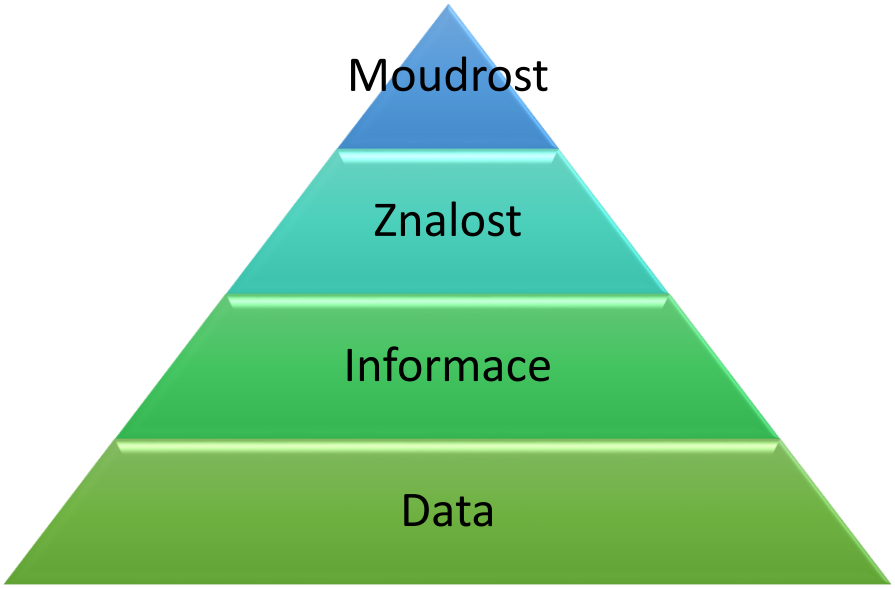
Kyberprostor – prostředí, kde se v dnešní době hromadí nejvíce informací. Digitální, nebo chcete-li virtuální prostředí, které slouží k přepravě a zpracování informací a ke vzniku samotných informací. [2]

Kryptografie – neboli také šifrování dat, je nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí. Blízce souvisí s kryptoanalýzou, která se zabývá dešifrováním. Dříve byly využívány samostatné přístroje, dnes lze vše (nebo skoro vše) zašifrovat i dešifrovat z počítače. [7]

Malware – název je zkratku z anglického Malicious Software. Jedná se o škodlivý software. Útočník by díky němu získat přístup do zařízení. Příkladem může být spyware, adware, či trojský kůň. [8]

Nepopiratelnost – z názvu lze vyčíst, že se jedná o neschopnost popřít předešlé akce, či jednání, nebo jejich provedení. [2]

Znalost – informace s přidanou hodnotou. Na jejich základě je možné se rozhodovat. Znalosti jsou založené na interpretaci, zkušenostech, poznávání a porozumění. Dále jsou závislé na inteligenčních schopnostech a na schopnostech dávat si věci do souvislosti. [9]



Obrázek č. 2: Vazba mezi daty
(Zdroj: Vlastní zpracování dle č. 9)

1.2 Oblast analýzy rizik

Aktivum – vše co má pro organizaci nějakou hodnotu a je organizací využíváno. Jedná se o hmotný i nehmotný majetek. [10]

Dopad – nepříznivá změna ovlivňující stupeň dosažených cílů v rámci organizace. [10]

Hrozba – potenciální příčina nechtěného incidentu, která může vést k poškození systému nebo organizace. [10]

Opatření – akt nebo předpis, který je speciálně navržen tak, aby snížil zranitelnost aktiva. Tímto je aktivum chráněno. [10]

Riziko – nejistý výsledek, který může znamenat potenciální problém. Rizikům lze předcházet pomocí jejich analýzy a následně pomocí návrhu opatření. [10]

Zranitelnost – slabé místo aktiva nebo skupiny aktiv, které může být zneužito jednou nebo více hrozbami. [10]

1.3 Oblast GDPR

GDPR – obecné nařízení o ochraně osobních údajů (General Data Protection Regulation) je poměrně nové nařízení EU, které slouží ke zvyšování ochrany osobních údajů obyvatel. Týká se firem, institucí, ale i jednotlivců. [13]

Anonymní údaj – je údaj, který po zpracování nelze vztáhnout k subjektu údajů. Nejsou regulována pravidly o ochraně osobních údajů. [11]

Citlivý údaj – speciální kategorie zahrnující údaje o politických názorech, rasovém či etnickém původu, náboženském vyznání, zdravotním stavu, sexuální orientaci a členství v odborech. Tyto údaje mohou subjekt poškodit (diskriminace). [12]

Osobní údaj – jakékoli informace o subjektu údajů, které lze přímo či nepřímo identifikovat na základě určitého identifikátoru (jméno, číslo, síťový identifikátor), nebo na základě zvláštních prvků (fyzické, fyziologickém genetické, psychické, ekonomické, kulturní, společenské identity). [12]

Pověřenec pro ochranu osobních údajů – data protection officer monitoruje soulad zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, auditů, školení a celkové řízení agendy interní ochrany dat. [13]

Pseudonymizace – proces skrytí identity. Účelem je sbíraní dalších údajů, které se týkají stejného jednotlivce, aniž by bylo nutné znát jeho totožnost (např. kódování pomocí klíče). [12]

Souhlas se zpracováním osobních údajů – v případě, že je zpracování založeno na souhlasu, je třeba, aby byl správce schopen doložit, že fyzická osoba udělila souhlas se zpracováním údajů o své osobě svobodně a souhlas byl konkrétní, informovaný, jednoznačný a ničím nepodmíněný. [13]

Správce osobních údajů – určuje účel a prostředky pro zpracování osobních údajů. Primárně odpovídá za zpracování OÚ. [13]

Subjekt údajů – fyzická osoba, k níž se vztahují osobní údaje. Nejedná se o právnickou osobu. [12]

Zpracování – libovolný úkon, který správce (nebo zpracovatel) systematický provádí s osobními údaji. [12]

1.4 ISMS

Information Security Management System neboli Systém řízení informační bezpečnosti. Je to systematický přístup ke správě citlivých informací o subjektu. Zprávy musí zůstat zabezpečené. Jedná se o součást celkového systému řízení organizace.

Zabývá se problematikou IT bezpečnosti, komunikační bezpečnosti, fyzické bezpečnosti, administrativní bezpečnosti, dokumentací a bezpečnostními funkcemi a mechanismy. [14]

ISMS je definován souborem norem (ISO/IEC 27000), ve kterých je specifikován celý proces, včetně popisu základních pojmů. [14]

ISMS je založeno na Demingově cyklu, který obsahuje následující etapy: [14]

- Ustanovení (včetně určení odpovědných osob a rozsahu)
- Zavádění a provoz (implementace vybraných bezpečnostních opatření)
- Monitorování (hodnocení a zpětná vazba systému)
- Údržba a zlepšování (odstraňování případných slabin systému)

1.4.1 Postupy zavádění ISMS

Pro zavedení ISMS bez případných komplikací je třeba postupovat podle předem daných pravidel. Tato pravidla lze rozdělit do čtyř základních bodů: [14]

1. Souhlas o zavádění a vytvoření požadovaného dokumentu
2. Identifikace aktiv, jejich ocenění, analýza rizik
3. Návrh opatření vůči rizikům
4. Zavádění ISMS certifikace

1.5 Normy a zákony

Zákon je obecně platný předpis, kterému se člověk musí podřídit. Zákony jsou nadřazeny podzákonným předpisům (vyhláškám a nařízením). Podřízeny jsou Ústavě a ústavním zákonům. [15]

Standard jsou pravidla využívána jako směrnice či pravidla. Jsou jasně daná, v písemné podobě. [2]

Norma popisuje přijatelné nebo obvyklé chování. Jedná se o požadavek. Názvy norem jsou zkratkami tří organizací: [2]

- **ČSN**

  Chráněné označení Českých technických norem. Přidává šestimístné číslo za svou zkratku, kde první dvě čísla specifikují třídu norem, další dvě čísla označují skupinu a podskupinu normy. Poslední dvojice čísel je pořadové číslo normy. [16]

- **ISO**

  International Organization for Standartization nebo-li Mezinárodní organizace pro normalizaci. Zabývá se tvorbou mezinárodních norem (kromě elektrotechniky). Mezi členy ISO patří národní normalizační organizace v daných zemích. V ČR se jedná o Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. [17]

- **IEC**

  International Electrotechnical Commission nebo-li Mezinárodní elektrotechnická komise. Zabývá se tvořením a publikací mezinárodních norem v oblasti elektrotechniky, elektroniky a sdělovací techniky. [18]

1.5.1 Normy řady 27000

- ISO/IEC 27000, principy a slovník;
- ISO/IEC 27001, požadavky na ISMS (resp. BS 7799-2:2004);
- ISO/IEC 27002, návody pro zavádění;
- ISO/IEC 27003, analýzy rizik (souvisí s ISO 13335-3);
- ISO/IEC 27004, metriky a měření;
- ISO/IEC 27005, řízení rizik;
- ISO/IEC 27006, kontinuita podnikání a obnova po havárii.

ČSN ISO/IEC 27000

Norma obsahuje všechny definice, které tvoří ISMS, a zároveň slouží jako podklad pro další normy. První vydání vyšlo v roce 2009, aktuálně je k dispozici třetí vydání z roku 2016. [19]

ČSN ISO/IEC 27001

Norma specifikuje požadavky na ustanovení, implementování, udržování a neustále zlepšování systému. Obsahuje 28 stránek. Jde o doporučení, jak aplikovat normu ČSN ISO/IEC 27002. Využívá PDCA cyklus. První vydání vyšlo v roce 2005, aktuálně je k dispozici vydání z roku 2014. [19]

ČSN ISO/IEC 27002

Norma je sbírkou bezpečnostních praktik a postupů. Je možné ji využít jako podklad pro vyvíjení směrnic pro řízení bezpečnosti informací. Mimo stovky praktik pro zajištění informační bezpečnosti obsahuje 35 cílů opatření pro ochranu informačních aktiv, které slouží jako základna pro bezpečnostní politiku. [19]

ČSN ISO/IEC 27003

Norma poskytuje doporučení pro ustanovení a implementaci ISMS (v souladu s ISO/IEC 27001) pomocí popisu zahájení, definování a plánování. Proces plánování implementace probíhá v pěti etapách (získání souhlasu se zavedením ISMS a aktivní podpora, definice rozsahu, provedení analýzy, provedení hodnocení rizik, návrh ISMS). Dále obsahuje popis rolí a odpovědností, informace o firemních auditech, politiky a informace o monitorování a měření informační bezpečnosti. [19]

ČSN ISO/IEC 27004

Norma poskytuje doporučení k vývoji a používání metrik. Zároveň uvádí doporučení pro měření účinnosti ISMS. Zahrnuje řídící procesy z ČSN ISO/IEC 27001 a opatření z ČSN ISO/IEC 27002. Norma obsahuje 63 stran. [19]

ČSN ISO/IEC 27005

Norma poskytuje doporučení pro řízení rizik bezpečnosti informací. Stanovuje tyto činnosti řízení rizik: stanovení kontextu, hodnocení rizik, zvládání rizik, akceptace rizik, seznámení s riziky, monitorování a přezkoumávání rizik. Podporuje ČSN ISO/IEC 27001. Je určená manažerům a pracovníkům, kteří jsou v dané organizaci pověření odpovědností za řízení rizik. Norma má 54 stran. [19]

ČSN ISO/IEC 27006

Norma specifikuje požadavky a doporučení pro orgány provádějící audit a certifikace ISMS. Primární určení je tedy podpora při procesu akreditace certifikačních orgánů, které poskytují certifikaci ISMS. Aktuální norma je platná od listopadu 2016. [19]

1.5.2 NIST standardy

National Institute for Standards and Technology je vládní standardizační orgán, který se zabývá vývojem a podporou standardů, měřícími technikami a technologií za účelem zvýšení produktivity, zjednodušení obchodu a zlepšení kvality života. NIST je tedy ve zkratce americká certifikační instituce. [2]

Tato diplomová práce vychází z programu SAE pro nějž jsou důležité dva standardy – NIST SP 800-16 a NIST SP 800-50.

NIST SP 800-16

Jedná se o model založený na rolích a výkonnosti. Zabývá se požadavky na školení v oblasti zabezpečení informačních technologií, pro které poskytuje koncepční rámec. Tyto požadavky jsou vhodné pro distribuované výpočetní prostředí. Rámec umožňuje také jistou flexibilitu pro rozšíření, která je využitelná pro budoucí technologie a související rozhodnutí o řízení rizik. [20]

NIST SP 800-50

Tento standard slouží k budování programu pro zvyšování povědomí (a s ním spojené školení) o informačních technologiích. Jedná se o návod, který poskytuje pro vybudování efektivního bezpečnostního programu. Tento dokument obsahuje čtyři kritické kroky: [21]

- Návrh
- Rozvoj
- Implementace
- Post-implementace

Dokument slouží jako doprovodná publikace pro NIST SP 800-16, se kterým se vzájemně doplňují. Zatímco NIST SP 800-16 je na nižší taktické úrovni (popisuje přínos školení založeného na rolích), NIST SP 800-50 je na vyšší strategické úrovni – zabývá se vybudováním programu na zvyšování povědomí o informační bezpečnosti, včetně školení. [21]

1.5.3 Kybernetický zákon č. 205/2017 Sb.

„Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.“ (Zákon č. 205/2017*, 2017, s.104)*

Kybernetický zákon upravuje:

- práva a povinnosti osob
- působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti

Zákon vychází z předpisů Evropské unie a zabývá se zajišťováním bezpečností informačních systémů a sítí elektronických komunikací. Nevztahuje se na ty informační systémy, jež pracují s utajovanými informacemi. [23]

1.5.4 Vyhláška č. 316/2014 Sb.

„Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti neboli vyhláška o kybernetické bezpečnosti.“ (Vyhláška č. 316/2014 Sb, 2014, s.82)

Vyhláška stanovuje: [22]

- strukturu bezpečnostní dokumentace informačního systému kritické informační infrastruktury
- komunikační systém kritické informační infrastruktury nebo významného informačního systému
- obsah bezpečnostních opatření a rozsah jejich zavedení
- typy a kategorie kybernetických bezpečnostních incidentů
- způsoby hlášení kybernetického bezpečnostního incidentu
- oznámení o provedení reaktivního opatření a jeho výsledku

1.6 Bezpečnost informací v akademickém prostředí

Akademické prostředí se od prostředí běžné firmy lehce odlišuje. Je nutné dodržovat následující bezpečnostní politiky, kteří řeší ISMS: [2]

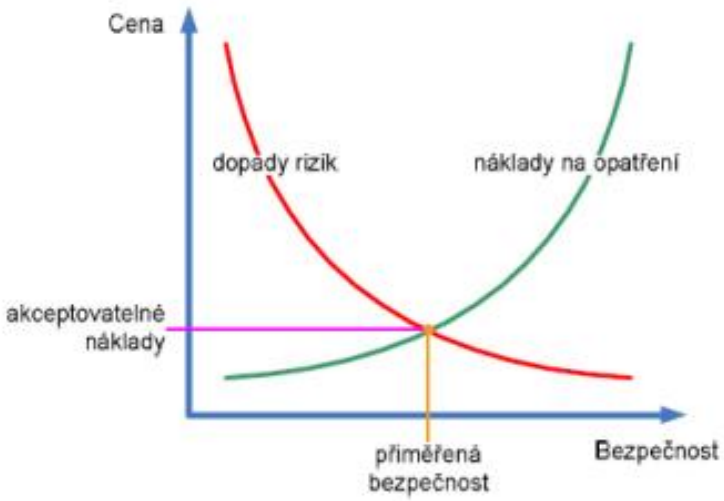
- správa osobních dat zaměstnanců
- správa osobních dat žáků
- správa osobních dat zákonných zástupců

- řešení objektové a přístupové bezpečnosti

Škola je poskytovatelem internetu studentům, proto je nutné dbát na další opatření, jako je například silné zabezpečení sítě Wi-Fi, která je oddělena pro studenty, zaměstnance a výuku. Je nutné provádět autentizaci a autorizaci uživatelů a logování jejich aktivit. Samozřejmostí by mělo být zavedení bezpečnostní politiky a dodržování IT standardů. [2]

1.7 Přiměřená bezpečnost

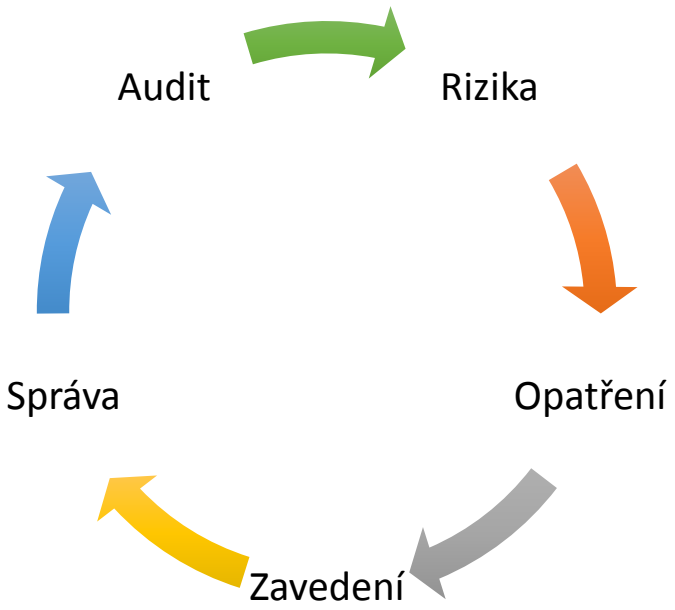
Je důležité zmínit, že mluvíme o tzv. přiměřené bezpečnosti. Absolutní bezpečnost je téměř nedosažitelná, a i když jí dosáhneme, tak na velmi krátký okamžik a za velmi vysokých výdajů. Následující graf vysvětluje, kolik finančních prostředků je vhodné vložit ke snížení dopadu rizik, aby to bylo přiměřené hodnotě objektu. [2]



Obrázek č. 3: Přiměřená bezpečnost
(Zdroj č.2)

1.8 Kybernetická bezpečnost v ČR

Cyber Security je odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů, tak i sítí. Cílem informační bezpečnosti je ochrana Informací a majetku před krádeží, korupcí, nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné jeho předpokládaným uživatelům. Jedná se o celý kyberprostor. Bezpečnost informací řeší ochranu informací a dostupnost informací. Je ve vzájemném vztahu s bezpečností organizace a bezpečností IS/ICT. [25]



Obrázek č. 4: Životní cyklus informační bezpečnosti
(Zdroj: Vlastní zpracování dle č.2)

19.října 2011 NBÚ (Národní bezpečnostní úřad) se stal gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast (usnesení vlády č.781), vzniká NCKB (Národní centrum kybernetické bezpečnosti) jako součást NBÚ. [2]

13.srpna 2004 prezident republiky Miloš Zeman podepsal zákon o kybernetické bezpečnosti a o změně souvisejících zákonů. [2]

29.srpna 2014 ve Sbírce zákonů ČR byl publikován zákon o kybernetické bezpečnosti (č. 181/2014 sb.). [2]

1.ledna 2015 vstoupil v platnost Zákon o kybernetické bezpečnosti. [2]

1.9 NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost je ústředním správním orgánem v oblasti kybernetické bezpečnosti, a to včetně ochrany utajovaných informací v oblasti komunikačních systémů, informačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby (od srpna 2017 systém Galileo, zákon č. 205/2017 Sb., který změnil zákon o kybernetické bezpečnosti č.181/2014 Sb.). [25]

1.10 Bezpečnostní týmy v ČR

CERT (Computer Emergency Response Team) skupina vzniklá roku 1988 po incidentu s jedním z prvních počítačových červů (Morrisův červ), který ke svému působení využíval sítě internet. V České republice se jedná o GovCERT. [26]

CSIRT.CZ (Computer Security Incident Respondent Team) bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích. Bezpečnostní tým provozuje sdružení CZ.NIC, což je správce české domény (2012, na základě memoranda s NBÚ). U Trusted Introducer je akreditovaný od roku 2011, členem FIRST od roku 2015. [26]

CSIRT-MU je bezpečnostní tým Masarykovy univerzity. Je tvořen třemi skupinami – reakce na incidenty, proaktivní bezpečnost, bezpečnost digitálních identit. [26]

CIRC-MO je organizační prvek AKIS (Agentura komunikačních a informačních systémů). Jeho úkolem je proaktivní identifikace bezpečnostních hrozeb a incidentů, čehož je dosaženo nepřetržitým monitoringem důležitých segmentů, následnou analýzou a vyhodnocením. [26]

1.11 Evropské nařízení GDPR

„NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES neboli obecné nařízení o ochraně osobních údajů.“ (Nařízení evropského parlamentu a rady, 2016, s.119)

Obecné nařízení o ochraně osobních údajů je legislativa EU, která má za úkol výrazně zvýšit ochranu osobních dat občanů. Toto nařízení vzniklo dne 26. dubna 2016 a v platnost vešlo 28. května 2018. Platnost GDPR je celosvětová – platí pro všechny, kteří pracují s osobními údaji občanů EU. Nařízení musí akceptovat a dodržovat všechny instituce členských států EU, které sbírají, zpracovávají a uchovávají osobní údaje. [12]

Hlavním úsilím je, aby organizace zahrnuly bezpečnostní požadavky a principy do vývoje svých služeb, řešení a produktů (ochrana by design a by default). K základním principům patří pseudonymizace a kryptování dat. [13]

GDPR zavedlo vysoké pokuty za porušování pravidel. Nařizuje zřídit kontrolní funkci DPO (Data Protection Officer – Pověřenec pro ochranu osobních údajů). Národní autorita může udělit pokutu až 4% z celosvětového obratu, nebo 100 milionů euro. [13]

1.11.1 DPO

Data Protection Officer – Pověřenec pro ochranu osobních údajů. Hlavním úkolem DPO je monitorování míry naplnění nařízení při zpracování osobních údajů. V organizacích nad 250 zaměstnanců je pověřenec pracovníkem na plný úvazek, u menších organizací lze tuto pozici zajistit externě (každý pracovník organizace vykonávající funkci DPO musí splňovat všechny příslušné požadavky GDPR). Existují však tři případy, kdy je povinné pověřence jmenovat: [13]

a) zpracování provádí orgán veřejné moci či veřejný subjekt (nutné dle čl. 37 odst. 1 písm. a)
b) „hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů
c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů“

V každém z výše zmíněných případů je správci/zpracovateli nápomocna osoba s odbornými znalostmi v oblasti právních předpisů a postupů, které se týkají ochrany údajů. [13]

Podle článku 30 povinnosti pověřence zahrnují:

- Proškolení organizace a jejích zaměstnanců, proškolení zaměstnanců organizace zpracovávajících osobní data.
- Provádění auditů k ověření plnění požadavků regulace a náprava případně zjištěných nedostatků.
- Kontaktní bod mezi danou organizací a kontrolními orgány dohlížejícími na plnění požadavků GDPR.
- Sledování míry naplnění jednotlivých opatření v souladu s normou a poradenství uvnitř organizace směřující k udržení ochranných opatření.

- Vedení úplných záznamů o všech činnostech zpracovávání osobních dat včetně účelu všech činností prováděných během zpracování osobních údajů. Tyto záznamy musí být schopen na vyžádání poskytnout kontrolnímu orgánu.
- Komunikace se subjekty osobních údajů za účelem poskytnutí informace, jak je s jejich osobními údaji nakládáno, včetně práva na výmaz osobních údajů a poskytnutí údajů, jaká opatření organizace přijala k ochraně osobních údajů.

Práva pro občany (subjekty údajů):

- Právo na přístup
- Právo být zapomenut
- Právo na opravu
- Právo na výmaz
- Právo na omezení zpracování
- Právo na přenositelnost údajů
- Právo vznést námitku

1.11.2 Správce – povinnosti, odpovědnost

K významným povinnostem správce patří:

- ochrana osobních údajů
- jmenování pověřence pro ochranu osobních údajů
- posuzování vlivu na ochranu osobních údajů a provádění předchozí konzultace
- ohlašování případů porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů
- oznamování případů porušení zabezpečení osobních údajů subjektu osobních údajů
- vést záznamy (netýká se všech správců)

Správce odpovídá za:

- dodržování zásad zpracování
- dodržování povinností upravených nařízením
- zabezpečení údajů

1.11.3 Zpracovatel – povinnosti, odpovědnost

Správce může ke zpracování osobních údajů využívat jiný subjekt, který osobní údaje zpracuje. Tento subjekt se poté nazývá zpracovatel. [13]

Povinnosti

- zpracovatel musí postupovat podle smlouvy nebo právního předpisu, které jsou zavazující vůči správci
- adekvátní zabezpečení osobních údajů
- příjem všech povinností z článku 32
- poskytování správci veškerých informací potřebné ke splnění
- umožnění auditů, které jsou prováděné správcem (nebo jiným auditorem, který získal pověření správce)

Veškeré povinnosti jsou uvedené v článku 28 GDPR. [13]

Zásady zpracování

- zákonnost, korektnost, transparentnost – správce musí zpracovávat osobní údaje korektně a transparentně (vzhledem k subjektu údajů)
- omezení účelu – osobní údaje musí být shromažďovány pro určité a legitimní účely a zpracování nesmí být neslučitelné s těmito účely
- minimalizace údajů – osobní údaje musí být především relevantní a přiměřené (ve vztahu k účelu, pro který jsou zpracovávány)
- přesnost – osobní údaje musí být přesné
- omezení uložení – osobní údaje jsou uloženy pouze po nezbytnou dobu (pro dané účely)
- integrita a důvěrnost – technické a organizační zabezpečení osobních údajů.

1.12 PDCA cyklus

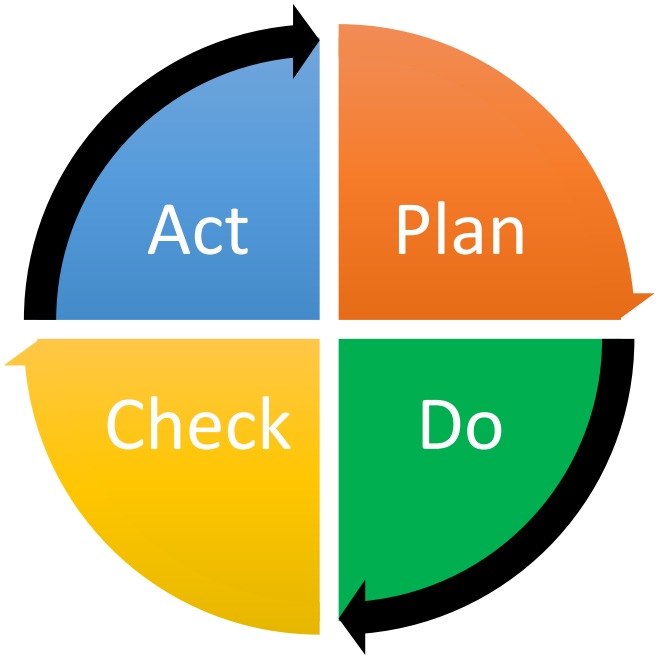
PDCA (Plan, Do, Check, Act) cyklus, nebo-li Demingův cyklus, je iteratická metoda kontrolování a zlepšování kvality v organizaci. Používá přesně daný sled kroků, který je důležitý při zavádění inovací a zlepšování kvality především ve výrobě. [2]

Plan (plánuj) – stanovení cílů, konkrétní způsoby řešení, personální obsazení projektu[2]

Do (proveď) – implementace vytvořeného plánu, sběr a měření dat (včetně dokumentace) [2]

Check (ověř) – analýza, porovnání, vyhodnocení vhodnosti a úplnosti plánu[2]

Act (jednej) – akceptace plánu, případně zavedení změn [2]



Obrázek č. 5: Cyklus PDCA
(Zdroj: Vlastní zpracování dle č. 2)

1.13 Program SAE

Security Awareness Education je program zvyšování bezpečnostního povědomí. Slouží ke zvýšení informovanosti zaměstnanců a tím ke snížení bezpečnostního rizika v organizaci. Zároveň dochází ke zvyšování bezpečnostního povědomí.

Pro úspěšné dokončení programu je třeba zahrnout tyto tři kroky:

- rozvíjení politiky informační bezpečnosti
- informování uživatele o jeho odpovědnosti
- určení kroků pro monitoring a přezkoumání programu

Zároveň je nutné vybudovat tzv. SAE plán, který se dá popsat v deseti bodech:

1. Role a odpovědnost
2. Stanovení cílů pro jednotlivé fáze programu (budování povědomí, školení, vzdělávání, profesní rozvoj, certifikace)
3. Rozdělení uživatelů do skupin
4. Vytvoření materiálů pro školení podle příslušných skupin
5. Vytvoření cíle pro jednotlivé skupiny
6. Vytvoření témat pro jednotlivé kurzy
7. Metodika
8. Vytvoření dokumentace, zpětná vazba, dotazníky (doložení výuky)
9. Vyhodnocení výukových materiálů a jejich případná aktualizace
10. Kalkulace, výpočet četnosti opakování včetně aktualizací materiálu

Model SAE by měl postihnout všechny uživatele informačního systému organizace. Mělo by se jednat o hlavní a klíčový prvek. Za nastavení zásad správného chování v organizaci by měl být zodpovědný management firmy. Program uvádí základní bezpečnostní politiky, kterými by se organizace měla řídit, a s nimi zároveň i systém sankcí za případné nedodržení povinností. Všichni uživatelé by měli být informování o své odpovědnosti.

1.13.1 Modely programu SAE

Pro výběr vhodného modelu je třeba brát v potaz několik faktorů, jako je velikost firmy, geografické rozmístění, organizační struktura a s tím spojené definování rolí a odpovědností. [21]

1. Centralizovaný model – veškerá odpovědnost připadá pověřené osobě. Vhodné u malých podniků, kde je vysoký stupeň centrálního řízení.
2. Částečně decentralizovaný model – vytvoření politik a strategie připadá pověřené osobě, nicméně samotná implementace je rozdělena mezi další uživatele. Vhodné u středně velkých podniků (důvodem je širší geografické umístění poboček nebo decentralizovaná organizační struktura podniku).
3. Decentralizovaný model – vytvoření bezpečnostní politiky je na pověřené osobě, implementace a vytvoření strategie je delegováno na jiné uživatele. Vhodné u velkých podniků.

1.13.2 Fáze programu

Program je koncipován tak, aby vzdělával uživatele v oblasti IT, kteří na základě školení získají nové zkušenosti, poznatky, znalosti a dovednosti, které přispějí k lepšímu vykonávání jejich funkce. [21]

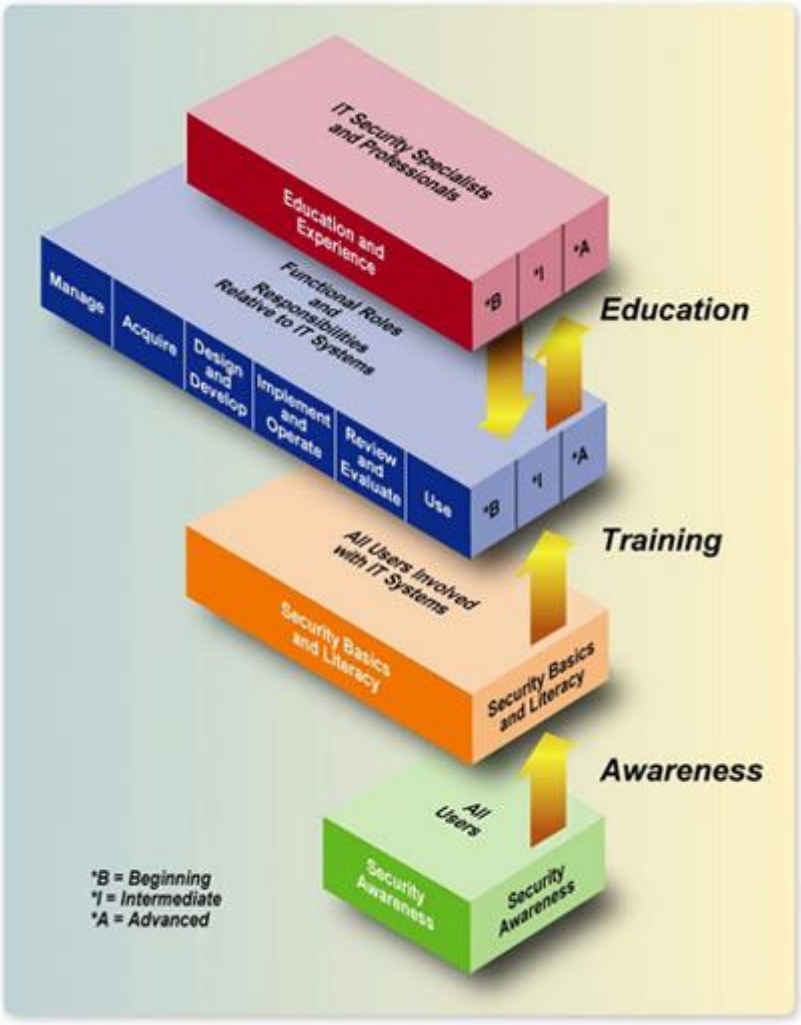


Figure 2-1: The IT Security Learning Continuum

Obrázek č. 6: SAE program
(Zdroj č.15)

Vzdělávání je kontinuální, tzn. začíná budováním povědomí, následuje školení a může se vyvinout ve vzdělávání. [21]

1.13.2.1 Bezpečnostní povědomí

Mít povědomí o něčem znamená mít znalost faktu nebo situace. Cílem prezentací o povědomí je jednoduše zaměření pozornosti na bezpečnost. Mnoho firem oblast informační bezpečnosti vynechává a zaměřují se pouze na podnikatelské činnosti. [21]

První stupeň programu, tedy budování povědomí, se týká všech členů organizace. Nelze předpokládat, že lidé budou rozumět možným rizikům a hrozbám, aniž by o nich věděli. Proto je nutné je s těmito informacemi seznámit.

Mezistupněm mezi budováním povědomí a školením je spojovací můstek s názvem „Security Basics and Literacy“, což by se dalo volně přeložit jako Základy bezpečnostní gramotnosti (NIST SP 800-16). Tento můstek poskytuje základní znalosti, které jsou nezbytné pro specializovaná školení. Security Basics and Literacy zahrnuje pochopení pojmů z mnohých oblastí, jako jsou například zranitelnosti IS, mechanismy kybernetických útoků, typy útočníků a další.

1.13.2.2 Školení

Školení je definováno v publikaci NIST 800-16 jako úsilí o vytvoření relevantních a potřebných bezpečnostních dovedností a kompetencí pro odborníky z jiných funkčních oborů, než je IT (např. management, audit). Největší rozdíl mezi budováním povědomí a školením je ten, že školení učí dovednostem, které dovolují člověku vykonávat určitou funkci, zatímco budování povědomí se zaměřuje na individuální pozornost na daný předmět.

Školení rozlišuje tři základní typy uživatelů:

- Začátečník
- Středně pokročilý
- Pokročilý

Uživatelé jsou rozřazováni do skupin na základě svých dosavadních znalostí a dovedností. Ke každému stupni pokročilosti je přistupováno individuálně. Zároveň každý z výše zmíněných typů má jiný cíl, kterého chce dosáhnout.

1.13.2.3 Vzdělávání

Úroveň „Vzdělávání“ integruje všechny bezpečnostní dovednosti a kompetence různých funkčních specialit do společného souboru znalostí, doplňuje multidisciplinární studium

pojmů, otázek a principů (technologických a sociálních) a snaží se vytvářet specialisty na bezpečnost informačních technologií a odborníků schopných vize a proaktivní reakce.

Vzdělávání jde nad rámec základních bezpečnostních kurzů a školení. Je realizováno prostřednictvím studijního programu na vysoké škole nebo jiném vzdělávacím fóru.

1.13.2.4 Profesní rozvoj

Tato fáze slouží k tomu, aby všichni uživatelé získali požadované znalosti z oblasti informační a kybernetické bezpečnosti, které dále zúročí ve svém profesním životě. Po prokázání znalostí je možné v této fázi získat jeden ze dvou typů certifikátů:

- Obecný (prokázání obecných znalostí z oblasti informační bezpečnosti)
- Technický (prokázání znalostí z oblasti technického zabezpečení)

1.13.3 Odpovědnosti v programu

Pro potřebu této diplomové práce je třeba zvolit a popsat několik základních rolí (odpovědných osob), jejichž odpovědnosti vychází z dokumentů NIST SP 800-50 a NIST SP 800-16. [20]

Vedení organizace

Odpovědnosti: určení CIO, určit program jako povinný pro všechny zaměstnance, zajistit všechny prostředky na podporu programu, přiřazení odpovědnosti za program, měření efektivity programu a sledování aktuálního stavu, na jehož základě iniciovat možná zlepšení. [20]

CIO

Odpovědnosti: správa školení, vytvoření strategie programu – kontrola dodržování a pochopení strategie, školení zaměstnanců se specializací na ICT, zajištění informovanosti o školení, dohled nad povinností účasti na školení, zajištění vhodných metod sledování a vyhodnocování programu[20]

Manažeři

Odpovědnosti: zajištění přístupu do IS firmy pouze těm zaměstnancům, kteří prošli školením a znají své odpovědnosti, snižování incidentů a chyb z nedbalosti nebo neznalosti, sledování a dokumentace průběhu. [20]

Zaměstnanci se specializací na ICT

Odpovědnosti: zúčastnit se programu, navrhovat další vhodná školení vedení organizace, kontrola kybernetické bezpečnosti, sledování úrovně bezpečnosti systému, reakce na zjištěné problémy s bezpečností. [20]

Uživatelé

Odpovědnosti: být informován, navštěvování školení, dodržování politiky. [20]

1.14 Bezpečnost počítačové sítě

Pod pojmem počítačová síť si můžeme představit spojení dvou a více počítačů za účelem vzájemné komunikace a sdílení prostředků. Význam počítačových sítí neustále narůstá, což můžeme velmi dobře sledovat právě ve školství. Do výuky jsou stále častěji zařazovány interaktivní hry a prezentace, které žáci spouštějí na školních netboocích a tabletech, které jsou připojeny k síti internet pomocí Wi-Fi. Nejčastějšími komunikačními uzly bývají stolní počítače či notebooky, ale může se jednat o jakékoli zařízení, například chytrý telefon nebo tiskárna. [27]

Pro implementaci bezpečnostních mechanismů můžeme využít normu ISO/IEC 27033, která obsahuje informace ke správnému zabezpečení správy, užívání sítí a jejich vzájemnému propojení. [27]

Abychom mohli mluvit o počítačové síti, musí obsahovat následující prvky:

- Propojovací SW
- Síťové systémy
- Síťové prvky

Obrázek č. 7: Počítačová síť
(Zdroj č.27)

Do značné míry lze zajistit bezpečnost počítačové sítě, pokud jsou dodržena následující pravidla: [28]

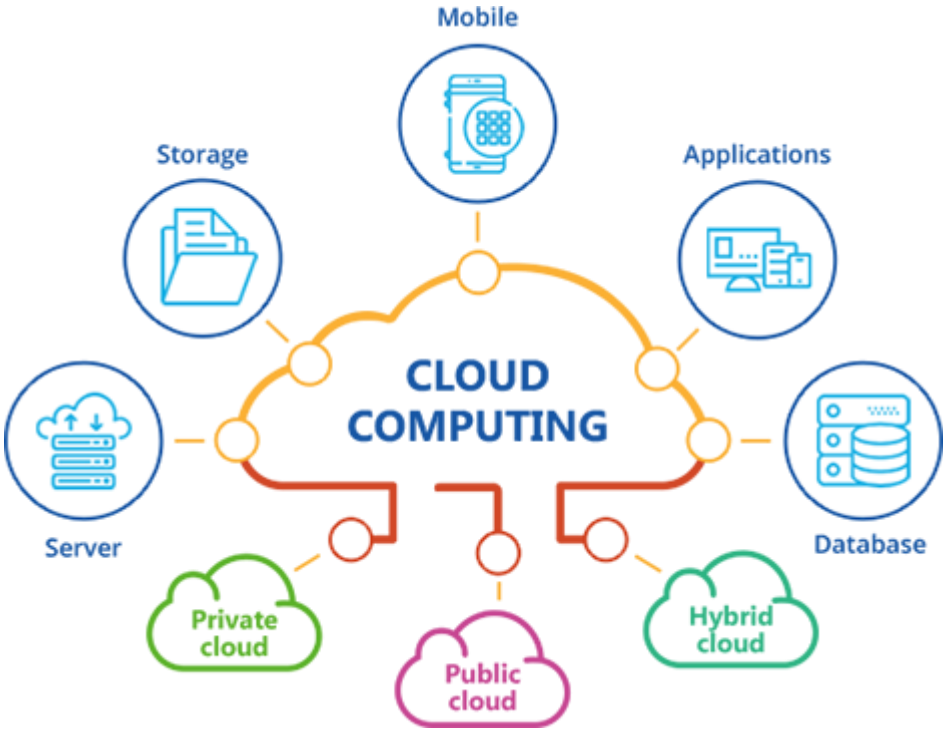
- Kvalitní firewall (sleduje příchozí a odchozí tok dat a určuje o shodě či neshodě s bezpečnostními pravidly)
- Šifrování dat (majitel elektronická data zašifruje a může e rozšifrovat pouze pomocí odpovídajícího šifrovacího klíče)
- IDS systémy (detekční zařízení, které indikuje neobvyklé chování v síti)
- IPS systémy (podobné firewallu, ale obsahuje seznam pravidel, podle kterých se rozhoduje o tom, která data nepustí dále do provozu)
- Seznam povolených IP/MAC adres

1.14.1 Cloud computing

Cloud computing je založen na principu sdílení hardwarových a softwarových prostředků pomocí sítě. Uživatelé ke cloudu mají přístup pomocí aplikace nebo webového prohlížeče. Nesmírnou výhodou je tedy dostupnost, jednoduchá správa, cena, vzdálená podpora a teoreticky vyšší výkon. K nevýhodám patří nutnost připojení k internetu, závislost na poskytovateli služby a možné nebezpečí pro uložená data. [29]

Existují čtyři typy cloudových řešení:

1. Veřejný cloud – není nutné vlastnit fyzickou serverovou strukturu (Microsoft, Google)
2. Soukromý cloud – vytvořené a vlastněné konkrétní organizací. Díky vyšším vstupním nákladům je řešení vhodné spíše pro větší firmy.
3. Komunitní cloud – sdílení napříč organizacemi, které mají podobné nároky na cloud (technologické klastry).
4. Hybridní cloud – kombinuje veřejný prostor a infrastrukturu inhouse. Je určen spíše větším firmám, neboť mohou rozdělit pracovní data na uložená v privátním a veřejném cloudu.



Obrázek č. 8: Cloud
(Zdroj č.29)

1.15 Analýza rizik

Jedná se o první krok v procesu snižování rizik. Pomocí tohoto nástroje jsme schopni odpovědět na otázky:

- Jaký bude dopad, pokud informace nebudou chráněny?
- Jaké jsou hrozby působící na organizaci?

- Jaká je pravděpodobnost, že bude porušena bezpečnost informací?

Jedná se o proces, kdy jsou definovány možné hrozby, pravděpodobnost uskutečnění a vážnost dopadu na aktiva. Dalším krokem je potom řízení rizik. [10]

Analýza rizik zahrnuje:

1. Identifikace aktiv
2. Stanovení hodnoty aktiv
3. Identifikace hrozeb a slabin
4. Stanovení závažnosti hrozeb a míry zranitelnosti

Podle podrobnosti analýzy rozlišujeme čtyři úrovně:

- Hrubá úroveň (zpracování dat na úrovni činnosti organizace)
- Neformální přístup (heuristický, ke zpracování dat dochází na základě zkušeností)
- Podrobný přístup (detailní kontrola zahrnující výše zmíněně 4 kroky analýzy)
- Kombinovaný přístup (v první řadě dojde ke zpracování na hrubé úrovní, následně k podrobné analýze u důležitých aktiv)

Dle interpretace výsledků rozlišujeme tři metody analýzy:

- Kvalitativní: využívá rozsahu hodnot, například <1,10>. Hodnocení je subjektivní, ale snadno pochopitelné.
- Kvantitativní: využívá matematické výpočty. Vyšší náročnost na provedení analýzy.
- Kombinovaná: využívá matematické výpočty z kvantitativní metody, ale interpretace výsledků je pro větší srozumitelnost vycházející z kvalitativní metody.

1.16 SLEPT

Tato analýza bývá označována jako prostředek pro analýzu změn okolí (analýza vnějších faktorů). Vyhodnocuje případné dopady změn na projekt, které pochází z konkrétních oblastí podle následujících faktorů – sociální, legislativní, ekonomické, politické, technologické. [30]

Analýza zkoumá následující skutečnosti:

1) Sociální faktory
   a) Demografické
   b) Sociálně-kulturní
   c) Dostupnost pracovní síly
2) Legislativní faktory
   a) Existence zákonných norem
   b) Autorská práva
3) Ekonomické faktory
   a) Makroekonomická situace
   b) Daňové faktory
   c) Přístup k finančním zdrojům
4) Politické faktory
   a) Hodnocení politické stability
   b) Politicko-ekonomické faktory
   c) Externí vztahy
5) Technologické faktory
   a) Výzkum
   b) Obecná technická úroveň

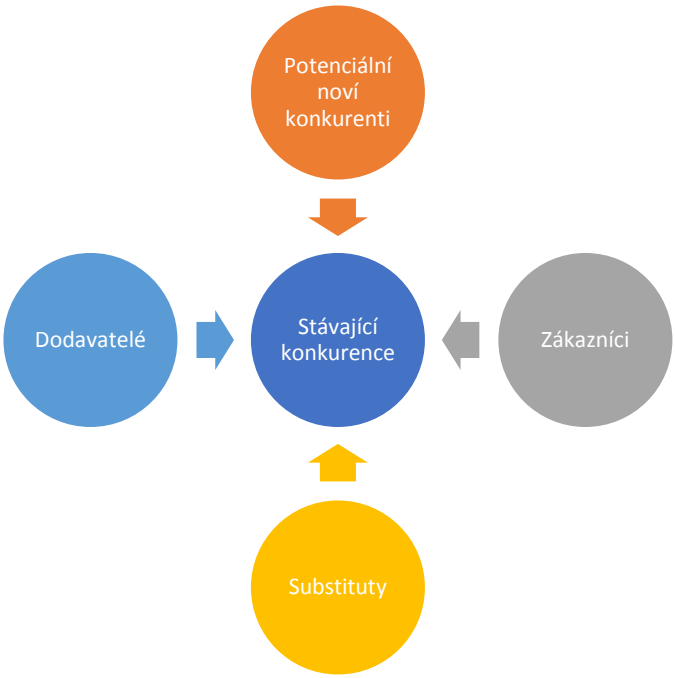
1.17 Porterova analýza pěti sil

Patří k základním a zároveň je jedním z nejvýznamnějších nástrojů pro analýzu konkurenčního prostředí firmy a jejího strategického řízení. Model odvozuje sílu konkurence (v analyzovaném odvětví) a tím i ziskovost daného sektoru trhu. [31]

K dosažení cíle rozebírá pět klíčových vlivů:

- stávající konkurence (schopnost ovlivnit cenu a prodávané množství výrobku nebo služby)
- nová konkurence (možnost vstoupení na trhu nové konkurence, která zapříčiní změny ceny)
- vliv odběratelů (schopnost ovlivnit cenu a poptávané množství)
- vliv dodavatelů (schopnost ovlivnit cenu a nabízené množství)

- substituční produkty (možnost nahradit výrobek jiným)



Obrázek č. 9: Porterova analýza pěti sil
(Zdroj: Vlastní zpracování dle č.31)

1.18 Analýza 7S

McKinsleyho model 7S patří mezi nejužívanější metody strategické analýzy. Tento model říká, že je možné na každou společnost nahlížet jako na množinu sedmi základních faktorů, které se vzájemně ovlivňují. [32]

Mezi hlavní faktory úspěchu dle definice rámce 7S patří:

- strategie (definice cílů a jejich dosažení)
- organizační struktura společnosti (mechanismus řízení)
- systémy a postupy (metody, postupy a procesy)
- spolupracovníci a jejich schopnosti (dovednosti, znalosti, zkušenosti)
- styl řízení (způsob konání, jednání)
- sdílené hodnoty firmy (vize, poslání, firemní kultura)

Obrázek č. 10: Model 7S
(Zdroj: Vlastní zpracování dle č.32)

1.19 SWOT analýza

SWOT analýza je univerzální analytická technika zaměřená na zhodnocení vnitřních a vnějších faktorů ovlivňujících úspěšnost organizace nebo nějakého konkrétního záměru. [33]

SWOT je akronym z počátečních písmen anglických názvů jednotlivých faktorů

- strengths - silné stránky
- weaknesses - slabé stránky
- opportunities – příležitosti
- threats – hrozby.

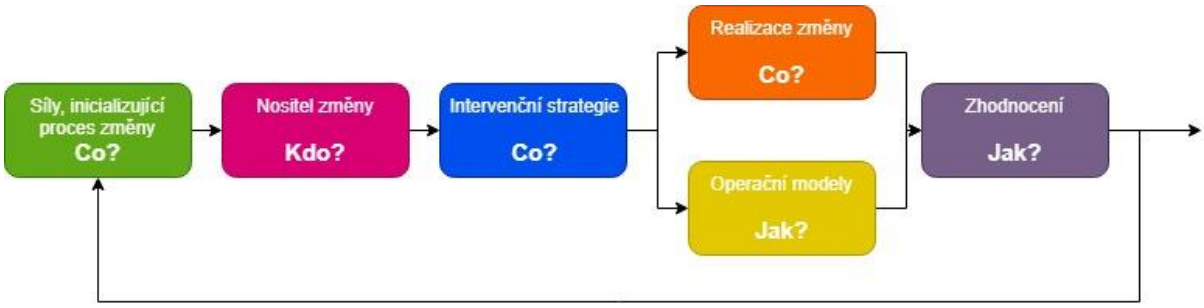
Obrázek č. 11: SWOT analýza
(Zdroj č.33)

1.20 Lewinův model

Lewinův třífázový model změn patří mezi nejstarší a nejznámější modely změn v organizaci. [10]

Při realizaci řízené změny s pomocí Lewinova modelu je daná změna rozdělena do jednotlivých fází:

- analytická fáze – síly, inicializující proces změny
- definování nositele změny
- identifikace hlavních firemních procesů – intervenční strategie
- návrhová fáze – operační modely
- realizační fáze – provedení změn
- zhodnocení



Obrázek č. 12: Lewinův model
(Zdroj: Vlastní zpracování dle č.10)

1.21 PERT

Je jednou ze standardních metod síťové analýzy. Metoda PERT je zobecněním metody kritické cesty CPM. Doba trvání každé dílčí činnosti se chápe jako náhodná proměnná mající určité rozložení pravděpodobnosti. [34]

Při provádění odhadů se berou v úvahu jen ty vlivy, které je možno klasifikovat jako náhodné jevy:

- vliv počasí
- vliv organizace práce
- vliv kvalifikace
- vliv pracovní morálky a disciplíny
- výkonnost
- poruchovost

Cílem modelů PERT je takové uspořádání činností, které by zajistilo dodržení termínu dokončení projektu s dostatečně vysokou pravděpodobností. Základní odlišností od metody CPM je, že doba trvání činnosti není přesně známa, nýbrž je dána pouze s určitou pravděpodobností. Doba trvání činnosti je zde udávána oproti metodě CPM s pomocí tří odhadů – optimistický, pesimistický a nejpravděpodobnější. Délka trvání jednotlivých činností je pak vypočítána na základě těchto tří odhadů. [34]

2 ANALÝZA SOUČASNÉHO STAVU

Cílem této části diplomové práce je provést analýzu současného stavu vybrané základní školy, která poté poslouží jako podklad k vlastnímu návrhu.

V úvodní části je popsána základní škola jako organizace, organizační struktury a procesy. Poté je rozebrána analýza SLEPT, Porterova analýza pěti sil, analýza 7S a SWOT, které podrobně mapují současnou situaci ve škole a jejím okolí. Při analýze současného stavu byl zjištěn vážný nedostatek v bezpečnosti práce s IS školní jídelny, který je podrobně analyzován, neboť tento problém je třeba vyřešit před samotným návrhem a zavedení školení pro zaměstnance a žáky školy.

Všechny získané informace pochází od vedení školy a učitele ICT.

2.1 Popis organizace

Vybraná základní škola se nachází v Jihomoravském kraji, konkrétně v městě Brně. Navštěvují ji žáci převážně z blízkého okolí, ale díky specializaci některých tříd na sport i žáci ze vzdálenějších částí Brna. Kapacita škola je 600 žáků. Ve škole je 37 pedagogických pracovníků a 24 nepedagogických pracovníků. Jedná se o jednu ze dvou škol, které se nachází v brněnské městské části. Škola je vedená jako příspěvková organizace, přičemž zřizovatelem je město.

Materiální zázemí školy čítá několik odborných učeben (chemie, fyzika, informatika, biologie, několik jazykových učeben, hudební výchova, výtvarná výchova, dílny), atrium pro společenské události, venkovní sportovní areál, dvě kryté tělocvičny, knihovnu, hernu, školní družinu, bazén a školní jídelnu.

2.2 Organizační struktura

Struktura školy se sestává z ředitele školy, který je v roli vedoucího, pod ním pak dále zástupce ředitele pro první stupeň a zástupce ředitele pro druhý stupeň. Dále pod tuto pozici spadá systém správy a údržby, který zahrnuje školníka, kuchařky a uklízečky. Pod přímým dohledem zástupce ředitele jsou výchovní poradci a učitelé školy, kteří jsou přímo nadřazeni žákům školy.

Z výše zmíněné struktury je třeba zvlášť zmínit, že pod pojmem zaměstnanci školy nejsou zahrnuti pouze pedagogičtí pracovníci, ale i nepedagogičtí, kteří jsou nepostradatelní pro

správný chod školy. Pouze k rukám zaměstnanců školní jídelny jsou však předkládána data o studentech a jejich zákonných zástupcích, z čehož vyplývá nutnost zúčastnit se stejného školení, jako pedagogičtí pracovníci, a také nést odpovědnost za zacházení s těmito daty.

2.3 Vybavení školy

V této části je popsáno HW a SW vybavení školy.

2.3.1 Hardware

Stolní počítače

V budově základní školy se nachází dvě počítačové učebny, které slouží k výuce ICT. V první z nich se nachází 30 počítačů, ve druhé 15 počítačů. Všechny počítače jsou značky HP.

Kromě počítačových učeben každý kabinet obsahuje jeden stolní počítač, dohromady tedy 21 počítačů. Jedná se většinou o starší a vyřazené kusy z učeben ICT.

Netbooky pro studenty

Škola nabízí studentům k zapůjčení netbooky značky Lenovo pořízené roku 2013. Ty, ač jsou staršího data, slouží primárně k výuce hodin biologie a fyziky. Celkově škola disponuje 10ti kusy. Odpovědnost za případné poškození připadá studentům i dozorujícím pedagogům.

Tablety pro studenty

V roce 2017 dochází k nákupu 10ti tabletů, které studenti mají k dispozici pouze pro výukové účely. Jedná se o značku Apple s kapacitou 16 GB.

Notebooky pro pedagogy

Od roku 2016 mají pedagogové k dispozici notebooky značky Dell pořízené v zahraničí. Jediný zásah povolený školou je přelepení tlačítek tlačítky s českou diakritikou. Jiné zásahy jsou možné pouze s povolením správce ICT.

Notebooky slouží primárně k zapisování do elektronické třídní knihy, k ovládání projektoru, k pouštění prezentací a dalším výukovým potřebám. Zabezpečení se sestává

z přihlašovacího hesla do systému, které pedagogům přidělila škola. Toto heslo si však mnozí z nich změnili.

Projektory a interaktivní tabule

Téměř ve všech odborných učebnách je k dispozici projektor, v běžných třídách pak převládají interaktivní tabule.

Multifunkční tiskárna (tisk, kopírování, scanner)

Tato multifunkční zařízení se nachází ve sborovně školy, u obou zástupců ředitele a u školního psychologa. Studenti nemají právo zařízení používat. V přilehlé budově gymnázia se však nachází 5 multifunkčních zařízení, z nichž jedno je možné studenty používat – po zakoupení speciální karty. Této možnosti často využívají i žáci ze základní školy, kteří se domluví s přáteli z vedlejší školy a materiály si nechají vytisknout. Ani jedna ze škol zatím neplánuje opatření proti tomuto chování.

Server

Škola vlastní dva servery, oba značky Dell. Využívaný je však pouze jeden z nich. K jejich uložení je využita speciální místnost, který svými podmínkami plně nahrazuje serverovnu, jak ji známe. Primární účel je využití k chodu informačního systému Edookit a správě všech účtů. Zároveň je v místnosti umístěn hardwarový firewall, který slouží k lepší síťové ochraně. Přístup do místnosti má ředitel školy, školním a správce ICT. Nepsaným pravidlem ale je, že místnost navštěvuje pouze správce ICT.

Školní síť

Síť je pomocí několika switchů rozprostřena po celé budově, včetně kabinetů a učeben. Přístup mají však pouze učitelé. Důvod zavedení bylo jednodušší připojení notebooků ve třídách k síti internet. Žáci školy využívají opět možnosti přilehlé školy, kde se po zadání jednoduchého hesla připojují k jejich místní síti. Rychlost sítě základní školy je 100 Mbit/s.

Kabeláž je vedena pod plastovými lištami podél stropů. Původní uložení bylo podél země, nicméně časté ničení zapříčinilo rekonstrukci v roce 2012. Datové zásuvky jsou pouze v kabinetech a přístupné tedy jedině pedagogům školy.

2.3.2 Software

Informační systém

Škola využívá systém Edookit, který se stává stále rozšířenějším po školách v České republice. Jedná se o poměrně nový systém, který byl na školu zaveden roku 2016. Informační systém Edookit je využíván k evidenci žáků, zaměstnanců školní matriky a rozvrhu hodin.

Přístup do systému mají učitelé, ředitel školy, žáci a rodiče. Rozdíly jsou v uživatelském rozhraní a udělených právech pro zápis, editace apod. Pro nižší ročníky stále platí zápis důležitých informací do deníčku a žákovské knížky, u druhého stupně ale systém plně nahrazuje veškeré dříve používané materiály.

Školní jídelna využívá vlastní informační systém, který je velmi zastaralý a nesplňuje ani základní bezpečnostní opatření. Pokud vezmeme v potaz, že systém je tak silný, jako jeho nejslabší článek, nastává zde vážný problém. Škola je připravena pro přechod IS školní jídelny na jednotný IS školy, a to systém Edookit, který je již využívaný. Je tedy nutné provést analýzu, která popíše následnou integraci těchto dvou systémů.

Vybavení počítačů

Ve větší učebně jsou starší počítače běžící na systému Windows 7, starší periferní zařízení, druhá byla zrekonstruovaná v roce 2018 a OS je Windows 10. Pro notebooky učitelů a stolní počítače v kabinetech je využíván systém Windows 7.

K dalšímu vybavení patří Microsoft Office a antivirový program AVG.

2.3.3 Fyzická bezpečnost objektu

Vstup do budovy je umožněn několika vchody. Hlavní vstup pro první stupeň, který obsahuje dvoje vchodové dveře, neboť za prvními z nich je vchod pro dětského zubaře, hlavní vchodové dveře pro druhý stupeň, kde se nachází i zvonky na různá družinová oddělení a vedení školy, vchod do tělocvičny a bazénu, vchod do školní jídelny. V rámci areálu potom osm dveří vedoucích z atria školy, dva vchody do koridoru, kde se nachází vedení školy, vchod do koridoru, který vede do vedlejší školy, dva vchody do školní jídelny.

Žádný z vchodů není monitorován kamerovým systémem. Vchodové dveře otvírá každé ráno v 7:45 školník, který je chvíli po osmé uzavře. Pozdější vstup je tedy možný pouze po zazvonění na vedení školy, případně (v odpoledních hodinách) na školní družinu.

Klíče od budovy má každý pedagog. Tento klíč zároveň odemyká i třídy, příslušný školní kabinet a vchod do tělocvičny.

2.4 Bezpečnost dat

Školy v České republice mají mnoho povinností. Například uchovávat data o svých žácích, zákonných zástupcích, ale i o svých zaměstnancích. Bezpečnost těchto dat je zajištěna dvojím ukládáním. První z nich je ukládání dat na lokální disk, druhá záloha slouží jako offsite mimo budovu školy.

Do roku 2016 byla všechna data tištěna na jehličkové tiskárně EPSON, a to na předem stanovené formuláře. Tento proces byl zastaralý a ne příliš efektivní. Tisk trval příliš dlouho, vyžadoval zastaralé technologie (počítač, operační systém) a byl chybový. Po zavedení systému Edookit byla všechna data přenesena do něj, což vyřešilo i základní bezpečnostní opatření, neboť je obsahuje IS samotný. Informace o studentech jsou ukládány elektronicky, informace o zaměstnancích se nachází i v papírově podobě, a to v kartotékách v ředitelně školy. Šifrování dat je také řešeno systémem Edookit, kde probíhá monitoring logů a sítě.

Data ze školních počítačů mají na starosti učitelé, jež mají notebook propůjčeny. Tudíž záloha neprobíhá centrálně, ale za zálohu zodpovídají učitelé jednotlivě. Při poruše notebooku se o nápravu nejprve pokouší správce sítě, poté (v případě neúspěchu) se posílá na opravu externí firmě. Zabezpečení dat na HDD není vyřešeno, neboť se notebook posílá kompletní, včetně všech uložených dat.

2.5 Budování bezpečnostního povědomí SAE

V současné době není SAE ve škole řešeno, nicméně zaměstnanci při přebírání techniky jsou seznámeni s pokyny pro zacházení. V oblasti práce s daty však nemají žádné poznatky.

Žáci by měli být seznamováni pravidelně každý rok s bezpečností práce v učebnách ICT. Ačkoli je vyhrazena jedna výuková hodina pro každou třídu, v praxi se poučení děje spíše jen papírově. V případě, že k poučení skutečně dojde, žáci získají poučení o chování v

učebně, jako je zákaz jezení či pití, zákaz používání počítače k soukromým účelům, zákaz připojování USB disků a další. Výuka předmětu informační technologie je povinná od 6.třídy, na prvním stupni je nabízena jako volitelná zájmová aktivita. Náplní výuky je především práce s MS Office, programy Zoner Callisto a GIMP.

Školní psycholog v nepravidelných intervalech iniciuje školení na téma kyberšikana. Často se tak děje na základě podnětu z řad rodičů žáků školy.

2.6 SLEPT

Sociální

Jeden z hlavních sociálních faktorů, které mají vliv na školu, je úbytek žáků. Mnozí přechází po 1. stupni na gymnázia, či na druhou základní školu v okolí, neboť ta zaručuje přijetí na učiliště bez přijímacích zkoušek. Dříve byla tato škola se specializací na hokej jediná v okolí, postupem času se ale začaly specializovat i dvě další, což znamenalo a znamená neustálý úbytek žáků.

Legislativní

Jako každá škola musí i tato splňovat různé právní předpisy.

- Zákony
- Vládní nařízení
- Vyhlášky Ministerstva školství
- Vnitřní předpisy Ministerstva školství
- Bezpečnost práce

Ekonomické

Vzhledem k tomu, že se jedná o státní školu, bereme v úvahu tabulkové platy. Průměrný hrubý plat v roce 2018 činil 31 632 Kč. Výše příjmu se odvíjí od dosaženého stupně vzdělání a celkové praxi v oboru.

Politické

Politické faktory do jisté míry souvisí s legislativními faktory. Každá vláda s sebou přináší novely zákonů, velmi často i zákona týkajícího se školství. Škola je zároveň

ovlivněná i zřizovatelem. Na těchto dvou institucích je víceméně závislé to, kolik peněz ročně dostane škola na platy učitelů a provoz.

Technologické

Je nutné neustále sledovat trendy a pokusit se zařídit novou techniku žákům v co nejkratším čase. Jelikož škola je základem života, je nutné seznámit žáky s tím, co je může v běžné praxi potkat, již od útlého věku. V současné době škola disponuje moderními počítači, projektory i interaktivními tabulemi a tablety.

2.7 Porterova analýza pěti sil

Stávající konkurence

V Brně se nachází mnoho základních škol, které jsou velmi dobře zavedené. Podobně nebo stejně zaměřené školy jsou v Brně tři.

Pokud vezmeme v potaz, že většina žáků dochází na základní školy v místě bydliště, nezávisle na zaměření, je konkurence v podobě jedné školy v těsném sousedství. Oba instituty nabízí následné vzdělání na střední škole, přičemž naše zvolená škola je propojena s víceletým gymnáziem a druhá zmíněna s odborným učilištěm.

Nová konkurence

Příchod nové konkurence není vyloučen, je dokonce velmi pravděpodobný. V současné době se rozvíjí trend alternativních výukových metod provozovaných například Waldorfskými či Montessori školami. Do obliby se také dostávají tzv. lesní školy.

Dodavatelé

Mezi dodavatele školy patří například dodavatelé energií, svačinových boxů, nábytku, učebnic, pomůcek pro výuku, surovin pro školní jídelnu a další. Dodavatelé většinou nemají přílišnou vyjednávací sílu, neboť škola má na výběr z více možností. Zároveň se ale také řídí vyhláškami Ministerstva školství, které například před třemi lety vydalo tzv. „pamlskovou vyhlášku“. Školní automaty s jídlem musely být odstraněny. Poté byly nahrazeny jinými, které obsahovaly zdravější potraviny. Slazené nápoje byly taktéž odstraněny a nahrazeny automaty na mléko a mléčné výrobky.

Zákazníci

Podle definice je zákazník příjemce statků, služeb, produktů nebo nápadů, které získává od prodejce, obchodníka nebo dodavatele za peněžní nebo jinou hodnotovou úplatu. Ve školství tedy bereme v úvahu jako zákazníka žáky školy a jejich rodiče. Ti totiž požadují od školy jistou kvalitu služeb (tedy vzdělání), spolehlivost, osobní přístup a další.

Žáci školy se dělí na potencionální, tedy ty, kterým bude v září nového akademického roku minimálně 6 let, a které si škola připravuje v tzv. přípravkách v sousedních mateřských školách, a ty, které již do školy nastoupili.

Substituty

Za hlavní substituty můžeme považovat vlastně všechny základní školy, které se ve městě nachází. Pokud vezmeme v potaz zaměření školy, tedy na sport, zúží se jejich výběr na 3 základní školy. Nicméně škola je jako jediná vybavena bazénem a smlouvou s DRFG arénou, tudíž pokud rodiče mají za prioritu například kroužek plavání a hokeje, vhodný substitut budou hledat těžko.

2.8 Analýza 7S

Strategie

Jedním z primárních cílů je držet krok s novými technologiemi, které je potřebné v co nejkratším úseku zařadit do výuky. Moderní učebny mohou přilákat více žáků do tříd. S tím se pojí další výrazný prvek, a to školení učitelů. Protože se okolí i informace mění, je zapotřebí věnovat školení dostatek času.

Struktura

Základní škola je vedena jako příspěvková organizace, jejímž zřizovatelem je město Brno. Řídí se pokyny Ministerstva školství i pokyny města Brna. Zřizovatel se podílí na volbě nového ředitele (jednou třetinou), rozhoduje o rozpočtu školy, odměňování a kontroluje správný chod hospodaření. Ve vedení školy je jeden ředitel a s ním i dva zástupci ředitele – pro první a druhý stupeň základní školy.

Systémy

V současné době škola používá informační systém Edookit, do kterého učitelé zapisují známky, docházku, pochvaly a napomenutí, školní akce, obsahuje rozvrh a další potřebné materiály pro výuku a chod školy. Systém se zaváděl teprve před rokem, což znamená, že se na něm stále pracuje. Důležitým faktem je, že zatím nejsou správně přiřazena práva učitelům, kteří si v současnosti mohou vzájemně přepisovat známky. Na tomto problému se nyní pracuje.

Druhým systémem je informační systém školní jídelny, který obsahuje jména studentů a zaměstnanců, data jejich narození (případně ročník studia), informace o zaplacení a zvolené objednávce.

Pro komunikaci s vnějším okolím fungují dvě služby. První z nich je výše zmínění Edookit, který umožňuje žákům a jejich zákonným zástupcům přijímat zprávy od pedagogů školy, druhým pak běžný e-mailový klient. Ten je potřebný z toho důvodu, že ne každá zpráva je mířena pouze rodičům, žákům či kolegům, ale k běžné praxi patří i domlouvání školních výletů, škol v přírodě, zájezdů a například i komunikace s pedagogicko-psychologickou poradnou.

Spolupracovníci

Mezi zaměstnance školy patří pedagogičtí a nepedagogičtí pracovníci. Během posledních dvou let došlo k výrazným změnám, neboť se obměnila polovina pedagogického sboru, který vyučuje na prvním stupni. Bylo tomu tak z důvodu odchodu pracovníků do důchodu a na mateřskou. Tímto faktem lze soudit, že atmosféra mezi kolegy je na dobré úrovni. O sbližování mezi nimi se ostatně snaží i vedení školy, které během roku pořádá různé společenské akce.

Schopnosti

Zaměstnanci, které škola přijímá, musí mít dostatečnou kvalifikaci pro vykonávání své práce. Pro získávání nových zkušeností a poznatků škola zajišťuje různá školení a kurzy. Například při změně osnov, kdy se anglický jazyk učí již od první třídy, došlo k otevření kurzu anglického jazyka pro 5 pedagogů, kteří tuto kvalifikaci neměli. Zároveň při každém zavedení moderní technologie do třídy pro modernizaci výuky dochází ke školení

pedagogů, kteří se učí, jak s daným předmětem zacházet a jak jej zahrnout do běžné výuky tak, aby byla pro žáky zajímavější a přínosnější.

Styl řízení

Do jisté míry se dá mluvit o autoritativním stylu řízení, nicméně je tu ponechána možnost pro pedagogy vyjádřit své požadavky a tím změnit rozhodnutí vedení školy. Ředitel školy mnohé povinnosti deleguje (v první řadě na zástupce ředitele) a sám si ponechává odpovědnost v klíčových úlohách. Důležitou roli také hraje při komunikaci školy s okolím.

Sdílené hodnoty

Ke sdíleným hodnotám určitě patří dobré vztahy mezi zaměstnanci. Pokud je učitel spokojený, dobrou atmosféru pak dokáže předat žákům ve třídě, zajistit jim dobré zázemí a tím i zajistit dobrou reklamu škole. S tím souvisí i poskytnutí dobrých služeb, což znamená kvalitní vzdělávání žáků školy. Ti poté mohou své zkušenosti a poznatky zúročit při dalším studiu.

2.9 SWOT analýza

Silné stránky

- Kvalifikovaní učitelé
- Dobrá pověst
- Moderní vybavení učeben
- Dobrá lokalita

Slabé stránky

- Nejednotný systém (Edookit + školní jídelna)
- Malý důraz na výuku jazyků
- Nedostatečné povědomí o bezpečnosti

Příležitosti

- Navazující studium na střední škole
- Přední postavení mezi základními školami
- Využívání dotací z EU (projekty)

Hrozby

- Vznik nové konkurence
- Úbytek žáků
- Nedostatek kvalifikovaných pedagogických pracovníků
- Změny ve financování

2.10 Zhodnocení analýzy

Po provedení analýz bylo zjištěno, že existuje několik příležitostí ke změnám. Jedna z hlavních změn by bylo sloučení dvou školních systémů, přičemž systém Edookit je na tuto změnu dobře připraven. Dále z analýzy vyplývá, že škola má dobré postavení ve městě, ve kterém se nachází, ale to neznamená, že by nadále neměla modernizovat učebny a nenabízet žákům co nejvíce vyhovující zázemí a možnosti dalšího rozvoje ve školních aktivitách. V neposlední řadě by bylo vhodné zaměřit se více na výuku cizích jazyků. Učitelé nižších tříd jsou velmi často o pár kapitol před žáky, což není dostatečné. Je tu prostor pro zaměstnáni rodilé/ho mluvčí, který by se uplatnil při výuce jak na druhém stupni, kdy se žáci připravují na další studium, tak na prvním stupni – děti v nižším věku informace pochytí rychleji, vybudují si dobré základy pro další rozvoj jazyka.

Nedůležitější změna by se měla týkat bezpečnosti. Zaměstnanci školy jsou nedostatečně školeni a žáci neumí nakládat správně s informacemi v jakékoli podobě.

2.10.1 Informační systém školní jídelny

V současné době školní jídelna zahrnuje 15 zaměstnanců, přičemž přístup do systému mají všichni zaměstnanci. Se systémem ale prioritně pracuje 1 zaměstnanec.

HW vybavení

- Stolní PC (provoz od roku 2000)
- Tiskárna připojená k PC

SW vybavení

- Informační systém (provoz od roku 1998, aktualizace v roce 2000)

Veškeré vybavení se nachází v malé průchozí místnosti. Každý zákazník/žák může během procesu placení/objednávání/rušení/přeobjednání sledovat situaci, neboť na

monitor PC je z okénka velmi dobře vidět. Komunikace probíhá přes sklo a mikrofon, kdy dochází k vyřízení objednávky – 2x denně (svačinová a obědová přestávka) po omezený čas.

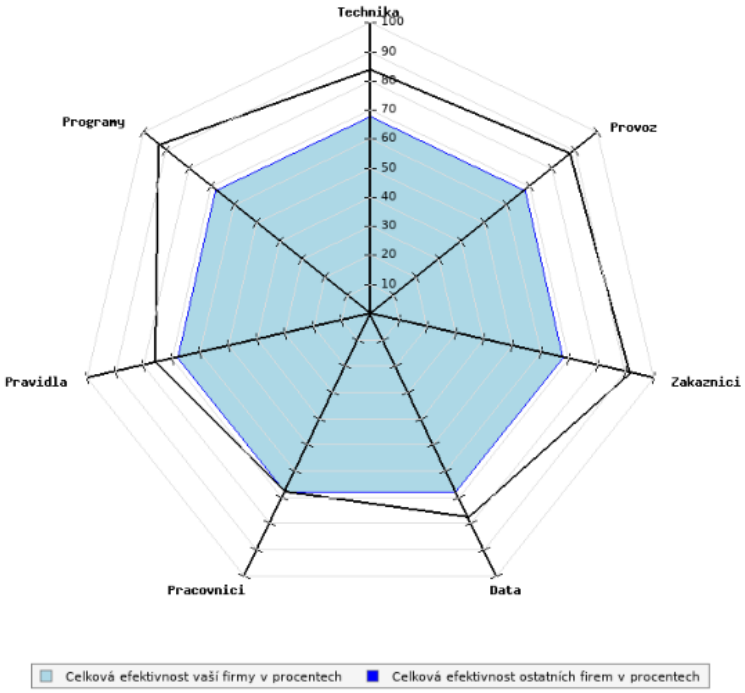
K auditu byl použit portál Zefis, ve kterém byl vytvořen proces objednávky jídla v IS školní jídelny na základní škole. Následně byly vyplněny příslušné dotazníky a došlo ke zhodnocení celkové efektivity a bezpečnosti systému.

2.10.1.1 Efektivita

Informační systém pro školní jídelnu byl navržen jako jednoduchý, ale účinný nástoj. Jelikož zahrnuje pouze základní procesy, jako je zaplacení jídla, přičemž je na výběr ze dvou možností, změnu výběru případně storno objednávky, v současné době se nedá vyloženě říci, že by účel nesplnil, nebo byl (funkčně) zastaralý. Nicméně prostředí, které vypadá spíše jako dvoubarevný Norton Commander, není příliš lákavé. Dalším mínusem může být, že veškeré objednávky jsou vyřizování pouze přes toto „okénko“, které má omezenou dobu provozu během dne. Na tyto poměrně krátké úseky připadá přibližně 800 lidí, kteří si chtějí své požadavky vyřídit. Dochází proto k velmi častým frontám a nepraktickému zdržování. Změna vybraného jídla je možná nejpozději 24 hodin předem u objednávacího automatu, poté je možné záměnu vyjednat u příslušného okénka.

Systém byl původně velmi jednoduchý – do roku 2000 se evidovala pouze jména strávníků a k nim příslušné informace zaplatil/nezaplatil. Při výdeji jídla docházelo k prokázání pomocí razítka v papírové tabulce. Od roku 2000 došlo ke změně, totiž k převedení na čipové kartičky, později malé kulaté čipy, a zároveň k rozšíření nabídky na výběr ze 2 jídel. V současné době IS eviduje jména strávníků, doklady o zaplacení jídla a zároveň druh jídla, který byl zvolen. Dále pak datum narození, případně ročník studia.

Veškeré informace se nachází v jednom stolním PC připojeném k místní síti, který spravuje prioritně jedna zaměstnankyně, která je zaměstnaná od samého počátku pořízení systému. Tudíž nebyla třeba školení ani zaučování nových zaměstnanců. Své práci rozumí a plní ji na 100%.

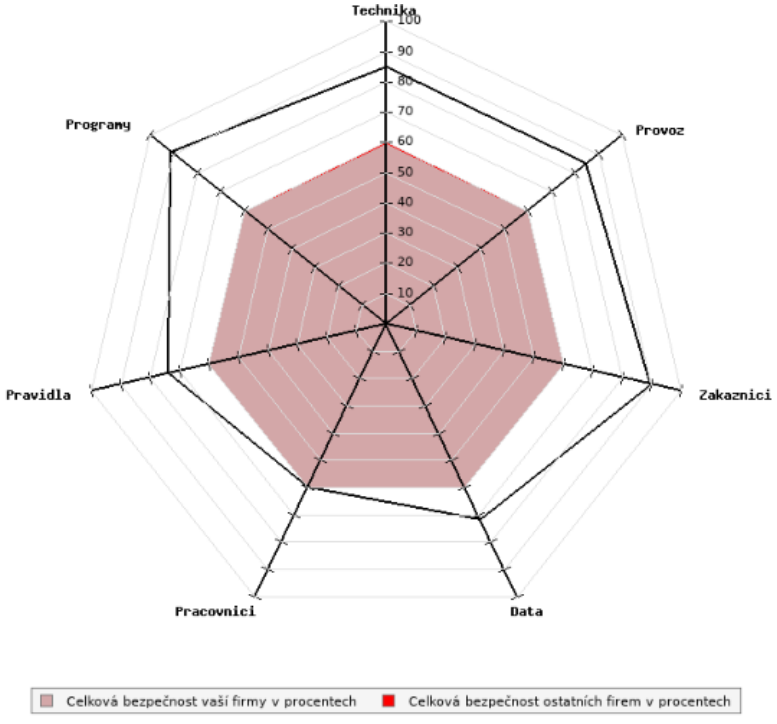


Obrázek č. 13: Hodnocení efektivity procesu
(Zdroj: Vlastní zpracování)

2.10.1.2 Bezpečnost

Bezpečnost IS školní jídelny není téměř zajištěna. Systém je velmi starý, běžící na starém HW zařízení. Stolní PC nevyžaduje heslo. Kdokoli se při vyřizování objednávky může dívat ze vzdálenosti 0,5m na monitor, kde vidí přesný průběh – a zároveň například jména dalších strávníků. Podle GDPR už v této chvíli dochází k porušení, neboť jméno je osobní údaj. Navíc je ve většině případů spjat s datem narození, případně ročníkem studia.

Počítač jako takový není chráněn antivirovým programem. Neexistuje bezpečnostní školení.



Obrázek č. 14: Hodnocení bezpečnosti procesu
(Zdroj: Vlastní zpracování)

2.10.1.3 Požadavky organizace

Vedení základní školy požaduje zvýšení bezpečnostního povědomí primárně z důvodu častých neúmyslných chyb zaměstnanců a žáků školy. Dále je velmi významným prvkem fakt, že narůstá práce s ICT technologiemi a s tím souvisí narůstající množství povinností a zvyšující se odpovědnost za možné chyby.

Ředitel školy stanovil následující cíle, které musí být naplněny:

- Každý zaměstnanec a žák školy musí znát a dodržovat základní pravidla informační bezpečnosti
- Každý zaměstnanec a žák by měl být schopen pracovat s internetem v souladu s informační bezpečností
- Učitelé by měli být schopni plně využívat ICT zařízení v učebnách, včetně používání elektronické třídní knihy
- Každý zaměstnanec by měl být schopen porozumět práci antivirových programů a zhodnotit výsledky jejich analýzy

- Každý zaměstnanec a žák by měl znát základní principy používání informačních a komunikačních technologií
- Každý uživatel IS by měl znát svá práva a odpovědnosti za své chování vůči informační bezpečnosti, včetně ochrany osobních údajů
- Každý zaměstnanec a žák školy by měl znát důsledky svých činů, které jsou v rozporu s pravidly informační bezpečnosti

Vedení školy požádalo o šest bloků po čtyřech hodinách, které probíhají vždy v pondělí podle stanoveného harmonogramu. Rozpočet na školení není stanoven, neboť škola spolupracuje na vytvoření metodik.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

Hlavním tématem této diplomové práce je vytvoření návrhu a zavedení programu budování bezpečnostního povědomí na základní škole. V této kapitole bude největší pozornost věnována jednotlivým fázím, rolím, koncepci programu a odpovědnostem. Zároveň bude popsána analýza možných rizik projektu. Na základě zjištěných poznatků budou vytvořeny metodiky školení a bude nastíněna implementační fáze.

3.1 Cíl programu

Prvním důležitým krokem je určit si, čeho se vlastně má v programu dosáhnout. Ve školním prostředí se nachází obrovská kvanta dat, která zahrnují osobní i citlivé údaje. Proto je nutné zajistit proaktivní ochranu. Toto prostředí je specifické v cílení útoků. Nepočítáme s jejich vyšším počtem pro získání osobních dat. Na druhou stranu zde hrozí vysoké riziko neúmyslného vyzrazení, kterému se dá vyhnout, pokud budeme zaměstnance a žáky školy dobře informovat.

Při analýze rizik byla identifikována různá nepřijatelná rizika, která je nutné eliminovat. K těmto rizikům patří zejména nešetrné zacházení s důležitými údaji (osobní údaje, citlivé údaje) a nedostatečné proškolení pracovníků školy. Tady je důležité zdůraznit, že školení se netýká pouze pedagogických pracovníků, nicméně i systému správy a údržby a také školní jídelny.

Cílem práce je tedy posílit ochranu dat a informací na gymnáziu s ohledem na jejich důvěrnost, integritu a dostupnost.

Návrh metodiky programu bude odpovídat legislativním podmínkám České republiky. Zejména vychází z evropského nařízení GDPR, norem řady ČSN ISO/IEC 27000 a z norem NIST SP 800-16 a NIST SP 800-50.

3.2 Výstupy

Po ukončení školení pro zaměstnance školy by každý pedagog měl být schopen školit žáky, a to s ohledem na jejich věkové zařazení. Rovněž by každý měl umět odpovědět na pár základních otázek, jako jsou například „Co řadíme k základním bezpečnostním zásadám?“, „Jaká jsou rizika informační bezpečnosti a která se mě bezprostředně týkají?“ „Mám zodpovědnost za nějaká pravidla, případně jaká?“ „Jaká je odpovědnost učitele/žáka vůči škole a okolí (z pohledu informační bezpečnosti)?“ a jiné.

3.3 Přínosy

Hlavní myšlenkou je zvýšit informovanost žáků a pedagogů, což by mělo vést k opatrnějšímu a správnějšímu zacházení s informacemi. V dnešní době se do rukou dítěte dostane velmi mnoho věcí připojených k síti internet. Od útlého věku se učí upozornění přeskakovat, neboť malé dítě ještě neumí číst, a poté se jen sporadicky stává, že by si upozornění číst začaly. Tyto návyky doprovází žáky i do pozdějšího věku. Mnoho pedagogů se nezamýšlí nad možnými důsledky například ukládání hesel v počítači, který nevyžaduje přihlášení, případně půjčování flash disků s citlivými údaji svých žáků přátelům. Podle GDPR by toto nemělo být dnes ani možné, bohužel praxe je jiná. Speciálně žáci a učitelé prvního stupně neberou tyto výzvy vážně.

Z těchto důvodů vyplývá, že hlavním přínosem by byla obezřetnost, která ale nesmí být přehnaná, a informovanost o možných důsledcích a opatřeních.

3.4 Plán

Pro správné dosažení libovolného cíle je vždy nutné vytvořit plán postupu s přibližnou časovou náročností jednotlivých částí. K dosažení cíle musí být splněna tři kritéria: seznámení zaměstnanců a žáků školy s bezpečnostními politikami (a případnými následky jejich nedodržení), zavedení těchto bezpečnostních politik do praxe a stanovení směrnic pro sledování a updaty programu. Vycházíme z Lewinova pojetí řízené změny (rozmražení, změna, zamražení).

3.5 Lewinův model

3.5.1 Analýza situace

Na základě analýzy byly zjištěny různé nedostatky. V této části je nutné si říci, jaký je stav (vyhovující, uspokojivý, nevyhovující) a rozhodnout, zda-li je nutné provést plánovanou změnu či nikoliv.

Je nutné ohodnotit klady a zápory projektu. Po vyhodnocení dojde ke zvážení, jestli projekt má smysl zavádět, nebo ne.

Síly působící pro změnu	**Váha**
Vedení školy	5
Zaměstnanci školy	4
Zlepšení konkurenceschopnosti	2
Zvýšení kvality vybraných procesů	3
MŠMT	3
	17

Síly působící proti změně	**Váha**
Finanční náklady	3
Časová náročnost	4
Zkrácení času na běžnou výuku	3
	10

Síly, které brzdí provedení změny	**Váha**
Nedokončená metodika (pro žáky)	5

Váhy jednotlivých sil jsou hodnoceny v intervalu 1 – 5 (1– nejméně působící, 5 – nejvíce působící).

Z výčtu je patrné, že sil působících pro je více, než sil působících proti. Významným faktorem je ovšem nedokončená metodika pro žáky, nicméně do konce dubna 2019 by i ta měla být zpracována.

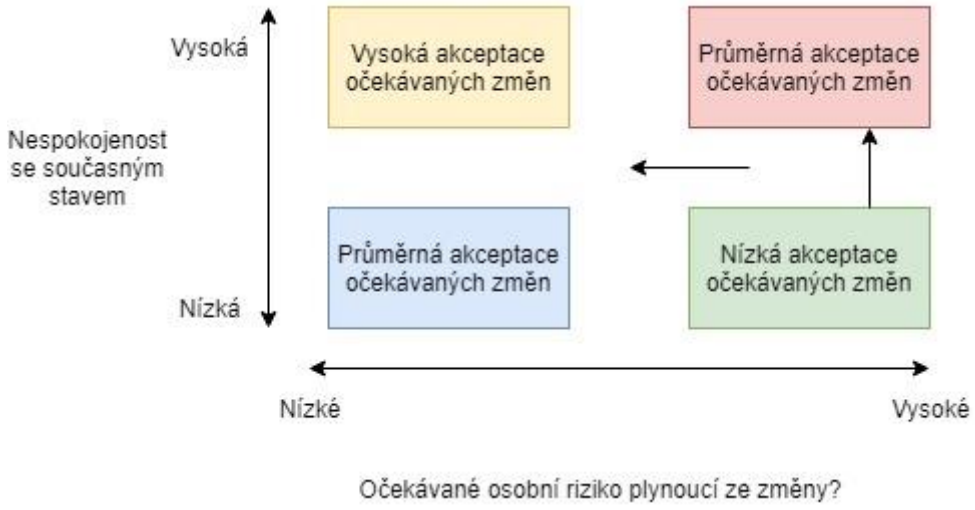
Dle konzultací a analýz byl stanoven závěr, že situace ve škole je nevyhovující. Je tedy nutné iniciovat proces změn.

3.5.2 Identifikace agenta změny

Agentem změny je externí pracovník, který má ovšem podporu takzvaného sponzora změny, v tomto případě Magistrátu města Brna. Ten agenta podporuje primárně finančními zdroji a politickou silou. Agent úzce spolupracuje s ředitelem školy.

V procesu plánování je nutné specifikovat nejdříve pár informací o prostředí, kde se projekt bude uskutečňovat. Zaměstnanci školy jsou poměrně dost vytížení, tudíž nejsou časově flexibilní. Nicméně jejich ochota akceptovat proces změny je vysoká. Pokud

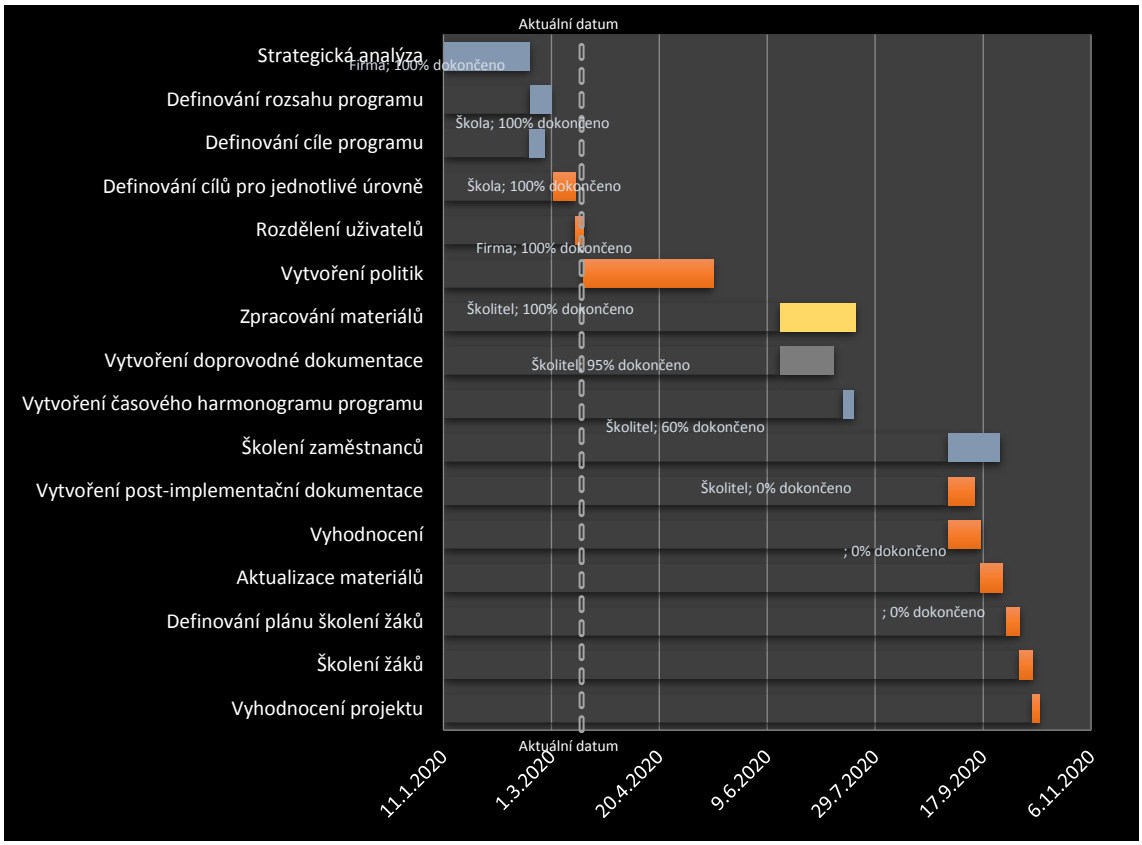
budeme vycházet z grafu o akceptaci očekávaných změn, můžeme je považovat za aktivní spolupracovníky.



Obrázek č. 15: Analýza rizik
(Zdroj: Vlastní zpracování dle č.10)

Agent by si také měl vést přehled o tom, v jaké fázi je projekt, informace o účastnících projektu a předpokládaném dokončení. K tomu mohou posloužit mnohé programy, z nichž některé jsou zdarma, jiné placené. Pro tyto účely slouží výborně například MS Project, který je velmi intuitivní a přehledný. Jednoduchý přehled lze ale vytvořit i například v MS Excel, který není plnohodnotnou náhradou, spíše finančně dostupným a jednoduchým nástrojem.

K popisu fází projektu se využívají Ganttovy diagramy. Projekt by poté mohl vypadat například takto:



Obrázek č. 16: Ganttův diagram
(Zdroj: Vlastní zpracování)

3.5.3 Identifikace intervenčních oblastí

V této části je důležité definovat oblasti, kterých se bude intervence týkat, a následně tyto zásahy specifikovat.

- **Lidské zdroje** – za dodržování pokynů je zodpovědný pracovník ICT (více práce), případně externí pracovník (záleží na rozhodnutí ředitele školy)
- **Technologie firmy** – zajištění lepší ochrany techniky v podobě SW
- **Komunikační a organizační toky a procesy firmy** – lepší zabezpečení komunikace na pracovišti i mimo něj

3.5.4 Intervence

Podle Kurta Lewina by měla změna probíhat ve třech fázích:

- **Rozmrazení** – stávající pravidla, zvyklosti a způsoby myšlení jsou rozmrazeny. Je nutné připravit podmínky pro provedení změny (analýzy, informovat

zaměstnance, minimalizovat odpor, připravit technologii firmy, zajistit zdroje, vytvořit rezervy).

- **Změna** – proběhne zamýšlená změna, její součástí může být zmatenost a nejistota. Vlastní změna je zaměřena na intervenční oblasti. Cílem je dosažení požadovaných parametrů (v tomto případě větší informovanost zaměstnanců, případně žáků).
- **Zamrazení** – nová pravidla, zvyklosti a způsoby myšlení jsou zamrazeny (zafixovány). V této fázi hrozí největší riziko neúspěchu. Je nutné projekt správně zakonzervovat, aby vše nespadlo zpět do starých kolejí.

3.5.5 Verifikace

Po zavedení projektu a jeho realizaci je nutné provést kontrolu výsledků. Ta by měla mít dvě úrovně. První by měla být provedena kontrola výsledků po školení zaměstnanců, poté, pokud vše dopadne v pořádku, po provedení výuky u žáků provést kontrolu výsledků i u nich. Výsledek by měl vést k lepší informovanosti a správnému zacházení s informacemi.

3.6 PERT

3.6.1 Seznam činností

Tabulka č. 1: Seznam činností
(Zdroj: Vlastní zpracování)

Činnost	Označení činnosti
Strategická analýza	A
Definování rozsahu programu	B
Definování cíle programu	C
Definování cílů pro jednotlivé úrovně	D
Rozdělení uživatelů	E
Vytvoření politik	F
Zpracování materiálů	G
Vytvoření doprovodné dokumentace	H
Vytvoření časového harmonogramu programu	I
Školení zaměstnanců	J

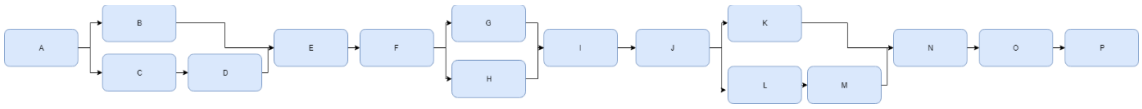
Vytvoření post-implementační dokumentace	K
Vyhodnocení	L
Aktualizace materiálů	M
Definování plánu školení žáků	N
Školení žáků	O
Vyhodnocení projektu	P

3.6.2 Návaznost a odhad doby trvání činností v hodinách

Tabulka č. 2: Návaznost a odhad doby trvání činnosti
(Zdroj: Vlastní zpracování)

Činnost	Následující činnost	Optimistický odhad	Realistický odhad	Pesimistický odhad
A	B, C	25	40	60
B	E	5	10	20
C	D	5	7	10
D	E	7	10	13
E	F	2	4	6
F	G, H	35	60	85
G	I	20	35	50
H	I	10	25	40
I	J	2	5	7
J	K, L	20	24	28
K	N	8	12	17
L	M	9	15	20
M	N	7	10	13
N	O	5	6	8
O	P	4	6	7
P	-	2	3	4

3.6.3 Návaznost činností



Obrázek č. 17: Síťový graf
(Zdroj: Vlastní zpracování)

3.6.4 Časová analýza

Základní charakteristiky metody PERT

Optimistický odhad	**a**	
Realistický odhad	**m**	
Pesimistický odhad	**b**	
Deterministický model	$\mathbf{T_e}$	$\frac{a+4m+b}{6}$
Začátek možný	**ZM**	KM předchůdce
Konec možný	**KM**	ZM + t_{eij}
Začátek přípustný	**ZP**	KP – t_{eij}
Konec přípustný	**KP**	ZP následníka
Rezerva celková	**RC**	ZP – ZM
Rezerva volná	**RV**	ZM následníka – KM
Rozptyl	$\boldsymbol{\sigma^2}$	$\frac{(b-a)^2}{36}$

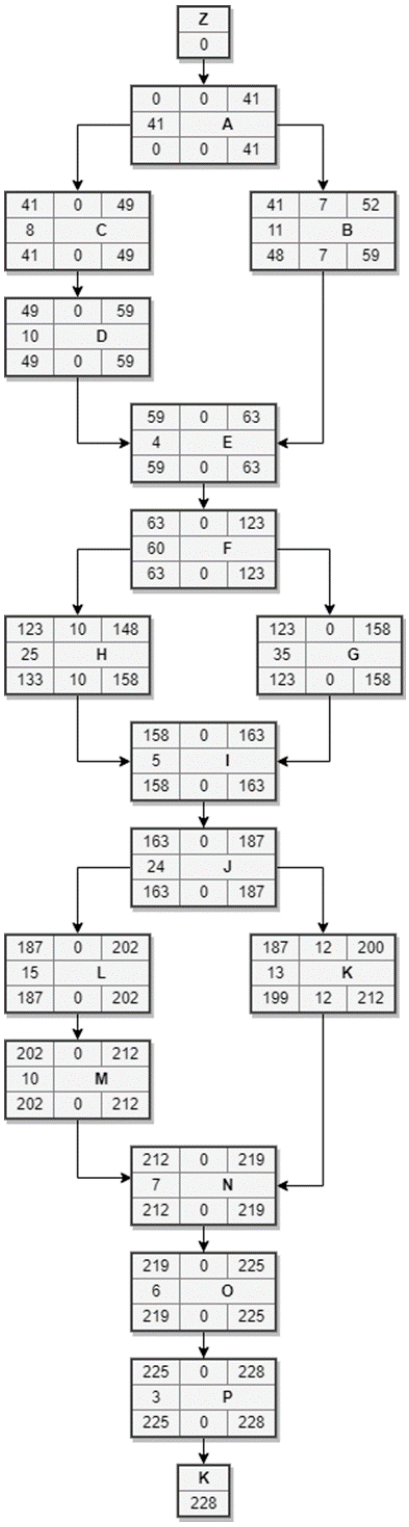
Tabulka č. 3: Výpočty metody PERT
(Zdroj: Vlastní zpracování)

Činnost	Nás. činnost	te	ZM	KM	ZP	KP	RC	RV	σ^2
A	B, C	41	0	41	0	41	0	0	34,03
B	E	11	41	52	48	59	7	7	6,25
C	D	8	41	49	41	49	0	0	0,69
D	E	10	49	59	49	59	0	0	1,00
E	F	4	59	63	59	63	0	0	0,44
F	G, H	60	63	123	63	123	0	0	69,44
G	I	35	123	158	123	158	0	0	25,00
H	I	25	123	148	133	158	10	10	25,00
I	J	5	158	163	158	163	0	0	0,69

J	K, L	24	163	187	163	187	0	0	1,78
K	N	13	187	200	199	212	12	12	2,25
L	M	15	187	202	187	202	0	0	3,36
M	N	10	202	212	202	212	0	0	1,00
N	O	7	212	219	212	219	0	0	0,25
O	P	6	219	225	219	225	0	0	0,25
P	-	3	225	228	225	228	0	0	0,11

3.6.5 Síťový graf

Na základě znalosti návaznosti a po zpracování časové analýzy všech činností zvoleného procesu jsme schopni sestavit podrobný síťový graf a z něj určit kritickou cestu a její délku.



Obrázek č. 18: Síťový graf
(Zdroj: Vlastní zpracování)

Kritická cesta

A-C-D-E-F-G-I-J-L-M-N-O-P

Délka kritické cesty

41+8+10+4+60+35+5+24+15+10+7+6+3 = 228 hodin

3.7 Analýza rizik

Analýza rizik byla vytvořena po konzultaci s ředitelem školy a učitelem ICT. Následné ohodnocení aktiv, pravděpodobností hrozby a zranitelností je stanoveno na základě zkušeností a subjektivního pohledu.

Hodnocení a řízení rizika projektu obsahuje čtyři kroky, které musí být prováděny opakovaně. Jsou to: rozpoznání rizika, vyhodnocení rizika, vytvoření rizikových plánů, sledování a řízení rizika.

Nejprve jsou rizika identifikována a ohodnocena s pomocí pravděpodobnosti výskytu rizika a závažnosti dopadu na chod společnosti. Následně jsou s pomocí mapy rizik rozdělena do čtyř různých kategorií závažnosti. S pomocí metod pro řízení rizik jsou navržena opatření pro snížení pravděpodobnosti výskytu rizik a jejich dopadu.

Pro analýzu rizik byla zvolena skórovací metoda.

Tabulka č. 4: Analýza rizik
(Zdroj: Vlastní zpracování)

Číslo rizika	Riziko	Pravděpodobnost	Dopad	Hodnota rizika
1	Chybně zpracovaná metodika	3	8	24
2	Malý zájem	4	6	24
3	Špatná interpretace	3	5	15
4	Nevhodně zvolený postup	2	4	8
5	Nedodržení časového plánu	2	6	12
6	Nedostatek vyškolených pracovníků	1	7	7
7	Nepřipravenost	3	6	18
8	Překročení rozpočtu	2	5	10
9	Ztráta dat	3	10	30

Ohodnocení rizik je provedeno v intervalu 1 – 10 (1– nejmenší váha, 10 – největší váha). Pokud vynásobíme pravděpodobnost rizika s příslušným dopadem, dostáváme hodnotu rizika, které využijeme pro zanesení do mapy rizik.

3.7.1 Mapa rizik

Mapa rizik rozděluje rizika do čtyř kvadrantů. Příslušný kvadrant je přiřazen dle pravděpodobnosti výskytu a dopadu rizika.

Obrázek č. 19: Analýza rizik
(Zdroj: Vlastní zpracování)

Kvadrant kritických hodnot rizik

Rizika s vysokou pravděpodobností výskytu a s velkým dopadem. Pro tato rizika je kriticky důležité vypracovat opatření.

Kvadrant významných hodnot rizik

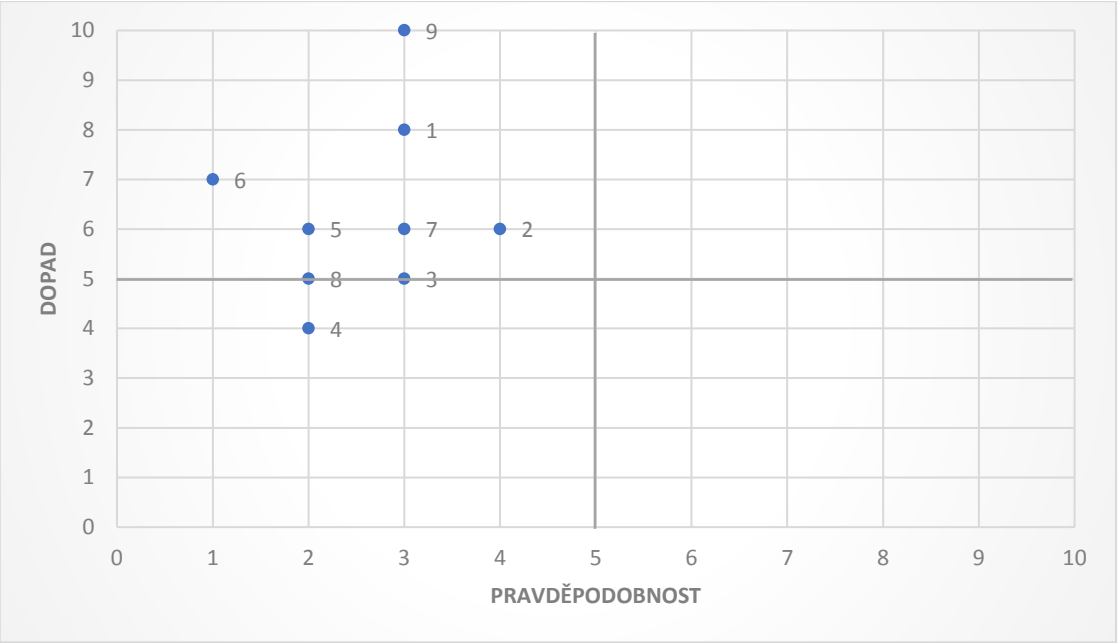
Rizika s nízkou pravděpodobností výskytu ale s velkým dopadem. Pro tato rizika je nutné vypracovat opatření.

Kvadrant běžných hodnot rizik

Rizika s vysokou pravděpodobností výskytu ale s malým dopadem. Pro tato rizika není nutné vypracovávat opatření, ovšem je dobré se těmto rizikům alespoň částečně věnovat.

Kvadrant bezvýznamných hodnot rizik

Rizika s malou pravděpodobností výskytu a s malým dopadem. Pro tato rizika není nutné vypracovávat opatření. Tato rizika akceptujeme.



Obrázek č. 20: Kvadranty naměřených hodnot rizik
(Zdroj: Vlastní zpracování)

Kvadrant kritických hodnot rizik = 0

Kvadrant významných hodnot rizik = 6

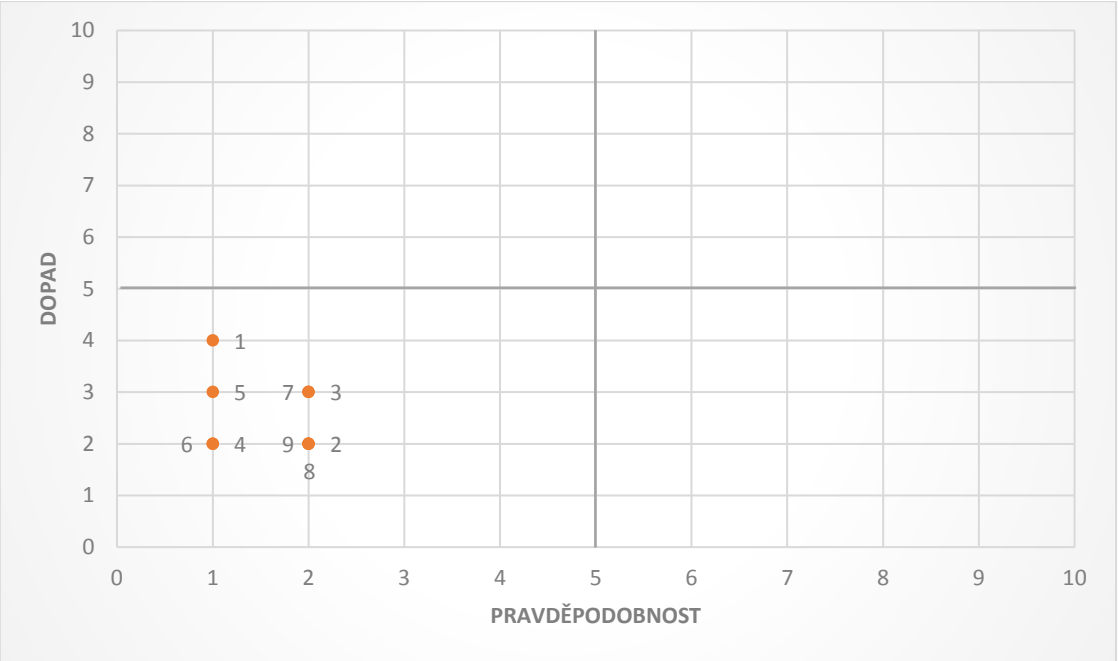
Kvadrant běžných hodnot rizik = 0

Kvadrant bezvýznamných hodnot rizik = 3

Pro všechna rizika hodnocena jako významná byla nalezena opatření, která by měla pomoci se snížením hodnoty pravděpodobnosti výskytu rizika a jeho dopadu. Tím, že nalezneme opatření, nepřestáváme s riziky počítat. Je nutné je nadále sledovat, což odpovídá čtyřem krokům hodnocení a řízení rizika zmíněných výše.

Tabulka č. 5: Opatření proti rizikům
(Zdroj: Vlastní zpracování)

Riziko	Opatření	Pravděpo-dobnost	Dopad	Hodnota rizika
1	**Důsledná příprava při zpracování metodiky**	1	5	5
2	**Projekt je interaktivní a zajímavý**	2	2	4
3	**Volba vhodného školitele**	2	3	6
4	**Znalost prostředí a aplikace na míru**	1	2	2
5	**Použití programů pro plánování projektů**	1	3	3
6	**Zajištění pracovníků ve vyhovujícím počtu (rezerva)**	1	2	2
7	**Tvorba podkladů (ke schválení předem)**	2	3	6
8	**Plánování rozpočtu s rezervou, domluva předem**	2	2	4
9	**Správný systém zálohování**	2	2	4



Obrázek č. 21: Kvadranty hodnot rizik protiopatření
(Zdroj: Vlastní zpracování)

Kvadrant kritických hodnot rizik = 0

Kvadrant významných hodnot rizik = 0

Kvadrant běžných hodnot rizik = 0

Kvadrant bezvýznamných hodnot rizik = 9

Po aplikování opatření se všechna rizika stala akceptovatelnými.

3.7.2 Zhodnocení analýzy rizik

Ve vypracovaných tabulkách lze vypozorovat nejvíce ohrožené oblasti. Z výsledků vyplývá, že je třeba dbát zvýšenou pozornost při zpracování metodik a přípravě školení, neboť právě tato místa jsou nejvíce kritická.

3.8 Rozsah programu

V analýze současného stavu byly zmínění požadavky stanovené ředitelem školy. Aby tyto požadavky mohly být naplněny, musí se školení týkat zejména těchto oblastí:

- Základy a zásady informační bezpečnosti (včetně možných rizik a odpovědností)
- Ochrana osobních údajů, včetně klasifikace dat
- Bezpečné využívání internetu (podvodné zprávy, nevhodné stránky)

- Zásady bezpečné komunikace (email, messenger)
- Bezpečné využívání informačních a komunikačních technologií
- Zásady správného zálohování dat
- Správa hesel
- Antivirové programy a jejich využití
- Pravidla pro využívání ICT ve výuce
- Práce s IS Edookit ve výuce (elektronická třídní kniha, známky, poznámky)
- Bezpečné používání sociálních sítí

Všechny požadavky musí odpovídat aktuálním legislativním zákonům.

3.9 Role a odpovědnosti SAE

Ačkoli se jedná podle počtu zaměstnanců o malý podnik, vzhledem k účelu této práce je vhodnější zvolit decentralizovaný model, neboť hlavní odpovědnost je především na pověřené osobě - CISO. Ten provádí školení zaměstnanců, kteří následně školí žáky školy.

V následující tabulce jsou přehledně zpracovány jednotlivé role a odpovědnosti v programu.

Tabulka č. 6: Role a odpovědnosti v programu
(Zdroj: Vlastní zpracování)

	Řízení	**Vývoj**	**Realizace**	**Vyhodnocení**
CISO	x	x	x	x
Ředitel	x		x	x
Učitelé			x	x
Žáci				x
Ostatní uživatelé				

3.9.1 CISO

CISO má na starosti vytvoření programu, což zahrnuje vytvoření strategie zavedení, přípravu a provedení školení. Jeho úkolem je dostatečně informovat účastníky o

přínosech školení a zároveň zdůraznit důležitost školení o kybernetické bezpečnosti. Následně dohlíží na správný průběh implementace a zajišťuje zpětnou vazbu programu.

Na této škole je CISO pověřená osoba týmem VUT, externista, který je na školu přidělen. Jeho úkolem je mimo jiné podrobná analýza školy, neboť je nutný mít celkový přehled o zázemí, kde daný program bude zavádět.

3.9.2 Ředitel školy

Jako hlava školy je ředitel nedůležitějším článkem mezi školitelem a zaměstnanci. Jeho hlavním úkolem je zajištění zdrojů (finančních, lidských), které jsou potřebné pro správný průběh vytvoření a zavedení programu. V jeho moci je také výběr kompetentní osoby, která bude zodpovídat za kontrolu a dohled. Ředitel je také v pozici kontrolora, kdy je nutné zkontrolovat, zda-li se požadavky školy shodují s metodikou školení, a je tedy možné program uvést do praxe.

3.9.3 Učitelé

Učitele ve škole můžeme rozdělit na dva typy. Třídní a ty, co vlastní třídu v současné době nemají. Nicméně to neznamená, že v budoucnu ji mít nebudou, z čehož vyplývá, že náplň školení je pro všechny stejná. Z důvodu implementační povinnosti školení pro žáky je nutné, aby každý pedagog uměl vzbudit v žácích zájem, dokázal jim vysvětlit důležitost školení a pravidla, kterými je třeba se řídit.

3.9.4 Ostatní uživatelé

Do této kategorie spadají žáci, zákonní zástupci a další zaměstnanci školy. Jedná se o nejrozsáhlejší a nejrizikovější skupinu. Je nutné dbát speciální pozornost na to, aby uživatelé správě chápali své povinnosti, možná rizika a odpovědnost za vzniklé chyby.

3.10 Rozdělení uživatelů

Jedním z prvních kroků je jednoznačně rozdělení uživatelů. To je nutné provést ve dvou fázích. V první fázi dochází k rozdělení podle pracovního nasazení, ve druhé potom do příslušného stupně pokročilosti (platí pouze pro fáze školení a vzdělávání). Na základě ověřených znalostí mohou být uživatelé přiřazeni do skupiny začátečníci, mírně pokročilí nebo pokročilí. Ke každé ze skupin se přistupuje individuálně a s ohledem na jejich potřeby. Rozřazení probíhá na základě odpovědí v dotazníku, který vychází z ECDL

certifikátů. Začátečníkem je automaticky nově příchozí zaměstnanec, který se poprvé seznamuje s IS školy.

V následující tabulce je znázorněno rozřazení uživatelů do jednotlivých fází programu i s jejich povinnostmi.

Tabulka č. 7: Fáze programu a odpovědnosti osob
(Zdroj: Vlastní zpracování)

	Povědomí		**Školení**		**Vzdělávání**	**Profesní rozvoj**	
	Základní bezpečnost	Bezpečnostní gramotnost	Normy a nařízení	Prohloubení vědomostí	Inovace v oblasti ICT	Obecná certifikace	Technická certifikace
Vedení školy	x	x	x	x	x	x	
Učitelé	x	x	x	x	x		
Správce sítě	x	x	x	x	x		x
Údržba	x	x					
Školní jídelna	x	x	x				
Žáci	x	x					
Zákonní zástupci	x	x					

Obecná certifikace není pro uživatele povinná, nicméně například pro vyučující ICT je velmi doporučená. Technická specifikace je povinná pro správce sítě.

Na zvolené škole není v současné době o profesní rozvoj zájem, ale vedení školy si ponechává možnost tuto část v budoucnu využít. Zároveň byl vznesen požadavek na vzdělávání učitelů i v oblasti novinek ICT, neboť mnozí z nich vyučují již několik let a je potřeba doplnit a rozšířit jejich znalosti o aktuální dění.

3.11 Fáze programu

V této kapitole jsou popsány jednotlivé fáze programu, které vychází z SAE, a jejich cíle.

3.11.1 Povědomí

Jak vyplývá z tabulky, fáze budování povědomí je společná pro všechny uživatele – od vedení školy, až po zákonné zástupce. Jedná se o nejrozsáhlejší část. Cílem této fáze je vzbudit zájem účastníků, kteří na základě získaných informací jsou schopni detekovat hrozbu či riziko z oblasti informační bezpečnosti, reagovat na něj odpovídajícím způsobem, případně umět s informacemi dále zacházet.

Pro tuto fázi je vhodné využít co nejvíce atraktivní metody. Vzbudíme-li zájem u pedagogů školy, je velice pravděpodobné, že budou dále schopni toto nadšení předávat svým studentům a ti se problematice budou více věnovat. K neosobním materiálům můžeme počítat různé letáčky, reklamy, emaily, informace na stránkách školy. Pro potenciální lepší výsledek je však dobré mít také osobní kontakt, tedy rozhovory. Na základě poznatků od zaměstnanců je možné lépe specifikovat dílčí cíle, které se ve fázi školení mohou využít. Stejně tak je vhodné zavést osobní kontakt se žáky školy, školním psychologem a zákonnými zástupci, což je možné primárně během třídních schůzek. Žáci vyššího stupně se mohou zapojit v rámci různých projektů.

Tímto způsobem dochází k nenásilnému předání informací, které pomáhá budovat povědomí o dané problematice.

3.11.2 Školení

Školení se účastní všichni zaměstnanci školy, kromě údržby. Je nutné zahrnout i zaměstnance školní jídelny, neboť pracují s osobními daty žáků. Cílem je předat (dle potřeb) bezpečnostní znalosti a dovednosti. V této fázi programu již rozdělujeme uživatele na začátečníky, mírně pokročilé a pokročilé. Ke každé skupině je přistupováno individuálně a na základě jejich potřeb jsou sestavené speciální metodiky.

Pro testování znalostí a rozřazení do úrovně je vhodné vybrat projekt ECDL. Tento projekt je zavedený i návrhu řešení budování bezpečnostního povědomí na gymnáziu, přičemž pro tento projekt vycházíme z požadavku, aby jednotlivé fáze na sebe navazovaly a žáci tak dostali během studia na základní, následně střední, škole komplexní informace

pro bezpečnou práci s daty. Rozdílné jsou ovšem doporučené moduly, které jsou přizpůsobené výuce na základní škole.

Tabulka č. 8: Kurzy ECDL
(Zdroj: Vlastní zpracování)

Stupeň pokročilosti a název kurzu	Témata	Výstupy
Začátečníci e-Citizen	- Řešení běžných situací a každodenních problémů - Bezpečné využívání online služeb - Komunikace na internetu - Vyhledávání informací a relevantnost dat	Po ukončení kurzu uživatel umí řešit běžně dennodenní situace, zvládá komunikovat skrze email a jiné komunikační portály, umí vyhledat data na internetu a zhodnotit důvěryhodnost vyhledaných dat.
Mírně pokročilí ECDL Start	Složení čtyř zkoušek z následujících modulů: - Internet a komunikace - Bezpečné používání IT - Počítač a soubory - Informace na internetu - Zpracování textu - Práce s tabulkami - Spolupráce na internetu Pozn.: doporučený je výběr prvních čtyř možností	Po ukončení kurzu uživatel umí zacházet s daty z webových stránek s ohledem na bezpečnost, rozumí pojmu záloha dat a je schopen činnost provádět, umí zabezpečit počítač před útoky škodlivého softwaru, dokáže třídit a vyhodnocovat informace z internetu pomocí podpůrných SW nástrojů.
Pokročilí ECDL Profile	Složení nejméně jedné zkoušky z nabízených modulů ECDL Core, ECDL Advanced, Digitální fotografie, e-Citizen a řady dalších.	Po ukončení kurzu uživatel umí tvořit webové stránky dle aktuálních požadavků trhu/upravit fotografie podle platných legislativních zákonů a norem/pracovat s tabulkami pro

	Doporučené moduly: - Webové stránky - Úpravy obrázků - Práce s tabulkami - Prezentace	následné využití analyzovaných dat/vytvářet prezentace na podporu výuky a možných projektových řešení.

Učitelé prvního stupně mají dle rozhodnutí ředitele školy požadavek na splnění minimálně úrovně mírně pokročilí, učitelé druhého stupně potom výrazné doporučení na splnění úrovně pokročilí. Zaměstnancům školní jídelny nebyly uděleny žádné požadavky.

3.11.3 Vzdělávání

Vzdělávání v oblasti inovací ICT je jeden ze základních požadavků ředitele školy.

Cílem této fáze je získat odborné znalosti z oblasti informační a kybernetické bezpečnosti, znalosti o hrozbách a technologických změnách. Na jejich základě je uživatel schopen včasné detekce a proaktivní reakce.

Z důvodu menšího počtu účastníků je vhodné vybrat externího školitele, neboť vytváření vlastních materiálů či objednání hromadného školení by bylo neefektivní a neekonomické. Kurzů nabízených dodavateli je celá řada a je jen na řediteli školy, případně vedení či správci sítě, kterou dodavatelskou firmu zvolí. Kurzy je vhodné navštívit jedenkrát ročně a doplnit si znalosti v případě změn legislativy či vzniku nových hrozeb.

Vybrané externí firmy nabízející školení:

Tabulka č. 9: Externí firmy nabízející školení
(Zdroj: Vlastní zpracování)

Název firmy	Místo školení	Témata kurzů
GoPas	Brno, Praha	HW, SW, IT bezpečnost, GDPR a další
Pcdir	Brno, Praha, Bratislava	HW, SW, Bezpečnost IT, manažerské kurzy
PCStorm	Praha, Kolín, Liberec, Trutnov, Pardubice, Hradec Králové, Jičín, na škole	Microsoft SW, grafika, zakázkové školení
NewHorizons	Praha, Bratislava, Košice	HW, SW, Bezpečnost IT, manažerské kurzy

Ceny kurzů jsou k dohledání pouze u některých firem. Rozmezí je přibližně 1500 Kč za méně náročné kurzy, až po 20 000 Kč za složitější kurzy.

Další možností je spolupráce s týmem VUT, který by tato školení zaštítil. Zatím na to ale není projekt připraven.

Po konzultaci s ředitelem školy byla vybrána firma GoPas, která má nejlepší reference a zkušenosti s oblastmi, které škola potřebuje.

3.11.4 Profesní rozvoj

Profesní rozvoj je nad rámec požadovaných znalostí většiny účastníků programu. Je však nutné zmínit, že správce sítě a vedení školy jsou v pozici, kdy by bylo vhodné znát aktuální legislativní podmínky a hrozby, kterým musí čelit. Ředitel je zároveň odpovědnou osobou za chod základní školy.

3.12 Povědomí – podpůrné a školící materiály

V této kapitole jsou popsány podklady, které slouží pro jednotlivé části budování povědomí. Vše vychází z požadavků ředitele školy a základních informací a pokynů z oblasti kybernetické bezpečnosti.

3.12.1 Bezpečnostní desatero

Pro výčet základních pravidel bezpečnosti je nutné zmínit, že neexistuje jednotný seznam, který by byl centrálně využíván. Pro potřeby této práce bylo tedy zvoleno bezpečnostní desatero, které je uzpůsobené jak žákům základní školy, tak i učitelům a dalším uživatelům programu.

1. Neotvírejte neznámé odkazy
2. Využívejte antivirové programy – a to nejen na notebooku či stolním PC, ale i na mobilním telefonu a tabletu
3. Pro práci s citlivými údaji nevyužívejte veřejných sítí Wi-Fi
4. Pozorně čtěte požadovaná povolení při instalaci aplikací
5. Pravidelně zálohujte
6. Svá hesla nikomu nesdělujte, ani je nezapisujte
7. Nenechávejte svá zařízení přihlášená bez dozoru, hrozí krádež dat
8. Ověřujte si informace, které na internetu nacházíte, neboť ne vše je pravdivé
9. Informace, které sdělujete, si pečlivě rozmyslete. Sdělte jen to, co jste schopni vyvěsit na vlastní vchodové dveře.
10. Pokud narazíte na něco, co se vám nezdá, informujte o tom

Zvláště je nutné specifikovat práci s hesly, neboť tato část je velmi rizikovým faktorem.

- Základní pravidla pro vytváření hesel (délka, složitost, důvěrnost)
- Základní pravidla pro správu hesel (pravidla změn, frekvence změn)

V současné době nejvíce času tráví žáci (a mnohdy i ostatní uživatelé) na sociálních sítích. Je tedy vhodné uvést základní pokyny pro bezpečnou práci mířené právě na tuto oblast.

- Nastavte si soukromí a pravidla sdílení (váš obsah uvidí jen ti, kterým to umožníte)
- Bezpečně se odhlašujte
- Pravidelně obměňujte přihlašovací heslo
- Čtěte pravidla pro používání sociální sítě pečlivě
- Do okruhu přátel schvalujte pouze ty lidi, které znáte
- Pokuste se omezit sdílení fotek v reálném čase

- Nenahrávejte intimní a hanlivé fotografie, které by mohly poškodit vás, nebo jinou osobu
- Nezveřejňujte osobní údaje

Proti škodlivému softwaru se většina uživatelů neumí, nebo nechce bránit. Útočníci jsou vždy krok napřed oproti těm, co se snaží vybudovat ochranu proti poškození (nejprve musí vzniknout slabina, než je opravena). Velmi častým současným trendem je také neinformovanost o možnosti pořídit si antivirový program na mobilní zařízení. Součástí programu by tedy mělo být i informování o škodlivém softwaru.

- Základní dělení škodlivého softwaru (zaměření na viry)
- Behaviorální analýza
- Příklady nejznámějších virů (historie, současnost)
- Detekce a protiopatření

Častým problémem, se kterým se setkává většina populace, je dezinformovanost. Uživatel neumí přesně odhadnout, co je pravdivé a co už ne. Na základě pravidel je ale možné zvýšit šanci odhalení falešné zprávy. Touto problematikou se v současné době zabývá autor knihy Fake News, která se stala velmi populární. Autor realizuje mnohá školení na středních školách, která se problematiky týkají. Se studenty diskutuje o příčinách, následcích a učí je detekovat hoaxy.

Mezi nejpoužívanější jednoduché metody patří prohlížení EXIFu fotografií (který je ovšem možné při exportu smazat, případně to lze i dodatečně v programech tomu uzpůsobených), vyhledávání částí textu, reverze obrázků a zdravý rozum.

Součástí updatů materiálů by mohl být seznam aktuálních hoaxů na internetu.

3.13 Bezpečnostní politika

Politika bezpečnosti je právní dokument, který popisuje, jakým způsobem organizace zaštiťuje bezpečnost. Musí být aktuální, srozumitelný, závazný a právně vymahatelný, zároveň musí existovat v písemné podobě a musí být dostupný. Je důležitou součástí obchodních podmínek. Šablona bezpečnostní politiky slouží mimo jiné i k vytvoření školících a podpůrných materiálů.

Politika bezpečnosti typicky obsahuje následující části:

1) Cíle bezpečnosti
2) Šíření působnosti a politiky bezpečnosti ve třech oblastech
    a) Fyzická a objektová bezpečnost
    b) Personální bezpečnost
    c) Informační bezpečnost (klasifikace dat, řízení oprávnění)
3) Odpovědnosti pracovníků

Pro zavedení programu byla vytvořena bezpečnostní politika, kterou již převzalo vedení školy a uvedlo do praxe. Z důvodu rozsahu celého dokumentu a obsahu dat, která škola nechce zveřejnit, bude dále popsána zkrácená verze této politiky.

3.13.1 Cíle bezpečnosti

1. Vytvoření vhodné úrovně zabezpečení pro celý informační systém základní školy, která vede ke zmírnění rizik (krádež, ztráta, zneužití, poškození)
2. Ochrana školy před zneužitím technických zařízení a ztrátou informací
3. Zajištění informovanosti účastníků o povinnostech a jejich odpovědnosti za ochranu důvěry, integrity a zabezpečení dat
4. Zajištění informovanosti účastníků o současných a relevantních právních předpisech České republiky a Evropské Unie, které je nutné dodržovat
5. Definování zásad pro informační systém školy

3.13.2 Šíření působnosti a politiky bezpečnosti

3.13.2.1 Fyzická a objektová bezpečnost

Cílem fyzické bezpečnosti je předejít neoprávněnému vniknutí, poškození, odcizení informací či materiálu.

Dle normy ISO/EIC 27001 jsme schopni rozdělit toto téma do dvou okruhů – Zabezpečení oblasti a Bezpečnost zařízení.

Zabezpečené oblasti

V analýze bylo popsáno, kolik vstupů (a přibližně kudy) vede do budovy školy. Z pohledu bezpečnosti není objekt příliš dobře střežen, je proto nutné zavést opatření. Například

zavedení systému, který v případě detekce neobvyklé činnosti uvědomí příslušníky policie ČR. Před školou se nachází několik přechodů, přičemž pouze před jedním z nich se nachází informační tabule pro řidiče o aktuální rychlosti a případné doporučení ke snížení rychlosti, aby nedošlo k úrazu. Bylo by vhodné v ranních hodinách zařídit alespoň dva policisty, kteří by pomáhali dětem přes přechod.

Pokud student přijde do školy později, než v 8:00 hodin, je nutné nahlásit se na vedení školy. Přilehlá střední škola má vstup na čipy. Tyto čipy již žáci používají ve školní jídelně, bylo by tedy vhodné systém zavést i pro vstup do budovy školy. Tím by se zvýšila bezpečnost pro žáky, neboť rodiče i učitelé by měli přehled o tom, jestli dítě dorazilo, nebo ne.

Uvnitř školy jsou všechny místnosti na klíč. Učebny se zamykají po ukončení poslední vyučovací hodiny. Bezpečnost je tedy přiměřeně zajištěna.

Škola je postavena v kopci, tudíž není třeba vymýšlet protipovodňová opatření. Budova je vybavena hasícími přístroji. Minimálně jedenkrát ročně dochází k nácviku evakuačního plánu školy, kterého se účastní všichni zaměstnanci i žáci školy.

Po zavedení doporučených postupů je potřebné ke každé části vytvořit bezpečnostní politiku, která bude shrnovat základní pravidla práce.

Bezpečnost zařízení

Veškeré technické i netechnické vybavení školy by mělo být uzavřeno v uzamykatelných skříních, kam žáci nemají přístup. Eliminuje se tím možné poškození vybavení.

Bezpečnost pasivních a aktivních prvků je řešena v nedostupnosti zařízení, a to jak pro žáky, tak pro zaměstnance. Síťová kabeláž je vedena pod lištami u stropu, switche se nachází v kabinetech učitelů, případně na chodbách vysoko u stropu. Ochrana síťových prvků je dostatečná.

3.13.2.2 Personální bezpečnost

Zaměstnanci školy absolvují jednou ročně školení o bezpečnosti práce poskytované externí firmou. Žáci školy jsou informováni o bezpečnosti v minimálním rozsahu jedné výukové hodiny a jejich znalosti jsou ověřovány formou testu. Zákonným zástupcům je předložen dokument k prostudování, který je následně stvrzen podpisem.

Každý zaměstnanec podepisuje smlouvu, v níž stvrzuje mlčenlivost, seznámení s právy a povinnostmi a případnými postihy.

3.13.2.3 Informační bezpečnost

Klasifikace dat

- Citlivá data (politický názor, náboženské vyznání, sexuální orientace, rasový a etnický původ, fyzické a duševní zdraví, záznamy z trestního rejstříku)
- Tajná data (jméno a příjmení, adresa, věk, telefonní číslo, fotografie, IP adresa)
- Interní data (interní komunikace, písemné práce žáků, posudky)
- Externí data (informace dostupné na webové stránce školy)

Řízení oprávnění

Rozdělení uživatelů do skupin bylo zmíněno již v analýze. Jedná se o pedagogické pracovníky, nepedagogické pracovníky, žáky a zákonné zástupce.

Žáci druhého stupně získávají přihlašovací údaje, nicméně bylo by vhodné zvýšit jejich bezpečnost – hesla se standartně skládají ze jména a příjmení žáka.

Pedagogičtí pracovníci mají k dispozici školní notebook. Ten je třeba opatřit heslem, které by mělo být delší než 8 znaků a mělo by obsahovat velká a malá písmena a číslice. Změna tohoto hesla je zavedena na 1x ročně. Notebook se automaticky uzamyká po pěti minutách. Při pěti neplatných pokusech je notebook uzamčen a je třeba zavolat správce sítě.

3.13.2.4 Odpovědnosti pracovníků

V současné době je veškerá odpovědnost na vedení školy. Výjimku tvoří pouze notebooky, které mají učitelé k dispozici. Za ty si zodpovídají pedagogové sami. Je doporučeno k seznamu aktiv přiřadit odpovědné osoby a ohodnotit důležitost aktiv. Za kompletní seznam je určena jedna odpovědná osoba.

Při poruše notebooku nese plnou odpovědnost učitel. Problém nastává při předání zařízení externí firmě, kdy pedagog poskytuje všechny informace uložené na HDD. Proto je nutné uchovávat je buď mimo HDD, nebo obměnit omezení a umožnit disk vyjmout.

Povinností správce sítě je zabezpečit notebook proti škodlivému softwaru a upozornit majitele notebooku na možná rizika a opatření. Vhodná témata pro výchovu zaměstnanců

dle požadavků personální bezpečnosti jsou například malware, zálohování, pohyb na internetu a další.

3.13.3 Doprovodná dokumentace

V rámci bezpečnostních politik školy je třeba přiložit několik dalších dokumentů. Vhodné je připojit slovníček pojmů z oblasti informační bezpečnosti (úvodní kapitola této práce může posloužit jako vhodný zdroj), vývoj a údržba IS (zajišťováno externí firmou), disciplinární politika, politika o ochraně osobních údajů a právní dokumenty, jako jsou Evropské nařízení GDPR, Kybernetický zákon č. 205/2017 Sb., Školský zákon č. 561/2004 Sb., Zákon č. 89/2012 Sb. O ochraně osobnosti.

Politika o ochraně osobních údajů

Pod pojmem politika o ochraně osobních údajů si většina zaměstnanců představila pouze GDPR. Ale tato politika se netýká jen nařízení GDPR, týká se i zákona č. 89/2012 Sb. a občanského zákoníku. Z tohoto důvodu byl vytvořen informační dokument týkající se tohoto tématu.

V úvodu dokumentu (politiky) je jasně specifikováno, že jediná odpovědná osoba za porušení práv žáků, zákonných zástupců a zaměstnanců (při ochraně osobních údajů), je ředitel školy. V případě újmy je povinen tuto ztrátu plně nahradit.

Vzhledem k nařízení GDPR, které vešlo v platnost roku 2018, je třeba zkontrolovat dokumenty školy a odpovědět na následující otázky:

- Jsou dokumenty zpracovávané školou potřebné?
- Jsou jasně specifikované uzavřené smlouvy, které mají přístup k osobním údajům?
- Jsou data zpracovávána na základě zákona nebo souhlasu?
- Jsou data zpracovávána v souladu s právními předpisy?

Uživatel nemá pouze povinnosti, ale má také svá práva. V politice by měla být tato práva popsána. Mezi ně patří:

- Právo na přístup k osobním údajům
- Právo na opravu
- Právo na omezení zpracování

- Právo být zapomenut
- Právo vznést námitku proti zpracování osobních údajů
- Právo na přenositelnost údajů
- Právo být obeznámen s bezpečnostním porušením

Politika by měla stanovit:

- Kodex chování
- Povinnosti a odpovědnosti pověřence pro ochranu osobních údajů
- Pravidla pro zpracování citlivých údajů
- Pravidelné výmazy dat
- Opatření proti úniku a zneužití osobních údajů
- Pravidla pro práci s osobními údaji v listinné/elektronické formě

3.14 Budování bezpečnostního povědomí u žáků

Výuka na základní škole je oproti výuce například na střední škole o něco rozmanitější. Nelze komunikovat s dítětem ve věku 6ti let stejně, jako s 15ti letým žákem v posledním ročníku. Proto je nutné zvolit různé metodiky, které povedou k efektivnímu výsledku.

Žáci školy jsou běžně rozdělováni na tyto skupiny:

- Žáci 1. – 3.třídy
- Žáci 4. – 5. třídy
- Žáci 6. – 9. třídy

Žáci 1. – 3. třídy

Do první skupiny spadají žáci ve věku 6-9 let. Nejmladší z nich neumí číst a psát. Je tedy nutné přistupovat k této věkové kategorie pomocí obrázků, videí a diskuze.

Ve spolupráci se školním psychologem a učitelem ICT bylo vytvořeno výukové video, které vychází z dostupného videa na youtube z dílny WNS Cares Foundation. Video je nutné představit jako popis dennodenních událostí, se kterými se děti setkávají. Po shlédnutí krátkého videa je učitelem iniciována diskuze. Každé dítě dostává prostor vyjádřit svůj názor a připojit do diskuze svou osobní zkušenost. Poté jsou zkušenosti rozebrány a žáci si vzájemně mohou udělovat rady, jak se v dané situaci v budoucnu zachovat.

Pro domácí přípravu a rozšíření bezpečnostního povědomí je připojena publikace vycházející ze spolupráce firmy Microsoft a Walta Disneye. Komix s názvem „Bezpečný internet“ žákům přibližuje témata počítačových virů, chování na internetu a například pirátství. Každé z témat je napsáno formou příběhů hrdinů, kteří se musí vypořádat se špatným chováním. Publikace je ukončena testem, který obsahuje vždy tři možnosti odpovědí, z nichž jen jedna je správná.

Žáci 4. – 5. třídy

Do této skupiny patří děti ve věku 9-11 let. K této kategorii je vhodné přistupovat ve třech etapách: podnícení debaty, ilustrace možných příběhů, diskuze.

V první části dochází k vysvětlení důležitosti tématu a ke zjištění současných znalostí žáků. Jelikož se jedná o věkovou skupinu, která začíná sledovat různé youtubery a blogery, jedno z témat, na které je vhodné se zaměřit, je sdílení obrázků, videí a aplikace, které žáci mohou znát a již využívat. K tomuto účelu je zpracován materiál, na kterém se nachází různá loga (WhatsApp, Instagram, Snapchat, Messenger, Twitter, Facebook, Youtube, Pinterest a další). Následně dochází k diskuzi o oprávnění, které aplikace vyžadují, a nebezpečích, ale i výhodách, které nabízí. S touto diskuzí souvisí otevření debaty, které vychází z pořekadla „Co nemáš řád, nečiň druhému.“ V poslední řadě je doporučeným tématem, které velmi souvisí s předešlým, selfie fotografie. Žák je tázán, zda si uvědomuje, co vše na svých fotografiích sděluje. Nabízí interaktivní činnost, kdy se žáci podívají do svých telefonů na pořízená selfie a vypíší si informace, které je možné z obrázku vyčíst.

Pro doplnění výuky, případně jako domácí příprava, se opět hodí obrazové publikace. Stránka bezpecninternet.cz nabízí několik interaktivních publikací, které je dobré spustit a projít. Jsou to například „Nekonečný les“ o počítači, síti a emailové komunikaci, „Annin nový přítel“, který je pokračováním a zabývá se chováním na internetu a fotografií, a „Ztráty a nálezy“ o zveřejňování osobních dat na internetu. Žáci tak nenásilnou formou proniknou do důležitých a složitějších témat.

Žáci 6. – 9. třídy

Žáci této kategorie jsou ve věku 11-15 let. Zaujmout tuto skupinu je velmi obtížné, proto je doporučeno projekt zavádět v učebně, kde jsou k dispozici počítače, či ve třídách se zapůjčenými netbooky nebo tablety.

V úvodní části je dobré vzbudit v žácích zájem, vysvětlit jim vážnost a důležitost probíraného tématu. V roce 2019 vychází film s názvem „V Síti“, který pojednává o zneužití dětí na českém internetu. Vzhledem k tomu, že tato věková skupina spadá do rizikové oblasti, je vhodné dokument žákům pustit a následně jej rozebrat. Vedení školy si rovněž přeje zmínit téma kyberšikany, které se na druhém stupni základní školy velmi nebezpečně rozšiřuje. Mezi interaktivní činnosti může být zapojeno vyhledávání informací na internetu o sobě a následně o spolužákovi. Žáci tak získají přehled o tom, co znamená chránit si soukromí a co je a není vhodné sdílet.

Alternativní možnosti

Pro žáky nižšího stupně je nutné vše provést pomocí hry. Inspiraci můžeme čerpat například v existující hře na Finanční gramotnost. Žák je postaven před hrací plán, na kterém pomocí figurek simuluje chod rodiny, která potřebuje své bydlení, má různé příjmy apod. Pro naše účely může být hra navržena tak, že žák je běžným uživatelem domácnosti připojené k síti internet. Používá chytrá zařízení dle libosti, schvaluje podmínky apod. Na druhé straně je „záškodník“, například v podobě učitele, který se snaží systém rozvrátit a získat citlivá data, která dále může zneužít.

Druhou variantou by bylo sepsání tzv. gamebooku. Dříve velmi oblíbená herní knížka, kdy po přečtení krátkého odstavce o současné situaci ve hře se čtenář rozhoduje o dalším kroku. Podle rozhodnutí „skáče“ v knížce na stránku, která mu byla přiřazena. Protože v současné době žáci příliš nečtou, bylo by vhodné knížku převést do elektronické podoby, například jako aplikaci pro tablet, neboť čím dál tím více škol tablety žákům do výuky pořizuje.

Pro žáky vyššího stupně musíme počítat se školením, které bude interaktivní a vtáhne je do problematiky. Inspiraci můžeme hledat například ve špionážním muzeu v Berlíně, které je vybudováno tak, aby si mladší i starší návštěvníci pomocí různých stanovišť vyzkoušeli různé šifry, ať už v roli toho, který šifruje, nebo člověka, který se snaží kód

rozšifrovat, a další. Jedno z prvních stanovišť je počítač, ke kterému je připojen další monitor. Na prvním z nich je možné zadat heslo, které například máme k emailové schránce. Druhý monitor poté vypíše, za jak dlouho by heslo rozluštil. Pokud je možné jej rozluštit do pár vteřin, řešení dokonce nabídne a rozšifrované heslo vypíše. Další možností je využití staré počítačové učebny, kde se nachází přibližně 15 osobních počítačů s Windows XP. Na těch je možné žákům ukázat, jak funguje například zahlcení a vysvětlit jim tím důležitost podpory, aktualizací apod.

Obecně řečeno vždy je dobré žáky do problematiky vtáhnout. Pokud si na něco takzvaně šáhnou, lépe si daný problém zapamatují a v budoucnu se pokusí snížit riziko možných problémů.

Výše zmíněná řešení byla v současné době školou odsunuta do pozadí, neboť vyžadují větší časovou přípravu jak ze strany školitele, tak ze strany žáků. Projekt je nutné zapojit do osnov, což v běžícím školním roce není možné. Po dohodě s vedením školy by se interaktivní hry měly zapojit ve školním roce 2021.

3.15 Post-implementační část

Podle programu SAE je poslední, a nedílnou, součástí post-implementační fáze. Zde je nutné vyhodnotit získané výsledky a získat zpětnou vazbu. Tato fáze se týká také počtu opakování školení a aktualizací, případně úprav, výukových materiálů.

3.15.1 Dokumentace

Dokumentaci je nutné vytvořit pro doložení výuky a pro uchování zpětné vazby uživatelů. Dokument musí být uložen v zabezpečeném archivu školy. Obsahem je každá část programu SAE.

Školení, která proběhla, je nutné doložit podpisy na prezenčních listinách, popřípadě vyplněnými testy. Certifikát, který účastníci získávají, se jako kopie ukládá do archivu školy. Vyhodnocení materiálů se ukládá v listinné formě a obsahuje kompletní historii proběhlých změn.

3.15.2 Četnost opakování, aktualizace materiálů

Vzhledem k faktu, že SAE je nikdy nekončící činnost, je třeba školení opakovat. Doporučená frekvence je jedenkrát ročně, pro učitele v tzv. přípravném týdnu (poslední týden prázdnin, standartně poslední týden v srpnu), pro žáky je rozhodnutí na vedení

školy. Během letních prázdnin dochází k aktualizaci výukových materiálů a možným změnám požadavků vedení školy. V případě náhlých změn je třeba školení zahrnout dříve, nejlépe na nejbližší možné schůzi pedagogů, které se konají pravidelně jedenkrát měsíčně, vždy v pondělí.

3.16 Přínos návrhů řešení

Veškeré potřebné materiály pro zavedení programu budování bezpečnostního povědomí na základní škole jsou obsaženy v této práci. Vybraná základní škola se rozhodla práce využít a program zavést.

V první řadě proběhlo školení zaměstnanců školy, které vedlo k několika významným výsledkům. Prvním z nich bylo propojení IS školní jídelny se stávajícím systémem Edookit, což samo o sobě zajistilo větší bezpečnost informací. Druhým významným výsledkem je fakt, že většina pedagogů ihned po školení požádala o pomoc se správou notebooků, a to s instalací dobrého antivirového programu, zálohou dat a změnou hesel v počítači za bezpečnější. Učitelé porozuměli systému automatického ukládání hesel a přestali jednat bezmyšlenkovitě. Zpětná vazba byla velmi pozitivní, v metodice školení byly vytvořeny drobné úpravy.

Po školení zaměstnanců proběhlo školení žáků, z časových důvodů zatím jen pro žáky na prvním stupni. Na základě dopoledního programu, který vedli třídní učitelé s mou pomocí, byly zjištěny nedostatky a plusy navrženého řešení. Zpětná reakce od žáků proběhla ve třech úrovních. Nejdříve pomocí diskuze okamžitě po ukončení programu, následně druhý den formou kratší písemné práce (žáci 1. a 2. třídy pomocí verbální komunikace) a naposledy na třídních schůzkách prostřednictvím rodičů, kteří hodnotili projekt z pohledu zadané domácí činnosti a podle reakce dětí, které doma byly jistě otevřenější a sdílnější. Ohlasy byly vesměs kladné. Menší žáci dokonce měli tendence rodiče doma poučovat o bezpečném chování na internetu.

Tato práce se tedy velmi osvědčila. Využití je široké, neboť po úpravách podle požadavků jiné školy je možné metodiku převzít a zavést celý program. Je však nutné dokončit ještě druhou část školení žáků, a to cílovou skupinu 11-15 let.

K přínosům jistě patří snížení bezpečnostních incidentů, které se na škole objevují a mají vzrůstající tendenci. Konkrétní čísla budou ovšem známá až po nějaké době od zavedení.

Splnění legislativních požadavků je jistě také významným přínosem, neboť může škole ušetřit nemalé peníze za porušení.

Z hlediska budoucnosti dochází k lepší konkurenceschopnosti, neboť tento program je inovativní a mnoho rodičů při volbě základní školy může dát právě na tuto skutečnost. Údaje žáků (i zákonných zástupců) jsou v přiměřeném bezpečí, neboť ti, co s daty nakládají, mají potřebné znalosti a informace, jak s daty nakládat.

V neposlední řadě je přínosem zvýšení digitální gramotnosti žáků, kteří ví, jak se chovat v kyberprostoru. Rozeznají, co je vhodné sdílet, a co nikoli. Ví, čím mohou poškodit druhou osobu. Jsou obezřetní při komunikaci s cizími osobami.

4 ZÁVĚR

Diplomová práce měla za cíl vybudovat program na zvyšování bezpečnostního povědomí na základní škole. Do práce byly zahrnuty i požadavky stanovené vybranou základní školou. Všech cílů bylo dosaženo a program mohl být zaveden.

Práce je rozdělena do několika částí. V první části jsou specifikovány základní termíny z oblasti informační a kybernetické bezpečnosti, ISMS a program SAE, včetně postupů zavádění. Dále jsou popsány normy, nařízení a zákony, které je třeba dodržet.

Druhá část se zabývá analýzou současné situace, tedy představení organizace a vybavení školy. Všechny informace byly poskytnuty vedením základní školy. Do této části patří také analýzy vnějších a vnitřních faktorů, jako jsou SLEPT, Porterova analýza pěti sil, analýza 7S a závěr analýzy SWOT.

Ve třetí části je popsán samotný návrh zavedení programu, včetně podrobné analýzy rizik, výpočtu potřebného času pomocí metody PERT a Lewinova modelu. V samotném závěru dochází ke zhodnocení přínosů projektu a podmínek možného dalšího využití.

SEZNAM POUŽITÉ LITERATURY

[1] RODRYČOVÁ, Danuše a Pavel STAŠA. Bezpečnost informací jako podmínka prosperity firmy. Praha: Grada, 2000. Manažer. ISBN 80-716-9144-5.

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

[3] ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

[4] DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 978-808-6946-887.

[5] Hoax: význam. IT Slovník: Počítačový slovník [online]. IT-Slovnik.cz team, ©20082018 [cit. 2019-05-02]. Dostupné z: https://it-slovnik.cz/pojem/hoax

[6] What is VPN? Whatismyipadress [online]. [cit. 2019-04-01]. Dostupné z: http://whatismyipaddress.com/vpn

[7] SINGH, Simon. Kniha kódů a šifer. Druhé. Dokořán, 2009. ISBN 978-80-7363-268-7

[8] Co je to Malware a jak ho odstranit. Avast: Ochrana před hrozbami na internetu [online]. AVAST Software, ©1988-2016 [cit. 2018-05-02]. Dostupné z: https://www.avast.com/cs-cz/c-malware

[9] PETŘÍKOVÁ, R. Moderní management znalostí: (principy, procesy, příklady dobré praxe). Praha: Professional Publishing, 2010. ISBN 978-80-7431-011-9.

[10] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[11] ŽŮREK, Jiří. Praktický průvodce GDPR. Olomouc: ANAG, 2017. Právo (ANAG). ISBN 978-80-7554-097-3.

[12] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016

[13] GDPR.cz [online]. Praha, ©2018 [cit. 2019-01-02]. Dostupné z: http://www.gdpr.cz/

[14] ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

[15] SOKOL, Jan. Malá filosofie člověka: Slovník filosofických pojmů. 5., rozš. vyd., (Ve Vyšehradu 3.). Praha: Vyšehrad, 2007. ISBN 978-80-7021-884-6.

[16] Technické normy ČSN. Technické normy [online]. 2008 [cit. 2019-03-05]. Dostupné z: https://www.technickenormy.cz/tridy-norem-csn/

[17] ISO members. ISO [online]. [cit. 2019-03-05]. Dostupné z: https://www.iso.org/members.html 8) ISO logo. DWG logo [online]. [cit. 2017-03-05]. Dostupné z: https://dwglogo.com/iso-logo/

[18] About the IEC. IEC [online]. 2017 [cit. 2019-03-09]. Dostupné z: http://www.iec.ch/about/

[19] Řada norem ISO/IEC 27000. Risk Analysis Consultants, s.r.o. [online]. Risk Analysis Consultants, ©2017 [cit. 2018-05-02]. Dostupné z: http://www.iso27000.cz/

[20] NIST SP 800-16. Information Security: A Role-Based Model for Federal Information Technology/ Cyber Security Training. Revision 1 (2nd Draft Version 2). Gaithersburg: National Institute of Standards and Technology, 2013.

[21] NIST SP 800-50. Computer Security: Building an Information Technology Security Awareness and Training Program. Gaithersburg: National Institute of Standards and Technology, 2003.

[22] Vyhláška č. 316/2014 Sb.: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Zákony pro lidi: Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. AION CS, ©2010-2018 [cit. 2018-05-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014316

[23] 12. Zákon č. 205/2017 Sb.: Zákon, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony. Zákony pro lidi: Sbírka zákonů ČR v aktuálním konsolidovaném znění [online]. AION CS, ©2010-2018 [cit. 201805-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

[24] Kybez [online]. [cit. 2019-05-10]. Dostupné z: https://www.kybez.cz/uvod

[25] NÚKIB [online]. [cit. 2019-05-10]. Dostupné z: https://www.govcert.cz

[26] Co to znamená kybernetická bezpečnost?. Prevence kriminality v ČR [online]. [cit. 2019-05-10]. Dostupné z: http://www.prevencekriminality.cz/kyberkriminalita-testovaci-provoz/kyberneticka-bezpecnost/?ftresult=syst%C3%A9m+v%C4%8Dasn%C3%25A

[27] SOSINSKY, B. Mistrovství - počítačové sítě: Vše, co potřebujete vědět o správě sítí. 1. vydání. Brno: Computer Press, 2011. ISBN 978-80-251-3363-7.

[28] Do you need an IDS or IPS, or both? Tech Target [online]. [cit. 2017-04-01]. Dostupné z: http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPSor-both

[29] Cloud computing services. KCS [online]. [cit. 2019-05-10]. Dostupné z: https://www.kcsitglobal.com/cloud-computing-services

[30] Zásady moderního projektového řízení [online]. Brno [cit. 2019-05-10]. Dostupné z: https://lacko.otw.cz/eseje/Co_je_projektove-rizeni.doc.pdf

[31] Analýza pěti sil 5F (Porter's Five Forces). Management Mania [online]. [cit. 2019-05-10]. Dostupné z: https://managementmania.com/cs/analyza-5f

[32] McKinsey 7S. Management Mania [online]. [cit. 2019-05-10]. Dostupné z: https://managementmania.com/cs/mckinsey-7s

[33] SWOT analýza. Management Mania [online]. [cit. 2019-05-10]. Dostupné z: https://managementmania.com/cs/swot-analyza

[34] Metoda PERT (Program Evaluation and Review Technique). *Management Mania* [online]. [cit. 2019-05-10]. Dostupné z: https://managementmania.com/cs/metoda-pert

SEZNAM TABULEK

Tabulka č. 1: Seznam činností 62
Tabulka č. 2: Návaznost a odhad doby trvání činnosti 63
Tabulka č. 3: Výpočty metody PERT 64
Tabulka č. 4: Analýza rizik 67
Tabulka č. 5: Opatření proti rizikům 70
Tabulka č. 6: Role a odpovědnosti v programu 72
Tabulka č. 7: Fáze programu a odpovědnosti osob 74
Tabulka č. 8: Kurzy ECDL 76
Tabulka č. 9: Externí firmy nabízející školení 78

SEZNAM OBRÁZKŮ

Obrázek č. 1: CIA triáda 13
Obrázek č. 2: Vazba mezi daty 15
Obrázek č. 3: Přiměřená bezpečnost 22
Obrázek č. 4: Životní cyklus informační bezpečnosti 23
Obrázek č. 5: Cyklus PDCA 28
Obrázek č. 6: SAE program 30
Obrázek č. 7: Počítačová síť 34
Obrázek č. 8: Cloud 35
Obrázek č. 9: Porterova analýza pěti sil 38
Obrázek č. 10: Model 7S 39
Obrázek č. 11: SWOT analýza 40
Obrázek č. 12: Lewinův model 41
Obrázek č. 13: Hodnocení efektivity procesu 54
Obrázek č. 14: Hodnocení bezpečnosti procesu 55
Obrázek č. 15: Analýza rizik 60
Obrázek č. 16: Ganttův diagram 61
Obrázek č. 17: Síťový graf 64
Obrázek č. 18: Síťový graf 66
Obrázek č. 19: Analýza rizik 68
Obrázek č. 20: Kvadranty naměřených hodnot rizik 69
Obrázek č. 21: Kvadranty hodnot rizik protiopatření 71