VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

ZVÝŠENÍ BEZPEČNOSTNÍHO POVĚDOMÍ VE SPOLEČNOSTI

INCREASING SECURITY AWARENESS IN THE COMPANY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Petr Novák

AUTHOR

VEDOUCÍ PRÁCE — Ing. Viktor Ondrák, Ph.D.

SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Petr Novák**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2020/21

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:

Zvýšení bezpečnostního povědomí ve společnosti

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Návrh systému zvyšování bezpečnostního povědomí.

Základní literární prameny:

ČSN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2014.

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

KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, 2017. ISBN 978-80-88168-15-7.

KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

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

SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Diplomová práce je zaměřena na zvýšení bezpečnostního povědomí ve společnosti. První kapitola obsahuje teoretická východiska nutná k vytvoření návrhu systému vzdělávání v oblasti bezpečnosti. Druhá kapitola pojednává o analýze současného stavu, která je potřebná pro zjištění nutnosti zvýšit bezpečnostní povědomí. Třetí a poslední kapitola obsahuje samotný návrh systému vzdělávání.

Klíčová slova

informační bezpečnost, kybernetická bezpečnost, SAE, ISO, sociální inženýrství

Abstract

The master's thesis is focused on increasing security awareness in the company. The first chapter contains the theoretical background, which is necessary for creating a security education system. The second chapter deals with the analysis of the current situation, which is needed for determinating the need to increase security awareness. The third and last chapter contains the design of the education system itself.

Key words

information security, cybersecurity, SAE, ISO, social engineering

Bibliografická citace

NOVÁK, Petr. Zvýšení bezpečnostního povědomí ve společnosti [online]. Brno, 2021 [cit. 2021-05-05]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/131766. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně.

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

V Brně dne 16.května 2021

…….

Podpis studenta

Poděkování

Nejprve bych rád poděkoval panu Ing. Viktorovi Ondrákovi, Ph.D. za cenné rady, připomínky a vedení diplomové práce. Dále bych rád poděkoval svojí rodině, přátelům a partnerce za podporu při psaní celé práce.

OBSAH

ÚVOD

Informační a kybernetická bezpečnost jsou v současnosti důležitá a hojně diskutovaná témata. S narůstající digitalizací a počtem nových a neznalých uživatelů se čím dál víc našich osobních údajů objevuje volně na internetu. Při zanedbání digitální gramotnosti mohou uživatelé prozradit i údaje, která mohou být použita například pro krádež identity, nebo peněz. Techniky sociálního inženýrství jsou lehce použitelné na digitálně negramotné uživatele, kterých v současné době přibývá.

Nejen běžní uživatelé, ale i společnosti jsou ohroženy různými druhy kyberkriminality. Mnoho společností je kriticky závislých na svoji komunikační infrastruktuře. Také citlivá data mnoha firem jsou uložena v nějaké digitální podobě na serverech společnosti. Pokud by komunikační infrastruktura takové organizace byla přerušena, nebo data ukradena pomocí kybernetického útoku, způsobilo by jí to výrazné finanční ztráty, nebo ztrátu konkurenceschopnosti.

Diplomová práce se zabývá zvýšením bezpečnostního povědomí ve společnosti World Technical Hub. V první kapitole se nacházejí teoretická východiska práce, která definují veškeré pojmy a témata nutná pro pochopení analytické a návrhové části práce.

Druhá kapitola se zabývá analýzou současného stavu společnosti. Analýza popisuje společnost, identifikuje rizika a určuje zranitelnost jednotlivých aktiv. Analýza odhalí, zda je ve společnosti nutné zvýšit bezpečnostní povědomí.

Třetí a poslední kapitola obsahuje vlastní návrh projektu na zvýšení bezpečnostního povědomí. Projekt má za úkol navrhnout vhodný systém vzdělávání v oblasti bezpečnosti. Celý projekt je v kapitole naplánován s ohledem na posloupnost a časovou náročnost činností. Po navržení systému vzdělávání je celý projekt i finančně ohodnocen.

CÍL PRÁCE

Cílem diplomové práce je zvýšení bezpečnostního povědomí ve společnosti. Pro dosažení tohoto cíle je potřebné znát teoretická východiska v oblasti informační bezpečnosti a řízení projektu, ze kterých je potřeba vytvořit vhodný systém vzdělávání.

Pro zjištění relevantnosti cíle je také zapotřebí provést analýzu současného stavu, ze které vyplyne potřeba zvýšit bezpečnostní povědomí. Tato potřeba je určena z rizikových aktiv, která jsou ohrožena právě nedostatkem bezpečnostního povědomí.

1 TEORETICKÁ VÝCHODISKA PRÁCE

První kapitola diplomové práce pojednává o teoretických východiscích, která jsou nutná pro pochopení analytické a návrhové části práce. Kapitola uvádí základní pojmy, normy, organizace a modely v oblasti informační bezpečnosti a řízení projektu.

1.1 Základní pojmy

Aktivum – veškerý hmotný a nehmotný majetek organizace (1, s.15).

Bezpečnost informací – zachování integrity, důvěrnosti a dostupnosti informací (1, s.15).

Bezpečnostní funkce – funkce produktu přispívající k jeho bezpečnosti (1, s.15).

Bezpečnostní mechanismus – mechanismus používaný pro implementaci bezpečnosti (1, s.15).

Dopad – vzniklá škoda působením hrozby (1, s.16).

Dostupnost – zajištění přístupnosti k informacím autorizovanému uživateli v nutný okamžik (1, s.15).

Důvěrnost – zajištění přístupnosti k informacím pouze autorizovanému uživateli (1, s.15).

Hrozba – událost, která ohrožuje bezpečnost informací (1, s.15).

Bezpečnostní událost (Security Event) – jedná se o stav systému, sítě nebo služby, který poukazuje na možnost selhání bezpečnostních opatření, nebo porušení bezpečnostní politiky (1, s.17).

Bezpečnostní incident (Security Incident) – nestandardní bezpečnostní událost, vede k narušení pravidel bezpečnosti v organizaci (1, s.17).

Integrita – zajištění úplnosti a správnosti informace (1, s.15).

Riziko – pravděpodobnost, že hrozba způsobí incident. Jedná se o kombinaci zranitelnosti a hrozby s vlivem na aktivum (1, s.16).

Míra rizika – očekávaný pravděpodobný dopad (součin riziko*dopad).

Opatření – aktivita, která umožňuje snížení míry rizika (1, s.16).

Zranitelnost – slabé místo aktiva (1, s.16).

1.2 Informační bezpečnost

Každá organizace pracuje s informacemi. Pro organizaci jsou informace hodnotná aktiva. Proto je potřeba informace chránit, především nyní, kdy se propojenost prostředí jednotlivých organizací zvyšuje. S tímto zvyšováním jsou informace ohroženy různými hrozbami a zranitelností (2, s.9).

Informace existují v různých formách, například napsány na papíře, řečeny při konverzaci, poslány poštou nebo uloženy v elektronické podobě (2, s.9).

Informační bezpečnost je zaměřena na velký výčet hrozeb. Zajišťuje tak kontinuitu činností organizace, maximalizuje návratnost investic a minimalizuje obchodní ztráty. Aby byly informace v bezpečí, je potřeba implementovat soustavu opatření, jako jsou například různá pravidla, organizační struktury, procedury, postupy a programové funkce (2, s.9).

Zavedení, zlepšování a podpora informační bezpečnosti může organizaci udržet konkurenceschopnou a ziskovou. Podpora informační bezpečnosti je také nutná pro udržení dobrého jména organizace (2, s.9).

Organizace a jejich informační systémy jsou čím dál více ohroženy bezpečnostními hrozbami, například sabotážemi, špionážemi a počítačovými podvody. Právě poslední zmíněná hrozba roste na množství, formou počítačových virů, útoků hackerů nebo útoku odepření služby (Denial of Service). Sofistikovanost a nebezpečnost těchto hrozeb se stále zvyšuje (2, s.9).

1.2.1 Kybernetická bezpečnost

I přes rozsáhlou problematiku se kybernetická bezpečnost dá definovat jako souhrn technických, právních, organizačních a vzdělávacích prostředků, které slouží k ochraně počítačových systémů a dalších aplikací, uživatelů, dat a prvků ICT. Je to schopnost počítačových systémů a jejich služeb včas reagovat na kybernetické útoky, hrozby a jejich následky, jakož i schopnost plánovat obnovu funkčnosti počítačových systémů a jejich služeb (3, s.44-45).

Kybernetická bezpečnost souvisí s každým, kdo používá jakékoliv informační nebo komunikační prvky. Pokud si uživatelé těchto prvků neuvědomí, že oni sami jsou klíčovým prvkem v kybernetické bezpečnosti, zvyšuje se tím pravděpodobnost úspěchu kybernetických útoků (3, s.40).

Kybernetická bezpečnost je oblast, která je pro mnoho organizací i jednotlivců stěžejní. Právě proto by měla být řešena dlouhodobě a systematicky. Je realizována v rámci kyberprostoru i mimo něj (3, s.40,45).

Abychom mohli uplatnit kybernetickou bezpečnost v praxi, musíme implementovat tzv. triády kybernetické bezpečnosti. Je možné využívat pouze triádu CIA, avšak pro udržení dostatečné úrovně kybernetické bezpečnosti je využívání pouze jedné triády nedostačující (3, s.45).

1.2.2 Triáda CIA

Triáda CIA patří mezi nejpoužívanější a nejznámější triádu kybernetické bezpečnosti. Triáda definuje principy používané k uplatňování kybernetické bezpečnosti. Písmena CIA odkazují na následující principy (3, s.45).

Confidentiality (Důvěrnost) – k prvkům ICT, datům a informacím mají mít přístup pouze autorizovaní uživatelé. Z důvodu velkého rozsahu zpracovávaných informací je vhodné zavést některou klasifikaci informací, např. klasifikaci informací v komerční sféře (chráněné, interní, citlivé, veřejné) (3, s.48-49).

Integrity (Integrita) – zásah do dat, informací a ICT je nemožné od neautorizovaných uživatelů. Jedná se o záruku neporušených dat, informací a systému (3, s.53).

Availability (Dostupnost) – garance možnosti přístupu k datům, informacím a ICT v okamžiku potřeby. Systém je nepoužitelný, pokud nezajišťuje spolehlivý přístup dle potřeby (3, s.54).

Obrázek č.1: Triáda CIA
(Zdroj: 4)

1.2.3 Prvky kybernetické bezpečnosti

Kybernetická bezpečnost se dá vytvořit pomocí vzájemné interakce těchto tří prvků.

Lidé – klíčový prvek jakékoliv bezpečnosti. Lidé se považují za nejslabší článek kybernetické bezpečnosti a jsou nejčastějším cílem útočníků (3, s.58).

Technologie – prostředek pro uživatele umožňující využívat různé aplikace a funkce dané užívanou technologií. Běžný uživatel používá pouze koncové prvky (mobilní telefon, PC) a nezajímá se o další technologické prvky nezbytné pro jeho fungování v kyberprostoru. Nejméně významný prvek (3, s.60-61).

Procesy – činnost, jež je nutná vynaložit, aby mohli lidé používat technologie a jejich služby. Jedná se o nejnáročnější část budování kybernetické bezpečnosti, z důvodu neustálé údržby a modifikace. Pro nalezení chyb v procesech se využívá penetrační testování (3, s.61-62).

1.2.4 Životní cyklus kybernetické bezpečnosti

Životní cyklus kybernetické bezpečnosti je definován třemi prvky.

- Prevence
- Detekce

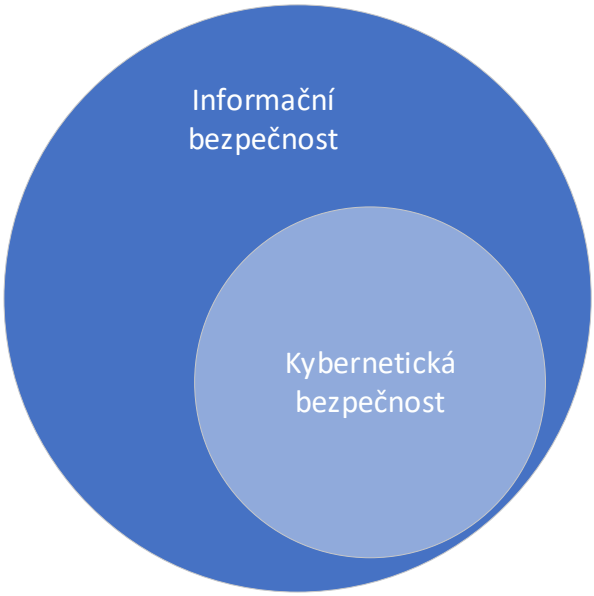
- Reakce

Obrázek č.2: Životní cyklus kybernetické bezpečnosti
(Zdroj: Vlastní zpracování dle 3, s.63)

Životní cyklus kybernetické bezpečnosti není nikdy dokončený proces. Jedná se o nekončící cyklus (3, s.64).

1.2.5 Informační bezpečnost a kybernetická bezpečnost

Tyto dva termíny bývají často zaměňovány a je jim přikládán stejný význam. Informační bezpečnost má za úkol chránit informace v jakékoliv formě (papír, e-mail, konverzace), kybernetická bezpečnost je pouze podmnožinou tohoto významu, chrání informace pouze v digitální podobě (5).



Obrázek č.3: Hierarchie informační a kybernetické bezpečnosti
(Zdroj: Vlastní zpracování dle 5)

Kybernetická bezpečnost se zabývá pouze úmyslnými útoky zvenčí organizace. Chrání a zajišťuje veškeré digitální informace, které jsou náchylné k hackingu, neoprávněnému přístupu a jiným formám útoků (6).

1.2.6 Systém řízení bezpečnosti informací (ISMS)

ISMS je řízení bezpečnosti informací se všemi vlastnostmi, které to obnáší. Je to součást řízení organizace, která je založená na přístupu k rizikům činností. Je zaměřena na ustanovení, zavádění, monitorování, provoz, údržbu, přezkoumání a zlepšování bezpečnosti informací (1, s.14,66).

Základem ISMS je model PDCA. Má čtyři etapy.

- Ustavení ISMS
- Zavádění a provoz ISMS
- Monitorování a přezkoumání ISMS
- Údržba a zlepšování

Ustavení ISMS

První etapa určuje rozsah a odpovědnost. Do této etapy patří následující procesy (1, s.14).

Řízení rizik (Risk Management) – koordinace potřebná ke kontrole a řízení organizace s ohledem na rizika (1, s.16).

Hodnocení rizik (Risk Assessment) – proces analýzy a zhodnocení rizik (1, s.16).

Analýza rizik (Risk Analysis) – systematické používání informací pro kalkulaci míry rizika a určení zdrojů těchto rizik (1, s.16).

Vyhodnocení rizika (Risk Evaluation) – proces porovnání odhadnutého rizika s určenými kritérii pro určení jeho významu (1, s.16).

Zvládání rizik (Risk Treatment) – proces výběru a přijetí opatření pro snížení rizika (1, s.16).

Akceptace rizika (Risk Acceptance) – rozhodnutí akceptovat riziko (1, s.16).

Prohlášení o aplikovatelnosti (Statement of Aplicability) – dokument s popisem opatření v ISMS organizace (1, s.16).

Zavádění a provoz ISMS

Druhá etapa pojednává o prosazení vybraných bezpečnostních opatření. I zde se nachází několik procesů a pojmů (1, s.14).

Účinnost bezpečnosti informací (Information Security Effectiveness) – rozsah bezpečnosti informací, které naplňují cíle organizace (1, s.16).

Míra (Measure) – ukazatel, který určuje informační potřebu (1, s.16).

Měření (Measurement) – proces určený k získání informací o účinnosti ISMS (1, s.16).

Záznam – dokument obsahující dosažený výsledek, nebo důkaz o činnosti řízení kvality (1, s.16).

Zavádění ISMS se ještě samo o sobě dělí na další čtyři etapy:

- Souhlas vedení organizace s nasazením systému
- Identifikace aktiv, jejich ocenění a analýza rizik
- Návrh opatření proti rizikům
- Certifikace ISMS (1, s.66-67)

Monitorování a přezkoumání ISMS

Třetí etapa slouží k zajištění zpětné vazby a hodnocení řízení. Níže jsou uvedené další pojmy a procesy spjaté s touto etapou (1, s.14).

Audit (Audit) – proces, který slouží k objektivnímu hodnocení podle stanovených kritérií. Je nezávislý, systematický a dokumentovaný (1, s.16).

Přezkoumání (Review) – proces sloužící k určení přiměřenosti, efektivity a vhodnosti předmětu přezkoumání k dosažení určených cílů (1, s.16).

Údržba a zlepšování ISMS

Čtvrtá a poslední etapa slouží k odstranění slabin a k soustavnému zlepšování. K této etapě patří další pojmy a procesy (1, s.14).

Neshoda (Nonconformity) – nesplnění požadavku (1, s.16).

Náprava (Correction) – opatření sloužící k odstranění neshody (1, s.16).

Opatření k nápravě (Correction Action) – slouží k odstranění příčiny neshody (1, s.16).

Preventivní opatření (Preventive Action) – slouží k odstranění potenciální neshody (1, s.17).

Řízení kontinuity organizace (Business Continuity Management) – poskytuje provozní a strategický rámec pro pohled na způsob, jakým organizace poskytuje služby a produkty a jak je odolná proti jejich ztrátě, zničení nebo narušení (1, s.17).

Systém řízení kontinuity organizace (Business Continuity Management System) – řídící proces, který identifikuje potenciální dopady ztrát. Cílem je vytvořit postupy a prostředí, které zajišťují obnovu klíčových činností a procesů organizace a kontinuitu na stanovené minimální úrovni, v případě ztráty nebo narušení (1, s.17).

1.3 Normy řady 27000

Poslední etapou zavádění ISMS je certifikace ISMS. Tato certifikace se provádí dle platných norem. Jejich podpora je obecná pro danou problematiku, nebo specifická podle oboru činnosti organizace (1, s.48).

„Respektování bezpečnostních norem znamená nezávislost na zařízení i dodavateli.“ (1, s.48)

Normy řady 27000 jsou rezervovány pro oblast informační bezpečnosti. Všechny standardy rodiny 27000 mají definovaná pravidla a strukturu (7).

1.3.1 ČSN ISO/IEC 27000

Poskytuje přehled systémů řízení bezpečnosti informací a definuje související termíny. Definice a termíny v této normě se týkají definic a termínů použitých v rodině norem ISMS, ne všech definic a termínů. Rodina ISMS norem pomáhá libovolně velkým a typově rozlišným organizacím zavést a provozovat ISMS systém (1, s.48).

Použitím rodiny norem ISMS mohou organizace vyvinout a implementovat rámec pro řízení bezpečnosti svých bezpečnostních aktiv a připravit ohodnocení svých ISMS, které se mohou týkat například duševního vlastnictví, finančních informací nebo informací o zaměstnancích (1, s.48).

Rodina ISMS norem obsahuje normy definující požadavky na ISMS, certifikace na takové požadavky, nebo normy poskytující přímou podporu (1, s.48).

První vydání bylo publikováno v roce 2009, momentálně nejnovější vydání je páté z roku 2018 (8).

1.3.2 ČSN ISO/IEC 27001

Norma ISO/IEC 27001 definuje doporučení k aplikaci ISO/IEC 27002 v rámci procesu ustavení, provozu, údržby a zlepšování ISMS v organizaci, která může díky normě definovat rozsah certifikovaného systému. Kritickým krokem při zavádění ISMS v organizaci, je správná definice ISMS. Norma byla původně publikována 15. října 2005, naposledy revidována byla 1. října 2013 (9).

Norma definuje adekvátní systém řízení, strukturu a procesy pro řízení bezpečnosti informací dle ISO/IEC 27002. Na základě hodnocení rizik z ISO/IEC 27002 mohou organizace nasadit ta správná opatření vhodná pro prostředí organizace. Hlavní části z ISO/IEC 27002 se z tohoto důvodu nacházejí v příloze normy ISO/IEC 27001 (9).

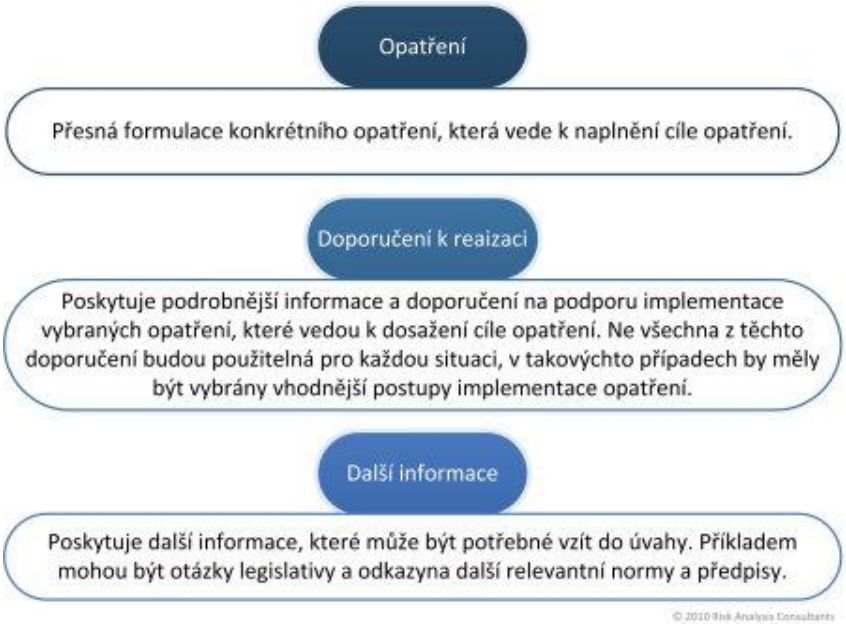
Norma využívá cyklus PDCA jako součást přístupu systému řízení k vývoji, implementaci a zdokonalování efektivnosti ISMS v organizaci (9).

1.3.3 ČSN ISO/IEC 27002

Norma ISO/IEC 27002 definuje nejvhodnější bezpečnostní praktiky a může být použita pro kontrolu správných kroků zajištění bezpečnosti informací v organizaci. Norma patří k mezinárodně přijatým standardům. ISO/IEC 27002 nepřikazuje opatření, které mají být v organizaci zavedeny, konečné rozhodnutí ponechává na organizaci, která by měla implementovat pouze ta opatření, nutná k implementaci (například dle hodnocení rizik). Aktuální verze normy pochází z roku 2013 (10).

ISO/IEC 27002 obsahuje 14 hlavních oddílů, které definují 35 kontrolních opatření pro ochranu informačních aktiv před narušením jejich integrity, důvěrnosti a dostupnosti. Cíle opatření patří mezi kvalitní základ pro budování bezpečnostní politiky v organizaci, avšak existují případy, ve kterých se opatření musí pozměnit, aby vyhovovala specifickým požadavkům organizace (10).

Nejnovější verze normy obsahuje 114 opatření, které se dále dělí na mnoho specifických opatření. Struktura je definována následovně (10).



Obrázek č.4: ČSN ISO/IEC 27002
(Zdroj: 10)

1.3.4 ČSN ISO/IEC 27003

Norma definuje návod k implementaci dalších norem z řady 27000. Původní norma byla publikována v únoru 2010, nejnovější revize v dubnu 2017 (11).

Norma může být používána organizací jakéhokoliv typu, která zavádí ISMS. Norma popisuje proces návrhu a implementace ISMS popisem zahájení, definování a plánování projektu implementace ISMS. Díky tomuto procesu získá organizace finální plán implementace projektu ISMS, ze kterého lze projekt realizovat (1, s.50).

Proces návrhu a implementace ISMS je definován v pěti etapách.

- Vedení organizace souhlasí se zahájením projektu ISMS
- Definice rozsahu, hranic a politiky ISMS
- Analýza požadavků bezpečnosti informací
- Hodnocení rizik a plánování zvládnutí rizik
- Návrh systému řízení bezpečnosti informací (1, s.50)

Dokončením poslední páté etapy získá organizace finální plán implementace projektu ISMS (1, s.50).

1.3.5 ČSN ISO/IEC 27004

ISO/IEC 27004 obsahuje doporučení pro vývoj a používání metrik a pro měření efektivity zavedeného ISMS. Zároveň měří efektivitu opatření, jak je uvedeno v ISO/IEC 27001 (1, s.51).

Norma zahrnuje procesy rozvoje měření a metrik, analýzy dat, provádění měření a hlášení výsledků měření. V příloze normy lze také najít příklady konceptů měření pro procesy ISMS nebo některá opatření (1, s.51).

První publikace byla vydána v prosinci 2009, aktuální vydání (druhé) bylo publikované v roce 2016 (12).

1.3.6 ČSN ISO/IEC 27005

Norma ISO/IEC 27005 obsahuje doporučení pro řízení rizik bezpečnosti informací. Norma je strukturovaná takovým způsobem, aby dostatečně podporovala implementaci informační bezpečnosti, která je založená na přístupu řízení rizik (1, s.51).

ISO/IEC 27005 nenabízí konkrétní metodiku pro řízení rizik, konečné rozhodnutí je na organizaci, která zvolí vhodný přístup, například vzhledem k rozsahu ISMS (1, s.51).

Činnosti řízení rizik definované normou:

- **Stanovení kontextu** – ohraničení základních kritérií, stanovení organizační struktury a definice hranic a rozsahu
- **Hodnocení rizik** – identifikování rizik, kvalitativní popis rizik nebo kvantifikace a prioritizace rizik na základě cílů hodnocení rizik
- **Zvládání rizik** – zvolení protiopatření ke snížení, podstoupení a vyhnutí se rizik a definice plánu zvládání rizik
- **Akceptace rizik** – rozhodnutí akceptace rizika a odpovědností za toto rozhodnutí
- **Seznámení s riziky** – sdílení a výměna informací o rizicích
- **Monitorování a přezkoumání rizik** – přezkoumání a monitorování rizik (13)

1.3.7 ČSN ISO/IEC 27006

Norma ISO/IEC 27006 stanovuje požadavky a doporučení pro orgány, které provádějí audit a certifikaci ISMS. Doplňuje tím požadavky obsažené v ISO/IEC 17021 a ISO/IEC 2001. Norma je především využívána k podpoře procesu akreditace certifikačních orgánů, které certifikují ISMS (1, s.51).

1.4 Kybernetická kriminalita a její formy

„Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.“ (14, s.57).

Kybernetická kriminalita (kyberkriminalita) se dá obecně definovat jako trestné jednání namířené proti počítači, nebo počítačové síti, případně jako jednání, při kterém je počítač používaný jako nástroj pro spáchání trestného činu (15, s.34).

Kybernetická kriminalita se projevuje kybernetickými útoky. Některé z nich jsou známé druhy protiprávního jednání (např. krádež, šikana a porušování autorských práv) přenesené do digitálního prostředí, další jsou ryze kybernetické (např. hacking, botnet a DDoS útoky) (15, s.181).

1.4.1 Sociální inženýrství

Sociální inženýrství je přesvědčování, manipulace a ovlivňování lidí za účelem donutit je provést určitou akci, nebo od nich získat informace, které by za normálních okolností neposkytli (15, s.186).

Sociální inženýrství nevyužívá ryze technické přístupy, hlavní myšlenkou je uvést oběť v omyl, ve kterém sama informace (nejčastěji heslo) dobrovolně prozradí. Jelikož nejslabším článkem bezpečnostního systému je člověk, jedná se o nejjednodušší formu kybernetického útoku (15, s.186).

Útoky jsou většinou vedeny třemi způsoby, které se navzájem kombinují:

- Sběr volně dostupných dat o cíli útoku
- Fyzický útok – útočník se snaží získat informace „zevnitř“ organizace, například prohledáváním odpadků v organizaci
- Psychologický útok (15, s.187-188)

Příklady nejčastějších metod útoků:

- Telefonický hovor
- Podvodný e-mail
- Prohledávání odpadků
- Zanechání paměťového média v zájmové oblasti (médium obsahuje malware)
- Prohledávání sociálních sítí nebo webu (veřejné informace zaměstnanců) (15, s.188)

1.4.2 Ransomware

Vyděračský malware, který brání uživateli používat počítačový systém do té doby, než dostane útočník zaplacené výkupné. Ransomware se nejčastěji dostane do počítače pomocí malware, který může být v příloze e-mailu, nebo umístěn na webové stránce (15, s.221).

Obecně se rozlišují dva typy ransomware:

- Omezení funkčnosti celého počítače, například zablokováním systémové obrazovky
- Systém je funkční, avšak data uživatele jsou uzamčena a znepřístupněna (15, s.221)

V současnosti je používanější druhý typ ransomware. Jeho účelem je zašifrovat pevný disk, nebo vybrané typy souborů, většinou obrázky, textové soubory, videa apod. Po dokončení šifrování se uživateli zobrazí zpráva o zašifrování jeho souborů, které může dešifrovat zaplacením určitého peněžního obnosu útočníkovi. K transakcím se většinou využívá kryptoměna, například Bitcoin (15, s.221).

Nejznámější ransomware v České republice i celosvětově je tzv. „policejní ransomware“. Uživatelům byl znemožněn přístup do operačního systému s oznámením, že počítač byl

zablokován policií daného státu, kvůli porušení práv. Dále byl uživatel vyzván k zaplacení požadované sumy peněz, pro odblokování počítače a ukončení falešného trestného řízení (15, s.222).

Obrázek č.5: Česká verze policejního ransomware
(Zdroj: 16)

1.4.3 Spam

Jedná se o hromadné šíření nevyžádaného sdělení, nejčastěji reklamního charakteru. Spam se šíří především pomocí elektronické komunikace (15, s.231).

Mezi nejpoužívanější elektronickou komunikaci pro šíření spamu se řadí:

- E-mail
- Různé aplikace pro zasílání zpráv (např. Messenger, Skype a Whatsapp)
- SMS
- Diskusní fóra (15, s.232)

Spam může obsahovat informace:

- Reklamní
- Finanční (např. nabídky půjček)
- Pornografické
- Hoax (řetězový dopis)

- Kriminální (např. zprávy obsahující malware) (15, s.232)

Spam může znemožnit veškerou elektronickou komunikaci zahlcením informační struktury. Tím snižuje důvěru společnosti v informační technologie (15, s.234).

Spam, který obsahuje kriminální nebo jiný podvodný obsah, se nazývá **scam**. Scamy v současnosti tvoří podstatnou část spamu a jejich účelem je, za použití sociálního inženýrství, získat důvěru uživatele a donutit ho vykonat požadované úkony (například navštívit zobrazené URL, nebo otevřít přílohu e-mailu) (15, s.235).

1.4.4 Phishing

Phishing je klamavé či podvodné jednání, jehož účelem je získat informace o uživateli (například heslo, číslo kreditní karty a PIN). Nejčastějším jednáním je nalákat uživatele k navštívení podvodné stránky (například falešné internetové bankovnictví) a vyplnění „přihlašovacích informací“. V některých případech jsou informace vyžadovány přímo ve zprávě (například formou dotazníku) (15, s.246).

Podstatou je využívání sociálního inženýrství. Virtuální prostředí umožňuje útočníkovi rozesílat podvodné zprávy velkému množství potenciálních obětí s minimem námahy. Phishing je primárně zaměřen na e-maily, sociální sítě, SMS a různé aplikace pro zasílání zpráv (např. Messenger, Skype a Whatsapp) (15, s.246-247).

1.5 General Data Protection Regulation (GDPR)

Obecné nařízení o ochraně osobních údajů (anglická zkratka GDPR) je významný mezinárodní právní dokument, který není primárně určený k oblasti ICT, ale s problematikou kybernetické bezpečnosti úzce souvisí (3, s.101).

GDPR představuje obecný právní rámec ochrany osobních údajů, který je platný a účinný v celé Evropské unii, v některých případech i mimo ni. Hlavním cílem tohoto nařízení je zajistit komplexní ochranu práv subjektů údajů proti neoprávněnému zacházení s jejich osobními údaji a daty. Dále například nastoluje rovnováhu mezi oprávněnými zájmy zpracovatelů, správců a subjektů údajů a vytváří systém jednotné vymahatelnosti práva a jednotného sankčního mechanismu v této oblasti (3, s.101).

GDPR se neuplatňuje pouze v EU, ale například i v případech, kdy provozovna správce nebo zpracovatele je v EU, i když zpracování v EU neprobíhá, nebo v případě, kdy správci nebo zpracovatelé nejsou usazení v EU, ale jejich služby nebo zboží jsou nabízeny subjektům údajů v EU, nebo je monitorováno chování subjektů údajů v EU (3, s.104).

1.6 Národní úřad pro kybernetickou bezpečnost (NÚKIB)

Národní úřad pro kybernetickou bezpečnost je ústřední správní orgán pro kybernetickou bezpečnost zahrnující kryptografickou ochranu a ochranu utajovaných informací v oblasti informačních a komunikačních systémů (17).

NÚKIB byl založen 1. srpna 2017 na základě zákona 205/2017 Sb. Tímto zákonem se zmaěnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Ředitel (momentálně Karel Řehka) se účastní jednání Bezpečnostní rady státu a je členem výboru pro kybernetickou bezpečnost (17).

Úřad je rozdělen na několik základních sekcí a odborů.

- Sekce provozně právní
- Sekce Národního centra kybernetické bezpečnosti (NCKB)
- Sekce informační bezpečnosti
- Odbor kabinet ředitele (OKŘ) (17)

1.7 Security Awareness Education (SAE)

SAE je program pro zvyšování bezpečnostního povědomí. Poskytuje pokyny pro budování a udržování komplexního bezpečnostního povědomí a školení jako součást IT bezpečnostního programu organizace. SAE je sestaven v životním cyklu, začínající designem, vývojem a implementováním programu pro zvyšování bezpečnostního povědomí a končící zhodnocením celého programu (18, s.1).

SAE také poskytuje pokyny pro IT bezpečnostní specialisty k identifikaci potřeb programu a jak plán školení vypracovat (18, s.1).

1.7.1 Modely pro budování bezpečnostního povědomí

Program SAE se v praxi dělí na tři základní modely, které se vybírají podle velikosti organizace, financí organizace a geografické lokace (18, s. ES-1).

- **Centralizovaný** – veškerá odpovědnost náleží centrální autoritě (například CIO a IT bezpečnostní programový manažer).
- **Částečně decentralizovaný** – školící politika a strategie náleží centrální autoritě, odpovědnost za implementaci je distribuovaná.
- **Plně decentralizovaný** – pouze odpovědnost za vytvoření bezpečnostních politik náleží centrální autoritě, všechny ostatní odpovědnosti jsou delegovány individuálním organizacím (18, s. ES-1).

1.7.2 Role a povinnosti

Nejprve je pro organizace důležité identifikovat role a povinnosti pro vytvoření a správu programu SAE.

Vrcholový management

Ředitel organizace, jednatel společnosti, nebo jiný typ vedoucího organizace, se musí ujistit, že má SAE v organizaci zajištěnou vysokou prioritu, aby byl plán efektivně vypracován. Hlava organizace by měla:

- najmout/určit CIO (Chief Information Officer)
- přidělit odpovědnost pro IT bezpečnostní tým
- ujistit se, že celá organizace využívá SAE, který je podporován potřebnými zdroji pro jeho efektivitu.
- ujistit se, že má organizace dostatečně vytrénovaný personál pro ochranu IT zdrojů (18, s. 3).

Chief Information Officer (CIO)

CIO má za úkol spravovat školení a dohlížet na personál. Má velkou odpovědnost za informační bezpečnost. Spolu s IT security program managerem má za úkol:

- určit celkovou strategii pro program SAE.
- ujistit se, že hlava organizace, senior manažeři, vlastníci dat a systémů a další rozumí konceptům a strategii programu SAE a jsou informování o stavu implementace programu.
- ujistit se, že je SAE dostatečně financován.
- zajistit zaškolení personálu organizace, kteří mají významné bezpečnostní odpovědnosti.
- ujistit se, že všichni uživatelé jsou dostatečně zaškoleni o svých bezpečnostních odpovědnostech.
- zajistit efektivní monitorování a hlášení o stavu programu SAE (18, s. 3-4).

Information Technology Security Program Manager

V jiné literatuře také jako CISO (Chief Information Officer). Dá se přeložit jako IT bezpečnostní programový manažer. Tato role zajišťuje taktickou odpovědnost za SAE. Povinnosti programového manažera jsou následující:

- ujistit se, že program SAE je vhodný a včasný pro zamýšlený personál.
- ujistit se, že SAE je efektivně nasazen pro zamýšlený personál.
- ujistit se, že uživatelé a manažeři mohou efektivně poskytnout zpětnou vazbu k SAE.
- ujistit se, že program SAE je pravidelně přezkoumáván a aktualizován, pokud nutno.
- asistovat při zřízení strategie monitorování a hlášení (18, s. 4).

Manažeři

Manažeři mají odpovědnost za kontrolu dodržování vytvořeného SAE plánu uživateli. Jejich role obnáší:

- spolupráce se CIO a IT bezpečnostním programovým manažerem s cílem seznámit se se společnými odpovědnostmi.
- slouží jako vlastník systému a/nebo dat, kde je to možné.
- uvažovat o vytváření individuálního plánu pro uživatele v rolích s významnou bezpečnostní odpovědností.

- ujistit se, že všichni uživatelé s přístupem k různým systémům znají své bezpečnostní odpovědnosti předtím, než mají povolený přístup.
- ujistit se, že uživatelé rozumí specifickým pravidlům používaných systémů a aplikací.
- pracují na omezení chyb od uživatelů z důvodu nedostatku bezpečnostního povědomí a/nebo školení (18, s. 4).

Uživatelé

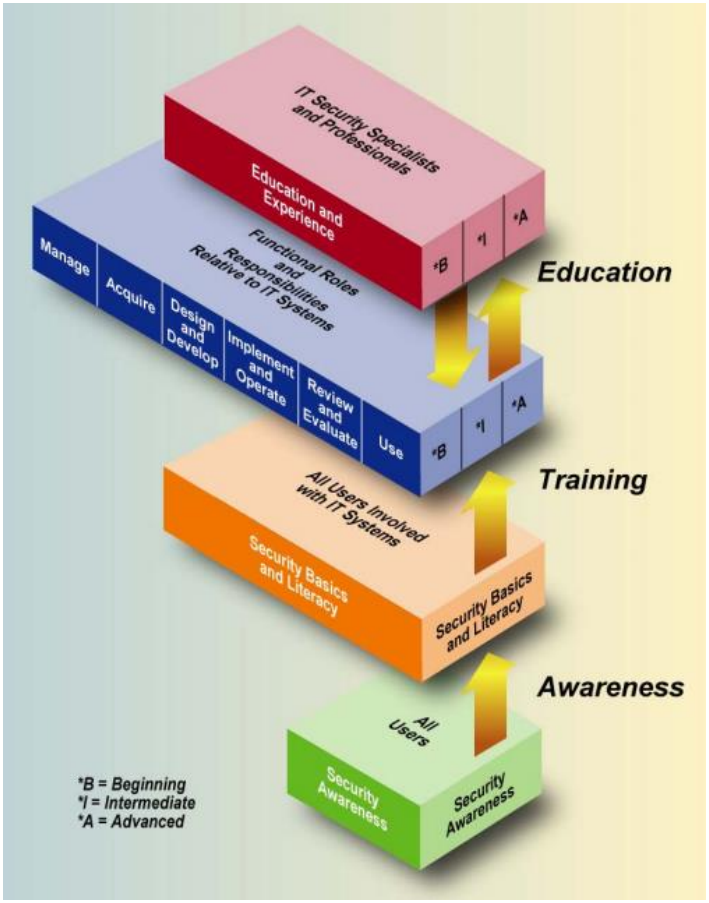
Uživatelé jsou největší skupinou v jakékoliv organizaci a jsou nejdůležitější skupinou lidí, která může poskytnout největší pomoc se snížením počtu neúmyslných chyb a IT slabin. Uživatelé mohou zahrnovat zaměstnance, externisty, domácí nebo zahraniční výzkumníky, návštěvníky, hosty a další. Uživatelé musí:

- pochopit a dodržovat organizační bezpečnostní politiku a procedury.
- být dostatečně zaškolení v pravidlech chování systémů a aplikací ke kterým mají přístup.
- spolupracovat s vedením ke splnění potřeb školení.
- aktualizovat software/aplikace bezpečnostními aktualizacemi.
- být seznámen s akcemi, které organizaci pomohou lépe chránit informace, například silným heslem, zálohou dat, řádnou antivirovou ochranou, nahlášením podezřelých indidentů, nebo porušením bezpečnostních pravidel a znát pravidla pro obranu proti sociálnímu inženýrství (18, s. 5).

1.7.3 Úrovně programu

Program SAE se dělí na tři fáze, povědomí, školení a vzdělávání. Fáze povědomí a školení jsou zásadními prostředky pro šíření bezpečnostních požadavků, které uživatelé, včetně manažerů, potřebují ke správnému konání své práce (18, s. 7).

Povědomí a školení vysvětlují správná pravidla chování pro používání systémů a informací organizace. Program zavádí bezpečnostní opatření a procedury které musejí být dodržovány. Program zároveň musí stanovit sankce za nedodržování těchto pravidel, uživatelé ale nejdřív musejí být informovaní o tom, co se od nich očekává (18, s. 7).



Obrázek č.6: Úrovně programu SAE

(Zdroj: 18, s. 8)

Povědomí

Smyslem této fáze je pouze zaměřit pozornost na informační bezpečnost. Fáze povědomí je určena pro jednotlivce k uvědomění si bezpečnostních obav a správných reakcí na tyto obavy. V této části SAE je školený uživatel v pasivní roli, pouze přijímá informace, nejčastěji pomocí audiovizuální prezentace. Ve fázi školení zastává už mnohem aktivnější roli. Fáze povědomí cílí na široké publikum pomocí atraktivních (obrazových, herních) technik, školení je více formální s cílem budování znalostí a zkušeností (19, s.15).

Prezentace k budování povědomí musejí být kreativní a motivující s cílem zaujmout posluchačovu pozornost po celou dobu prezentace. Pokud bude stimulus opakující, posluchač může ztratit pozornost. Prezentace by měla být krátká, specifická a bez zbytečných okolností. Školení zabere delší čas a vyžaduje větší zkušenosti (19, s.15).

Příkladem pro prezentaci o povědomí může být ochrana před počítačovými viry. Prezentace může obsahovat krátkou definici viru, co se může stát, když se virus v počítači nachází, co by měl uživatel dělat, aby systém ochránil a co by měl dělat, pokud virus objeví (18, s.9).

Níže je uvedený seznam dalších potenciálních témat na prezentaci o povědomí:

- Spam
- Phishing
- Správa a používání hesel
- E-maily od neznámých adresátů
- Sociální inženýrství
- Záloha dat
- Ochrana laptopu na cestách (18, s.24)

Školení

Tato fáze programu se zaměřuje na produkci relevantních a potřebných bezpečnostních dovedností a kompetenci pracovníků různých zaměření než IT (například management a auditování) (19, s.16).

Největší rozdíl mezi školením a povědomím je ten, že školení má za cíl naučit uživatele dovednosti, které jim dovolí praktikovat určitou funkci, ne pouze na problematiku upozornit. Dovednosti získané ve školení jsou postaveny na základech z fáze o povědomí. Školení nemusí nutně vést k získání formálního titulu z vysoké školy nebo jiné instituce, ačkoliv mnoho kurzů je odvozeno z materiálů vysokých škol (18, s.9).

Příklad školení může být IT bezpečnostní kurz pro systémové administrátory, ve kterém by měly být zmíněny řídící kontroly, operační kontroly a technické kontroly, které je potřeba implementovat.

Vzdělávání

Poslední fáze vzdělávání integruje všechny bezpečnostní dovednosti a kompetence do jednoho souboru znalostí a přidává různé studie konceptů, problémů a zásad. Tato fáze je určena především IT bezpečnostním specialistům (19, s.16).

V minulosti pouze hrstka organizací viděla potřebu zaměstnat bezpečnostní specialisty, ačkoliv pár organizací alespoň viděla potřebu v zavedení vzdělávacího bezpečnostního programu, nebo alespoň po zaměstnancích požadovala důkaz kvalifikace nebo certifikace v oblasti bezpečnosti (19, s.16).

Pozice bezpečnostního technika/specialisty/manažera je nyní tak technicky a manažersky komplexní, že je obtížné pozici úspěšně vykonávat. Obzvlášť nyní, kdy vedení organizace, zákazníci i technický personál vytvářejí tlak a požadavky na kreativní a užitečné řešení v rostoucím rozsahu bezpečnostních otázek. Důsledkem toho se specialisté IT bezpečnosti stále rychleji stávají nepostradatelným prvkem veřejných i soukromých organizací (19, s.16-17).

Ve fázi vzdělávání se studijní obsah stává rychle zastaralý důsledkem rychlého vývoje technologií. Vyškolený IT bezpečnostní specialista by měl mít komplexní přehled o oboru na takové úrovni, aby v takto měnícím se prostředí mohl dále prohlubovat své znalosti (19, s.17).

Na pokročilé úrovni IT bezpečnostní specializace, jako je například pozice IT bezpečnostního programového manažera, by měl být zaměstnanec schopen reprezentovat organizaci a aktivně a konstruktivně řešit vnitropodnikové problémy a obavy. Aby bylo možné dosáhnout takové úrovně, je potřeba dokončit formální vzdělání v bezpečnostním oboru, například pomocí školení, vysoké školy, či postgraduálního studia (19, s.17).

1.8 European Certification of Digital Literacy (ECDL)

ECDL je původem evropský projekt, který představuje celosvětově rozšířený certifikační a vzdělávací koncept zabývající se digitálními technologiemi. Nyní je koncept mezinárodně označován zkratkou ICDL (International Certification of Digital Literacy) (20).

ECDL pokrývá téměř všechny oblasti, ve kterých se digitální technologie v běžném životě využívají. ECDL nabízí velké množství certifikačních a vzdělávacích programů v oblasti digitálních kompetencí, od programů pro žáky základních a studenty středních škol, přes programy pro nezaměstnaně, zaměstnané nebo digitálně negramotné osoby až po programy určené pro odborníky z různých oborů (20).

Mezi nabízené certifikáty ECDL patří:

- **ECDL Start** – základní certifikát pro běžný život v prostředí digitálních technologií
- **ECDL Core** – certifikát dokazující digitální dovednosti potřebné pro vstup na trh práce
- **ECDL Profile** – univerzální certifikát pro libovolné studijní moduly (alespoň jeden úspěšně složený modul)
- **ECDL Advanced –** držitel certifikátu má profesionální uživatelské znalosti a dovednosti v oblasti uvedené na certifikátu a je plně připraven pro trh práce
- **ECDL Expert –** držitel certifikátu má profesionální uživatelské znalosti a dovednosti v oblasti nejpoužívanějších kancelářských aplikací a je plně připraven pro trh práce (20)

1.9 Program Evaluation and Review Technique (PERT)

Jedná se o standardní metodu síťové analýzy. Používá se k řízení složitých akcí, které mají stochastickou povahu. Doba trvání každé činnosti je chápána jako náhodná proměnná mající určité rozložení pravděpodobnosti (21).

Cílem modelu je uspořádat činnosti tak, aby byl zajištěný dohodnutý termín dokončení projektu s adekvátní mírou pravděpodobnosti. Doba trvání činnosti není přesně známá, je dána pouze s určitou pravděpodobností (21).

PERT se nejčastěji používá pro odhad doby trvání projektu, v praxi se tedy používá především při řízení projektu (21).

1.10 Lewinův model

Lewinův třífázový model změn se řadí mezi nejpoužívanější modely pro řízení změn v podniku. Autorem tohoto modelu je Kurt Lewin (22).

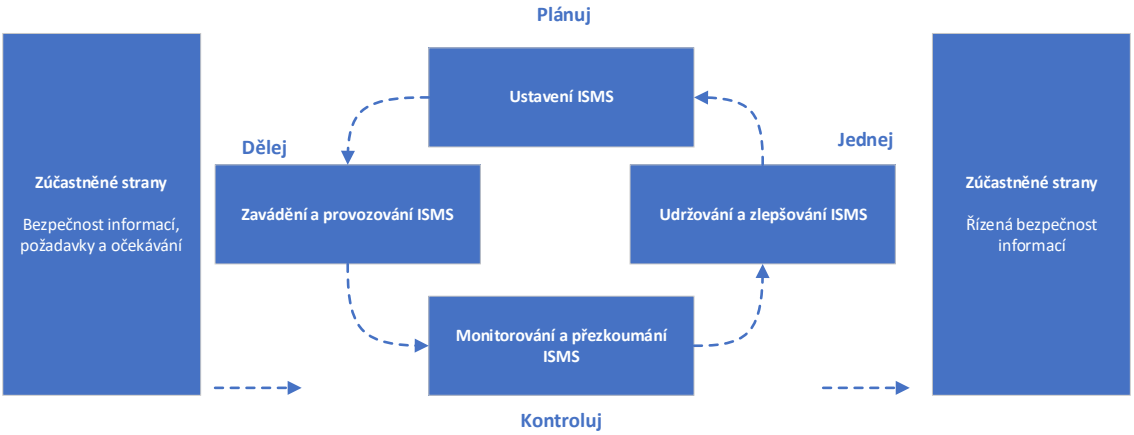
Mezi tři fáze modelu se řadí:

- **Rozmrazení** – nynější pravidla a způsoby myšlení jsou rozvolněny
- **Fáze změny** – navrhovaná změna proběhne, objevuje se nejistota a zmatenost
- **Zamrazení** – nová pravidla a způsoby myšlení jsou zafixovány v organizaci (22)

1.11 Cyklus PDCA

Cyklus PDCA slouží k postupnému zlepšování kvality, například služeb, výrobků a procesů. Tato metoda funguje pomocí opakovaného provádění čtyř základních činnosti (1, s.24).

- **Plan** (plánuj) – naplánování požadovaného zlepšení
- **Do** (dělej) – realizace plánu
- **Check** (kontroluj) – ověření výsledku oproti původnímu plánu
- **Act** (jednej) – úprava záměru a provedení na základě ověření a plošná implementace do praxe (1, s.24-25)



Obrázek č.7: Cyklus PDCA
(Zdroj: Vlastní zpracování dle 9)

PDCA je také potřeba dokumentovat v každé jeho etapě. Tato dokumentace je jedna z klíčových částí celého modelu. Procesy je potřeba identifikovat, popsat a zdokumentovat, řídit na základě vytvořené dokumentace, a nakonec optimalizovat jejich průběh (1, s.25).

2 ANALÝZA SOUČASNÉHO STAVU

Druhá kapitola pojednává o analýze současného stavu. Analýza zkoumá současnou situaci ve firmě, mezi kterou patří celkový popis společnosti a budovy, organizační struktura, hardwarové a softwarové vybavení společnosti a analýza zaměstnanců v oblasti bezpečnostního povědomí. Dále zjišťuje míru hrozeb, zranitelnosti aktiv a rizik, na jejichž základě je zjištěna potřeba zvýšení bezpečnostního povědomí ve společnosti.

2.1 Popis společnosti

Společnost XYZ je nadnárodní společnost obchodující se stavebními potřebami jako je beton, cement apod. Ve svém oboru patří k největším společnostem na světě. Sídlo společnosti je v Německu, avšak pobočky a dceřiné společnosti má všude po světě.

World Technical Hub je jedna z těchto dceřiných společnosti a je součástí této diplomové práce. Jedná se o podnik určený k poskytování IT služeb všem ostatním pobočkám, včetně té hlavní. Společnost se nachází v Brně a má přibližně 200 zaměstnanců, od administrativních pracovníků a personalistů až po odborníky na téměř všechna odvětví informačních technologií.

Společnost zaměstnává lidi mnoho různých národností, z důvodu poskytování IT podpory zaměstnancům v neanglicky mluvících zemích (Francie, Německo, Itálie a další). Kvůli této skutečnosti probíhá většina interní komunikace v anglickém jazyce.

Svou velikostí je společnost náchylná na různé typy sociálního inženýrství, spamu a DoS útoky (Denial of Service).

2.2 Popis budovy a místností

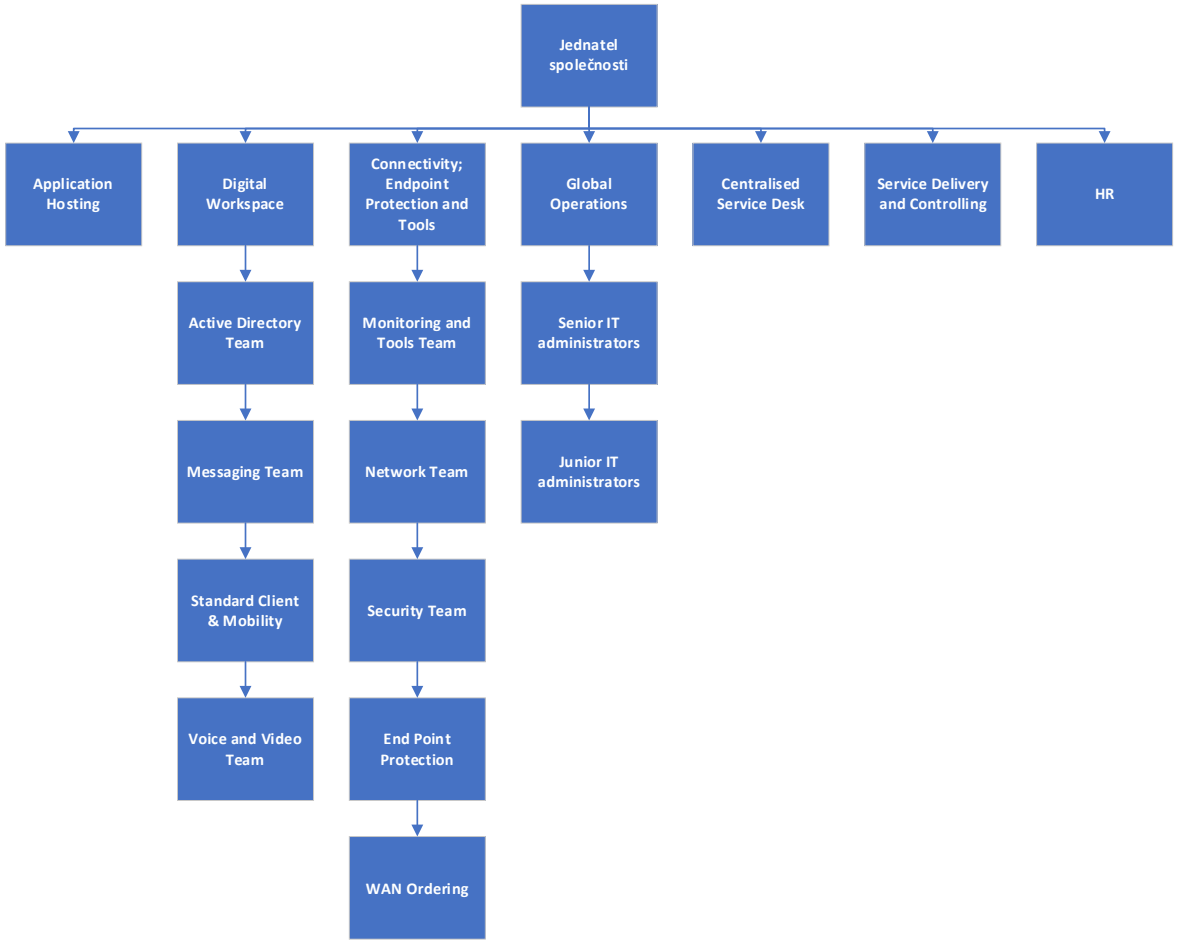
Kanceláře se nacházejí v nově postavené budově, kde každá společnost obsazuje jedno patro budovy. Vstup do budovy je chráněn turniketem, který se otevře pouze zaměstnaneckou kartou. U turniketu se také nachází recepce, na které se dá vyžádat návštěvnická karta. Ta je vydána pouze potom, co je host ohlášen společnosti, do které zamýšlí vstup.

Společnost sídlí v prvním patře. Zde jsou vstupní dveře, které jsou znovu chráněné proti neoprávněnému vstupu zaměstnaneckou kartou. Návštěvnická karta dveře neotevře. Hned za vstupem se nachází recepce. Drtivá většina prostoru jsou kanceláře ve stylu open space, výše postavení manažeři mají vlastní kanceláře, jednatel společnosti má největší.

Všechny prostory jsou opatřeny protipožárními hlásiči a požárními rozprašovači. Budova je nově postavená, majitel budovy dělá časté revize, riziko požáru je tedy nízké.

Dále se v prostoru nacházejí dvě kuchyně, dva páry toalet, velká terasa a odpočinková místnost s televizí a virtuální realitou, určená pro zaměstnance pracující na nočních směnách, kdy je nápor práce minimální.

2.3 Organizační struktura společnosti



Obrázek č.8: Organizační struktura společnosti

(Zdroj: Vlastní zpracování)

Organizační struktura je značně komplexní, společnost zaměstnává přibližně 200 lidí odlišných zaměření, většina z nich jsou různá odvětví informačních technologií. Společnost je rozdělena na různá oddělení, která mezi sebou spolupracují. Každé oddělení má svého vedoucího manažera a každý tým v oddělení svého týmového vedoucího.

Jednatel společnosti

Jednatel je logicky ředitelem celé organizace. Manažeři oddělení se zodpovídají přímo jemu. Jednateli se také zodpovídá několik menších týmů, jedním z nich je i security management team, který odpovídá za bezpečnostní politiky a směrnice. Tým také definuje a zajišťuje implementaci bezpečnostní strategie. Tento tým řídí CISO společnosti, který se zodpovídá právě řediteli.

Application Hosting

Toto oddělení zajišťuje virtualizaci, uložiště a zálohu dat, databáze, apod.

Digital Workspace

Oddělení spravuje digitální pracoviště, tudíž funkčnost e-mailů, zajištění přenosu videa a zvuku (například při online schůzkách), správu Active Directory atd.

Connectivity; Endpoint Protection and Tools

Oddělení se stará o správnou konektivitu, monitoring a softwarovou bezpečnost mezi jednotlivými zařízeními napříč všemi pobočkami.

Global Operations

Další oddělení se stará o podporu koncových uživatelů a ostatních oddělení. Na oddělení se posílají problémy a požadavky koncových uživatelů, které nedokážou vyřešit na service desku, nebo na ně nemají dostatečná práva. Oddělení se dělí na juniory, kteří řeší základní problémy každého odvětví a seniory, kteří jsou zaměření na jednu specifickou problematiku.

Centralised Service Desk

Centralizovaná podpora pro všechny kolegy z organizace. Poskytují základní podporu, pokud je problém příliš komplexní, posílá se na oddělení Global Operations. Oddělení je sestaveno ze zaměstnanců mnoha národností z důvodu znalosti cizích jazyků a dorozumění se s koncovým uživatelem.

Service Delivery and Controlling

Administrativní pracovníci.

HR

Personalisté.

2.4 Hardwarové a softwarové vybavení společnosti

Každý zaměstnanec má přidělený pracovní notebook. Stoly v open space kancelářích jsou tedy obsazeny pouze dvěma monitory, klávesnicí, myší a dokem pro notebook. Pokud si zaměstnanec notebook zapomene přinést, nemůže pracovat. Notebooky si zaměstnanci nosí domů, není doporučeno je nechávat ve firmě. Pokud se tak stane, je potřeba notebook uložit do zamykatelné zásuvky.

Ve společnosti se nachází i menší serverovny. Tyto místnosti jsou uzamčené a běžní zaměstnanci se do místnosti nedostanou.

Softwarové vybavení společnosti je značně velké, jelikož se jedná o společnost zabývající se správou IT zařízení. Většina směrovačů a přepínačů je zakoupena od společnosti Cisco, tudíž mnoho zaměstnanců pracuje s operačním systémem Cisco IOS.

Přístup k jednotlivému softwaru je také limitován podle oddělení. Celá společnost, včetně všech dalších poboček, využívá především produkty od společnosti Microsoft. Všechny notebooky používají operační systém Windows 10, drtivá většina všech serverů používá Windows Server edice. Každý zaměstnanec má přidělenou Office 365 licenci, která zahrnuje Microsoft Teams, který je používaný jako komunikační software napříč pobočkami, nebo Microsoft Outlook, který se také používá na všech pobočkách jako emailový klient. Dále má každý zaměstnanec svůj vlastní cloudový disk ve službě OneDrive.

Všichni zaměstnanci také používají lístkovací systém Cherwell, který je používaný jako systém pro sledování problémů. Pokud má zaměstnanec nějaký problém, nebo vyžaduje servisní zásah, zaznamená to do lístku v Cherwellu a lístek odešle na příslušné oddělení. Tam se lístek zpracuje.

2.5 Analýza zaměstnanců

Společnost World Technical Hub má velkou řadu zaměstnanců. Organizace je zaplněná především IT odborníky, ačkoliv zaměstnává i několik administrativních pracovníků a IT začátečníků, kteří nemusejí mít vysoké povědomí o bezpečnosti (například juniorní IT administrátoři, nebo IT podpora pro koncové uživatele).

Z důvodu velmi jednotvárného složení zaměstnanců se dělí pouze na čtyři základní skupiny:

- **Administrativní pracovníci** – žádné nebo malé bezpečnostní povědomí, pracovníci nemají přístup k serverům a používají základní softwarové vybavení.
- **Service Desk a junioři** – základní bezpečnostní povědomí, pracovníci mají omezený přístup k některým serverům a používají pokročilé softwarové vybavení.
- **IT specialisté a manažeři** – střední bezpečnostní povědomí, pracovníci mají plný přístup k většině serverům a používají pokročilé softwarové vybavení.
- **IT bezpečnostní technici** – vysoké bezpečnostní povědomí, pracovníci mají plný přístup k většině serverům a používají pokročilé softwarové vybavení.

Každá z těchto skupin zaměstnanců vyžaduje jinak definovaný rozsah a obsah školení.

2.6 Analýza informační bezpečnosti

Aby byl projekt zvýšení bezpečnostního povědomí podpořen daty, je potřeba provést analýzu informační bezpečnosti. Ohodnocení aktiv a pravděpodobnost hrozeb je provedeno dle mého subjektivního názoru s pomocí bezpečnostního specialisty ve firmě.

2.6.1 Klasifikace aktiv

První krok, k zajištění informační bezpečnosti firmy, je určení aktiv. Aktivum může být cokoliv, co má pro společnost nějakou hodnotu (data, hardware, software atd.). Každému aktivu se klasifikuje integrita, důvěrnost a dostupnost. Z těchto parametrů dále vyplyne celková váha.

Tabulka č.1: Legenda ke klasifikačním kritériím
(Zdroj: Vlastní zpracování)

Klasifikační stupeň	Klasifikační kritérium
1	Žádný dopad na organizaci
2	Zanedbatelný dopad na organizaci
3	Potíže či finanční ztráty
4	Vážné potíže či podstatné finanční ztráty
5	Existenční potíže organizace

Tabulka č.2: Ohodnocená aktiva
(Zdroj: Vlastní zpracování)

Aktivum	Integrita	Důvěrnost	Dostupnost	Váha
Hardwarové vybavení	-	-	-	-
Servery	4	5	5	5
Notebooky	3	3	3	3
Tiskárny	2	1	2	2
Aktivni prvky sítě	4	5	4	4
Pasivní prvky sítě	4	5	4	4
Softwarové vybavení	-	-	-	-
Operační systém	4	4	4	4
Licencovaný software	4	4	4	4
Data	-	-	-	-
Data o zaměstnancích	4	5	4	4
Interní data společnosti	5	5	4	5
Zálohovaná data	5	4	4	4

Smlouvy a jiné listiny	3	3	4	3
Služby	-	-	-	-
Elektřina	2	2	3	2
Připojení k internetu	3	3	4	3

Z tabulky výše vyplývá, že pro společnost jsou nejcennější interní data a servery. Jelikož se jedná o společnost poskytující IT podporu, jsou pro ni velmi cenné téměř veškeré hardwarové a softwarové vybavení, obzvlášť právě servery, kterých společnost vlastní více než 5000 (fyzických i virtuálních) všech různých zaměření po celém světě. Výpadkem několika serverů může být uživatelům zabráněn přístup k jednotlivým aplikacím, které jsou nezbytné pro správnou funkčnost organizace.

2.6.2 Analýza hrozeb

V analýze hrozeb se nachází výčet různých hrozeb od přírodních, až po lidské hrozby. Pravděpodobnost uskutečnění takové hrozby je uvedena v tabulce.

Tabulka č.3: Legenda k pravděpodobnosti hrozby
(Zdroj: Vlastní zpracování)

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

Tabulka č.4: Pravděpodobnost hrozby
(Zdroj: Vlastní zpracování)

Hrozba	**-**
Přírodní a fyzické hrozby	**Pravděpodobnost**
Požár	**2**
Přerušení dodávky elektřiny	**1**
Přerušení internetového připojení	**2**
Technické hrozby	**Pravděpodobnost**
Porucha IT komponent	**3**
Výpadek LAN sítě	**3**
Porucha požárního systému	**1**
Lidské chyby (úmyslné)	**Pravděpodobnost**
Odposlech	**2**
Hacking	**2**
Loupež	**3**
Smazání důležitých informací	**2**
Nepřátelský program	**2**
Zneužití důvěrných informací	**2**
Neoprávněný přístup k informacím	**2**
Neoprávněný přístup k aplikacím	**2**
Lidské chyby (neúmyslné)	**Pravděpodobnost**
Smazání dat	**2**
Porušení mlčenlivosti	**2**
Zanedbání práce	**2**

Neodborná práce	**1**
Nedostatečné bezpečnostní povědomí	**3**

Společnost je dobře zabezpečená proti různým hrozbám. Jelikož sídlí v nové budově uprostřed Brna, nemusí se bát přírodních ani fyzických hrozeb. Technické hrozby jsou více pravděpodobné, jelikož organizace vlastní mnoho IT komponent a spravuje mnoho LAN sítí. Proti úmyslným chybám je společnost taky dobře chráněna, největší nebezpečí spočívá v loupeži, jak fyzické (ve společnosti se nacházejí velmi drahá zařízení), tak kybernetické (například data). U neúmyslných chyb je největší pravděpodobnost nedostatečného bezpečnostního povědomí, což je důvod zpracování diplomové práce.

2.6.3 Analýza zranitelnosti aktiv

Zranitelnost aktiv se vypočítá sečtením pravděpodobnosti hrozby a hodnoty aktiva.

Tabulka č.5: Matice zranitelnosti
(Zdroj: Vlastní zpracování)

Matice zranitelnosti	**Pravděpodobnost**	**Servery**	**Notebooky**	**Tiskárny**	**Aktivní prvky sítě**	**Pasivní prvky sítě**	**Operační systém**	**Licencovaný software**	**Data o zaměstnancích**	**Interní data společnosti**	**Zálohovaná data**	**Smlouvy a jiné listiny**	**Elektřina**	**Připojení k internetu**
Hodnota aktiva	-	5	3	2	4	4	4	4	4	5	4	3	2	3
Přírodní a fyzické hrozby	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Požár	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Přerušení dodávky elektřiny	1	6	4	3	5	5	5	5	5	6	5	4	3	4
Přerušení internetového připojení	2	7	5	4	6	6	6	6	6	7	6	5	4	5

Technické hrozby	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Porucha IT komponent	3	8	6	5	7	7	7	7	7	8	7	6	5	6
Výpadek LAN sítě	3	8	6	5	7	7	7	7	7	8	7	6	5	6
Porucha požárního systému	1	6	4	3	5	5	5	5	5	6	5	4	3	4
Lidské chyby (úmyslné)	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Odposlech	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Hacking	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Loupež	3	8	6	5	7	7	7	7	7	8	7	6	5	6
Smazání důležitých informací	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Nepřátelský program	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Zneužití důvěrných informací	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Neoprávněný přístup k informacím	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Neoprávněný přístup k aplikacím	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Lidské chyby (neúmyslné)	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Smazání dat	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Porušení mlčenlivosti	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Zanedbání práce	2	7	5	4	6	6	6	6	6	7	6	5	4	5
Neodborná práce	1	6	4	3	5	5	5	5	5	6	5	4	3	4

Nedostatečné bezpečnostní povědomí	3	8	6	5	7	7	7	7	7	8	7	6	5	6
Celkem	-	134	96	77	115	115	115	115	115	134	115	96	77	96

Z tabulky vyplývá, že nejzranitelnějšími aktivy jsou servery a interní data společnosti, obzvlášť důsledkem loupeže, výpadku LAN sítě, poruše IT komponent a nedostatečnému bezpečnostnímu povědomí.

2.6.4 Analýza rizik

Matici pro analýzu rizik počítám pomocí vzorce:

Riziko = Pravděpodobnost hrozby * Hodnota aktiva * Zranitelnost

Tabulka č.6: Legenda k matici rizik
(Zdroj: Vlastní zpracování)

<40	Přijatelné riziko
40-80	Střední riziko
>80	Vysoké riziko

Tabulka č.7: Matice rizik
(Zdroj: Vlastní zpracování)

Matice rizik	**Pravděpodobnost**	**Servery**	**Notebooky**	**Tiskárny**	**Aktivní prvky sítě**	**Pasivní prvky sítě**	**Operační systém**	**Licencovaný software**	**Data o zaměstnancích**	**Interní data společnosti**	**Zálohovaná data**	**Smlouvy a jiné listiny**	**Elektřina**	**Připojení k internetu**
Hodnota aktiva	-	5	3	2	4	4	4	4	4	5	4	3	2	3
Přírodní a fyzické hrozby	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Požár	2	70	30	16	48	48	48	48	48	70	48	30	16	30

Přerušení dodávky elektřiny	1	30	12	6	20	20	20	20	20	30	20	12	6	12
Přerušení internetového připojení	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Technické hrozby	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Porucha IT komponent	3	120	54	30	84	84	84	84	84	120	84	54	30	54
Výpadek LAN sítě	3	120	54	30	84	84	84	84	84	120	84	54	30	54
Porucha požárního systému	1	30	12	6	20	20	20	20	20	30	20	12	6	12
Lidské chyby (úmyslné)	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Odposlech	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Hacking	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Loupež	3	120	54	30	84	84	84	84	84	120	84	54	30	54
Smazání důležitých informací	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Nepřátelský program	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Zneužití důvěrných informací	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Neoprávněný přístup k informacím	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Neoprávněný přístup k aplikacím	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Lidské chyby (neúmyslné)	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Smazání dat	2	70	30	16	48	48	48	48	48	70	48	30	16	30

Porušení mlčenlivosti	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Zanedbání práce	2	70	30	16	48	48	48	48	48	70	48	30	16	30
Neodborná práce	1	30	12	6	20	20	20	20	20	30	20	12	6	12
Nedostatečné bezpečnostní povědomí	3	120	54	30	84	84	84	84	84	120	84	54	30	54
Celkem	-	1410	612	330	972	972	972	972	972	1410	972	612	330	612

Podobně jako u analýzy zranitelnosti, i zde tabulka ukázala, že nejrizikovější jsou servery a interní data o společnosti. K vysoce rizikovým aktivům patří i hardwarové a softwarové vybavení společnosti, stejně jako zálohovaná data.

2.7 Požadavky bezpečnostního oddělení společnosti

Záměr diplomové práce je zvýšení bezpečnostního povědomí v analyzované společnosti. Bezpečnostní oddělení organizace tedy od diplomové práce požaduje zmenšení pravděpodobnosti rizik, způsobené nedostatečným bezpečnostním povědomím a loupeží (fyzické i softwarové). Snížení pravděpodobnosti rizik způsobené výpadkem LAN sítě a poruchou IT komponent má na starost oddělení Connectivity; Endpoint Protection and Tools, kteří se starají o funkčnost zařízení v organizaci. Tyto dvě témata jsou mimo rozsah diplomové práce.

2.8 Shrnutí analýzy

Analýza vyhodnotila servery a interní data o společnosti jako nejrizikovější a nejzranitelnější aktiva. Tato aktiva jsou ohrožena loupeží, poruchou IT komponent, výpadkem LAN sítě a nedostatečným bezpečnostním povědomím. Analýza také identifikovala typy zaměstnanců, pro které budou navrženy jednotlivé plány na zvýšení povědomí.

Diplomová práce se soustředí na snížení rizika z důvodu nedostatečného bezpečnostního povědomí. Zlepšením bezpečnostního povědomí se sníží i riziko loupeže, jelikož společnost je obzvlášť náchylná na loupeže kybernetického charakteru (phishing, ransomware apod.). Také se sníží riziko fyzické loupeže, pokud zaměstnanci budou, po absolvování bezpečnostního školení, více dbát na podezřelé osoby snažící se proniknout do prostor společnosti.

Zvýšením bezpečnostního povědomí se také sníží zranitelnost serverů, které mohou být se znalostí přihlašovacích údajů vypnuty, nebo jinak zneužity. Zranitelnost interních dat se rovněž sníží, jelikož jsou většinou uloženy v digitální podobě na některém serveru. Zranitelnost ostatních aktiv bude také snížena, jelikož se většinou jedná o aktiva softwarového typu, která jsou nejvíce ohrožena právě nedostatečným povědomím.

3 VLASTNÍ NÁVRH ŘEŠENÍ

Na základě analýzy byla zjištěna potřeba zvýšení bezpečnostního povědomí, které výrazně sníží míru rizika, způsobenou nedostatečným bezpečnostním povědomím, a zranitelnost některých aktiv, která jsou také ovlivněna tímto nedostatkem.

Zvýšení bezpečnostního povědomí je možné vyřešit systematickým a trvalým vzděláváním. V organizaci je tedy nutné navrhnout systém vzdělávání vhodný pro všechny skupiny zaměstnanců.

Navrhuji využít program SAE, který je jako systém vzdělávání v oblasti informační bezpečnosti nejpoužívanějším. Návrhová část se tedy zabývá řízením projektu, jehož cílem je vytvořit přínosný SAE plán pro celou organizaci. Veškeré návrhy programu by měly být v souladu s normami řady ISO 27000.

3.1 Cíl programu SAE

Analýza odhalila vysoká rizika spojená s nedostatečným bezpečnostním povědomím. Tato rizika se týkala především serverů a interních dat společnosti. Rizika se dají významně snížit pomocí poskytnutí základní bezpečnostní gramotnosti těm nejméně bezpečnostně znalým zaměstnancům (administrativní pracovníci), prohloubení bezpečnostního povědomí řadových uživatelů ve firmě (service desk, junioři, IT specialisté a manažeři) a konstantní vzdělávání těch nejpokročilejších uživatelů (IT bezpečnostní specialisté).

Cílem programu je posílit bezpečnostní povědomí zaměstnanců ve společnosti a tím snížit pravděpodobnost výskytu rizik. Programu se účastní všechny skupiny zaměstnanců ve firmě, plán programu navrhuji podle jejich dovedností a potřebných znalostí.

3.2 Přínosy programu SAE

Mezi přínosy programu se řadí předejití úspěšných fyzických nebo kybernetických krádeží interních dat, lepší bezpečnostní gramotnost zaměstnanců, která je vhodná i v osobním životě a menší pracovní vytíženost bezpečnostních specialistů, kteří musí případné bezpečnostní hrozby eliminovat.

3.3 Plán programu SAE

Celý projekt návrhu, implementace a post-implementace programu SAE by měl být důkladně naplánován a časově ohodnocen. Pro schválení a vymezení celé změny navrhuji použít Lewinův model, pro časové zhodnocení metodu PERT.

3.3.1 Lewinův model

První fáze Lewiova modelu je rozmrazení, do které se řadí analýza silového pole a definování agenta a sponzora změny.

Druhá fáze je změna, ve které se definuje postupný plán realizace změny.

Třetí fáze je zamrazení, jak budeme úspěšnost změny sledovat.

Analýza silového pole

Analýza silového pole určuje síly inicializující proces změny, síly působící pro změnu a síly působící proti změně. Analýza silového pole se určuje ve dvou škálách:

- +1 až +10 (síly působící pro změnu)
- -1 až -10 (síly působící proti změně)

Jako síly inicializující proces změny se považuje podnik samotný. Zvýšení bezpečnostního povědomí je ve společnosti důležitým tématem. Většina zaměstnanců má administrátorský přístup ke komunikační infrastruktuře podniku. Neúmyslným prozrazením přihlašovacích údajů takového zaměstnance může útočník získat přístup k citlivým informacím, které by vážně ohrozily integritu společnosti, například jejich smazáním nebo zveřejněním.

Síly působící pro změnu:

- Nižší riziko kybernetické a fyzické loupeže (+8)
- Vyšší bezpečnostní gramotnost zaměstnanců (+5)
- Menší pracovní vytíženost bezpečnostního oddělení (+5)

Síly působící proti změně:

- Plánování a realizace komplexního projektu (-6)
- Méně času zaměstnanců na hlavní pracovní náplň (-3)

Celkově vycházejí síly na hodnotě +9, tudíž změnu je možné realizovat.

Agent a sponzor změny

Agentem změny jsou CISO a jeho bezpečnostní tým. Budou se starat o návrh, implementaci (spolu s manažery oddělení) i post-implementaci celého programu. Budou zpracovávat studijní materiály a v určité fázi programu přednášet probíraná témata. Na konci programu také budou sbírat a zpracovávat celkovou zpětnou vazbu.

Sponzorem změny je jednatel společnosti, který celý projekt financuje. Jednatel také bude muset o plánovaném projektu informovat vedení mateřské společnosti ke schválení a uvolnění finančních prostředků.

Realizace změny

Proces realizace změny navrhuji rozdělit do několika činností:

1) Schválení projektu
2) Určení cíle programu
3) Určení rozsahu programu
4) Definování rolí a odpovědností
5) Vytvoření skupin uživatelů
6) Návrh fází programu
7) Externí školení ve fázi vzdělávání
8) Vytvoření videí pro fázi povědomí
9) Vytvoření studijních materiálů pro fázi školení
10) Implementace programu
11) Vytvoření post-implementační dokumentace
12) Vyhodnocení zpětné vazby
13) Aktualizace studijních materiálů
14) Vyhodnocení projektu

Sledování úspěšné implementace změny

Úspěšnost implementace změny bude vyhodnocena na základě zpětné vazby od účastníků programu. Pokud se nevyskytnou významné problémy při realizaci změny a zpětná vazba bude pozitivní, dá se změna považovat za úspěšnou.

Proces zpětné vazby je popsán v kapitole 3.9.1.

3.3.2 Metoda PERT

Pro použití metody je nejdříve potřeba vytvořit tabulku s jednotlivými činnostmi a časově ji ohodnotit. Po vytvoření tabulky je nutné vytvořit síťový graf s označenou kritickou cestou. Časové ohodnocení navrhuji s ohledem na další pracovní vytížení zaměstnanců. Projektu nemohou věnovat celý den, proto některé činnosti trvají déle, než by ve skutečnosti měly.

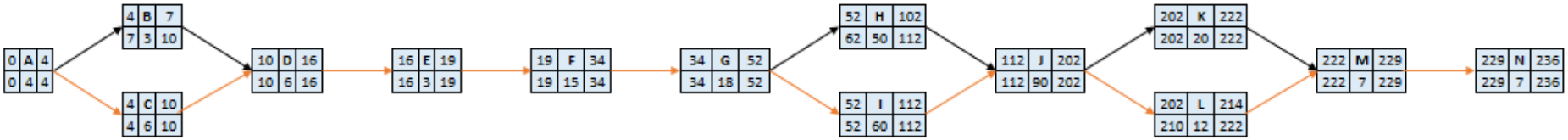
Před vytvořením tabulky je potřeba definovat zkratky, které jsou v ní obsažené:

- **i** – předchozí činnost
- **j** – nadcházející činnost
- **a** – optimistická doba trvání
- **m** – realistická doba trvání
- **b** – pesimistická doba trvání
- $\mathbf{t_{(i,j)}}$ – deterministický model
- **ZM** – začátek možný
- **KM** – konec možný
- **ZP** – začátek přípustný
- **KP** – konec přípustný
- **RC** – celková rezerva

Tabulka č.8: Tabulka činností

(Zdroj: Vlastní zpracování)

Údaje o postupnosti činností projektu				Trvání (dny)				Termíny zahájení a ukončení činností				Rezerva
Činnost	Popis činnosti	i	j	a	m	b	$t_{(ij)}$	ZM	KM	ZP	KP	RC
A	Schválení projektu	-	B, C	2	4	6	4	0	4	0	4	0
B	Určení cíle programu	A	D	2	3	4	3	4	7	7	10	3
C	Určení rozsahu programu	A	D	4	6	8	6	4	10	4	10	0
D	Definování rolí a odpovědností	B, C	E	4	6	8	6	10	16	10	16	0
E	Vytvoření skupin uživatelů	D	F	2	3	4	3	16	19	16	19	0
F	Návrh fází programu	E	G	12	15	18	15	19	34	19	34	0
G	Externí školení ve fázi vzdělávání	F	H, I	14	18	22	18	34	52	34	52	0
H	Vytvoření videí pro fázi povědomí	G	J	40	50	60	50	52	102	62	112	10
I	Vytvoření studijních materiálů pro fázi školení	G	J	50	60	70	60	52	112	52	112	0
J	Implementace programu	H, I	K, L	70	90	110	90	112	202	112	202	0
K	Vytvoření post-implementační dokumentace	J	M	15	20	25	20	202	222	202	222	0
L	Vyhodnocení zpětné vazby	J	M	10	12	14	12	202	214	210	222	8
M	Aktualizace studijních materiálů	K, L	N	5	7	9	7	222	229	222	229	0
N	Vyhodnocení projektu	M	-	6	7	8	7	229	236	229	236	0



Obrázek č.9: Síťový graf

(Zdroj: Vlastní zpracování)

Zhodnocení metody PERT

Celková doba projektu vyšla na 236 dní. Doba projektu je adekvátní z důvodu sekundární priority projektu před hlavní náplní pracovního dne. Kritická cesta leží na činnostech A-C-D-E-F-G-I-J-K-M-N. V síťovém grafu je kritická cesta označená červenou barvou.

3.4 Role a odpovědnosti v programu SAE

Program SAE navrhuji vytvořit podle částečně decentralizovaného modelu z důvodu velikosti společnosti a její značně rozvinuté organizační struktuře. Ve společnosti se nachází čtyři typy osob, které budou dohlížet na různé fáze programu SAE.

Tabulka č.9: Role a odpovědnosti v programu SAE
(Zdroj: Vlastní zpracování)

	Činnosti													
Osoba	Schválení projektu	Určení cíle programu	Určení rozsahu programu	Definování rolí a odpovědností	Vytvoření skupin uživatelů	Návrh fází programu	Externí školení ve fázi vzdělávání	Vytvoření videí pro fázi povědomí	Vytvoření studijních materiálů pro fázi školení	Implementace programu	Vytvoření post-implementační dokumentace	Vyhodnocení zpětné vazby	Aktualizace studijních materiálů	Vyhodnocení projektu
Jednatel														
CISO														
Manažeři oddělení														
Uživatelé														

3.4.1 Jednatel společnosti

Jednatel společnosti bude dohlížet na celý program a bude ho konzultovat spolu s CISO. Jeho role je spíše kontrolní, po konzultaci cílů a rozsahu programu přenechává veškerou

zodpovědnost CISO a pouze kontroluje, jestli projekt postupuje dle plánu. Po implementaci a vyhodnocení zpětné vazby programu zhodnotí, jestli má program smysl a rozhodne o jeho dalším pokračování. Jednatel společnosti ve společnosti funguje také jako CIO.

3.4.2 CISO

CISO bude mít hlavní zodpovědnost za celý program a bude se podílet na všech jeho fázích. CISO navrhne a vytvoří program SAE pro definované skupiny zaměstnanců a bude školit manažery o správné implementaci programu dle jejich potřebných dovedností. Po implementaci bude sbírat vyhodnocení zpětné vazby programu od manažerů a podá celkové vyhodnocení jednateli společnosti.

CISO bude delegovat některé své povinnosti na bezpečnostní specialisty ve svém týmu.

3.4.3 Manažeři oddělení

Manažeři budou zodpovědní za implementaci a kontrolu plánu SAE v rámci svého oddělení. Po absolvování programu sbírají zpětnou vazbu od podřízených, kterou vyhodnotí a pošlou nadřazené osobě v programu (CISO). Manažeři by se měli programu účastnit také.

3.4.4 Uživatelé

Uživatelé jsou nejdůležitější skupinou v rámci programu. Jedná se o skupinu, která se programu bude účastnit a která poskytne zpětnou vazbu, nutnou pro vyhodnocení funkčnosti a užitečnosti programu. Mezi uživatele se řadí všichni zaměstnanci, včetně manažerů a bezpečnostních specialistů.

3.5 Rozdělení uživatelů

Uživatele navrhuji rozdělit podle úrovně bezpečnostního povědomí:

- Žádné nebo malé bezpečnostní povědomí

- Základní až střední bezpečnostní povědomí
- Vysoké bezpečnostní povědomí

Uživatelé jsou do těchto kategorií roztříděni podle svoji pracovní pozice. Administrativní pracovník má ve většině případech mnohem menší bezpečnostní povědomí než IT specialista s mnoholetými zkušenostmi. Také vyžaduje menší bezpečnostní povědomí, než uživatel s přístupem ke komunikační infrastruktuře podniku.

Podle úrovně bezpečnostního povědomí navrhuji uživatele zařadit do příslušné fáze programu (povědomí, školení, vzdělávání).

Tabulka č.10: Zařazení do fáze programu
(Zdroj: Vlastní zpracování)

Bezpečnostní povědomí	Povědomí	Školení	Vzdělávání
Žádné nebo malé			
Základní až střední			
Vysoké			

3.6 Fáze programu SAE

SAE obsahuje tři fáze, každá z nich má rozdílné cíle a výstupy. Každé fáze se také účastní určitá skupina uživatelů.

3.6.1 Povědomí

Oblast povědomí je první fází programu. Slouží pro základní pochopení informační bezpečnosti a rozpoznání obecných bezpečnostních rizik. Uživatelé by po absolvování této fáze také měli vědět, jak správně na tato rizika reagovat. Této fáze se účastní všichni uživatelé v organizaci, kromě IT bezpečnostních specialistů (skupina vysokého bezpečnostního povědomí), jejichž znalosti daleko přesahují úroveň povědomí.

Fázi povědomí je zapotřebí vytvořit zábavnou a lehce zapamatovatelnou formou. Zde navrhuji využít podnikový e-learning, kde by se nacházela zpracovaná videa na různá témata informační bezpečnosti. Videa budou maximálně deset minut dlouhá a budou vysvětlovat pouze základní témata bezpečnosti, mezi která mohou patřit:

- Sociální inženýrství
- Spam
- Hesla
- Ransomware

Videa nevyžadují téměř žádnou interakci od uživatele, tudíž pokud budou dostatečně zábavná, měla by udržet uživatelovu pozornost. Také by neměla být příliš odborná, aby se uživatel v problematice vyznal.

Videa není těžké vytvořit, tudíž by je mohl zpracovat CISO s pomocí Voice and Video týmu v podniku, ostatních bezpečnostních specialistů, nebo některých manažerů. Pokud by CISO měl dovednosti ve vytváření videí, mohl by je zpracovat sám, avšak pro zkrácení projektového času navrhuji zapojit celé bezpečnostní oddělení.

Po zhlédnutí všech videí bude uživatelům odemčen krátký kvíz na zpracovaná témata. Podle správně zodpovězených odpovědí uživatelé obdrží slovní hodnocení. Manažer oddělení a CISO by pomocí kvízu získal zpětnou vazbu o úspěšnosti fáze programu.

Noví zaměstnanci, kromě nových bezpečnostních specialistů, budou mít povinnost videa zhlédnout a složit závěrečný kvíz.

3.6.2 Školení

Fáze školení se zaměřuje na získání dovedností v oblasti informační bezpečnosti. Navazuje na znalosti získané z předchozí fáze, tudíž fáze školení musí začít bezprostředně po fázi povědomí.

Uživatelé by po absolvování školení měli získat potřebné znalosti v oblasti bezpečnosti. Této fáze se zúčastní všichni uživatelé ve skupině základního až středního bezpečnostního povědomí.

Pro školení navrhuji využít dva studijní moduly od organizace ECDL. Jako přidanou hodnotu by účastníci školení měli možnost získat certifikát ECDL Profile, pro který stačí složit zkoušku pouze z jednoho modulu.

Modul 1 - Ochrana osobních údajů

První modul se bude zabývat ochranou osobních údajů, konkrétně nařízení GDPR. Po absolvování tohoto modulu by měl uživatel rozumět zásadám, důvodům, rozsahu a cílům GDPR. Uživatel by měl znát svá práva jako subjekt údajů. V případě narušení bezpečnosti údajů by měl umět vyřešit důsledky porušení GDPR (23).

Nařízení GDPR mnoho zaměstnanců nechápe, z důvodu jeho komplexnosti. Přitom GDPR se týká mnoho údajů, které zaměstnanec podniku poskytuje. Absolvování modelu zvýší bezpečnostní povědomí zaměstnanců v oblasti osobních dat, které jsou zahrnuty v rizikových interních datech společnosti.

Modul 2 - Bezpečné používání informačních technologií

Druhý modul bude zaměřený na základní principy bezpečného používání počítačů a internetu. Absolvováním modulu získá zaměstnanec znalost principů bezpečného používání informačních a komunikačních technologií a schopnosti zabezpečit datová média, počítačovou síť nebo počítače před škodlivými programy (23).

Tento modul je nejpodstatnější, jelikož se přímo týká kybernetické bezpečnosti a všech spjatých pojmů. Po absolvování modulu by měl mít zaměstnanec rozsáhlé znalosti ochrany proti různým formám kybernetické kriminality, čehož je potřeba školením dosáhnout především.

Jelikož se nejedná o komplikované moduly, navrhuji, aby CISO zpracoval materiály na školení sám, pomocí navrhované literatury a předepsaného sylabu jednotlivých modulů. Se zpracováním materiálů mohou pomoci ostatní bezpečnostní specialisté. Studijní materiály pro modul bezpečného používání informačních technologií je na webu ECDL zdarma k dispozici, stejně jako doporučená literatura pro další moduly. Vlastním zpracováním materiálů také firma ušetří náklady na externí školitele.

Navrhuji zpracované studijní materiály vystavit na e-learning organizace pro všechny zaměstnance. CISO a ostatní bezpečnostní specialisté mohou pomocí komunikačního softwaru Teams uspořádat několik přednášek na navrhované moduly, vycházet mohou právě z vypracovaných materiálů.

Po absolvování přednášek navrhuji, aby zaměstnanci podstoupili závěrečný test z vybraných modulů, který by znovu vypracoval CISO s asistencí ostatních bezpečnostních specialistů. Pro získání certifikátu ECDL Profile je zapotřebí vykonat test v akreditovaném testovacím středisku. Pokud by zaměstnanci měli zájem, mohli by podstoupit tento test namísto interního a získat oficiální certifikát. Po vyhodnocení testu CISO získá zpětnou vazbu o úspěšnosti fáze.

Jelikož informační bezpečnost není hlavní pracovní náplní školících skupin, neměl by být test příliš složitý a čas na přípravu k testu by měl být dlouhý.

Noví zaměstnanci budou povinni se fáze účastnit v momentě, kdy se bude plán SAE opakovat.

3.6.3 Vzdělávání

Vzdělávání je poslední fáze programu SAE. Tato fáze je určená pouze pro zaměstnance s vysokým bezpečnostním povědomím. Do této skupiny se řadí pouze IT bezpečnostní technici (včetně CISO). Jelikož se jedná o zaměstnance, kteří mají nejvyšší bezpečnostní povědomí ve firmě, je potřeba, aby byli školení externími školiteli.

Fáze vzdělávání je velmi podstatná. Pokud CISO a bezpečnostní technici nebudou konstantně vzdělávaní v oblasti bezpečnosti, budou i vytvořené materiály pro zaměstnance ve zbylých dvou fázích zastaralé a nepoužitelné.

Navrhuji, aby fáze vzdělávání proběhla jako první. Fáze se účastní bezpečnostní specialisté, kteří vytvářejí studijní materiály pro zbylé dvě fáze. Je tedy nutné, aby jejich znalosti byly při vytváření materiálů co největší, nejobsáhlejší a nejaktuálnější.

Noví bezpečnostní specialisté se fáze účastní v momentě, kdy se bude plán SAE opakovat.

Následující společnosti se zabývají návrhem školení pro společnosti.

OKSystem

OKSystem je školící centrum sídlící v Praze. Učebny má společnost v Praze i v Brně. Organizace se soustřeďuje na školení v oblasti IT profesionálů a projektového řízení.

OKSystem nabízí čtyři typy školení o IT bezpečnosti:

- Pravidla IT bezpečnosti pro zaměstnance
- Principy kryptografie
- Úvod do zabezpečení datových sítí
- Linux – bezpečnost a zabezpečení

Všechny školení probíhají v Praze, kromě úvodu do zabezpečení datových sítí, které probíhá i online. Společnost také nabízí mnoho bezpečnostních kurzů v oblasti Cisco technologií, které analyzovaný podnik využívá.

GoPas

GoPas je počítačová škola zaměřená na nabídku školení IT bezpečnosti. Škola nabízí obrovské množství bezpečnostních kurzů, od oblasti GDPR až po oblast hackingu. Škola se také řadí mezi největší poskytovatele IT bezpečnostních kurzů v České republice. Kurzy probíhají v Praze a Brně, online i prezenčně.

Amenit

Školící centrum Amenit nabízí spoustu kurzů v oblasti informačních technologiích, včetně bezpečnosti. Bezpečnostních kurzů je znovu několik, probíhají online, nebo prezenčně v Novém Jičíně.

Z uvedených možností navrhuji využít školení od společnosti GoPas. Svou velikostí a počtem klientů je ověřena kvalita poskytnutých školení. Počet bezpečnostních kurzů je zde obrovský, tudíž je možné vybrat přímo potřebné kurzy, které by se měly týkat GDPR, hackingu, zranitelnosti webových aplikací apod. Společnost také na svých serverech používá především operační systémy Windows Server 2016 a 2019. Navrhuji tedy do školení zařadit i správu bezpečnosti těchto serverů. Důraz by měl být kladen na aktuální a budoucí bezpečnostní hrozby.

Jelikož se GoPas nachází v Brně, mohly by školení probíhat přímo na pobočce, nebo online. Pro lepší časovou flexibilitu a pohodlí navrhuji školení uspořádat online.

Níže se nachází seznam vybraných kurzů pro školení. Kurzy jsou seřazeny postupně.

- GDPR - technické a procesní požadavky a kybernetický zákon
- Network Security – Hacking v praxi
- Testování bezpečnosti webových aplikací
- Windows Server 2019/2016 - správa bezpečnosti
- Bezpečnostní povědomí zaměstnance – pravidelné přezkoušení

3.7 Témata videí pro fázi podvědomí

Fáze podvědomí je jediná fáze, kde školící materiály nebudou odvozeny od jiné literatury, ani nebudou školeny externí firmou. V následující kapitole navrhuji několik témat vhodných pro zpracování do výukových videí. Témata byla vybrána podle potřebných dovedností.

3.7.1 Hesla

Ve společnosti je kladen velký důraz na dostatečně silná hesla. Navrhuji, aby jedno z videí tuto problematiku vysvětlilo dopodrobna. Společnost využívá heslovou politiku u administrátorských i běžných účtů, ale i přes tyto politiky je možné nastavit slabé heslo.

Video by mělo vysvětlit pravidla heslové politiky, tj. malé a velké písmeno, minimální počet znaků a číslo. Ve videu by mělo být zdůrazněné, jak je důležité dodržovat tuto politiku, například ukázkou rychlého prolomení slabého hesla.

Je potřebné, aby bylo heslo důvěrné a nikde zveřejněné. Heslo by tedy nemělo být nikde napsané a uživatel by si ho měl pouze pamatovat. Na to by měl být ve videu také kladen důraz.

3.7.2 Sociální inženýrství

Druhé video navrhuji zaměřit na sociální inženýrství a jeho nejčastější formy, mezi které patří například phishing. Je důležité, aby uživatelé uměli rozeznat různé typy sociálního inženýringu, a tak dokázali identifikovat bezpečnostní rizika. Ve videu by měl být také kladen důraz na rozeznání podezřelých jedinců, kteří se snaží fyzicky proniknout do podniku.

Pro vysvětlení problematiky navrhuji využít co nejvíce praktických ukázek úspěšného sociálního inženýrství. Na internetu lze nalézt spoustu takových případů, jako například spear phishing útok na společnost Sony. Praktické příklady jsou zajímavější a udrží tak posluchačovu pozornost lépe.

3.7.3 Malware a viry

Třetí video navrhuji obsáhnout problematikou malwarů a virů. Ve videu budou znovu zobrazeny různé formy malwarů a co mohou v počítači způsobit.

Nejznámější typ malwaru posledních let je ransomware. Zde navrhuji zobrazit praktické příklady, které se stali i v České republice, jako například policejní ransomware.

3.7.4 Kyberbezpečnost v osobním životě

Čtvrté video navrhuji zaměřit na důležitost kyberbezpečnosti v osobním životě. Důraz bude kladen na dodržování kyberbezpečnosti nejen v zaměstnání, ale i v osobním životě, co se týče například ochrany dětí na sociálních sítí, což je téma, o kterém se díky dokumentu „V síti“ začalo hojně diskutovat.

Když si uživatelé uvědomí, že se kyberbezpečnost týká i jejich osobního života, začnou klást důraz na kyberbezpečnost i v místě zaměstnání.

3.8 Studijní materiály pro fázi školení

Studijní materiály pro fázi školení si bude společnost vytvářet sama. Studijní materiály nebudou příliš rozsáhlé, jelikož navrhuji vyučovat pouze dva moduly ECDL.

3.8.1 E-learning ECDL SPŠE V Úžlabině

SPŠE v Úžlabině nabízí pro všechny zájemce zdarma e-learning, kde se nachází studijní materiály pro několik modulů, včetně potřebného modulu „Bezpečné používání informačních technologií“. Odkaz na stránku lze nalézt přímo na webu ECDL, tudíž materiály jsou ověřené.

Na stránkách se také nachází video návody a různé testy k procvičení. Studijní materiály je možné nahrát na podnikový e-learning, avšak navrhuji zaměstnancům pouze poskytnout odkaz na školní e-learning, kde vše najdou sami. Přednášky pro tento modul mohou vycházet z těchto studijních materiálů.

Obrázek č.10: Ukázka e-learningu SPŠE v Úžlabině
(Zdroj: 24)

3.8.2 Doporučená literatura pro druhý modul

Druhý modul není obsažený ve školním e-learningu. Studijní materiály navrhuji vytvořit z knih a webových stránek zabývajících se tématem ochrany osobních údajů a přípravy na ECDL testy. Materiály je potřeba vytvořit dle zveřejněného sylabu modulu „Ochrana osobních údajů“.

Doporučená literatura:

- ECDL: Průvodce přípravou na testy (ISBN: 978-80-251-3144-2)
- GDPR v kostce (ISBN: 978-80-7400-704-0)
- Webová stránka www.gdpr.cz

Správně ocitované studijní materiály navrhuji umístit na podnikový e-learning.

3.9 Post-implementace

Post-implementace je poslední fází projektu. Jedná se o významnou část, díky které lze vyhodnotit celkový přínos a úspěšnost projektu ze získané zpětné vazby. Post-implementace také definuje četnost opakování včetně aktualizování materiálů a post-implementační dokumentaci.

3.9.1 Zpětná vazba

Zpětnou vazbu navrhuji vyhodnotit na základě vypracovaných testů z fáze povědomí a školení. Pokud většina zaměstnanců složí test alespoň se 70% úspěšností, dá se považovat fáze za úspěšnou. Také navrhuji zaměstnancům poskytnout dotazník spokojenosti s kurzem, ve kterém by jako ve škole známkovali různé aspekty programu a byli by dotázáni, co by v programu zlepšili.

Zpětná vazba z fáze vzdělávání by měla být především o spokojenosti účastníků s vybranou externí zaškolovací společností. Pokud by většina byla spokojena, externí firma by byla znovu oslovena i při dalším opakování fáze.

Zpětnou vazbu vysbírají manažeři oddělení, kteří ji zkompletují a pošlou CISO vyhodnocení programu za svoje oddělení. CISO udělá ze zpětné vazby všech oddělení kompletní zprávu, kterou podá jednateli společnosti. Zpráva bude obsahovat jak úspěšnost testů, tak i spokojenost účastníků s programem.

3.9.2 Dokumentace

Jelikož se bude program v určitém intervalu opakovat, je potřeba archivovat výsledky všech testů, jednotlivé zpětné vazby oddělení a celkovou zprávu podanou jednateli společnosti.

Díky archivaci je možné zpětně porovnat úspěšnost programu a zjistit, jestli případné aktualizace studijních materiálů, změny témat videí, nebo jiné změny, byly úspěšně

přijaty. Po vydání aktualizovaných studijních materiálů navrhuji archivovat původní materiály, pokud by ty aktualizované byly nedostatečné, či jinak nevyhovující.

Pokud se zaměstnanci účastní akreditované zkoušky na certifikát ECDL Profile, je potřeba, aby kopie certifikátu byla také archivovaná. Kromě certifikátu navrhuji veškerou dokumentaci uchovávat v digitální formě.

Navrhuji, aby archivaci mělo na starost HR oddělení organizace, které archivuje i další dokumenty.

3.9.3 Četnost opakování včetně aktualizace materiálů

Program SAE je nekončící životní cyklus, tudíž opakování školení je nedílnou součástí. Fázi vzdělávání bezpečnostních specialistů navrhuji opakovat každý rok, z důvodu neustále se vyvíjejících technik v oblasti informační bezpečnosti. Znalosti bezpečnostních specialistů by tedy měly být vždy aktuální se současnou dobou. Studijní materiály navrhuji aktualizovat jednou ročně, nebo dle potřeby.

Fáze povědomí a školení rovněž navrhuji opakovat každý rok, z důvodu časté výměny zaměstnanců na pracovních pozicích. Opakování programu, včetně aktualizace studijních materiálu, by mělo časově vyjít na významně kratší dobu než při první implementaci z důvodu nabytých zkušeností a hotovým návrhem fází.

3.10 Finanční zhodnocení

Finanční zhodnocení se týká především dvou aspektů:

- CISO a bezpečnostní tým navrhující program
- Externí školitel pro fázi vzdělávání (GoPas)

Jelikož CISO s asistencí navrhuje, zpracovává i vyučuje jednotlivá témata v oblasti povědomí i školení, dá se jejich mzda po čas celého projektu považovat za významný výdaj. CISO vede další tři bezpečnostní specialisty, celkově jsou tedy ve společnosti čtyři bezpečnostní specialisté.

Pro výpočet mzdy jsem použil průměrný plat bezpečnostního specialisty v Jihomoravském kraji, 60 000 Kč měsíčně. Celkový projekt trvá 236 dní, necelých osm měsíců.

Navrhnutý školitel GoPas určený pro fázi vzdělávání bezpečnostních specialistů (včetně CISO) je dalším nutným výdajem.

Tabulka č.11: Stručný rozpočet
(Zdroj: Vlastní zpracování)

Mzda bezpečnostních specialistů po dobu projektu	**Cena**
CISO a bezpečnostní specialisté	1 920 000 Kč
Bezpečnostní kurzy společnosti GoPas	**Cena (bez DPH)**
GDPR - technické a procesní požadavky a kybernetický zákon	54 400 Kč
Network Security – Hacking v praxi	138 000 Kč
Testování bezpečnosti webových aplikací	124 000 Kč
Windows Server 2019/2016 - správa bezpečnosti	114 000 Kč
Bezpečnostní povědomí zaměstnance - pravidelné přezkoušení	18 000 Kč
Celkem	**2 368 400 Kč**

Celková částka za celý projekt činí 2 368 400 Kč. Drtivou část nákladů obsahují mzdy bezpečnostních specialistů, které by společnost vyplácela i při neexistenci projektu. Bezpečnostní kurzy jsou tedy jediné náklady, které se objevují čistě z existence projektu. Tyto náklady činí 448 400 Kč.

ZÁVĚR

Cílem diplomové práce je zvýšit bezpečnostní povědomí ve společnosti World Technical Hub. Pomocí analýzy byla zjištěna potřeba zvýšit bezpečnostní povědomí k omezení míry rizika a zranitelnosti aktiv. Pro zvýšení bezpečnostního povědomí jsem navrhl využít program SAE, který je k tomuto účelu určen. Celý projekt návrhu, implementace a post-implementace programu byl naplánován a časově ohodnocen. Pomocí analýzy zaměstnanců jsem navrhl tři skupiny zaměstnanců dle jejich bezpečnostních dovedností. Následně jsem tyto skupiny zařadil do jednotlivých fází programu podle požadované úrovně dovedností, které by měli z určité fáze získat.

Pro všechny tři fáze jsem navrhl obsah a rozsah probíraných témat, včetně doporučení, kde studijní materiály získat, či jak je vytvořit.

Po implementaci programu následuje post-implementace. Všechny výstupy z programu musí být řádně dokumentovány a program navrhuji opakovat alespoň jednou ročně. Pomocí zpětné vazby z výstupů programu jednatel společnosti zjistí, zda byl projekt úspěšný, či nikoliv. Opakování zavedeného projektu již nebude tolik časově náročné.

Na závěr jsem celý projekt finančně zhodnotil. Náklady za projekt nejsou příliš vysoké, pokud se odečtou mzdy bezpečnostních specialistů, které by byly vypláceny i při neexistenci projektu. Jelikož se společnost zabývá informačními technologiemi, které jsou pro ně kriticky důležité, je investice do bezpečnosti významnou položkou.

Pokud bude program úspěšný, dal by se s menšími úpravami využít i v organizacích podobného zaměření.

SEZNAM POUŽITÝCH ZDROJŮ

1. ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.
2. ČSN ISO/IEC 17799 Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací. Český normalizační institut, 2006.
3. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.
4. Comtact: What is the CIA triad? [online]. 2019 [cit. 2021-5-6]. Dostupné z: https://comtact.co.uk/blog/what-is-the-cia-triad/
5. Clever and Smart: Informační bezpečnost vs. kybernetická bezpečnost [online]. 2014 [cit. 2021-5-6]. Dostupné z: https://www.cleverandsmart.cz/information-security-vs-cybersecurity/
6. SecurityScorecard: Cybersecurity vs Information Security: What's the difference? [online]. 2020 [cit. 2021-5-6]. Dostupné z: https://securityscorecard.com/blog/information-security-versus-cybersecurity
7. Risk Analysis Consultants: Řada norem ISO/IEC 27000 [online]. [cit. 2021-5-6]. Dostupné z: https://www.rac.cz/cs/rada-norem-iso-iec-27000/
8. Risk Analysis Consultants: ISO/IEC 27000:2018 [online]. [cit. 2021-5-6]. Dostupné z: https://www.rac.cz/cs/iso-iec-27000/
9. Risk Analysis Consultants: ISO/IEC 27001:2013 [online]. [cit. 2021-5-6]. Dostupné z: https://www.rac.cz/cs/iso-27001
10. Risk Analysis Consultants: ISO/IEC 27002:2013 [online]. [cit. 2021-5-6]. Dostupné z: https://www.rac.cz/cs/iso-iec-27002/
11. Risk Analysis Consultants: ISO/IEC 27003:2017 [online]. [cit. 2021-5-6]. Dostupné z: https://www.rac.cz/cs/iso-iec-27003/
12. Risk Analysis Consultants: ISO/IEC 27004:2016 [online]. [cit. 2021-5-6]. Dostupné z: https://www.rac.cz/cs/iso-iec-27004/

13. Risk Analysis Consultants: ISO/IEC 27005:2018 – standard pro analýzu informačních rizik [online]. [cit. 2021-5-6]. Dostupné z: https://www.rac.cz/cs/iso-iec-27005/
14. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti. Praha: Policejní akademie ČR v Praze, 2012. ISBN 978-80-7251-378-9.
15. KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.
16. Comfor: Šifrovací viry – co je to Ransomware a jak se bránit? [online]. 2018 [cit. 2021-5-6]. Dostupné z: https://www.comfor.cz/blog/sifrovaci-viry-%E2%80%93-co-je-to-ransomware-a-jak-se-bran
17. Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 2021-5-6]. Dostupné z: https://www.nukib.cz/cs/
18. NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program. Washington: U.S. Government Printing Office, 2003.
19. NIST Special Publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model. Washington: U.S. Government Printing Office, 1998.
20. ECDL Czech Republic [online]. [cit. 2021-5-6]. Dostupné z: https://www.ecdl.cz/
21. Managementmania.cz: Metoda PERT (Program Evaluation and Review Technique) [online]. [cit. 2021-5-6]. Dostupné z: https://managementmania.com/cs/metoda-pert
22. Managementmania.cz: Lewinův třífázový model změn (Lewin's Three-Stage Model of Change) [online]. [cit. 2021-5-6]. Dostupné z: https://managementmania.com/cs/lewinuv-trifazovy-model-zmen
23. ECDL Czech Republic: Standardní moduly ECDL / ICDL [online]. [cit. 2021-5-6]. Dostupné z: https://www.ecdl.cz/sylaby_standard.php
24. SPŠE v Úžlabině: Modul 12: Bezpečné využívání informačních a komunikačních technologií [online]. [cit. 2021-5-6]. Dostupné z: https://ecdl.uzlabina.cz/M12/

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM ZKRATEK

CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CISO	Chief Security Information Officer
ČSN	Česká soustava norem
DDoS	Distributed Denial of Service
DoS	Denial of Service
ECDL	European Certification of Digital Literacy
EU	Evropská unie
GDPR	General Data Protection Regulation
HR	Human Resources
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISMS	Information Security Management Systém
ISO	International Organization for Standardization
IT	Informační technologie
LAN	Local Area Network
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PC	Personal Computer
PDCA	Plan-Do-Check-Act
PERT	Program Evaluation and Review Technique
PIN	Personal Identification Number
SAE	Security Awareness Education
SMS	Short Message Service
SPŠE	Střední průmyslová škola elektrotechnická
URL	Uniform Resource Locator