VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH METODIKY BUDOVÁNÍ BEZPEČNOSTNÍHO POVĚDOMÍ NA STŘEDNÍ ŠKOLE

DESIGN METHODOLOGY OF SECURITY AWARENESS AT THE SECONDARY SCHOOL

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Hana Sobotková**
AUTHOR

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

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Hana Sobotková**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

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:

Návrh metodiky budování bezpečnostního povědomí na střední škole

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Pro vybranou střední školu vypracujte metodický postup pro budování bezpečnostního povědomí v rámci ISMS.

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

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 28. 2. 2017

L. S.

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Tato diplomová práce řeší téma budování bezpečnostního povědomí na středních školách. Cílem je vytvořit jednotnou metodiku budování bezpečnostního povědomí, která může být využívána středními školami k zajištění ochrany vlastního perimetru, svých uživatelů i okolí před jednáním uživatelů. Úvodní část se věnuje základní terminologii, existujícím či připravovaným český i mezinárodním zákonům, normám, předpisům a certifikaci v oblasti informační a kybernetické bezpečnosti. V praktické části jsou popsány jednotlivé kapitoly metodiky budování bezpečnostního povědomí v prostředí středních škol.

Abstract

The diploma thesis addresses the topic of security awareness education at secondary schools. The goal is to develop a standardized methodology for building security awareness, which can be used by secondary schools to ensure the protection of their perimeter, their users and others from the user's actions. The introductory part deals with the basic terminology, existing and forthcoming Czech and international legal acts, norms, regulations and certification in the area of information and cyber security. The practical part includes the methodology chapters describing the building of security awareness at secondary schools.

Klíčová slova

Systém řízení bezpečnosti informací, Budování bezpečnostního povědomí, Metodika, Školení, Speciální publikace NIST SP 800-50

Keywords

Information Security Management System, Security Awareness Education, Methodology, Training, Special Publication NIST SP 800-50

Bibliografická citace

SOBOTKOVÁ, H. Návrh metodiky budování bezpečnostního povědomí na střední škole. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 91 s. Vedoucí diplomové práce Ing. 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 neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 26. května 2017

……...

Hana Sobotková

Poděkování

Za ochotu, poskytnuté konzultace a komentáře k mé diplomové práci děkuji Ing. Petru Sedlákovi. Současně mé poděkování patří také zástupcům spolupracující střední školy za doplňující informace ke zpracovávanému tématu, poskytnutí podkladů potřebných k praktické části práce, vstřícný přístup a profesionální spolupráci.

Obsah

Úvod

Když téměř před sto lety v roce 1920 poprvé použil Karel Čapek slovo „robot“ ve významu „umělý dělník“ ve svém vědeckofantastickém dramatu R. U. R. (celý název díla Rossumovi univerzální roboti), pravděpodobně netušil, že za několik desítek let bude téma robotizace a automatizace natolik aktuální a rozšířené, že se bude dotýkat běžného života všech lidí.

Nyní se nacházíme na počátku 21. století a původní myšlenka robotizace a automatizace, a to snaha pomoci lidem od těžké a namáhavé práce, je sice stále na pořadu dne a většina výzkumných a vývojových odborníků ji ve svých hlavách stále střeží, ovšem doba pokročila a lidská touha po moci a chtíč ovládat či vykořisťovat druhé u některých osob roste, a tak se již mnoho let objevuje i druhá temná strana mince s negativními dopady.

S rozvojem informačních a komunikačních technologií se rychlost přenosu i objem dat zvýšil několikanásobně a i nadále exponenciálně roste. Zároveň se díky masové výrobě snižují náklady na pořízení stále novějších a lepších zařízení. Důsledkem toho je fakt, že dnešní dospělý člověk mnohdy nevlastní jedno komunikační zařízení (např. smartphone), ale má jich po ruce hned několik, a to navíc v různých podobách (telefon, tablet, netbook, notebook a další). Toto však v posledních letech nebývá výsadou pouze dospělých. S informačními technologiemi i výpočetní technikou se dnes do kontaktu dostávají stále mladší a mladší jedinci. Některé děti si sice ve věku pěti let neumí zavázat tkaničky u bot, ale spustit si hru na tabletu jim nedělá sebemenší problém. Už od útlého věku přicházejí děti o možnosti naučit se některým dovednostem, což jistě neplatí plošně pro všechny, ale postihuje stále větší procento osob této věkové kategorie. Za tím se však skrývá problém s daleko kritičtějšími riziky a dopady. Jde o to, že většina zařízení, se kterými si děti hrají, je neustále připojena k internetu. Špatným zacházením se tak lehko může stát, že dojde k úniku soukromých dat a zneužití informací uložených v zařízení třetí osobou. Toto se dotýká nejen dětí, ale i dospívajících jedinců, dospělých a seniorů.

Účinnou obranou proti zneužití informací je budování bezpečnostního povědomí u všech věkových kategorií uživatelů informačních a komunikačních technologií. Zpracováním metodiky budování bezpečnostního povědomí na střední škole se zabývá tato diplomová práce.

Cíle a metodika práce

V dnešním světě se už války neodehrávají pouze na bitevním poli v určitých místech na naší planetě, ale útoky přicházejí stále častěji z kybernetického prostoru prostřednictvím připojení do veřejné sítě. Cíl bitev se změnil ze získání území a surovinového bohatství na získání informací. Účinnou obranou proti novým hrozbám a útokům, kterým čelí každý uživatel informačních a komunikačních technologií a výpočetní techniky, je budování bezpečnostního povědomí (angl. zkratka SAE). Právě na toto téma budu nahlížet z různých úhlů pohledu v rámci této diplomové práce.

Primárním cílem je uspokojit potřebu, která se v souvislosti s masovým používáním informačních a komunikačních technologií a nových zařízení připojených k internetu objevila mezi mladými lidmi, a to vytvořit jednotnou metodiku budování bezpečnostního povědomí, která může být využívána středními školami k zajištění ochrany vlastního perimetru, svých uživatelů i okolí před jednáním uživatelů.

Z pohledu teoretických východisek je potřeba se zmínit o normách řady ČSN ISO/IEC 27000, které řeší nastavení, udržování a neustálé zlepšování systému informační bezpečnosti. V další části bude rozebrána s tématem budování bezpečnostního povědomí související kybernetická bezpečnost a zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů. Na toto téma naváži obecnými informacemi o budování bezpečnostního povědomí, jeho cíli, fázích a přístupech. Zmíním také možnosti certifikace, a to nejen z pohledu organizace (normy řady ČSN ISO/IEC 27000), ale i jednotlivců, a to prostřednictvím mezinárodní společnosti ISACA a konceptu ECDL a jeho modulu Managing Online Information, který byl v letošním roce v České republice představen jako v jediné zemi na celém světě.

Abych zajistila relevantní informace a odraz reálného prostředí střední školy, naváži spolupráci se zástupci konkrétní střední školy, s jejichž pomocí provedu analýzu současného stavu budování bezpečnostního povědomí v organizaci. V další části se budu zabývat samotnou tvorbou metodiky budování bezpečnostního povědomí na středních školách, při níž se nechám inspirovat normami řady ČSN ISO/IEC 27000, zákonem o kybernetické bezpečnosti a speciálními publikacemi NIST SP 800-50 a NIST SP 800-16. Zpracovanou metodiku SAE pak budou moci aplikovat v praxi všechny střední školy v České republice.

1 Teoretická východiska práce

V této části práce se zaměřím na přiblížení základních stavebních kamenů, na kterých lze bezpečnostní povědomí vybudovat a dále rozvíjet. Za důležité považuji uvést základní terminologii spjatou s tématem řízení bezpečnosti informací a zmínit se o zákonech, normách a předpisech, ať už ryze českých nebo z mezinárodního prostředí, jež poskytují této problematice určitý rámec. Téma budování bezpečnostního povědomí nahlédnu jak z pohledu komplexního, tj. jako součást celé organizace, tak i detailního, a to na systém jako takový.

1.1 Slovník základních pojmů

Pro sladění výkladu základních pojmů zmiňovaných v dalších částech této práce je třeba hned v úvodu vymezit význam často používaných výrazů. Při jejich výkladu vycházím z normy ČSN ISO/IEC 27000:2014 [1] a odborné publikace Problematika ISMS v manažerské informatice [2]. Nejčastější pojmy seřazené podle abecedy uvádí následující tabulka.

Název	Anglický překlad	Výklad
Aktivum	Asset	Veškerý hmotný a nehmotný majetek mající pro organizaci nějakou hodnotu.
Analýza rizik	Risk Analysis	Proces pochopení povahy rizika a určení jeho zdrojů.
Audit	Audit	Systematický, nezávislý a zdokumentovaný proces sloužící k objektivnímu hodnocení podle předem stanovených kritérií.
Bezpečnost informací	Information Security	Zachování důvěrnosti, integrity a dostupnosti informací.
Bezpečnostní incident	Security Incident	Pojem označující nějakou nestandardní či nepříjemnou bezpečnostní událost, která vede k narušení pravidel bezpečnosti v organizaci.
Bezpečnostní	Security	Technika použitá pro implementaci

mechanismus	Mechanism	bezpečnosti.
Bezpečnostní politika	Security Policy	Pravidla určující systém řízení, ochrany a distribuce aktiv.
Bezpečnostní událost	Security Event	Identifikovatelný stav systému, služby nebo sítě, ukazující na možnost porušení bezpečnostní politiky nebo selhání bezpečnostních opatření.
Data	Data	Údaje, používané pro popis nějakého jevu nebo vlastnosti pozorovaného objektu. Plnění informace, kterou vytváří.
Dopad	Impact	Vznik škody v důsledku působení hrozby.
Dostupnost	Availability	Zajištění přístupnosti k informaci oprávněnému uživateli v požadovaný okamžik.
Důvěrnost	Confidentiality	Zajištění přístupnosti k informaci pouze oprávněnému uživateli.
Hrozba	Threat	Událost ohrožující bezpečnost.
Informace	Information	Obecně lze informace chápat jako údaj o reálném prostředí, o jeho stavu a procesech. V užším pojetí se jedná o poznatek/znalost mající v daném kontextu specifický význam.
Informační systém	Information System	Aplikace, služby, aktiva informační technologie nebo další komponenty zacházející s informacemi.
Integrita	Integrity	Zajištění správnosti a úplnosti informace.
Míra	Measure	Ukazatel určující informační potřebu.
Opatření	Countermeasure	Aktivita umožňující snížení hrozby.
Preventivní opatření	Preventive Action	Opatření k odstranění potenciální neshody.
Prohlášení o aplikovatelnosti	Statement of Applicability	Dokument s popisem opatření v ISMS organizace.
Riziko	Risk	Kombinace hrozby a zranitelnosti s dopadem

		na aktivum.
Zranitelnost	Vulnerability	Slabé místo aktiva.

1.2 Systém řízení bezpečnosti informací (ISMS)

Každý podnikatelský subjekt, ať už hovoříme o fyzické či právnické osobě, shromažďuje, zpracovává, uchovává a šíří informace. Tyto informace mohou nabývat v různých fázích procesu jejich šíření odlišné podoby. Rodí se v hlavách jejich tvůrců, kteří je dále poskytují ostatním zainteresovaným osobám ústně, nebo je napíší na papír, příp. je rovnou zaznamenávají elektronicky za pomoci výpočetní techniky. Z tohoto vyplývá, že nejen samotné informace, ale i lidé, systémy a procesy jsou důležitými aktivy pro dosažení cílů organizace. Všechny tyto aspekty čelí řadě rizik, která mohou ovlivnit fungování organizace. Tato práce se zaměřuje na oblast bezpečnosti informací, implementaci takových opatření, jimiž organizace vědomě čelí existujícím rizikům, a budování bezpečnostního povědomí.

Norma ČSN ISO/IEC 27000 říká, že: *„ochrana informačních aktiv stanovením, dosažením, udržováním a zlepšováním bezpečnosti informací je nezbytná pro to, aby organizace mohla dosáhnout svých cílů a udržovat a zlepšovat soulad s právními normami a udržovat a zlepšovat svoji image.“* [1] Díky až překotně rychlému vývoji zejména v oblasti informačních technologií dochází k častým změnám a objevují se stále nová rizika. Aby organizace v závislosti na měnících se okolnostech monitorovaly a vyhodnocovaly efektivnost stávajících opatření, je třeba zjišťovat nová rizika a zavádět příslušná bezpečnostní opatření. Pro zajištění koordinace a kontinuálnosti celého procesu je zapotřebí jej vnímat jako součást systému, který by měl směřovat prostřednictvím nastavených politik k určitému cíli.

Za vhodný nástroj lze považovat systém řízení bezpečnosti informací (angl. název Information Security Management System, zkratka ISMS) definovaný souborem norem ISO/IEC řady 27000. Norma ČSN ISO/IEC 27000 vykládá ISMS jako soubor *„politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování*

bezpečnosti informací organizace tak, aby byly dosaženy její cíle. Je založen na posuzování rizik […].“ [1]

1.2.1 Principy a cíl ISMS

Systém řízení bezpečnosti informací je nedílnou součástí řízení organizace. Může být zaveden jak pro organizační složku subjektu, tak pro informační systém příp. jeho část, anebo může zahrnovat celou organizaci. Implementace ISMS je vhodná jak pro činnosti organizace státního, tak i komerčního sektoru. Zavedení ISMS je strategickým rozhodnutím vedení společnosti, které musí být přijato, odstupňováno a aktualizováno podle aktuálních potřeb organizace. Jedná se o efektivní a dokumenty podložený systém řízení a správy informačních aktiv, jehož cílem je eliminovat možnou ztrátu nebo poškození těchto aktiv tím, že jsou:

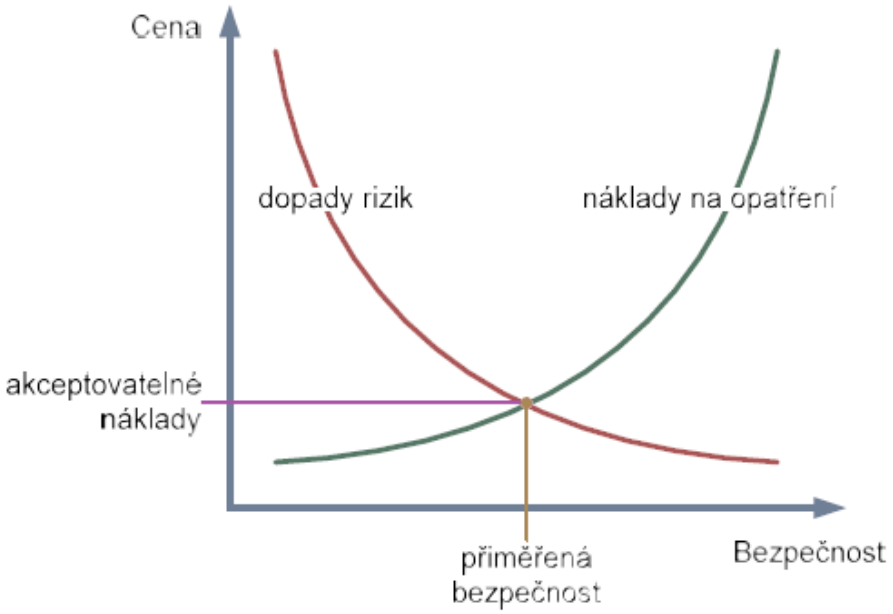
- určena aktiva, která je třeba chránit;
- zvolena a řízena možná rizika bezpečnosti informací;
- zavedena opatření s požadovanou úrovní záruk, která jsou kontrolována.

K úspěšné implementaci systému řízení bezpečnosti informací přispívají níže uvedené základní principy:

- komplexní přístup k řízení bezpečnosti informací;
- posouzení rizika a nastavení příslušných opatření;
- začlenění závazku vedení a zájmů zúčastněných stran;
- určení odpovědnosti za bezpečnost informací;
- **povědomí o potřebě bezpečnosti informací;**
- bezpečnost jako základní prvek informačních sítí a systémů;
- prevence a detekce incidentů bezpečnosti informací;
- neustálé opakované posuzování nastavených bezpečnostních opatření a jejich modifikace podle potřeby. [1]

Aby mohl být systém řízení bezpečnosti informací úspěšně a efektivně zaveden, implementován a v organizaci dodržován, neobejde se bez investic, a to jak z pohledu času, lidských zdrojů, materiálního vybavení, tak i finančních prostředků. Bezpečnostní

politika organizace stanovuje velikost úsilí a investic do bezpečnosti informací. Celkové investice musí odpovídat hodnotě aktiv a míře možných rizik. [3] Na níže uvedeném obrázku je zobrazen graf, který udává představu o přiměřené bezpečnosti za akceptovatelný objem finančních nákladů.



Obr. 1: Graf přiměřené bezpečnosti za akceptovatelné náklady [2]

Ze samotného názvu „systém řízení bezpečnosti informací“ je patrné, že předmět zájmu se bude týkat bezpečnosti informací, ať už jsou existující rizika organizací vnímána jako interní či externí. Pojem bezpečnost informací bývá širokou veřejností občas zaměňován s kybernetickou bezpečností, ačkoliv se jedná o dvě specifické oblasti bezpečnosti. Více informací k oběma přibližují následující subkapitoly.

1.2.2 Bezpečnost informací

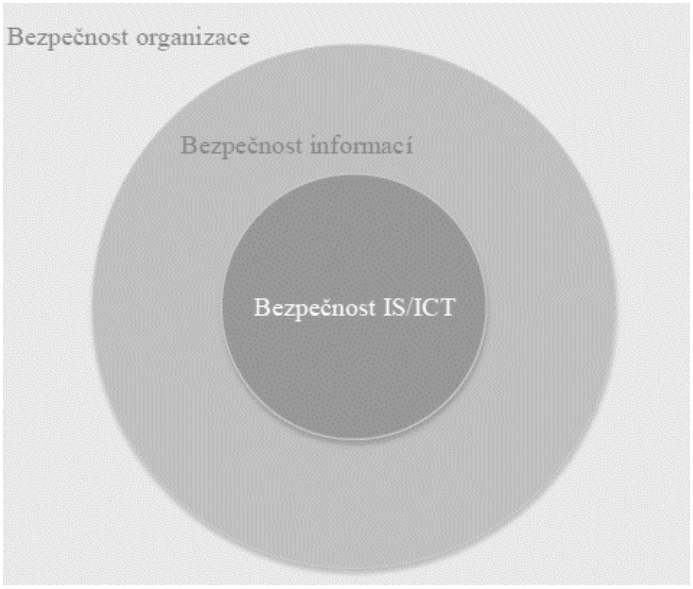
O vnímání informací jako aktiva a o jejich důležitosti z pohledu organizace se zmiňuje již kapitola 1.2 Norma ČSN ISO/IEC 27002:2014 zaměřená na soubor postupů pro opatření bezpečnosti informací uvádí, že: *„hodnota informací přesahuje napsaná slova, čísla a obrázky […]. V navzájem propojeném světě jsou informace a související procesy, systémy, sítě a pracovníci podílející se na jejich provozování a nakládání*

s nimi a ochraně aktiva, která jsou, jako jiná významná obchodní aktiva, cenná pro podnikání organizace, a proto si zaslouží nebo vyžadují ochranu proti různým rizikům.“ [4] Bezpečnost informací neboli informační bezpečnost řeší ochranu informací a jejich dostupnost.

Bezpečnost informací cílí na ochranu informací a majetku před krádeží, korupcí či přírodní katastrofou, přičemž oboje musí být dostupné oprávněným uživatelům. Z toho vyplývá, že mezi základní požadavky (seřazené dle důležitosti) patří:

- důvěrnost – přístup k informacím pouze oprávněným osobám;
- integrita – správnost a úplnost informací;
- dostupnost – informace dostupné pouze oprávněným uživatelům v okamžiku potřeby. [2]

Bezpečnost informací bezprostředně souvisí s bezpečností organizace a bezpečností IS/ICT. Nejširší pojetí zastupuje bezpečnost organizace, jejímž cílem je zajištění majetku společnosti. Automaticky tedy zahrnuje informační bezpečnost a bezpečnost IS/ICT. Naopak nejužší záběr má bezpečnost IS/ICT, která se zaměřuje na ochranu informačních systémů, komunikačních technologií a informací v nich uchovávaných a zpracovávaných.



Obr. 2: Vztahy bezpečností v organizaci [Upraveno podle 2]

1.2.3 Kybernetická bezpečnost

Jestliže se bezpečnost informací týká organizace, neboli ochrany dat před jejich poškozením, zničením, ztrátou či zcizením z pohledu důvěrnosti, dostupnosti a integrity, pak kybernetická bezpečnost se zaměřuje na kybernetický prostor. Takovým prostorem se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořený informačními systémy, službami a sítěmi elektronických komunikací. Pojem kybernetická bezpečnost představuje souhrn právních, organizačních, technických a vzdělávacích prostředků, směřujících k zajištění ochrany kybernetického prostoru.

V roce 2011 přijala vláda České republiky usnesení č. 781/2011, kterým ustavuje Národní bezpečnostní úřad (NBÚ) gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast. [5] O tři roky později byl České republice schválen zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, který nabyl účinnost 1. ledna 2015. *„Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.“* [6]

Kybernetická bezpečnost není tématem pouze lokálním a krátkodobým. Hrozby, kterým v rámci kybernetického prostoru čelíme, se týkají každého běžného uživatele celosvětové sítě Internet a dalších systémů a jsou tématem vždy aktuálním. Je tedy třeba brát tuto problematiku vážně. Vždyť jedna z nejběžnějších hrozeb, a to zneužití osobních údajů, se týká každého z nás.

1.2.4 Demingův cyklus - PDCA

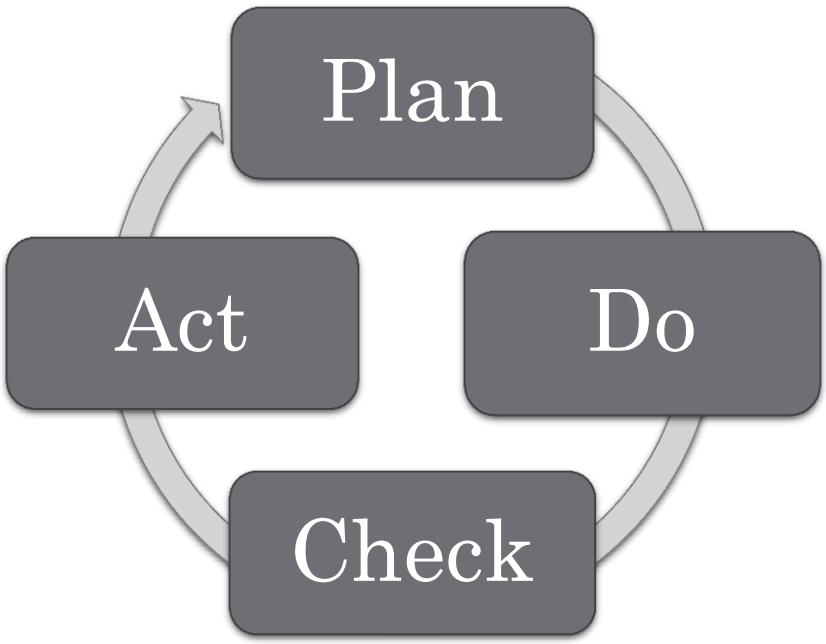
Demingův cyklus nebo jinak také PDCA cyklus je jedním ze základních manažerských principů. Tento model je založen na postupném zlepšování procesů (např. kvality výrobků či služeb) probíhajícím formou opakovaného provádění čtyř po sobě jdoucích aktivit. Tato metoda neustálého zlepšování se dá využít ve všech typech organizací. Cyklus PDCA lze chápat jako součást každého procesu, který se plánuje, realizuje a kontroluje. Demingův cyklus zahrnuje následující čtyři fáze (uvedeny angl. názvy):

- Plan – naplánování zamýšleného zlepšení, sestavení plánu;
- Do – realizace plánu;

- Check – porovnání výsledku realizace s původním záměrem;
- Act – úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe. [7]

V praxi se PDCA cyklus využívá k zavedení různých změn. V případě aplikace ISMS představují jednotlivé fáze PDCA cyklu tyto aktivity:

- Plánuj – Ustanovení ISMS;
- Dělej – Zavádění a provozování ISMS;
- Kontroluj – Monitorování a přezkoumání ISMS;
- Jednej – Udržování a zlepšování ISMS. [2]



Obr. 3: Demingův cyklus [Upraveno podle 8]

1.2.5 Normy řady ISO/IEC 27000

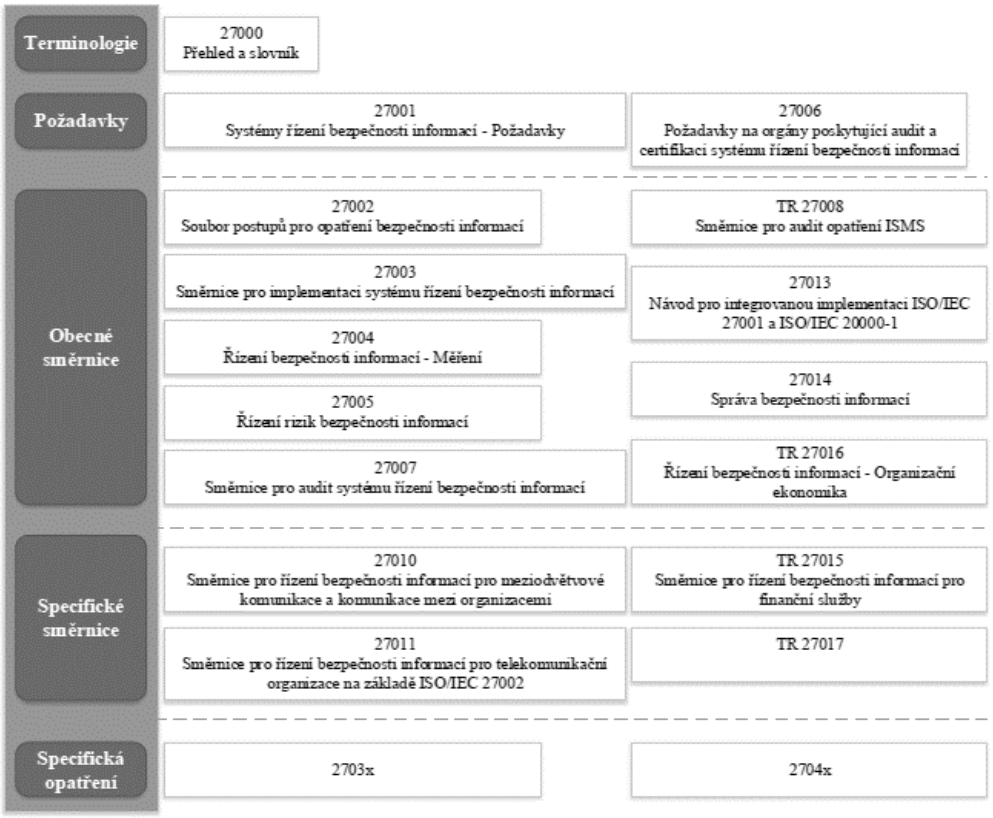
Standardizaci systému řízení bezpečnosti informací (Information Security Management System) řeší normy řady ISO/IEC 27000. Na jejich vypracování se podílejí národní orgány prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti, které jsou členy Mezinárodní organizace pro normalizaci (International Organization for Standardization – ISO) a Mezinárodní

elektrotechnické komise (International Electrotechnical Commission – IEC). [1] Překlad souboru norem zajišťuje v České republice Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Mezinárodní označení norem je ČR převzato a doplněno o zkratku ČSN, což je zákonem chráněné označení pro českou technickou normu. Neoficiálně je pro zkratku ČSN zažit také výklad česká soustava norem.

Normy řady ISO/IEC 27000 vznikly doplněním a aktualizací původních příkladů dobré praxe a standardů v rámci britské normy BS 7799 a zahrnutím vybraných opatření uvedených v normě ISO/IEC 17799:2005. Cílem norem je nejen specifikovat systém řízení bezpečnosti informací, ale i poskytnout organizacím rámec, jak bezpečnost informací implementovat a řídit. [2] Některé vybrané normy, jež se dotýkají tématu budování bezpečnostního povědomí, jsou uvedeny níže.

ČSN ISO/IEC 27000:2014

Jedná se o mezinárodní normu, která definuje pojmy a uvádí definice obecně používané ve všech ostatních normách z této série. Neobsahuje však veškeré termíny. Smyslem normy je pomoci se zavedením a provozem systému ISMS v organizacích všech typů a bez rozdílu velikosti a povahy činnosti. [1]

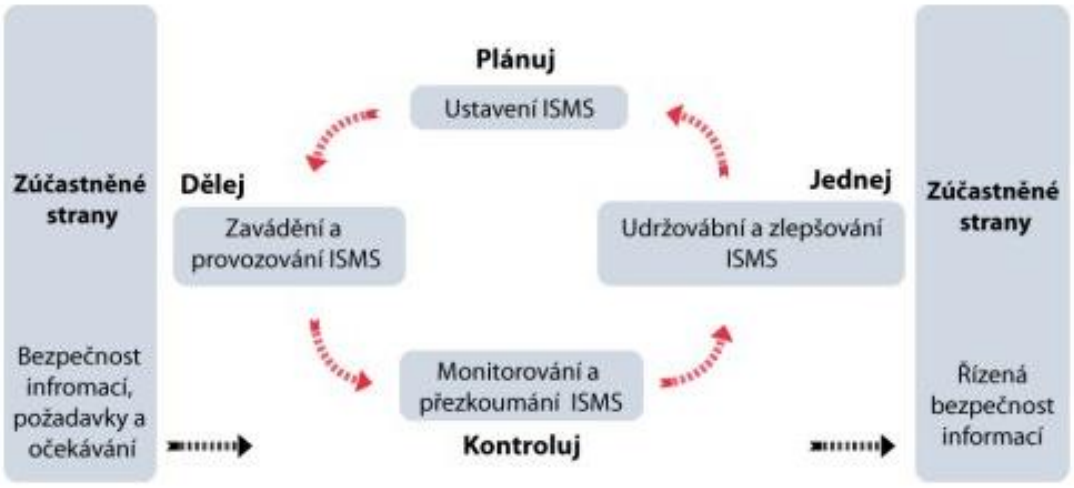


Obr. 4: Struktura vybraných norem řady ISO/IEC 27000 [9]

ČSN ISO/IEC 27001:2014

Další z mezinárodních norem si klade za cíl poskytnout doporučení, jak aplikovat normu ISO/IEC 27002 v rámci procesu budování, implementace, provozu, monitorování, přezkoumání, udržování, neustálého zlepšování a případné certifikace systému řízení bezpečnosti informací v organizaci. V normě jsou specifikovány požadavky na výběr a zavedení bezpečnostních opatření chránících informační aktiva. Norma aplikuje strukturu vyšší úrovně, totožné názvy článků i text, společné termíny a hlavní termíny, čímž zajišťuje kompatibilitu s ostatními normami systémů řízení dle přílohy SL v části 1 Směrnic ISO/IEC. [10]

V normě je prosazován procesní přístup k řešení ISMS, který využívá Demingova modelu PDCA (Plan-Do-Check-Act). Tento cyklus může být aplikován na veškeré procesy ISMS tak, jak jsou definovány touto normou. [2]



Obr. 5: PDCA model v kontextu ISMS [11]

ČSN ISO/IEC 27002:2014

Aktualizované vydání mezinárodní normy ISO/IEC 27002:2006 je sbírkou nejlepších bezpečnostních praktik rozdělených do 14 hlavních oddílů, které definují 35 cílů kontrolních opatření pro ochranu informačních aktiv proti narušení jejich důvěrnosti, integrity a dostupnosti. K naplnění identifikovaných cílů obsahuje norma 114 základních opatření. Většina z nich je obecně použitelná v různých organizacích bez ohledu na jejich typ, velikost či povahu činnosti. [4]

ČSN ISO/IEC 27003:2010

Norma ČSN ISO/IEC 27003 z roku 2010 obsahuje především návod na implementaci ostatních norem řady ISO/IEC 27000. Mohou ji využít všechny organizace, které mají v úmyslu zavést ISMS dle ČSN ISO/IEC 27001:2014. Tato norma uvádí popis procesu plánování implementace ISMS v následujících pěti etapách:

- získání souhlasu managementu společnosti se zahájením projektu ISMS;
- definování rozsahu, hranic a politiky ISMS;
- provedení analýzy požadavků bezpečnosti informací;
- hodnocení rizik a plánování jejich zvládání;
- návrh systému řízení bezpečnosti informací. [2]

ČSN ISO/IEC 27004:2016

Tato norma je pro organizace pomůckou, jak měřit a prezentovat účinnost jimi nastaveného systému řízení bezpečnosti informací. Implementace opatření uvedených v ISO/IEC 27001 je předmětem programu měření bezpečnosti informací. Tento program zahrnuje procesy rozvoje metrik a měření, provádění měření, analýzu dat a hlášení výsledků měření, dále pak proces vyhodnocení a neustálého zlepšování programu měření bezpečnosti informací. [2]

ČSN ISO/IEC 27005:2013

Základ této normy tvoří revize dříve vydaných norem ISO/IEC TR 13335-3:1998, ISO/IEC TR 13335-4:2000 a využití některých pasáží BS 7799-3. Tato mezinárodní norma obsahuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace. Mezi aktivity řízení rizik v této normě patří:

- stanovení kontextu – vymezení základních kritérií, definice rozsahu a stanovení organizační struktury pro řízení rizik;
- hodnocení rizik – identifikace rizik a jejich kvantifikace nebo kvalitativní popis;
- zvládání rizik – výběr opatření k redukci, podstoupení, vyvarování se či přenosu rizik;
- akceptace rizik – záznam rozhodnutí o akceptaci rizika a odpovědnosti za tato rozhodnutí;
- seznámení se s riziky – sdílení informací o rizicích;
- monitorování a přezkoumání rizik – kontrola identifikovaných rizik v čase. [12]

ČSN ISO/IEC 27006:2015

Další z mezinárodních norem řady ISO/IEC 27000 specifikuje požadavky a doporučení pro orgány provádějící audit a certifikaci ISMS a doplňuje požadavky obsažené v ČSN ISO/IEC 17021:2016 a ČSN ISO/IEC 27001:2014. Tato norma je především určená k podpoře procesu akreditace certifikačních orgánů poskytujících certifikace systému řízení bezpečnosti informací. [2]

1.3 Budování bezpečnostního povědomí (SAE)

Nacházíme se v 21. století, které se nese v duchu překotného vývoje výpočetní techniky a informačních technologií. Často se setkáváme s pojmem čtvrtá průmyslová revoluce (tzv. Průmysl 4.0), což je označení pro současný trend digitalizace, automatizace a robotizace výroby. V souvislosti s rozvojem informačních technologií se také začíná objevovat termín „Internet of Things“ (IoT), čili Internet věcí, který se vykládá jako propojení vestavěných zařízení s internetem. Prakticky se jedná o trend, kdy člověk bude moci (a mnohdy již může) vzdáleně ovládat např. svá domácí zařízení jako ledničku, pračku či topení prostřednictvím aplikace, kterou má nainstalovanou ve svém chytrém telefonu. Jedinec tak může spravovat svá zařízení vzdáleně pomocí bezdrátového připojení. Takový průlom v technologiích a využívání bezdrátového připojení s sebou nese mnoho výhod. Ovšem jako každá mince má dvě strany i v tomto případě je třeba brát v úvahu stinnou povahu nového řešení.

Útokům prostřednictvím světové sítě Internet čelí dnes a denně každý její uživatel. Zneužity bývají nejen osobní údaje, ale také např. data o bankovních účtech a transakcích, e-mailová korespondence, hesla, firemní data podnikajících subjektů, údaje ze smluv i fotografie ze sociálních sítí. To vše a mnohdy i více může být využito k nekalým účelům. Internet věcí rozšiřuje oblast ohroženou potenciálními riziky o další skupinu zařízení, která mohou být zneužita, a proto je třeba je chránit a zabezpečovat.

Samotnou ochranou před útoky a hrozbami mám na mysli nejen bezpečnost z pohledu jednotlivých vrstev ISO/OSI modelu, ale i po stránce osobní (uživatelské). Potřeba ochránit lidský faktor je tématem stejně důležitým jako ochrana všech údajů o člověku samotném.

Budováním bezpečnostního povědomí bychom měli začít již u dětí, které se začínají stále častěji v nižším věku dostávat k hraní her na tzv. smartphonech[1] či tabletech s přístupem k internetu. Mezi vysoce ohroženou skupinu patří žáci a studenti, kteří se často konfrontují s obsahem sociálních sítí a různých blogů či videí. Mobilní telefony jim mnohdy neslouží jen ke komunikaci s rodiči a přáteli. Využívají je i jako prostředek k sebeprezentaci, pořízení fotografií a sdělování informací o sobě vůči celému světu

[1] Smartphone – čili chytrý telefon, je mobilní telefon, který využívá mobilní operační systém (např. Android, iOS, Windows Phone atd.) a aplikační rozhraní, jež umožní instalaci nebo úpravy programů.

prostřednictvím internetu. Dalšími skupinami, u nichž je třeba budovat bezpečnostní povědomí, jsou lidé v produktivním věku, senioři i osoby ohrožené sociálním vyloučením. Vzhledem k tématu této práce bude pozornost zaměřena na tři cílové skupiny, a to žáky, pedagogy a vedení střední školy.

1.3.1 Návaznost, cíl a účel SAE

Budování povědomí o potřebě bezpečnosti informací patří, jak je uvedeno v subkapitole 1.2.1 Principy a cíl ISMS, mezi jeden ze základních principů systému řízení bezpečnosti informací. Investovat se proto vyplatí jak do technického vybavení a bezpečnostních opatření, tak i do lidských zdrojů coby správců informací v informačních systémech a především uživatelů veřejné celosvětové sítě Internet.

V České republice neexistuje dokument (ať už norma, směrnice, zákon či metodika), který by se komplexně věnoval tématu budování bezpečnostního povědomí a zároveň by byl brán jako závazný a jediný platný. Otisk této problematiky najdeme v normách řady ČSN ISO/IEC 27000 blíže rozpracovaných v předchozích částech této práce. Jako další počin na cestě k zajištění a budování bezpečnosti informací v kybernetickém prostoru lze chápat schválení zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů. Této problematice se věnuji v subkapitole 1.2.3 Kybernetická bezpečnost [6]. Tím však oficiální snahy o jednotné a komplexní pojetí budování bezpečnostního povědomí v tuto chvíli v naší zemi končí.

Inspirovat se zástupci České republiky mohou v zahraničí. Ovšem ani tam nenajdou bohatou odbornou literaturu. Přesto se určité pokusy o sjednocení pojetí ochrany dat v Evropě objevují. Přesněji řečeno ve státech Evropské unie (EU) vejde v květnu příštího roku v platnost tzv. Obecné nařízení na ochranu osobních údajů (General Data Protection Regulation, angl. zkratka GDPR). Toto nařízení se dotkne každého, kdo shromažďuje nebo i jen zpracovává osobní údaje o občanech EU. Míří na firmy, instituce i jednotlivce (např. zaměstnance, zákazníky či klienty), zkrátka na všechny fyzické i právnické osoby, které zacházejí s osobními údaji nebo i jen sledují a analyzují chování uživatelů na webu. GDPR je dosud nejucelenějším souborem pravidel na ochranu dat na světě. [13]

Ve Spojených státech amerických (angl. zkratka USA) existuje od roku 1901 při Ministerstvu obchodu USA národní fyzikální laboratoř s oficiálním názvem Národní institut standardů a technologie (National Institute of Standards and Technology, angl. zkratka NIST). Svým zaměřením, vytvářenými standardy i službami se tato instituce s téměř pěti tisíci odborníky dotýká oblastí jako nanotechnologie, elektronická zařízení používaná speciálně ve zdravotnictví, informační technologie, chemie, forenzní vědy a mnoho dalších od zařízení o tak miniaturní velikosti, že by se jich i desítky tisíc vešly na koneček lidského vlastu, až po mrakodrapy odolné vůči zemětřesením a globální komunikační sítě. Mezi stěžejní témata, která zástupci NIST již nějakou dobu řeší, patří také budování bezpečnostního povědomí. [14]

V říjnu roku 2003 vydal Národní institut standardů a technologie speciální publikaci pod označením NIST Special Publication 800-50 věnující se tématu vybudování programu pro zvyšování bezpečnostního povědomí a školení o informačních technologiích (oficiální název „Building an Information Technology Security Awareness and Training Program“). Tato norma poskytuje návod na vybudování účinného bezpečnostního programu v oblasti informačních technologií. V USA navíc tato publikace podporuje požadavky uvedené ve federálním zákoně o řízení bezpečnosti informací. Byť odlišnými slovy a v jiném jazyce je zde ovšem hned v úvodu obsahově totožné vyjádření, které jsem uvedla v textu této práce o několik odstavců výše, a to, že realizovat v organizaci program na zajištění ochrany dat je věc důležitá, avšak bez toho, aniž by byla věnována pozornost zpracovatelům a uživatelům těchto dat, nebude navržené řešení kompaktní. Technické zabezpečení je částí „jing“ a školení uživatelů o bezpečném přístupu a zacházení s daty částí „jang“. Spolu dohromady vytváří ideální kombinaci. [15]

Publikace NIST SP 800-50 se vzájemně doplňuje s další normou taktéž vydanou Národním institutem standardů a technologie, a to NIST SP 800-16 se zaměřením na požadavky kladenými na školení v informačních technologií v rámci modelu založeného na rolích a výkonnosti (oficiální název: Information Technology Security Training Requirements: A Role-and Performance-Based Model). Zatímco NIST SP 800-50 se zaměřuje na strategickou úroveň budování bezpečnostního povědomí z pohledu organizace jako celku, NIST SP 800-16 jde do větší míry detailu a poskytuje jakýsi návod na přípravu vzdělávacích kurzů zacílených na budování bezpečnostního

povědomí. [16] Vybrané pasáže by se daly do určité míry a s drobnými obměnami aplikovat také v prostředí českých společností a institucí.

Cíl budování bezpečnostního povědomí (Security Awareness Education, angl. zkratka SAE) tkví v představě, že organizace nemohou chránit důvěrnost, integritu a dostupnost informací v dnešním světě moderních informačních technologií zapojených do sítě, aniž by zajistily, že všichni lidé, podílející se na používání těchto technologií a jejich řízení:

- porozumí své roli a budou si vědomi své zodpovědnosti vůči organizaci a okolí;
- pochopí bezpečnostní zásady a postupy organizace v oblasti řízení a správy informačních technologií a informačních systémů;
- budou mít alespoň základní znalosti o řídicích, provozních a technických mechanismech používaných k zajištění ochrany informačních zdrojů, za které odpovídají a se kterými pracují. [15]

Při pokusech o zabezpečení sítě bylo prokázáno a v mnoha auditorských zprávách, odborných periodikách i na konferencích doloženo, že jedním z nejslabších míst v zabezpečení dat jsou právě lidé. Lidský faktor, nikoliv technologie, je klíčovým článkem k zajištění přiměřené úrovně bezpečnosti dat. Pokud si tato dvě vyjádření dáme dohromady, a sice že jsou lidé hlavním faktorem úspěchu a zároveň jeho nejslabším místem, vyplývá nám to podstatné. Tomuto aktivu musí být věnována větší pozornost. Propracovaný systém budování bezpečnostního povědomí má pro pochopení odpovědnosti lidí v oblasti bezpečnosti dat a jejich role v rámci nastaveného systému v organizaci zásadní význam. Důležité je před umožněním přístupu do systému zajistit, aby byli všichni jednotlivci v rámci organizace náležitě vyškoleni, informovat je o dostupných technických a bezpečnostních produktech, technikách a mechanismech. Školení cílových skupin (vzhledem k problematice této práce mezi ně patří: žáci, pedagogové a vedení střední školy) by obecně mělo zahrnovat:

- rizika informační bezpečnosti spojená s jejich činností a
- odpovědnost za dodržování nastavených pravidel v rámci bezpečnostní politiky vedoucích ke snížení míry identifikovaných rizik, příp. jejich dopadu. [15]

Chce-li společnost dosáhnout přiměřené úrovně bezpečnosti svého systému, musí počítat s investicemi. Nejedná se však pouze o investice z pohledu času, prostoru či

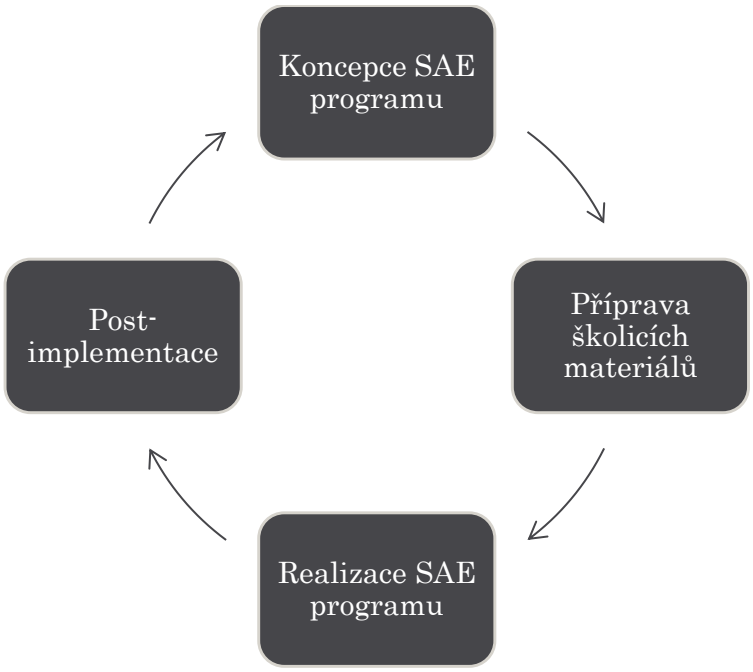
osob, nýbrž také o finanční prostředky, které musí být na aktivity spojené s budováním bezpečnostního povědomí a zabezpečení informačních systémů vyčleněny v rozpočtu organizace a skutečně vynaloženy. Deklarované prohlášení o záměru investic je třeba podložit reálně provedenými kroky. Jak je již uvedeno v této práci v subkapitole 1.2.1, celkové finanční investice musí odpovídat hodnotě aktiv a míře možných rizik.

1.3.2 Fáze životního cyklu SAE

Stejně jako je celý systém řízení bezpečnosti informací založen na principu neustálého zlepšování sebe sama za pomoci Demingova cyklu PDCA, i proces budování bezpečnostního povědomí sestává z několika fází. Faktorem úspěchu implementace procesu SAE je postupovat v jednotlivých krocích od počátku ke konci. Přeskočením určité fáze by se organizace mohla dostat do nesnází, dosažení požadovaného cíle by bylo ohroženo a vynaložené úsilí by se minulo účinkem.

Jsou identifikovány tyto čtyři základní kritické fáze budování bezpečnostního povědomí:

- **stanovení koncepce SAE programu** – v tomto kroku se odehrává identifikace a hodnocení cílů a potřeb organizace v oblasti budování bezpečnostního povědomí, je vypracována strategie a akční plán implementace, který stanoví jednotlivá opatření a kroky k naplnění strategie;
- **příprava podkladů a školicích materiálů** – v této fázi je potřeba provést monitoring dostupných materiálů (zda je možné se při tvorbě vhodného programu inspirovat), stanovit role a odpovědnosti a zhotovit školicí materiály;
- **realizace SAE programu** – tento krok řeší efektivní komunikaci a zavádění programu budování bezpečnostního povědomí pomocí tréninku, školení či jiných vhodně zvolených aktivit;
- **post-implementace** – tato fáze je zaměřena na získání zpětné vazby a evaluaci SAE programu a jeho účinnosti, navržení a implementaci opatření vedoucích k zajištění aktuálnosti nastaveného systému. [15]

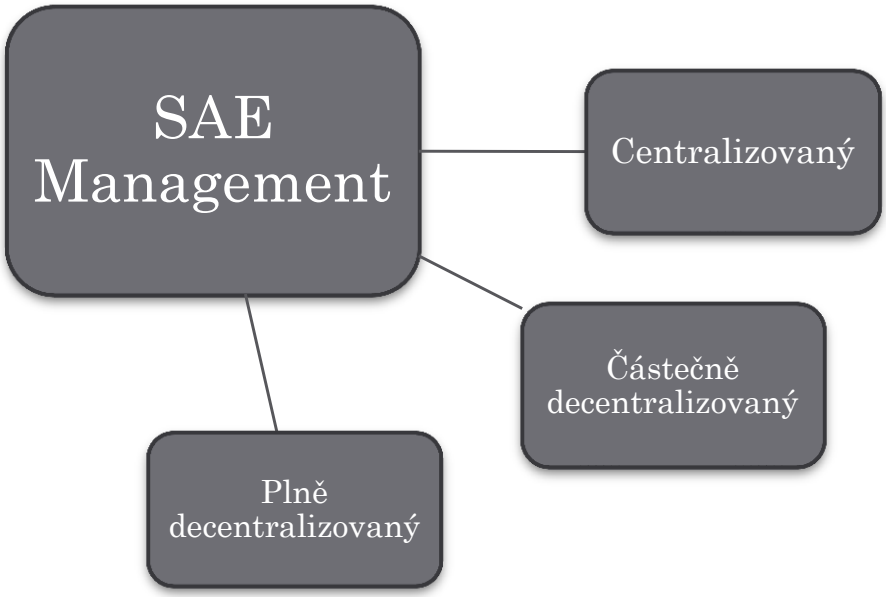


Obr. 6: Fáze životního cyklu SAE programu [Zdroj: Vlastní zpracování]

1.3.3 Přístupy k budování bezpečnostního povědomí

Na základě zkušeností s řízením bezpečnosti informací a budováním bezpečnostního povědomí jsou v praxi uplatňovány tyto tři modely:

- **centralizovaný** – veškerá odpovědnost za správu a řízení SAE spočívá na pověřené osobě (v podnikajících subjektech to bývá Chief Information Officer (CIO), příp. Chief Information Security Officer (CISO), v mnohých státních institucích se hovoří o správci IT);
- **částečně decentralizovaný** – za přípravu, dodržování a naplňování bezpečnostní politiky a strategie školení zodpovídá pověřená osoba, vlastní řešení a implementace jsou distribuovány;
- **plně decentralizovaný** – pouze vývoj a tvorba bezpečnostní politiky je svěřena zodpovědné osobě, zbylé aktivity jsou delegovány na jednotlivé složky organizace. [15]



Obr. 7: Přístupy k řízení SAE [Zdroj: Vlastní zpracování]

1.4 Certifikace informační bezpečnosti (ISACA)

Každá organizace, chce-li na své zákazníky, dodavatele, odběratele a další zainteresované strany působit spolehlivě a důvěryhodně, má možnost se nechat v různých oblastech certifikovat. Přísná kritéria hodnocení zaručují exkluzivitu společností, které mohou ocenění získat a potvrdit tím svou silnou pozici na trhu. Zároveň je pro mnohé společnosti získané osvědčení vstupní branou ke spolupráci s mezinárodními organizacemi, u kterých je důvěryhodnost klíčovým faktorem spolupráce.

Certifikace typu ČSN EN ISO 9001:2016 Systémy managementu jakosti, ČSN EN ISO 14001:2016 Systémy environmentálního managementu, ČSN EN ISO 50001:2012 Systémy managementu hospodaření s energií a další se zdály být zpočátku jakýmsi „módním trendem“. Nyní však ukazují zcela jasnou cestu všem společnostem, které chtějí obstát ve stále se zvyšující konkurenci tržního prostředí. [17]

Kromě v této práci zmíněné certifikace organizace dle normy ČSN ISO/IEC 27001:2014 Systémy řízení bezpečnosti informací existuje profesní asociace ISACA (Information Systems Audit and Control Association), která vydává osvědčení

dokládající odbornou způsobilost v oblasti informační bezpečnosti konkrétním fyzickým osobám (nikoliv společnostem). Tato organizace sdružující IT profesionály již od roku 1967 se zaměřuje na oblast řízení, kontroly, auditu a bezpečnosti informačních systémů. V České republice působí od roku 1997 lokální pobočka ISACA Czech Republic Chapter, která v současné době sdružuje na 300 odborníků z různých podnikatelských oblastí a státní správy. *„Z důvodu velkého nárůstu informačních technologií v posledním desetiletí a kritického zvýšení jejich vlivu na úspěch v podnikání vznikl ve spolupráci s ISACA v roce 1998 IT Governance Institute. Posláním institutu je pomáhat manažerům nalézat rovnováhu mezi řízením IT a řízením podnikatelských cílů. Prostřednictvím výzkumů, pořádáním vzdělávacích seminářů a konferencí, publikací odborné literatury a poskytováním elektronických zdrojů a nástrojů pomáhá manažerům lépe chápat a efektivně řídit společnosti s využitím informačních technologií.“* [18]

Organizace ISACA v současné době nabízí odborníkům na bezpečnost informací čtyři celosvětově uznávané certifikace. Jde o následující zaměření:

- **CISA** (Certified Information Systems Auditor) – standard vhodný pro experty, kteří se zaměřují na audit, řízení, kontrolu, monitoring a vyhodnocení bezpečnosti informačních technologií a podnikových informačních systémů. Uchazeč v průběhu zkoušky prokazuje své auditorské znalosti, dovednosti a zkušenosti, schopnost posoudit zranitelnost informačního systému a provést kontrolu v rámci dané organizace.
- **CISM** (Certified Information Security Manager) – certifikát určený manažerům informační bezpečnosti i osobám, které za řízení bezpečnosti informací nesou ve společnosti odpovědnost. CISM certifikace je zaměřena na ověření znalostí a dovedností z oblasti řízení, postupů a procesů, správy, kontroly a vyhodnocení podnikové informační bezpečnosti.
- **CGEIT** (Certified in the Governance of Enterprise IT) – odborník s tímto certifikátem splnil požadavky na znalosti a dovednosti z oblasti řízení a správy podnikových informačních technologií a umí rychle a pružně reagovat na změny.

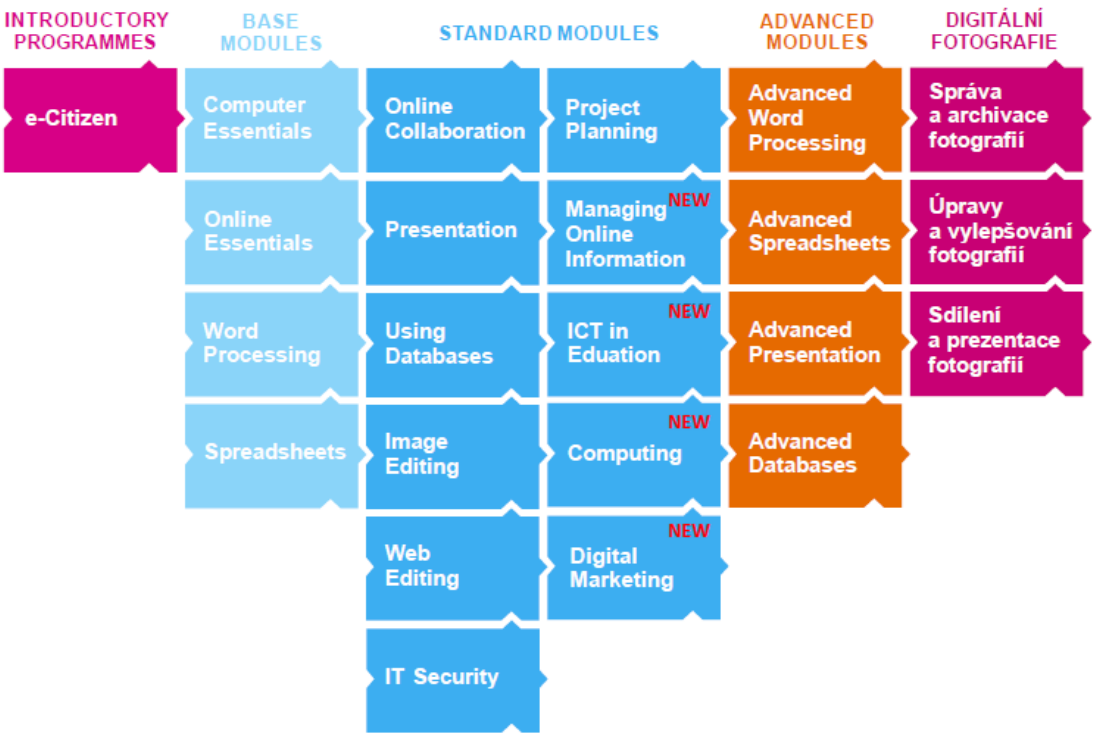
- **CRISC** (Certified in Risk and Information Systems Control) – standard dokládající jeho vlastníkovi zkušenosti s řízením rizik v oblasti IT a informačních systémů. Detailně se jedná o prokázání odborných znalostí a dovedností s procesem identifikace, hodnocením, optimalizací a monitorováním rizik IT a nastavením vhodných opatření. [19]

Zkoušku z uvedených oblastí certifikace lze absolvovat ve 220 městech po celém světě včetně Prahy. Česká republika aktuálně eviduje 195 certifikovaných profesionálů. [18]

1.5 Mezinárodní standard ECDL

Další z celosvětově uznávaných vzdělávacích konceptů týkající se oblasti počítačové neboli digitální gramotnosti je Mezinárodní standard pro digitální znalosti a dovednosti (European Computer Driving Licence, angl. zkratka ECDL). Také v tomto případě se certifikace dotýká fyzických osob a ověření jejich digitálních znalostí a dovedností.

„Mezinárodní koncept ECDL je vzdělávací a certifikační systém zaměřený především na ***přenositelné digitální kompetence*** *běžných uživatelů digitálních technologií. Jednotlivé tematické oblasti, které koncept ECDL pokrývá, jsou nazývány moduly. Pro každý modul existuje volně dostupný ECDL sylabus, který zcela konkrétně specifikuje vzdělávací obsah. Koncept ECDL umožňuje kombinovat jednotlivé moduly.“* [20]



Obr. 8: Moduly ECDL dostupné v České republice [20]

Nový modul „**Managing Online Information**“ byl oficiálně představen v České republice jako v první zemi na celém světě v dubnu letošního roku. Tento standard se snaží o vymezení základních dovedností z oblasti digitálního a bezpečnostního povědomí. Po absolvování výcvikového programu bude účastník schopen:

- porozumět informacím na internetu;
- seznámit se se zdroji informací, způsoby jejich vyhledávání při zachování principu bezpečnosti a rozpoznání důvěryhodnosti zdroje;
- správně definovat dotazy vedoucí k nalezení požadovaných informací;
- vyhodnotit získané informace, umět je třídit a uspořádat;
- vytvořit nový obsah na základě nalezených informací;
- strukturovaně získané informace předávat při dodržení etických i zákonných norem. [20]

Základ tohoto modulu by mohl být součástí fáze realizace školení v rámci programu budování bezpečnostního povědomí. Svým obsahovým zaměřením je využitelný pro širokou škálu potenciálních cílových skupin, jako např. žáci i pedagogové střední školy.

2 Analýza současného stavu

Není pochyb o tom, že v souvislosti s neustálým a až překotným technologickým vývojem budou některé pracovní pozice zanikat, příp. se radikálně měnit a nové pracovní příležitosti vznikat. Přesto většina firem navzdory automatizaci a robotizaci svých provozů dle průzkumu společnosti ManpowerGroup očekává spíše nárůst počtu zaměstnanců (až o 7 %). Nejvíce nových pracovních míst lze očekávat v oblasti informačních technologií (o 26 %), řízení lidských zdrojů (o 20 %) a v oblasti obchodu a péče o zákazníky (o 15 %). „*Až 65 % pracovních pozic, které bude generace Z*[2] *vykonávat, dosud ani neexistují*.“ Faktorem úspěchu této skupiny lidí bude schopnost přizpůsobit své dovednosti, flexibilita a učenlivost. [21]

Je potřeba nejen připravovat současné žáky na výkon jejich budoucích povolání, ale informovat je také o rizicích a hrozbách, která s sebou moderní informační technologie, v budoucnu používané také k pracovním účelům, a přístup k internetu přinášejí. Budovat bezpečnostní povědomí bychom měli začít postupně už od dětí předškolního věku, žáků na základních školách a až po žáky na středních i vysokých školách. Aby byl takový program účinný a odpovídal aktuálním požadavkům, je zapotřebí počítat také s vyškolením pedagogů i vedení příslušné organizace. S ohledem na téma této diplomové práce bude program budování bezpečnostního povědomí aplikován na žáky střední školy, jejich vyučující a management instituce.

2.1 Představení organizace

Pro účely této diplomové práce se mi podařilo navázat na dosavadní úspěšnou spolupráci se zástupci střední školy, jejíž zástupci si z důvodu možného zneužití informací nepřejí uvádět úplný název instituce. Pro účely této diplomové práce bude použit zkrácený název „střední škola“. Zástupci managementu střední školy se proaktivně snaží přizpůsobit výuku identifikovaným potřebám, a to jak na trhu práce, tak i z pohledu společenské odpovědnosti. Program budování bezpečnostního povědomí je současně vzhledem k zaměření střední školy oborově blízký.

[2] Generace Z (neboli internetová generace) – je společný název pro skupinu osob narozených ve druhé polovině 90. let minulého století až do současnosti; moderní technologie (počítače, tablety, chytré telefony, internet, sociální sítě, online nástroje pro komunikaci) používají odjakživa.

Historie střední školy sahá do 50. let 20. století, kdy 1. září 1949 zahájilo svoji činnost nové technické učiliště se zaměřením na telekomunikace. Po stěhování z nevyhovujících prostor se v 60. letech podle školského zákona z té doby řadí mezi školy II. stupně, poskytující střední vzdělání. O 20 let později se pro školu začínají budovat zcela nové a moderní objekty, jejichž součástí je i domov mládeže. Ve školním roce 1993/1994 v nich střední škola zahajuje svoji výuku. Rozšířením o obory střední odborné školy došlo od 1. září 1997 ke změně názvu střední školy. Instituce v té době zajišťovala komplexní teoretickou i praktickou přípravu na povolání z oblasti telekomunikací, pošt a nově také bankovnictví a techniky administrativy. O rok později, v roce 1998, byla struktura oborů rozšířena o sdělovací a zabezpečovací techniku v dopravě.

Teoretická výuka, odborný výcvik i praktické vyučování probíhá v učebnách vybavených moderní didaktickou a výpočetní technikou a nejmodernějšími technologiemi. Žákům je k dispozici moderní domov mládeže s klubovnami, tělocvičny, venkovní sportovní areál s umělým povrchem. Vzdělávání žáků zajišťují kvalifikovaní pedagogové.

Škola vedle své primární činnosti vyvíjí v rámci svých kapacit další aktivity, např. vzdělávání dospělých, poskytování ubytovacích a stravovacích služeb, organizaci sportovních a kulturních akcí. Střední škola dále umožňuje svým žákům získat mezinárodně platné certifikáty z oblasti informačních a komunikačních technologií (ICT), zapojuje se do mnoha vzdělávacích aktivit včetně projektů financovaných z Evropských strukturálních fondů (ESF). Součástí střední školy se stala také lokální síťová akademie CISCO. Od roku 2012 vystupuje střední škola pod novým názvem. Mnohé průkopnické aktivity, navázaná spojení se zaměstnavateli, získané certifikáty pro školu, realizace projektů a spolupráce s dalšími institucemi jsou spojeny s manažerským potenciálem a neutuchajícím entuziasmem ředitele této střední školy. [22]

Střední škola nabízí svým žákům vzdělání na úrovni **středního vzdělání s výučním listem** v následujících oborech:

- 26-52-H/01 elektromechanik pro zařízení a přístroje
- 26-59-H/01 spojový mechanik

- 37-51-H/01 manipulant poštovního provozu a přepravy

Dále tato škola nabízí svým žákům vzdělání na úrovni **středního vzdělání s maturitní zkouškou** v těchto oborech:

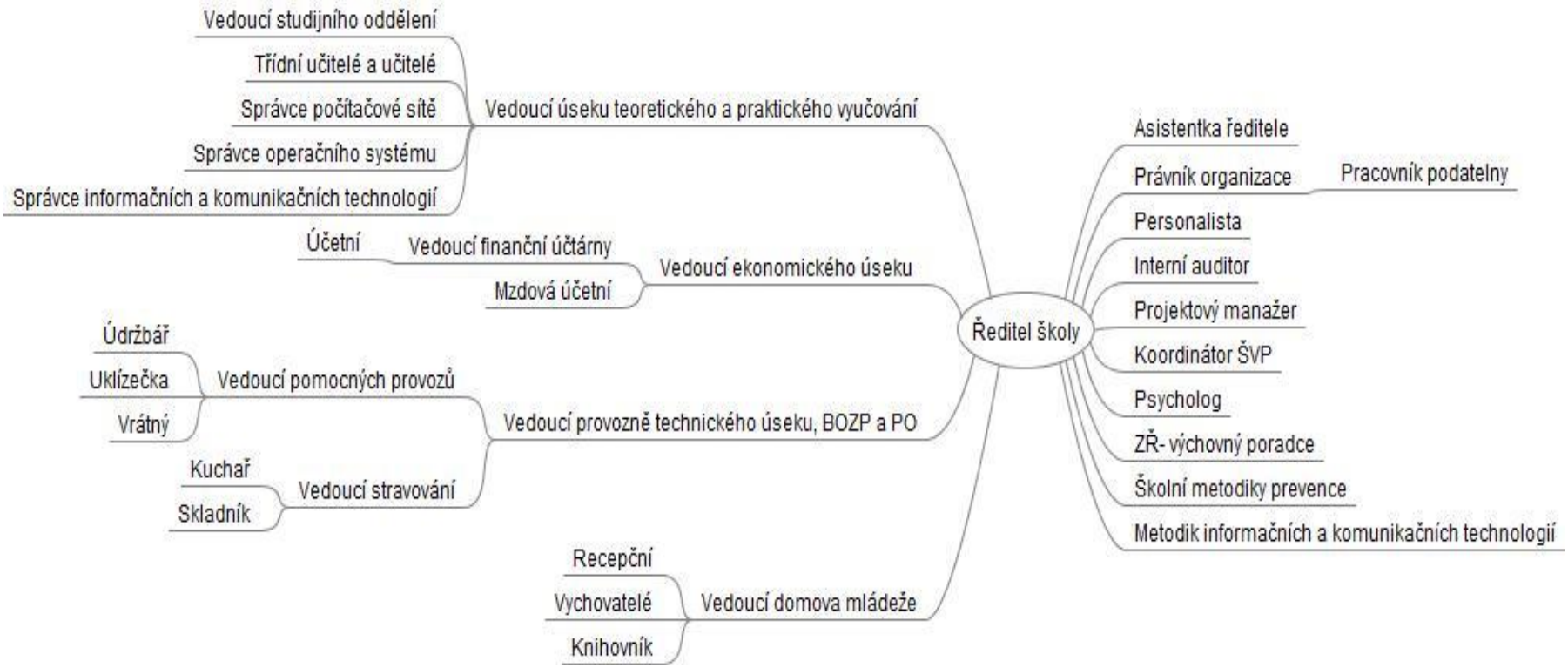
- 18-20-M/01 informační technologie
- 26-41-L/01 mechanik elektrotechnik
- 26-41-L/51 mechanik elektrotechnik
- 26-41-M/01 elektrotechnika
- 26-45-M/01 telekomunikace
- 37-42-L/51 logistické a finanční služby
- 37-42-M/01 logistické a finanční služby
- 63-41-M/01 ekonomika a podnikání [23]

Nově se ve školním roce 2017/2018 otevře obor **kybernetická bezpečnost.** Na výuce se budou přímo podílet odborníci z praxe a budoucí potenciální zaměstnavatelé v oblasti kybernetické bezpečnosti (např. Cisco, NSM Cluster, KYBEZ, Národní centrum kybernetické bezpečnosti v Brně, AFCEA a další). Absolventi tohoto oboru najdou uplatnění při zavádění a řízení kybernetické bezpečnosti v organizaci, na pozici bezpečnostního technika informačních technologií, technika datového centra, technika datových analýz a programátora specifických algoritmů, pracovníka uživatelské podpory, správce aplikací, operačních systémů a sítí. [24]

2.2 Organizační struktura školy

Střední škola byla zřízena 1. dubna 2001 jako příspěvková organizace. Ředitel školy je statutárním orgánem střední školy a za její chod nese plnou zodpovědnost. Organizační strukturu určuje organizační řád a organizační schéma. V organizaci se na nachází tyto řídící stupně: ředitel školy a vedoucí jednotlivých úseků (viz plné schéma na obrázku níže).

Řediteli školy přímo podléhá vedoucí úseku teoretického a praktického vyučování, vedoucí ekonomického úseku, vedoucí provozně technického úseku, vedoucí domova mládeže a administrativní aparát střední školy.



Obr. 9: Možné plné schéma střední školy [Zdroj: Vlastní zpracování]

2.3 Aktuální projekty a postoj k budování bezpečnostního povědomí

Zástupci vedení střední školy si uvědomují důležitost tématu budování bezpečnostního povědomí a informační a kybernetické bezpečnosti. Aby mohli svým žákům i zaměstnancům zprostředkovat co nejaktuálnější informace a trendy z těchto oblastí, spolupracují se zaměstnavateli, kteří se kybernetickou bezpečnosti a vzděláváním v této oblasti zabývají, zapojují se do profesních sdružení a účastní se odborných konferencí.

2.3.1 Network Security Monitoring Cluster

Jedním takovým odvětvovým uskupením zaměřeným na oblast bezpečnosti počítačových sítí a bezpečnosti v informačních a komunikačních technologiích je **Network Security Monitoring Cluster** (dále NSM Cluster). Klastr sdružuje 21 členů a další partnery a jeho součástí je i střední škola. Momentálně klastr působí na regionální úrovni v Jihomoravském kraji. Do budoucna má však ambici díky možnosti vstupu dalších členů stát se nadregionálním uskupením s působností na celém území České republiky.

Mezi prioritní aktivity tohoto klastru mimo jiné patří:

- osvěta týkající se bezpečnosti počítačových sítí a informací;
- sdílení informací o aktuálních trendech v oblasti bezpečnosti počítačových sítí;
- návrhy úpravy právních norem v oblasti bezpečnosti ICT infrastruktury a jejího zabezpečení;
- komunikace s organizacemi a asociacemi zabývající se bezpečností počítačových sítí. [25]

Management střední školy přistoupil k podpisu memoranda o spolupráci v rámci technologické platformy, kde se bude účastnit diskusí nad podmínkami pro naplňování vzdělávání.

2.3.2 Platforma kybernetické bezpečnosti (KYBEZ)

Další platformou řešící efektivní spolupráci akademických institucí a komerčních firem zabývajících se osvětou, systematickým vzděláváním, managementem, službami

a technologiemi v oblasti bezpečnosti informací, a to včetně kybernetické bezpečnosti a obrany je KYBEZ. Partneři projektu KYBEZ jsou připraveni pomoci organizacím veřejné správy i podnikajícím subjektům ve splnění požadavků, které na ně zákon o kybernetické bezpečnosti klade.

Všech 36 členů této platformy se dohromady ať už větším či menším poměrem podílí na následujících službách:

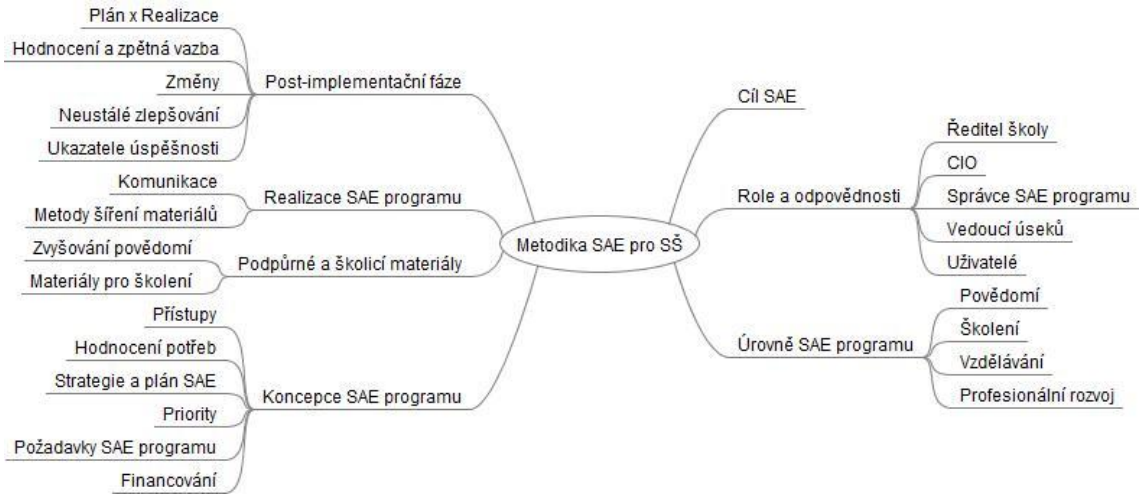
- analytické služby – základní a pokročilá analýza stavu bezpečnosti a ochrany osobních údajů;
- kurzy a školení – nabídka jednodenního kurzu s uvedením do problematiky informační bezpečnosti a kurzu Manažer informační bezpečnosti;
- audit – provedení nezávislé kontroly, zda bezpečnost informací v organizaci odpovídá platné legislativě a je v souladu s příslušnými normami;
- bezpečnostní služby – zpracování analýzy rizik IS, vypracování dokumentace, vnitřních předpisů a postupů pro řízení bezpečnosti, zavedení ISMS, nabídka penetračních testů IS pomocí „hackerských“ technik.

Tyto a mnoho dalších služeb z oblasti informační bezpečnosti nabízí platforma KYBEZ. Zástupce managementu střední školy se účastní setkání Rady pro vědu, výzkum a vzdělávání KYBEZ. [26]

3 Návrh metodiky budování bezpečnostního povědomí v prostředí střední školy

Praktickou část práce věnuji zpracování návrhu metodiky budování bezpečnostního povědomí v prostředí střední školy. Jednotlivé části vypracovaného návrhu jsou primárně určeny pro potřeby v předchozí kapitole uvedené střední školy. Metodika stanovuje cíl budování bezpečnostního povědomí, určuje role a odpovědnosti jednotlivých aktérů, rozpracovává všechny čtyři části programu SAE od koncepce, přes přípravu školicích materiálů a realizaci školení, až k post-implementační fázi, vyhodnocuje účinnost zpětné vazby a pokouší se i o celkovou kalkulaci nákladů.

Při přemýšlení nad problematikou budování bezpečnostního povědomí jsem si pro představu o rozsahu tématu vytvořila myšlenkovou mapu. Ta znázorňuje oblasti, na které by se při zpracování metodiky SAE pro střední školy nemělo zapomenout a které je potřeba detailněji rozepsat a okomentovat.



Obr. 10: Myšlenková mapa metodiky SAE pro střední školy [Zdroj: Vlastní zpracování]

3.1 Cíl SAE

Každá organizace musí ochránit svá aktiva. Z pohledu střední školy se jedná o prostředky, u kterých se předpokládá, že přináší užitek. Mezi základní a zároveň zásadní aktiva se řadí majetek (dlouhodobý i oběžný, materiální i finanční), lidské zdroje (zaměstnanci střední školy, žáci), know-how a bezesporu informace a informační

systémy. Správu, řízení a ochranu uvedených aktiv ovlivňují na různých úrovních zákony, normativní dokumenty, předpisy, zásady, pokyny či směrnice. Komplexní závazná dokumentace, která by pojímala a řešila oblast budování bezpečnostního povědomí, v České republice chybí. Oporu lze hledat v:

- normách řady ČSN ISO/IEC 27000;
- zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů;
- publikacích NIST SP 800-50 a NIST SP 800-16.

Globálním cílem SAE je ochrana dat a informací s ohledem na jejich důvěrnost, integritu a dostupnost. Toho může být dosaženo pouze za předpokladu, že všichni lidé, podílející se na tvorbě těchto informací a jejich zpracování či ukládání:

- porozumí své roli a budou si vědomi své zodpovědnosti vůči organizaci a okolí;
- pochopí bezpečnostní zásady a postupy organizace v oblasti řízení a správy informačních technologií a informačních systémů;
- budou mít alespoň základní znalosti o řídicích, provozních a technických mechanismech používaných k zajištění ochrany informačních zdrojů, za které odpovídají a se kterými pracují.

Důležité je před umožněním přístupu do systému zajistit, aby byly všechny cílové skupiny v rámci střední školy náležitě vyškoleny, informovat je o dostupných technických a bezpečnostních produktech, technikách a mechanismech. Školení klíčových lidských zdrojů (vzhledem k problematice této práce mezi ně patří: žáci, pedagogové a vedení střední školy) by obecně mělo zahrnovat:

- rizika informační bezpečnosti spojená s jejich činností a
- odpovědnost za dodržování nastavených pravidel v rámci bezpečnostní politiky vedoucích ke snížení míry identifikovaných rizik, příp. jejich dopadu.

3.2 Role a odpovědnosti

Definování rolí a stanovení odpovědností je jedním z témat bezpečnostní politiky organizace. Ta sice mimo jiná témata obsahuje povinnost provádět školení a rozvíjet

v rámci instituce povědomí o bezpečnosti informací, ovšem na druhou stranu je podstatné, aby organizace sama stanovila, kdo je za informovanost o bezpečnosti informačních technologií a příslušná školení zodpovědný. Jedním ze způsobů, jak zajistit, že bude SAE program funkční, je přiřadit zainteresovaným stranám jejich role a odpovědnosti a vše písemně zdokumentovat.

3.2.1 Ředitel školy

Ředitel školy musí zajistit, aby program budování bezpečnostního povědomí byl zpracován s vysokou mírou důležitosti a odrážel aktuální požadavky na bezpečnost informací v prostředí celé střední školy pro všechny zainteresované cílové skupiny. Ředitel školy je zodpovědný za:

- jmenování osoby odpovědné za přípravu a správu školení o bezpečnosti informací (běžně používaný termín Chief Information Officer[3], angl. zkratka CIO);
- přiřazení odpovědnosti za bezpečnost informačních technologií;
- dohled nad SAE programem v rámci střední školy;
- zajištění zdrojů (lidských, materiálních, informačních, finančních) potřebných k efektivnímu SAE programu;
- zajištění dostatečně vyškoleného personálu v ochraně informačních zdrojů a jejich bezpečnosti.

3.2.2 Osoba odpovědná za přípravu a správu školení o bezpečnosti informací

Pracovník v této roli (CIO) je zodpovědný za přípravu a správu školení o bezpečnosti informací. Zároveň dohlíží na pracovníky, jimž byla svěřena odpovědnost za bezpečnost informačních systémů. CIO spolupracuje se správcem SAE programu na:

- vytvoření celkové koncepce a strategie budování bezpečnostního povědomí;
- přípravě příslušných školení;

[3] Chief Information Officer (CIO) – je zvolený název pro tuto roli a podoba s názvem pracovní pozice používaná především v komerčních společnostech je čistě náhodná.

- zajištění, aby všechny relevantní cílové skupiny pochopily koncepci a strategii SAE programu a byly informovány o pokroku v jeho zavádění;
- zajištění financování programu budování bezpečnostního povědomí;
- zajištění školení a vyškolení relevantních cílových skupin;
- nastavení účinných mechanismů sledování a podávání zpráv o stavu SAE programu.

3.2.3 Správce SAE programu

Správce programu budování bezpečnostního povědomí zodpovídá za samotný program a příslušná školení z pohledu taktické úrovně. Spolupracuje s CIO na přípravě strategie SAE programu a jeho výkaznictví. Pracovník v této roli je zodpovědný za:

- zpracování potřebných podpůrných a školicích materiálů;
- efektivnost a vhodnost zvolených informačních kanálů, jejichž prostřednictvím jsou školicí materiály aplikovány;
- stanovení způsobu poskytnutí zpětné vazby od všech cílových skupin SAE programu;
- zajištění aktuálnosti a revize zpracovaných podpůrných a školicích materiálů.

3.2.4 Vedoucí úseků

Tito pracovníci jsou zodpovědní za dodržování požadavků na informovanost o bezpečnosti informací v rámci střední školy a školení určené pro jejich podřízené. Vedoucí úseků zodpovídá za následující aktivity:

- spolupráci s CIO a správcem SAE programu vzhledem k plnění nastavených povinností;
- splnění úlohy vlastníka systému, ev. vlastníka dat (pokud je to vhodné a žádoucí);
- zvážení vypracování individuálních rozvojových plánů pro konkrétní uživatele (je-li to třeba);
- podporu profesionálního rozvoje a certifikaci odpovědných pracovníků;

- zajištění, aby všichni uživatelé (včetně dodavatelů, je-li to vhodné) jejich systémů (hlavních i podpůrných aplikací) byli náležitě vyškoleni v plnění bezpečnostních opatření ještě před tím, než jim bude umožněn přístup;
- zajištění, aby všichni uživatelé (včetně dodavatelů, je-li to vhodné) porozuměli specifickým pravidlům každé části informačního systému, kterou používají;
- snižování chybovosti a opomenutí uživatelů v důsledku nedostatečné informovanosti nebo absence školení.

3.2.5 Uživatelé

Uživatelé představují nejpočetnější a zároveň jednu z nejdůležitějších cílových skupin, která může pomoci se snížením neúmyslných chyb a stupně zranitelnosti informačního systému organizace. Do této skupiny patří zaměstnanci střední školy, žáci, dodavatelé, návštěvníci, hosté školy a další spolupracovníci vyžadující přístup do systému. Uživatelé jsou zodpovědní za:

- pochopení a dodržování zvolených bezpečnostních zásad a postupů střední školy;
- řádné vyškolení v pravidlech svého chování v rámci aplikací a těch částí systému, do kterých mají přístup;
- spolupráci se školiteli;
- udržení aktuálnosti a platnosti bezpečnostních řešení (např. antivirových programů);
- porozumění jednotlivým krokům své činnosti v rámci systému a jejich dopadům a důsledkům.

Uživatelé musí být srozuměni se správným používáním hesla, zálohováním dat, vhodnou antivirovou ochranou, postupem hlášení jakýchkoliv podezřelých incidentů nebo porušení bezpečnostních zásad, dodržením pravidel nastavených k odvrácení potenciálních útoků a šíření spamů nebo virů.

3.3 Komponenty SAE programu

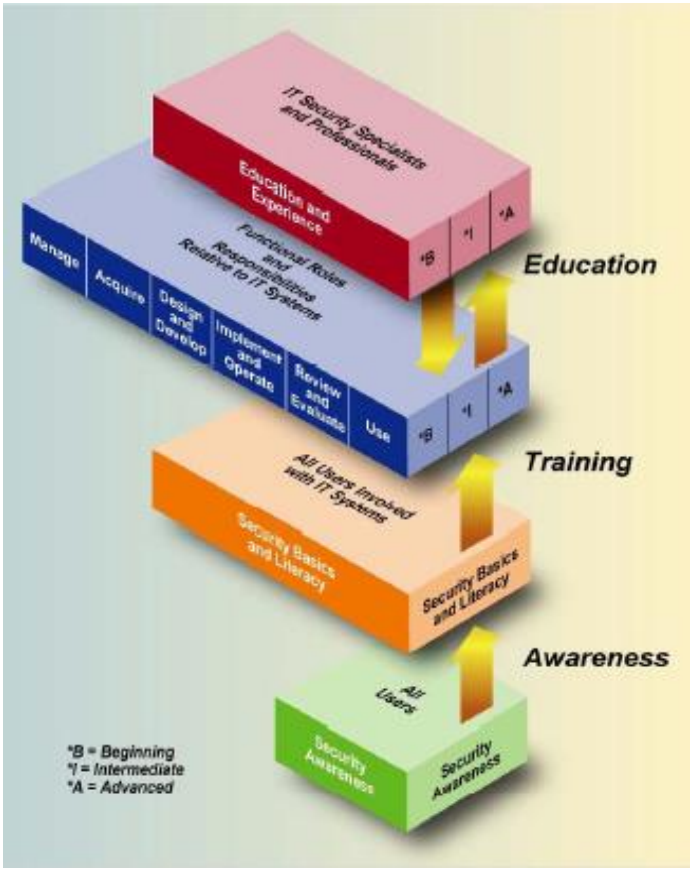
Úspěšný program budování bezpečnostního povědomí se skládá ze tří základních oblastí aktivit:

- rozvoje bezpečnostní politiky reflektující známá a potenciální rizika;
- informování všech uživatelů systému střední školy o jejich odpovědnostech v oblasti informační bezpečnosti tak, jak je uvedeno v bezpečnostní politice;
- stanovování postupů pro monitorování a revidování SAE programu.

SAE program by měl začít snahou o identifikaci různých způsobů budování bezpečnostního povědomí se zaměřením na všechny úrovně střední školy, včetně vedoucích pracovníků. Účinnost tohoto úsilí obvykle určuje účinnost celého SAE programu.

Program budování bezpečnostního povědomí je zásadní v tom, že je prostředkem k šíření informací, které uživatelé včetně jejich vedoucích potřebují k tomu, aby vykonávali svou práci. Efektivně nastavený SAE program včetně školení o bezpečnosti informací obsahuje pravidla správného chování při používání informačního systému střední školy, bezpečnostní politiku a postupy, které je třeba dodržovat. Vše výše uvedené dává základ pro stanovení případných sankcí při nedodržení nastavených opatření.

SAE program obsahuje čtyři úrovně: povědomí, školení, vzdělávání a profesionální rozvoj.



Obr. 11: Úrovně SAE programu [15]

3.3.1 Povědomí

Základy SAE programu staví v prvním stupni na povědomí. Publikace NIST SP 800-16 vykládá tento pojem jako schopnost uživatele vyvarovat se takového chování, jež by ohrozilo informační i kybernetickou bezpečnost. Za správné je považováno takové chování, které vede k účelnému a efektivnímu zacházení se svěřenými technologiemi. [16]

Snahy o zvýšení povědomí uživatelů o bezpečnosti jsou navrženy tak, aby vedly ke změně chování, příp. k posílení dobrých bezpečnostních postupů. Účelem budování povědomí je zaměřit pozornost na informační bezpečnost. Prezentace, jako jeden ze způsobů zvyšování bezpečnostního povědomí, jsou zaměřeny na informovanost uživatelů s cílem umožnit jednotlivcům rozpoznat hrozby v zabezpečení informačních systémů a poskytnout jim návod, jak odpovídajícím způsobem jednat.

Budování povědomí na základní úrovni není totéž co školení. Zatímco je při činnostech zvyšování povědomí uživatel příjemcem informací, v průběhu školení má aktivnější roli. Mnohdy se zvyšování povědomí i informační a kybernetické bezpečnosti odehrává bezděčně, např. v průběhu rozhovoru nebo v rámci obecného sdělení základních informací širokému spektru uživatelů. Školení v bezpečnostním povědomí je v tomto ohledu více formální a má za cíl vštípit potřebné znalosti a vybudovat požadované dovednosti, které mají za cíl uživatelům usnadnit práci.

Příkladem zvyšování bezpečnostního povědomí na první úrovni je šíření informací o ochraně před viry. Předmět sdělení lze jednoduše vysvětlit popisem toho, co je to virus a co se může stát, pokud virus napadne systém uživatele, jak se zachovat, aby byl systém chráněn a co dělat, pokud je virus detekován.

3.3.2 Školení

Na druhém stupni programu budování bezpečnostního povědomí se nachází školení. Publikace NIST SP 800-16 definuje pojem školení jako poskytnutí relevantních a potřebných znalostí a dovedností k infomační a kybernetické bezpečnosti uživatelům. Vedoucí úseků jsou povinni zajistit, aby všem jejich podřízeným byla poskytnuta odborná příprava a že všichni uživatelé informačního systému střední školy (v rámci daného úseku) jsou řádně vyškoleni. V rámci školení se usiluje o vytvoření potřebných dovedností. [16]

Prostřednictvím školení se správce SAE programu snaží naučit uživatele takovým dovednostem, které jim následně umožní vykonávat určitou funkci. Kompetence získané v průběhu školení jsou založeny na povědomí o podpůrných bezpečnostních materiálech a gramotnosti. Obsah kurzu stanoví správce SAE programu ve spolupráci s CIO a vedoucími úseků. Školení nemusí nutně obsahovat vše, co se žák naučí např. v rámci formálního počátečního vzdělávání.

Školení o budování bezpečnostního povědomí by se mělo opakovat v pravidelných intervalech, příp. tehdy, vyžaduje-li si to daná situace.

3.3.3 Vzdělávání

Vzdělávání v informační a kybernetické bezpečnosti se nachází na třetí úrovni programu budování bezpečnostního povědomí. Podle publikace NIST SP 800-16 vzdělávání integruje všechny potřebné bezpečnostní znalosti a dovednosti různých dílčích funkcionalit do jednoho celku, který je obohacen o koncepty a zásady příbuzných oblastí (např. technologické a sociální), čímž dosahuje synergického efektu. Absolvent vzdělávání v bezpečnostním povědomí se stává odborníkem na informační a kybernetickou bezpečnost schopným stanovit vizi a řešit problematiku bezpečnosti proaktivně. [16]

V rámci procesu vzdělávání se řeší tři typy uživatelů: začátečníci, středně pokročilí a pokročilí, čemuž následně odpovídá hloubka jejich znalostí a dovedností. Ke každému z těchto typů uživatelů by se mělo přistupovat individuálně s ohledem na konkrétní potřeby.

Příkladem takového vzdělání jsou studijní programy na vysokých školách a univerzitách. Některé vysoké školy ke standardnímu formálnímu diplomu o dosaženém stupni vzdělání v daném oboru nabízí různé druhy certifikátů zaměřených již na konkrétní oblast. Podobně je tomu např. na Vysokém učení technickém Brno, kde žáci v rámci studia oboru Informační management při volbě zaměření na Management informační bezpečnosti mohou při splnění určitých podmínek získat certifikát ISMS manažer a ISMS specialista.

3.3.4 Profesionální rozvoj

Čtvrtý stupeň a tedy nejvyšší úroveň SAE programu obsahuje profesionální rozvoj odborníků na oblast řízení systému bezpečnosti informací. Smyslem této úrovně je zajistit, aby všichni uživatelé od začátečníků až po profesionály měli požadovanou úroveň znalostí a dovedností nezbytně nutných pro výkon jejich funkce.

Při splnění stanovených podmínek a prokázání požadovaných kompetencí je možné v rámci profesionálního rozvoje získat certifikát. Příprava na certifikaci obvykle zahrnuje studium předepsaného penza znalostí nebo technických učebních osnov. To vše může být doplněno o praktické zkušenosti. Existují dva druhy certifikace:

- obecná – zaměřena na vytvoření základů znalostí o mnoha aspektech profesí v oblasti bezpečnosti informací;
- technická – zaměřena na technické otázky zabezpečení týkající se konkrétních platforem, operačních systémů, produktů a dalších.

Některé organizace se na držitele certifikátů zaměřují již při náboru nových zaměstnanců a v inzerátu přímo uvádějí, která osvědčení mohou uchazeči přinést výhodu. Jiní zaměstnavatelé nabízejí svým zaměstnancům za získané certifikáty zvýšení platu nebo jiné bonusy, a tím nepřímo motivují k certifikaci i ostatní.

3.4 Koncepce SAE programu

Existují tři zásadní kroky ve vývoji informačního a výcvikového programu budování bezpečnostního povědomí pro oblast bezpečnosti informací, kterými jsou:

- návrh SAE programu;
- vytváření podpůrných a školicích materiálů;
- realizace SAE programu.

Dokonce i minimální informovanost a základní školení v bezpečnosti informací mohou značně přispět ke zlepšení bezpečnostní pozice a bdělosti v organizaci. V této části bude řešena první fáze vývoje informačního a výcvikového programu budování bezpečnostního povědomí, a to návrh SAE programu.

Program budování bezpečnostního povědomí a příslušná školení musí být navrženy na míru dané organizace. Základním požadavkem je, aby SAE program:

- reflektoval potřeby organizace a podporoval jejich uspokojení,
- respektoval kulturu a strukturu organizace.

Úspěšný program budování bezpečnostního povědomí odpovídá předmětu organizace a řeší její aktuální bezpečnostní problémy. Koncepce SAE programu je odpovědí na otázku: "jaký je plán rozvoje a realizace příležitostí ke zvyšování bezpečnostního povědomí a odborné přípravy, které jsou v souladu s platnými směrnicemi?". Ve fázi návrhu SAE programu jsou identifikovány potřeby odbornosti a odborných školení

uživatelů organizace, vytváří se akční plán zvyšování bezpečnostního povědomí, jsou stanoveny priority a alokovány finanční zdroje na jeho pozdější realizaci.

Koncepce SAE programu se zaměřuje na:

- strukturu programu budování bezpečnostního povědomí;
- odůvodnění, proč provádět hodnocení potřeb;
- rozvoj plánu budování bezpečnostního povědomí a školení;
- stanovení priorit;
- nastavení požadavků pro jednotlivé úrovně SAE programu;
- stanovení finančního rámce programu budování bezpečnostního povědomí.

3.4.1 Struktura SAE programu

Program budování bezpečnostního povědomí a příslušná školení mohou být navrženy, zpracovány a realizovány mnoha různými způsoby. Níže jsou popsány tři nejčastější přístupy:

- centralizovaný – centralizovaná politika, strategie i implementace;
- částečně decentralizovaný – centralizovaná politika a strategie, distribuovaná implementace;
- decentralizovaný – centralizovaná politika, distribuovaná strategie a implementace.

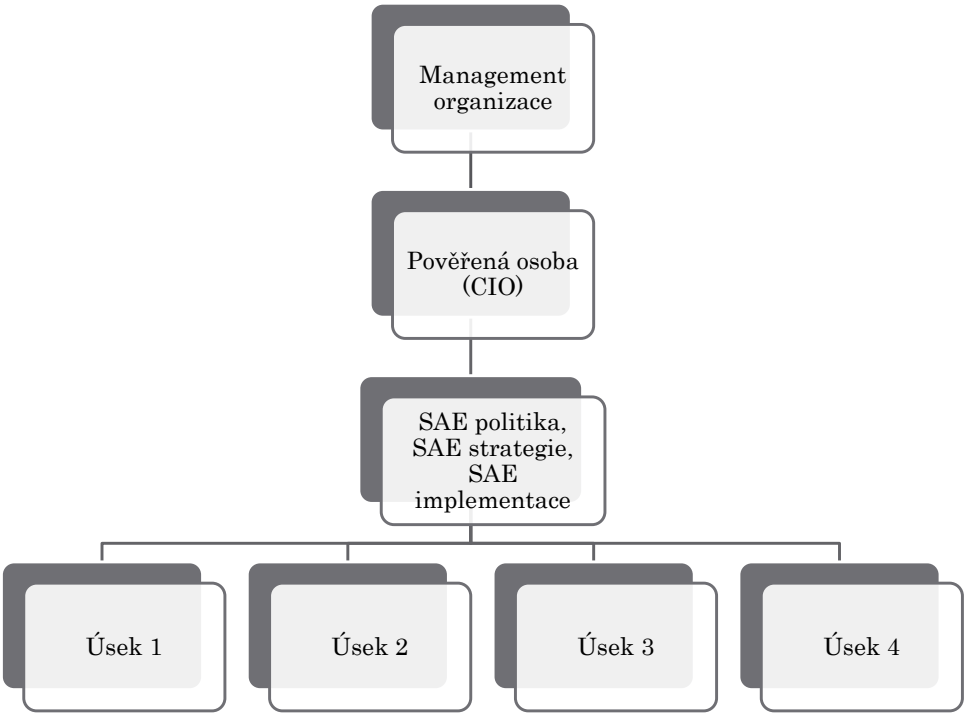
Zavedení konkrétního přístupu k budování bezpečnostního povědomí a školení závisí na:

- velikosti a geografickém uskupení organizace;
- definovaných rolích a odpovědnostech v rámci organizace;
- výši finanční alokace a pravomocích.

Centralizovaný přístup

V rámci tohoto modelu zodpovídá za rozpočet i tvorbu celého SAE programu ústřední orgán, v případě střední školy by se jednalo o ředitele školy nebo jím pověřenou osobu (CIO). Zpracování veškeré dokumentace (bezpečnostní politiky, strategie i podkladů

pro školení), rozvoj, implementace i plánování SAE programu závisí na této pověřené osobě, jak znázorňuje obrázek níže.



Obr. 12: Centralizovaný přístup k SAE programu [Zdroj: Vlastní zpracování]

Pověřená osoba (CIO) vypracovává bezpečnostní politiku organizace a strategii budování bezpečnostního povědomí, provádí hodnocení potřeb, stanovuje a rozvíjí plán školení a vzdělávání a vytváří i podpůrné školicí materiály. Za určení způsobu implementace SAE programu zodpovídá management organizace, jehož součástí mnohdy bývá i CIO.

Komunikace mezi pověřenou osobou (CIO) a jednotlivými úseky probíhá oběma směry. Pověřená osoba realizuje odsouhlasenou a schválenou strategii implementace programu budování bezpečnostního povědomí prostřednictvím stanovených metod v rámci příslušných školení. Zástupci jednotlivých úseků zprostředkovávají informace požadované CIO. Příkladem fungující komunikace jsou dostupné informace o počtech účastníků na hromadných zasedáních svolaných za účelem zvyšování povědomí, nebo údaje o počtu účastníků školení pořádaných na konkrétní témata bezpečnosti informací. Jednotliví vedoucí úseků mohou poskytnout zpětnou vazbu např. o účinnosti školení

a školicích materiálů a vhodnosti použitých metod, což umožňuje pověřené osobě upravit, rozvíjet nebo revidovat podpůrné materiály a měnit způsob implementace programu budování bezpečnostního povědomí.

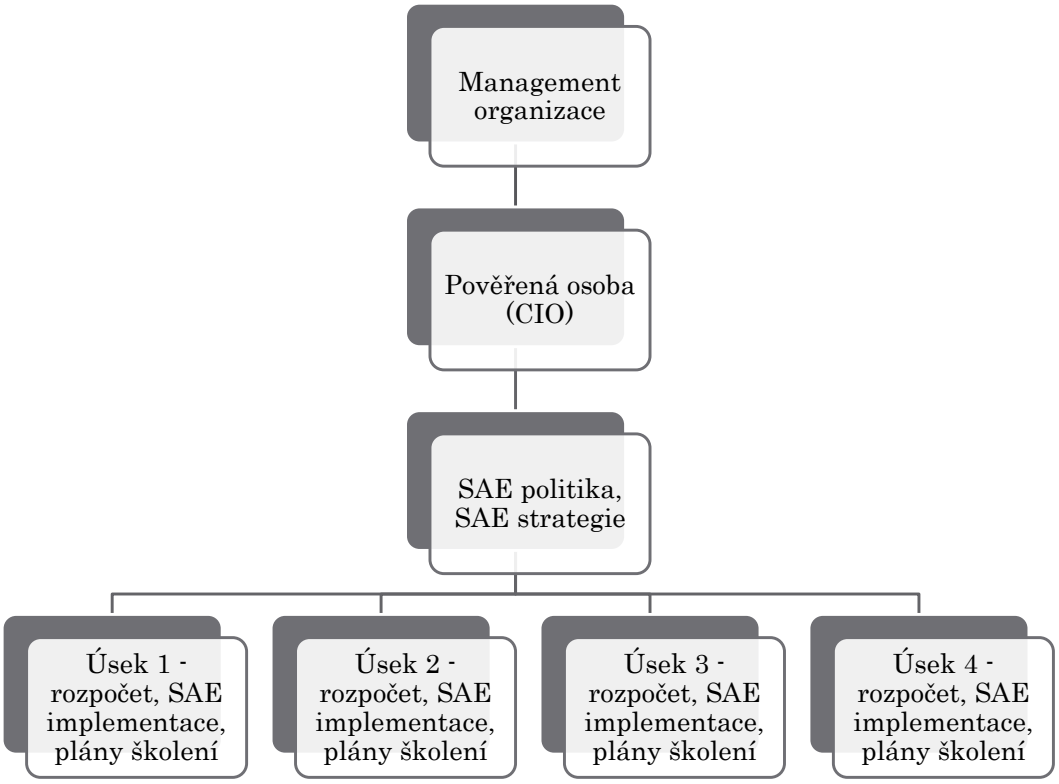
Centralizovaný model řízení a implementace SAE programu se často využívá v malých organizacích s vysokým stupněm centrálního řízení.

Částečně decentralizovaný přístup

Pro tento typ modelu je typická centralizovaná SAE politika a strategie a distribuovaná implementace SAE programu. Bezpečnostní politiku a strategii programu budování bezpečnostního povědomí má na starosti ústřední orgán. Stejně jako v předchozím modelu by se v případě střední školy jednalo o ředitele školy nebo jím pověřenou osobu (CIO). Proces implementace SAE programu je přidělen vedoucím úseků, kteří v jeho rámci zodpovídají také za rozdělení rozpočtu na zvyšování povědomí a konání školení mezi jednotlivé úseky a plánování a rozvoj podpůrných materiálů.

Hodnocení potřeb provádí pověřená osoba, protože určuje strategii programu budování bezpečnostního povědomí. Bezpečnostní politiku, strategii i alokované finanční prostředky předává pověřená osoba vedoucím úseků. Na základě strategie SAE programu zpracovávají vedoucí úseků své vlastní vzdělávací plány, připravují školicí materiály a určují způsob jeho předání relevantním uživatelům v rámci svých úseků.

Stejně jako v předchozím centralizovaném přístupu probíhá komunikace mezi pověřenou osobou a vedoucími úseků obousměrně. CIO mimo výše uvedené aktivity a odpovědnosti může vedoucím úseků poradit s přípravou podpůrných materiálů pro zvyšování povědomí i školení a zároveň jim poskytuje školení, příp. vzdělávání v oblasti bezpečnosti informací tak, aby mohli vedoucí úseků řádně plnit své povinnosti. Pověřená osoba si může od vedoucích úseků vyžádat podávání pravidelný reportů o vynaložených finančních prostředcích na zvyšování povědomí a školení uživatelů, o stavu plánu výcviku, zprávy o pokroku při budování bezpečnostního povědomí, informace o počtech účastníků na hromadných zasedáních uskutečněných za účelem zvyšování povědomí nebo údaje o počtu účastníků školení pořádaných na konkrétní témata bezpečnosti informací. Pověřená osoba může požádat také o zpětnou vazbu, kterou může poskytnout jako pokyny ostatním vedoucím úseků.



Obr. 13: Částečně decentralizovaný přístup k SAE programu [Zdroj: Vlastní zpracování]

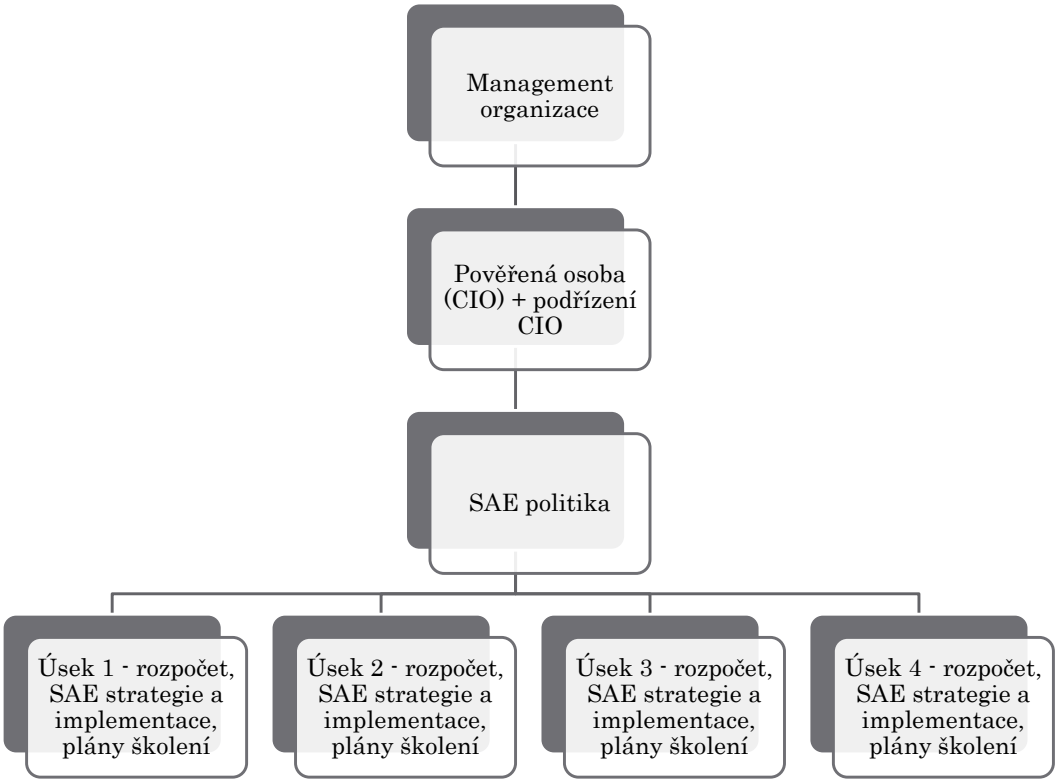
Částečně decentralizovaný model lze uplatnit v organizacích, které:

- jsou střední nebo i velké, příp. mají decentralizovanou organizační strukturu s jasnými odpovědnostmi;
- mají funkční jednotky, které jsou geograficky rozmístěny v různých zeměpisných oblastech;
- mají úseky s rozmanitými úkoly a program zvyšování povědomí a školení by se mohly významně lišit vzhledem k zaměření úseku.

Plně decentralizovaný přístup

Tento model budování bezpečnostního povědomí pracuje s centralizovaným přístupem k bezpečnostní politice a distribuovanou strategií a implementací SAE programu. Zodpovědnost za zpracování bezpečnostní politiky podobně jako v obou předchozích přístupech přísluší ústřednímu orgánu, a sice řediteli střední školy, ev. jím pověřené osobě. Za zpracování strategie a zajištění implementace programu budování bezpečnostního povědomí jsou zodpovědní vedoucí jednotlivých úseků. Tento přístup

obvykle používá sérii směrnic řešících problematiku bezpečnosti informací a více pověřených osob podřízených CIO.



Obr. 14: Plně decentralizovaný přístup k SAE programu [Zdroj: Vlastní zpracování]

Hodnocení potřeb provádí každý úsek zvlášť, jelikož si v tomto modelu určují úseky strategii SAE programu samy. Bezpečnostní politika a rozpočet jsou předávány pověřenou osobou. Vzhledem k individuálně zpracovaným strategickým plánům si každý úsek zpracovává i své konkrétní školení a podpůrné školicí materiály a určuje způsob jejich šíření v rámci svého úseku.

Také v přístupu plně decentralizovaném je oboustranná komunikace mezi pověřenou osobou a vedoucími úseků důležitou součástí budování bezpečnostního povědomí. CIO předává pokyny týkající se bezpečnostní politiky a finančních prostředků do rukou vedoucích úseků. Zároveň jim poskytuje poradenské služby při vytváření strategií a zajišťováním implementace SAE programu a pomáhá s přípravou školení a školí vedoucí úseků v oblasti bezpečnosti informací tak, aby mohli vedoucí úseků řádně plnit své povinnosti. Pověřená osoba může vyžadovat pravidelné informace o čerpání

finančních prostředků, o stavu a výsledcích hodnocení potřeb, o plánech implementace SAE programu a uskutečněných jednáních ke zvyšování bezpečnostního povědomí a školeních v bezpečnosti informací, dále také údaje o počtu účastníků školení a jednání, zprávy o pokroku a školicí materiály.

Plně decentralizovaný přístup k řízení SAE programu je vhodný pro:

- velké organizace;
- organizace s decentralizovanou organizační strukturou a jasně definovanými a stanovenými odpovědnostmi;
- organizace mající funkční jednotky, které jsou geograficky rozmístěny v různých zeměpisných oblastech;
- organizace mající úseky s rozmanitými úkoly a program zvyšování povědomí a školení by se mohly významně lišit vzhledem k zaměření úseku.

3.4.2 Hodnocení potřeb

Posouzení potřeb je proces, který lze využít pro stanovení potřeb organizace. Výsledky tohoto procesu mohou posloužit jako zdůvodnění – určené vedení organizace – potřeby vyčlenit dostatečné finanční prostředky na program budování bezpečnostního povědomí.

Do procesu hodnocení potřeb je žádoucí zapojit níže uvedené klíčové pracovníky, kteří v rámci budování bezpečnostního povědomí musí řešit některou úroveň SAE programu:

- vedení organizace – zástupci managementu organizace se musí orientovat v zákonech a směrnicích, které tvoří základ SAE programu;
- osoba odpovědná za přípravu a správu školení o bezpečnosti informací (CIO) – tato osoba zastupuje organizaci v oblasti bezpečnosti informací a v případě potřeby poskytuje relevantním cílovým skupinám odborné konzultace, a proto musí být dobře informována o bezpečnostní politice a osvědčených postupech;
- správce SAE programu – tato osoba musí mít hluboké znalosti bezpečnostní politiky a kontroly a rozumět požadavkům na systém, který spravuje;

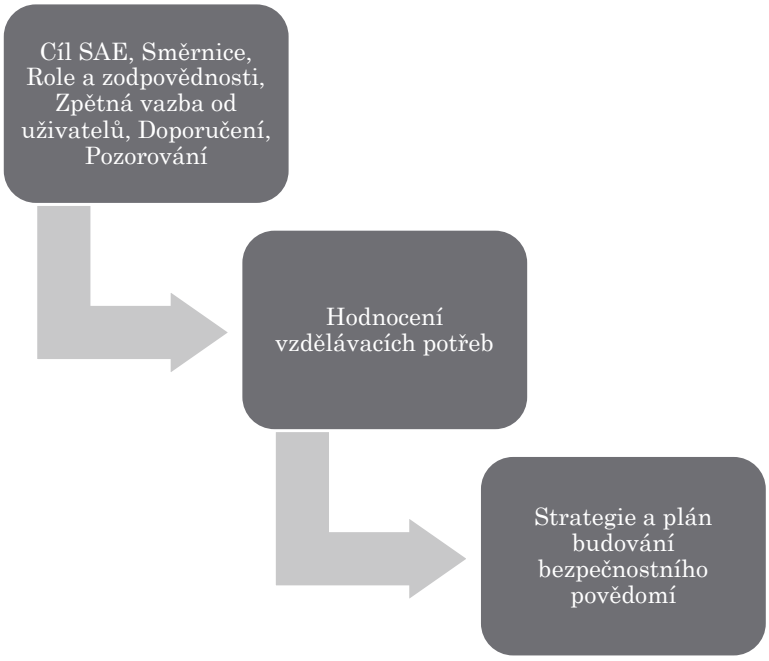
- systémový administrátor a pracovníci IT podpory – tito lidé potřebují vyšší stupeň technických znalostí o efektivních bezpečnostních postupech a implementaci SAE programu;
- vedoucí úseků, uživatelé – zástupci těchto cílových skupin potřebují zvýšit bezpečnostní povědomí a projít školením o vhodném chování v systému, do kterého mají přístup.

Informace z různých zdrojů dají základ k určení SAE programu a potřebnosti školení. Existují různé techniky pro zjišťování a shromažďování potřebných informací. Mezi nejčastěji používané patří:

- průzkumy v organizaci (např. dotazníková šetření);
- přezkoumání a vyhodnocení dostupných materiálů k budování bezpečnostního povědomí (např. školicí materiály, plán implementace SAE programu, seznamy proškolených a další);
- analýza metrik souvisejících s potřebou školení (např. procento uživatelů, kteří absolvovali trénink ve zvýšení povědomí nebo školení);
- dokumentace k používaným systémům (pro identifikaci vlastníků systémů a aplikací);
- kontrola databáze provedených inventarizací a databáze uživatelských ID (pro určení všech osob majících přístup do systému);
- doporučení a výstupy z provedených kontrol a auditů;
- rozhovory s vedením organizace, CIO, správcem SAE programu, vedoucími úseků a uživateli;
- analýza událostí (např. identifikované útoky virem, zamítnuté/zakázané webové stránky);
- provedené technické změny a infrastruktura organizace;
- trendy (např. ve vydaných tuzemských či zahraničních publikacích).

V situaci, kdy je program budování bezpečnostního povědomí v organizaci již zaveden, může posloužit dotazník jako zpětná vazba ze zasedání pro zvyšování bezpečnostního povědomí a ke zpřesnění obsahu prováděných školení. Vzor dotazníku je uveden v příloze č. 1. Výstupy z analýzy metrik jsou důležitým a efektivním nástrojem pro stanovení potřeb SAE programu. Údaje z metrik poskytují mimo jiné také informace

o dosažení cílů programu budování bezpečnostního povědomí prostřednictvím kvantifikace úrovně dosaženého povědomí a účinnosti školení a doporučení pro možné zlepšení nastaveného SAE programu.



Obr. 15: Proces od identifikace potřeb k přípravě SAE plánu [Zdroj: Vlastní zpracování]

Obrázek výše znázorňuje specifické oblasti, na které je třeba se zaměřit při zjišťování vstupů potřebných pro proces hodnocení vzdělávacích potřeb. K uvedeným oblastem lze získat více informací za pomocí technik zmíněných na předchozí stránce. Analýza všech relevantních informací by měla poskytnout odpovědi na tyto klíčové otázky:

- Co je zapotřebí? Jaké povědomí, školení a/nebo vzdělávání jsou potřebné?
- Jaký je současný stav?
- Co pro splnění potřeb provádíme již nyní?
- Co je třeba ještě provést?
- Které potřeby jsou nejdůležitější?

V souvislosti s hodnocením potřeb a získáním potřebných informací je třeba brát v úvahu také související požadavky. Jestliže se např. plánuje zvyšovat povědomí formou hromadného setkání, musí být předem ověřeno, zda k tomuto účelu existují vhodné prostory, příp. technické vybavení nebo kompetentní osoby. Při plánování

takových akcí nesmí být opomenuti uživatelé se zvláštními potřebami (např. se zdravotním postižením).

Porozumění všem identifikovaným potřebám vede k sestavení strategie a plánu budování bezpečnostního povědomí. Plán by měl pokrývat celou organizaci a zohledňovat přiřazené priority identifikovaných potřeb.

3.4.3 Vypracování strategie a plánu SAE programu

Dokončení procesu hodnocení potřeb umožňuje organizaci zpracovat strategii vývoje, implementace a udržování programu budování bezpečnostního povědomí. Strategii tvoří jednotlivé prvky jako:

- stávající předpisy, které se obsahově týkají budování bezpečnostního povědomí (např. zákon o kybernetické bezpečnosti);
- rozsah SAE programu;
- určené role a odpovědnosti (zejména pracovníků, kteří mají na starosti přípravu, realizaci a aktualizaci programu budování bezpečnostního povědomí;
- cíle, kterých má být na každé úrovni SAE programu dosaženo (povědomí, školení, vzdělávání a profesionální rozvoj);
- cílové skupiny pro každou úroveň SAE programu;
- povinné, ev. podpůrné a školicí materiály pro jednotlivé cílové skupiny uživatelů;
- témata jednotlivých kurzů, školení, vzdělávání atd.;
- vhodné metody použité při implementaci programu budování bezpečnostního povědomí;
- doprovodná dokumentace ke každé úrovni SAE programu (např. prezenční listiny, důkaz o proškolení, zpětná vazba a další);
- vyhodnocení výcviku na každé úrovni SAE programu a způsob aktualizace školicích materiálů;
- frekvence výcvikových akcí v SAE programu.

Plán obsahuje jednotlivé prvky strategie zasazené do časového harmonogramu.

3.4.4 Stanovení priorit

Jakmile je zpracována strategie a plán programu budování bezpečnostního povědomí, musí být SAE program aplikován. V případě, že je potřeba implementaci SAE programu rozdělit do dílčích kroků (např. kvůli omezenému rozpočtu nebo dostupnosti zdrojů), je důležité rozhodnout o faktorech, které mají určovat prioritu jednotlivým prvkům strategie a plánu SAE programu. Mezi klíčové faktory, které je vhodné zvážit, patří:

- dostupnost zdrojů a materiálů – jsou-li materiály pro zvyšování povědomí a školení a potřebné zdroje v daném okamžiku dostupné, nic nebrání jejich naplánování, ovšem musí-li být materiály pro výcvik vypracovány, příp. správce SAE programu vybrán, měly by být tyto požadavky při stanovení priorit zohledněny;
- dopad přidělení rolí na organizaci – přiřadíme-li stávajícímu zaměstnanci novou roli (např. správce SAE programu), ev. konkrétní nové dílčí úkoly související např. s přípravou školení, je žádoucí upřesnit jejich prioritu s ohledem na další aktivity, zároveň by měla být zohledněna potřeba rozvoje znalostí a dovedností u pozic s vysokou důvěrou (např. správce informačního systému, vedoucí úseků);
- současný stav – identifikace hlavních nedostatků SAE programu;
- závislost na souběžném projektu – pokud existují projekty závislé na bezpečnostním školení za účelem přípravy potřebných požadavků na daný systém (např. nový operační systém, virtuální privátní sít (VPN), firewally), je třeba zohlednit časový souběh plánovaných školení.

3.4.5 Nastavení požadavků SAE programu

Nastavením požadavků programu budování bezpečnostního povědomí se rozumí učinění rozhodnutí o složitosti a rozsahu podpůrných a školicích materiálů. Tyto materiály k SAE programu by měly být vypracovány z pohledu dvou důležitých kritérií:

- pozice cílové osoby nebo skupiny osob (uživatelů) v organizaci;

- požadavků na znalosti a dovednosti jednotlivých uživatelů v problematice budování bezpečnostního povědomí.

Složitost materiálů musí odpovídat úloze cílové osoby nebo skupiny osob, které se budou podrobovat procesu zvyšování bezpečnostního povědomí. Určení rozsahu a složitosti materiálů musí být stanoveno před zahájením další fáze SAE programu (tzn. před započetím tvorby podpůrných a školicích materiálů) pro minimálně první tři úrovně SAE programu (povědomí, školení, vzdělávání).

Při stanovení požadavků by se osoba pověřená touto činností měla zaměřit na předpokládaná pravidla chování při používání informačních technologií a informačních systémů. Tato pravidla by měla vycházet přímo z politiky dané organizace a měla by být přesně vymezena, aby nevznikal žádný prostor pro zmatek či nedorozumění. S ohledem na vývoj SAE programu v čase a současně v souvislosti s již uskutečněnými jednáními na téma zvyšování bezpečnostního povědomí a školeními, mohou být požadavky SAE programu zpřesňovány a zkvalitňovány.

Stanovení odpovídající úrovně složitosti výcvikových materiálů je velmi důležité vzhledem k faktu, že cílem zvyšování povědomí a školení je taková skladba a úroveň dovedností uživatelů, které jsou potřebné pro bezpečný výkon jejich pracovních činností. Podpůrné výcvikové materiály mohou na prvním stupni zvyšování povědomí obsahovat např. základní informace pro uživatele, kteří se prvně setkávají s prací na počítači, ev. s různými tabulkovými či textovými editory, anebo s přístupem k internetu. Výcvikové materiály pro druhou úroveň (školení) mohou být vytvořeny např. pro uživatele typu vedoucí úseků, kteří zodpovídají za správu určité části informačního systému. Budování bezpečnostního povědomí na úrovni vzdělávání může být zaměřeno např. na správce sítě, který si potřebuje pro bezpečný výkon povolání neustále rozšiřovat své obzory v souvislosti s vývojem stále nových technologií a systémů.

Na nastavení požadavků v rámci úrovně zvyšování povědomí, školení i vzdělávání může organizace spolupracovat se zástupci vzdělavatelů, škol i univerzit, jejichž zaměření studijních programů odpovídá zvolené problematice SAE programu. Je však potřeba zohlednit aktuální požadavky dané organizace pro každý stupeň bezpečnostního povědomí a na konkrétních příkladech aplikovat teoretické znalosti. Další možností, jak zajistit požadovanou úroveň kompetencí uživatelů, může být přímá spolupráce se

střední, ev. vysokou školou či univerzitou, která poskytuje potřebný vzdělávací proces nejlépe dálkovou formou. V průběhu kurzu získá uživatel požadované znalosti a dovednosti, které prokáže při závěrečném ověření (např. ústní zkouška, test, praktické předvedení), za což obdrží osvědčení.

3.4.6 Zajištění financování SAE programu

Jakmile je dohodnuta strategie budování bezpečnostního povědomí a jsou stanoveny priority, musí být do plánu doplněny požadavky na přidělení finančních prostředků. Je třeba stanovit, jaký rozsah finanční podpory má být přidělen v závislosti na zvoleném modelu (viz subkapitola 3.4.1: centralizovaný, částečně decentralizovaný, plně decentralizovaný). Osoba odpovědná za přípravu a správu školení o bezpečnosti informací (CIO) musí přesně vymezit očekávání o dodržování pravidel v této oblasti. Plán pro zvyšování bezpečnostního povědomí a školení je považován za soubor minimálních požadavků, které musí být splněny, a tyto požadavky musí být organizací finančně podpořeny.

V případě, že organizace bude postupovat ve zvyšování bezpečnostního povědomí formou vzdělávacích programů nabízených střední nebo vysokou školou, které povedou ke zvýšení[4] či prohlubování[5] kvalifikace uživatele, doporučuje se sepsat s tímto pracovníkem kvalifikační dohodu v písemné podobě dle příslušných ustanovení zákoníku práce. Dohoda upřesňuje podmínky zvyšování či prohlubování kvalifikace a práva a povinnosti zaměstnavatele a zaměstnance. [27]

Vyjádření požadavku na objem finančních prostředků potřebných pro jednotlivé komponenty SAE program lze pojmout různými způsoby, např.:

- procentem z celkového rozpočtu na školení v rámci organizace;
- vyčíslením přesných částek pro potřeby zvyšování povědomí, školení a vzdělávání konkrétních pracovníků vykonávajících specifické role, viz subkapitola 3.2;

[4] Zvýšení kvalifikace – podle zákoníku práce se zvýšením kvalifikace rozumí změna hodnoty kvalifikace, stejně jako její získání nebo rozšíření. [27]
[5] Prohlubování kvalifikace – podle zákoníku práce se prohlubováním kvalifikace rozumí její průběžné doplňování, kterým se nemění její podstata, udržování a obnovování. [27]

- procentem z celkového rozpočtu IT úseku;
- určením nákladů na implementaci SAE programu v rámci jednotlivých úseků.

Problémy při implementaci programu budování bezpečnostního povědomí a jeho příslušné strategie mohou nastat, jestliže jsou iniciativy týkající se bezpečnosti považovány za méně prioritní než jiné iniciativy organizace. Odpovědnost za posouzení konkurenční priority a vypracování strategie, která by řešila jakkoliv vysoký nedostatek finančních prostředků, nese CIO. Především záleží na přístupu vedení střední školy, zda bude SAE program a jeho rozsah přizpůsobovat dostupnému objemu finančních prostředků, anebo hledat způsoby financování SAE programu, příp. uvažovat o přerozdělení stávajících finančních zdrojů.

3.5 Příprava podpůrných a školicích materiálů

V momentě, kdy je odsouhlasena vize budování bezpečnostního povědomí v organizaci a je vytvořena základní strategická dokumentace pro tuto oblast včetně zajištění alokace potřebných finančních prostředků, mohou být zpracovány podpůrné a školicí materiály.

Při tvorbě materiálů je potřeba zohlednit:

- jaké chování chceme posílit (v případě zvyšování povědomí);
- jakou dovednost, příp. dovednosti by si uživatelé měli osvojit a v praxi aplikovat (v případě školení).

V obou případech musí být obsah podpůrných i školicích materiálů zpracován pro konkrétní cílovou skupinu, a to tak, aby sloužil jako pomyslný průvodce s nápovědou, jak se ve specifických případech zachovat a co vykonat. Materiály zpracované na obecné úrovni mohou na účastníky působit zmatečně a neosobně. Lehce se tak může stát, že si uživatel bude myslet, že se ho daná informace netýká a pojme zvyšování povědomí nebo školení jako akci, na které musí být a ze které si nic neodnese. SAE program bude účinný za předpokladu, že vytvořené podpůrné a školicí materiály budou zajímavé a aktuální.

Obecně lze konstatovat, že smyslem a cílem materiálů je soustředit pozornost na aplikaci bezpečnostních postupů v organizaci, a proto musí být poselství těchto

materiálů krátké a jednoduché. Každý dílčí podpůrný nebo školicí materiál se může zabývat jedním tématem, příp. několika příbuznými tématy, o nichž by uživatelé měli mít povědomí.

Mezi příjemce zvyšování povědomí by měli patřit všichni uživatelé v organizaci. Zprávy, které se mají šířit na první úrovni zvyšování povědomí, by měly informovat každého jednotlivce o společných sdílených odpovědnostech v oblasti bezpečnosti informací. Na druhém stupni v rámci školení už je problematika bezpečnosti zaměřena vždy na konkrétní cílovou skupinu. Školicí materiál by měl obsahovat vše, co souvisí s bezpečnostní úrovní, na kterou se konkrétní uživatelé musí dostat, aby mohli vykonávat své pracovní činnosti. Materiály vytvořené pro školení jdou do větší hloubky oproti podpůrným materiálům připraveným pro zvyšování povědomí.

3.5.1 Zpracování materiálů pro zvyšování povědomí (témata, zdroje)

Zásadní otázka, na kterou je třeba najít odpověď v době příprav podpůrných materiálů pro zvyšování povědomí, zní:

- čeho si mají být všichni uživatelé v oblasti informační a kybernetické bezpečnosti vědomi?

Plán pro zvyšování povědomí by měl obsahovat seznam témat budování bezpečnostního povědomí na této úrovni a přehled zdrojů, ze kterých lze čerpat inspiraci.

Výběr tématu pro zvyšování povědomí

Existuje mnoho témat, která se dají řešit na této úrovni budování bezpečnostního povědomí. Mezi ty základní patří:

- bezpečnostní politika v organizaci a důsledky jejího nedodržení;
- použití a správa hesel včetně jejich tvorby a frekvence změn;
- ochrana před viry, trojskými koni a jiným nebezpečným kódem;
- přijetí e-mailu, ev. přílohy od neznámé osoby, spamy;
- používání webových stránek (povolené versus zakázané);
- zálohování a ukládání dat (centralizovaný versus decentralizovaný přístup);

- sociální inženýrství (manipulace osob za účelem provedení určité akce nebo získání specifických informací);
- reakce na incident (koho kontaktovat a co udělat);
- tzv. shoulder surfing (typ sociálního inženýrství používaného k získání informací, jako např. heslo, identifikační číslo a další důvěrná data při pohledu přes rameno);
- rizika systému z vnějšího prostředí (voda, požár, prach, nečistoty aj.);
- inventura majetku (odpovědná osoba a odpovědnosti jednotlivých uživatelů);
- rizika při využití informačních technologií pro osobní použití;
- přenos citlivých a důvěrných informací prostřednictvím internetu (postupy, kontakty pro pomoc);
- problémy související s omezením softwarové licence;
- povolený software v systémech organizace;
- problémy s kontrolou přístupu (přidělení oprávnění dle pracovního zařazení a pracovních povinností);
- individuální odpovědnost (dopad jednání jedince);
- kontrola hostů organizace a fyzický přístup k prostorům (fyzická bezpečnost a zásady zacházení s majetkem organizace);
- zabezpečení plochy obrazovky (šetřiče obrazovky, omezení přístupu kolemjdoucích k informacím na obrazovce a další);
- etiketa používání e-mailů (např. velikost a množství připojených souborů).

Zdroje informací pro tvorbu podpůrných materiálů

Existuje široké spektrum zdrojů informací o bezpečnostním povědomí, a to jak z vnitřního, tak i vnějšího prostředí organizace. Inspiraci pro zajímavá témata a relevantní informace lze hledat např. ve zdrojích typu:

- normy, předpisy, legislativní dokumenty;
- auditní zprávy a interní kontroly;
- odborné konference, semináře, kurzy;
- best practises organizací podobného typu a zaměření;
- odborná periodika;

- zapojení se do profesionálních sdružení existujících v dané oblasti;
- on-line zpravodajské webové stránky o informační a kybernetické bezpečnosti;
- zprávy z aktuálního dění ve světě na téma informační a kybernetické bezpečnosti;
- sebehodnocení.

Metody zvyšování bezpečnostního povědomí

Každý materiál pro zvyšování bezpečnostního povědomí může obsahovat jedno téma, příp. řešit i více konkrétních problémů. V závislosti na složitosti konkrétního bezpečnostního rizika a závažnosti jeho dopadu je možné volit mezi různými metodami vhodnými pro sdělení uživatelům. Z těch nejčastěji používaných se jedná o:

- e-mailové zprávy s upozorněním;
- tisk a šíření letáků;
- řízené rozhovory na daná témata s jednotlivými cílovými skupinami i jednotlivci;
- společné schůzky;
- články na intranetu dané organizace;
- plakáty na informačních tabulích a vývěskách;
- speciální bulletin.

Pro zvyšování povědomí o jednom tématu je možné využít např. plakát, zatímco v průběhu rozhovoru či schůzky lze sdělit a prodiskutovat řadu témat. Bez ohledu na použitý přístup by množství informací nemělo přesáhnout kapacitu publika. Stručná informace o bezpečnostní politice, souvisejících problémech a opatřeních, která je potřeba přijmout, plně postačí.

Složitějším bezpečnostním tématům, která vyžadují hlubší znalosti a dovednosti, by mělo být věnováno více prostoru. Vzhledem k tomu, že základní informace o bezpečnostním povědomí tvoří most k potřebným znalostem a dovednostem budovaným prostřednictvím školení, je tato úroveň podrobnosti a složitosti přiměřená.

3.5.2 Zpracování školicích materiálů (modely, zdroje)

Podobně jako u zvyšování povědomí je i při plánování školení v bezpečnostním povědomí potřeba zodpovědět zcela zásadní otázku, a to:

- jakou dovednost, ev. dovednosti by měli uživatelé ovládat?

V rámci procesu plánování školení by měla být identifikována konkrétní cílová skupina, příp. i jeden či více uživatelů, kterým se dané školení ušije na míru tak, aby získali požadované znalosti a dovednosti v oblasti informační a kybernetické bezpečnosti. Takový typ školení je založen na rolích v dané organizaci. Existuje také druhý model školení, který se orientuje na jednotlivá bezpečnostní témata. Tento typ výcviku nepracuje s konkrétní cílovou skupinou. Naopak se zaměřuje na široké spektrum uživatelů a řeší určité téma, na které nahlíží z různých úhlů pohledu. Jednotlivci se musí v takovém případě sami zorientovat a vybrat si z uvedených opatření ta, která se na ně vztahují. Každý z uvedených modelů školení je vhodný pro jiný typ uživatelů. Školení orientované průřezově na jednotlivá bezpečnostní témata bude určeno pro všeobecné pracovníky (např. asistentky), kdežto model založený na rolích bude uplatněn u expertů a odborníků (např. zaměstnanci ekonomického úseku).

Model školení založený na rolích

Metodika na této úrovni SAE programu člení účastníky školení do tří základních skupin:

- začátečníci (např. noví zaměstnanci);
- středně pokročilí;
- pokročilí.

V této souvislosti také definuje složitost a rozsah vzdělávacích kurzů. Pro každou z uvedených skupin musí být určen specifický cíl kurzu. Každý jedinec může z pohledu úrovně své role vykonávat v rámci procesu určitého tématu specifické funkce (jednu i více). Pro každou oblast existuje sedm následujících funkcí:

- řízení – kategorie určena jednotlivcům, kteří na strategické úrovni rozhodují o používání informačních technologií a systémů;

- získávání a výběr – kategorie určená osobám, které se účastní výběrových komisí a vyhodnocují návrhy jednotlivých dodavatelů IT produktů nebo služeb;
- vývoj – kategorie činností související s návrhem a vývojem informačních systémů a aplikací;
- správa – kategorie určená osobám, které provozují a spravují informační technologie a systémy a jejich komponenty (např. webové servery, LAN, WAN);
- kontrola a hodnocení – kategorie činností související s auditem, a to jak interním, tak i externím;
- používání – kategorie určená těm uživatelům, kteří využívají informační technologie a systémy k výkonu své práce.
- jiné – kategorie využívaná ve zvláštních případech, kdy se nehodí ani jedna z výše uvedených funkcí.

Spojení jednotlivých témat (uvedených ve sloupcích) a jejich funkcí (zanesených do řádků) dohromady pak vytváří matici, kterou lze zpracovat pro každou roli v organizaci. Přidělením pracovníků podle jejich rolí ke každému tématu a funkci umožňuje správci SAE programu (ev. CIO) vytvořit kurzy šité na míru.

Správce systému							
	Funkční oblasti						
Odborná témata	**Řízení**	**Výběr**	**Vývoj**	**Správa**	**Kontrola**	**Používání**	**Jiné**
1. Legislativa a normy				x		x	x
2. SAE program				x		x	x
3. Bezpečnost životního cyklu systému				x			
3.1 Zahájení				x			
3.2 Vývoj				x			
3.3 Testování, hodnocení	x	x		x			
3.4 Implementace			x	x			

3.5 Používání	x		x	x			
3.6 Ukončení		x	x	x		x	

Obr. 16: Příklad matice témat a funkcí správce systému [Zdroj: Vlastní zpracování]

Zdroje pro tvorbu školicích materiálů

Prvním krokem při určování zdrojů výcvikového materiálu musí být rozhodnutí, zda budou materiály pro jednotlivé kurzy a školení vytvářeny interně nebo externě. Disponuje-li organizace vlastními odbornými zdroji, může si dovolit je přidělit na přípravu a vývoj školicích materiálů.

Při rozhodování o způsobu tvorby výcvikových materiálů je třeba vzít v úvahu odpovědi na níže uvedené otázky.

- Má organizace k dispozici dostatek vlastních zdrojů pro vývoj materiálů? Patří sem počet osob a jejich odborné znalosti, dovednosti a zkušenosti.
- Je nákladově efektivnější vytvářet a vyvíjet školicí materiál v rámci organizace, nebo formou outsourcingu?
- Disponuje organizace zaměstnancem schopným monitorovat činnost dodavatele?
- Existuje dostatečný objem finančních prostředků?
- Dokáže organizace vyčlenit zdroje (především finanční a lidské) potřebné k zajištění udržení materiálů, pokud jsou vypracovány dodavatelem?
- Odpovídá obsah citlivosti údajů možnosti použití dodavatele?

V případě, že se organizace rozhodne jít cestou outsourcingu, a tedy zajištěním tvorby výcvikových materiálů za pomoci dodavatele, měla by odpovědná osoba před výběrem dodavatele pečlivě porozumět potřebám školení a být schopna určit, zda materiál potenciálního dodavatele odpovídá konkrétním potřebám organizace.

Organizace mají více možností, z nichž si mohou vybírat při rozhodování, zda budou potřebné materiály vytvářet vlastními silami, nebo jejich tvorbu zadají externímu dodavateli. Odpovědní zástupci organizace mohou vytvářet nebo rozvíjet stávající partnerství s podobně zaměřenými organizacemi s cílem spolupracovat na vývoji podpůrných a školicích materiálů nebo společně koordinovat vzdělávací akce, které

splňují požadavky programu budování bezpečnostního povědomí. Kupříkladu několik organizací může podle dohody kombinovat své zdroje a odborné znalosti a připravovat školení pro určitou cílovou skupinu dohromady. V případě, že je některý z modulů specifický pro jednu organizaci, mohou zbylé spolupracující organizace využít většinu připravovaného materiálu a přizpůsobit pouze ten modul, který obsahuje specifické informace pro vybranou organizaci.

Existují různé způsoby spolupráce napříč organizacemi. Jedním takovým je například bezpečnostní den nebo každoroční pořádaná konference na téma budování bezpečnostního povědomí, kam jsou zváni také zaměstnanci jiných organizací. Zatímco prezentovaný obsah o informační a kybernetické bezpečnosti nemusí nutně odpovídat přesně tomu, co je v obou, příp. více organizacích potřebné, jedná se o poměrně levný způsob naplnění určitých potřeb odborné přípravy konkrétně vybraných cílových skupin. V případě shody o spolupráci při akci tohoto typu se doporučuje mezi organizacemi nastavit jasná pravidla, např. pro sledování účasti cílových skupin, použitelnosti školicích materiálů, určení zodpovědnosti za administrativní a další otázky.

Dalším z relativně levných způsobů zajištění vzdělávacích materiálů může být průzkum školicích podkladů vyvinutých jinými organizacemi. Důraz by v tomto případě měl být dán na použitelnost dostupných materiálů pro konkrétní cílovou skupinu, resp. je nutné, aby zdroj řešil takovou problematiku SAE programu, kterou potřebují účastníci školení znát pro výkon svých pracovních činností.

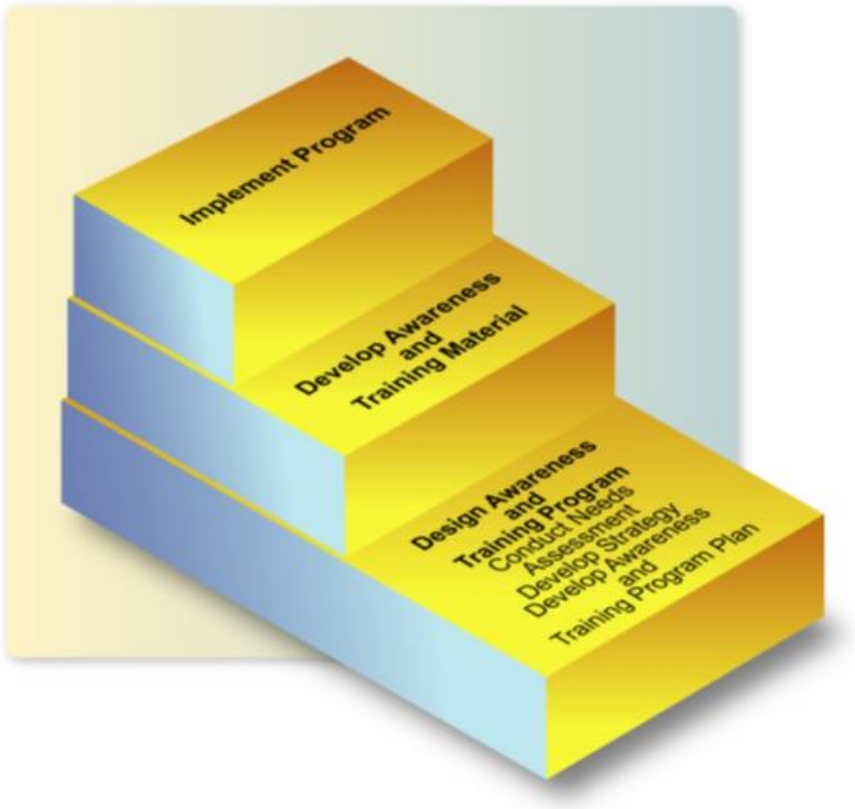
Pro tvorbu relevantních vzdělávacích materiálů zohledňujících všechny možné aspekty se doporučuje navazovat nová či rozvíjet stávající partnerství s podobnými typy organizací, které se zabývají obdobnou problematikou. Výhodou této spolupráce je zapojení více osob do diskuse o konkrétní oblasti informační a kybernetické bezpečnosti. Prostřednictvím partnerství může osoba odpovědná za přípravu a správu školení požádat o přezkoumání stávajících materiálů, kontrolu úplnosti a přesnosti a doplnění chybějících pasáží.

3.6 Realizace SAE programu

Program budování bezpečnostního povědomí by měl být spuštěn až poté, co:

- bylo provedeno posouzení potřeb;
- byla vypracována strategie;
- byl dokončen plán pro zvyšování bezpečnostního povědomí a určeny vzdělávací akce pro implementaci SAE programu;
- byly zpracovány podpůrné a školicí materiály.

Tyto klíčové kroky vedoucí k realizaci programu budování bezpečnostního povědomí znázorňuje také obrázek níže.



Obr. 17: Klíčové kroky vedoucí k realizaci SAE programu [15]

3.6.1 Komunikace plánu SAE programu

Implementace SAE programu musí být v organizaci transparentně komunikována. Toto je důležitý krok, vedoucí k získání podpory cílových skupin pro realizaci programu budování bezpečnostního povědomí a závazku potřebných zdrojů, a proto není radno jej

opomíjet. Samotná komunikace by měla zahrnovat nejen očekávání organizace, vyjádření podpory zaměstnanců (tj. uživatelů), ale také předpokládané výsledky SAE programu a jeho přínosy. Téma, které bývá opomíjeno, a přesto nese zcela zásadní informace, je otázka financování a přidělené alokace na realizaci SAE programu. Minimálně vedoucí úseků by měli být informováni o svěřených finančních prostředcích, které mohou na potřebná školení vynaložit. Zároveň by měli vědět, zda náklady na realizaci SAE programu budou hrazeny z prostředků CIO, nebo z rozpočtu IT úseku, příp. zda ponesou část nákladů z přiděleného objemu financí daného úseku.

Každý, kdo se podílí na implementaci programu budování bezpečnostního povědomí, musí chápat svoji roli a být si vědom svých povinností. Současně je třeba komunikovat harmonogram s určením požadavků na termín dokončení svěřených implementačních aktivit.

Způsob komunikace programu budování bezpečnostního povědomí lze rozdělit do různých scénářů podle tří implementačních modelů (modely viz subkapitola 3.4.1).

- **Scénář komunikace v modelu centralizovaného přístupu implementace SAE programu** – v tomto případě zajišťuje kompletní přípravu i realizaci programu budování bezpečnostního povědomí pověřená osoba (CIO), což obsahuje zpracování bezpečnostní politiky organizace, vývoj strategie i plánu implementace a realizaci SAE programu včetně zvyšování povědomí a školení. Veškeré nezbytné finanční prostředky pro vývoj a implementaci všech potřebných materiálů spravuje CIO. Do začátku fáze realizace SAE programu musí pověřená osoba provést hodnocení potřeb, vypracovat plán výcviku a vytvořit podpůrné a školicí materiály pro úrovně zvyšování povědomí a školení. CIO by měl informovat zástupce vedení organizace (v případě střední školy ředitele školy) o plánu implementace SAE programu a získat k němu souhlas. Jakmile management organizace plán schválí, může pověřená osoba spustit proces realizace SAE programu, tzn. obrátit se na vedoucí úseků s vysvětlením dílčích aktivit vedoucích k naplnění strategie programu budování bezpečnostního povědomí. Vedoucí úseků pak sdělují plán svým podřízeným, identifikují požadavky na zvyšování povědomí a školení, přiřadí ke každé úrovni

jednotlivé zaměstnance (v případě školy se přiřazují nejen zaměstnanci školy, ale i žáci) a předkládají své nominace pověřené osobě.

- **Scénář komunikace v modelu částečně decentralizovaného přístupu implementace SAE programu** – v případě využití tohoto modelu zpracovává CIO v rámci programu budování bezpečnostního povědomí pouze bezpečnostní politiku a strategii. Současně provádí hodnocení potřeb, jelikož ze získaných informací připravuje strategii SAE programu. Vedoucím jednotlivých úseků je přidělen rozpočet na přípravu materiálů pro zvyšování povědomí a školení a jejich realizaci. Jako zpětnou vazbu poskytují vedoucí úseků informace o stavu implementace SAE programu a účinnosti zavedených opatření.
- **Scénář komunikace v modelu plně decentralizovaného přístupu implementace SAE programu** – v tomto modelu zodpovídá CIO za zpracování bezpečnostní politiky a za nastavení očekáváných cílů programu budování bezpečnostního povědomí. Za provedení zbylých částí (přípravu strategie a implementaci SAE programu nesou odpovědnost vedoucí jednotlivých úseků. Od těchto pracovníků se očekává, že budou provádět hodnocení potřeb, formulovat strategii, vypracovávat plán zvyšování povědomí a školení, připravovat podpůrné a školicí materiály a implementovat program budování bezpečnostního povědomí. Na všechny zmíněné aktivity jsou jim přiděleny finanční prostředky. Pověřené osobě poskytují vedoucí úseků informace o stavu implementace SAE programu a účinnosti zavedených opatření.

Jakmile byl plán implementace programu budování bezpečnostního povědomí v organizaci relevantním osobám vysvětlen a akceptován, realizace může být spuštěna.

3.6.2 Metody šíření podpůrných materiálů pro zvyšování povědomí

Existuje nepřeberné množství technik, jak zajistit předání podpůrných materiálů pro zvyšování povědomí, a v té souvislosti také mnoho distribučních kanálů. Vybrané techniky závisí na zdrojích (zejména lidských, technologických a finančních) a složitosti jednotlivých sdělení. Z těch nejpoužívanějších si organizace může vybrat např.:

- plakáty (s jednoduchými příklady, co dělat a co nedělat, když…);

- šetřiče obrazovky;
- varovné zprávy (formou e-mailů či sms);
- propagační materiály s krátkými a výstižnými bezpečnostními motty (např. propisky, klíčenky, poznámkové bloky, záložky, informační karty, hodiny, CD příp. DVD s bezpečnostními tipy a další);
- informační bulletin;
- webová videa s instruktáží;
- videokonferenční schůzka;
- individuální rozhovory na téma informační a kybernetické bezpečnosti;
- bezpečnostní dny;
- kalendáře s informacemi o bezpečnostních kontaktech, příp. s měsíčními bezpečnostními tipy;
- křížovky;
- potištěné hrnky;
- plakety.

Při výběru konkrétní metody vhodné pro zvyšování povědomí je třeba dbát na obsah sdělení, kterým chce organizace dosáhnout požadovaného cíle. V případě šíření jediné zprávy lze využít např. informační plakáty, varovné bannery, tištěný jednostránkový bulletin nebo hromadné e-mailové zprávy. Mezi techniky vhodné pro poskytnutí více zpráv patří např. zprávy typu „co dělat a nedělat, když…“, vícestránkové bulletiny, webová videa, telekonferenční sezení nebo individuální rozhovory.

Použití jednotlivých metod je závislé na přiděleném objemu finančních prostředků. Z těch méně nákladných technik lze využít např. plakáty, spořiče obrazovky, výstražné bannery, krátké tištěné materiály, program odměn (např. plakety, hrnky, frisbee), společné schůzky a rozhovory. Vzor bezpečnostního plakátu se nachází v příloze č. 2. Naopak za dražší metody jsou považovány telekonferenční jednání, webová videa, vícestránkové informační bulletiny, propagační materiály.

Kromě zajištění požadavků na aktuálnost, vhodnost a přiměřenost sdělení podpůrných materiálů je považováno za důležité opakování daného tématu, a proto se doporučuje používat různé způsoby prezentace jedné zprávy, tzn. kombinovat metody, což může výrazně zvýšit bezpečnostní povědomí uživatelů. Kupříkladu diskuse s instruktorem

o zamezení útoku sociálního inženýrství může být doplněna plakáty nebo pravidelnými hromadnými e-mailovými zprávami v rámci organizace.

3.6.3 Metody poskytování školicích materiálů

Druhý stupeň programu budování bezpečnostního povědomí zahrnuje školení. Jako podklad pro uživatele se zpracovávají vzdělávací materiály. Techniky pro efektivní poskytování těchto materiálů by měly využívat technologii, která odpovídá následujícím znakům:

- snadné použití (tzn. snadný přístup, aktualizace a údržba);
- škálovatelnost (použití pro různě velkou cílovou skupinu na různých místech);
- zodpovědnost (pravdivost sdělení podložit informacemi ze statistik);
- široká základna podpory (dostatečný počet potenciálních dodavatelů).

Mezi běžně používané techniky budování bezpečnostního povědomí na úrovni školení patří:

- **Interaktivní video výcvik** – jedná se o jednu z několika metod distančního učení. Tato technologie podporuje obousměrné interaktivní audio i video instrukce. Interaktivní funkce činí techniku užitečnější, ovšem na druhou stranu také dražší.
- **Trénink založený na webové aplikaci** – tato technika je v současné době jednou z nejoblíbenějších pro distribuovaná prostředí. Účastníci webové relace mohou studovat samostatně a učit se vlastním tempem. Testovací a odpovědnostní funkce mohou být postaveny na měření výkonnosti. Některé testovací modely, zahrnující tuto techniku, začínají poskytovat další přínos, a to interakci mezi instruktorem a žákem nebo mezi žáky.
- **Trénink prostřednictvím informačních technologií (zejména počítače) bez přístupu k internetu** – tato technika je navzdory dostupnosti dat prostřednictvím webových aplikací stále populární. I nadále se považuje za účinnou metodu pro distribuci školicích materiálů. Stejně jako předchozí technika, ani tato neumožňuje vzájemnou interakci mezi instruktorem a žákem, ev. více žáky.

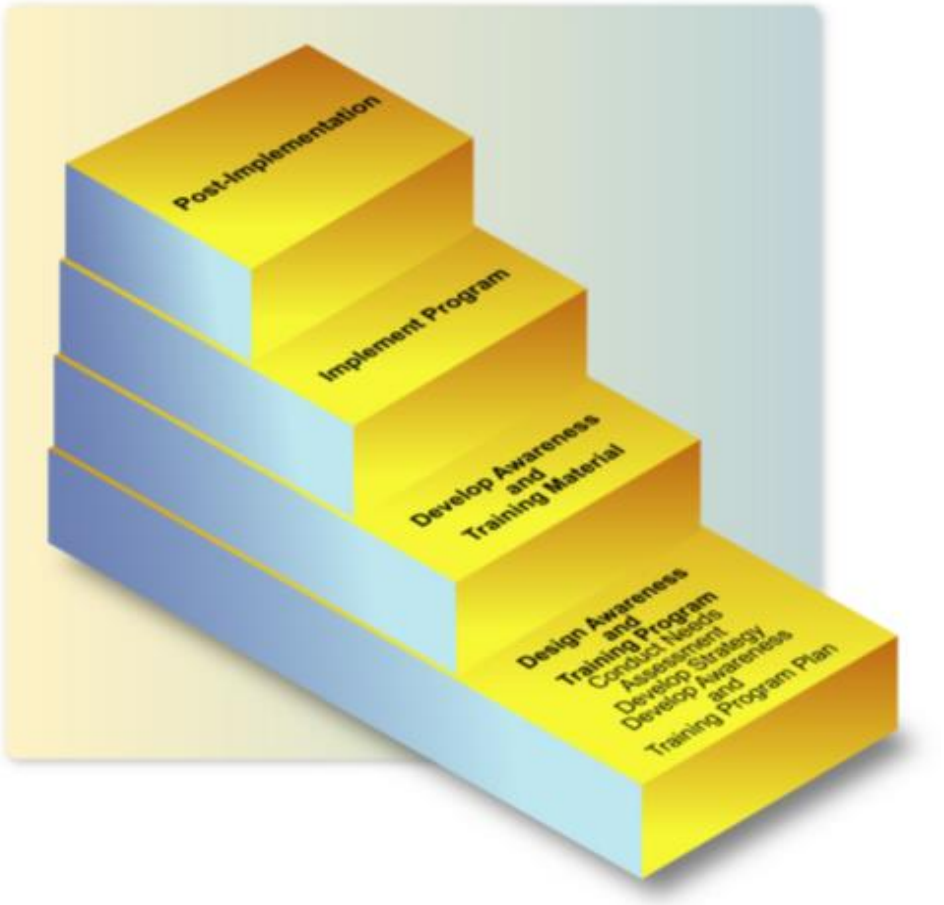
- **Školení na pracovišti prováděné instruktorem** (včetně odborné prezentace a mentoringu) – jedná se o jednu z nejstarších a současně stále jednu z nejoblíbenějších metod pro šíření školicích materiálů cílové skupině. Bezesporu největší výhodou této techniky je interaktivní povaha výcviku. Na druhou stranu má i svá negativa. Ve velké organizaci mohou nastat při plánování rozdělení uživatelů potíže se zajištěním prostor pro účast všech cílových skupin. V organizacích, které mají zastoupení v různých geografických oblastech, mohou být v souvislosti s potřebou přemístění vysoké cestovní náklady pro instruktory i žáky. Navzdory všem nevýhodám stále většina uživatelů upřednostňuje tuto tradiční metodu oproti ostatním.

Sloučením a kombinací různých technik výcviku lze déle udržet pozornost účastníků školení. To může v organizaci vést k vyšší efektivitě při budování bezpečnostního povědomí. Například zobrazování videí během školení vedeného instruktorem umožňuje účastníkům soustředit se na jiný zdroj informací. Video záznam může zvýšit důraz na problematiku, kterou instruktor předkládá.

3.7 Post-implementační fáze

Po implementaci SAE programu prostřednictvím zvyšováním povědomí a realizací školení následuje fáze, které je potřeba věnovat minimálně stejnou pozornost jako všem předchozím. Program budování bezpečnostního povědomí může vlivem neustálých změn reality poměrně rychle zastarat. To nastane, nebude-li věnována dostatečná pozornost technologickému pokroku, vývoji infrastruktury IT, anebo organizačním změnám, posunům v prioritách či poslání samotné organizace. Správce SAE programu a osoba odpovědná za přípravu a správu školení musí mít tyto potenciální problémy na zřeteli a umět včas a správně zareagovat. Zahrnutím vhodně zvolených mechanismů do strategie SAE programu lze zajistit, že program budování bezpečnostního povědomí zůstane relevantní a bude v souladu s cíli organizace.

Neustálé zlepšování by mělo být tématem jak na úrovni zvyšování povědomí, tak i z pohledu školení, jelikož se jedná o oblast, kde „nikdy nemůžete udělat dost“.



Obr. 18: Fáze SAE programu [15]

3.7.1 Shoda plánu s realizací SAE programu

Jakmile se uskutečnila fáze implementace SAE programu, musí být stanoveny a zavedeny procesy, které sledují shodu realizace programu budování bezpečnostního povědomí s plánem a její úspěšnost. Vhodným nástrojem je automatizovaný sledovací systém, který by měl být navržen tak, aby zachytil klíčové informace o aktivitách SAE programu, a to uskutečněné vzdělávací akce a jejich obsah, přehled účastníků, výši nákladů a použité zdroje. Sledovací systém by měl všechna tato data obsahovat, aby byl využitelný k poskytování analýzy celé organizace a podávání zpráv o iniciativách zaměřených na budování bezpečnostního povědomí. Požadavky na databázi by měly zahrnovat potřeby všech relevantních uživatelů. Mezi typické uživatele této databáze patří:

- **správce SAE programu** – osoba v této roli může databázi využít k podpoře strategického plánování, informování managementu organizace a vedoucích úseků o aktuálnosti programu budování bezpečnostního povědomí včetně podpůrných a školicích materiálů, identifikaci možností a kritických potřeb vedoucích pracovníků, provádění analýzy SAE programu, identifikaci aktivit programu budování bezpečnostního povědomí v rámci celé organizace a potřeb zlepšování SAE programu, posuzování shody plánu a realizace SAE programu a jako podpůrný informační zdroj při zajišťování bezpečnosti a čerpání a alokaci finančních prostředků;
- **úsek IT a bezpečnostních pracovníků** – tito zaměstnanci mohou využít databázi k podpoře plánování bezpečnosti, poskytování zpráv o stavu bezpečnostního povědomí CIO, managementu organizace a ostatním vedoucím úseků, zdůvodnění žádosti o přidělení finančních prostředků, prokázání splnění stanovených cílů, identifikaci zdrojů pro zvyšování povědomí a školení, identifikaci aktuálního stavu realizace SAE programu, provedení úprav kritických opomenutí a jako informační zdroj pro zodpovězení otázek týkajících se bezpečnostního povědomí;
- **úsek lidských zdrojů** – pracovníci z tohoto úseku mohou využít databázi k zachycení veškerých informací o uskutečněných vzdělávacích akcích na téma zvyšování povědomí a realizovaných školeních, určení nákladů souvisejících s výcvikem v oblasti budování bezpečnostního povědomí, hlášení o stavu podpory, identifikaci aktuálního stavu realizace SAE programu a jako informační zdroj pro zodpovězení otázek týkajících se bezpečnostního povědomí a pomoc v profesionálním rozvoji;
- **CIO (osoba odpovědná za přípravu a správu školení)** – tato osoba může využít databázi jako informační podklad pro přípravu a úpravy strategie SAE programu, ke stanovení požadavků na školení týkající se bezpečnostních směrnic, identifikaci možných zdrojů školení, podpoře žádosti o školení, určení relevance a popularizace vzdělávacích akcí a jako informační zdroj pro zpracování rozpočtů jednotlivých výcviků a pro zodpovězení otázek týkajících se bezpečnostního povědomí;

- **vedoucí jednotlivých úseků** – tito pracovníci mohou využít databázi ke sledování pokroku ve výcviku svých podřízených a podle potřeby plány vzdělávacích akcí upravovat, získávání zpráv o aktuálním stavu SAE programu, možnosti reagovat na dotazy týkající se bezpečnostních výcviků a školení v rámci svých úseků, určování zdrojů školení a finančních nákladů a jako informační zdroj pro zodpovězení otázek týkajících se bezpečnostního povědomí a pomoci v profesionálním rozvoji;
- **auditoři** – pracovníci v této roli mohou využívat informace z databáze k monitorování souladu s bezpečnostními směrnicemi a deklarovanými postupy v organizaci;
- **finanční ředitel** – tato osoba může využít informace z databáze k zodpovídání dotazů týkajících se rozpočtu a alokace finančních prostředků na jednotlivé aktivity budování bezpečnostního povědomí, jako informační zdroj při finančním plánování a k poskytnutí zpráv managementu organizace o financování dílčích částí SAE programu.

Sledování shody realizace SAE programu s původním plánem zahrnuje posouzení stavu programu budování bezpečnostního povědomí a jeho mapování z pohledu protnutí se směrnicemi organizace a používanými normami. Zprávy o stavu a dílčích aktivitách SAE programu lze z databáze generovat a používat k identifikaci mezer, ev. problémů. V návaznosti na zjištění neshod mohou být podniknuty nápravné kroky. Ty mohou mít podobu formálních připomínek, potřeby další osvěty ve zvyšování bezpečnostního povědomí či školení nebo nabídky vzdělávání, anebo zavedení opravného plánu s harmonogramem realizace a plánovaným termínem dokončení.

3.7.2 Hodnocení SAE programu a zpětná vazba

Formální hodnocení a mechanismy zpětné vazby jsou kritickými součástmi jakéhokoliv programu budování bezpečnostního povědomí. Proces neustálého zlepšování nemůže nastat bez dobrého úmyslu vedoucího k zajištění fungování stávajícího SAE programu. Mechanismus zpětné vazby musí být nastaven tak, aby řešil původní stanovené cíle programu budování bezpečnostního povědomí. Strategie zpětné vazby může být navržena a implementována teprve poté, co jsou ustáleny a zakotveny základní

požadavky. Následující obrázek znázorňuje různé mechanismy hodnocení a získávání zpětné vazby, které lze k aktualizaci SAE programu a jeho plánu použít.

Obr. 19: Mechanismy hodnocení SAE programu a zpětné vazby [15]

Strategie zpětné vazby musí obsahovat prvky, které se budou zabývat jakostí, rozsahem, metodou zavádění (metody realizace školení – např. trénink založený na webové aplikaci, interaktivní video výcvik nebo školení na pracovišti prováděné instruktorem a další), úrovní obtížnosti, vhodností použití, délkou trvání dané vzdělávací akce, relevancí, náklady a návrhy na změnu.

Pro zajištění zpětné vazby lze použít mnoho různých metod. Mezi ty nejběžnější patří následující metody.

- **Formuláře pro hodnocení / dotazníky** – je možné použít různé formáty. Nejlepší návrhy eliminují potřebu rozepisování se ze strany účastníka vzdělávací akce. Klíčem k získání relevantní zpětné vazby je navrhnout formuláře tak, aby byly co nejvíce „uživatelsky přívětivé“. Při jejich vytváření se doporučuje spolupracovat s odborníky, kteří jsou obeznámeni s nejlepšími praktikami pro sestrojení těchto hodnoticích nástrojů, ev. je možné je alespoň požádat o rady a tipy.

- **Focus groups**[6] – vytvořené podpůrné a školicí materiály jsou předneseny určité skupině odborníků (o velikosti cca 8-10 osob), kteří diskutují o jejich perspektivách či efektivnosti a dávají podněty k úpravě materiálů a jejich vylepšení.
- **Řízené rozhovory** – tento přístup nejprve identifikuje cílové skupiny pro vzdělávání na základě dopadu, priority nebo jiných předem stanovených kritérií a určuje specifické oblasti pro zpětnou vazbu. Obvykle probíhají ve formě rozhovorů jeden na jednoho, ev. v malých homogenních skupinách (obvykle méně než 10 osob).
- **Nezávislá pozorování / analýzy** – dalším možným přístupem k získání zpětné vazby je udělení pokynu o sledování programu budování bezpečnostního povědomí včetně monitoringu vzdělávacích akcí jako úkol externímu dodavateli nebo jiné třetí straně v rámci auditu iniciovaného organizací. Kromě běžných kontrolních aktivit tak zástupci organizace činí, aby získali nestranný názor na efektivitu SAE programu.
- **Status reporty (formální hlášení o stavu)** – jedním z vhodných způsobů, jak se zaměřit na monitoring zvyšování bezpečnostního povědomí a uskutečněných školení v organizaci, je zavést požadavek na pravidelné reporty o stavu SAE programu zpracovávané vedoucími jednotlivých úseků.
- **Benchmarking**[7] - mnoho organizací považuje porovnávání vybraných ukazatelů za součást své strategie neustálého zlepšování a úsilí o „dosažení dokonalosti“. Tento typ benchmarkingu je zaměřen na otázku „Jak se hodnotím ve srovnání s ostatními účastníky?“. Externě zaměřená forma benchmarkingu v oblasti budování bezpečnostního povědomí porovnává výkonnost organizace na základě pozorovaných základních údajů, které jsou v daném momentu k dispozici, s řadou dalších organizací a tím poskytuje zpětnou vazbu managementu organizace. Tento typ benchmarkingu obvykle provádí odborníci na tuto oblast,

[6] Focus groups – jedná se o jednu z metod získávání dat především v kvalitativním výzkumu, kdy je do diskuse na určité téma zapojeno cca 8-10 osob a mentor vedoucí diskusi, tato metoda se používá např. při zjišťování motivů jednání, informací kvalitativního charakteru, tvorbě hypotéz.

[7] Benchmarking – je metoda založená na systematickém měření a porovnávání vybraných ukazatelů, základem je porovnání indikátorů vůči jiným referenčním hodnotám, které mohou být buď historické, nebo mohou být porovnávány vůči jinému referenčnímu subjektu.

kteří jsou schopni se dostat k rozsáhlým informacím v široké škále organizací za poměrně dlouhou dobu (pět let a více).

3.7.3 Správa změn

Řízení změn je součástí programu budování bezpečnostního povědomí, jehož cílem je zajistit, aby zvyšování povědomí, školení a vzdělávání se nestaly stagnujícími, a v důsledku toho pozbyly relevance pro skutečně vznikající problémy, kterým organizace čelí. Systém řízení změn je navržen takovým způsobem, aby řešil změny v bezpečnostní politice a postupech, které se odrážejí v kultuře organizace.

Do budoucna je potřeba zajistit, aby byl SAE program stále stejně strukturován a průběžně aktualizován z důvodu stále se objevujících nových a nových informačních technologií a s tím souvisejících bezpečnostních problémů. Požadavky na zvyšování povědomí a školení rozvíjejí o nové znalosti a dovednosti nezbytné k tomu, aby uživatelé dokázali reagovat na nové technologické změny. Změny v poslání organizace, příp. jejích cílech, mohou také ovlivnit smysl, rozložení a obsah jednotlivých vzdělávacích akcí.

Stále aktuálnější problémy, jako je např. obrana vlasti, budou také mít vliv na povahu a rozsah činností týkajících se povědomí o bezpečnosti, které jsou nezbytné k tomu, aby byli uživatelé informováni o nejnovějších praktikách a uplatňovaných protiopatřeních. Zároveň nové zákony a normy mohou mít také dopad na agendu budování bezpečnostního povědomí a obsah podpůrných a školicích materiálů. Dalším faktorem, který se v průběhu času vyvíjí a mění, jsou změny směrnic v organizaci. Tyto změny by se taktéž měly odrazit v obsahu vzdělávacích materiálů.

3.7.4 Neustálé zlepšování SAE programu

Tato fáze programu budování bezpečnostního povědomí je zaměřena na vytváření vyšší úrovně bezpečnostního povědomí a excelence řešených témat, které se dosahuje prostřednictvím všudypřítomného vnímání této problematiky v organizaci. Procesy, které poskytují jednotlivým cílovým skupinám zvyšování povědomí, školení a vzdělávání, by měly být zcela začleněny do celkové strategie organizace. Vyvinutý

SAE program definuje soubor metrik pro tuto oblast a stanovuje, že by měly být zavedeny automatizované sledovací systémy, které by podporovaly zachycování kvantitativních i kvalitativních dat a poskytovaly informace odpovědným osobám a vedoucím jednotlivých úseků v předem stanovených pravidelných intervalech.

V této fázi organizace začleňují do svého programu budování bezpečnostního povědomí formální mechanismy pro průběžný výzkum v oblastech technologického pokroku, osvědčených postupů a příležitostí pro srovnávání.

3.7.5 Ukazatele úspěšnosti SAE programu

Správce SAE programu a osoba odpovědná za přípravu a správu školení by měli být primární obhájci a iniciátoři neustálého zlepšování a podpory programu budování bezpečnostního povědomí v organizaci. Klíčovým faktorem úspěchu SAE programu je, aby každý byl schopen a ochoten vykonávat svěřenou bezpečnostní roli v organizaci. Pravidlo „organizace je tak silná jako její nejslabší článek“ platí i v oblasti bezpečnosti. Zabezpečení informací a infrastruktury organizace je týmovým úsilím. Níže jsou uvedeny některé klíčové ukazatele pro posouzení podpory a přijetí SAE programu. Mezi ně patří:

- dostatečné finančních prostředky na realizaci strategie SAE programu;
- vhodné přidělení rolí a odpovědností, které umožní osobám s klíčovými povinnostmi efektivně implementovat strategii SAE programu;
- podpora různých distribučních kanálů (např. web, e-mail, tištěné a propagační materiály a další) a zveřejňování informací o informační a kybernetické bezpečnosti;
- zprávy zaměstnancům o budování bezpečnostního povědomí (obsah může být sdělován i prostřednictvím schůzek);
- použití metrik (např. označení poklesu bezpečnostních incidentů nebo porušení značí, že se zmenšuje rozdíl mezi stávajícím povědomím a záměrem realizovaných výcviků a vzdělávacích akcí a zjištěnými potřebami, zvyšuje se procento uživatelů vystavených podpůrným a školicím materiálům a procento uživatelů s náležitě vyškolenými bezpečnostními povinnostmi);

- vedoucí jednotlivých úseků nepoužívají svůj status v organizaci, aby se vyhnuli bezpečnostním kontrolám, které jsou důsledně dodržovány;
- úroveň účasti na povinných bezpečnostních vzdělávacích akcích;
- uznávání dodržení bezpečnostních pravidel (např. ocenění, plakety);
- motivace demonstrovaná osobami, které hrají klíčovou roli při řízení a koordinaci programu budování bezpečnostního povědomí.

Závěr

Zajištění bezpečnosti aktiv organizace vůči hrozbám a útokům okolí je tématem stále aktuálním. Problém představuje nejen krádež dlouhodobého, krátkodobého a finančního majetku, ale čím dál tím častěji ztráta a zcizení dat a know-how. Rizika se v dnešní době neobjevují jen ve fyzickém světě. S existencí kyberprostoru přichází útoky také prostřednictvím připojení k internetu, a pokud si někdo myslí, že se ve světě neválčí, nechť navštíví webové stránky společnosti Fortinet, kde může v reálném čase sledovat množství kybernetických útoků, které se právě ve světě odehrávají.

Abychom dokázali těmto hrozbám čelit, je potřeba se chránit. Existují tři pohledy na bezpečnost organizace, a sice bezpečnost objektu, informací a kybernetická bezpečnost. Klíčovým kritickým faktorem jsou v procesu zajištění bezpečnosti všech aspektů organizace lidé. V rámci prevence se jako vhodný nástroj ukazuje program budování bezpečnostního povědomí. Každá organizace v České republice k tomuto tématu přistupuje po svém. Patrně se tak děje z důvodu, že v našem prostředí neexistuje žádná norma, legislativní dokument nebo nařízení, které by oblast budování bezpečnostního povědomí řešilo komplexně.

Protože mě téma ochrany a bezpečnosti dat zajímá, pokusila jsem se ve své diplomové práci návrh metodiky budování bezpečnostního povědomí vypracovat a jako cílovou skupinu jsem si vybrala střední školy, a to hned z několika důvodů. Jednak se domnívám, že dospívající populace bere aktuální situaci v kybernetickém prostoru na lehkou váhu a současně si myslím, že si tato cílová skupina neuvědomuje dopad svého jednání, např. na sociálních sítích. Zároveň jsou to právě pedagogové, kteří žáky učí všeobecným znalostem i odborným dovednostem a právě oni by se měli zajímat o aktuální situaci a být řádně proškoleni, jak se zachovat v případě, že nastane bezpečnostní incident. Tyto a mnohé další důvody mě inspirovaly ke zpracování metodiky budování bezpečnostního povědomí, podle které by mohly postupovat všechny střední školy v České republice.

Nejprve jsem se zaměřila na teoretická východiska a základní stavební kameny, na kterých lze bezpečnostní povědomí vybudovat a dále rozvíjet. Uvedla jsem základní terminologii používanou v této oblasti. Zmínila jsem také existující či připravované

české i mezinárodní zákony, normy, předpisy a certifikace, jež poskytují této problematice určitý rámec.

Podařilo se mi navázat spolupráci se zástupci konkrétní střední školy, což mi pomohlo k relevantním informacím a reálnému pohledu na rizika a možnosti uživatelů a bezpečnostní požadavky. S pomocí vedení střední školy jsem provedla analýzu současného stavu budování bezpečnostního povědomí v organizaci. Veškerá zjištění pro mě byla vstupními informacemi pro návrh metodiky.

Pro utřídění myšlenek o rozsahu a obsahu jednotlivých dílčích částí metodiky jsem si vytvořila myšlenkovou mapu, která mi pomohla držet se daného tématu a nezabíhat do přílišných podrobností a přitom zpracovat komplexní a ucelený materiál o budování bezpečnostního povědomí na střední škole.

Zároveň mi při zpracovávání tohoto tématu byly ku prospěchu mé znalosti strategických dokumentů zabývajících se digitální gramotností (Strategie digitálního vzdělávání a Strategie digitální gramotnosti v ČR) a mnohaleté pracovní zkušenosti z oblasti školství, spolupráce se zástupci významných IT společností a škol zabývajících se výukou informačních a komunikačních technologií a dále pak zkušenosti s přípravou systémového projektu orientovaného na další vzdělávání v digitálních kompetencích, jehož výstupy v podobě vzdělávacích modulů by bylo možné převzít a implementovat v rámci zvyšování povědomí a školení vedoucích k získání přenositelných a specifických digitálních kompetencí týkajících se informační a kybernetické bezpečnosti.

Pevně věřím, že jsem splnila všechny cíle, které jsem si v úvodu diplomové práce stanovila, a že zpracovaný návrh metodiky budování bezpečnostního povědomí na středních školách bude inspirací, jak k takto složitému tématu mohou střední školy přistupovat.

Seznam použité literatury

[1] ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky – Systémy řízení informací - Přehled a slovník*. Třetí vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

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

[4] ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Soubor postupů pro opatření bezpečnosti informací.* Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[5] ČESKÁ REPUBLIKA. *Usnesení vlády č. 781/2011: o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast*. Praha: Vláda České republiky, 2011.

[6] ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb.: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů*. Praha, 2014, ročník 2014, částka 75, číslo 181.

[7] GRASSEOVÁ, Monika, Radek DUBEC a Roman HORÁK. *Procesní řízení ve veřejném sektoru: teoretická východiska a praktické příklady*. Brno: Computer Press, 2008. ISBN 978-80-251-1987-7.

[8] KNESL, Jiří. *SprintMethod: agilní metodika vycházející ze Scrumu* [online]. Copyright © 2012 [cit. 2017-04-30]. Dostupné z: http://www.sprintmethod.cz/.

[9] KORNELLY, A. *Budování bezpečnostního povědomí na střední a vyšší odborné škole*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 88 s. Vedoucí diplomové práce Ing. Petr Sedlák.

[10] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[11] ISO/IEC 27001:2013. *Information technology – Security techniques – Information security management systems – Requirements* [online]. Praha: © 2017 Risk Analysis Consultants, 2017 [cit. 2017-05-07]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27001

[12] ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[13] ČESKÁ REPUBLIKA. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679: o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník Evropské unie*. 2016.

[14] About NIST. National Institute of Standards and Technology: U.S. Department of Commerce [online]. Gaithersburg: NIST, 2016 [cit. 2017-05-10]. Dostupné z: https://www.nist.gov/about-nist

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

[16] 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.

[17] Třídy norem ČSN: 01 OBECNÁ TŘÍDA NOREM. *Technické normy* [online]. Technické normy.cz [cit. 2017-05-12]. Dostupné z: https://www.technickenormy.cz/tridy-norem-csn/01-obecna-trida/

[18] ISACA Czech Republic Chapter. *ISACA Czech Republic Chapter: Serving IT Governance Professionals* [online]. © 2008 ISACA Czech Republic Chapter [cit. 2017-05-12]. Dostupné z: http://www.isaca.cz/cs/isaca-crc

[19] ISACA Certification: IT Audit, Security, Governance and Risk. *ISACA: Trust in, and value from, information systems* [online]. © 2017 ISACA, 2017 [cit. 2017-05-12]. Dostupné z: http://www.isaca.org/CERTIFICATION/Pages/default.aspx

[20] ECDL – Mezinárodní standard pro digitální znalosti a dovednosti. *ECDL Czech Republic* [online]. © 1999-2017 ČSKI, 2017 [cit. 2017-05-12]. Dostupné z: http://www.ecdl.cz/index.php

[21] *Revoluce dovedností: Jak digitalizace a robotizace navždy změní zaměstnanost* [online]. © 2016 Manpower Group, 2016, 8 s. [cit. 2017-05-13]. Dostupné z: https://www.manpower.cz/manpower/wp-content/uploads/2017/01/revoluce-dovednosti.pdf

[22] Pro zájemce o studium: Historie školy. *Střední škola* [online]. [cit. 2017-05-13]. Dostupné z: https://www.stredniskola.cz/informace-pro-zajemce-o-studium-historie-skoly

[23] Pro zájemce o studium: Informace ze zákona. *Střední škola* [online]. [cit. 2017-05-13]. Dostupné z: https://www. stredniskola.cz/informace-pro-zajemce-o-studium-informace-ze-zakona

[24] Kybernetická bezpečnost: Obor vzdělání. *Střední škola* [online]. [cit. 2017-05-13]. Dostupné z: https://www.stredniskola.cz/menu-kyberneticka-bezpecnost-obor-vzdelani

[25] Kdo je Network Security Monitoring Cluster. *NSM (C): Network Security Monitoring Cluster* [online]. [cit. 2017-05-13]. Dostupné z: http://www.nsmcluster.com/

[26] O nás. *KYBEZ: Platforma kybernetické bezpečnosti* [online]. Copyright © GORDIC, 2017 [cit. 2017-05-13]. Dostupné z: https://www.kybez.cz/o-nas

[27] ČESKÁ REPUBLIKA. Zákon č. 262/2006 Sb.: zákoník práce. In: *Sbírka zákonů*. 2006, ročník 2006, částka 84, číslo 262.

Seznam použitých zkratek

CGEIT	Certified in the Governance of Enterprise IT
CIO	Chief Information Officer, pro potřeby této práce se jedná o osobu odpovědnou za přípravu a správu školení
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CRISC	Certified in Risk and Information Systems Control
ČR	Česká republika
ČSN	Česká technická norma
ECDL	Mezinárodní standard pro digitální znalosti a dovednosti
ESF	Evropské strukturální fondy
EU	Evropská unie
GDPR	Obecné nařízení na ochranu osobních údajů
ICT	Informační a komunikační technologie
ID	Identifikační údaje
IEC	Mezinárodní elektrotechnická komise
IoT	Internet věcí
IS	Informační systém
ISACA	Information Systems Audit and Control Association
ISMS	Systém řízení bezpečnosti informací
ISO	Mezinárodní organizace pro normalizaci
IT	Informační technologie
LAN	Lokální síť
NBÚ	Národní bezpečnostní úřad
NIST	Národní institut standardů a technologie
OSI	Propojení otevřených systémů
SAE	Budování bezpečnostního povědomí
SP	Special Publication
USA	Spojené státy americké
VPN	Virtuální privátní síť
WAN	Rozsáhlá síť

Seznam obrázků, grafů a tabulek

Seznam příloh

Příloha 1 - Dotazník pro hodnocení potřeb

Název organizace: …….
Název pracovní pozice: …….
Datum: …….

Tento dotazník slouží k zjištění znalostí, dovedností a zkušeností, které potřebujete pro správu automatizovaných informačních systémů a sítí vaší organizace. Jde o zjištění pracovních činností, které vykonáváte, jak jste se jim naučili a o druzích školení, o kterých si myslíte, že by vám nejlépe prospěly pro efektivnější výkon Vašich činností. Informace, které poskytnete, budou použity k vytvoření bezpečnostního školení. Vyplnění dotazníku zabere přibližně 30 minut.

Část první (nehodící se škrtněte)

1) Pracujete v současné době jako správce systému? Ano Ne
   a. Pokud ano, děláte práci na plný úvazek? Ano Ne
2) Jak dlouho pracujete jako správce systému? .... let …. měsíců
3) Máte formální vzdělání v oblasti správy systému? Ano Ne
   a. Pokud ano, uveďte níže jaké
      ……
4) Máte formální vzdělání v oblasti zabezpečení systému? Ano Ne
   a. Pokud ano, uveďte níže jaké
      ……
5) Kolika seminářů nebo konferencí týkajících se správy systému nebo bezpečnosti informačních systémů jste se zúčastnil/a v loňském roce? …….
6) Čtete pravidelně odborné časopisy zabývající se problematikou související s Vaší profesí? Ano Ne
   a. Pokud ano, uveďte níže jaké
      ……

Část druhá: Výkon pracovních činností

Pro každý úkol ve sloupci A zakroužkujte písmeno ve sloupci B, které udává, jak často provádíte úkol: O – nikdy, L - méně než jednou za měsíc, M – měsíční, T – týdenní, D - denně		Označte způsob, jakým jste se dovednostem naučil/a (u „ostatní“ uveďte jiný způsob, např. workshop, konference a další)	U každého úkolu zakroužkujte úroveň znalostí a dovedností, které považujete za potřebné pro výkon pracovních
A	B		

			činností Z – základní S – středně pokročilý P - pokročilý
Správa hardwaru (HW)			
Plánování instalace HW	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Nákup HW	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Rozmístění HW	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Zajištění údržby HW	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Oprava HW	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Instalace HW	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Diagnostika HW	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa operačního systému			
Optimalizace operačního systému	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Plánování změn systému	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Uvést systém do původního nastavení	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Testování systému	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa příkazových souborů	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa postupů spouštění a	O L M T D	ve škole v práci	Z S P

vypnutí systému		samostudiem	ostatní ……..	
Instalace operačního systému	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Instalace změn operačního systému	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Instalace specifického HW dodavatele	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Instalace aktualizací a oprav	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Správa dokumentace o systému	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Správa a uchovávání dat				
Plánování struktury uchovávání dat	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Plánování postupů zálohování	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Implementace postupů zálohování	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Monitorování ukládání dat	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Zajištění integrity systému souborů	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Audit systému souborů	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Odstranění nepotřebných souborů	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Údržba rozložení ukládání dat	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Formátování paměťových médií	O L M T D	ve škole samostudiem	v práci ostatní	Z S P

		……..	
Načítání dat	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Obnovení dat ze zálohy	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa aplikačního softwaru (SW)			
Hodnocení efektivity SW balíčků	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Optimalizace parametrů aplikací	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Plánování změn aplikací	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Zajištění kompatibility mezi aplikacemi	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Přidělení systémových zdrojů aplikacím	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Ověření integrity aplikací před instalací	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Testování instalace SW	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Instalace aplikačního softwaru	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa aplikační dokumentace	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Instalace aktualizací aplikací	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Plánování připojení k síti	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Získání domény	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P

Sestavení síťových kabelů	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Konfigurace souborových serverů a klientů	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Konfigurace firewallů	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Sledování aktivity sítě	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Správa síťových služeb	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Správa síťových mostů a směrovačů	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Správa topologie sítě	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Přiřazení adres uzlům	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Instalace síťového SW	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Nastavení přístupových oprávnění	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Spuštění síťového SW	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Testování komunikačního připojení	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Stanovení pokynů pro audit	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Nastavení pokynů pro zabezpečení uživatelů	O L M T D	ve škole samostudiem	v práci ostatní ……..	Z S P
Součinnost při testování bezpečnostních mechanismů	O L M T D	ve škole samostudiem	v práci ostatní	Z S P

		……..	
Součinnost při analýze kontrolních záznamů	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Součinnost při řešení incidentů	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa fyzické bezpečnosti systému	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Hlášení bezpečnostních incidentů	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa účtů			
Plánování strategie správy účtů	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Tvorba přihlašovacího prostředí pro uživatele	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa oprávnění účtu	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Vysvětlení základních provozních postupů	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Součinnost při úpravě hesla	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Odstranění účtu	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Řešení problémů			
Interpretace problémového scénáře	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Interpretace chybových hlášek	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Správa přehledu problémů a jejich řešení	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Obnovení zařízení po havárii systému	O L M T D	ve škole v práci samostudiem ostatní	Z S P

		……..	
Schopnost reagovat na problémy identifikované uživatelem	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Použití diagnostických nástrojů	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
Provedení nápravných opatření	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P

Do tabulky níže označte další úkony při správě systému, které provádíte, a nejsou uvedeny výše. U každého z nich uveďte, jak často provádíte úkol, primární způsob, jakým jste byli vyškoleni k výkonu této práce.

Pro každý úkol ve sloupci A zakroužkujte písmeno ve sloupci B, které udává, jak často provádíte úkol: O – nikdy, L - méně než jednou za měsíc, M – měsíční, T – týdenní, D - denně		Označte způsob, jakým jste se dovednostem naučil/a (u „ostatní“ uveďte jiný způsob, např. workshop, konference a další)	U každého úkolu zakroužkujte úroveň znalostí a dovedností, které považujete za potřebné pro výkon pracovních činností Z – základní S – středně pokročilý P - pokročilý
A	B		
	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P
	O L M T D	ve škole v práci samostudiem ostatní ……..	Z S P

Příloha 2 - Vzor plakátu s bezpečnostní tematikou

Tipy pro bezpečnost informací

1) **Zabezpečte přístup k datům**

Nejen fyzická ochrana dat, ale i zabezpečení pomocí identifikace.

2) **Používejte silná hesla**

Kombinujte písmena s čísly, znaky a symboly.

3) **Zálohujte**

Vaše data budou v bezpečí a předejdete tím jejich ztrátě.

4) **Používejte antivirové programy**

Instalujte je, používejte a udržujte je aktuální.

5) **Šifrujte**

Chraňte veškerou komunikaci (e-maily, přenášená data).

6) **Neotvírejte podezřelé e-maily**

Před otevřením se ujistěte, že znáte odesílatele e-mailu.